жизнь

гражданственность

ЦИФРОВОЙ ЩИТ

ОСНОВНЫЕ ПРАВИЛА БЕЗОПАСНОСТИ В СЕТИ ИНТЕРНЕТ

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ
к сценарию 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.

Планируемые результаты занятия[1]

Личностные результаты

В сфере гражданского воспитания: уважение прав, свобод и законных интересов других людей; неприятие любых форм экстремизма, дискриминации; понимание роли различных социальных институтов в жизни человека; представление об основных правах, свободах и обязанностях гражданина, социальных нормах и правилах межличностных отношений в поликультурном и многоконфессиональном обществе.

В сфере патриотического воспитания: формирование ценностного отношения к достижениям своей Родины — России, к науке, искусству, спорту, технологиям.

В сфере духовно-нравственного воспитания: ориентация на моральные ценности и нормы в ситуациях нравственного выбора; готовность оценивать свое поведение и поступки, поведение и поступки других людей с позиции нравственных и правовых норм с учетом осознания последствий поступков; свобода и ответственность личности в условиях индивидуального и общественного пространства.

В сфере физического воспитания, формирования культуры здоровья и эмоционального благополучия: соблюдение правил безопасности, в том числе навыков безопасного поведения в интернет-среде; способность адаптироваться к стрессовым ситуациям и меняющимся социальным, информационным и природным условиям, в том числе осмысляя собственный опыт и выстраивая дальнейшие цели.

В сфере трудового воспитания: уважение к труду и результатам трудовой деятельности.

[1] В соответствии с рабочей программой курса внеурочной деятельности «Разговоры о важном» на 2025–2026 годы.

В сфере понимания ценности научного познания: установка на осмысление опыта, наблюдений, поступков.

В сфере адаптации обучающегося к изменяющимся условиям социальной и природной среды: повышение уровня своей компетентности через практическую деятельность; развитие умения оценивать свои действия с учетом влияния на окружающую среду.

Метапредметные результаты

В сфере овладения познавательными универсальными учебными действиями: сравнивать объекты, устанавливать аналогии, причинно-следственные связи в ситуациях, поддающихся непосредственному наблюдению или знакомых по опыту, делать и формулировать выводы; прогнозировать возможное развитие процессов, событий и их последствия в аналогичных или сходных ситуациях.

В сфере овладения коммуникативными универсальными учебными действиями: воспринимать и формулировать суждения; признавать возможность существования разных точек зрения, корректно и аргументированно высказывать свое мнение; сопоставлять свои суждения с суждениями других участников диалога, обнаруживать различие и сходство позиций.

В сфере овладения регулятивными универсальными учебными действиями: оценивать соответствие результата цели и условиям; давать оценку приобретенному опыту; осознанно относиться к другому человеку, его мнению.

Предметные результаты

Русский язык: формирование умений речевого взаимодействия: создание устных монологических высказываний на основе жизненных наблюдений, личных впечатлений.

Обществознание: освоение и применение системы знаний о социальных свойствах человека, особенностях его взаимодействия с другими людьми, о характерных чертах

общества, о содержании и значении социальных норм, регулирующих общественные отношения; формирование умения сравнивать деятельность людей, социальные объекты, явления, процессы в различных сферах общественной жизни, оценивать собственные поступки и поведение других людей с точки зрения их соответствия моральным, правовым и иным видам социальных норм.

Информатика: освоение и соблюдение требований безопасной эксплуатации технических средств информационно-коммуникационных технологий; развитие умения соблюдать сетевой этикет, базовые нормы информационной этики и права при работе с приложениями на любых устройствах и в сети Интернет, выбирать безопасные стратегии поведения в сети.

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 видеоролика, беседа, выполнение практического задания.

Заключительный этап: беседа.

Мотивационно-целевой этап

Основные смыслы: личная ответственность в цифровой среде — это осознанная забота о себе, которая становится вкладом в безопасность общества и государства.

Задачи:

- побудить познавательный интерес к теме занятия;
- сформировать у обучающихся представление о важности разговора о проблемах безопасности в цифровом пространстве;
- развивать умение формулировать собственные суждения, аргументировать точку зрения.

Формы работы:

- просмотр видеоролика-анонса;
- беседа.

Основной этап

1. Кибермошенничество и последствия неверных действий

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.

