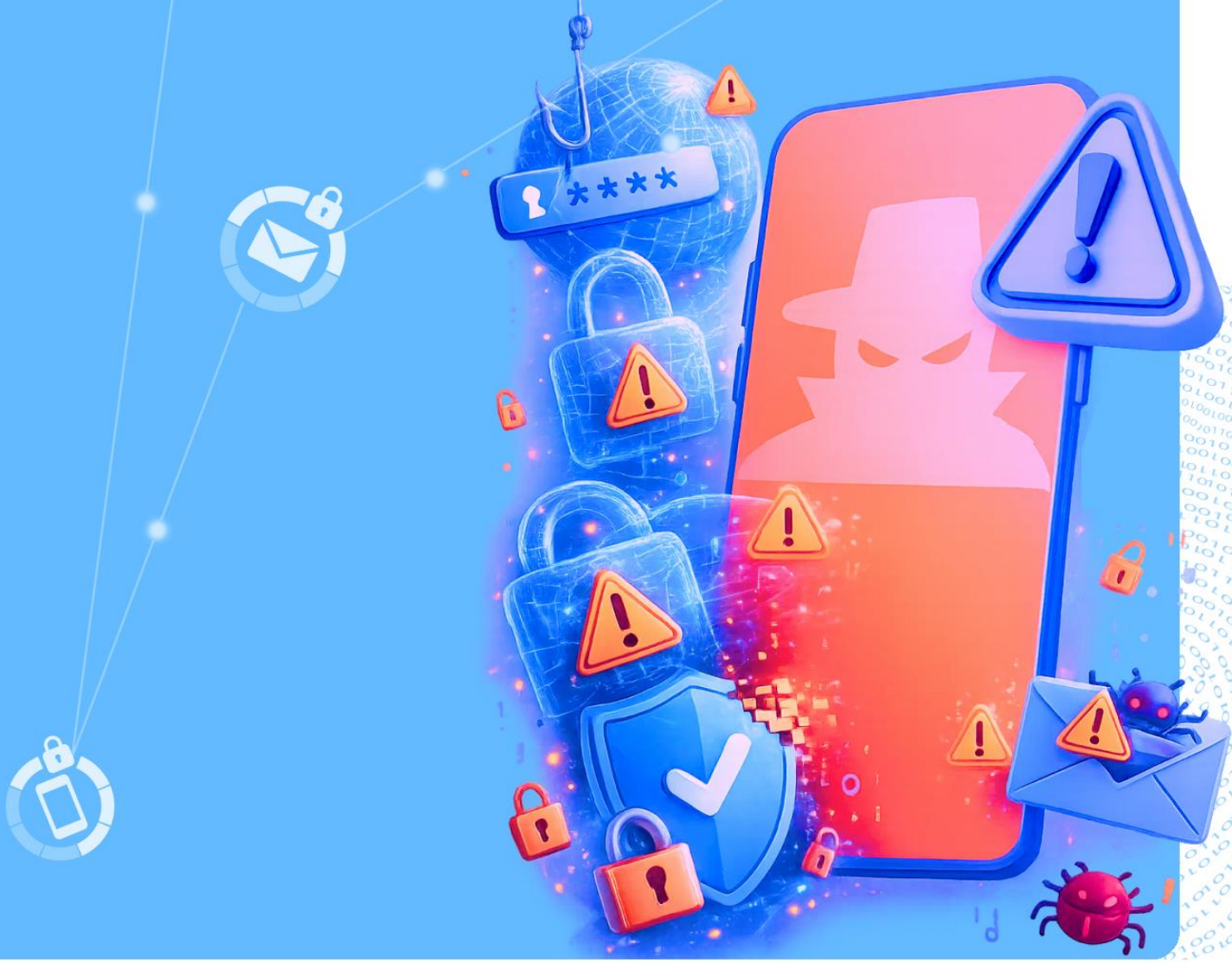
МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ПСИХОЛОГО-ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ
ДИАЛОГ РЕГИОНЫ
ИНСТИТУТ ИЗУЧЕНИЯ ДЕТСТВА, СЕМЬИ И ВОСПИТАНИЯ
РАЗГОВОРЫ О ВАЖНОМ
2026 ГОД ЕДИНСТВА НАРОДОВ РОССИИ

жизнь | гражданственность

Сценарий занятия | 8–9 классы

# ЦИФРОВОЙ ЩИТ

## ОСНОВНЫЕ ПРАВИЛА БЕЗОПАСНОСТИ В СЕТИ ИНТЕРНЕТ



**СЦЕНАРИЙ**

**занятия «РАЗГОВОРЫ О ВАЖНОМ»**

**для обучающихся 8–9 классов**

**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

**Учитель:** Сегодня мы поговорим о правилах безопасности в цифровом пространстве. На одном из сентябрьских занятий мы уже обсуждали цифровой суверенитет страны и развитие цифровых технологий. Вместе с возможностями появляются и новые риски: от утечки личных данных до вовлечения в преступные схемы. Расскажите: приходили вам когда-нибудь

сообщения с незнакомых номеров с какими-то «выгодными» предложениями? Встречались ли вам группы или чаты, где обсуждают темы, связанные с чем-то шокирующим или агрессивным?

