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

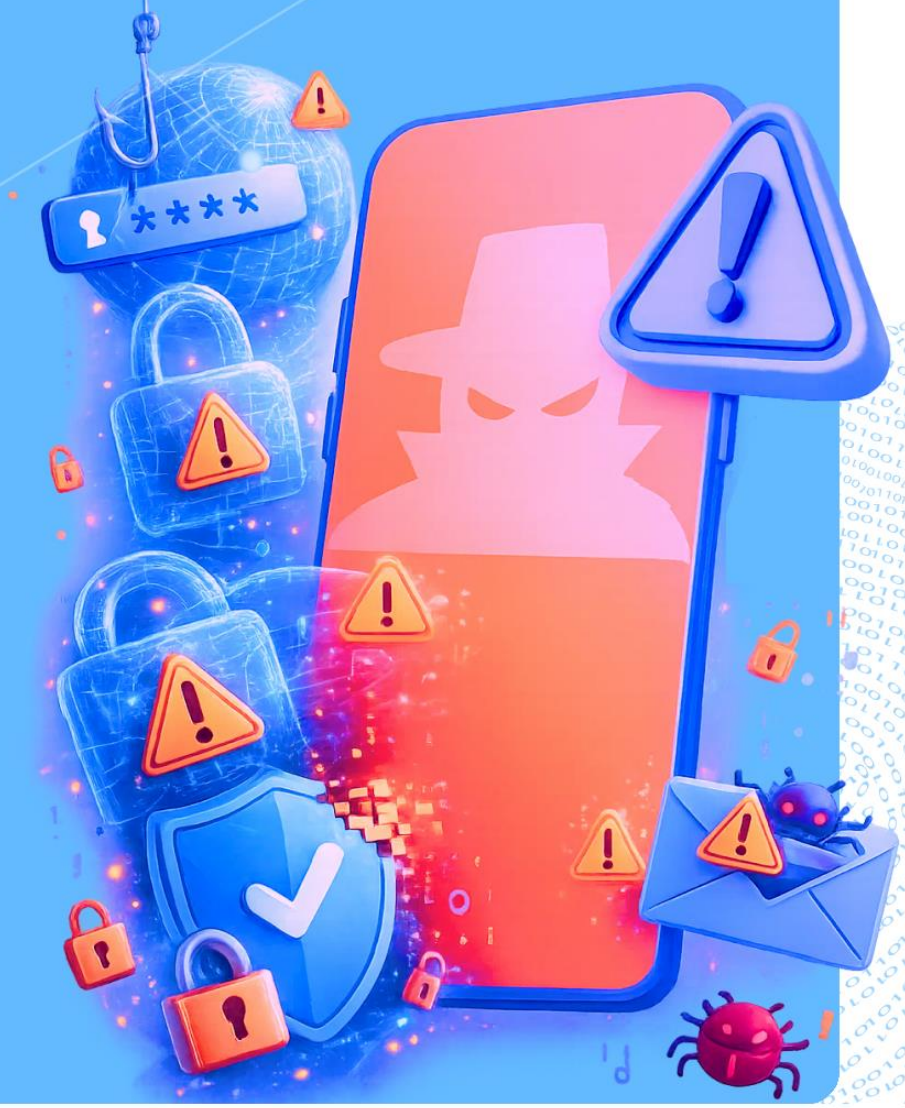
жизнь

гражданственность

Сценарий занятия | 5–7 классы

ЦИФРОВОЙ ЩИТ

ОСНОВНЫЕ ПРАВИЛА БЕЗОПАСНОСТИ В СЕТИ ИНТЕРНЕТ



СЦЕНАРИЙ

занятия «РАЗГОВОРЫ О ВАЖНОМ»

для обучающихся 5–7 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 интерактивного задания.

Заключительный этап: беседа.

