Кузнецова Елена Анатольевна
Подписан: Кузнецова Елена Анатольевна
DN: OU=Директор, O=МБОУ СШ №3 г.Котово, CN=Кузнецова Елена Анатольевна, E=msoch33@yandex.ru
Основание: я подтверждаю этот документ
Местоположение: Котово
Дата: 2026.10.19 17:30:09+04'00'
Foxit Reader Версия: 10.1.0

Муниципальное бюджетное общеобразовательное учреждение
«Средняя школа № 3 с углубленным изучением отдельных предметов г. Котово»
Котовского муниципального района Волгоградской области

РАССМОТРЕНО	СОГЛАСОВАНО	УТВЕРЖДЕНО
на заседании педагогического совета МБОУ СШ №3 г. Котово Протокол №1 от 27.08.2026 г.	Заместитель директора по УВР _____Е.П. Кузнецова 28.08.2026 г.	Директор МБОУ СШ №3 г. Котово _____Е.А. Кузнецова Приказ от 28.08.2026 г. №131

РАБОЧАЯ ПРОГРАММА

курса дополнительного образования «Кибербезопасность»
для учащихся 9 класса
Уровень образования ООО

(68 часов)
2026-2027 учебный год

Составитель:
Белошапкина Елена Вячеславовна,
учитель математики и информатики

Котово, 2026

Пояснительная записка

Программа дополнительного образования «Кибербезопасность» для 9 класса разработана с учётом требований федеральных государственных образовательных стандартов основного общего образования и ориентирована на формирование у обучающихся компетенций безопасного и ответственного поведения в цифровой среде. Актуальность программы обусловлена стремительным расширением цифрового пространства, в котором современный подросток проводит значительную часть учебного и свободного времени: образование, общение, развлечения и потребление информации всё больше перемещаются в онлайн-формат. В этих условиях отсутствие базовых навыков кибергигиены создаёт реальные риски для личной безопасности, психологического благополучия и финансовой защищённости несовершеннолетних и их семей.

Программа носит практико-ориентированный характер. Значительная часть учебного времени отводится на освоение прикладных приёмов защиты устройств, настройки приватности, распознавания фишинга и социальной инженерии, анализа правовых ситуаций. Курс способствует развитию критического мышления, формированию устойчивости к манипулятивному воздействию и воспитанию цифровой этики. Программа адресована обучающимся 9 класса (14–15 лет) и не требует предварительной подготовки сверх базового курса информатики.

Цель программы: формирование у обучающихся системы знаний, умений и навыков в области кибербезопасности, обеспечивающих безопасную и ответственную жизнедеятельность в современной информационной среде.

Задачи программы:

- сформировать представление об основных видах киберугроз и механизмах их реализации;
- освоить практические приёмы защиты персональных данных, устройств и сетевых подключений;
- развить навыки распознавания социальной инженерии, фишинга и мошеннических схем;
- сформировать установку на ответственное цифровое поведение и соблюдение этических норм онлайн-коммуникации;
- ознакомить с правовыми нормами Российской Федерации в сфере информационной безопасности и защиты информации;

- способствовать развитию критического мышления при работе с цифровым контентом.

Нормативно-правовые основания разработки программы:

- Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»;
- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- 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 № 152-ФЗ «О персональных данных»;
- Концепция информационной безопасности детей, утверждённая Правительством РФ;
- Приказ Минпросвещения России от 25.08.2026 № 591 «Об утверждении федерального перечня электронных образовательных ресурсов, допущенных к использованию при реализации имеющих государственную аккредитацию образовательных программ начального общего, основного общего, среднего общего образования».

