ПРОСВЕЩЕНИЕ

ОСНОВАНО В 1930

Методические рекомендации
педагогу по организации и проведению
Всероссийского урока безопасности
по теме

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Рекомендовано для начального, основного
и среднего образования

Аннотация

Министерством просвещения Российской Федерации подготовлен календарь образовательных событий на 2021/2022 учебный год, приуроченных к государственным и национальным праздникам России, памятным датам и событиям российской истории и культуры. Именно этот календарь станет основой для проведения тематических классных часов, организации спецпроектов и поездок, проведения школьных и внеклассных мероприятий.

В течение всего 2021/2022 учебного года во всех образовательных организациях страны будут проводиться открытые уроки ОБЖ.

Мы понимаем, как важно приобщить ребят самого разного возраста к базовым национальным ценностям, как важно привить им правила грамотного поведения в Интернете, на улицах и дорогах, в школе и дома, как важно сформировать у детей понимание ценности человеческой жизни.

С целью реализовать все вышеуказанные задачи группой компаний «Просвещение» была запущена образовательная Всероссийская акция «УРОКБЕЗОПАСНОСТИ.РФ».

Методические рекомендации адресованы школьным учителям, педагогам дополнительного образования, заместителям директоров по воспитательной работе общеобразовательных учреждений. Все материалы могут быть использованы педагогами начальной и средней школы. Подойдут для организации работы в самых разных форматах: урочная деятельность, тематические проекты, уроки-дискуссии, классные часы и внеурочные занятия.

Методические материалы разработаны на основе учебных изданий АО «Издательство «Просвещение»

Содержание

Телевизор и компьютер — друзья или враги? 3

Киберугрозы и кибероопасности в Сети 5

Виды интернет-афер 8

Признаки негативного воздействия и правила информационной гигиены 11

Как защититься от кибераграссии, сомнительных знакомств, интернет-мошенничества и нежелательного контента? 13

Какие интернет-ресурсы могут быть доступны школьникам? 16

Как родителю помочь ребёнку создать хороший и безопасный аккаунт в социальных сетях? 18

Что делать, если… ? 20

Список литературы 22

Телевизор и компьютер — друзья или враги?

УЧЕБНЫЕ ВОПРОСЫ

1. Опасность телевизора и компьютера как приборов, излучающих электромагнитные волны.
2. Допустимое и правильное поведение при просмотре телепередач.
3. Правила безопасного обращения с компьютером.
4. Основы информационной безопасности.

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Обучающиеся должны понимать опасность телевизора и компьютера как приборов, излучающих электромагнитные волны; уметь определять разумные пределы пользования этими приборами; знать правила безопасного обращения с компьютером и основные правила по защите от вредной и опасной информации.

ОСНОВНЫЕ ТЕРМИНЫ И ПОНЯТИЯ

Телевизор / компьютер / планшет / смартфон / игровая приставка / наушники / электромагнитное излучение / информационная безопасность

СОДЕРЖАНИЕ УРОКА

Такие устройства, как телевизор, монитор компьютера, планшет, смартфон, наушники, и многие другие приборы являются источниками электромагнитного излучения и могут нанести вред здоровью глаз.

Телевизор может быть прекрасным помощником в обучении и приятным способом проведения досуга, но не следует забывать, что телевизор достаточно опасен, даже если находиться от него на расстоянии не меньше 1,5 м.

Электромагнитное излучение — распространяющееся в пространстве возмущение электромагнитного поля, влияет на биофизическое поле человека, вызывая нарушения в организме. Чтобы уменьшить вредное влияние телевизора на здоровье, следует дозировать количество времени, затрачиваемое на просмотр.

Чтобы избежать вредных последствий для здоровья, **нужно выполнять следующие правила:**

- размещать аппаратуру на безопасном для глаз расстоянии;
- во время перерывов в работе выполнять физические упражнения, стимулирующие кровообращение в мышцах спины, рук, шеи (какие именно, может порекомендовать учитель физкультуры), также очень важно выполнять зарядку для глаз;
- постоянно контролировать состояние своего здоровья, при появлении головных болей, головокружения, тошноты, при нарушении сна сказать об этом родителям.

Потребность в информации — одна из базовых потребностей человека. Главные информационные средства: телевидение, Интернет, радио. Они не только выполняют свои прямые функции по информированию населения, но и формируют вкусы, взгляды, привычки и даже сознание людей. Их воздействие на умы и сердца людей может приводить как к положительным, так и к отрицательным последствиям.