Мотивационно-целевой этап

Учитель: Интернет стал неотъемлемой частью нашей жизни. Возможность быстро найти нужную информацию, проходить обучение, обмениваться идеями, делиться опытом, находить друзей по всему миру — все это делает нашу жизнь удобнее и интереснее.

Вопросы для обсуждения:

- Какие преимущества интернета вы считаете важными для себя?
- С какими проблемами можно столкнуться в сети?
- Как вы думаете, кто чаще становится мишенью для мошенников в интернете?

Ответы обучающихся.

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

Основной этап

Учитель: Лучший способ защиты от злоумышленников — знать о существующих рисках и сознательно их избегать. **Цифровая гигиена, основы кибербезопасности и понимание актуальных схем обмана — это те знания и навыки, которые необходимы каждому из нас** *(презентация к занятию, слайд 2).*

Вопросы для обсуждения:

- Как вы понимаете значение понятия «цифровая гигиена»? Какие правила цифровой гигиены вы знаете?
- Что, по вашему мнению, означают понятия «кибермошенники» и «кибербезопасность»?
- Какими способами вы можете защитить личную информацию о себе в интернете? Какую информацию не следует публиковать в сети?

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 игре обещают что-то бесплатно или очень дешево, но просят прислать пароль или фото карты. Это подарок или ловушка? Почему?
- Если бы это был настоящий друг или ваш знакомый, попросил бы он сфотографировать мамину карту?
- Что нужно было сделать девочке, когда незнакомый человек в игре заговорил про деньги? Кому она должна была сразу рассказать?
- Как вы думаете, можно ли фотографировать карту и отправлять ее кому-то, даже если этот человек очень убедительно просит?
- Какие вопросы задавали мальчику во втором ролике незнакомцы в самом начале? (Где живет, есть ли ж/д). Почему для обычной подработки спрашивают именно про это, а не про навыки или умения?
- 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)*

Учитель: Представьте, мошенник ищет потенциальную жертву в социальной сети. У него есть только никнеймы. Какую информацию он уже может собрать о людях, если они не подумали о своей личной безопасности?

Ответы обучающихся[1]*.*

Учитель: Публикация таких данных, как номер телефона, адрес проживания или полное имя, многократно повышает уязвимость, открывая мошенникам прямой канал для шантажа, фишинга[2] и других манипуляций. Очень часто мы сами рассказываем о себе слишком много, что в итоге помогает мошенникам найти наши уязвимые стороны и добиться своей цели. Как вы думаете, когда мы теряем бдительность?[3] *(Презентация к занятию, слайд 3)*

Ответы обучающихся.

[1] Методический комментарий
Учитель направляет беседу в сторону обсуждения распространенных ошибок пользователей, например таких: открытый профиль, геолокация, номер школы / адрес на фото, имя и фамилия в профиле, номер телефона в открытом доступе, состав семьи, номер карты и пароль в сохраненных сообщениях.

[2] Самая распространенная цель фишинга (кибератаки) — получить доступ к аккаунту пользователя в мессенджере, чтобы потом атаковать людей из его списка контактов, например с просьбой одолжить небольшую сумму денег.

[3] Методический комментарий для учителя: например, не принимай решений и не предпринимай действий в состоянии гнева, усталости, болезни и т. п.

Учитель: Представьте ситуацию, когда вам пишут: «Дай доступ к аккаунту, я буду постить рекламу, а ты будешь получать 1000 рублей в неделю». Как бы заманчиво это ни звучало, перед вами опасная ловушка.

Вопросы для обсуждения:

- Почему сдача аккаунта в аренду — это рискованно? *(Аккаунт могут использовать для мошеннических операций, например выманить деньги у ваших друзей, размещать от вашего имени запрещенный контент, оскорбления, призывы к чему-то плохому. За это отвечает хозяин аккаунта, а не тот, кто это делает).*
- Как вы поступите, если друг предложит вам «заработать» на сдаче аккаунта, уверяя, что сам так делает?

Ответы обучающихся.