Содержание обучения

1. Введение в кибербезопасность (2 ч)
Теоретические сведения. Понятия «кибербезопасность», «информационная безопасность», «киберугроза», «уязвимость», «киберинцидент». Место кибербезопасности в системе современного знания. Актуальность темы для школьников: рост числа цифровых сервисов, увеличение объёма персональных данных в сети, распространённость мошенничества. Классификация угроз: технические, социально-психологические (социальная инженерия), правовые. Краткий обзор содержания курса и правил работы на занятиях.
Практическая деятельность. Дискуссия «С какими киберугрозами я уже сталкивался». Составление «карты угроз» для подростка. Входная диагностика (беседа, анкетирование).
Ключевые понятия: кибербезопасность, киберугроза, уязвимость, киберинцидент.

2. Персональные данные и цифровой след (4 ч)
Теоретические сведения. Понятие персональных данных. Категории персональных данных (общие, специальные, биометрические). Что относится к персональным данным школьника: ФИО, дата рождения, адрес, номер телефона, фотографии, геолокация, биометрия. Цифровой след: активный и пассивный. Как формируется цифровой след (соцсети, поисковые запросы, покупки, геометки). Риски неосторожной публикации информации: мошенничество, буллинг, кража личности. Основы

законодательства о персональных данных (ознакомительно): права субъекта персональных данных, согласие на обработку.
Практическая деятельность. Анализ собственного цифрового следа (по чек-листу). Упражнение «Что можно и что нельзя публиковать». Разбор ситуаций: последствия избыточной публичности. Составление памятки «Мои персональные данные под защитой».
Ключевые понятия: персональные данные, цифровой след, активный и пассивный след, согласие на обработку, кража личности.

---

3. Пароли и аутентификация (6 ч)
Теоретические сведения. Понятия «пароль», «аутентификация», «авторизация», «учётная запись». Принципы создания надёжных паролей: длина, сложность, уникальность, регулярная смена. Типичные ошибки: использование одного пароля для разных сервисов, личные данные в пароле, простые последовательности. Двухфакторная аутентификация: виды (SMS, приложение-аутентификатор, аппаратные ключи), преимущества и ограничения. Менеджеры паролей: принцип работы, обзор популярных решений, правила безопасного использования. Восстановление доступа: контрольные вопросы, резервные коды, привязанный номер телефона и почта. Как происходит взлом аккаунтов (подбор, утечки, фишинг) и как его предотвратить.
Практическая деятельность. Практикум «Создаём надёжный пароль» (оценка стойкости паролей по критериям). Упражнение «Настройка двухфакторной аутентификации» (на учебных аккаунтах). Знакомство с менеджером паролей (демонстрация, настройка). Разбор сценариев восстановления доступа. Составление личной стратегии управления паролями.
Ключевые понятия: пароль, аутентификация, авторизация, двухфакторная аутентификация, менеджер паролей, учётная запись, взлом аккаунта.

4. Фишинг и социальная инженерия (8 ч)
Теоретические сведения. Понятие фишинга. Виды фишинга: массовый, целевой (spear-phishing), вишинг (телефонный), смишинг (SMS), фарминг, клонирование сайтов. Признаки фишинговых сообщений: подозрительный адрес отправителя, срочность, угрозы, ошибки в тексте, странные ссылки и вложения, запрос конфиденциальных данных. Социальная инженерия: определение, психологические приёмы (авторитет, срочность, доверие, любопытство, страх, выгода). Телефонное мошенничество: типичные сценарии («служба безопасности банка», «родственник в беде», «выигрыш», «оплата доставки»). Правила безопасного поведения при подозрительных контактах.
Практическая деятельность. Практикум «Разбор фишинговых писем» (анализ примеров по чек-листу признаков). Ролевая игра «Меня пытаются обмануть»: отработка сценариев телефонного мошенничества. Упражнение «Проверь ссылку перед переходом». Командный разбор кейсов социальной инженерии. Составление памятки «Как распознать мошенника».
Ключевые понятия: фишинг, вишинг, смишинг, социальная инженерия, мошенничество, конфиденциальные данные.

