

**МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ
ДЛЯ ПРОВЕДЕНИЯ ЗАНЯТИЯ ПО ТЕМЕ «БЕЗОПАСНЫЙ ИНТЕРНЕТ.
ЦИФРОВОЙ ИММУНИТЕТ» (10-11 КЛ., СПО)**

ЦЕЛЬ

Формирование у обучающихся осознанного и ответственного подхода к использованию цифрового пространства

ЗАДАЧИ

ОБРАЗОВАТЕЛЬНЫЕ	– актуализация знаний обучающихся о киберугрозах (фишинг, интернет-мошенничество, кибербуллинг, кража личных данных)
РАЗВИВАЮЩИЕ	– развитие навыков критического анализа информации в сети и защиты персональных данных; – формирование алгоритмов безопасного поведения в различных онлайн-ситуациях
ВОСПИТАТЕЛЬНЫЕ	– способствование воспитанию цифровой культуры и этики

РЕЗУЛЬТАТЫ ОСВОЕНИЯ ТЕМЫ

МЕТАПРЕДМЕТНЫЕ	<i>Работа с информацией:</i> – владеть навыками получения информации из источников разных типов, самостоятельно осуществлять поиск, анализ, систематизацию и интерпретацию информации различных видов и форм представления; – оценивать достоверность, легитимность информации, ее соответствие правовым и морально-этическим нормам; – использовать средства информационных и коммуникационных технологий в решении когнитивных, коммуникативных и организационных задач с соблюдением требований эргономики, техники безопасности, гигиены, ресурсосбережения, правовых и этических норм, норм информационной безопасности; – владеть навыками распознавания и защиты информации, информационной безопасности личности
ЛИЧНОСТНЫЕ	<i>Гражданское воспитание:</i>

	– соблюдение основополагающих норм информационного права и информационной безопасности; – готовность противостоять идеологии экстремизма, национализма, ксенофобии, дискриминации по социальным, религиозным, расовым, национальным признакам в виртуальном пространстве <i>Духовно-нравственное воспитание:</i> – сформированность нравственного сознания, этического поведения; – способность оценивать ситуацию и принимать осознанные решения, ориентируясь на морально-нравственные нормы и ценности, в том числе в сети Интернет <i>Ценность научного познания:</i> – сформированность мировоззрения, соответствующего современному уровню развития науки, достижениям научно-технического прогресса и общественной практики за счет понимания роли информационных ресурсов, информационных процессов и информационных технологий в условиях цифровой трансформации многих сфер жизни современного общества
--	---

СТРУКТУРА ЗАНЯТИЯ

ЭТАПЫ	– <i>Организационный момент. Мотивация</i> (3 мин.); – <i>Деятельностный. Станции-практикумы</i> (25 мин.); – <i>Подведение итогов. Рефлексия</i> (2 мин.)
СОДЕРЖАНИЕ	– Введение в тему, просмотр видеороликов, их обсуждение, проведение блиц-опроса; – Станция 1: «Парольный щит»; – Станция 2: «Информационный детектив»; – Станция 3: «Поле цифровой чести»; – Проведение опроса; – Подведение итогов

ХОД ЗАНЯТИЯ

Слайд 2.

Просмотр видеороликов и их обсуждение.

Примерные вопросы для обсуждения: «Были ли видеоролики интересны? На что обратили внимание? Как вы думаете, о чем мы будем сегодня говорить?».

Слайд 3. Введение в тему

Задача: вступить в межличностный контакт для решения практических и жизненных задач, мотивация обучающихся для обсуждения вопросов безопасного использования сети Интернет.

Возможные реплики учителя:

«Добрый день! Сегодня мы поговорим о пространстве, в котором проводим значительную часть жизни – об интернете. Он дает нам невероятные возможности, но, как и любой мегаполис, имеет свои «темные переулки». Наша задача сегодня – не запугать друг друга, а выработать своего рода «цифровой иммунитет» – набор привычек и знаний, которые помогут нам уверенно и безопасно ориентироваться в сети».

Беседа по теме занятия. Примерные вопросы аудитории:

«Что такое информация в сети, чем мир реальный отличается от виртуального. С какими проблемами вы сталкивались в сети?»

