Методические рекомендации

Занятие 4: «Цифровая безопасность: щит в онлайн-мире»

Нижний Новгород, 2025 год

Оглавление

1. **Цель и задачи занятия**

Цель занятия: сформировать у учащихся комплексное представление о цифровой безопасности как элементе правовой культуры, развить практические навыки защиты личных данных, критической оценки информации и ответственного поведения в онлайн-среде в соответствии с законодательством Российской Федерации.

Задачи занятия:

Предметные:

- Изучить современные угрозы в цифровой среде;
- Освоить правовые основы цифровой безопасности;
- Сформировать критическое отношение к информации, получаемой из онлайн-источников;
- Скачать и установить национальный мессенджер MAX, присоединиться к образовательному каналу в Telegram, MAX и сообществу ВК.

Метапредметные:

- Развивать навыки критического анализа информации и фактчекинга;
- Формировать умения эффективной командной работы и принятия совместных решений в условиях ограниченного времени;
- Стимулировать креативное мышление при решении нестандартных задач в цифровой среде;
- Развивать навыки безопасной и этичной онлайн-коммуникации.

Личностные:

- Формировать активную гражданскую позицию и неприятие идеологии экстремизма в любых ее проявлениях;
- Развивать чувство личной ответственности за свою безопасность и безопасность окружающих в онлайн- и офлайн-среде;
- Мотивировать к безопасному и правомерному поведению в интернете и офлайн, а также к своевременному обращению за помощью.

Целевая аудитория:

- Учащиеся 9–11 классов (15–17 лет).

Продолжительность:

- 90 минут.

2. Подготовка занятия

Формат проведения:

- Интерактивное занятие с элементами командной игры, использованием смартфонов, анализа кейсов и практических заданий.

Необходимые материалы и оборудование:

Техническое оборудование:

- Компьютер/ноутбук для демонстрации презентации.
- Проектор и экран (или интерактивная доска);
- Смартфоны учащихся с доступом в интернет и установленным приложениями MAX, Telegram и ВК.

Раздаточные материалы (все выдается в начале занятия):

- Приложение 1: Карточки для деления на команды «Кибер-детективы», «Цифровые стражи», «Медиа-аналитики», «IT-защитники» - 4 листа А4, сложенных пополам ставятся на стол, по одному на каждую группу;
- Приложение 2: Памятка «Щит в онлайн-мире» - по одному на каждого учащегося;
- Приложение 3: Кейс-карточки «Цифровые угрозы» - по **два** на каждую группу;
- Приложение 4: Рабочий лист «План защиты» - по **два** на каждую группу.

Канцелярские принадлежности:

- Ватман\Лист А4 (по одному на каждую группу)
- Письменные принадлежности (ручки, карандаши);
- Маркеры\Карандаши\Фломастеры разных цветов;
- Флипчарт или доска для записи идей (по желанию).

Подготовка к занятию для учителя:

За день до занятия:

- Изучить методические рекомендации и все приложения к уроку;
- Изучить и проверить презентацию (Приложение 5);

- Распечатать все раздаточные материалы в необходимом количестве;
- Подготовить ответы на возможные сложные вопросы учащихся.

В день занятия (за 5–10 минут до начала):

- Проверить работоспособность технического оборудования;
- Организовать пространство класса для групповой работы (столы для групп по 4–8 человек);
- Разложить раздаточные материалы по группам;
- Подготовить доску/флипчарт для записи ключевых идей;
- Создать доброжелательную атмосферу в классе.

3. Легенда занятия

В рамках программы «Молодые амбассадоры безопасности» учащиеся проходят «Сертификацию цифрового гражданина». Это занятие, где каждая команда, выполняя задания, доказывает свою компетентность в вопросах цифровой безопасности. Это финальное занятия все цикла, и финальным этапом является получение каждым участником «Сертификата Молодого амбассадора безопасности» через Telegram-бот, что подтверждает их готовность быть защитниками в онлайн-мире.