5. Безопасность устройств и сетей (6 ч)

Теоретические сведения. Безопасность домашней сети Wi-Fi: надёжный пароль, шифрование (WPA2/WPA3), скрытие сети, гостевой доступ, обновление прошивки роутера. Обновления операционной системы и приложений как мера защиты. Антивирусная защита: назначение, виды, правила использования. Безопасность мобильных устройств: блокировка экрана, шифрование, права приложений, установка ПО только из проверенных источников. Публичные сети Wi-Fi: риски перехвата данных, правила безопасного подключения. VPN: назначение, принцип работы, ограничения. Резервное копирование данных: виды (локальное, облачное), периодичность, правила хранения резервных копий.
Практическая деятельность. Практикум «Настройка базовой защиты устройства» (по инструкции: блокировка, обновления, антивирус). Аудит настроек домашней сети Wi-Fi (по чек-листу). Упражнение «Безопасно ли подключаться к этой сети?». Настройка резервного копирования (демонстрация). Разбор ситуаций «Что делать, если устройство заражено».
Ключевые понятия: Wi-Fi, шифрование, антивирус, обновление ПО, публичная сеть, VPN, резервное копирование, права приложений.

6. Кибербуллинг и цифровая этика (6 ч)
Теоретические сведения. Понятие кибербуллинга. Формы кибербуллинга: оскорбления, угрозы, распространение слухов, публикация компрометирующих материалов, исключение из групп, троллинг, преследование (сталкинг). Отличия кибербуллинга от обычного буллинга (анонимность, круглосуточность, широкая аудитория, устойчивость следа). Последствия для жертвы, агрессора и свидетелей. Стратегии противодействия: не отвечать агрессией, сохранять доказательства, блокировать, сообщать взрослым, обращаться в администрацию сервиса, при необходимости — в правоохранительные органы. Роль свидетеля. Цифровая этика и сетевой этикет: уважение, ответственность, конфиденциальность чужой информации. Репутация в цифровой среде и её долгосрочные последствия.
Практическая деятельность. Разбор кейсов по кибербуллингу (анализ ситуаций, выбор стратегии поведения). Ролевые упражнения «Я — свидетель», «Я — жертва», «Я — агрессор» (анализ мотивов и последствий). Упражнение «Сетевой этикет: правила общения». Составление памятки «Что делать, если тебя травят в сети». Дискуссия «Репутация в цифровом мире».
Ключевые понятия: кибербуллинг, троллинг, сталкинг, сетевой этикет, цифровая репутация, доказательства, блокировка.

7. Медиаграмотность и проверка информации (8 ч)
Теоретические сведения. Понятия «информация», «дезинформация», «фейк», «фактчекинг». Признаки недостоверной информации: эмоциональный заголовок, отсутствие источника, искажённые цитаты, манипулятивные приёмы, ошибки в фактах. Механизмы распространения фейков: социальные сети, боты, «сарафанное радио». Глубокие фейки (deepfake): что это, как создаются, признаки распознавания (артефакты изображения, несоответствия звука и мимики, странности в деталях). Оценка надёжности источника: авторство, дата, репутация, первоисточник, перекрёстная проверка. Инструменты фактчекинга: обратный поиск изображений, проверка по первоисточникам, специализированные сервисы.
Практическая деятельность. Практикум «Проверка информации из открытых источников» (пошаговый фактчекинг новости). Упражнение «Найди признаки фейка».

Анализ медиатекста на достоверность (работа в группах). Практикум по распознаванию deepfake (разбор примеров). Упражнение «Оцени надёжность источника» (сравнение нескольких источников по одной теме). Составление алгоритма проверки информации.
Ключевые понятия: дезинформация, фейк, фактчекинг, deepfake, источник информации, перекрёстная проверка, манипуляция.