Задачи:

- обсудить значение понятия «цифровая гигиена» и ее правила;
- познакомить обучающихся с понятиями и формами мошенничества в цифровом пространстве;
- объяснить критически важное значение кибербезопасности как защиты личной информации;
- на примере дропперства раскрыть значение цифрового следа;
- способствовать формированию понимания личной ответственности в управлении собственными данными;
- развивать способность выявлять признаки мошенничества в различных цифровых ситуациях.

Формы работы:

- просмотр видеоролика;
- беседа.

2. Кибербезопасность: цифровой щит и критическое мышление пользователей сети Интернет

Основные смыслы: 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.

Задачи:

- обсудить понимание термина «деструктивный контент» и основные способы защиты от него;
- развивать навыки критического мышления для анализа и оценки поступающей информации;
- учиться идентифицировать мошеннические схемы по характерным признакам и знать, как на них реагировать;
- мотивировать обучающихся использовать проверенные ресурсы сети Интернет для определенных целей.

Формы работы:

- выполнение практического задания;
- беседа.

Заключительный этап

Основные смыслы: личная ответственность в цифровой среде — это осознанная забота о себе, которая становится вкладом в безопасность общества и государства. В ситуации неопределенности или угрозы в сети Интернет необходимо незамедлительно обратиться за помощью в полицию.

Задачи:

- способствовать формированию установки на ответственное отношение к своей цифровой безопасности как неотъемлемой части повседневной жизни;
- мотивировать к применению правил цифровой гигиены в качестве главного инструмента защиты от мошенников.

Форма работы:

- беседа.

Дополнительные рекомендации

Куда обращаться родителям в случае, если ребенок столкнулся с мошенничеством

Скажите ребенку, что он не виноват в сложившейся ситуации, но при этом крайне важно ограничить любое дальнейшее общение с мошенниками, так как это недопустимо и опасно. Самое простое — добавить номера в черный список.

Обращаться в полицию необходимо даже при неудачной попытке, так как это поможет сотрудникам зафиксировать

дополнительные факты противоправной деятельности, установить причастных лиц и предотвратить другие преступления.

Куда можно обращаться, чтобы сообщить о преступлении

В любой отдел внутренних дел (по месту жительства или ближайший к вам). Заявление о преступлении обязаны принять независимо от места его совершения. При подаче заявления очень важно не удалять переписки, зафиксировать максимум доказательств. Это могут быть скриншоты, файлы, ссылки, реквизиты, СМС-сообщения, выписки и т. д. Важно понимать, что для подачи заявления необходимо присутствие родителя или законного представителя несовершеннолетнего.

По телефонам 102/112. Кратко описываете ситуацию и просите зарегистрировать сообщение. После чего в присутствии родителей или законных представителей необходимо дождаться прибытия следственно-оперативной группы.

Куда можно обращаться, если ребенок столкнулся с подозрительным звонком или сообщением

Информацию о подозрительном звонке можно подать через «Госуслуги», сообщив при этом номер телефона, на который звонили, и номер телефона, с которого поступил звонок (https://pos.gosuslugi.ru/lkp/poll-anti-fishing/).

Также советуем обратиться к вашему сотовому оператору, чтобы звонок промаркировали как нежелательный. Например, https://moscow.megafon.ru/help/antifraud/form/

Куда можно обращаться, если вы или ваш ребенок столкнулись с деструктивной информацией или с фишинговым сайтом

В соответствии с действующим законодательством Российской Федерации государственная функция по ограничению доступа к интернет-ресурсам, содержащим

запрещенную или деструктивную информацию, реализуется Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) на основании решений уполномоченных Правительством Российской Федерации федеральных органов исполнительной власти (Постановление Правительства Российской Федерации от 26.10.2012 № 1101).

В связи с этим в случае выявления сайтов, располагающих противоправным содержанием, целесообразно использовать электронную форму направления обращений, расположенную на официальном сайте Роскомнадзора по адресу https://eais.rkn.gov.ru/feedback/, либо мобильное приложение «РКН», указав при этом точный адрес интернет-страницы, на которой размещена запрещенная информация.

Фишинг — вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей методами социальной инженерии, а также нанесение пользователям другого ущерба.

Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации в целях противодействия мошенничеству в сети Интернет разработана информационная система мониторинга фишинговых сайтов «Антифишинг», предназначенная для автоматизации и повышения эффективности процессов сбора, систематизации, обработки, анализа и хранения сведений о фишинговых ресурсах и фишинговой активности на территории Российской Федерации.

