Муниципальное автономное
образовательное учреждение
дополнительного образования
«Детско-юношеский центр»

Детско Юношеский Центр
Верхняя Салда

Сборник методических материалов
по Интернет-безопасности
«В сети с умом»

Автор - составитель:
Малкина Елена Олеговна
Педагог - организатор

г. Верхняя Салда
2026 год

Содержание

Паспорт проекта

Название проекта	**В сети с умом!**
Краткое описание проекта	Данный проект направлен на формирование у обучающихся знаний и навыков безопасного поведения в сети Интернет. В ходе реализации проекта были разработаны мероприятия, которые учат школьников ответственному использованию цифровых технологий, формируют навыки защиты личных данных и безопасного общения в онлайн-среде. Все мероприятия несут в себе идею повышения цифровой грамотности и привлечения внимания молодежи к актуальным проблемам Интернет-угроз: мошенничеству, кибербуллингу, распространению недостоверной информации. Также проект направлен на информированность обучающихся о способах противодействия киберугрозам и обучение их практическим действиям в ситуациях, связанных с рисками в онлайн-пространстве.
Обоснование значимости проекта	Проблема киберугроз в Российской Федерации является одним из факторов, угрожающих личной безопасности граждан и информационной безопасности государства. По данным экспертов, ежегодно фиксируется рост числа преступлений, связанных с Интернет-мошенничеством, кибербуллингом, распространением недостоверной информации и вовлечением несовершеннолетних в деструктивные сообщества. Особую уязвимость в цифровом пространстве демонстрируют дети и подростки, активно использующие социальные сети и онлайн-сервисы. На федеральном уровне особое внимание вопросам цифровой грамотности уделяется в рамках проекта «Урок цифры», целью которого является формирование у школьников базовых навыков безопасного поведения в сети Интернет и развитие ответственного отношения к использованию современных технологий. Приоритетными направлениями деятельности в сфере Интернет-безопасности являются: • обучение детей и подростков правилам защиты персональных данных; • профилактика вовлечения молодежи в мошеннические и деструктивные практики; • формирование навыков критического восприятия информации и предупреждение распространения вредоносного контента. Поэтому формирование знаний и практических навыков у обучающихся в области Интернет-безопасности является крайне актуальной задачей на сегодняшний день. Для успешной реализации данного проекта необходим комплексный подход, который позволит своевременно предупреждать риски, связанные с киберугрозами, и создавать условия для безопасного и

	ответственного поведения детей и подростков в цифровой среде.
Целевые группы проекта	Целевыми группами проекта выступают участники Летней оздоровительной кампании 2025 года в ЗОЛ «Лесная сказка». Возраст участников проекта 14 – 17 лет.
Цель проекта	Формирование у обучающихся знаний и навыков безопасного поведения в сети Интернет и ответственного использования цифровых технологий.
Задачи проекта	- Разработать и провести мероприятия, способствующие просвещению молодёжи в вопросах профилактики экстремистской и террористической деятельности; - Организовать взаимодействие структур гражданского общества, образовательных организаций, органов государственной власти и местного самоуправления, направленного на объединение правовых, кадровых, научных ресурсов по вопросам профилактики терроризма и экстремизма в молодежной среде. - Вовлечь молодежь в социально значимую деятельность по профилактике терроризма и экстремизма. - Обучить безопасному поведению при угрозе террористического акта.
Планируемые результаты	• Совершенствование форм и методов работы по формированию у обучающихся навыков безопасного поведения в сети Интернет; • Повышение уровня цифровой грамотности участников образовательного процесса, в том числе в вопросах защиты персональных данных и ответственного использования цифровых ресурсов; • Развитие критического мышления и культуры безопасного поведения в цифровой среде; • Вовлечение обучающихся в социально значимую деятельность, направленную на популяризацию знаний о правилах Интернет-безопасности.
Ресурсное и методическое обеспечения проекта	**Кадровые ресурсы:** педагог, осуществляющий мероприятия в рамках профилактики Интернет-безопасности и цифровой безопасности среди молодёжи, партнёры сетевого взаимодействия. **Информационные ресурсы:** 1. Методические рекомендации по проведению уроков безопасного Интернета в школах. – Лига безопасного Интернета, г. Москва, 2022 г. 2. Методическое пособие Профилактика кибермоббинга и кибербуллинга в среде несовершеннолетних: методическое пособие / Т.А. Дёгтева и др. – Ставрополь: Ставропольское издательство «Параграф», 2017 г. – 81 с.

	3. Пережогин Л.О., Федонкина А.А. Интернет-зависимость: предпосылки формирования, клиническая картина, лечение и профилактика: Методические рекомендации. – М.: ФГБУ “НМИЦ ПН им. В.П. Сербского” Минздрава России, 2024. – 33 с 4. Методические рекомендации для несовершеннолетних, родителей (законных представителей) несовершеннолетних, наглядные информационные материалы по безопасному использованию сети «Интернет» в целях предотвращения преступлений, совершаемых с ее использованием, как самими несовершеннолетними, так и в отношении них. Методические рекомендации / Авторы-составители: Артамонова Е.Г., Бородина А.С., Мелентьева О.С. – М.: ФГБУ «Центр защиты прав и интересов детей», 2021 – 35 с. 4. Сборник сценариев по профилактике Интернет-безопасности, ДЮЦ. Интернет – ресурсы: 5. Федеральный закон от 27.07.2006 №149-ФЗ (ред. от 24.06.2025) «Об информации, информационных технологиях и о защите информации».
Руководитель проекта	Малкина Елена Олеговна – педагог – организатор ДЮЦ, первой квалификационной категории.

Перечень мероприятий, проводимых в рамках проекта

Формы и название мероприятий	Аннотация
Круглый стол «Сеть вокруг нас»	В ходе данного занятия будут рассмотрены основные угрозы, возникающие при использовании Интернета, и способы защиты от них. Мероприятие направлено на формирование у учащихся навыков безопасного поведения в цифровой среде, развитие критического мышления и ответственности при работе с информацией.
Квест-игра «Интернет - территория безопасности!»	В ходе квест-игры «Интернет: территория безопасности» участники, разделённые на команды, будут проходить несколько интерактивных станций, выполняя задания, связанные с созданием надёжных паролей, распознаванием фишинга, анализом цифровых следов, соблюдением интернет-этикета и безопасной работой с электронной почтой. Игра направлена на формирование у учащихся навыков безопасного поведения в сети, развитие критического мышления и умения работать в команде.
Игра по станнциям «КиберБОБЕР»	В ходе игры по станциям «КиберБОБЕР» участники, разделённые на команды, будут проходить различные интерактивные станции, выполняя задания, направленные на развитие навыков безопасного и этичного поведения в Интернете, распознавание киберугроз, освоение правил сетевого этикета, а также развитие критического мышления и командной работы. Игра способствует формированию ответственного отношения к цифровой среде, расширению знаний о киберрисках и закреплению полученных знаний на практике.
Онлайн – олимпиада «БЕЗопасный Интернет»	Олимпиада направлена на привлечение внимания обучающихся ВСГО к вопросам безопасного и этичного использования сети Интернет..
Ролевая игра «Суд над Интернетом»	В ходе ролевой игры «Суд над Интернетом» участники примут на себя различные роли (обвинение, защита, свидетели, присяжные) и разберут реальные и смоделированные ситуации, связанные с интернет-мошенничеством, фишингом, кибербуллингом и утечкой данных. Мероприятие направлено на формирование у учащихся критического мышления, ответственности за собственное поведение в сети, навыков аргументации и работы в команде.
Онлайн – интеркатив «Угрозам.NET»	Мероприятие в формате активного обучения в онлайн формате. Учащимся предстоит просмотреть информационные видеоролики и выполнить интеллектуальные задания.
Квиз – игра «Садись 5!»	В течение 7 раундов участники игры, проявляя внимание, логику и критическое мышление, ответят на вопросы КВИЗа, связанные с безопасным поведением в Интернете, защитой персональных данных, распознаванием киберугроз и профилактикой мошенничества и кибербуллинга в виртуальной среде.

Круглый стол «Сеть вокруг нас»

Цель занятия – формирование у подростков ответственного и критического отношения к использованию интернета, развитие навыков безопасного поведения в сети.

Задачи:

1. Познакомить учащихся с положительными и отрицательными сторонами интернета.
2. Рассмотреть основные угрозы онлайн-пространства (вредоносные программы, кибербуллинг, мошенничество, деструктивные сообщества).
3. Научить правилам безопасного поведения в сети.
4. Сформировать критическое мышление при восприятии интернет-контента.

