

Рабочая программа курса внеурочной деятельности

«Информационная безопасность»

для обучающихся 10–11 классов

Содержание

1. Пояснительная записка
2. Общая характеристика курса
3. Цель и задачи курса
4. Место курса в плане внеурочной деятельности
5. Содержание курса
6. Планируемые результаты
7. Формы организации и оценивание
8. Требования безопасности и этические ограничения
9. Тематическое планирование
10. Календарно-тематическое планирование
11. Учебно-методическое обеспечение

1 Пояснительная записка

Рабочая программа курса внеурочной деятельности «Информационная безопасность» предназначена для обучающихся 10–11 классов. Она направлена на формирование безопасного, ответственного и правомерного поведения в цифровой среде, развитие способности распознавать угрозы, снижать риски и действовать по установленному алгоритму при возникновении инцидента.

Курс имеет практико-ориентированный и исключительно защитный характер. Обучающиеся работают с учебными кейсами, обезличенными данными, симуляторами и разрешёнными настройками собственных либо школьных устройств. Изучение угроз не предполагает несанкционированного доступа, обхода защиты, перехвата данных, подбора учётных данных, разработки вредоносного кода или воздействия на реальные информационные системы.

Нормативная основа

- Федеральный закон от 29 декабря 2012 года № 273-ФЗ «Об образовании в Российской Федерации» в действующей редакции.
- Федеральный государственный образовательный стандарт среднего общего образования, утверждённый приказом Минобрнауки России от 17 мая 2012 года № 413, с последующими изменениями.
- Федеральная образовательная программа среднего общего образования, утверждённая приказом Минпросвещения России от 18 мая 2023 года № 371, с последующими изменениями.
- Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» в действующей редакции.
- Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных» в действующей редакции.
- Федеральный закон от 29 декабря 2010 года № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» в действующей редакции.
- Федеральный закон от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» — в обзорной части курса.
- Основная образовательная программа среднего общего образования, план внеурочной деятельности и локальные акты МАОУ Лицей № 185.

2 Общая характеристика курса

В 10 классе основное внимание уделяется личной цифровой безопасности: защите учётных записей и устройств, распознаванию социальной инженерии, безопасной работе в сети, резервному

копированию, приватности, цифровому следу, проверке информации и действиям при инциденте. В 11 классе обучающиеся переходят к системному взгляду: активам, угрозам, уязвимостям и рискам, принципам криптографической защиты, сетевой безопасности, безопасной конфигурации, защите данных в организации, безопасной разработке и реагированию на инциденты.

Каждое занятие сочетает краткое объяснение, разбор ситуации и практическое действие: анализ признаков фишинга, настройку параметров безопасности, построение модели угроз, проверку резервной копии, работу с журналом событий, подготовку памятки или политики. Все задания выполняются в пределах выданного педагогом разрешения.

3 Цель и задачи курса

Цель курса — сформировать у обучающихся устойчивые навыки безопасного, этичного и правомерного использования цифровых технологий, а также основы риск-ориентированного мышления в области информационной безопасности.

Задачи курса:

- сформировать представление о ценности информации, персональных данных и цифровой репутации;
- научить применять парольную защиту, многофакторную аутентификацию, обновления и резервное копирование;
- развить умение распознавать фишинг, социальную инженерию, мошеннические сценарии и признаки компрометации;
- познакомить с правовыми и этическими требованиями работы с информацией;
- сформировать понимание целей защиты: конфиденциальности, целостности и доступности;
- освоить базовый анализ активов, угроз, уязвимостей, вероятности и последствий;
- познакомить на концептуальном уровне с шифрованием, хэшированием, электронной подписью и сертификатами;
- научить документировать инцидент, сохранять значимые сведения и своевременно обращаться за помощью;
- развивать критическое мышление, командное взаимодействие и академическую честность.

4 Место курса в плане внеурочной деятельности

Программа рассчитана на два учебных года: 34 часа в 10 классе и 34 часа в 11 классе, всего 68 часов. Занятия проводятся один раз в неделю по одному академическому часу. Допускается уточнение последовательности тем с учётом календарного учебного графика, изменений цифровых сервисов и уровня подготовки группы при сохранении общего объёма и планируемых результатов.