Проведение блиц-опроса (интерактивного голосования) по примерным вопросам:

«Кто из вас проверяет соцсети в первые 5 минут после пробуждения?»;

«Кто сталкивался с предложением «легкого заработка» в сети?»;

«Кто или чьи знакомые сталкивались со взломом аккаунта?»;

«Кто уверен, что его пароли от почты и соцсетей достаточно надежны?».

Комментарий учителя: «Как видим, с этими ситуациями сталкиваются многие. Давайте разберемся, как из потенциальной жертвы превратиться в грамотного и защищенного пользователя».

Учитель объясняет суть работы: обучающиеся объединяются в команды и поочередно проходят «станции», на которых выполняют интерактивные задания. На каждую станцию отводится по 7-8 минут.

Слайд 4. Станция 1: «Парольный щит»

Задача: сформулировать правила создания надежных паролей.

Задание 1. Проанализировать предложенные пароли (слабые, средней надежности и надежные) на предмет надежности и сделать выводы.

Задание 2. Сформулировать правило составления пароля.

На экране приведены примеры паролей: слабые (ненадежные), пароли средней надежности и надежные пароли. Учащимся необходимо определить, какой пароль к какому виду надежности относится, и аргументировать свой ответ.

Комментарий для учителя:

Слабые (ненадежные) пароли.

123456 – самый популярный пароль в мире. Подбирается мгновенно.

Password – второе слово в топе самых слабых паролей.

Qwerty – простое сочетание клавиш на клавиатуре. Очень распространен.

Ivanov1990 – содержит распространенную фамилию и год рождения, легко находится через социальный инжиниринг.

loveyou – очень распространенное словосочетание, не представляет сложности для взлома.

Пароли средней надежности.

MyPass123 – сочетание заглавных букв, строчных и цифр — это хорошо. Но это шаблонная структура (СловоЧисло), а цифры в конце предсказуемы.

july2024! – содержит название месяца, год и распространенный спецсимвол. Лучшие, чем просто слово, но все еще может быть уязвим для атак по словарю с подстановкой дат.

Надежные пароли.

Tr7@1kL#p\$9qBm& – длинный (16 символов), содержит случайный микс заглавных и строчных букв, цифр и специальных символов. Не имеет очевидной логики или слов.

Далее учителю необходимо подвести итог: как создать надежный пароль?

1. Длина – главный приоритет. Необходимо стремиться к 8 и более символам.

2. Используйте сложность. Комбинируйте:

Заглавные буквы (A-Z);

Строчные буквы (a-z);

Цифры (0-9);

Специальные символы (!, @, #, \$, % и т.д.).

3. Избегайте осмысленных слов и личной информации.

4. Используйте технику запоминания с помощью фразы.

Возьмите легко запоминающуюся фразу: «Котик съел 2 кусочка колбасы в субботу!».

Возьмите первые буквы каждого слова и замените цифры/знаки: Kс2кквс!

Усложните, добавив разные регистры и английские буквы: Ks2kkvS!

5. Лучшее решение – использовать менеджер паролей (например, Bitwarden, KeePass, 1Password). Он сгенерирует и запомнит за вас уникальные сложные пароли для каждого сайта.

Вывод: безопасность ваших аккаунтов начинается с создания надежного пароля.

Слайды 5-8. Станция 2: «Информационный детектив»

Задача: научиться распознавать фишинговые сайты и фейковые (ложные, поддельные) новости.

Командам демонстрируются:

- 1) Поддельное письмо от «банка» с просьбой «подтвердить данные карты».
- 2) Сенсационная «новость» из сомнительного паблика.
- 3) Подозрительное сообщение в мессенджере со вложенной ссылкой.
- 4) Предложение о высокооплачиваемой работе без опыта.

Задача команды: проанализировать каждый кейс и найти 3-5 «признаков лжи», используя чек-лист (распечатанный вариант раздается группе):

проверка адреса отправителя/сайта (орфографические ошибки, странные домены);

наличие давления и срочности («Срочно перейдите по ссылке!»);

проверка информации по другим надежным источникам;

анализ грамматики и стиля.

После выводов обучающихся им представляется подробный анализ сообщений с указанием основных признаков неправдоподобной информации.

Комментарий для учителя по каждой ситуации:

- 1) Письмо из банка на почту (представлено на слайде).

Что подозрительно?