Планируемые результаты:

- **Знания:** учащиеся понимают преимущества и риски интернета.
- **Умения:** умеют распознавать опасные ситуации в сети и знают, как себя вести.
- **Отношения:** осознают важность ответственного и безопасного поведения в интернете.

Возраст: 12–17 лет

Форма: круглый стол с элементами дискуссии и практики

Время: 40–45 минут

Электронная презентация к занятию: https://disk.yandex.ru/i/TQKZ7SLdnS-5ug

1. Организационный момент (2 мин)

Ведущий: «Здравствуйте, ребята! Сегодня мы поговорим об очень важной теме — об интернете. Интернет окружает нас повсюду. Он помогает нам учиться, общаться, развлекаться, но вместе с этим может быть и опасен. Наша задача — научиться пользоваться им безопасно».

2. Деление на группы (5 мин)

- Участники делятся на две команды:
  - Группа 1**:** называет положительные стороны интернета**.**
  - Группа 2**:** называет отрицательные стороны интернета**.**

Ведущий: «У вас есть 3 минуты, чтобы составить список преимуществ или недостатков интернета. Подумайте о том, с чем вы сталкивались сами».

- Обсуждение результатов, ответы фиксируются на доске.

3. Актуализация знаний (слайды 2–3) (5 мин)

Ведущий: «Посмотрите на слайды. Сравните: что из того, что вы назвали, совпадает с тем, что указано в презентации? Что нового для себя заметили?»

- Краткое обсуждение: делаем вывод, что интернет — это и возможности, и риски.

4. Основной этап (15–17 мин)

Форма работы: обсуждение + коллективный поиск выхода. **Ведущий демонстрирует слайды 4–11.**

Структура для каждой угрозы:

1. В чём опасность?
2. Вопросы детям («Сталкивались ли вы с этим?»).
3. Решения (обсуждаем, затем показываем на слайде).

Угроза 1. Вредоносные программы (слайд 4)

- Опасность: вирусы портят компьютер, крадут данные.
- Решения: не открывать вложения, скачивать только из официальных источников, обновлять антивирус.
- Вопрос: «Кто из вас видел предупреждение об опасном файле? Как вы поступили?»

Угроза 2. Фишинг и спам (слайд 5-8)

- Опасность: мошенники выманивают пароли и данные карт.
- Решения: не переходить по подозрительным ссылкам, проверять адрес сайта, не вводить данные на непроверенных ресурсах.
- Вопрос: «Какие письма или сообщения вызывают у вас подозрение?»

Угроза 3. Кибербуллинг (слайд 9)

- Опасность: травля в сети, угрозы, давление.
- Решения: не отвечать, блокировать, жаловаться, сохранять доказательства.
- Вопрос: «Почему важно не реагировать на обидчиков?»

Угроза 4. Зависимость от интернета и игр

- Опасность: тратим слишком много времени онлайн, ухудшение здоровья, падает успеваемость.
- Решения: ограничивать время, устраивать «цифровую диету», заниматься спортом и хобби.
- Вопрос: «Сколько времени вы проводите в интернете в день?»

Угроза 5. Запрещённый контент и деструктивные сообщества (слайды 12–13)

- Опасность: группы про наркотики, экстремизм, трэш-стримы, суицидальные паблики.
- Решения: критически относиться к информации, проверять источники, не вступать в сомнительные группы, рассказывать взрослым.
- Вопрос: «Почему такие сообщества особенно опасны для подростков?»

Угроза 6. Распространение личных данных (слайды 14)

- Опасность: фото и видео могут попасть к мошенникам, шантаж.
- Решения: не выкладывать личное в открытый доступ, проверять настройки приватности.
- Вопрос: «Что может случиться, если фото попадёт к незнакомым людям?»

Угроза 7. «Лёгкие деньги» и интернет-мошенничество (слайд 15)

- Опасность: обещания быстрого заработка, фальшивые магазины, выманивание данных карт.
- Решения: не верить в чудо-заработки, проверять продавцов, не сообщать личные данные, подключить SMS-уведомления.
- Вопрос: «А вы видели рекламу «лёгких денег»? Что в ней настораживает?»

Угроза 8. Риски для здоровья

Опасность: зрение, осанка, сон, психическая усталость.

- Решения: перерывы каждые 40 минут, правильная посадка, физическая активность.
- Вопрос: «Что вы делаете, когда устали от гаджета?»

5. Практическая часть «Дерево решений» (слайд 16) (10 мин)

Ведущий: «Теперь давайте попробуем построить "дерево решений". Это схема:

- Проблема → Возможные действия → Последствия → Правильное решение».
- Участники делятся на группы. Каждой группе выдаётся ситуация:
  - Группа 1: Получили письмо с подозрительным вложением.
  - Группа 2: Столкнулись с кибербуллингом.
  - Группа 3: Приглашение в опасное сообщество.
  - Группа 4: Обещание "лёгких денег".
- Задание: составить дерево (можно нарисовать схему).
- Презентация решений каждой группой.

Итоговое обсуждение и выводы (5 мин)

Ведущий: «Сегодня мы разобрали, что интернет может быть и полезным, и опасным. Но главное — мы всегда можем выбрать правильный путь».

Вопросы для рефлексии:

- Что нового вы узнали сегодня?
- Какие правила вы точно будете использовать?
- Чем интернет может быть другом, а чем врагом?

Заключение: «Интернет — это инструмент. Всё зависит от того, как мы его используем. Пусть он будет вашим помощником, а не источником проблем!»

Квиз-игра «Садись 5»

Цель игры: обеспечение информационной безопасности учащихся путем формирования умений ответственного и безопасного поведения в сети Интернет.

Задачи:

- обратить внимание обучающихся на вероятность возникновения опасных ситуаций в сети Интернет;
- систематизировать знания детей в области интернет-безопасности;
- формировать умения осознанно противодействовать интернет-угрозам;
- развивать критическое мышление обучающихся.

Возраст участников: 12-15 лет

Электронная презентация к занятию:
https://drive.google.com/drive/folders/12_dFIXg55If-2onN2Aq8i0gBB0HZDwHC?usp=sharing

Деление участников на команды

Участники делятся на две-три команды в целях обеспечения активного участия в игре всех обучающихся. Команды придумывают название, связанное с сетью Интернет. Представляются.

Возможно введение балльной системы за участие в командных испытаниях

Введение в тему квиза

Упражнение «Встаньте все те, кто…»

- является пользователем Интернета;
- у кого есть своя страничка в социальных сетях;
- много времени проводит в социальных сетях;
- у кого друзей в соцсетях больше, чем в реальной жизни;
- использует Интернет, чтобы узнать что-то новое, интересное о мире и людях;
- считает, что Интернет – это свободное пространство, в котором по своему усмотрению можно делать все, что пожелаешь;
- у кого были какие-либо неприятные случаи, связанные с Интернетом;
- считает, что Интернет приносит вред физическому здоровью;
- считает, что Интернет приносит вред психическому здоровью.

Итак, мы видим, что многие из нас являются активными пользователями Интернета, поэтому сегодня мы с вами поговорим о безопасности в сети Интернет.

Сегодня реальность во многом заменяется виртуальным пространством. Мы знакомимся, общаемся и играем в Интернете; у нас есть друзья, с которыми в настоящей жизни мы никогда не встречались. Мы активно выкладываем личную информацию.

Многие из нас, к сожалению, думают, что это безопасно, потому что мы делимся всего лишь информацией о себе и к нашей обычной жизни это вроде бы не относится.

Однако информация о человеке, его персональные данные могут использоваться по-разному:

- кто-то использует эти данные для того, чтобы при помощи рекламы продать вам какую-то вещь;
- кому-то вы просто не нравитесь, и в Интернете вас могут пытаться оскорбить, выставить вас в дурном свете, создать плохую репутацию;
- с помощью ваших персональных данных мошенники, воры, могут украсть ваши деньги, шантажировать вас и заставлять совершать какие-то действия и многое другое.

Поэтому очень важно научиться правильному и безопасному поведению в сети Интернет.

Ход КВИЗ-игры

Раунд 1. Полезные программы (Слайд 2-7)

Задание - на экране появляются иконки различных программ.

Задача – вспомнить название программы и рассказать о функциях.

На обсуждение дается 20 секунд. За каждый правильный ответ команда получает 1 балл. За объяснение работы программы команда получает еще 1 балл.

Ответы записываются на бланках. После сдачи бланков, ведущий озвучивает правильные ответы (Слайд 11-18).