4. Ход занятия (Хронометраж)

Этап занятия	Время (мин)	Деятельность учителя	Деятельность учащихся	Используемые материалы/слайды	Цель этапа
1. Введение и мотивация		Приветствие, объявление темы и легенды занятия. Деление на команды.	Слушают, знакомятся с правилами. Делятся на команды с помощью карточек.	Слайд 1: «Цифровая безопасность: щит в онлайн-мире». Слайд 2: Легенда «Сертификация цифрового гражданина».	Создать мотивирующую среду, погрузить в игровую легенду.
Текст для учителя		"Здравствуйте, ребята! Сегодня мы с вами отправляемся в увлекательное путешествие по миру цифровой безопасности. Наше занятие называется «Цифровая безопасность: щит в онлайн-мире». Вы станете участниками программы «Молодые амбассадоры безопасности» и пройдете финальную «Сертификацию цифрового гражданина». Сегодня мы поговорим о цифровой безопасности и о вопросах защиты в интернете. Ваша миссия – стать настоящими защитниками в онлайн-мире, научиться распознавать угрозы и эффективно им противостоять. В конце занятия каждый из вас получит официальное подтверждение своих навыков – «Сертификат Молодого амбассадора безопасности» через специальный Telegram-бот. Но для этого нам предстоит пройти несколько испытаний. Для			

Этап занятия	Время (мин)	Деятельность учителя	Деятельность учащихся	Используемые материалы/слайды	Цель этапа
		начала мы разделились на команды по названиям: «Кибер-детективы», «Цифровые стражи», «Медиа-аналитики», «IT-защитники». Готовы? Тогда начинаем!"			
Презентация домашнего задания		Организация презентации домашнего задания из Занятия №2.	Представители от групп презентуют свои медиапродукты.	Работы учащихся.	Закрепление пройденного материала, развитие навыков публичных выступлений.
Текст для учителя		"Отлично, команды! Прежде чем мы углубимся в новые аспекты цифровой безопасности, давайте уделим 10 минут презентации вашего домашнего задания из Занятия №2. Напомню, что вашим заданием было разработать информационные материалы, демонстрирующие правовые последствия экстремистской или террористической деятельности. Это очень важный этап, так как он позволяет нам закрепить пройденный материал и увидеть, как вы применили полученные знания на практике. Кто готов начать? Пожалуйста, представьте свои работы на 1–2 минуты, расскажите о вашей идее, о том, что вы хотели донести, и какие выводы сделали в процессе работы. Мы внимательно слушаем …"			
Теоретический блок: «Основные угрозы в сети»		Объясняет понятия. Демонстрирует слайды с инфографикой. Отвечает на вопросы.	Внимательно слушают учителя, могут задавать уточняющие вопросы по ходу объяснения. Фиксируют ключевые моменты в своих записях (если ведут), изучают памятку	Слайд 3: «152-ФЗ» Слайд 4: «149-ФЗ» Слайд 5: «КОАП РФ» Слайд 6: «УК РФ» Слайд 7: «Фишинг» Слайд 8: «Deepfake» Слайд 9: «Утечки данных» Слайд 10: «Кража биометрических данных» Слайд 11: «Кибербуллинг» Слайд 12: «Манипуляция информацией» Слайд 13: «Цифровая зависимость» Приложение 2: Памятка Щит в онлайн-мире»	Дать базовые знания об угрозах в цифровой среде.
Текст для учителя		«Отлично, друзья, спасибо Вам за презентации! Теперь давайте разбираться с очень важным вопросом: а что говорит закон?			

