Министерство Просвещения Российской Федерации

Московский государственный психолого-педагогический университет

ДИАЛОГ РЕГИОНЫ

Институт изучения детства, семьи и воспитания

РАЗГОВОРЫ О ВАЖНОМ

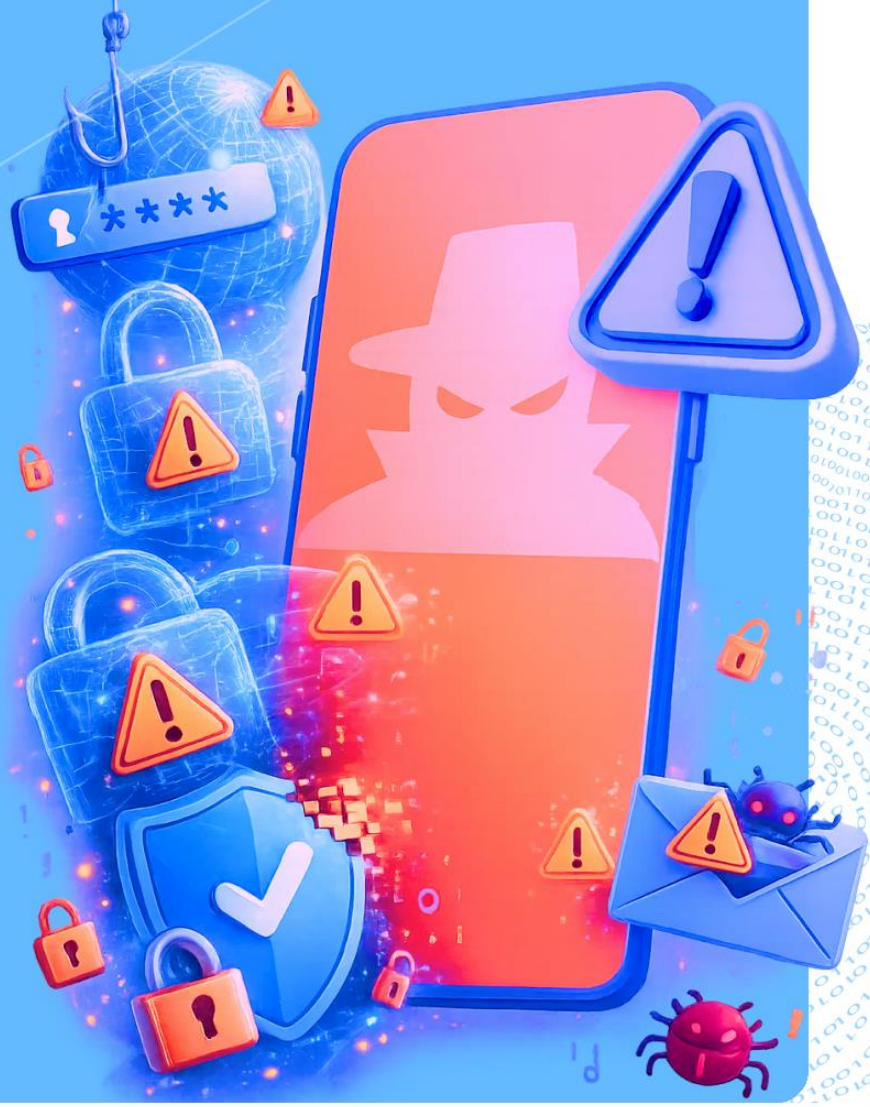
2026 Год единства народов России

жизнь | гражданственность

Сценарий занятия | СПО

ЦИФРОВОЙ ЩИТ

ОСНОВНЫЕ ПРАВИЛА БЕЗОПАСНОСТИ В СЕТИ ИНТЕРНЕТ



СЦЕНАРИЙ

занятия «РАЗГОВОРЫ О ВАЖНОМ»

для обучающихся по программам среднего профессионального образования

Занятие 24

Цифровой щит.
Основные правила безопасности в сети Интернет

Дата занятия: 2 марта 2026 года.