Раунд 2. Знаток этикета (Слайд 19-26)

Задание - на экране появляется ситуация. Задача команды – рассказать проводящему правильное решение ситуации. На обсуждение дается 30 секунд. За каждый правильный ответ команда получает 1 балл.

Раунд 3. Ребусы

На экране появляются ребусы (Слайд 28-34). Задача команды – отгадать, какое слово скрывается за ребусами. За каждый правильный ответ команда получает 1 балл.

Ответы записываются на бланках. После сдачи бланков, ведущий озвучивает правильные ответы (Слайд 35-41).

Раунд 4. Перевертыши

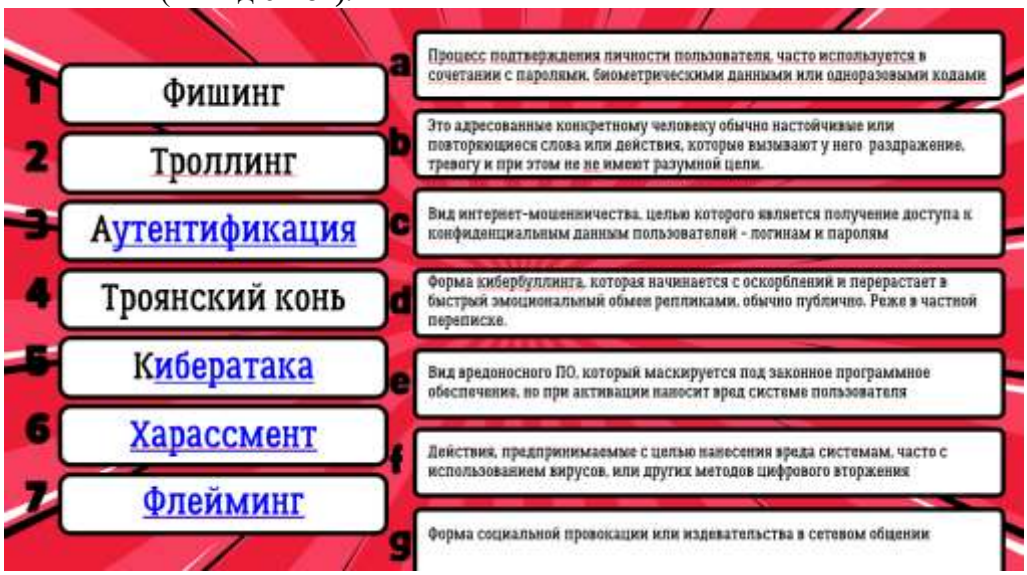
На экране появляются зашифрованные словосочетания (синонимы или антонимы) (Слайд 42-49). Задача — записать в бланк загаданное словосочетание. За каждый правильный ответ команда получает 1 балл. На обсуждение даётся 20 секунд.

Ответы записываются на бланках. После сдачи бланков, ведущий озвучивает правильные ответы (Слайд 50-57).

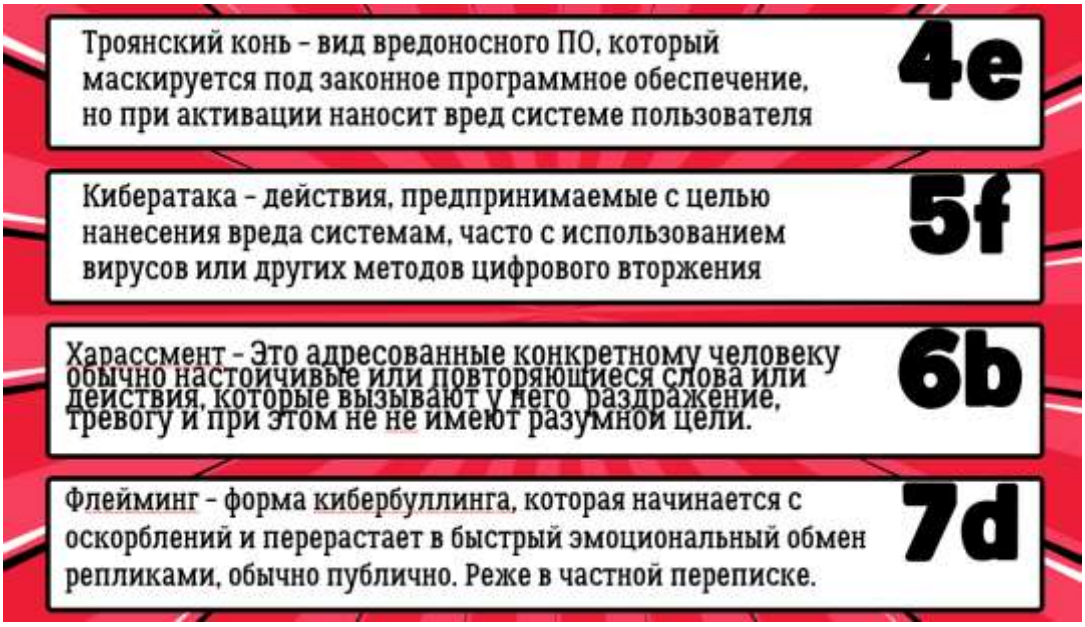
Раунд 4. Основные понятия

На экране появляются понятия и их определения. Задача – соединить определения с понятиями. За каждый правильный ответ команда получает 1 балл.

Ответы записываются на бланках. После сдачи бланков, ведущий озвучивает правильные ответы (Слайд 61-62).



Правильные ответы



Раунд 6. Я всегда/никогда не буду..

На экране появляются различные правила, которые должны начинаться со слов «Я никогда не буду…» или «Я всегда буду…». Задача – написать правильное начало каждого правила (отнести к одному из двух столбиков). За каждое правило команда получает 1 балл. На обсуждение дается 2 минуты.

Раунд 7. Старинная пословица не на ветер молвится

На экране отображаются зашифрованные пословицы (Слайд 67-74). Задача – угадать русскую народную пословицу из выдуманной. За каждый правильный ответ команда получает 1 балл. На обсуждение дается 30 секунд.

Ответы записываются на бланках. После сдачи бланков, ведущий озвучивает правильные ответы (Слайд 75-82).

Рефлексия

Давайте подведем итоги нашей игры через **Дерево рефлексии**. Начнем с **корня** — нашего опыта. Подумайте: что вы знали о интернет-безопасности до этого квиза и что узнали нового? Это помогает нам понять, с чего мы стартовали и какой прогресс сделали.» *(Участники делятся мыслями.)*

«Теперь переходим к **ветвям — что важно знать**. Здесь мы фиксируем основные правила и принципы:

- **Пароли:** они должны быть сложными, уникальными и мы рекомендуем включать двухфакторную аутентификацию, чтобы аккаунты были надежно защищены.
- **Фишинг:** никогда не переходите по подозрительным ссылкам и письмам, проверяйте отправителя и официальный сайт.
- **Сети:** открытые Wi-Fi могут быть опасны, поэтому для важных действий используйте VPN или мобильный интернет.
- **Обновления:** устанавливайте их только через официальные источники, чтобы не подхватить вредоносное ПО.»

«Следующий уровень — **ветви: что делать дальше**. Это наши конкретные действия:

- Проверить и обновить пароли.
- Включить двухфакторную аутентификацию.
- Быть внимательнее к ссылкам и письмам.
- Использовать безопасные сети.»

«И наконец, **ветви — почему это важно**. Всё, что мы делаем, направлено на защиту наших данных, предотвращение взломов и минимизацию любых рисков, связанных с использованием интернета.»

Таким образом, наше Дерево рефлексии показывает, что мы не только узнали новые вещи, но и можем сразу применять их на практике. Кто хочет поделиться, что возьмет себе в привычку прямо сейчас?

Подведение итогов

Ведущий подсчитывает количество баллов и объявляет победителя.

В завершении квиза обучающимся выдаются памятки по безопасному поведению в сети Интернет (Приложение к конспекту).

Приложение к конспекту

Памятка для обучающихся

Правила безопасного использования интернета

1. Ограничь список друзей. Добавляй только тех, с кем знаком лично.
2. Избегай случайных и незнакомых людей.
3. Защищай свои личные данные. Не указывай пароли, телефоны, адреса, дату рождения, планы на выходные и другую информацию.
4. Относись с осторожностью к размещению в социальных сетях личных фото. Не выкладывай фото других людей без их согласия.
5. Подумай, прежде чем что-то написать, опубликовать и загрузить. Ответь на вопрос: хочешь ли ты, чтобы это видели другие?
6. При регистрации в социальной сети используй сложные пароли. Для разных сайтов используй разные пароли.
7. Помни, что в интернете действуют те же правила вежливости, что в реальной жизни.
8. Будь осторожен, если тебе предлагают бесплатные услуги. Возможно за них придется платить.
9. Всегда сообщай взрослым обо всех случаях в интернете, которые вызвали у тебя смущение или тревогу

Квест-игра «Интернет: территория безопасности»

Цель: Научить учащихся основам безопасности в Интернете через командную работу и игровую деятельность, развить критическое мышление и навыки анализа цифровых угроз.