8. Безопасность в социальных сетях и мессенджерах (6 ч)

Теоретические сведения. Настройки приватности в социальных сетях: кто видит профиль, публикации, список друзей, геометки. Разделение аудитории (круги общения). Безопасность переписки в мессенджерах: сквозное шифрование, проверка контактов, осторожность с вложениями и ссылками. Взаимодействие с незнакомцами: правила (не сообщать личные данные, не переходить по ссылкам, не встречаться без ведома взрослых). Овершеринг: чем опасна избыточная публичность (фото с геометками, документы, расписание, место учёбы). Риски публикации фото несовершеннолетних. Настройка уведомлений и цифровая гигиена.
Практическая деятельность. Практикум «Аудит настроек приватности» (по чек-листу на учебном профиле). Упражнение «Анализ профиля на предмет рисков» (что можно узнать о человеке по открытым данным). Разбор ситуаций «Незнакомец в сети». Упражнение «Овершеринг: стоп-кадр» (анализ публикаций). Составление личных правил безопасного поведения в соцсетях и мессенджерах.
Ключевые понятия: приватность, настройки доступа, сквозное шифрование, овершеринг, геометка, незнакомец в сети, цифровая гигиена.

9. Основы криптографии (4 ч)

Теоретические сведения. Понятие криптографии, её назначение. Зачем нужны шифры: защита информации при передаче и хранении. Простые шифры (шифр Цезаря, шифр замены) — ознакомительно, для понимания принципа. Симметричное и асимметричное шифрование (ознакомительно, на уровне идей). Понятие ключа. HTTPS и защищённое соединение: что означает замок в адресной строке, сертификаты. Практическое значение криптографии для повседневной безопасности (мессенджеры, банковские приложения, сайты).
Практическая деятельность. Практическое знакомство с простыми шифрами (шифрование и дешифровка коротких сообщений). Упражнение «Проверка безопасности соединения» (анализ адресной строки, HTTPS). Демонстрация принципа работы шифрования (наглядные примеры). Обсуждение «Где в повседневной жизни мы встречаемся с шифрованием».
Ключевые понятия: криптография, шифр, ключ, симметричное и асимметричное шифрование, HTTPS, сертификат.

10. Практикум: разбор кейсов и ситуационные задачи (10 ч)

Содержание. Комплексное применение полученных знаний в практических ситуациях. Разбор реальных и модельных инцидентов кибербезопасности. Ситуационные задачи по всем изученным темам: защита персональных данных, пароли и аутентификация, фишинг и социальная инженерия, безопасность устройств, кибербуллинг, медиаграмотность, безопасность в соцсетях. Командные формы работы: разбор инцидентов, разработка памяток, игровые упражнения, кейс-тест.
Практическая деятельность.

- Разбор кейсов: реальные инциденты кибербезопасности (анализ причин, последствий, мер prevention).

- Ситуационные задачи: «Что бы ты сделал в этой ситуации?».
- Командный разбор инцидентов (работа в группах, презентация решений).
- Разработка памятки по безопасности (групповой проект).
- Игровые упражнения: «Защита от фишинга», «Кейсы по социальной инженерии».
- Комплексный анализ ситуации (интеграция тем).
- Разработка сценария безопасного поведения.
- Итоговый кейс-тест (промежуточный контроль).

Ключевые понятия: киберинцидент, кейс, ситуационная задача, алгоритм действий, памятка безопасности.

11. Итоговый проект и защита (6 ч)

Содержание. Выбор темы итогового проекта (индивидуально или в малой группе). Примерные темы: «Моя памятка по защите персональных данных», «Как распознать фишинг: руководство для школьника», «Безопасность в социальных сетях: настройки приватности», «Кибербуллинг: как помочь себе и другу», «Фактчекинг: как не поверить фейку», «Безопасный Wi-Fi дома», «Криптография в повседневной жизни» и др. Структура проекта: введение (актуальность, цель), основная часть (содержание, практические рекомендации), заключение, продукт (памятка, буклет, презентация, видеоролик, инструкция). Сбор материала, оформление, подготовка защиты. Предзащита и доработка. Защита проекта: представление, ответы на вопросы, самооценка.