Цели занятия: осмысление понятия «кибергигиена»; расширение представлений об основных видах киберугроз и способах противодействия им; формирование у обучающихся осознанного отношения к цифровой среде как к пространству, требующему личной ответственности; формирование осознанной взаимосвязи между личной цифровой гигиеной и безопасностью государства; развитие критического мышления и цифровой грамотности.

Формирующиеся ценности: жизнь, гражданственность.

Основные смыслы

- Личная ответственность в цифровой среде — это осознанная забота о себе, которая становится вкладом в безопасность общества и государства.
- Цифровой след — это необратимая совокупность данных. Информация, размещенная в виртуальной среде, становится общедоступной и может быть использована злоумышленниками либо обращена против самого пользователя, в том числе в рамках противоправных действий.

- Цифровой мир — часть единого правового поля государства. Противоправные действия, совершаемые в цифровом пространстве, не анонимны и преследуются по закону.
- В ситуации неопределенности или угрозы в сети Интернет необходимо незамедлительно обратиться за помощью в полицию.

Продолжительность занятия: 30 минут.

Рекомендуемая форма занятия: познавательная беседа. Занятие включает просмотр видеоматериалов, выполнение практического задания.

Комплект материалов:

- сценарий;
- методические рекомендации;
- дополнительные материалы;
- видеоматериалы;
- практическое задание;
- презентация.

Мотивационно-целевой этап: просмотр видеоролика-анонса, беседа.

Основной этап: просмотр видеороликов, беседа, выполнение практического задания.

Заключительный этап: беседа.

Мотивационно-целевой этап

Педагог: Сегодня мы продолжим наш разговор о цифровой безопасности, который начали еще в сентябре. Наша цель — детально разобрать конкретные мошеннические схемы, в которые чаще всего вовлекают подростков, и, опираясь на ваш уже

имеющийся опыт, **выработать алгоритмы защиты, чтобы обезопасить себя и не стать жертвой злоумышленников.**

Педагог организует ***просмотр видеоролика-анонса с Кариной Каграманян.***

Педагог: Интернет дает нам различные возможности: учеба, общение, друзья. Но чем больше времени мы проводим в сети, тем выше риски. От банальной утечки данных **до реальных сроков лишения свободы за участие в преступных схемах.**

Вопросы для обсуждения:

- Как думаете, почему мошенники в интернете так часто охотятся именно на подростков? Что делает эту возрастную группу удобной мишенью?
- Слышали ли вы реальные истории, когда ровесники попадали в неприятные ситуации из-за переписки или сомнительной подработки? Чем заканчивалось?
- И еще один важный вопрос: почему люди, которых уже обманули, часто молчат и никому не рассказывают — даже родителям? Что их останавливает?

Ответы обучающихся.

Основной этап

Педагог: Многие по ошибке или невнимательности становятся **соучастниками цифровых преступлений.** Давайте послушаем истории ребят, которые готовы поделиться своим опытом, чтобы предостеречь других.

Педагог организует ***просмотр и обсуждение видеоролика-интервью с подростками, совершившими противоправные действия под влиянием злоумышленников.***

Вопросы для обсуждения:

- В ролике парень говорит: «У меня даже ни одной малейшей мысли не возникло об обмане». Как вы думаете почему?
- Какой фразой из видео мошенники усыпили бдительность мальчика? («Об этом даже никто не узнает»). Почему, если кто-то обещает, что «никто не узнает», это всегда должно настораживать?
- Мальчик думал, что занимается «подработкой», а полиция назвала это поступок «терроризмом». Почему его действия (поджог на железной дороге) считаются таким страшным преступлением?
- Представьте, что вам в мессенджере пишет незнакомец и предлагает легкие деньги за то, чтобы вы что-то сфотографировали, передали или подожгли. Назовите три ваших первых действия. (Не отвечать. Сделать скриншот. Показать родителям/учителю и обратиться в полицию)
- Во втором ролике герой говорит: «Где-то внутри я, конечно, понимал, что что-то не так». Что именно его должно было насторожить с самого начала? *(Слишком легкие деньги, работа с наличными и криптой, фраза: «Не задавай вопросов»)*
- Парень думал, что он умный, потому что удалил переписки. Почему это не сработало? Как его нашли? *(Камеры, геолокация телефона, восстановление данных экспертами — цифровой след)*
- Почему мошенники всегда ищут курьеров? Кто рискует больше — организатор или курьер? *(Курьер рискует*