5 Содержание курса

10 класс 34 часа

Введение, право и цифровая идентичность — 5 часов. Правила курса. Законное и этичное поведение. Персональные данные, согласие на обработку, цифровой след и репутация.

Аутентификация и социальная инженерия — 7 часов. Парольные фразы, менеджеры паролей, резервные коды, многофакторная аутентификация, фишинг, социальная инженерия, безопасная электронная почта и мессенджеры.

Защита устройств и программ — 5 часов. Блокировка устройства, обновления, разрешения приложений, признаки вредоносного ПО, безопасная установка программ.

Безопасность веба и сетей — 4 часа. Приватность браузера, HTTPS и сертификаты, публичный Wi-Fi, базовая защита домашней сети.

Защита данных и приватность — 5 часов. Резервное копирование, облачный доступ, назначение шифрования, метаданные, настройки приватности.

Безопасность цифровых платформ — 5 часов. Кибербуллинг, дезинформация и дипфейки, ИИ-сервисы, интернет-покупки, игровые платформы.

Инциденты и итоговый проект — 3 часа. Признаки инцидента, первые действия, аудит цифровой гигиены, итоговый практикум.

11 класс 34 часа

Основы управления информационной безопасностью — 7 часов. Конфиденциальность, целостность, доступность; активы, угрозы, уязвимости, модель нарушителя, риск, минимальные привилегии, разграничение доступа.

Криптографические основы — 4 часа. Назначение симметричного и асимметричного шифрования, хэш-функций, электронной подписи и сертификатов.

Сети и средства защиты — 6 часов. Основы сетевого взаимодействия, IP, DNS, HTTP/HTTPS, обзор угроз, межсетевые экраны, сегментация, Wi-Fi, журналы и мониторинг.

Уязвимости, конфигурация и восстановление — 3 часа. Жизненный цикл уязвимости, своевременные обновления, безопасная конфигурация, резервирование и восстановление.

Данные, право и политика — 4 часа. Жизненный цикл данных, персональные данные в организации, критическая информационная инфраструктура, политика безопасности и роли сотрудников.

Безопасная разработка и цепочка поставок — 4 часа. Безопасный жизненный цикл ПО, типовые риски веб-приложений, валидация данных, защита секретов, зависимости и открытое ПО.

Реагирование, профессии и проект — 6 часов. Этапы реагирования, сохранение цифровых следов, профессиональная этика, проектирование защитных мер и защита проекта.

6 Планируемые результаты

Личностные результаты

- ответственное отношение к собственным и чужим данным, цифровой репутации и правам человека;
- готовность соблюдать закон, этические нормы, правила доступа и требования безопасности;
- понимание личной ответственности за действия в сети и ценности своевременного обращения за помощью;
- устойчивость к манипуляциям, мошенническим предложениям и давлению в цифровой среде.

Метапредметные результаты

- выделять проблему, собирать признаки, оценивать риск и выбирать соразмерную защитную меру;
- критически оценивать источник, сообщение, ссылку, файл и цифровой контент;
- работать по инструкции, документировать действия и представлять вывод в понятной форме;
- взаимодействовать в группе, распределять роли и соблюдать конфиденциальность учебных данных.

Предметные результаты

- настраивать базовую защиту учётной записи и устройства, применять многофакторную аутентификацию;
- распознавать распространённые признаки фишинга, социальной инженерии, вредоносной активности и мошенничества;
- объяснять назначение обновлений, резервных копий, шифрования, хэширования, электронной подписи и сертификатов;
- различать идентификацию, аутентификацию, авторизацию и разграничение доступа;
- строить простую модель угроз и оценивать риск по вероятности и последствиям;

- объяснять роль сетевых протоколов, межсетевого экрана, сегментации, журналирования и мониторинга;
- предлагать защитные меры для школьного или бытового цифрового сценария;
- действовать по алгоритму при инциденте, не уничтожая потенциально значимые сведения.

7 Формы организации и оценивание

Формы работы: мини-лекция, анализ кейса, практикум по настройкам, тренажёр распознавания фишинга, ролевая ситуация, работа с чек-листом, моделирование угроз, настольное учение по реагированию, мини-проект и защита. Работа ведётся индивидуально, в парах и малых группах.