Практическая деятельность. Выбор темы и планирование работы. Сбор и систематизация материала. Оформление проекта и продукта. Подготовка выступления. Предзащита (обратная связь). Доработка по итогам предзащиты. Защита итоговых проектов (2 занятия). Рефлексия.

Ключевые понятия: проект, продукт проекта, защита, презентация, практические рекомендации.

12. Резерв (2 ч)

Содержание. Повторение ключевых тем курса. Итоговое тестирование (проверка предметных результатов). Обобщение: составление «свода правил кибербезопасности» для класса. Рефлексия по итогам года. Завершение курса.

Практическая деятельность. Повторение в формате викторины/квиза. Итоговое тестирование. Коллективное составление «свода правил безопасного поведения в сети». Обсуждение итогов, планов на будущее.

Требования к результатам освоения содержания

Обучающиеся должны знать:

- основные понятия кибербезопасности и виды киберугроз;
- что относится к персональным данным и как формируется цифровой след;
- правила создания надёжных паролей и назначение двухфакторной аутентификации;
- признаки фишинга и приёмы социальной инженерии;
- основы защиты устройств и сетей, правила безопасного использования публичного Wi-Fi;
- формы кибербуллинга и стратегии противодействия;
- признаки недостоверной информации и алгоритм фактчекинга;
- правила безопасного поведения в социальных сетях и мессенджерах;
- назначение криптографии и понятие HTTPS.

Обучающиеся должны уметь:

- оценивать стойкость пароля и настраивать двухфакторную аутентификацию;
- распознавать фишинговые сообщения и мошеннические сценарии;
- проводить базовую настройку защиты устройства и сети;
- анализировать цифровой след и настраивать приватность профиля;
- проверять информацию на достоверность (фактчекинг);
- выбирать стратегию поведения в ситуации кибербуллинга;
- применять правила безопасного поведения в сети в практических ситуациях;
- создавать памятки и рекомендации по кибербезопасности.

Обучающиеся должны владеть:

- навыками критического анализа цифровой информации;
- приёмами безопасной работы с учётными записями и устройствами;
- способами противодействия социальной инженерии;
- навыками командной работы и презентации результатов;
- основами цифровой этики и ответственного поведения в сети.

Планируемые результаты

Предметные:

- знать основные виды киберугроз и методы противодействия;
- уметь настраивать параметры безопасности операционных систем, браузеров и социальных сетей;
- владеть приёмами создания надёжных паролей и организации двухфакторной аутентификации;
- распознавать признаки фишинга и социальной инженерии;
- понимать правовые нормы, регулирующие информационную безопасность.

Метапредметные:

- развитие критического мышления при оценке цифрового контента;
- формирование навыков анализа рисков и принятия решений в нестандартных ситуациях;
- совершенствование коммуникативных навыков при обсуждении проблем кибербезопасности.

Личностные:

- осознание ответственности за собственное цифровое поведение;
- формирование установки на безопасный и этичный образ действий в цифровой среде;
- развитие эмпатии и толерантности в онлайн-коммуникации.

Формы контроля и оценочные материалы

- **Текущий контроль:** практические работы, устный опрос, выполнение заданий на образовательных платформах.
- **Промежуточный контроль:** контрольная работа № 1 по разделам 1–4.
- **Итоговый контроль:** контрольная работа № 2 и защита индивидуального/группового проекта.
- **Критерии оценивания:** уровень освоения теоретического материала, качество выполнения практических заданий, самостоятельность и креативность в проектной работе.
-

Учебно-тематический план

№	Название раздела	Количество часов
1	Введение в кибербезопасность. Цифровая гигиена	8
2	Защита персональных данных и приватность	10
3	Безопасность устройств и сетей	10
4	Социальная инженерия и фишинг	10
5	Безопасность в социальных сетях и мессенджерах	8
6	Кибербуллинг и цифровая этика	8
7	Правовые аспекты кибербезопасности	6
8	Итоговое повторение и проект	8
Итого		**68**