Возраст участников: 12-15 лет

Продолжительность: 60–75 минут

Формат: Квест

Материально-техническое обеспечение:

- Раздаточные материалы для каждой станции (карточки с заданиями, примеры ситуаций, загадки)
- Компьютеры/планшеты (по возможности) для выполнения заданий, связанных с цифровыми следами и фишингом
- Проектор для показа инструкций и подсказок
- Карточки для команд (персонализированные для каждой команды)
- Листочки для записи решений (для команд)
- Таймер или секундомер для контроля времени на станциях
- Секретные конверты с подсказками для каждой станции

1. **Вступление (5–7 минут)**

Цель: Ознакомить участников с правилами квеста, объяснить структуру игры и назначение станций.

Ведущий: "Дорогие друзья, сегодня вас ждёт увлекательное приключение — квест, в котором вы будете решать задачи, связанные с безопасностью в Интернете. Вам предстоит пройти несколько станций, и на каждой из них вы будете проверять свои знания и умения по защите от интернет-угроз. Важно помнить: чтобы выиграть, вам нужно работать в команде, быстро реагировать на задания и быть внимательными."

Ведущий: "В каждой команде будет свой набор заданий, а для того, чтобы пройти станцию, вам нужно будет правильно решить её задание. На выполнение каждого задания у вас будет определённое время. После каждой станции вы получите подсказку, которая поможет вам двигаться дальше. На последней станции вас ждёт главный приз!"

Ведущий: "Давайте разделимся на команды. Каждая команда получит свой набор карточек с заданиями и подсказками."

Ход мероприятия

Станция 1: «Парольная башня» (10 минут)

Цель: Научить создавать надёжные пароли и объяснить важность их использования для безопасности личной информации.

Задание: Команды получают карточку с зашифрованным паролем, который нужно расшифровать и затем создать свой собственный надёжный пароль по следующим критериям:

- Должен содержать как минимум 8 символов.
- Включать заглавные и строчные буквы.
- Использовать цифры и специальные символы (например, @, #, $, %, &).

Инструкция:

1. На карточке находятся подсказки, которые помогают выбрать правильный пароль. Например, "Секрет: 7 + 3 = 10" (значит, использовать цифры 7 и 3 в пароле).
2. После того как команда создаст пароль, она должна объяснить, почему он является надёжным.

Подсказка для команд: "Пароль должен быть сложным, как замок на башне, чтобы никто не смог его открыть."

Ключевой момент: Команды учат важность создания уникальных и сложных паролей для защиты личных данных.

Станция 2: «Фишинг или правда?» (10 минут)

Цель: Развить навыки выявления фишинга (поддельных сайтов и сообщений) и научить распознавать подозрительные действия в Интернете.

Задание: Команды получают 5 различных сообщений (например, фальшивое электронное письмо, SMS, сообщение в соцсетях), в которых скрыты попытки фишинга. Участники должны определить, какие из этих сообщений являются фальшивыми, и объяснить, почему.

Пример сообщений:

1. Сообщение о «выигрыше» в лотерее, с просьбой ввести личные данные.
2. Запрос на изменение пароля с неизвестного адреса.
3. Вопросы от якобы друзей с просьбой перевести деньги.

Инструкция: Внимательно изучите каждое сообщение. На первом шаге нужно распознать фишинг и на втором — объяснить, что в этих сообщениях могло бы насторожить вас. Каждое сообщение нужно оценить по нескольким параметрам: кто отправитель, какие ссылки, есть ли ошибки.

Подсказка для команд: Если что-то кажется слишком хорошим, чтобы быть правдой, скорее всего, это фальшивка.

Ключевой момент: Важно распознавать фишинговые угрозы, чтобы защититься от мошенников.

Станция 3: «Следопыт» (10 минут)

Цель: Научить следить за своими цифровыми следами и анализировать, как можно улучшить свою безопасность в Сети.

Задание: Команды получают информацию о нескольких персонажах и их активности в Интернете (например, что они публикуют на своих страницах, как часто они делятся личной информацией). Участники должны выявить риски для безопасности, основываясь на цифровых следах.

Инструкция: Вам нужно проанализировать информацию о персонаже, чтобы понять, какие его действия могут быть опасными. Например, если человек часто выкладывает фотографии с геолокацией, это может привести к утечке личных данных.

Пример:

- Персонаж 1: "Всё время размещает фото с указанием точного местоположения."
- Персонаж 2: "Иногда публикует информацию о финансовых тратах."

Задание: Какие из этих действий могут привести к угрозам? Что нужно изменить, чтобы обеспечить свою безопасность?

Подсказка для команд: Следы в Интернете — это ваша цифровая визитка. Защищайте её, как личные данные.

Ключевой момент: Поддержание личной безопасности в Интернете связано с тем, как управлять своими цифровыми следами.

Станция 4: «Почта в беде» (10 минут)

Цель: Научить правильно работать с электронной почтой и распознавать фальшивые сообщения.

Задание: Команды получают набор электронных писем, среди которых есть как настоящие, так и фальшивые. Нужно выбрать фальшивые письма и объяснить, чем они могут быть опасны.

Пример:

1. Письмо с просьбой «обновить пароль на сайте банка» с неизвестного адреса.
2. Письмо от известной компании с инструкциями по обновлению подписки.
3. Письмо с предложением поучаствовать в конкурсе и выиграть приз.

Инструкция: Проанализируйте каждое письмо. Обратите внимание на адрес отправителя, грамматику, ссылку на сайт, которую предлагают открыть. Какая информация вызывает у вас сомнение?

Подсказка для команд: "Когда пишут из банка или других организаций, они не требуют срочного действия через письма. Всегда проверяйте информацию."

Ключевой момент: Понимание, как правильно распознавать опасные письма и избегать фишинга.

Станция 5: «Интернет-этикет» (10 минут)

Цель: Научить основам общения в Интернете, правильному реагированию в сложных ситуациях и культуре общения.

Задание: Команды получают карточки с различными ситуациями, которые могут возникнуть в Сети. Нужно выбрать правильное поведение в каждой из ситуаций и объяснить свой выбор.

Пример ситуаций:

1. Кто-то оскорбил вашего друга в комментариях, что делать?
2. Получили сообщение от незнакомца с предложением дружбы — как ответить?
3. Кто-то делится с вами личными данными в чате — как реагировать?

Инструкция: Каждая ситуация требует от нас правильного поведения. В некоторых случаях нужно немедленно заблокировать человека, в других — обратиться за помощью к взрослым. Обсудите ситуацию с командой и выберите лучший ответ.

Подсказка для команд: В Интернете, как и в реальной жизни, важно быть вежливым и уважительным. И если что-то кажется неправильным, лучше сообщить об этом.

Ключевой момент: Соблюдение интернет-этикета помогает избежать конфликтов и неприятных ситуаций.

3. Подведение итогов и награждение (5–7 минут)

Цель: Обсудить результаты квеста, наградить победителей и подчеркнуть важность безопасного поведения в Интернете.

Ход:

Ведущий: Поздравляю вас, друзья! Вы справились с заданиями, и теперь вы точно знаете, как безопасно использовать Интернет! Ребята, давайте вспомним, какие станции вы прошли сегодня. Что показалось самым сложным? Что запомнилось лучше всего?» (ответы обучающихся)

Ведущий: Не забывайте про безопасность в Сети и всегда следуйте простым правилам, чтобы оставаться защищёнными.