Оценивание носит формирующий характер. Используются входная и итоговая диагностика, наблюдение, практический чек-лист, карточка анализа риска, памятка, мини-тест, защита проекта и рефлексия. Оцениваются правомерность и безопасность действий, полнота анализа, обоснованность защитных мер, качество документации и самостоятельность объяснения. Скорость выполнения потенциально рискованных действий не является критерием успеха.

8 Требования безопасности и этические ограничения

- практические действия выполняются только на собственных устройствах, школьном оборудовании или в учебной среде с явного разрешения педагога;
- запрещены несанкционированное сканирование, подбор паролей, обход ограничений, перехват трафика, эксплуатация уязвимостей, создание или запуск вредоносного кода;
- запрещается собирать, копировать, публиковать или передавать реальные пароли, резервные коды, платёжные сведения и иные секреты;
- в заданиях используются вымышленные, обезличенные или специально подготовленные данные; реальные персональные данные одноклассников и сотрудников не применяются;
- подозрительные ссылки, вложения и носители не открываются: обучающийся фиксирует признаки и сообщает педагогу;
- изменения в школьных учётных записях, сетях и устройствах выполняются только в пределах задания и предоставленных полномочий;
- отработка инцидента проводится как анализ кейса или настольное учение без воздействия на действующие системы;
- соблюдаются правила электробезопасности, эргономики, смены видов деятельности и зрительных пауз; о неисправности немедленно сообщают педагогу.

9 Тематическое планирование

№	Класс	Раздел	Часы
1	10 класс	Введение, право и цифровая идентичность	5
2	10 класс	Аутентификация и социальная инженерия	7
3	10 класс	Защита устройств и программ	5
4	10 класс	Безопасность веба и сетей	4
5	10 класс	Защита данных и приватность	5
6	10 класс	Безопасность цифровых платформ	5
7	10 класс	Инциденты и итоговый проект	3
8	11 класс	Основы управления информационной безопасностью	7
9	11 класс	Криптографические основы	4
10	11 класс	Сети и средства защиты	6
11	11 класс	Уязвимости, конфигурация и восстановление	3

№	Класс	Раздел	Часы
12	11 класс	Данные, право и политика	4
13	11 класс	Безопасная разработка и цепочка поставок	4
14	11 класс	Реагирование, профессии и проект	6
		Итого	68

10 Календарно-тематическое планирование

Планируемая и фактическая даты заполняются педагогом с учётом календарного учебного графика. Все практические действия проводятся в разрешённой учебной среде; содержание кейсов и названия сервисов могут актуализироваться без изменения планируемых результатов.

10 класс 34 часа

№	Тема занятия	Краткое содержание	Ч	Виды деятельности	Контроль	План	Факт
1	Введение. Цели курса и входная диагностика	Ключевые понятия, ожидаемые результаты, правила курса. Самооценка цифровых привычек без раскрытия секретов.	1	Диагностика, беседа	Индивидуальная карта		
2	Правила безопасной работы в цифровой среде	Разрешённые действия, учебные среды, принцип «остановись и сообщи», обращение за помощью.	1	Инструктаж, кейсы	Зачёт по безопасности		
3	Правовые и этические основы	Право на информацию и неприкосновенность частной жизни. Ответственность за неправомерный доступ и распространение данных.	1	Семинар-практикум	Мини-тест		
4	Персональные данные и согласие	Категории персональных данных, цель и минимизация сбора, согласие, права субъекта.	1	Кейс-практикум	Карточка анализа		
5	Цифровой след и репутация	Активный и пассивный цифровой след, долговременные последствия публикаций, аудит открытой информации.	1	Практикум	Чек-лист		
6	Учётные записи и парольная защита	Уникальные парольные фразы, запрет повторного использования, признаки компрометации.	1	Практическая работа	Чек-лист настройки		
7	Менеджеры паролей и резервные коды	Назначение менеджера паролей, мастер-пароль, хранение и восстановление доступа.	1	Демонстрация, практикум	Памятка		
8	Многофакторная аутентификация	Факторы аутентификации, приложения-коды, ключи доступа, резервные сценарии.	1	Практикум	Карточка выбора		
9	Фишинг и поддельные сайты	Признаки сообщения, домен, срочность, форма входа, безопасная проверка через официальный канал.	1	Тренажёр	Мини-зачёт		
10	Социальная инженерия	Манипуляции доверием, авторитетом, страхом и дефицитом. Скрипт безопасного отказа.	1	Рольевые кейсы	Лист наблюдения		
11	Безопасность электронной почты	Отправитель, вложения, ссылки, скрытая копия, сообщения о подозрительном письме.	1	Практикум	Карточка анализа		
12	Безопасность мессенджеров	Настройки приватности, групповые приглашения, файлы, резервные копии и захват аккаунта.	1	Кейс-практикум	Чек-лист		
13	Мобильные устройства и блокировка	PIN-код, биометрия, автоматическая блокировка, поиск устройства, уведомления на экране.	1	Практическая работа	Чек-лист		
14	Обновления операционной системы	Исправления безопасности, автоматические обновления, поддерживаемые версии, перезагрузка.	1	Практикум	Краткий отчёт		
15	Разрешения приложений	Камера, микрофон, геолокация, контакты; принцип минимально необходимого доступа.	1	Аудит настроек	Таблица решений		
16	Вредоносное ПО: признаки и профилактика	Типы и признаки заражения на обзорном уровне. Изоляция, отключение и обращение к специалисту.	1	Кейсы	Алгоритм действий		