Этап занятия	Время (мин)	Деятельность учителя	Деятельность учащихся	Используемые материалы/слайды	Цель этапа
		Многие из вас, наверное, думают: "Ну что там может быть в законах про интернет?" А на самом деле, цифровое пространство — это не "дикий запад", где каждый делает что хочет. Это полноценная правовая среда, где действуют конкретные законы Российской Федерации, которые защищают ваши права и устанавливают ответственность за нарушения. Сегодня мы с вами станем не просто грамотными пользователями интернета, а юридически подкованными цифровыми гражданами, которые знают свои права и понимают, к каким последствиям могут привести те или иные действия в сети. Посмотрите на экран. Перед вами — основные федеральные законы, которые регулируют нашу жизнь в цифровом мире. Давайте разберём каждый из них подробно». **Федеральный закон № 152-ФЗ «О персональных данных» (3 минуты)** «Начнём с самого важного для каждого из нас закона — ФЗ-152 "О персональных данных". Этот закон был принят в 2006 году и с тех пор неоднократно обновлялся. Что такое персональные данные? Это любая информация, которая относится к конкретному человеку: ваше имя, фамилия, дата рождения, адрес, номер телефона, адрес электронной почты, фотографии, даже IP-адрес вашего компьютера. Всё это — ваши персональные данные. Что регулирует этот закон? Во-первых, он устанавливает ваши права: •Право знать, кто и какие ваши данные обрабатывает •Право требовать удаления или исправления неверных данных •Право отозвать согласие на обработку данных Во-вторых, он устанавливает обязанности компаний и организаций: •Они обязаны получить ваше согласие перед сбором данных •Они обязаны обеспечить безопасность хранения ваших данных •Они не могут передавать ваши данные третьим лицам без вашего согласия Важный момент для вас, как для несовершеннолетних: до 14 лет согласие на обработку персональных данных дают ваши родители или законные представители. С 14 до 18 лет вы можете давать согласие сами, но с письменного согласия родителей. Пример из жизни: когда вы регистрируетесь в социальной сети или скачиваете приложение, и вас просят поставить галочку "Я согласен с обработкой персональных данных" — это как раз требование ФЗ-152. И важно читать, что именно вы разрешаете делать с вашими данными!» **Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (3 минуты)** «Следующий важный закон — ФЗ-149 "Об информации, информационных технологиях и о защите информации". Это более широкий закон, который регулирует всё, что связано с информацией в цифровом пространстве. Ключевые положения этого закона: Право на достоверную информацию — закон гарантирует, что вы имеете право получать		

Этап занятия	Время (мин)	Деятельность учителя	Деятельность учащихся	Используемые материалы/слайды	Цель этапа
		правдивую информацию. Если кто-то распространяет заведомо ложные сведения (фейки), это может быть наказуемо. 2. Защита от вредоносной информации — закон запрещает распространение информации, которая: •Призывает к насилию или экстремизму •Содержит детскую порнографию •Пропагандирует наркотики •Содержит инструкции по созданию оружия или взрывчатых веществ 3. Ответственность за распространение информации — если вы что-то публикуете в интернете, вы несёте за это ответственность. "Я просто репостнул" или "Я не знал, что это запрещено" — не освобождает от ответственности. Важно понимать: этот закон также регулирует работу интернет-сервисов, социальных сетей, мессенджеров. Например, именно на основании этого закона в России блокируются сайты с запрещённым контентом. Пример из практики: если вы увидели в интернете информацию, которая кажется вам опасной или незаконной (например, призывы к насилию в школе), вы можете и должны сообщить об этом взрослым или на специальные горячие линии. Это не "стукачество" — это гражданская ответственность». **Кодекс об административных правонарушениях РФ (КоАП РФ) (3 минуты)** «Теперь поговорим о том, что будет, если законы нарушить. Начнём с административной ответственности— это более "мягкий" вид ответственности по сравнению с уголовной, но всё равно серьёзный. Статья 13.11 КоАП РФ — "Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)" Что это значит? Если кто-то: •Собирает ваши данные без согласия •Передаёт их третьим лицам без разрешения •Не обеспечивает их безопасность То этому человеку или компании грозит штраф: •Для граждан — от 1 500 до 800 000 рублей •Для должностных лиц — от 6 000 до 2 000 000 рублей •Для организаций — от 30 000 до 20 000 000 рублей и выше Повторные нарушения штрафуются строже! Статья 13.15 КоАП РФ — "Злоупотребление свободой массовой информации" Эта статья касается распространения запрещённой информации через интернет. Штрафы здесь уже серьёзнее — от 2 000 до 400 000 рублей для граждан. Важно для вас: С 16 лет вы уже можете быть привлечены к административной ответственности. До 16 лет ответственность несут ваши родители.		