Маршрутный лист для квест-игры

№	Станция	Время (мин)	Задание	Ключевые навыки	Баллы
1	Парольная башня	10	Расшифровать подсказку и создать надёжный пароль	Генерация сложных паролей, шифрование	до 10
2	Фишинг или правда?	10	Определить фальшивые сообщения и объяснить выбор	Критическое мышление, распознавание фишинга	до 10

№	Станция	Время (мин)	Задание	Ключевые навыки	Баллы
3	Следопыт	10	Проанализировать цифровой след вымышленного персонажа	Анализ информации, оценка рисков	до 10
4	Почта в беде	10	Выбрать фальшивые письма и обосновать выбор	Анализ писем, распознавание фишинга	до 10
5	Интернет-этикет	10	Разобрать ситуации и выбрать корректное поведение	Этикет, коммуникация, критическое мышление	до 10
	Итоги и награждение	5–7	Подведение итогов, вручение сертификатов и призов	Рефлексия, командная работа	—

Ролевая игра «Суд над Интернетом»

Цели:

1. Повышение осведомленности участников о вопросах интернет-безопасности.
2. Развитие навыков критического мышления и аргументации при обсуждении современных угроз в сети.
3. Формирование ответственности за безопасное поведение в Интернете.
4. Развитие навыков работы в группе, решения конфликтов и соблюдения норм безопасности в виртуальном пространстве.

Задачи:

1. Разобрать возможные угрозы в Интернете, такие как кибербуллинг, фишинг, вирусы, утечка данных.
2. Проанализировать, кто и как может быть ответственен за безопасное поведение в сети.
3. Обсудить способы защиты личных данных и конфиденциальности.
4. Рассмотреть законодательные меры по защите пользователей в Интернете.
5. Вовлечь участников в активное обсуждение и поиск решений проблем интернет-безопасности.

Планируемые результаты:

- Участники получат ясное представление о мерах безопасности в Интернете.
- Осознание роли каждого пользователя Интернета в обеспечении безопасности.
- Повышение уровня доверия к онлайн-платформам и улучшение их защиты.
- Умение аргументировать свою позицию и работать в команде.

Необходимый реквизит:

- Карточки с ролями (судья, обвинитель, защита, эксперты, свидетели, присяжные).
- Реквизит для зала суда (столы, стулья, микрофоны, подставки для карточек).
- Презентации или плакаты с информацией об угрозах в Интернете.
- Раздаточные материалы с основными понятиями по интернет-безопасности.
- Компьютеры или планшеты для поиска информации в процессе обсуждения.
- Таймер для соблюдения времени на выступления.

Мотивационный этап (10-15 минут)

Цель: Привлечь внимание участников, настроить их на тему интернет-безопасности и подготовить к ролевой игре, заставив задуматься о важности этой темы в реальной жизни. Этот этап должен вовлечь учащихся в обсуждение, побудить их задуматься о реальных угрозах в Интернете и их ответственности за свою безопасность.

Приветствие и введение в тему

Ведущий: "Здравствуйте, ребята! Сегодня у нас необычное занятие. Мы будем говорить о важной теме. Поднимите руки те, у кого есть телефоны? А у кого есть ноутбук? А у кого есть Интернет? Как вы думаете, о чем мы будем с вами говорить сегодня? С каждым годом все больше и больше аспектов нашей жизни связано с интернетом. Мы общаемся в социальных сетях, покупаем товары и услуги онлайн, работаем удаленно. Но задумывались ли вы, что интернет может быть опасным? Мы часто воспринимаем его как место для развлечений или работы, но там есть и скрытые угрозы. Именно об этом мы сегодня и поговорим."

Ведущий: Давайте рассмотрим несколько реальных угроз, с которыми может столкнуться любой из нас. Например, **кибербуллинг** — когда люди оскорбляют или унижают других в интернете. Это может происходить через социальные сети, мессенджеры, игровые платформы. Люди могут публиковать неприятные комментарии, угрожать или насмехаться, что приводит к стрессу и даже депрессии. Кто из вас слышал об этом? (ответы учащихся)

Ведущий: Точно. А что насчет фишинга? Это когда мошенники пытаются обмануть нас, отправляя письма или создавая фальшивые сайты, которые выглядят как настоящие. Они могут попросить вас ввести личные данные, например, логин и пароль от вашего аккаунта. Когда вы это делаете, они могут украсть вашу информацию (ответы учащихся).

Ведущий: Нужно быть очень внимательным, проверять адрес сайта, быть осторожными с неизвестными ссылками. Далее, еще одна угроза — мошенничество с деньгами. Мы часто покупаем товары через интернет-магазины, переводим деньги за услуги. Но иногда можно столкнуться с фальшивыми сайтами, которые просто берут ваши деньги и исчезают. Вы когда-нибудь попадали в такие ситуации? (ответы учащихся)

Ведущий: И, наконец, еще одна угроза, о которой стоит помнить, это утечка данных. Мы делаем покупки в интернете, вводим номера карт и личные данные, и если сайт не защищен, эта информация может быть украдена. Задумывались ли вы, как часто вы вводите личные данные на разных сайтах? Как вы защищаете себя от утечек?(ответы обучающихся)

Ведущий: Итак, теперь, когда мы немного поговорили о рисках, давайте посмотрим на эту ситуацию с другой стороны. Представьте, что интернет — это место, где происходит настоящий суд. Мы будем играть в ролевую игру, где некоторые из вас будут выступать в роли обвинителей, защита будет отстаивать свою позицию, а присяжные — решать, кто прав. Мы будем рассматривать, кто и как несет ответственность за безопасность в Интернете.

Ведущий: Прежде чем мы начнем, мне хотелось бы задать вам несколько вопросов. Как вы думаете, кто несет ответственность за безопасность в Интернете? Мы ведь все им пользуемся, но кто из нас должен следить за тем, чтобы все было безопасно? (ответы обучающихся). Правильно, ответственность лежит на всех, но как же быть с теми, кто нарушает правила и наносит вред? И какие меры можно предпринять для того, чтобы защитить себя и других от угроз в интернете? (ответы обучающихся). Отличные идеи! Сегодня мы попробуем разобраться в этих вопросах более подробно, и каждый из вас сможет представить свою точку зрения в игре. А теперь давайте начнем!

Основной этап (40-50 минут)

Цель: Погрузить учащихся в ситуацию, где они смогут обсудить и оценить ответственность за интернет-безопасность, выявить угрозы и проблемы, связанные с Интернетом, а также найти возможные решения. Участники должны принимать активное участие в обсуждении, представлять различные точки зрения и работать в команде.

Ведущий: Представьте, что интернет — это не просто место для общения или работы, а целая экосистема, где люди, компании, государственные органы и даже преступники взаимодействуют друг с другом. Сегодня вы будете принимать участие в судебном процессе, где разыграется случай интернет-мошенничества или нарушения безопасности. Мы постараемся разобраться, кто и за что должен нести ответственность, а также что можно сделать, чтобы повысить безопасность в сети.

Ведущий: В этой игре каждый из вас будет играть свою роль. Мы будем судить ситуацию, которая касается безопасности в Интернете. Ситуация будет связана с интернет-мошенничеством, утечкой данных или кибербуллингом. Давайте посмотрим, кто какие роли будет исполнять.

Распределение ролей

Ведущий: В игре будет несколько групп: обвинение, защита, свидетели и присяжные. Вот как это будет выглядеть:

- **Обвинитель (2-3 человека):** обвинители будут выступать против виновных сторон, аргументируя, почему они должны быть наказаны за свои действия, которые привели к угрозам безопасности в Интернете. Обвинитель будет акцентировать внимание на нарушениях закона и угрозах, которые были созданы в сети.
- **Защита (2-3 человека):** защитники будут отстаивать позицию обвиняемых, пытаясь доказать, что их действия не были преступными или что они не несут ответственности за случившееся. Это могут быть представители компаний, разработчиков

или пользователей, которые, по их мнению, соблюдали все необходимые меры безопасности.

- **Свидетели (3-4 человека):** свидетели — это участники, которые расскажут о своей личной ситуации или опыте, связанном с интернет-безопасностью. Они могут быть свидетелями реальных ситуаций с интернет-мошенничеством, фишингом, кибербуллингом или утечкой данных. Свидетели будут выступать с целью подкрепить свою позицию о важности повышения безопасности в Интернете.
- **Присяжные (все остальные участники):** присяжные должны внимательно слушать все стороны, оценивать их аргументы и в конце принять решение о том, кто прав, а кто виноват. Присяжные должны будут основывать свои решения на фактах, а не на личных симпатиях или предвзятости.

Ведущий: Теперь я расскажу вам о ситуации, которая будет обсуждаться в суде. Представьте, что одна крупная социальная сеть использовала данные своих пользователей для продажи рекламных услуг без их ведома, и в результате этого произошла утечка личной информации миллионов людей. Эта утечка привела к серьезным последствиям для пользователей: несколько людей стали жертвами фишинговых атак, мошенники начали использовать их данные для обмана. Также один из пользователей стал жертвой кибербуллинга. В суде мы будем решать, кто несет ответственность за это — сама сеть, пользователи или третьи лица.