В связи с этим в случае выявления сайтов указанной категории целесообразно использовать электронную форму направления обращений, расположенную по адресу: https://paf.occsirt.ru.

Куда обращаться, если обнаружены персональные данные ребенка в сети Интернет

При обнаружении распространения персональных данных вашего ребенка в интернете важно обратиться в надзорные органы в целях защиты от возможного интернет-мошенничества.

Обратиться в общественную электронную приемную Роскомнадзора, выбрав тематику обращения «Обработка персональных данных» и далее «Защита прав субъектов персональных данных…».

Напрямую потребовать от владельца ресурса прекратить незаконное распространение персональных данных.

В случае если известно, какой именно ресурс распространяет данные, можно направить письменное требование об удалении персональных данных и прекращении их обработки (через форму обратной связи или электронную почту, указанную в политике конфиденциальности). Рекомендуется сразу приложить скриншоты и ссылки. Важно знать, что невыполнение вашего законного требования может закончиться привлечением лица к административной ответственности.

В случае если при обращении появились вопросы, то можно обратиться в Центр правовой помощи гражданам в цифровой среде, специалисты которого безвозмездно консультируют россиян, ставших жертвами незаконного использования персональных данных.

Полезные ссылки

- Центр правовой помощи гражданам в цифровой среде:

https://4people.grfc.ru/

- Общественная электронная приемная Роскомнадзора:

https://rkn.gov.ru/treatments/ask-question/

- В Роскомнадзоре рассказали, как подать жалобу на разглашение персональных данных:

https://senatinform.ru/news/v_roskomnadzore_rasskazali_kak_podat_zhalobu_na_razglashenie_personalnykh_dannykh/

Что делать в случае кражи аккаунта ребенка на «Госуслугах»

Если мошенники украли аккаунт на «Госуслугах», то следует немедленно переходить к восстановлению доступа через техподдержку или банковские приложения.

Что можно сделать

- Позвонить на горячую линию по номеру: **8-800-100-70-10.** Для подтверждения личности следует приготовить паспорт. Оператор поможет восстановить доступ и подскажет дальнейшие действия.
- Если по телефону восстановить доступ не удалось, то следует обратиться в ближайший центр обслуживания. Там вам помогут восстановить доступ.

Полезные ссылки

Карта центров обслуживания «Госуслуг»:

https://map.gosuslugi.ru/?layer=co

Как восстановить доступ к «Госуслугам»

1. Попробуйте сбросить пароль: на странице входа нажмите «Забыли пароль?» и следуйте инструкциям. Ссылка для сброса придет на ваш email или телефон, который вы указали при регистрации.
2. Если мошенники успели сменить контактные данные, сброс не сработает. Тогда:

- восстановите доступ через приложение банка-партнера (https://www.gosuslugi.ru/help/faq/general/7000001);
- позвоните на горячую линию «Госуслуг»:

8 (800) 100-70-10;
- обратитесь в центр обслуживания (https://www.gosuslugi.ru/help/faq/login/100461).

После восстановления доступа:

- смените пароль на более надежный — используйте комбинацию букв, цифр и символов;
- проверьте и обновите личные данные (номер телефона, электронную почту или адрес), если они были изменены мошенниками;
- изучите историю операций, чтобы отследить подозрительные действия: запросы на выплаты или подачу заявлений;
- закажите кредитную историю, чтобы убедиться, что на вас не оформили заем.

Как защитить аккаунт на Госуслугах в будущем:

- включите двухфакторную аутентификацию — при входе на ваш номер будет приходить СМС с кодом подтверждения.
- укажите доверенный контакт в настройках безопасности. Это может быть кто-то из ваших близких или друзей. Ему отправят оповещение, если кто-то захочет сменить пароль.

Дополнительно поставьте самозапрет на кредиты — это можно сделать на «Госуслугах» или в МФЦ. Тогда мошенники не смогут взять заем на ваше имя, даже если получат ваши данные.

Правила кибербезопасности

- Никогда не передавать логины, пароли и коды из СМС для двухфакторной аутентификации третьим лицам, под каким бы предлогом их ни просили.
- Регулярно проверять раздел «Активные сессии» или «Устройства» в настройках мессенджеров, чтобы

убедиться, что к аккаунту не подключены посторонние лица.

- С осторожностью относиться к предложениям о покупке или аренде аккаунтов. Подобные сделки в 100% случаев связаны с противоправной деятельностью.
- Критически оценивать предложения о «легком заработке» в интернете, которые требуют выполнения простых технических действий с личными данными или социальными сетями.