Этап занятия	Время (мин)	Деятельность учителя	Деятельность учащихся	Используемые материалы/слайды	Цель этапа
		Пример: если вы опубликовали в социальной сети чужие личные данные (например, номер телефона одноклассника с подписью "Звоните, троллите"), это может быть квалифицировано как нарушение статьи 13.11 КоАП РФ, и Вы или ваши родители получат штраф». **Уголовный кодекс РФ (УК РФ) (5 минут)** «А теперь самое серьёзное — уголовная ответственность. Это уже не штрафы, а реальные последствия, вплоть до лишения свободы. Давайте разберём основные статьи, которые касаются цифровой безопасности. Статья 137 УК РФ — "Нарушение неприкосновенности частной жизни" Если кто-то: •Незаконно собирает или распространяет сведения о вашей частной жизни •Публикует вашу личную переписку без согласия •Распространяет ваши интимные фотографии или видео То ему грозит: •Штраф до 350 000 рублей •Обязательные работы до 360 часов •Исправительные работы до 1 года •Принудительные работы до 4 лет •Арест до 6 месяцев •Лишение свободы до 5 лет Важно: это одна из самых частых статей, по которым привлекают за кибербуллинг и "слив" личной информации. Статья 272 УК РФ — "Неправомерный доступ к компьютерной информации" Если кто-то: •Взломал ваш аккаунт в социальной сети •Получил доступ к вашему компьютеру или телефону без разрешения •Украл ваши пароли То ему грозит: •Штраф до 500 000 рублей •Исправительные работы до 2 лет •Ограничение свободы до 4 лет •Принудительные работы до 5 лет •Лишение свободы до 7 лет Статья 273 УК РФ — "Создание, использование и распространение вредоносных компьютерных программ"		

Этап занятия	Время (мин)	Деятельность учителя	Деятельность учащихся	Используемые материалы/слайды	Цель этапа
		Это про вирусы, трояны, программы-шпионы. Если кто-то создаёт или распространяет такие программы, ему грозит: •Ограничение свободы до 4 лет •Принудительные работы до 5 лет •Лишение свободы до 6 лет •Дополнительный штраф до 200 000 рублей Статья 274.1 УК РФ — "Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации" Это про серьёзные кибератаки на государственные системы, банки, больницы. Наказание •Принудительные работы до 5 лет •Лишение свободы до 10 лет •Дополнительный штраф до 1 000 000 рублей Важно для вас: С 14 лет наступает уголовная ответственность за тяжкие преступления (например, по статье 137 УК РФ при отягчающих обстоятельствах). С 16 лет — полная уголовная ответственность по всем статьям. Реальный случай из практики: В 2023 году 17-летний подросток был осуждён на 2 года условно за взлом аккаунтов одноклассников и вымогательство денег за возврат доступа. Он думал, что это "просто прикол", но суд посчитал иначе». Запомните главное правило цифрового гражданина: "Не делай в интернете того, что не стал бы делать в реальной жизни. И помни: интернет — это тоже реальная жизнь, со всеми её последствиями". Теперь, когда мы знаем правовые основы, мы готовы перейти к краткому обзору цифровых угроз. Первая угроза, о которой мы поговорим, – это фишинг. Кто-нибудь слышал это слово? Что оно означает? (Выслушать ответы учащихся). Верно! Фишинг – это вид интернет-мошенничества, целью которого является получение доступа к вашим конфиденциальным данным: логинам, паролям, номерам банковских карт. Мошенники маскируются под известные бренды, банки, государственные учреждения и отправляют вам поддельные письма, сообщения или создают фальшивые сайты. Главное правило: всегда проверяйте адрес отправителя и URL-адрес сайта. Если что-то вызывает подозрение – не переходите по ссылкам и не вводите свои данные. Основные статьи ответственности: Статья 272 УК РФ (неправомерный доступ к компьютерной информации), статья 159.6 УК РФ (мошенничество в сфере компьютерной информации). Далее, Deepfake (Дипфейк) и искусственный интеллект – это использование нейросетей для создания поддельных видео, аудио или изображений, которые выглядят очень реалистично. Основные статьи ответственности: Статья 137 УК РФ (нарушение неприкосновенности частной жизни), статья 128.1 УК РФ (клевета). Следующая угроза – утечки данных. Вы, наверное, слышали новости о том, как крупные компании теряют данные своих пользователей. Что это значит для нас? Это значит, что наши личные данные – имена, фамилии, адреса электронной почты, телефоны, а иногда и пароли – могут попасть в руки злоумышленников. Как себя защитить? Используйте сложные и уникальные пароли для разных сервисов, включите двухфакторную		

