



СЦЕНАРИЙ ЗАНЯТИЯ | 6–7 классы

БЕЗОПАСНОСТЬ В СЕТИ ИНТЕРНЕТ. СОЦСЕТИ. КАК ЗАЩИТИТЬСЯ ОТ МОШЕННИКОВ.

жизнь

гражданственность

СЦЕНАРИЙ

занятия «РАЗГОВОРЫ О ВАЖНОМ»

для обучающихся 6–7 классов

Занятие 6

Соцсети. Как защититься от мошенников. Безопасность в сети Интернет

Дата занятия: 12 октября 2026 года.

Цели занятия: расширение представлений обучающихся о цифровой среде, ее возможностях и основных угрозах, с которыми человек может столкнуться при использовании интернета и социальных сетей; раскрытие значения ответственного и безопасного поведения в сети, умения распознавать потенциально опасные ситуации, защищать личную информацию и соблюдать границы личного пространства; формирование ответственного отношения к собственному поведению в цифровой среде, уважительного отношения к другим пользователям и неприятия мошенничества, кибербуллинга и других форм опасного или недопустимого поведения в сети.

Формируемые ценности: жизнь, гражданственность.

Основные смыслы

- Интернет — это важная часть современной жизни, которая открывает большие возможности для общения, обучения, творчества и получения информации, но требует ответственного поведения и навыков работы с информацией.
- Цифровая среда может быть источником различных угроз, поэтому важно уметь распознавать опасные ситуации и понимать, как действовать, чтобы защитить себя.
- Уважительное отношение к другим людям в сети так же важно, как и в реальной жизни: слова и поступки в цифровой среде могут иметь реальные последствия.
- Если ситуация в интернете вызывает тревогу, страх или сомнение,

важно не оставаться с проблемой один на один и своевременно обратиться за помощью к взрослому.

Продолжительность занятия: 45 минут.

Рекомендуемая форма занятия: познавательная беседа. Занятие включает просмотр видеоматериалов, выполнение интерактивного и практического заданий.

Комплект материалов:

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

Этапы занятия:

Мотивационно-целевой этап: беседа.

Основной этап: беседа, просмотр и обсуждение видеороликов, выполнение интерактивного и практического заданий.

Заключительный этап: беседа.

Мотивационно-целевой этап (5 минут)¹

! Учитель: Мы проводим в цифровом пространстве не меньше времени, чем в обычном. Это целый мир — со своими законами и возможностями. Как и в реальной жизни, здесь можно встретить искренних, добрых людей или столкнуться с обманом, а ошибочные действия могут привести к осязаемым последствиям.

Вопросы для обсуждения:

- С какими опасностями можно столкнуться именно в соцсетях?

¹ Методический комментарий: знаком «!» в сценарии обозначены обязательные компоненты занятия, знаком «*» обозначены вариативные компоненты занятия.

(Взлом, мошенники, травля, вредоносные ссылки, незнакомцы)

- Почему в интернете очень легко попасть в ловушки мошенников? *(Злоумышленники часто маскируются — пишут от лица банка, госорганов или даже от лица знакомых вам людей; также мошенники часто играют на эмоциях, и под давлением человек сообщает ту информацию, которую следовало бы скрывать от посторонних)*
- Как вы обычно проверяете, безопасно ли то, что вам пришло в личном сообщении, достоверна ли информация, которую вы увидели в соцсетях²?

Ответы обучающихся.

! Учитель: Одна из самых хитрых и распространенных угроз — это социальный инжиниринг. Звучит сложно, но, на самом деле, этот термин обозначает не ситуацию, когда преступник взламывает не компьютер, а нас: нашу доверчивость, наше желание быть своим в компании или получить что-то быстро. И если раньше мошенники пугали вирусами: «Твой компьютер заблокирован!», «Твои фото удалят!», и это работало на взрослых, то для современного молодого пользователя придумываются совершенно новые методики обмана: зачем пугать, когда можно заинтриговать различными способами.

Вопросы для обсуждения:

- Как вы думаете, чем можно заинтересовать школьника в интернете? *(Познакомиться с новыми людьми, поучаствовать в конкурсе, легко заработать деньги и т. д.)*
- Что может заставить вас нажать на ссылку, ответить или отправить что-то незнакомцу?
- Почему мошенники чаще всего просят не деньги напрямую, а код из СМС, фотографию дневника или номер карты родителей?

Ответы обучающихся.