Как распознать деструктивный контент?

Распознавание деструктивного контента требует внимательности к деталям и критического анализа поступающей информации.

Первым признаком является резкая эмоциональная реакция, которую пытается вызвать автор: если после прочтения или просмотра возникают сильное чувство тревоги, страха, гнев или ненависть к определенной группе людей, вероятно, контент создан для манипуляции.

Важно обращать внимание на способ подачи материала. Деструктивные сообщения часто содержат ультимативные утверждения, не допускающие сомнений, или делят мир на «черное и белое», «своих и чужих».

Использование шокирующих заголовков, которые не соответствуют содержанию, а также обильное использование агрессивной лексики и капслока служат индикаторами токсичной информационной среды.

Следует анализировать предлагаемые действия. Если контент призывает к изоляции от близких, отказу от критического мышления, участию в опасных для здоровья активностях или оправдывает насилие как единственный способ решения проблем, это явные признаки опасности.

Отсутствие ссылок на проверяемые источники или ссылки на анонимные ресурсы также должны вызывать подозрение.

Деструктивный контент может романтизировать депрессивные состояния или рискованные поступки, представляя их как признак исключительности или силы духа. Деструктивная группа, как правило, является закрытой, чтобы придать оттенок «исключительности» и «эксклюзивности информации».

Понимание этих признаков позволяет вовремя прекратить взаимодействие с вредным ресурсом.

Как ребенку самостоятельно защититься от деструктивных сообществ?

Будьте критичны. Если вам что-то предлагают, навязывают, требуют, необходимо задать вопрос самому себе: какую цель преследует собеседник?

Оставайтесь на связи. Поддерживайте контакты с семьей, друзьями и обществом в целом. Это поможет вам сохранить критичность мышления и не поддаться влиянию группы.

Осознанно принимайте решения. Анализируйте, на какой информации вы основываетесь при принятии решений, сколько источников используете, принимаете ли во внимание последствия.

Не бойтесь задавать вопросы. Если вам предлагают присоединиться к группе, не стесняйтесь спрашивать о правилах, целях и последствиях выхода из сообщества.

Сверяйтесь со своими эмоциями. Если что-то кажется вам подозрительным или неправильным, доверяйте своему чувству.

Важно быть осведомленным о признаках деструктивных сообществ и оказывать поддержку тем, кто может оказаться в опасной ситуации. Если вы или кто-то, кого вы знаете, сталкивается с подобной проблемой, рекомендуется обратиться за помощью к близким, друзьям, специалистам или

организациям, занимающимся вопросами обеспечения безопасности личности, в том числе и психологической.

Базовые правила цифровой гигиены

Использовать сложные пароли. Не «123456» и не дату рождения. Пароль должен содержать прописные и строчные буквы, цифры и символы. Лучше — уникальный для каждого сервиса.

Включить двухфакторную аутентификацию. Даже если пароль утечет, без дополнительного кода злоумышленник не получит доступ к аккаунту.

Устанавливать приложения только из официальных магазинов. Сторонние сайты часто распространяют программы-шпионы, которые перехватывают данные.

Пользоваться отдельной картой для онлайн-платежей. Виртуальная или дополнительная карта с ограниченным балансом снижает риски при компрометации данных.

Настроить приватность в соцсетях и мессенджерах. Ограничьте круг лиц, которые видят ваши публикации, номер телефона и личную информацию.

Не сохранять пароли в браузере на чужих устройствах. Если доступ к компьютеру получит посторонний, он автоматически войдет в ваши аккаунты.

Не использовать публичный Wi-Fi для банковских операций. В открытых сетях данные могут быть перехвачены.

Не переходить по неизвестным ссылкам. Фишинговые сайты выглядят как настоящие банки или «Госуслуги», но созданы для кражи данных.

Не отправлять фото документов и коды из СМС. Код подтверждения — это ключ к вашему аккаунту. Его никогда не запрашивают сотрудники банков или ведомств.

Не публиковать избыточную личную информацию. Адрес, геолокация, данные о семье и поездках — это материал для социальной инженерии.