Этап занятия	Время (мин)	Деятельность учителя	Деятельность учащихся	Используемые материалы/слайды	Цель этапа
		аутентификацию везде, где это возможно, и будьте осторожны с тем, какой информацией вы делитесь в интернете. Основные статьи ответственности: Статья 5, 6, 7 ФЗ № 152-ФЗ (принципы обработки персональных данных, согласие, конфиденциальность). Отдельно выделим кражу биометрических данных – это незаконный сбор и использование твоих биометрических данных (отпечатки пальцев, изображение лица, голос) для мошенничества или подмены личности. Основные статьи ответственности: Статья 10 ФЗ № 152-ФЗ (обработка специальных категорий персональных данных), статья 6 и 9 ФЗ № 152-ФЗ (согласие на обработку биометрических данных). Далее – кибербуллинг. Это травля, преследование или запугивание в интернете. Это могут быть оскорбления, распространение слухов, публикация компрометирующих фотографий или видео. Кибербуллинг может иметь очень серьезные последствия для психического здоровья человека. Если вы столкнулись с кибербуллингом или стали его свидетелем, не молчите! Расскажите об этом взрослым, заблокируйте обидчика, сохраните доказательства. Помните, что вы не одни, и вам всегда помогут. Основные статьи ответственности: Статья 5.61 КоАП РФ (оскорбление), статья 137 УК РФ (нарушение неприкосновенности частной жизни), статья 128.1 УК РФ (клевета). Далее - манипуляция информацией. В интернете очень много информации, и не вся она правдива. Фейковые новости, пропаганда, искажение фактов – все это направлено на то, чтобы повлиять на ваше мнение, заставить вас поверить во что-то или сделать что-то. Как этому противостоять? Развивайте критическое мышление! Проверяйте информацию в нескольких источниках, обращайте внимание на авторитетность источника, анализируйте, кто и зачем мог опубликовать ту или иную новость. Не верьте всему, что видите и читаете в интернете. Основные статьи ответственности: Статья 15.3 ФЗ № 149-ФЗ (блокировка недостоверной информации), статья 13.26 КоАП РФ (нарушение порядка распространения информации в сети Интернет). И, наконец, цифровая зависимость – это чрезмерное использование социальных сетей, видеохостингов и игр, которое мешает учёбе, общению с друзьями и здоровью. Основные статьи ответственности: Статья 16 ФЗ № 149-ФЗ (защита прав пользователей на достоверную информацию). Помните, что знание – это уже половина защиты!"			
Командные игра-квест «Цифровой щит»		Объяснение правил. Выдача кейсов командам. Консультирование групп. Консультирует группы. Отвечает на вопросы.	Работают в командах, анализируют кейсы, разрабатывают «План защиты».	Слайд 14: «Цифровой щит»; Приложение 3: Кейс-карточки «Цифровые угрозы»; Приложение 4: Рабочий лист «План защиты».	Применить теоретические знания на практике, развить навыки командной работы.
Текст для учителя		Уважаемые, Амбассадоры! Теперь, когда мы знаем основные угрозы, пришло время применить наши знания на практике в нашей командной игре под названием «Цифровой щит». Ваша задача – стать настоящими кибер-защитниками и разработать план действий для различных ситуаций. Каждая команда получит набор из 2-х «Кейс-карточек «Цифровые угрозы» (Приложение 3). На каждой карточке описана реальная или потенциальная ситуация, связанная с цифровой безопасностью. Ваша задача – выбрать 1 кейс (если успеете, то 2) внимательно изучить его, определить, какая угроза в нем			