№	Тема занятия	Краткое содержание	Ч	Виды деятельности	Контроль	План	Факт
17	Безопасная загрузка и установка программ	Официальный источник, издатель, подпись, разрешения, отказ от сомнительных сборок.	1	Практикум	Чек-лист		
18	Браузер: приватность и расширения	Обновления, разрешения сайтов, файлы cookie, загрузки, проверка расширений.	1	Практическая работа	Аудит браузера		
19	HTTPS и цифровые сертификаты	Назначение защищённого соединения, доменное имя, предупреждения браузера и границы защиты.	1	Демонстрация	Мини-тест		
20	Публичный Wi-Fi	Риски открытой сети, проверка имени, отказ от чувствительных операций, защищённое соединение.	1	Кейс-практикум	Памятка		
21	Домашняя сеть	Пароль администратора, актуальная прошивка, современная защита Wi-Fi, гостевая сеть.	1	Моделирование	Схема настроек		
22	Резервное копирование	Правило нескольких копий, периодичность, носители, проверка восстановления.	1	Практикум	План копирования		
23	Облачные хранилища и общий доступ	Права просмотра и изменения, срок ссылки, отзыв доступа, история версий.	1	Практическая работа	Чек-лист доступа		
24	Шифрование данных: назначение	Защита данных при хранении и передаче, ключ и пароль, ограничения шифрования.	1	Моделирование	Карточка понятий		

№	Тема занятия	Краткое содержание	Ч	Виды деятельности	Контроль	План	Факт
25	Метаданные файлов и изображений	Автор, время, геопозиция и свойства документа. Безопасная публикация учебных материалов.	1	Практикум	Краткий отчёт		
26	Приватность в социальных сетях	Аудит аудитории, отметок, геолокации, поиска профиля и старых публикаций.	1	Практическая работа	Чек-лист		
27	Кибербуллинг и безопасная коммуникация	Границы общения, блокировка, жалоба, сохранение доказательств, поддержка пострадавшего.	1	Ситуационные задачи	Алгоритм помощи		
28	Дезинформация и дипфейки	Источник, дата, контекст, обратный поиск, признаки синтетического контента, подтверждение фактов.	1	Медиапрактикум	Карточка проверки		
29	Безопасное использование ИИ-сервисов	Запрет ввода секретов и лишних персональных данных, проверка ответа, авторство и ответственность.	1	Кейс-практикум	Памятка		
30	Интернет-покупки и платёжное мошенничество	Проверка продавца и адреса сайта, безопасная оплата, признаки ложной доставки и возврата.	1	Кейсы	Мини-зачёт		
31	Игровые платформы	Кража аккаунтов, поддельные подарки, внутриигровые сделки, родительские настройки и жалобы.	1	Кейс-практикум	Карточка риска		
32	Признаки инцидента и первые действия	Компрометация аккаунта, потеря устройства, подозрительная активность. Изоляция, фиксация, сообщение.	1	Настольное учение	Лист действий		
33	Мини-проект: аудит цифровой гигиены	Проверка учебного профиля по чек-листу и разработка памятки без раскрытия личных данных.	1	Проектная работа	Черновик памятки		
34	Итоговый практикум и зачёт	Комплексные сценарии: сообщение, учётная запись, устройство, публикация и инцидент. Рефлексия.	1	Практический зачёт	Итоговая карта		