Проверка адреса отправителя/сайта. Домен отправителя: tinkkoff-bank.ru (две буквы «к») вместо официального tinkoff.ru. Домен в ссылке: tinkoff-bank-security.ru – это вымышленный домен. Настоящий банк использует свой основной домен (tinkoff.ru), а ссылки для входа ведут на защищенные страницы с https:// и знакомым адресом.

Наличие давления и срочности: слова «Срочно!», «в течение 2 часов», «Ваша карта будет заблокирована» – классический прием, чтобы вы действовали быстро, не думая; угроза «доступ... будет приостановлен» – давление через страх.

Проверка по другим источникам: не переходя по ссылке, можно открыть официальное приложение банка или позвонить по номеру с его сайта. Там либо будет такое же сообщение (если оно реальное), либо ничего. В 99.9% случаев в приложении не будет никаких предупреждений о блокировке.

Анализ грамматики и стиля: официальные письма от банков почти всегда содержат ваше имя и фамилию, а не безликое «Уважаемый клиент!»; стиль может быть излишне драматичным и неформальным для официального финансового учреждения.

- 2) Сенсационная «новость» из сомнительного паблика (пост в социальной сети) (представлена на слайде).

Что подозрительно?

Проверка адреса отправителя/сайта: источник – паблик с громким, но непрофессиональным названием, не связанный с официальными научными или новостными СМИ; ссылка ведет на непонятный сайт, а не на публикацию в научном журнале или пресс-релиз реального института.

Наличие давления и срочности: использование капса («ШОК»), множественных восклицательных знаков и слова «ВЛАСТЬ СКРЫВАЕТ» создает эмоциональный ажиотаж и ощущение исключительной важности, чтобы вы перешли по ссылке, не проверяя факты.

Проверка по другим источникам: если поискать эту новость по названию в авторитетных СМИ (РИА Новости, Коммерсант, ВВС и т.д.) или научных порталах, вы не найдете ни одного подтверждения. Полное отсутствие информации в надежных источниках — главный признак фейка.

Анализ грамматики и стиля: стиль желтой прессы: кричащий заголовок, отсутствие конкретных деталей (имя ученого, название НИИ), расплывчатые формулировки («спецслужбы», «Кремль»), теория заговора.

3) Подозрительное сообщение в мессенджере со вложенной ссылкой (представлено на слайде).

Что подозрительно?

Проверка контакта. Отправитель: Аккаунт с именем «Мама» может быть любым. Нужно всегда проверять номер телефона. Если это не тот номер, что сохранен у вас в контактах, это 100% мошенник; ссылка: подозрительный домен quick-money-transfer.online не имеет ничего общего с известными платежными системами или банками.

Наличие давления и срочности: «Срочно!», «сломался телефон», «не могу дозвониться» — создается искусственная критическая ситуация, чтобы вы не стали звонить настоящей маме и проверять информацию.

Проверка по другим источникам. Единственный и главный источник — позвонить маме (или другому отправителю) на ее настоящий номер. Если она в порядке и ничего не знает об этом сообщении — это мошенничество.

Анализ грамматики и стиля: сообщение может быть написано в несвойственном для вашего близкого человека стиле. Фраза «это безопасно» — классический прием, который мошенники добавляют, чтобы развеять ваши сомнения.

4) Предложение о высокооплачиваемой работе без опыта (представлено на слайде).

Что подозрительно?

Проверка адреса отправителя/сайта: домен job-global-finance-hh.ru имитирует сайт по поиску работы hh.ru, но является подделкой. Настоящие компании размещают вакансии на официальных доменах (hh.ru, superjob.ru) или на своих корпоративных сайтах.

Наличие давления и срочности: давление здесь другого рода — это давление на жадность. «Высокая зарплата без опыта» — слишком хорошо, чтобы быть правдой. Это делается, чтобы человек отбросил критическое мышление из-за желания быстро и легко заработать.

Проверка по другим источникам: поиск названия компании и вакансии на том же hh.ru или LinkedIn не даст результатов. Если компания такая «крупная и международная», о ней точно будет информация в интернете.

Анализ грамматики и стиля: расплывчатые, но при этом подозрительные обязанности: «обработка транзакций», «контроль финансовых потоков» для человека без опыта — это часто эвфемизм для работы «дропа» (перевода через свой счет нелегальных денег); слишком низкий порог входа: «наличие карты и смартфона» — единственное требование для зарплаты в 150 тысяч.