Этап занятия	Время (мин)	Деятельность учителя	Деятельность учащихся	Используемые материалы/слайды	Цель этапа
		присутствует, и разработать «План защиты» (Приложение 4) – то есть, пошаговый алгоритм действий, который поможет человеку в этой ситуации. У вас будет 12 минут на анализ кейсов и разработку планов. Важно- если успеете сделать 2 кейса это будет высший пилотаж, можно разделить ответственность внутри команды. После этого каждая команда представит свой план защиты на 3 минуты, если вы сделали 2 кейса, то у вас будет по 1,5 минуты на презентацию каждого. Помните, что важна не только правильность решения, но и креативность, а также четкость и логичность ваших рекомендаций. Я буду ходить между командами и отвечать на ваши вопросы. Если вы готовы, приступаем!" (После 12 минут – выслушать презентации каждой группы, 3 минуты на выступление +2 минуты комментарий учителя)			
Получение сертификатов и подведение итогов всего курса		Инструктаж по работе с Telegram-ботом. Обсуждение результатов курса, рефлексия.	Каждый ученик заходит в Telegram-бот @pushkin_help_bot и получает сертификат. Делятся впечатлениями, обсуждают, что нового узнали.	Слайд 15: «Цифровой сертификат» Слайд 16: «Рефлексия по итогам курса» Слайд 17: «Заключение»	Закрепить полученные знания, создать ситуацию успеха. Обобщить полученный опыт, мотивировать на дальнейшее изучение темы.
Текст для учителя		Ну вот и подошел наш курс по безопасности, прежде чем мы завершим наше занятие, давайте вместе вспомним весь путь, который мы прошли за эти четыре встречи. Это был не просто курс — это было настоящее обучение защитников, которые теперь могут защитить себя, своих друзей, свою семью от серьёзных угроз. Давайте вспомним, что мы изучили, чему научились и как это изменило нас» Итак, наш путь начался четыре занятия назад... На первом занятии мы стали участниками «Лаборатории анализа информации». Мы узнали, что такое экстремизм и терроризм, какие формы они принимают — политический, националистический, религиозный, социальный, киберэкстремизм, экотерроризм. Что мы сделали? •Научились распознавать маркеры экстремистской деятельности — в идеологии, в поведении, в информационной среде. •Поняли, какие факторы делают человека уязвимым к вербовке: одиночество, поиск смысла, финансовые трудности, желание принадлежать к группе. •Разработали информационную памятку для сверстников, чтобы помочь им распознать риски и избежать вовлечения. На втором занятии мы стали «Юридическими консультантами» и погрузились в мир права и ответственности.			