Предположительные действия учащихся:

— Учащиеся начинают обсуждать ситуацию, анализируют, что им известно о подобных случаях.

— Некоторые могут поднять руки, чтобы спросить о подробностях или дополнениях к делу.

— Остальные уже начинают думать о своей роли в игре.

Ведущий: Теперь у вас есть несколько минут, чтобы обсудить и подготовить свои аргументы в рамках вашей роли. Подготовьте несколько важных моментов, которые вы будете представлять в суде. Не забывайте, что ваша задача — убедить присяжных в своей правоте.

Ведущий: Давайте начнем судебный процесс! Мы начинаем с заявления обвинителя. Помните, что у вас есть определенное количество времени, чтобы представить свои аргументы.

Роль обвинителя (2-3 человека): Уважаемый суд, мы обвиняем компанию, владельцев социальной сети и разработчиков в том, что они не обеспечили должную защиту данных своих пользователей. В результате этого произошла утечка личной информации, которая была использована мошенниками. Мы считаем, что они должны нести полную ответственность за это. Пользователи доверяли свои данные этим сервисам, а они не смогли их защитить. Кроме того, этот случай привел к случаям фишинга и кибербуллинга, что нанесло огромный ущерб пострадавшим.

Предположительные действия учащихся (как обвинитель):

— Обвинители могут обращаться к конкретным фактам (например, случаям утечек данных), приводить примеры из реальной жизни (известные случаи мошенничества, утечек данных и т.д.), анализировать последствия.
— Учащиеся в роли обвинителей используют яркие и убедительные примеры.

Роль защиты (2-3 человека): Уважаемый суд, мы понимаем, что ситуация с утечкой данных действительно трагична, однако мы уверены, что компания приложила все усилия для обеспечения безопасности. Мы установили многоуровневую защиту данных и старались не допустить утечек. Но иногда даже самые защищенные системы могут быть взломаны. Мы считаем, что ответственность за произошедшее лежит не только на нас, но и на самих пользователях, которые не соблюдали элементарные меры безопасности, такие как использование сложных паролей.

Предположительные действия учащихся (как защита):

— Защита может привести контраргументы о том, что компания сделала все возможное, ссылаясь на политику безопасности, процедуры шифрования и защиту данных.

— Они могут попытаться оправдать действия компании, объяснив, что не всегда можно предотвратить все угрозы.

Роль свидетелей (3-4 человека):Я был одним из пользователей этой социальной сети. Когда произошла утечка данных, мне начали приходить странные письма, которые я сначала проигнорировал. Но потом мне взломали аккаунт. Мне пришлось потратить много времени на восстановление своих данных, а также я стал жертвой фишинга.

Предположительные действия учащихся (как свидетели):
— Свидетели будут рассказывать о своем опыте, как это повлияло на их личную безопасность, приводя реальные примеры из жизни.
— Они будут делиться личными переживаниями, подчеркивая важность защиты данных и ответственность как пользователей, так и платформы.

Ведущий: Теперь, когда все стороны выслушаны, давайте обратимся к присяжным. На основе представленных аргументов, вы должны принять решение, кто несет ответственность в этой ситуации и какие меры нужно принять для улучшения безопасности в интернете.

Предположительные действия учащихся:

— Присяжные начинают обсуждать между собой, анализируя аргументы сторон, пытаются прийти к объективному выводу.

— Они могут задавать вопросы участникам игры, чтобы уточнить детали, а затем голосуют за решение.

Заключительный этап и рефлексия (10-15 минут)

Цель: Подвести итоги игры, обсудить результаты, укрепить усвоенные знания и навыки, а также дать возможность участникам осознать важность интернет-безопасности и свою ответственность за действия в сети.

Ведущий: Спасибо всем за активное участие в сегодняшней ролевой игре. Мы рассмотрели много важных вопросов, связанных с интернет-безопасностью: утечка данных, кибербуллинг, фишинг и ответственность разных сторон. Важно понимать, что интернет — это не просто место для общения или развлечений, это пространство, где важно соблюдать правила безопасности и понимать, что каждое наше действие может иметь последствия.

Ведущий: Итак, давайте еще раз подведем итоги. В чем заключается наша ответственность за безопасность в Интернете? Кто-то из вас может поделиться выводами, которые он сделал в процессе игры (ответы обучающихся).

Ведущий: Присяжные, ваше мнение очень важно. Вы принимали решение, кто должен нести ответственность за произошедшее. Как вы считаете, какая мера будет наиболее эффективной для повышения безопасности в интернете? Что мы можем сделать для предотвращения подобных инцидентов? (ответы обучающихся)

Рефлексия (5-7 минут)

Ведущий: Теперь, когда мы подведем итоги, давайте немного подумаем о том, что мы узнали и как это может быть полезно в повседневной жизни. Каждый из вас должен быть осведомлен о рисках в Интернете и знать, как защищать себя. Поделитесь, пожалуйста, своими мыслями.(ответы обучающихся)

Ведущий: Что же, ребята, на основании того, что мы сегодня обсудили, давайте выделим несколько важных принципов, которые помогут нам быть безопасными в Интернете. Вот что важно помнить:

1. Не раскрывайте свои личные данные: Пароли, номера карт, личную информацию нужно хранить в безопасности.
2. Проверяйте сайты и приложения: Прежде чем что-то покупать или вводить свои данные, убедитесь, что сайт защищен (обратите внимание на ‘https’ в адресной строке).
3. Используйте сложные пароли и двухфакторную аутентификацию: Это поможет вам защитить свои аккаунты от взлома.
4. Не доверяйте подозрительным письмам и сообщениям: Мошенники могут пытаться обмануть вас через фальшивые сообщения.

Это очень важно, чтобы каждый из нас понимал свою роль в обеспечении безопасности в интернете."

Ведущий: Спасибо всем за участие и активность! Сегодня мы много узнали и разобрались в важной теме интернет-безопасности. Я уверен, что теперь вы будете еще более внимательны и осторожны в сети. На этом урок завершен. Если у вас возникнут дополнительные вопросы или вы захотите узнать больше о безопасности в интернете, всегда можно обратиться за помощью.

Игра по станциям «КиберБОБЕР»

Цель Игры: привлечение внимания обучающихся ВСГО к вопросам безопасного и этичного использования сети Интернет; пропаганда в детской и подростковой аудитории позитивного контента Интернета, способствующего их образованию и развитию.

Задачи Игры:

- сформировать навыки ответственного и безопасного поведения в современной информационно-телекоммуникационной среде;

– расширить знания о киберугрозах среди обучающихся и оценки таких рисков;

- развить критическое и логическое мышление обучающихся.

Возраст участников – 12-14 лет.

Материально-технические средства:

1. **Технические средства:**
   - Компьютеры или планшеты (для доступа к Интернету и демонстрации материалов).
   - Мобильные телефоны (для записи видеороликов, если есть возможность).
   - Проекторы или экраны для отображения инструкций, видеоматериалов и презентаций.
   - Микрофоны (для ведущего и команд).
   - Динамики или звуковая система для фанфар, музыки и голосового сопровождения.
2. **Печатные материалы:**
   - Маршрутные листы для каждой команды, с указанием станций и баллов.
   - Карточки с терминами для станции «Компьютерный крокодил».
   - Стикеры для станции «Суд над Интернетом» (с маркерами для написания).
   - Инструкции по заданиям для каждой станции (раздаточные материалы).
   - Шаблоны для доски правил сетевого этикета.
   - Карточки с ситуационными задачами для станции «Все в онлайне».
   - Карточки с симптомами Интернет-зависимости для станции «Здоровье.com».
3. **Аудио и видеоматериалы:**
   - Фоновые аудиотреки (торжественная музыка, фанфары).
   - Видеоролик (примерный видеоролик на тему «Советы безопасного Интернета» для демонстрации на станции «Я всегда с собой беру»).
4. **Игровые атрибуты:**
   - **Р**еквизит для съемки проморолика (например, плакаты или аксессуары, которые помогут подчеркнуть тему безопасности в Интернете).
   - Интерактивные доски или флипчарты для станции «Сетевой этикет», где команды смогут создать доску с правилами.
   - Набор для сортировки симптомов Интернет-зависимости (картинки или карточки для визуального разделения симптомов по категориям).
   - Таймер для ограничения времени выполнения заданий (например, на станции «Компьютерный крокодил»).