Календарно-тематическое планирование

№ занятия	Дата	Раздел / Тема	Кол-во часов
Раздел 1. Введение в кибербезопасность. Цифровая гигиена (8 ч)			
1	01.09.2026	Вводное занятие. Понятие кибербезопасности. Цифровая среда как пространство рисков	1
2	04.09.2026	Основные виды киберугроз: классификация и	1

		источники	
3	08.09.2026	Цифровая гигиена: базовые правила безопасной работы	1
4	11.09.2026	Парольная защита: принципы создания надёжных паролей	1
5	15.09.2026	Менеджеры паролей и двухфакторная аутентификация	1
6	18.09.2026	Практикум: настройка двухфакторной аутентификации	1
7	22.09.2026	Обновление программного обеспечения как мера защиты	1
8	25.09.2026	Резервное копирование данных: стратегии и инструменты	1
Раздел 2. Защита персональных данных и приватность (10 ч)			
9	29.09.2026	Персональные данные: понятие и ценность в цифровом мире	1
10	02.10.2026	Цифровой след: формирование и управление	1
11	06.10.2026	Настройки приватности в браузерах и операционных системах	1
12	09.10.2026	Cookies и трекеры: механизмы работы и способы ограничения	1
13	13.10.2026	Практикум: аудит цифрового следа и настройка приватности	1
14	16.10.2026	Безопасное использование облачных хранилищ	1
15	20.10.2026	Защита данных на мобильных устройствах	1
16	23.10.2026	Шифрование: базовые принципы и инструменты	1
17	06.11.2026	Практикум: шифрование файлов и контейнеров	1
18	10.11.2026	Обобщение раздела: защита персональных данных	1
Раздел 3. Безопасность устройств и сетей (10 ч)			
19	13.11.2026	Вредоносное программное обеспечение: типы и	1

		признаки заражения	
20	17.11.2026	Антивирусная защита: принципы работы и выбор	1
21	20.11.2026	Безопасность домашней Wi-Fi сети	1
22	24.11.2026	Практикум: настройка безопасности роутера	1
23	27.11.2026	Публичные Wi-Fi сети: риски и меры предосторожности	1
24	01.12.2026	VPN: назначение, принципы работы, выбор сервиса	1
25	04.12.2026	Безопасность в браузере: расширения, песочницы, режим инкогнито	1
26	08.12.2026	Фишинговые сайты и поддельные приложения: распознавание	1
27	11.12.2026	Практикум: анализ подозрительных сайтов и приложений	1
28	15.12.2026	Обобщение раздела: защита устройств и сетей	1
Раздел 4. Социальная инженерия и фишинг (10 ч)			
29	18.12.2026	Социальная инженерия: психологические основы манипуляции	1
30	22.12.2026	Фишинг: виды, каналы распространения, признаки	1
31	25.12.2026	Практикум: разбор реальных примеров фишинговых писем	1
32	12.01.2027	Телефонное мошенничество и голосовой фишинг (вишинг)	1
33	15.01.2027	Мошенничество в мессенджерах и социальных сетях	1
34	19.01.2027	Практикум: анализ сценариев социальной инженерии	1
35	22.01.2027	Защита от манипуляций: стратегии противодействия	1
36	26.01.2027	Правила поведения при подозрении на мошенничество	1
37	29.01.2027	Обобщение раздела: социальная инженерия	1