Учитель: Таким способом вас могут втянуть в **дропперство**[4] — когда через ваш банковский счет переводят деньги преступников, например за вознаграждение или обманным путем. Так мошенники используют других людей, чтобы скрыть свои следы. Образно говоря, вас просят подержать дверь, пока грабитель выносит вещи. **Тот, кто соглашается, сам попадает в беду, потому что становится соучастником преступления, и** его могут привлечь к ответственности[5].

[4] Дропперство — это вид мошенничества, когда преступники используют банковский счет постороннего человека («дропа») для вывода денег, добытых преступным путем.
[5] С 5 июля 2025 года за дропперство предусмотрена уголовная ответственность с 16 лет (ст. 187 УК РФ). За неправомерные действия грозит до 6 лет лишения свободы, а также штраф от 300 тыс. до 1 млн рублей. Если дропом становится ребенок младшего возраста, его могут поставить на учет в полиции, а родителям — выписать штраф или обязать вернуть похищенные деньги.

Вопросы для обсуждения:

- Как вы думаете, если на вашу карту приходит перевод от незнакомого человека и вам тут же пишут с просьбой вернуть деньги «на правильный счет», почему нельзя соглашаться? *(Если переведете, станете дропом: вы поможете преступникам, а ваш счет может быть заблокирован)*
- Какая цель у мошенников? *(Скрыть свой цифровой след)*

Ответы обучающихся.

Учитель: Некоторая информация, которая содержится и распространяется в интернете, **может носить деструктивный характер.**

Вопросы для обсуждения:

- Что значит деструктивный контент? Может ли такой контент навредить? Почему?
- Как вы думаете, зачем кто-то создает такой контент?
- На что рассчитывают злоумышленники? Что будете делать вы, если встретится деструктивный контент?

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 ждет, если перейти по указанной ссылке? *(Презентация к занятию, слайд 4).*

Ответы обучающихся.

Учитель: Задача мошенников — вызвать эмоциональный отклик и получить желаемое. Обычно все это сопровождается кричащим заголовком: «Только сейчас!», «Срочно!», «Нажми и узнаешь то, что так давно скрывали!», «Смотри, пока не удалили!». Если материал вызывает у вас сильную эмоцию и желание немедленно что-то сделать — сделайте паузу.

Вопрос для обсуждения:

- Сталкивались ли вы с чем-то подобным или слышали о нем? Как вы поступали в этих ситуациях?

Ответы обучающихся.

Учитель: Чтобы не позволить себя обмануть, необходимо учиться отличать правду от фейков, анализировать информацию, проверять ее источники и не распространять непроверенные данные. Увидев сомнительный заголовок, подумайте, прежде чем кликнуть на него.

Вопрос для обсуждения:

- Что бы вы сделали, если бы столкнулись с деструктивным контентом?

Ответы обучающихся.[6]

[6] Методический комментарий
Не реагировать, не распространять дальше, закрыть страницу или приложение, сообщить знакомым взрослым, подать жалобу на платформе (кнопка «Пожаловаться»).

Учитель: Ваши действия в интернете — ваша ответственность. Даже безобидный на первый взгляд секретный чат может оказаться ловушкой: сначала просто общение, а потом — **вовлечение в незаконные действия (кибербуллинг, сваттинг). Не вступайте в подозрительные группы.** Если вас уговаривают на жестокие или противоправные поступки, говорите «нет», не становитесь соучастником преступления. Беспечность оставляет цифровые следы, и **вас могут привлечь к ответственности — от постановки на учет в правоохранительных органах до уголовного наказания.** Сохраняйте скриншоты угроз, рассказывайте взрослым.

Вопросы для обсуждения:

- Что делать, если ваш друг начал общаться с подозрительной группой и его поведение меняется?
- Почему мошенники в своих схемах часто требуют действовать срочно? Что было бы, если бы они дали вам время подумать?

Ответы обучающихся.