свободой напрямую, а мошенники часто находятся за границей)

- Что он мог сделать вместо того, чтобы ехать к бабушке? *(Понять, что это мошенники, не отвечать, сделать скриншот, рассказать родителям и сообщить в полицию)*

Ответы обучающихся.

Педагог: Если вы переводите чужие деньги через свой счет, таким образом вас делают частью преступной схемы. Ваш счет используют как транзитный — через него проводят деньги, полученные незаконным путем, и вы становитесь *соучастником мошенничества*. **И ответственность за это наступает по Уголовному кодексу.** Фразы «я не знал» или «меня просто попросили» в суде не освобождают от ответственности. Кто такой соучастник и как отличить нормальное предложение от опасного?[1]

Ответы обучающихся.

Педагог: В Иркутской области в сентябре прошлого года произошла следующая история: 18-летний юноша поверил человеку, который представился сотрудником финансового мониторинга. Перевел на «безопасный счет» бабушкины сбережения, а потом по указке лжесотрудника ФСБ поджег объект инфраструктуры. Сейчас ему грозит до 20 лет по статье «Террористический акт». Такая мошенническая схема состоит из трех шагов. Сначала — легенда про «безопасный счет» или

[1] Методический комментарий для педагога
- Если за простые действия обещают очень высокий доход — это повод насторожиться. Легких денег не бывает.
- Если от вас требуют доступ к банковскому счету, карте или аккаунту — это не работа, а ловушка. Личные данные и доступы нельзя передавать никому.
- Если собеседник слишком настойчив, убеждает, что «все законно», «все так делают», «я тоже так работаю», — скорее всего, он пытается на вас морально давить. Законные предложения не нуждаются в таком давлении.

необходимость срочного перевода или передачи средств под предлогом их «спасения» или «декларации». Потом — прикрытие авторитетом: «ФСБ», «госструктуры». И наконец — ступенчатое вовлечение: сначала перевод денег, потом поджог. Человек уже нарушил закон, и страх ответственности (или шантаж) становится инструментом для вовлечения в последующие противоправные действия. Что делать, если вам такое пишут?

Ответы обучающихся.

Педагог: Не вступайте в диалог. Сразу блокируйте. Расскажите взрослым, чтобы увидеть ситуацию со стороны. **Легкие деньги — всегда ловушка.**

Вопросы для обсуждения:

- Как вы думаете, с чего началась эта история? С какого сообщения, с какого обещания или предложения?
- Почему молодой человек поверил мошеннику? Что сыграло роль: возраст, наивность, доверие к «официальным» людям, желание заработать?
- Если бы вы узнали, что ваш друг согласился на такую «подработку», — какие слова вы бы подобрали, чтобы объяснить ему риски?

Ответы обучающихся.

Педагог: Можно получить такое предложение в мессенджерах: «Просто дай доступ к аккаунту — получишь 1000 рублей за 5 минут». Аккаунты используют зарубежные мошеннические кол-центры, чтобы обходить блокировки и продолжать обманывать людей. Чем это опасно? Для чего могут использовать ваш аккаунт? *(Через него могут рассылать*

мошеннические сообщения, распространять экстремистский контент, организовывать схемы обмана)

Ответы обучающихся.

Педагог: Еще одной распространенной проблемой в интернете является деструктивный контент.

Вопросы для обсуждения:

- Что такое деструктивный контент? Как его отличить? *(Обычно — громкие заголовки: «Смотри, пока не удалили», «Только для своих», «Слив». Или картинки и видео, от которых становится не по себе. Или сообщения, где кого-то унижают, угрожают, призывают травить)*
- Что делать, если вы наткнулись на такой контент?[2] Нужно ли пересылать или сохранять эту информацию?