! Учитель: Даже самый надёжный, казалось бы, сайт не даёт гарантии безопасности. Мошенники бьют точно в цель: туда, где мы не

² Методический комментарий: важно не принимать на веру первое увиденное утверждение, а всегда проверять информацию в нескольких независимых источниках. Разные точки зрения и сопоставление данных из авторитетных СМИ, официальных отчётов и экспертных материалов позволяют сформировать более точную картину происходящего.

разбираемся, где ошибаемся, где боимся или доверяем сомнительным источникам. Самое первое и главное правило: не передавать личные данные тем, кто обещает золотые горы в закрытых чатах (*презентация к занятию, слайд 2*). О том, как распознать подобные ловушки и не попасться, мы и поговорим сегодня.

** Вопросы для обсуждения:*

- Как вы думаете, почему мошенники продолжают успешно действовать, несмотря на постоянный технологический прогресс?
- Получали ли вы когда-нибудь сообщения от незнакомцев в интернет-пространстве, например в игре?
- Если вы оказывались в подобной ситуации, то что вы предпринимали?

Ответы обучающихся.

Основной этап (30 минут)

! Учитель организует **просмотр видеоролика-интервью с оперуполномоченным отдела по предупреждению распространения и выявлению деструктивной и запрещенной информации в сети интернет УБК МВД России Кириллом Романовым и начальником отдела контентного обеспечения АНО «Диалог Регионы» Евгенией Варакиной.**

! Учитель: Интернет создан для общения, обучения и творчества, но пользоваться им надо умело и безопасно. Далеко не все приходят в соцсети за дружбой. Для некоторых это становится местом охоты. Мошенники, распространители запрещённых веществ, психически нездоровые люди быстро поняли: Всемирная паутина даёт то, что им нужнее всего, — возможность оставаться незамеченными. Именно анонимность делает их опасными. Остаться защищёнными онлайн помогут правила. Назовите те, которые вам уже известны.

Ответы обучающихся. (Возможными ответами могут быть: не передавать личные данные, фотографии документов, делать сложные пароли, не выкладывать компрометирующую информацию и т. д.)

! Учитель: Первое и самое главное — прервать общение с виртуальным знакомым, как только он предложил что-то, вызывающее сомнения (чаще всего впоследствии это становится противозаконным

действием). Но ещё лучше — сделать шаг раньше: рассказать семье о том, что такое знакомство вообще состоялось. Даже если пока никто ни к чему плохому не призывал. Умение открыто обсуждать подозрительные ситуации с близкими до того, как что-то было сделано, — и есть настоящая защита (*презентация к занятию, слайд 3*).

! Вопросы для обсуждения:

- Если вы сомневаетесь, безопасно ли то, что происходит в сети, как разумнее поступить? (*Остановиться и спросить взрослого*)
- По каким признакам можно распознать опасное предложение?
- Почему нельзя давать свой пароль от игр и соцсетей, даже если тебе обещают подарки, деньги и сюрпризы?
- Какую информацию о себе и своей семье нельзя раскрывать в своих профилях в социальных сетях? (*Здесь учитель может обратить внимание на то, что в социальных сетях важно осознанно относиться к объёму личной информации, которой мы делимся. При общении с малознакомыми людьми не стоит сразу раскрывать сведения о себе, своей семье, месте жительства, планах или других личных обстоятельствах. Доверие формируется постепенно, поэтому в начале знакомства безопаснее выбирать нейтральные темы и самостоятельно определять границы того, чем вы готовы делиться*)

Ответы обучающихся.

! Учитель: Если вам обещают деньги без усилий и просят логин, пароль или данные карты — это обман. Не передавайте доступ к аккаунтам и банковским данным никому, даже если вас уверяют: «Это безопасно, я уже так делал!»

Мошенники даже могут убеждать, что своими действиями человек спасёт своих родных и близких в какой-то опасной ситуации. Как можно проверить, правда это или нет? (*Прервать разговор с мошенником и самостоятельно связаться по телефону со своими родными*)

Ответы обучающихся.

Учитель: Наши действия в цифровом пространстве влияют не только на нас самих, но и на общество в целом. Как думаете почему? Что вам известно о цифровом следе?

Ответы обучающихся.

! Учитель: Смартфон — это компьютер, который круглосуточно собирает информацию о своём владельце: фото, переписки, увлечения, места, где он бывает. Эти данные могут позволить злоумышленникам узнать о человеке как можно больше.

Всё, что попадает в сеть, формирует уникальный цифровой след. По нему можно создать цифрового двойника — и неизвестно, как его используют. Поэтому важно внимательно относиться к словам, действиям и особенно к личным фотографиям. Наша безопасность зависит от нас: мы всегда должны стараться оценивать возможные риски.