*Учитель организует проведение **практического задания «Разоблачи мошенника»**, в ходе которого обучающимся предлагаются ситуации, которые нужно проверить на подлинность по алгоритму (презентация к занятию, слайды 5–8, Приложение).*

Заключение

Учитель: Мы настолько привыкли к цифровому миру, что порой перестаем задумываться о том, что собеседники в сети действуют исключительно исходя из собственных интересов.

Вопрос для обсуждения:

- Как правильно поступить, если незнакомец в сети пытается завязать разговор, дружбу, предлагает подарить подарок, задает личные вопросы или просит встретиться?

Ответы обучающихся.

Учитель: Основа безопасного нахождения в сети Интернет — цифровая гигиена и критическое мышление. Сохраняйте бдительность и соблюдайте правила кибербезопасности *(презентация к занятию, слайд 9).*

Если вам нужна помощь, вы можете позвонить по единому общероссийскому телефону доверия или обратиться в полицию *(презентация к занятию, слайд 10).*

Постразговор

Уважаемые коллеги!

Предлагаем вам и обучающимся поучаствовать во Всероссийской акции «Движения Первых» *(презентация к занятию, слайд 11).*

Что посмотреть

- Видеоматериалы «Движения Первых» по марафону «Кибербезопасность» на сайте https://xn--80aeshm0g.xn--90acagbhgpca7c8c7f.xn--p1ai/ в разделе «Навыки для жизни»: информационная безопасность.

Проектная и внеурочная деятельность, внеклассные мероприятия

- Школьный флешмоб #ЦифровойЩит: обучающиеся записывают короткие видео с одним правилом безопасности и выкладывают в соцсетях с хештегом или делятся в общем чате класса. В конце недели формируется общий ролик.
- Мини-исследование «Какие правила безопасности знаешь ты?»: обучающиеся проводят опрос среди друзей или семьи, чтобы узнать, какие правила безопасности в интернете они знают, затем анализируют полученные данные и составляют общую памятку для распространения.
- «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.

Приложение

Алгоритм проверки

Вопрос	Что проверяем	Комментарий
Кто отправитель?	*Знаком ли этот человек? Почему он мне пишет? Его аккаунт настоящий?*	
Куда ведет ссылка?	*Совпадает ли адрес с официальным? Нет ли ошибок, лишних символов?*	
К чему призывают?	*Слова «срочно», «немедленно», «последний шанс», угрозы, «никому не говори»*	
Можно ли взять паузу?	*Что будет, если подождать, посоветоваться с родителями?*	
Есть ли безопасный способ?	Позвонить в банк / написать в службу поддержки, спросить у взрослых.	

Ситуации

1. Света увлеклась Roblox и мечтала купить редкий скин за игровую валюту. В игровом чате написал незнакомец: «Хочешь заработать валюту? Сделай пару простых заданий». Света согласилась и выполнила. Задания оказались простыми: взять телефон мамы, открыть онлайн-банк, сделать пару кликов и переслать данные «другу». Что произошло? Какие ошибки совершила девочка?

2. Маше позвонили с номера, на экране высветилось «Полиция». Женский голос представился сотрудницей отдела по борьбе с мошенничеством и спросил: «Горячева Валентина Михайловна вам кем приходится?» — «Мамой». — «На работе у мамы проверка, нужно срочно задекларировать имущество, иначе на нее заведут уголовное дело и посадят в тюрьму». Чтобы спасти маму, нужно собрать все деньги и ценности, которые есть дома, и передать курьеру. Теперь Маша гордится, что спасла маму. А что произошло на самом деле?

3. Рома получил сообщение от одноклассника с просьбой проголосовать за него в конкурсе со ссылкой. Перешел, авторизовался через соцсеть, проголосовал. Через пару часов не смог зайти в свой мессенджер, и тут же ему позвонил друг: «Ты просил у меня деньги в долг?» Что произошло?