Для защиты детей от негативной информации **в 2010 г. в России принят Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию».** В этом законе сказано, что информационные материалы, оправдывающие насилие, агрессию, жестокость, противоправное поведение, содержащие пропаганду нездорового образа жизни, отрицающие семейные ценности, вызывающие страх, ужас и панику, являются опасными и вредными.

Основные правила информационной безопасности:

- критически относиться к информации в Сети, оценивать ее достоверность;
- уделять больше времени чтению книг, творчеству и саморазвитию;
- заполнять своё время не только компьютером и телевизором, но и живым общением, спортивными занятиями, помощью родителям, прогулками.

Важно! Вся информация, находящаяся в Интернете, доступна всем. Поэтому, прежде чем что-то разместить, надо хорошо подумать и посоветоваться со взрослыми.

Рекомендации при работе за компьютером

При работе на компьютере следует беречь глаза. Расстояние от глаз

до экрана монитора должно быть не менее 50 см. Из задней части монитора идёт максимальное излучение, поэтому она ни в коем случае не должна быть направлена на людей. Взрослым рекомендуется работать на компьютере не более 4 часов в день с перерывами через каждые 20–30 минут, а школьникам — не более 2 часов с 10-минутными перерывами через каждые 25 минут. Электромагнитное излучение от компьютера при невыполнении правил безопасности может способствовать развитию опухоли головного мозга и ухудшению зрения.

Киберугрозы и кибероопасности в Сети

УЧЕБНЫЕ ВОПРОСЫ

1. Основные киберугрозы.
2. Кибербуллинг и его формы.

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Обучающиеся должны знать о внешних и внутренних киберугрозах, иметь представление о том, что относят к внешним киберугрозам, понимать, насколько опасен кибербуллинг и его формы.

ОСНОВНЫЕ ТЕРМИНЫ

Вирусы / спам / фишинг / удалённый взлом компьютеров / кибербуллинг (анонимные угрозы) / преследование, использование личной информации (флейминг, хипплейпинг)

СОДЕРЖАНИЕ УРОКА

Информационные технологии всё больше проникают в общественные сферы, что вызывает значительный рост разного рода киберугроз и приводит к серьёзным изменениям в сознании миллиардов людей.

Риски, присущие цифровому пространству, можно разделить на две большие группы:

1. Электронные риски, или киберриски, угрожающие самому устройству, установленным на нём программам, банковским счетам, паролям.
2. Информационные риски, угрожающие сознанию владельца цифрового

устройства, фальшивые новости (фейк-ньюз), опасный контент.

К рискам для устройств относят: вредоносное программное обеспечение — программы, предназначенные для осуществления несанкционированного доступа к информации или ресурсам информационной системы и/или воздействия на них. Наиболее распространёнными видами вредоносных программ являются: вирусы (могут удалять как отдельные файлы, так и всю операционную систему, блокировать работу пользователей), троянские программы (проникают в компьютер под видом легального ПО, могут собирать данные банковских карт, нарушать работоспособность компьютера и даже использовать IP-адрес пользователя.

Вирусы скрытно проникают в компьютерные системы, и без эффективной защиты бороться с ними невозможно. Чтобы вирусы проникли в компьютер, достаточно всего лишь открыть вложение в электронном письме (при этом совершенно не обязательно, чтобы письмо было отправлено неизвестным адресатом, хорошо известный компаньон также может прислать вирус, если ранее его компьютер был заражён, или адрес отправителя может быть подделан). Некоторым вирусам достаточно уже того, что компьютер просто подключён к локальной сети, к которой подключён и **заражённый компьютер**.

Большую опасность представляет также **удалённый взлом компьютеров**, за счёт которого злоумышленники могут получать возможность читать и редактировать документы, хранящиеся на файл-серверах и в компьютерах, по собственному желанию уничтожать их, внедрять собственные программы, которые следят за всеми действиями конкурентов и собирают определённую информацию, вплоть до незаметного аудио- и видеонаблюдения через микрофоны ноутбуков и штатные веб-камеры.

Важно! Для распространения значительного числа вирусов используют съёмные накопители информации (флешки, мобильные жёсткие диски и оптические носители), поэтому требуется внимательно относиться к подобным носителям и не вставлять бездумно в свой компьютер, а в обязательном порядке тестировать антивирусной программой. А уж найденную где-то флешку нельзя включать вообще.