Ответы обучающихся.

Педагог: Пересылая подобные материалы, вы становитесь частью распространения. Как устроены **деструктивные сообщества?** Как вообще люди в них попадают?

Ответы обучающихся.

Педагог: Первый **способ втягивания подростков в такие сообщества** — через обещание исключительности. Вам говорят:

[2] Методический комментарий
Необходимо сразу закрыть страницу и выйти. Не вступать в диалог, не комментировать, не спорить. Очень важно рассказать об увиденном тем, кому доверяете. Родителям, учителю, кому-то из взрослых, кто сможет адекватно оценить ситуацию. Ваша эмоциональная реакция — это то, на что рассчитывают те, кто создает такой контент.

«Ты не такой, как все. Ты видишь то, что скрыто от других». Второй — через секретность. «То, что здесь происходит, остается здесь. Если расскажешь — тебя не поймут». Так создается иллюзия доверия. Третий — через давление или жалость. «Ты что, слабак?» Или наоборот: «Тебя все обижают, а мы — твоя настоящая семья». Что продвигают такие сообщества?[3] *(Презентация к занятию, слайд 2).* Знаете ли вы, как можно защититься, чтобы не попасть в деструктивное сообщество?[4] *(Презентация к занятию, слайд 3)*

Ответы обучающихся.

Педагог: Цифровая гигиена — навыки, которые помогают защитить личные данные, не попадаться на уловки мошенников и сохранять спокойствие в сети. Давайте перечислим все правила, которые помогут нам обезопасить себя в интернете *(презентация к занятию, слайды 4–5).*

*Педагог организует **выполнение практического задания.** Обучающиеся делятся на команды и разбирают кейсы по предложенному алгоритму (приложение, презентация к занятию, слайды 6–13). Задачи обучающихся: 1) найти ошибку — тот самый момент, когда человек мог сказать «нет», но не сказал; 2) предложить алгоритм: что делать жертве прямо сейчас; 3) сформулировать, как надо было поступить, чтобы не попасть под контроль мошенников.*

---

[3] Методический комментарий для педагога
- Кибербуллинг — систематическая травля в сети.
- Сваттинг — ложные вызовы спецслужб по чужому адресу.
- Доксинг — публикация личных данных без согласия.
- Вербовка в криминальные схемы (сим-боксы, закладки, переводы денег).

[4] Методический комментарий для педагога
1. Если группа закрытая, вход только по приглашению — это повод насторожиться.
2. Если вас уговаривают сделать то, что вызывает сомнение, — скажите «нет». Сомнение — это защитный механизм.
3. Расскажите кому-то из взрослых. Родителям, учителю, психологу. Их задача — не оценивать, а помочь.
4. Помните: «ты особенный», «только для своих», «мы — семья» — не забота со стороны чужого человека, это контроль.

Заключительный этап

Педагог: Давайте подведем итог. Какие важные выводы вы для себя сделали?

Ответы обучающихся.

Педагог: Сегодня мы обсудили важные правила, которые касаются не только вашего спокойствия, безопасности, репутации, но и свободы. К сожалению, цифровой мир не безопаснее реального мира, в котором есть преступники и мошенники. Сотрудники киберполиции готовы помочь всем гражданам защитить свои права и обезопасить себя в интернете, но наша личная ответственность и внимательность также играют важную роль. Цифровой след всегда приведет к тому, кто его оставил. Будьте умнее мошенников и помните, что незнание закона не освобождает от ответственности.

Вопросы для обсуждения:

- Почему важно развивать критическое мышление при анализе информации, поступающей из интернета?
- Какое главное правило вы можете придумать для себя при любом подозрительном звонке или сообщении? *(Положить трубку, рассказать о звонке любому взрослому, сделать скрин сообщения и отправить его в полицию, не разговаривать с незнакомыми людьми в одиночку, а поставить на громкую связь)*
- К кому можно обратиться, если не знаешь, как поступить в сложной ситуации? Почему важно не пытаться решить всё самостоятельно и не бояться показаться слабым.

Ответы обучающихся.