11 класс 34 часа

№	Тема занятия	Краткое содержание	Ч	Виды деятельности	Контроль	План	Факт
1	Входная диагностика и повторение	Личная цифровая гигиена, социальная инженерия, резервные копии и первые действия при инциденте.	1	Диагностика	Индивидуальная карта		
2	Цели информационной безопасности	Конфиденциальность, целостность и доступность. Конфликты целей на примерах.	1	Семинар-практикум	Мини-тест		
3	Активы, угрозы и уязвимости	Различение ценного ресурса, возможного события и слабого места. Защитная мера как снижение риска.	1	Кейс-практикум	Карточка анализа		
4	Модель нарушителя	Возможности, мотив, доступ и ограничения. Внутренние и внешние источники угроз без профилирования людей.	1	Моделирование	Паспорт сценария		
5	Оценка риска	Вероятность, последствия, матрица риска, остаточный риск и приоритет мер.	1	Практикум	Матрица риска		
6	Принцип минимальных привилегий	Выдача только необходимого доступа, срок действия, пересмотр прав, разделение обязанностей.	1	Кейс-практикум	Таблица доступа		
7	Идентификация, аутентификация и авторизация	Различие процессов, учётная запись, сессия, роль, право и журналирование.	1	Практикум	Схема доступа		
8	Симметричное шифрование	Один общий секрет, назначение и сценарии применения. Понятие стойкости без реализации атак.	1	Моделирование	Карточка понятий		
9	Асимметричное шифрование	Пара ключей, конфиденциальность и обмен ключами на концептуальном уровне.	1	Моделирование	Мини-тест		
10	Хэш-функции и контроль целостности	Одностороннее преобразование, контрольная сумма, хранение паролей как общий принцип.	1	Практикум на учебных данных	Лист наблюдений		
11	Электронная подпись и сертификаты	Авторство, целостность, доверие к открытому ключу, проверка сертификата.	1	Кейс-практикум	Карточка проверки		
12	Основы компьютерных сетей	Устройства, узлы, каналы, локальная и глобальная сеть, клиент и сервер.	1	Моделирование	Схема сети		
13	IP, DNS, HTTP и HTTPS	Назначение адресации, разрешения имён и прикладных протоколов; защищённый канал.	1	Практикум	Мини-тест		
14	Сетевые угрозы и защитные меры	Подмена, прослушивание, перегрузка и неправомерный доступ — обзор признаков и защит.	1	Кейсы	Таблица «угроза—мера»		
15	Межсетевой экран и сегментация	Разрешающие правила, границы сети, разделение зон, принцип запрета по умолчанию.	1	Симулятор	Схема правил		
16	Безопасность Wi-Fi	Аутентификация, шифрование, гостевой доступ, отказ от устаревших режимов, физическое размещение.	1	Аудит макета	Чек-лист		
17	Журналы событий и мониторинг	Время, источник, событие, результат; признаки отклонений и уведомление ответственного.	1	Анализ учебного журнала	Краткий отчёт		
18	Уязвимости и обновления	Обнаружение, сообщение, исправление, проверка и раскрытие. Приоритет критичных обновлений.	1	Кейс-практикум	План обновления		

№	Тема занятия	Краткое содержание	Ч	Виды деятельности	Контроль	План	Факт
19	Безопасная конфигурация	Отключение лишнего, безопасные значения по умолчанию, учёт конфигураций, контроль изменений.	1	Практикум	Чек-лист		
20	Резервное копирование и восстановление	Цели по допустимой потере данных и времени восстановления на учебном уровне. Проверка копии.	1	Настольное учение	План восстановления		
21	Жизненный цикл данных	Создание, хранение, использование, передача, архивирование и уничтожение; минимизация данных.	1	Моделирование	Схема цикла		
22	Персональные данные в организации	Роли, цели обработки, доступ, согласие, меры защиты и действия при утечке.	1	Кейс-практикум	Карточка соответствия		
23	Критическая информационная инфраструктура	Назначение и общественная значимость, субъекты и объекты — обзор без анализа реальных систем.	1	Обзор, обсуждение	Мини-тест		
24	Политика информационной безопасности	Цели, область действия, роли, правила, исключения, ответственность и пересмотр.	1	Проектирование	Фрагмент политики		