Этап занятия	Время (мин)	Деятельность учителя	Деятельность учащихся	Используемые материалы/слайды	Цель этапа
		•Изучили конкретные статьи Уголовного кодекса РФ (УК РФ) и Кодекса об административных правонарушениях (КоАП РФ), которые регулируют ответственность за экстремистскую и террористическую деятельность. •Поняли, что даже репост экстремистского контента в соцсетях — это уже нарушение закона, за которое можно получить штраф или даже уголовное наказание. •Узнали, что ответственность наступает с 14 лет за тяжкие преступления (терроризм, участие в террористической организации), а с 16 лет — за большинство экстремистских действий. На третьем занятии мы стали «Аналитиками безопасности» и научились распознавать манипуляции и противостоять вербовке. Что мы сделали? •Изучили этапы вербовки: установление контакта, создание доверия, изоляция, идеологическая обработка, вовлечение в действия. •Научились распознавать манипулятивные техники: эмоциональное давление, обещания, угрозы, создание чувства долга, эксплуатация уязвимостей. •Разработали алгоритмы действий при подозрении на вербовку: как распознать, как отказать, куда обратиться за помощью. •Проанализировали реальные кейсы вербовки и разработали стратегии защиты. И вот сегодня, на четвёртом занятии, мы завершили наш путь, став «Молодыми амбассадорами безопасности». Какие моменты были для вас наиболее интересными или полезными? (Выслушать ответы учащихся). "Молодцы, Амбассадоры! Вы отлично справились с заданием, проявили себя как настоящие защитники цифрового мира. Теперь пришло время получить заслуженное подтверждение ваших навыков. Как я уже говорил в начале занятия, каждый из вас получит «Сертификат Молодого амбассадора безопасности». Для этого нам понадобится ваш смартфон и приложение Telegram. Пожалуйста, достаньте свои смартфоны. Откройте Telegram и найдите бота по имени @pushkin_help_bot. Взаимодействие с ботом очень простое: вам нужно будет следовать его инструкциям. Также вы можете воспользоваться памяткой, в которой указан QR-код для доступа к боту. Скорее всего, он попросит вас ввести ваше имя и фамилию, чтобы персонализировать сертификат от Генеральной прокуратуры РФ. После этого бот сгенерирует и отправит вам ваш личный сертификат. Убедитесь, что вы сохранили его, возможно, сделав скриншот или сохранив файл. Этот сертификат – подтверждение того, что вы теперь официально являетесь Молодым амбассадором безопасности и готовы защищать себя и других в онлайн-мире. Если у кого-то возникнут сложности, поднимите руку, я подойду и помогу." (Если в классе нет интернета или у кого-то нет смартфона – это можно и нужно сделать дома, зайдя в бот по адресу @pushkin_help_bot, который ученики должны записать или использовать информацию из Памятки, в которой указан QR-код для доступа к боту)		

Важные принципы проведения:

- Поддерживать конфиденциальность обсуждений
- Проявлять тактичность при обсуждении сложных тем
- Поощрять критическое мышление, а не готовые ответы
- Подчеркивать практическую значимость получаемых знаний

Дополнительные вопросы для проверки понимания (опционально, если осталось время)

Учитель может задать классу:

- «Поднимите руку, кто из вас когда-либо давал согласие на обработку персональных данных? А кто читал, что именно он разрешает?»
- «Как вы думаете, почему закон особенно защищает персональные данные несовершеннолетних?»
- «Представьте ситуацию: ваш одноклассник опубликовал в группе класса вашу личную переписку. Какой закон он нарушил? Какая ответственность ему грозит?»
- «С какого возраста наступает уголовная ответственность за компьютерные преступления?»

Дополнительные рекомендации

Для учителя:

- **Темп речи:** умеренный, с паузами для осмысления информации
- **Интонация:** серьёзная, но не запугивающая. Акцент на защите прав, а не только на наказаниях
- **Визуализация:** активно использовать слайды, указывать на конкретные законы
- **Примеры:** приводить реальные, понятные подросткам ситуации
- **Вовлечение:** задавать риторические вопросы, поощрять комментарии учащихся
- **Баланс:** не перегружать юридическими терминами, объяснять простым языком

Ключевые акценты:

- Закон защищает, а не только наказывает
- Знание законов — это сила и защита
- Ответственность наступает реально, это не абстракция
- Интернет — это часть реальной жизни с реальными последствиями

5. Приложения

- Приложение 1: Карточки для деления на команды.
- Приложение 2: Памятка «Щит в онлайн-мире».
- Приложение 3: Кейс-карточки «Цифровые угрозы».
- Приложение 4: Рабочий лист «План защиты».
- Приложение 5: Презентация занятия 4