Планируемые результаты:

1. Формирование ответственного отношения к использованию Интернета Участники игры поймут важность безопасного и этичного поведения в сети, научатся осознавать возможные риски и угрозы, а также научатся применять знания для защиты себя и других в онлайн-среде.
2. Расширение знаний о киберугрозах. В ходе игры участники получат информацию о различных типах киберугроз, таких как кибербуллинг, мошенничество,

вирусы, а также научатся оценивать риски, с которыми могут столкнуться пользователи Интернета.

3. Развитие навыков критического и логического мышления. В ходе выполнения заданий участники развивают умение анализировать ситуации, оценивать риски и находить оптимальные решения в различных интернет-ситуациях. Это также способствует развитию навыков критического и логического мышления.

4. Освоение правил сетевого этикета. Участники изучат основные правила поведения в Интернете, научатся создавать положительный имидж в сети и соблюдать этические нормы общения и взаимодействия в онлайн-среде.

5. Развитие творческих и командных навыков. Участники игры научатся работать в командах, что способствует развитию навыков совместной работы, обсуждения решений и креативного подхода к выполнению заданий (например, создание видеороликов или составление доски правил).

6. Повышение осведомленности о проблемах Интернет-зависимости. Через задания, связанные с симптомами Интернет-зависимости, участники получат более полное представление о возможных негативных последствиях чрезмерного использования Интернета и научатся распознавать симптомы зависимости.

7. Укрепление умения применять полученные знания на практике. В процессе выполнения различных заданий участники смогут применить полученные теоретические знания на практике, что позволит им стать более уверенными пользователями Интернета.

Ход Игры

1. Введение (5-7 минут)

Фанфары, торжественная музыка.

Ведущий: Добрый день! Я рада приветствовать вас на нашем увлекательном уроке-игре «В сети с умом», посвященном безопасному и этичному использованию Интернета! Сегодня мы будем говорить о том, как важно соблюдать безопасность в сети, защищать себя от киберугроз и, конечно же, как использовать Интернет для обучения и развития.

Для начала, поднимите руки, у кого есть компьютер или телефон? А у кого есть доступ в Интернет? А теперь – у кого есть страничка в социальных сетях? О, как много нас, кто использует Интернет!

Но знаете ли вы, с какими угрозами можно столкнуться в сети? Как избежать кибербуллинга, взлома аккаунтов или попасть в ловушку Интернет-мошенников? Сегодня на эти и многие другие вопросы мы будем отвечать в ходе нашей игры.

Перед началом игры предлагаю Вам поделиться на команды. Для этого каждый из вас получит жетон определенного цвета, после чего Вам необходимо сгруппироваться по группам по определенному цвету.

Наша игра будет проходить в формате игры по станциям. У каждого задания есть свои правила, а также баллы, которые вы будете зарабатывать. Чем лучше и точнее выполните задания – тем больше баллов получите.

Наша игра не на скорость, а на качество выполнения, так что не торопитесь, думайте и обсуждайте все вопросы!

Итак, давайте познакомимся с нашими командами! *Представление команд.*

Теперь, когда все команды готовы, перейдем к игровому процессу. Вы получите маршрутные листы, которые покажут вам, в какой последовательности проходить станции (Приложение 4). На каждой станции будут станционные распорядители, которые расскажут о задании и помогут вам.

2. Прохождение станций (40-50 минут)

Каждая команда начинает на своей станции, потом перемещается на другую станцию по мере выполнения задания.

Станция 1: «Суд над Интернетом» (10 минут)

Задание: Участникам нужно отобразить преимущества и недостатки использования Интернета на стикерах, создав чашу весов. Затем обсудить, что преобладает: положительные или отрицательные стороны.

Оценка: За подробность и полноту ответа – максимум 10 баллов.

Станция 2: «Компьютерный крокодил» (10 минут)

Задание: Капитан команды получает карточки с терминами по Интернет-безопасности и должен описать их своей команде за 3 минуты, не используя слова на карточке. Команда должна угадать как можно больше терминов.

Оценка: Чем больше угаданных терминов, тем больше баллов – максимум 20 баллов.

Станция 3: «Я всегда с собой беру» (10 минут)

Задание: Команды должны снять 30-секундный видеоролик на тему «Советы безопасного Интернета». Видеоролик оценивается по оригинальности и креативности.

Оценка: Максимум 10 баллов.

Станция 4: «Все в онлайне» (10 минут)

Задание: Команды получают ситуационные задачи, в которых нужно правильно выбрать ответ на вопросы о безопасности в Интернете (Приложение 2). За каждый правильный ответ дается 2 балла.

Оценка: Каждый правильный ответ – 2 балла.

Станция 5: «Сетевой этикет» (10 минут)

Задание: Команды составляют доску правил сетевого этикета и в творческой форме представляют их остальным участникам.

Оценка: Полнота ответа и оригинальность презентации – максимум 10 баллов.

Станция 6: «Здоровье.com» (10 минут)

Задание: Команды должны отсортировать симптомы Интернет-зависимости по категориям: психологические симптомы, физические симптомы и предвестники зависимости (Приложение 3).

Оценка: За правильную сортировку и точность – максимум 10 баллов.

3. Завершение игры (5-7 минут)

Фанфары, торжественная музыка.

Ведущий: Дорогие участники, мы подошли к концу нашей игры! Большое спасибо всем за активное участие, за ваши идеи и креативные подходы к заданиям! Ваши результаты будут сейчас подсчитаны, и мы вскоре объявим победителей! (*подсчитывает баллы).*

Ведущий: А теперь, внимание! Мы готовы объявить результаты игры!

Объявление победителей.

Ведущий: Поздравляем победителей! Но хочу отметить, что каждый из вас проделал огромную работу, узнал много нового и, главное, стал более осведомленным в вопросах безопасного и этичного поведения в Интернете.

Помните, что Интернет – это мощный инструмент для обучения и общения, но важно уметь пользоваться им ответственно и безопасно. Будьте грамотными и осознанными пользователями сети!

Благодарим всех за участие! Будьте Интернет-грамотными! До новых встреч!

Приложение к конспекту

Станция «Компьютерный крокодил»

Кибербуллинг
Троллинг
Фишинг
Сетевой этикет
Вирусы
Персональные данные
Пароль
Хакер
Червь
Конфиденциальность
Профиль
Авторизация
Опасные группы
Антивирусная программа
Браузер
Геймерство
Нежелательный
контент
Интернет-зависимость
Неконтролируемые покупки
Социальные сети

Станция «Все в онлайне»

Ситуация 1. В социальной сети твой виртуальный «друг» просит подробно рассказать о себе, где живёшь, кем работают твои родители, есть ли у тебя айфон и т.п. Как ты поступишь?

Ситуация 2. В одном из Интернет-магазинов вы увидели, что смартфон, о котором вы давно мечтали, и у вас есть для этого некоторая сумма денег, продается очень дешево. Каковы ваши действия?

Ситуация 3. Вы находитесь в транспорте, кругом много пассажиров, есть бесплатный Wi-Fi. Каковы Ваши действия?

Ситуация 4. На вашем компьютере установлено противовирусное ПО. Друг просит побыстрее скачать ему на флешку некоторые файлы. Каковы Ваши действия?

Ситуация 5. Ваш приятель посоветовал вам скачать понравившийся фильм через торрент. Как вы поступите?

Ситуация 6. Представьте, что Вы на протяжении месяца общаетесь с незнакомцем в социальных сетях. Он пригласил Вас на встречу. Ваши действия.

Станция «Здоровье.com»

Мы с Вами все являемся пользователями Интернета. но не многие из Вас знают, как понять Интернет-зависимый человек или нет. Давайте узнаем, по каким признакам распознать Интернет-зависимого человека! Вам необходимо распределить симптомы интернет зависимости по 3 категориям:

- Психологически симптомы Интернет-зависимости;
- Физические симптомы Интернет-зависимости;
- Предвестники Интернет-зависимости;

Психологические:

- возникновение проблем с учебой;
- пренебрежение семьей, друзьями, близкими
- отсутствие контроля за временем
- потеря интереса к окружающему миру;
- хорошее самочувствие или эйфория за компьютером;
- резкие перепады настроения;
-ощущения скуки, пустоты, раздражения при нахождении вне сети

Предвестники интернет-зависимости:

• навязчивое стремление постоянно проверять электронную почту;
• предвкушение следующего сеанса онлайн;
• увеличение времени, проводимого онлайн;
• увеличение количества денег, расходуемых на Интернет.