Советы по защите от приемов социальной инженерии

- Проверять любую информацию через официальный источник. Если звонят «из банка» — положите трубку и перезвоните по номеру с официального сайта. Если пишут «из вуза» — уточните у преподавателя или в деканате.
- Брать паузу. Фразы «срочно», «прямо сейчас», «иначе будет поздно» — главный маркер манипуляции. Законные организации не требуют немедленных действий под угрозой.
- Обсуждать подозрительные ситуации с близкими. Мошенники всегда требуют сохранить «секрет». Любое требование никому не рассказывать — тревожный сигнал.
- Разделять онлайн и реальную жизнь. Человек в мессенджере — не обязательно тот, за кого себя выдает. Фото, голос, видеосвязь могут быть поддельными.
- Использовать принцип нулевого доверия. Это означает: *по умолчанию не доверять никому в сети, пока информация не подтверждена*. Даже если собеседник представляется одноклассником, сотрудником полиции или «новым другом».
- Не сообщать коды из СМС, пароли и данные карт — никому. Ни «банку», ни «службе безопасности», ни «следователю».
- Не переводить деньги на «безопасные счета». Таких счетов не существует. Так же как не бывает «дистанционных обысков» и «декларации наличных накоплений».
- Не передавать данные под давлением. Страх уголовной ответственности, обвинения в «спонсировании терроризма» или «утечке данных» — распространенная легенда.
- Не выполнять «проверочные задания». Если вас просят оформить карту, скачать приложение, включить

демонстрацию экрана или передать устройство курьеру — это вовлечение в преступную схему.

ТЕЗАУРУС (ОСНОВНЫЕ ПОНЯТИЯ)

Дропперы/дропы (от англ. drop — бросать, уронить) — люди, которые задействованы в нелегальных схемах по выводу средств с банковских карт через свои счета и карты. Люди, в том числе и несовершеннолетние лица, нередко становятся дропперами, даже не подозревая об этом (что не освобождает их от ответственности за необдуманный шаг).

Дропперство (дроппинг) — то, чем занимаются дропперы.

Кибербезопасность — защита личной информации имеет критическое значение, поскольку в цифровом пространстве данные становятся ценным активом. Персональные сведения, такие как пароли, номера банковских карт или домашний адрес, могут стать целью злоумышленников для кражи средств или использования личных данных в корыстных целях.

Соблюдение правил цифровой гигиены — использование сложных паролей, двухфакторной аутентификации и осторожность при переходе по подозрительным ссылкам — помогает сохранить приватность и обезопасить свою цифровую жизнь от взломов и мошенничества.

Среди основных угроз в интернете выделяются следующие:

Фишинг (англ. phishing, от **fishing** —рыбная ловля, выуживание) — вид интернет-мошенничества, с помощью которого злоумышленники получают доступ к конфиденциальным данным пользователей (реквизиты банковских карт, логины и пароли аккаунтов), а также обманом предлагают загрузить вредоносные программы или продают несуществующие услуги.

Фишинговые сайты — это поддельные сайты известных компаний, например банков, социальных сетей, маркетплейсов,

госорганов. Они могут походить на оригиналы интерфейсом, однако у них искаженное доменное имя.

Жертвы злоумышленников «попадают на крючок» — посещают такие сайты переходя из сообщений в мессенджерах, социальных сетях или фишинг-писем на электронной почте, где им предлагают срочно перейти по ссылке под каким-либо увлекательным предлогом.

Интернет-мошенничество — может проявляться в различных схемах обмана с целью кражи денег.

Компьютерные вирусы и вредоносное программное обеспечение — способны повредить файлы, ограничить доступ к мобильному устройству или компьютеру, тайно собирать данные о действиях пользователя.

Сваттинг (от англ. SWAT, swatting — вызов спецназа) — заведомо ложное сообщение об угрозе преступления или о происшествии. Делается это для того, чтобы привлечь внимание экстренных служб или правоохранительных органов и направить сотрудников служб по ложному адресу.

Доксинг (англ. doxing, от сокр. docs — документы) — это сбор и распространение личной информации о человеке без его согласия. Эти действия не всегда незаконны, но являются нарушением сетевого этикета и часто запрещены внутренними правилами интернет-сообществ. Причиной доксинга может являться желание шантажировать жертву, отомстить ей или затравить ее. Также термин употребляется в отношении сбора чувствительной информации об организациях.

Кардинг (от англ. carding) — вид мошенничества, при котором производится операция с использованием платежной карты или ее реквизитов. Мошенники, кроме звонков напрямую, могут находить реквизиты платежных карт на взломанных серверах интернет-магазинов, платежных и расчетных систем, а также с персональных компьютеров.

Постразговор

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.