Учитель организует выполнение **интерактивного задания «Действия в сети Интернет»**, в ходе которого обучающимся предлагаются кейсы, основанные на реальных ситуациях. В каждом кейсе необходимо выбрать вариант действия. Учитель может обсуждать с обучающимися механизм действия после прохождения каждого кейса или после выполнения всего интерактивного задания.

Вопросы для обсуждения к кейсу 1:

- Почему «знакомый» в соцсети — не то же самое, что друг в реальной жизни?
- Что могут сделать злоумышленники с фотографией чужого дневника или удостоверения?
- Почему обещание «закрытого чата» — это приманка?
- **!** Что в таких сообщениях должно насторожить³?
- Если вы уже отправили фотографию, что нужно делать? (Не паниковать, рассказать взрослому, сохранить переписку)

Вопросы для обсуждения к кейсу 2:

- За что в итоге обещают заплатить 1500 рублей?
- Что значат слова «цифровой след будет связан с владельцем»?
- Почему просьба «не говорить родителям» — самый главный маркер обмана?

³ Методический комментарий: просьба прислать документы; обещание привилегированного доступа; ссылка на «закрытый чат»; попытка вызвать любопытство или желание попасть в группу избранных.

- **!** Что в таких сообщения должно насторожить и что следует делать⁴?
- Может ли аккаунт считаться удостоверением личности?

Вопросы для обсуждения к кейсу 3:

- «Это же не настоящее видео» — почему это оправдание не работает?
- Кто пострадает: только учитель/ученик или ещё и автор?
- Чем отличается безобидная шутка от травли?
- Если нейросеть создала продукт, то кто отвечает за результат и его использование?
- **!** Что в таких сообщения должно насторожить и что делать⁵?

Вопросы для обсуждения к кейсу 4:

- Что делает этот кейс безопасным? (Учебная цель, вымышленный персонаж, нет чужих фотографий и документов, известный преподаватель, ограниченная публикация)
- Можно ли пользоваться ИИ в школе? Когда — да, когда — нет?
- Откуда причина риска: в самой технологии или способе её применения⁶?

Вопросы для обсуждения к кейсу 5:

- Чем этот закрытый чат отличается от «закрытого чата для избранных» из кейса 1?
- Что подтверждает безопасность этого кейса: организатор, цель, правила, прозрачность?

⁴ «Лёгкие деньги» за простое действие; просьба сообщить код входа; слова «полностью законно»; секретность; непонятно, зачем нужен именно ваш аккаунт. Не делиться никакой информацией. Сделать скриншот предложения, заблокировать отправителя и рассказать родителям или другому доверенному взрослому.

⁵ Тайная съёмка; реальный человек как объект насмешки; обещание «никто не узнает»; публикация в общий чат; оправдание «это всего лишь ИИ». Стоит отказаться от съёмки и публикации. Если ролик уже появился — не пересылать, сохранить доказательства при необходимости и сообщить взрослому или администрации школы.

⁶ Методический комментарий: стоит следовать правилам урока и не загружать в сервис лишние личные данные. Если задание меняется и требует фото реального человека — уточнить согласие и правила.

- «Закрытый чат» — это всегда плохо? (*Нет. Важно, кто является организатором*)

Ответы обучающихся.

Учитель: Итак, мы рассмотрели пять кейсов, в каждом из которых был выбор и возможность изменить его. Но в жизни нет кнопки «начать заново», а значит, всё, что происходит в интернет-пространстве, требует ответственности до нажатия кнопки «Отправить» и после. За каждым сообщением в сети стоит живой человек — и не всегда с добрыми намерениями. «Знакомый» в соцсети — это не друг во дворе или одноклассник, которого вы хорошо знаете. Настоящий друг не будет просить рисковать деньгами семьи, документами или законом ради «интересного чата», он не будет угрожать и запугивать.

Чем тщательнее мы соблюдаем цифровую гигиену и правила безопасности в сети Интернет, тем более защищёнными мы будем.

Вопросы для обсуждения:

- Зачем нужен сложный пароль⁷?
- Где можно скачивать приложения?
- Объясните простыми словами, что такое двухфакторная аутентификация? Зачем она нужна?

Ответы обучающихся.

Учитель: Прервать общение со злоумышленником или прекратить выполнять опасные действия можно на любом этапе взаимодействия. Обязательно нужно остановиться и рассказать об этом родителям, учителю или доверенному взрослому. Давайте проговорим алгоритм действий в случае, когда случаются ситуации подобного рода.