38	02.02.2027	Контрольная работа № 1 (разделы 1–4)	1
Раздел 5. Безопасность в социальных сетях и мессенджерах (8 ч)			
39	05.02.2027	Анализ контрольной работы. Цифровой имидж и репутация	1
40	09.02.2027	Настройки безопасности в социальных сетях	1
41	12.02.2027	Опасности геолокации и публикации личной информации	1
42	16.02.2027	Безопасность в мессенджерах: настройки и правила	1
43	19.02.2027	Практикум: настройка безопасности аккаунта социальной сети	1
44	26.02.2027	Нежелательный контент: фильтрация и родительский контроль	1
45	02.03.2027	Обобщение раздела: безопасность в социальных сетях	1
46	05.03.2027	Практикум: создание чек-листа безопасности профиля	1
Раздел 6. Кибербуллинг и цифровая этика (8 ч)			
47	09.03.2027	Кибербуллинг: формы проявления и последствия	1
48	12.03.2027	Правовые и этические аспекты кибербуллинга	1
49	16.03.2027	Стратегии противодействия кибербуллингу	1
50	19.03.2027	Практикум: разбор кейсов и алгоритм действий	1
51	23.03.2027	Цифровая этика и ответственное поведение в сети	1
52	06.04.2027	Троллинг и конфликтные коммуникации: управление ситуацией	1
53	09.04.2027	Психологическая поддержка и обращение за помощью	1
54	13.04.2027	Обобщение раздела: кибербуллинг и цифровая этика	1
Раздел 7. Правовые аспекты кибербезопасности (6 ч)			
55	16.04.2027	Законодательство РФ в сфере информационной	1

		безопасности	
56	20.04.2027	Ответственность за киберправонарушения	1
57	23.04.2027	Защита прав потребителей в цифровой среде	1
58	27.04.2027	Практикум: анализ правовых ситуаций	1
59	30.04.2027	Авторское право и лицензии в цифровой среде	1
60	04.05.2027	Обобщение раздела: правовые аспекты	1
Раздел 8. Итоговое повторение и проект (8 ч)			
61	07.05.2027	Повторение ключевых тем курса	1
62	11.05.2027	Контрольная работа № 2 (итоговая)	1
63	14.05.2027	Анализ контрольной работы. Выбор тем проектов	1
64	18.05.2027	Работа над проектом: планирование и сбор материала	1
65	21.05.2027	Работа над проектом: оформление результатов	1
66	21.05.2027	Работа над проектом: подготовка презентации	1
67	25.05.2027	Защита проектов	1
68	25.05.2027	Итоговое занятие. Рефлексия. Резерв	1

Электронные образовательные ресурсы

Перечень ЭОР сформирован в соответствии с Федеральным перечнем, утверждённым приказом Минпросвещения России от 25.08.2026 № 591, и включает ресурсы, используемые в образовательном процессе и соответствующие требованиям обновлённых ФГОС:

1. **Библиотека цифрового образовательного контента** — https://моиуроки.рф/
2. **Образовательная платформа «Сферум»** — https://sferum.ru/
3. **Яндекс.Учебник** — https://education.yandex.ru
4. **Фоксфорд** — https://help.foxford.ru
5. **ЯКласс** — https://www.yaklass.ru
6. **Медиатека «Просвещения»** — https://media.prosv.ru

7. **Тренажёр «Облако знаний»** (ООО «Физикон Лаб»)
8. **Образовательный портал Учи.ру** — https://uchi.ru/teachers/lk/main

Дополнительно могут использоваться материалы проекта «Урок цифры» (https://урокцифры.рф) и портала «Сетевичок» (https://сетевичок.рф), не входящие в федеральный перечень, но рекомендованные для тематики кибербезопасности.

Учебно-методическое обеспечение

- Босова Л. Л., Босова А. Ю. Информатика: учебник для 9 класса. — М.: БИНОМ. Лаборатория знаний.
- Методические материалы портала «Урок цифры» (уроки по кибербезопасности).
- Ресурсы проекта «Цифровой ликбез».
- Материалы сайта «Сетевичок» (квесты и тесты по кибербезопасности).
- Демонстрационные материалы и практикумы, разработанные педагогом.