Слайды 9-10. Станция 3: «Поле цифровой чести»

Задача: обсудить проблему кибербуллинга и выработать стратегию поведения для ролей жертвы, агрессора, свидетелей, адвокатов и судьи.

Обучающимся предлагается кейс «В школьном паблике появился анонимный пост с насмешками над учеником 10 класса. Пост активно комментируют и лайкают». Ваши действия? (пост представлен на слайде).

Учащиеся распределяются по ролям:

жертва насмешек, агрессор, свидетели, адвокаты и судья. Даётся время на подготовку позиций.

Затем аудитории демонстрируется слайд с ролями. По наводящим вопросам по каждой роли обучающимся дается время на подготовку позиций. Далее происходит рассмотрение линий поведения каждого участника.

Итог задания: после обсуждения в ролях заслушиваем позиции каждой стороны и вместе пробуем найти наиболее эффективный и гуманный выход из ситуации.

Задача состоит в подготовке аргументов со своей позиции, после чего проходит общее обсуждение и выработка правильного алгоритма действий: не вступать в перепалку, сделать скриншоты, пожаловаться модераторам, обратиться к взрослому, которому доверяешь.

Комментарий для учителя.

Почему этот пример удачен для разбора в игре:

уничтожительные характеристики: пост высмеивает внешность («причёска», «кофта»), физические данные («бегает, как пингвин») и социальную активность («статус ВК»);

язык и стиль: используется язвительный, «мемный» язык, характерный для подростковой среды («эволюция — это миф», «местный гений»), что делает пост уязвимым и «релевантным» для аудитории;

анонимность: упоминание «анонимно» и использование иконки анонима подчёркивает главную проблему — безнаказанность;

хештеги: хештеги #нашашкола и #10Бпривет целенаправленно привлекают внимание именно той аудитории, где учится жертва, усиливая публичный эффект;

триггер для обсуждения: текст не является откровенно матерным или крайне жёстким, что часто бывает в реальности, но он содержит едкие намёки и издевки, что идеально подходит для анализа мотивов агрессора и чувств жертвы.

Этот пост служит отличной отправной точкой для обсуждения в ролях: «Жертва» может описать унижение от таких намёков, «Агрессор» — объяснить это «безобидным стёбом», а «Свидетели» — продемонстрировать, как такие, казалось бы, «невинные» шутки, могут запустить механизм травли.

Основные шаги, которые можно предпринять (дополнительно):

1. Стоп! Не отвечать и не нападать в ответ. Агрессия порождает агрессию.

2. Сохранить доказательства. Сделать скриншоты (это очень важно!).

3. Остановить травлю технически. Заблокировать обидчика, пожаловаться модераторам платформы.

4. Обратиться за поддержкой: рассказать взрослым, которым можно доверять (родителям, классному руководителю, школьному психологу). Не оставаться один на один с проблемой.

5. Помните! Если вы стали свидетелями травли кого-то из ваших друзей, окажите моральную поддержку. Поговорите или напишите слова утешения.

Учитель делает акцент на ответственности, предусмотренной за травлю.

Слайд 11. Об ответственности за кибербуллинг

Представлено на слайде.

Слайд 11. Проведение опроса.

Примерный перечень вопросов представлен на слайде.

Слайд 12. Подведение итогов

Сформулировать вывод о необходимости знания и соблюдения правил безопасного поведения в различных онлайн-ситуациях.

Возможные заключительные слова учителя:

«Ваш цифровой след – это ваша репутация. Ваша безопасность – это ваша ответственность. Сегодня мы сделали важный шаг к тому, чтобы наше онлайн-пространство стало безопаснее и комфортнее для каждого. Помните, что «цифровой мир», как и обычный, полон возможностей и знаний, но требует от своих обитателей ответственного отношения и знания правил безопасного поведения.

Благодарю вас за это путешествие! Оно было увлекательным и познавательным!».

Станция 2 «Информационный детектив»

Чек-лист

Критерий	Ситуация 1		Ситуация 2		Ситуация 3		Ситуация 4	
	Есть	Нет	Есть	Нет	Есть	Нет	Есть	Нет
Проверка адреса отправителя/сайта (орфографические ошибки, странные домены)								
Наличие давления и срочности								
Проверка информации по другим надежным источникам								
Анализ грамматики и стиля								