Злоумышленники могут пытаться не только заразить ваш компьютер или смартфон, но и подтолкнуть вас к тому, чтобы вы самостоятельно сообщили им конфиденциальные данные, которыми они могли бы воспользоваться для доступа к банковской карте (счёту) (вашей или кого-то из ваших близких). Для получения таких данных мошенники применяют методы социальной инженерии.

Социальная инженерия — приёмы, направленные на получение несанкционированного доступа к конфиденциальной информации и основанные на знании особенностей психологии людей.

Спам — массовая рассылка не запрошенных пользователем электронных писем и сообщений в мессенджерах. Как правило, спам-сообщения носят рекламный или агитационный характер. Спам может нанести вред компьютеру и причинить неудобства его пользователю, так как на очистку почтового ящика уходит значительное количество времени, а открытие некоторых сообщений может повлечь за собой установку вредоносного ПО.

Фишинг (в переводе с английского дословно означает «выуживание») — рассылка писем от имени известных фирм или крупных организаций с целью получения доступа к конфиденциальным данным (логин, пароль) пользователя Сети.

Одной из самых распространённых угроз, связанных с общением в Сети, является **кибербуллинг.** Это форма запугивания, насилия и травли детей с помощью телефонов и Интернета. Кибербуллинг опасен не меньше, чем издевательства в привычном понимании, ведь жертва кибербуллинга находится в большом психологическом напряжении, и не каждый ребёнок сможет его вынести самостоятельно.

Кибербуллинг включает в себя:

- анонимные угрозы — пересылка писем без подписи отправителя, содержащих угрозы, оскорбления, часто с использованием ненормативной лексики;
- преследование — рассылка неприятных писем своей жертве продолжительное время, которая в дальнейшем может вылиться в шантаж какими-либо фактами её жизни;
- использование личной информации — взлом электронной почты или страниц в социальных сетях для получения личной информации для шантажа или издевательств;
- флейминг — обмен эмоциональными репликами между агрессором (иногда их может быть несколько) и жертвой с целью получения удовольствия от нанесения оскорблений;
- хипплейпинг — видеозаписи с издевательствами, которые «заливают» на ресурсы, где их сможет увидеть большое количество пользователей. Такие ролики, естественно, «заливаются» без согласия потенциальной жертвы.

Источник: Региональная общественная организация «Центр интернет-технологий» (РОЦИТ).

Виды интернет-афер

УЧЕБНЫЕ ВОПРОСЫ

1. Схема действий кибермошенников.
2. Самые распространённые виды интернет-афер.

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Обучающиеся узнают схему работы кибермошенников, основные виды интернет-афер и как не стать жертвой кибермошенников.

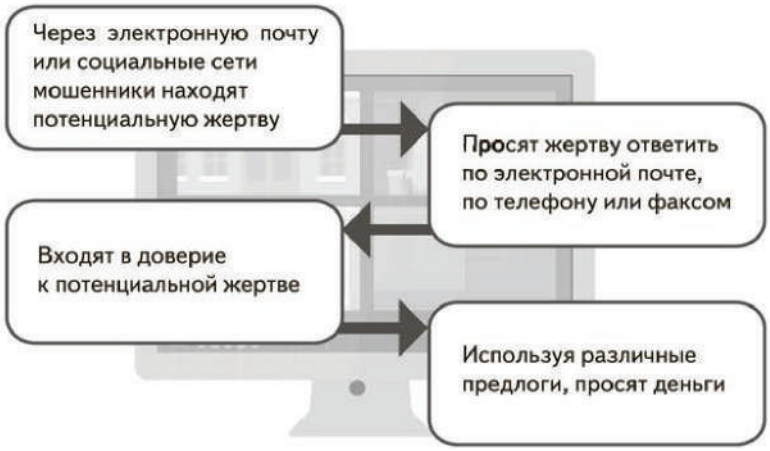
ОСНОВНЫЕ ТЕРМИНЫ

«Нигерийская афера» / «лотерея» / «подружка» / «приглашение на работу» / «личные страницы» / «компенсация» / «ошибка»

СОДЕРЖАНИЕ УРОКА

Интернет-аферы основаны на доверии и имеют самое широкое

распространение. Их цель — выманивание денег у пользователей. В большинстве случаев мошенники действуют по одной схеме, приведённой ниже.