⁷ Сложный пароль — базовая мера цифровой гигиены. Он нужен для того, чтобы защитить аккаунт от несанкционированного доступа. Простой пароль (например, 123456, qwerty, дата рождения или имя питомца) подбирается автоматическими программами за секунды. Сложный пароль — длинный, с буквами разного регистра, цифрами и символами — значительно увеличивает время подбора и делает взлом нецелесообразным.

Скачивать приложения можно только из официальных магазинов. Они проверяют программы на вирусы и опасный код. Ссылки из чатов, сообщений, всплывающих окон и подозрительных сайтов — это почти всегда ловушка. Через них распространяют вирусы, программы для кражи паролей и доступа к аккаунтам.

Двухфакторная аутентификация — это вход в аккаунт в два шага: сначала пароль, потом код из СМС или приложения. Даже если злоумышленник узнал пароль, без второго кода он не войдёт.

* Учитель организует проведение **практического задания «Алгоритм действий»** (презентация к занятию, слайд 4), в ходе которого обучающиеся делятся на три группы и разрабатывают алгоритм действий по полученной ситуации (приложение: информация для учителя).

* В случае нехватки времени на практическое задание учитель может сразу предложить обучающимся обсудить готовый алгоритм (презентация к занятию, слайд 5).

! Учитель организует **просмотр видеоролика — специального выпуска сериала «По УК» (совместный проект АНО «Диалог Регионы» и УБК МВД РФ).**

! Вопросы для обсуждения:

- Что мешает людям остановить опасную переписку или непосредственное выполнение действий? (*Стыд, страх, мысль о том, что уже поздно*)
- С какого момента общение в соцсети перестает быть безопасным?
- Зачем злоумышленнику понадобилась геолокация или личная информация?
- Почему выполнение требований не решит проблему, описанную в видеоролике, а только усилит давление?
- Какие фразы в переписке должны были насторожить героев видеоролика с самого начала?
- Что можно сказать тому, кто говорит: «Слабо? Ты что, боишься?»

Ответы обучающихся.

! **Учитель:** Желание быть популярным в сети или заработать, найти новых друзей и т. д. не должны стоять вам ни здоровья, ни репутации, ни денег ваших родителей. Интернет — пространство огромных возможностей для учёбы и творчества. Но эта свобода требует дисциплины, ответственности и соблюдения правил кибербезопасности. Ваш лучший антивирус — привычка советоваться с родителями и другими взрослыми, которым вы доверяете (педагог, психолог и др.). Если же данную ситуацию вы не можете разрешить самостоятельно, то вместе с родителями необходимо обратиться в правоохранительные органы. В данном случае стыд или страх могут

сыграть только отрицательную роль.

* Давайте убедимся на примерах историй, где именно привычка советоваться заранее в сложной ситуации могла бы всё изменить. Это случаи, которые произошли с настоящими школьниками — вашими ровесниками. И в каждой из них можно было поступить иначе.

Ситуация 1.

14-летний школьник из Омской области повторил увиденный в соцсетях химический эксперимент и получил тяжёлые ожоги лица и глаз.

Вопросы для обсуждения:

- Что нужно было сделать⁸?
- Почему так произошло? *(Не было уделено внимание технике безопасности, применению защитных инструментов, нехватка информации, отсутствие присмотра взрослого)*
- Что всегда остается за кадром? *(Неудачные дубли, подготовка, вероятные сложности, о которых умалчивается, и эксперимент кажется лёгким)*
- Несёт ли автор видео ответственность? Как можно повлиять на таких блогеров? *(Подать жалобу на автора видео или на видеоролик)*

Ответы обучающихся.

Ситуация 2.

13-летний подросток из Санкт-Петербурга публиковал видео опасных поездок снаружи электричек. После установления его личности школьника поставили на профилактический учёт.

Вопросы для обсуждения:

- Почему школьник был поставлен на учёт? *(Профилактический учёт — это не наказание, а мера, чтобы вовремя заметить сложности и помочь: разобраться в причинах поведения,*

⁸ Методический комментарий: на этапе просмотра видео нужно не сохранять ролик, не пробовать повторить увиденное без присмотра учителя химии или родителей, закрыть вкладку с опасным контентом и сообщить взрослым о том, что алгоритмы соцсетей показывают такие эксперименты детям.

скорректировать его и не допустить серьёзных проступков в будущем)

- Что нужно сделать при получении предложения снять такое видео⁹? Давайте попробуем кратко сформулировать алгоритм действий, когда незнакомцы в сети Интернет предлагают выполнить опасные для здоровья действия? *(В первую очередь необходимо сохранять спокойствие и попытаться оценить возможные риски, далее понять мотивы незнакомцев, зафиксировать доказательства — скрины сообщений, фото и видео, ссылки и т. д. — это нужно для обращения в правоохранительные органы)*

Ответы обучающихся.