Педагог: Если вам нужна помощь, вы можете позвонить по единому общероссийскому телефону доверия или обратиться в полицию *(презентация к занятию, слайд 14).*

Постразговор

Уважаемые коллеги!

Предлагаем вам и обучающимся поучаствовать во Всероссийской акции «Движения Первых» *(презентация к занятию, слайд 15).*

Что почитать

- Белоус А. «Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения»

Что посмотреть

- Молодежный цифровой омбудсмен о защите детей в сети: https://vk.com/wall-125745261_19874
- Цифровая гигиена: рецепты от МТС: https://vk.com/wall-214524833_77783
- Секреты защиты аккаунта от VK: https://vk.com/wall-214524833_77902

- Гули Базарова о защите от травли: https://vk.com/wall-214524833_78217
- Подкаст «Разговор по делу. Инфобезопасность»: https://vk.com/video-139211235_456239656, https://vk.com/video-139211235_456239642

Проектная и внеурочная деятельность, внеклассные мероприятия

- «Школа кибербезопасности “Движения Первых”»: в рамках постразговора участникам предлагается попробовать себя в роли юного наставника для сверстников. Для этого необходимо перейти на страницу проекта киберволонтеры.будьвдвижении.рф, выбрать номинацию и заполнить заявку. Затем предлагается изучить теоретические материалы по цифровой безопасности, а после этого провести просветительское мероприятие «КиберУрок» для одноклассников, участников первичного отделения, друзей или иного коллектива, на котором участник поделится полезными знаниями о безопасности в цифровой среде. Дополнительные материалы и форматы проведения мероприятий доступны по ссылке: https://id.pervye.ru/projects/2387.
- Онлайн-марафон «Навыки для жизни»
  - Навыки кибербезопасности: https://vk.com/wall-214524833_165091
  - Цифровая грамотность: https://vk.com/wall-214524833_177432
  - Цифровые защиты: https://vk.com/wall-214524833_178300
  - Безопасные игры: https://vk.com/wall-214524833_180738

Приложение

Кейсы для практического задания

Кейс	Содержание
Кейс 1. «Курьер»	Парню в мессенджере предложили подработку: забирать наличные у пожилых людей и переводить на биткоин-кошелек. За первый заказ заплатили 5000. На второй раз его задержала полиция. Оказалось, это были деньги обманутых бабушек *(презентация к занятию, слайды 6–7).*
Кейс 2. «Украли аккаунт»	Девушке написали: «Дайте доступ к аккаунту на час, нужно проголосовать в конкурсе, заплатим 1000». Она дала код. Через час с ее аккаунта начали рассылать сообщения всем контактам: «Срочно займи 10 000, потом объясню» *(презентация к занятию, слайды 8–9).*
Кейс 3. «Фото с геолокацией»	Парень вступил в чат фанатов игры. Ему предложили «особую миссию» — сфотографировать трансформаторную будку во дворе и прислать координаты. За это обещали «крутой скин». Он сделал фото. Через неделю пришли с обыском: оказалось, это была подготовка к теракту *(презентация к занятию, слайды 10–11).*
Кейс 4. «Розыгрыш?»	Парень несколько месяцев состоял в Telegram-канале с розыгрышами призов. Администраторы создавали теплую атмосферу «своих». Через пару месяцев ему написали: «Для участия в закрытом розыгрыше суперприза нужно подтвердить личность — пришли фото паспорта и селфи с ним. Это конфиденциально». Он отправил. Через неделю ему начали звонить из микрофинансовых организаций — на его имя пытались оформить займы. А фото паспорта выложили в открытый канал *(презентация к занятию, слайды 12–13).*

Алгоритм решения кейса

1. **Что случилось?** (Краткий пересказ)
2. **Где была совершена ошибка?** (Какое правило цифровой гигиены нарушено)
3. **Какие последствия могут возникнуть в данной ситуации для ее участников?** (Моральные, социальные, правовые)
4. **Что делать жертве?** (Алгоритм действий)
5. **Как надо было поступить правильно?** (Идеальный сценарий)