Самые распространённые виды интернет-афер

«Нигерийская афера». Обычно пользователю приходит электронное письмо от незнакомца, которому срочно нужно перевести большую сумму денег из одной страны в другую (например, из Нигерии, отсюда и название). Жертве обещают немалое вознаграждение за помощь в переводе денег. Однако сначала просят перевести определённую сумму, чтобы оплатить банковские расходы, а как только перевод денег состоялся, мошенник исчезает.

«Лотерея». Пользователь получает письмо по электронной почте, в котором сообщается, что он выиграл в лотерею и что для получения выигрыша ему необходимо прислать свои данные. Жертву просят перечислить определенную сумму денег, чтобы покрыть банковские и другие расходы. После перечисления денег мошенник исчезает.

«Подружка». На электронную почту пользователя приходит письмо с просьбой о знакомстве. Часто во вложении имеется фотография красивой девушки. В письме говорится, что она мечтает побывать в вашей стране и встретиться с вами, так как влюбилась с первого взгляда. Она хочет приехать незамедлительно, но в последний момент возникают какие-то проблемы, и ей необходимы деньги. Неудивительно, что после перевода названной суммы исчезают не только деньги, но и девушка.

«Приглашение на работу». Жертва получает письмо с приглашением на работу от иностранной компании, которая ищет финансовых агентов в её стране. Работа предельно проста, её можно выполнять, не выходя из дома, и при этом зарабатывать намного больше, чем сейчас. Если жертва

соглашается с данным предложением, её просят прислать банковские реквизиты. Деньги перечисляют на счёт жертвы, а потом просят снять деньги со счёта и переслать их через систему перевода. Так **жертва** становится «переходным звеном» в цепочке мошенников, а когда дело попадает в полицию, жертва превращается в соучастника. В отличие от афер другого типа, в этом случае жертва даже не подозревает о том, что совершает преступление.

«Личные страницы». Мошенники похищают данные для входа на личные страницы, затем меняют логин, чтобы у хозяина страницы больше не было возможности пользоваться своим аккаунтом. Далее преступники отправляют с этой страницы всем контактам сообщения, указывая, что владелец страницы сейчас в отпуске за границей, что его ограбили как раз перед возвращением домой.

«Компенсация». В электронном письме сообщается, что был создан специальный фонд для выплаты различных компенсаций и что адрес жертвы был в списке пострадавших.

«Ошибка». Этот тип мошенничества очень популярен. Мошенники выходят на контакт с жертвой, которая недавно размещала рекламу о продаже, например, дома, соглашаются купить дом и быстро высылают чек на определённую сумму, которая всегда «случайно» оказывается неверной (как ни странно, всегда больше, чем сумма, о которой договаривались). Жертву просят вернуть разницу. Позже оказывается, что чек недействителен, дом так и не продан, а переведённые жертвой **деньги потеряны**.

Жертвой **кибермошенников** может стать практически любой, у кого есть мобильный телефон, доступ в Интернет, банковская карта.
Для осуществления своей преступной деятельности кибермошенники используют как программные средства, так и технологии социальной инженерии.

Воспользовавшись ими, преступники могут завладеть персональными данными, похитить деньги с кредитной карты, баланса сотового телефона, при совершении покупок в интернет-магазинах или на торговых площадках в Интернете.

Чтобы не стать жертвами кибермошенников, вооружитесь вышеизложенной информацией и здравым смыслом. Относитесь внимательно и критично к поступающим сообщениям, звонкам, присылаемым ссылкам. Скачивайте программное обеспечение, файлы только из проверенных источников, используйте антивирусное программное обеспечение.

Признаки негативного воздействия и правила информационной гигиены

УЧЕБНЫЕ ВОПРОСЫ

1. Цель кибермошенничества.
2. Отличие официального сайта от мошеннического.
3. Правила информационной гигиены.

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Обучающиеся должны понимать, какую цель преследуют кибермошенники, уметь отличать официальный сайт от мошеннического, знать признаки того, что обижают в Сети.

ОСНОВНЫЕ ТЕРМИНЫ

Агрессия / буллинг / мошенничество / вымогательство

СОДЕРЖАНИЕ УРОКА

Чтобы избежать негативного воздействия, в первую очередь не следует оставаться с проблемами в Сети в одиночку, ведь виртуальная проблема несёт за собой реальные переживания.