*Ответы обучающихся.*

*Учитель организует* ***просмотр и обсуждение видеоролика-анонса с Кариной Каграманян.***

## Основной этап

**Учитель:** Уберечь себя и своих близких от обмана в интернете помогут **правила цифровой гигиены.** Давайте их повторим. Какие правила вы помните[1]? Соблюдаете ли вы их? *(Презентация к занятию, слайд 2)*

*Вопросы для обсуждения:*

- Слышали ли вы реальные истории, когда ровесники попадали в неприятные ситуации из-за переписки или сомнительной подработки? Чем заканчивалось?
- Представьте: вам звонит незнакомец и под различными предлогами просит сообщить код из СМС. Каков ваш алгоритм действий? Что сделаете в первую очередь?

[1] Методический комментарий для учителя:
- Не переходите по ссылкам, полученным от неизвестных отправителей.
- Избегайте публикации личных данных на ненадежных ресурсах (даже если вы хоть немного сомневаетесь в их безопасности)!
- Используйте антивирусную программу для защиты своего компьютера.
- Не участвуйте в сомнительных онлайн-играх!
- Не раскрывайте личные данные: адрес, номер телефона, фото документов, геолокацию.
- Используйте сложные пароли и двухфакторную аутентификацию.

– И еще один важный вопрос: почему люди, которых уже обманули, часто молчат и никому не рассказывают — даже родителям? Что их останавливает?

*Ответы обучающихся.*

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

*Учитель 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.*

**Учитель:** Такие предложения — уголовно наказуемые действия, вы **рискуете получить судимость по статьям Уголовного кодекса Российской Федерации.** Как распознать подвох? Что сразу должно насторожить в подобных предложениях?

*Ответы обучающихся.*

**Учитель:** Обещания высоких доходов за «простые действия» — это всегда обман.

*Вопросы для обсуждения:*

- Почему нужно быть осторожным с новыми знакомыми в интернете, которые появились внезапно и просят помощи?
- Какие слова или фразы должны вас насторожить в общении с новыми знакомыми?
- Зачем мошенникам нужен доступ к вашим личным данным?
- Как вы думаете, почему мошенники часто пытаются обмануть детей или подростков?

*Ответы обучающихся.*

**Учитель:** Помимо перевода денежных средств, мошенники предлагают **сдать в аренду за определенную сумму свой аккаунт.** Для чего им это может быть нужно? *(Через чужой аккаунт могут рассылать мошеннические сообщения, распространять экстремистский контент, организовывать схемы обмана людей)*

*Вопросы для обсуждения:*

- Какие действия они могут совершать от лица другого человека?
- В случае проведения расследования к кому приведет цифровой след, оставленный мошенниками?
- Как вы думаете, можно ли рассматривать того, кто сдал в аренду свой аккаунт, как преступника либо соучастника преступления? Есть ли уголовная ответственность

за предоставление доступа к своему аккаунту или соучастие в противоправных действиях?[2]

*Ответы обучающихся.*

**Учитель:** Еще одной распространенной проблемой в интернете является **деструктивный контент.** Знаете ли вы, что это такое?

*Ответы обучающихся.*

**Учитель:** Это информация, которая провоцирует агрессию или страх, призывает к насилию или нарушению закона, распространяет ненависть по различным признакам. Обычно она встречается в закрытых чатах и каналах. Как можно распознать, что вас ждёт, если перейти по указанной ссылке?

*Ответы обучающихся.*

**Учитель:** Обычно **маркерами такого контента будут** громкие заголовки: «Смотри, пока не удалили!», «Только для своих!». Что же делать, если вы все же попали на страничку с деструктивным контентом? *(Выключи экран или перелистни, заблокируй источник и отправь жалобу модераторам, не комментируй и не пересылай друзьям, если тревожно — расскажи родителям или учителю) (Презентация к занятию, слайд 3)*

[2] Методический комментарий для учителя

С 1 сентября 2025 года вступили в силу изменения, внесенные в Уголовный кодекс Российской Федерации и Кодекс Российской Федерации об административных правонарушениях. Введена ст. 274.5 УК РФ, ст. 13.29.2 КоАП РФ. В случае недостижения участником преступной схемы по аренде аккаунтов возраста уголовной ответственности к ответственности будут привлечены его родители по статье 5.35 КоАП РФ.

*Ответы обучающихся.*

**Учитель:** Также в закрытых чатах в мессенджерах или группах соцсетей могут попадаться **различные деструктивные сообщества.** Почему, на ваш взгляд, молодые люди попадают в такие сообщества? Что особенного им может предложить такая виртуальная дружба, в отличие от реальной компании друзей?

*Ответы обучающихся.*

**Учитель:** Деструктивные сообщества пропагандируют следующие направления: **кибербуллинг** — систематическая травля в сети; **сваттинг** — ложные вызовы спецслужб по чужому адресу; **доксинг** — публикация личных данных без согласия человека, информация о котором в этих сведениях содержится; вербовка в криминальные схемы (например, сим-боксы[3]) *(презентация к занятию, слайд 4).* Как же можно защититься от вступления в подобную группу?