Физические:

- онемение пальцев, атрофия мышц кисти, связанные с длительным напряжением руки
- сухость слизистых глаз с угнетением мигательного рефлекса
- головные боли, головокружение
- ощущения дискомфорта в спине, шеи, кисти
- нарушение образа питания
- пренебрежение гигиеническим содержанием тела
- ухудшение качества сна и процесса засыпания
- изменение режима отдыха и бодрствования

Возникновение проблем с учебой	**Пренебрежение семьей, друзьями, близкими**
Отсутствие контроля над временем	**Потеря интереса к окружающему миру**
Хорошее самочувствие или эйфория за компьютером	**Резкие перепады настроения**
Ощущения скуки, пустоты, раздражения при нахождении вне сети	**Навязчивое стремление постоянно проверять электронную почту**
Предвкушение следующего сеанса онлайн	**Увеличение времени, проводимого онлайн**

Увеличение количества денег, расходуемых на Интернет	**Онемение пальцев, атрофия мышц кисти, связанные с длительным напряжением руки**
Сухость слизистых глаз	**Головные боли, головокружение**
Ощущения дискомфорта в спине, шеи, кисти	**Нарушение образа питания**
Пренебрежение гигиеническим содержанием тела	**Ухудшение качества сна и процесса засыпания**
Изменение режима отдыха и бодрствования	

Психологические симптомы
Физические симптомы
Предвестники Интернет-зависимости

Маршрутные листы

Команда _____

№	Название станции	Баллы
1.	«Суд над Интернетом»	
2.	«Компьютерный крокодил»	
3.	«Я всегда с собой беру»	
4.	«Всегда в ONLINE»	
5.	«Сетевой этикет»	
6.	«Здоровье.com»	

Команда _____

№	Название станции	Баллы
1.	«Компьютерный крокодил»	
2.	«Я всегда с собой беру»	
3.	«Всегда в ONLINE»	
4.	«Сетевой этикет»	
5.	«Здоровье.com»	
6.	«Суд над Интернетом»	

Команда _____

№	Название станции	Баллы
1.	«Я всегда с собой беру»	
2.	«Всегда в ONLINE»	
3.	«Сетевой этикет»	
4.	«Здоровье.com»	
5.	«Суд над Интернетом»	
6.	«Компьютерный крокодил»	

Команда _____

№	Название станции	Баллы
1.	«Всегда в ONLINE»	
2.	«Сетевой этикет»	
3.	«Здоровье.com»	
4.	«Суд над Интернетом»	
5.	«Компьютерный крокодил»	
6.	«Я всегда с собой беру»	

Команда _____

№	Название станции	Баллы
1.	«Сетевой этикет»	
2.	«Здоровье.com»	
3.	«Суд над Интернетом»	
4.	«Компьютерный крокодил»	
5.	«Я всегда с собой беру»	
6.	«Всегда в ONLINE»	

Команда _____

№	Название станции	Баллы
1.	«Здоровье.com»	
2.	«Суд над Интернетом»	
3.	«Компьютерный крокодил»	
4.	«Я всегда с собой беру»	
5.	«Всегда в ONLINE»	
6.	«Сетевой этикет»	

Онлайн – олимпиада «БЕЗопасный Интернет»

Интернет стал частью нашей жизни. Компьютер широко используется не только на рабочем месте, но и в быту, дома, на отдыхе. Это общемировая тенденция, и наша страна не является здесь исключением. Число пользователей Интернета в России стремительно растёт, доля молодёжи и совсем юной аудитории среди пользователей Всемирной паутины очень велика. Результаты исследования показывают, что Россия входит в зону повышенного интернет-риска для детей: возраст пользователей снижается, контроль со стороны родителей минимален, а рискованные формы общения в Рунете очень распространены. В связи с этим образовательная среда должна быть направлена на формирование у обучающихся навыков грамотного и ответственного поведения в сети «Интернет».

Онлайн-олимпиада по **профилактике Интернет-безопасности «БЕЗопасный Интернет!»** направлена на привлечение внимания обучающихся к вопросам безопасного и этичного использования сети Интернет.

2.2 **Задачи Олимпиады:**

- сформировать навыки ответственного и безопасного поведения в современной информационно-телекоммуникационной среде;
- расширить знания об Интернет-угрозах среди обучающихся и оценки таких рисков;
- выработать необходимость использования в сети общепринятых нравственных норм поведения.

Онлайн – олимпиада проводилась на платформе «Google – формы», ссылка на прохождение олимпиады –

8-10 лет -https://docs.google.com/forms/d/e/1FAIpQLSe9l7ndqsRuGO4hozhRxQ0vcZo-zDVuCRGan8MU7_dj_xJ4bA/viewform?usp=sf_link

11-13 лет – https://docs.google.com/forms/d/e/1FAIpQLSdXtLvlEyLuW82tG2M0LYEOvy6I8TKMZ5ZFeoyNTh2vlZ6GLQ/viewform?usp=sf_link

Онлайн – интеркатив «Угрозам.NET»

Данное мероприятие проходит в формате активного обучения в онлайн формате. Онлайн - интерактив **«Угрозам.NET»** проводился с целью формирования у обучающихся культуры безопасного и ответственного поведения в сети Интернет, развития навыков критического восприятия информации, защиты личных данных и уважительного отношения к другим пользователям виртуального пространства.

Онлайн – интерактив проводился на специальной платформе **learningapps.org,** в которую входило 5 упражнений, направленных на привлечение внимания к угрозам глобальной сети.

Ссылка для прохождения интерактива: https://learningapps.org/watch?v=p8udpxyuk25

Заключение

Интернет-безопасность обучающихся является одной из наиболее значимых проблем современного общества, что связано, прежде всего, с интенсивным развитием цифровых технологий, массовой доступностью сети Интернет и увеличением числа киберугроз, оказывающих деструктивное воздействие на личность ребёнка и подростка.

Среди всех негативных явлений, связанных с цифровой средой, особое место занимают кибербуллинг, интернет-мошенничество, распространение деструктивного контента, а также угрозы утечки персональных данных. Данные факторы представляют непосредственную опасность для психологического и социального благополучия обучающихся, создают риск нарушения прав и свобод личности, а также влияют на уровень безопасности общества в целом. Вследствие этого необходимым шагом становится системная профилактика киберугроз и формирование культуры ответственного поведения в сети у детей и подростков.

Говоря об опыте реализации профилактических мероприятий, можно сделать вывод: на федеральном уровне вопросы цифровой грамотности и интернет-безопасности закреплены в стратегических программах и нормативных документах, направленных на развитие информационного общества и защиту детей в цифровой среде («Цифровая экономика»). Так же созданы специализированные проекты и ресурсы («Урок цифры»), ориентированные на повышение цифровой культуры подрастающего поколения. На региональном уровне активно реализуются комплексные программы по обучению детей, родителей и педагогов безопасному и ответственному использованию информационно-коммуникационных технологий.

Проблема интернет-безопасности обучающихся ещё долгие годы будет оставаться актуальной в силу динамичного развития цифровой среды и появления новых угроз, однако реализуемая система профилактики на государственном и региональном уровнях создаёт предпосылки для формирования грамотной, ответственной и защищённой личности, способной эффективно использовать возможности Интернета и минимизировать связанные с ним риски.

Список литературы

1. Артамонова Е.Г., Бородина А.С., Методические рекомендации для несовершеннолетних, родителей (законных представителей) несовершеннолетних, наглядные информационные материалы по безопасному использованию сети «Интернет» в целях предотвращения преступлений, совершаемых с ее использованием, как самими несовершеннолетними, так и в отношении них. Методические рекомендации / Авторы-составители: Артамонова Е.Г., Бородина А.С., Мелентьева О.С. – М.: ФГБУ «Центр защиты прав и интересов детей», 2021 – 35 с.
2. Дёгтева Т. А, Методическое пособие Профилактика кибермоббинга и кибербуллинга в среде несовершеннолетних: методическое пособие / Т.А. Дёгтева и др. – Ставрополь: Ставропольское издательство «Параграф», 2017 г. – 81 с.
3. Методические рекомендации по проведению уроков безопасного Интернета в школах. – Лига безопасного Интернета, г. Москва, 2022 г.
4. Пережогин Л.О., Федонкина А.А. Интернет-зависимость: предпосылки формирования, клиническая картина, лечение и профилактика: Методические рекомендации. – М.: ФГБУ “НМИЦ ПН им. В.П. Сербского” Минздрава России, 2024. – 33 с
5. Сборник сценариев по профилактике Интернет-безопасности, ДЮЦ.

Интернет – ресурсы

Федеральный закон от 27.07.2006 №149-ФЗ (ред. от 24.06.2025) «Об информации, информационных технологиях и о защите информации».