Мошенники не отстают от хулиганов и также активно разворачивают свою деятельность в Сети. Зачастую жертвами кибермошенников становятся и дети. Целью кибермошенничества является причинение материального или другого ущерба путём похищения личной информации (номера банковских счетов, логинов и паролей, кодов, паспортных данных и др.).

Важно! Сайты, запрашивающие слишком много информации о пользователе при совершении покупок в Интернете (данные счетов, пароли, домашние адреса и номера телефонов), могут оказаться мошенническими.

Администратор или модератор сайта никогда не станет требовать полные данные счетов, пароли или ПИН-коды. Нужно знать об основных методах мошенничества, а также о том, как можно отличить официальный и надёжный сайт от мошеннического, советоваться с родителями при желании совершить покупку в Сети.

Совет! Лучшим вариантом будет взять процесс совершения покупки родителям на себя или сделать так, чтобы он шёл в их присутствии и под их контролем. Так они будут в курсе того, на что и как ребёнок тратит деньги, и смогут предостеречь его от киберпреступников.

Общаясь в цифровом пространстве, помните о том, что:

- вы находитесь в публичном пространстве, где следует соблюдать общепринятые правила поведения и общения (быть вежливым, корректным по отношению к собеседникам, проявлять уважительное к ним отношение и т. д.);
- за безобидными и даже привлекательными аватарами могут скрываться опасные люди (не вступайте в контакт с незнакомцами, поведение которых кажется вам подозрительным);
- мошенники могут завладеть аккаунтом ваших друзей (если вы получили от друга подозрительное сообщение, удостоверьтесь с помощью вопросов, что это действительно он);
- популярные блогеры и сетевые кумиры — обычные люди со своими слабостями и недостатками (не следует идеализировать их, относитесь критически к тому, что они пропагандируют, к чему призывают);
- виртуальные друзья не являются реальными (они могут быть интересными собеседниками, но вряд ли их личностные качества в полной мере проявятся в интернет-общении);
- очень важно соблюдать баланс между виртуальной и реальной жизнью (выходя в Интернет — по учёбе или для общения с приятелями, продолжайте заниматься спортом, искусством, наукой, ремёслами, читайте больше книг).

Находясь в цифровой среде, относитесь к размещённому в ней контенту критически: не вся информация полезна и безвредна. Избегайте просмотра запрещённого контента. Негативные последствия от получения информации такого рода могут проявиться не сразу, а для их преодоления может потребоваться помощь психологов и врачей.

Как защититься от киберагрессии, сомнительных знакомств, интернет-мошенничества и нежелательного контента?

УЧЕБНЫЕ ВОПРОСЫ

1. Способы родительского контроля в Сети.
2. Вопросы о поведении в Интернете, которые родители должны обсудить с детьми, и правила безопасности и общения.
3. Выбор и защита смартфона.

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Обучающиеся должны понимать, что существует родительский контроль за их действиями в Сети, усвоить правила безопасности и общения в интернет-пространстве. Родители должны знать, как выбрать смартфон и защитить его от киберугроз.

СОДЕРЖАНИЕ УРОКА

Интернет — прекрасное средство для обучения, отдыха, общения, но в нём есть не только полезная информация, существует также множество опасностей. Поэтому родители должны принимать меры по предотвращению негативного воздействия в Сети и рассказывать о правилах безопасности.

Создать отдельную учётную запись и ограничить права пользователя. Не должно быть возможности удалять и устанавливать программы без ведома родителей. Заходить в учётную запись родителей тоже нельзя.

Активировать функцию родительского контроля и включить безопасный поиск в браузере. Можно составить список разрешённых сайтов или заблокировать нежелательные. Лучше, чтобы не было допуска к интернет-аукционам, платёжным системам и онлайн-банкингу.

Установить специальный детский поисковик, например «Гогуль» или «Спутник.дети». Данные ресурсы безопасны и ориентированы именно на детскую аудиторию.

Важно! Оба этих способа имеют один недостаток — не всегда можно найти актуальную и важную информацию по своему запросу, поэтому не должно

быть категорического запрета на пользование обычными поисковыми системами. В этой ситуации важен постоянный контроль. Например, множество антивирусов сегодня имеют функцию родительского контроля, позволяющую наблюдать за действиями в Сети.

Поговорить с ребёнком и объяснить ему, что далеко не всему и не всем в Сети можно доверять. Нельзя публиковать онлайн домашний адрес, слишком много рассказывать о себе и своей семье, хвастаться дорогими гаджетами и игрушками.