* *Творческое задание: учитель может предложить обучающимся в парах придумать безопасную альтернативу опасному заданию: как получить лайки и одобрение, не рискуя здоровьем¹⁰ и не нарушая закон?*

Заключительный этап (5 минут)

! Учитель: Мы увидели, что за каждым выбором в той или иной ситуации стоит конкретный риск: потеря денег, здоровья, доверия семьи, а иногда и её репутации. Главное правило: если незнакомец просит сохранить общение в тайне от родных — это сигнал остановиться. При этом остановиться можно на любом этапе, даже если уже был дан ответ, отправлено фото или код: закрыть чат, заблокировать пользователя и рассказать взрослым никогда не поздно. Отсюда и формула, которая остаётся с нами: нет секретам от семьи, нет чужим деньгам на карте, никаких фотографий документов в личных сообщениях.

Наши действия в цифровом пространстве влияют не только на нас самих, но и на общую безопасность и благополучие других.

⁹ Методический комментарий: при получении предложения снять такое видео («зацени идею для клипа», «слабо?»): отказаться выполнять опасные трюки ради лайков и одобрения компании, сославшись на правила безопасности и здравый смысл, сохранить скриншоты переписки, заблокировать чат с подстрекателем и рассказать родителям или доверенному взрослому о давлении сверстников.

¹⁰ Методический комментарий: учителю важно подчеркнуть, что некоторые действия приводят к необратимым (серьёзные травмы, инвалидность и т. д.) и даже к несовместимым с жизнью последствиям.

Вопросы для рефлексии:

- К кому можно будет обратиться, если вам понадобится помощь¹¹?
- Почему важно не молчать, если случайно стал жертвой мошенников, а обязательно рассказать об этом близким и предостеречь своих друзей?

Ответы обучающихся.

¹¹ Методический комментарий: можно позвонить по Единому общероссийскому телефону доверия 8-800-2000-122, номер с мобильных 124, или обратиться в полицию.

Приложение

Практическое задание «Алгоритм действий»

Передача фотографий документов и личных данных	«Аренда» аккаунта в мессенджере	ИИ-ролик с реальным человеком без согласия
1. Первичный контакт (получение сообщения): - Не отправлять фотографию. - Проверить, действительно ли сообщение пришло от знакомого: написать ему в другом чате или позвонить. - Сделать скриншот переписки. - Заблокировать отправителя, если есть сомнения. - Обсудить ситуацию с родителями или другим доверенным взрослым. 2. Если началось давление: - Сообщить родителям или учителю о ситуации. - Игнорировать угрозы и давление («Если не пришлешь, тебя не возьмут в чат», «Все уже прислали, ты один отстаешь»). - Сохранить все сообщения с шантажом как доказательства. 3. Уже сделал (фото отправлено): - Сразу сообщить взрослому. - Сохранить переписку и все связанные материалы. - При необходимости — обратиться в поддержку соцсети с просьбой помочь удалить данные. - Предупредить друзей, чтобы они не попадались на такую уловку.	1. Первичный контакт (получение предложения): - Рассказать родителям или другому доверенному взрослому. - Не сообщать код и пароль. - Сделать скриншот переписки. - Заблокировать отправителя. 2. Если продолжают уговаривать: - Сообщить взрослым о попытках шантажа. - Не поддаваться на уговоры («Да что такого, всего на пару часов», «Никто не узнает»). - Игнорировать угрозы и давление. - Сохранить все сообщения, содержащие давление или угрозы. 3. Если код отправлен: - Сменить пароль. - Включить двухфакторную аутентификацию. - Сообщить родителям. - Предупредить друзей, чтобы не верили сообщениям с вашего аккаунта. - При необходимости — подать заявление в полицию.	1. Первичный контакт (предложение снять видео): - Твёрдо отказаться: «Я не стану этого делать, это неуважительно и может навредить человеку». 2. Если оказывают давление: - Сообщить классному руководителю или родителям о ситуации. - Не поддаваться на давление («Да ладно, все так делают», «Ты что, слабак?»). - Сохранить сообщения с давлением или угрозами. 3. Уже сделал (ролик создан или опубликован): - Не пересылать ролик дальше. - Сообщить классному руководителю, школьному психологу или родителям. - Извиниться перед тем, кого сняли и предложить помощь.