*Ответы обучающихся.*

**Учитель:** Не вступайте в закрытые группы с подозрительной активностью. Если вас уговаривают сделать что-то незаконное — скажите «нет». Расскажите взрослым: родителям, учителю, школьному педагогу-психологу, **обратитесь в полицию вместе с родителями.**

[3] Методический комментарий для учителя
Сим-бокс — это устройство, объединяющие в единый программно-аппаратный комплекс десятки сим-карт с обеспечением удаленного доступа и возможностью дистанционно звонить неограниченному кругу людей. То есть в устройство вставляется некоторое количество сим-карт, с которых удаленно совершаются звонки или рассылаются сообщения. Заблокируют одну карту, устройство переключится на другую, и работа продолжится.

*Вопросы для обсуждения:*

- Если твой друг уговаривает тебя только один раз помочь ему перевести или снять чужие деньги, уверяя, что все легально, как ты поступишь? Насколько стоит задумываться о дружбе, если речь идет о нарушении закона? Захочешь ли стать преступником «за компанию»?

*Ответы обучающихся.*

*Учитель организует* ***выполнение практического задания.*** *Обучающиеся делятся на 3 группы. Первая группа выступает в роли эксперта по кибербезопасности и выявляет элементы мошенничества. Вторая группа предлагает варианты выхода из сложившейся ситуации. Третья группа анализирует причины и последствия сложившейся ситуации.*

***Кейс 1.*** *Вечером в социальной сети Мише пришло сообщение: «Привет! Мы с тобой как-то виделись у наших общих друзей. Решил тебя найти в сетях. Классная у тебя страничка! Может, пойдем завтра погуляем?» Как нужно отреагировать на это сообщение? (Презентация к занятию, слайд 5)*

***Кейс 2.*** *К психологу школы за советом обратился ученик 8 класса. Ученик рассказал, что около двух недель назад по электронной почте он получил приглашение от своего друга поиграть в интернет-игру, доступ к которой открывается по прикрепленной ссылке. Перейдя по указанной в письме ссылке, ученик в появившемся окне подтвердил свое участие, нажав какую-то кнопку. Игра оказалась очень увлекательной, но спустя день на электронную почту пришло письмо с незнакомого адреса с требованием оплаты участия. Ученик его проигнорировал, однако письма стали появляться каждый день и содержать угрозы благополучию его семьи. Со слов ученика, он должен уже около 100 000 рублей. Родителям рассказать боится. Что предпринять, не знает. Как думаете, что необходимо сделать ученику для решения ситуации? (Презентация к занятию, слайд 6)*

**Учитель: Любое действие человека в интернете остается навсегда.** Это называется **«цифровой след».**

*Вопросы для обсуждения:*

- Как можно контролировать свой цифровой след?
- Какие последствия могут возникнуть из-за наличия негативной информации в вашей цифровой репутации?

*Ответы обучающихся.*

**Заключительный этап**

**Учитель:** Важно понимать: даже если вы используете **вымышленные имена и ставите картинки вместо фотографий, это не дает вам полной анонимности.** В сети каждый шаг оставляет цифровой след, и рассчитывать на то, что есть возможность остаться неизвестным, — большая ошибка. **Цифровой след всегда приведет к тому, кто его оставил.** Будьте умнее мошенников и помните, что **незнание закона не освобождает от ответственности.**

*Вопросы для рефлексии:*

- Почему важно не молчать, если случайно стал жертвой мошенников, а обязательно рассказать об этом близким и предостеречь своих друзей?

- К кому можно обратиться, если не знаешь, как поступить в сложной ситуации? Почему важно не пытаться решить все самостоятельно и не бояться показаться слабым?

*Ответы обучающихся.*

**Учитель:** В любой трудной ситуации вы не одни. **Родители и учителя всегда рядом и готовы помочь.** Если вам нужна дополнительная поддержка или совет, вы можете позвонить на единый общероссийский телефон доверия или обратиться в полицию *(презентация к занятию, слайд 7).*

## Постразговор

**Уважаемые коллеги!**

**Предлагаем вам и обучающимся поучаствовать во Всероссийской акции «Движения Первых»** *(презентация к занятию, слайд 8).*

### Что почитать

- Каретникова Е. «Маршрут не построен»

### Что посмотреть

- Сериал «Первых» «Золотые сети» о кибербезопасности

- Антивербовка: психологические навыки: https://vkvideo.ru/video-214524833_456245845
- Антивербовка: лайфхаки для подростков: https://vkvideo.ru/video-214524833_456245864
- Антивербовка в цифровом мире: https://vkvideo.ru/video-214524833_456245876
- Антивербовка: главные секреты безопасности: https://vkvideo.ru/video-214524833_456245886
- Подкаст «Разговор по делу. Инфобезопасность»

**Проектная и внеурочная деятельность, внеклассные мероприятия**

- «Интернет-этика»: обучающиеся 8–9 классов разрабатывают для учеников начальной школы памятку по правилам поведения в интернете, используя знания, полученные в рамках занятия. Презентация проектов может проходить в рамках общешкольного 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.