За всё сказанное и сделанное в Интернете придётся отвечать. Все действия можно отследить, поэтому не стоит совершать необдуманных поступков. Важно делиться своими сомнениями с родителями, а если появляется что-то непонятное или неприятное, агрессия или повышенное внимание со стороны незнакомых, следует обратиться к ним за советом.

Нельзя скачивать файлы с подозрительных сайтов, из писем и сообщений неизвестных отправителей.

Научить использовать настройки конфиденциальности и посоветовать закрыть профили в социальных сетях, пусть они будут только для друзей. Не надо добавлять во френды всех подряд. Лучше всего, если это будут лично знакомые или хотя бы друзья друзей.

Научить не реагировать на киберагрессию. Хамство и троллинг в Интернете — признак скверного воспитания и неуверенности в себе. Если кто-то будет писать оскорбительные сообщения или угрожать, нужно рассказать родителям, а вот оппонента следует игнорировать. Отсутствие ответа будет лучшим наказанием для интернет-агрессора, и он скоро потеряет интерес.

Важно! Самый лучший способ — просто заблокировать обидчика (внести его в чёрный список) самостоятельно или с помощью модератора — пользователя форума или сайта, который следит за соблюдением правил ресурса, имеет право редактировать и удалять сообщения других пользователей и вносить их в чёрный список (банить).

Предупредить об опасностях. Ни в коем случае нельзя общаться с посторонними взрослыми людьми, особенно если они просят прислать фотографии или предлагают встретиться. Сразу же сообщать родителям, если такое произойдёт.

Рассказать о мошенниках. Администрация сервиса никогда не станет требовать конфиденциальную информацию: полные данные счетов, пароли или ПИН-коды. Знать об основных видах мошенничества и научиться отличать поддельные сайты.

При покупке онлайн предварительно посоветоваться с родителями. Хорошо, если будет подключена виртуальная карта с ежемесячно вносимой на неё суммой, которую можно тратить онлайн по своему усмотрению.

Научить правилам безопасности в Интернете. Не скачивать файлы с подозрительных сайтов, не открывать письма и сообщения от неизвестных отправителей. Никогда не отключать антивирусные программы. Выходить из своих аккаунтов, если пользовался чужим устройством.

При выборе смартфона не полагаться только на сенсорный экран. Лучше выбрать телефон, где функции приёма и сброса звонков и вызова меню продублированы кнопками. В устройстве должно быть достаточно памяти либо слот для SD, чтобы загрузить все необходимые приложения. Отдайте предпочтение модели с большим объёмом батареи и носите с собой зарядное устройство или дополнительный блок питания.

Защитить смартфон, сделав следующее:

- установить на устройство пароль и никому, кроме родителей, не сообщать его, даже лучшему другу;
- установить специальное приложение, которое поможет контролировать устройство удалённо, даже если его потеряют или украдут;
- скачивать приложения и игры можно только в официальных магазинах приложений: App Store, Google Play;
- завести специальную банковскую карту для ребенка, при этом родители будут иметь полный контроль.

Установить полезные приложения. Загрузите в смартфон карты, чтобы можно было определить своё местоположение, если потерялись. Научитесь прокладывать маршрут и ориентироваться.

Установить специальное приложение, которое поможет определять местоположение устройства. Поставьте несколько мессенджеров и научитесь передавать с их помощью фото и данные о геопозиции.

Какие интернет-ресурсы могут быть доступны школьникам?

УЧЕБНЫЕ ВОПРОСЫ:

1. Специальные средства защиты, которые применяют родители и дети в Интернете.
2. Интернет-ресурсы, доступные школьникам.
3. Правила, помогающие оградить пользователя от противоправного контента.
4. Опасности, с которыми сталкиваются в Сети.

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Обучающиеся должны знать о специальных средствах защиты в Сети, о том, какие интернет-ресурсы для них доступны, усвоить правила, чтобы оградить себя от противоправного контента, понимать, какие опасности существуют в Интернете.

СОДЕРЖАНИЕ УРОКА

Для защиты юных пользователей родители применяют специальные средства защиты, например, установка антивируса, просмотр истории браузера, фильтры родительского контроля.

Источник: Региональная общественная организация «Центр интернет-технологий» (РОЦИТ).