№	Тема занятия	Краткое содержание	Ч	Виды деятельности	Контроль	План	Факт
25	Безопасный жизненный цикл ПО	Требования, проектирование, разработка, проверка, выпуск, сопровождение и вывод из эксплуатации.	1	Семинар-практикум	Схема процесса		
26	Веб-приложения: типовые риски и защита	Ошибки контроля доступа, обработки ввода и сессий — только защитные принципы и учебные кейсы.	1	Кейс-практикум	Таблица мер		
27	Безопасное программирование	Проверка входных данных, обработка ошибок, управление секретами и безопасное журналирование.	1	Ревью учебных фрагментов	Чек-лист ревью		
28	Цепочка поставок и открытое ПО	Зависимости, источник пакета, версии, обновления, лицензии, ведомость компонентов.	1	Практикум	Реестр зависимостей		
29	Реагирование на инцидент	Подготовка, обнаружение, локализация, устранение, восстановление и разбор уроков.	1	Настольное учение	Карточка этапов		
30	Сохранение цифровых следов	Фиксация времени и наблюдаемых признаков, сохранение исходных материалов, запрет самовольного исследования.	1	Кейс-практикум	Протокол сообщения		
31	Профессиональная этика и профессии	Ответственное раскрытие, полномочия и конфиденциальность. Роли специалиста по защите информации.	1	Дискуссия	Рефлексивная заметка		
32	Проект: модель угроз школьного сервиса	Выбор учебного объекта, активы, пользователи, угрозы, ограничения и приоритет защитных мер.	1	Проектная работа	Модель угроз		
33	Проект: политика и защита решения	Краткая политика безопасности, план реагирования, обоснование мер и подготовка выступления.	1	Проектная работа	Проектный отчёт		
34	Защита проекта и итоговая диагностика	Представление решения, ответы на вопросы, анализ остаточного риска и индивидуальная рефлексия.	1	Конференция, диагностика	Итоговый зачёт		

11 Учебно-методическое обеспечение

Оборудование и программная среда

- компьютеры или ноутбуки с актуальными обновлениями, школьные учётные записи с ограниченными правами и доступом в сеть под контролем педагога;
- демонстрационный проектор, локальные учебные материалы, тестовые профили, обезличенные наборы данных и распечатанные кейсы;
- учебные симуляторы настройки доступа, сетевого взаимодействия и реагирования на инциденты;
- браузер, офисные приложения, средство просмотра свойств файлов, электронные таблицы и инструменты проверки контрольных сумм — по утверждённому перечню;
- тестовые носители и резервные копии, не содержащие реальных персональных или конфиденциальных данных.

Материалы педагога и обучающихся

- инструкция по безопасной и этичной работе, правила использования школьной сети и порядок сообщения об инциденте;
- карточки фишинговых и мошеннических сценариев, чек-листы цифровой гигиены, шаблоны модели угроз и матрицы риска;
- шаблоны плана резервного копирования, сообщения об инциденте, фрагмента политики безопасности и проектного отчёта;
- актуальные памятки государственных органов и поставщиков используемых сервисов, проверенные педагогом перед занятием;
- учебники и пособия по информатике и информационной безопасности, соответствующие возрасту обучающихся и действующим требованиям.

Условия реализации

Педагог заранее проверяет учебную среду, права доступа, отсутствие реальных секретов и персональных данных, а также возможность безопасного восстановления исходного состояния. Для практикумов используются демонстрационные профили и данные. При невозможности выполнить настройку на устройстве обучающийся работает с макетом, скриншотами или симулятором. Любой обнаруженный реальный инцидент выводится за рамки занятия и передаётся ответственному сотруднику по установленному порядку.