Как уже отмечалось, в вопросах безопасности детей в Интернете важное место занимают доверительные отношения с родителями. Любопытно, что родители сегодня переоценивают степень честности своих детей. Лишь 6% родителей считают, что не знают ничего о том, чем занимаются их дети в Интернете, а по словам детей, на деле их сразу 14%.

Чтобы оградить себя от противоправного контента (тексты, картинки, аудио, видеофайлы, ссылки на сторонние ресурсы), следует выполнять ряд несложных правил:

- сообщать о нахождении нежелательной информации родителям;
- осознавать, что не вся информация в Интернете достоверная, и поэтому советоваться с родителями по любому непонятному вопросу;
- рассказывать родителям о том, какие сайты посещали и какую информацию видели;
- понимать, что должны быть включены программы родительского контроля, которые оградят от нежелательного контента;
- не будет лишним вспомнить правила безопасности в Сети.

Важно! Помните, что чрезмерный контроль может усилить желание выйти за рамки дозволенного, поэтому доверительное и открытое общение зачастую гораздо эффективнее.

Весьма часто дети сталкиваются с опасностями в социальных сетях. 20% детей отметили, что им приходили сомнительные сообщения от незнакомцев. При этом 3 из 5 детей сообщают своим родителям о тех опасностях, которые встречаются им в Сети.

Всё чаще общению вживую дети предпочитают общение в социальных сетях. Более того, общение с друзьями в Интернете является самым популярным занятием. Очевидно, что переход общения в виртуальную сеть может оградить от некоторых опасностей, как, например, уличные драки, но не стоит думать, что общение в Сети абсолютно безопасно и не может причинить никакого морального и физического вреда.

Как родителю помочь ребёнку создать хороший и безопасный аккаунт в социальных сетях?

УЧЕБНЫЕ ВОПРОСЫ

1. Помощь родителей ребёнку в создании аккаунта.
2. Правила работы в социальных сетях.
3. Метаданные фотографий в Сети.

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Обучающиеся должны с помощью родителей уметь создавать хороший и безопасный аккаунт в социальных сетях, следовать правилам работы в соцсетях, знать, что такое метаданные фотографий.

СОДЕРЖАНИЕ УРОКА

Придумайте вместе хорошее имя для аккаунта, но не используйте одновременно имя, фамилию и дату рождения. Такой никнейм может раскрыть слишком много личной информации.

Помощь родителей в создании уникального безопасного пароля.

Как создать надёжный пароль?

Источник: Региональная общественная организация «Центр интернет-технологий» (РОЦИТ).

Помощь в определении с направленностью блога и выставлении правильных настроек приватности.

Совет школьнику по ведению блога/страницы!

Хочешь вести личный блог для семьи и друзей — сделай свой аккаунт закрытым и не позволяй подписываться на него тем, кому ты не доверяешь.

Хочешь вести тематический блог про красоту, архитектуру, еду, искусство и т. д. — сделай его открытым, чтобы максимальное количество людей могло подписаться на него. И в дальнейшем постарайся придерживаться выбранной тематики.

Можно рассказывать истории о себе, люди их очень любят. Но всегда необходимо оставлять недосказанность. Например, идёшь гулять — не рассказывай, куда пойдёшь, публикуй фотографии после прогулки. Идёшь на мероприятие — опубликуй фотографии по возвращении домой.

Чтобы иметь больше подписчиков, нужно иметь открытый аккаунт. В этом случае необходимо использовать правильные #хештеги.

Что значит «правильные #хештеги»?

- Хештеги должны быть не массовые (не #love #nature #Moscow), ваша классная фотография просто утонет в миллионе похожих в течение часа, и никто её не увидит.
- Хештеги не должны быть слишком редкими (#форумпобезопасности, #летнийфестиваль), такие хештеги используются только для конкретных мероприятий, и их увидят только люди, которые на этом мероприятии были.
- Где же найти правильные хештеги? Проще всего посмотреть, какие хештеги ставят популярные блогеры при схожей теме блога. Если они не сработали, посмотри хештеги в других аккаунтах.

Stories — очень популярный формат. Но даже в сториз не должно быть компрометирующей или личной информации, потому что любой человек может сделать её скриншот и переслать или сохранить её.

Фотографии в Сети

Фото содержит намного больше данных, чем вы думаете. На какое устройство снято фото, при каких настройках, какие координаты, дата и время, размер и формат файла, в какой операционной системе редактировались фотографии — всё это называется метаданные или exif-данные.

К счастью, социальные сети научились удалять лишнюю информацию с фотографий. Но вы можете сделать это сами, воспользовавшись любой программой для удаления метаданных с фотографии.

Советы!

- Запретите приложению «Камера» на телефоне доступ к геолокации.
- Выставляйте геолокацию в социальных сетях вручную.
- Не загружайте фотографии в виде документов.

Необходимо следить за тем, чтобы не подписывалось слишком много ботов. Для этого можно использовать специальные программы для оценки подписчиков, например **hypeauditor.com.**

Что делать, если… ?

УЧЕБНЫЕ ВОПРОСЫ

1. Порядок действий при взломе аккаунта.
2. Советы, как реагировать на троллинг. Как остановить кибербуллинг.
3. Работа горячей линии.

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Обучающиеся должны знать, что нужно делать, если взломали аккаунт; уметь противостоять троллингу, пресекать кибербуллинг; понимать, как работает горячая линия.

СОДЕРЖАНИЕ УРОКА

Источник: Региональная общественная организация «Центр интернет-технологий» (РОЦИТ).

Что делать, если в отношении вас начался троллинг?

- Самый главный совет любому юзеру в Интернете: «СЛЕДУЙТЕ ЭТИКЕТУ!» Если большинство юзеров будут следовать правилам хорошего тона на интернет-сайте, то на нём будет удобно общаться.
- Во-первых, не нарушать в ответ. Достойно ответить всегда можно, не выходя за рамки хорошего тона.
- Призвать хама к порядку. Без угроз и оскорблений.
- «Не кормить тролля». Если вы видите, что целью собеседника является травля, выведение вас из себя, лучше занести его в собственный «игнорлист».
- Если была опубликована крайне оскорбительная и унижающая информация, нужно обратиться к модератору с просьбой удалить ЭТО и принять меры к тому, кто ЭТО опубликовал. Стесняться не надо: модератор на то и модератор, чтобы наводить порядок.
- Если хам или тролль пользуется защитой модераторов — в той или иной форме, — то есть смысл просто покинуть такой ресурс. Своя репутация и нервы значительно дороже.
- Можно обратиться на горячую линию по борьбе с подобным контентом — это просто и анонимно. Только не надо посылать заведомо ложные сообщения. А если дело пахнет преступлением, то можно обратиться к родителям, чтобы уже они связались с правоохранительными органами.

Как остановить кибербуллинг?

1. Выйдите из своего аккаунта на сайте.
2. Внесите в чёрный список сообщения и их отправителя. Не отвечайте им.
3. Сохраните сообщения и покажите взрослым.

Важно! Горячая линия Рунета — это сервис защиты и информационной поддержки пользователей, куда можно сообщить о некачественном сервисе, противозаконных материалах и мошенничестве в Интернете.

СПИСОК ЛИТЕРАТУРЫ

Основы безопасности жизнедеятельности. 8–9 классы. В 2 частях. Под ред. Шойгу Ю. С. М.: Просвещение, 2021.

Основы безопасности жизнедеятельности. 5–9 классы. Хренников Б. О., Гололобов Н. В., Льняная Л. И., Маслов М. В./ под ред. С. Н. Егорова. М.: Просвещение, 2021.

Виноградова Н. Ф., Смирнов Д. В., Сидоренко Л. В., Таранин А. Б. **Основы безопасности жизнедеятельности**. **8–9 классы**: учебник. — М.: Вентана-Граф, 2021.

РЕКОМЕНДУЕМЫЕ РЕСУРСЫ

ФКУ «Центр экстренной психологической помощи МЧС России»
http://www.psi.mchs.gov.ru/

Федеральная служба безопасности Российской Федерации
http://www.fsb.ru/

Министерство внутренних дел Российской Федерации
https://мвд.рф

Министерство Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий
https://mchs.gov.ru

Центральный научно-исследовательский институт организации и информатизации здравоохранения Министерства здравоохранения Российской Федерации
https://mednet.ru

ЕДИНЫЙ РЕСУРС УЧЕБНО-МЕТОДИЧЕСКИХ МАТЕРИАЛОВ ПО ОБРАЗОВАНИЮ ДЛЯ УЧИТЕЛЕЙ, РОДИТЕЛЕЙ И ШКОЛЬНИКОВ

https://uchitel.club/