МЧС России

Департамент ГОЧСиПБ г. Москвы

УФСБ по г. Москве и Московской области

ГКУ ЦОДД

РОЦИТ

Корпорация «Российский учебник»

УЧЕБНЫЙ МАТЕРИАЛ
по теме
«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

РЕКОМЕНДОВАНО ДЛЯ
НАЧАЛЬНОГО, ОСНОВНОГО
И СРЕДНЕГО ОБЩЕГО ОБРАЗОВАНИЯ

Аннотация

Министерством просвещения Российской Федерации подготовлен календарь образовательных событий на 2019/2020 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.

Одной из важных дат этого учебного года станет акция **«Неделя безопасности»**, которая пройдёт с 2 по 8 сентября 2019 года во всех образовательных организациях страны.

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 Министерством Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий **(МЧС России)**, Департаментом по делам гражданской обороны, чрезвычайным ситуациям и пожарной безопасности города Москвы **(Департамент ГОЧСиПБ г. Москвы)**, Государственное казённое учреждение города Москвы - Центр организации дорожного движения Правительства Москвы **(ГКУ ЦОДД)**, Региональной общественной организацией «Центр интернет-технологий» **(РОЦИТ)** и корпорацией **«Российский учебник»** была запущена образо- вательная **Всероссийская акция «УРОКБЕЗОПАСНОСТИ. РФ»**.

Материалы включают в себя почти весь спектр важных вопросов безопасности жизнедеятельности при чрезвычайных ситуациях, Правил дорожного движения и безопасной работы с информационными и коммуникационными ресурсами сети Интернет.

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

В основе материалов лежат работы экспертов МЧС России, Департамента ГОЧСиПБ г. Москвы, ГКУ ЦОДД,РОЦИТ, а также авторов учебных изданий корпорации «Российский учебник».

Тестовые материалы разработаны автором методических пособий по БЖ и ОБЖ кандидатом педагогических наук, доцентом кафедры теории и методики адаптивной физической культуры Российского государственного университета физической культуры, спорта и туризма (ГЦОЛИФК) С.Н. Фалько.

СОДЕРЖАНИЕ

Телевизор и компьютер — друзья или враги?

Кто из нас не любит смотреть телевизионные передачи! Мы узнаём из них много интересного и нового для себя, расширяем свой кругозор, особенно если смотрим различные познавательные передачи. Хорошо посмотреть и интересный кинофильм, и спортивную передачу. Однако надо помнить, что нельзя сидеть перед телевизором часами. Дело в том, что в этом случае его электромагнитное излучение плохо скажется на здоровье, даже если находиться на рекомендуемом расстоянии от него (не ближе 1,5 м). Поэтому не стоит смотреть всё подряд, переключаясь с одного канала на другой в надежде найти что-нибудь интересное.

Многие дети охотно занимаются с компьютером. Это замечательно: навыки обращения с ним очень пригодятся в будущей работе. Но и тут надо помнить, что многочасовое сидение перед включённым компьютером, тоже излучающим вредные электромагнитные волны, опасно для здоровья, особенно девочек. Лучше использовать компьютер для приобретения новых знаний. Не стоит часами играть в компьютерные игры — можно попасть в зависимость от них, и тогда не обойтись без длительного лечения у психолога.

Чтобы избежать вредных последствий при работе на компьютере, нужно выполнять следующие правила:

- размещать аппаратуру и оборудовать рабочее место в соответствии с инструкцией, прилагаемой к компьютеру;
- во время перерывов в работе выполнять физические упражнения, стимулирующие кровообращение в мышцах спины, рук, шеи (какие именно, может порекомендовать учитель физкультуры);
- постоянно контролировать состояние своего здоровья, при появлении головных болей, головокружения, тошноты, при нарушении сна сказать об этом родителям.

Сегодня информационные средства, прежде всего телевидение, Интернет и радио, 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 не только к положительным, но и к отрицательным последствиям.

ВАЖНО! 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:

- оценивать и критически относиться к любой информации;
- для профилактики зависимости ограничивать время пребывания за компьютером и дозировать просмотр телепередач;
- освобождаться от негативной информации, вспоминая о чём-нибудь приятном, красивом и светлом;
- заполнять своё время не только компьютером и телевизором, но и живым общением, спортивными занятиями, помощью родителям, прогулками.

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

Киберугрозы и киберопасности в Сети

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

В результате исследований установлено, что 9 из 10 компаний регулярно сталкиваются с внешними киберугрозами. За 2016 г. 91% иностранных и 96% российских компаний, представители которых приняли участие в опросе, сталкивались с угрозами информационной безопасности. Было осуществлено большое количество кибератак, направленных на финансовые организации и приведших к огромным финансовым потерям, простоям в работе.

Ну что же тогда говорить о детях? Ведь Интернет — это кладезь информации для ребёнка, неисчерпаемый источник общения, бездонное море пользовательских приложений и в то же время бескрайние просторы для действий различных криминальных и полукриминальных личностей.

Основные виды киберугроз

В настоящее время все киберугрозы принято разделять на **внешние** и **внутренние**. Причины и источники внешних угроз находятся вне компьютеров компании, как правило в глобальной сети Интернет.

Внутренние угрозы зависят исключительно от персонала компании, программного обеспечения и оборудования.

К **внешним угрозам** относят:

- вирусы;
- спам;
- фишинг;
- удалённый взлом;
- кибербуллинг.

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). Некоторым вирусам достаточно уже того, что компьютер просто подключён к локальной сети, к которой подключён и заражённый компьютер.

ВАЖНО! Для распространения значительного числа вирусов используют съёмные накопители информации (флешки, мобильные жёсткие диски и оптические носители).

Спам не только вызывает раздражение у пользователей, но и забивает каналы связи, расходует трафик, отвлекает от работы, вынуждая людей искать важную корреспонденцию среди рекламы. В конечном счёте всё это приводит к финансовым потерям. Помимо этого, спам также является одним из распространённых каналов внедрения троянских программ и вирусов.

Фишинг, в отличие от спама, нацелен на узкие группы пользователей и содержит сообщения с социальным контекстом, призывающие потенциальную жертву открыть исполняемый файл или перейти на сайт, содержащий вредоносный код.

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.

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:

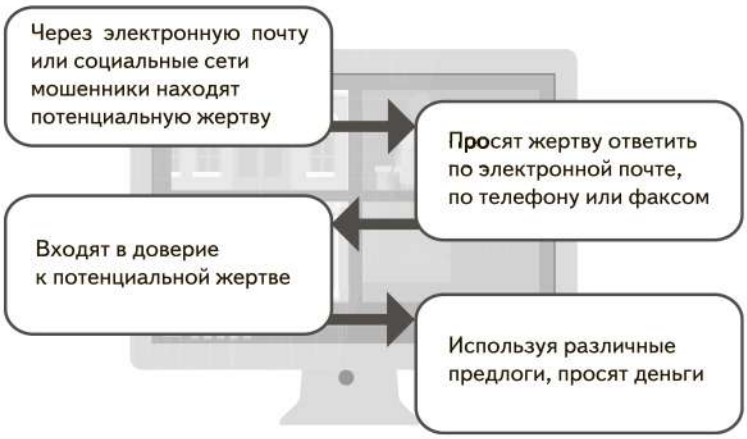
- анонимные угрозы — пересылка писем без подписи отправителя, содержащих угрозы, оскорбления, часто с использованием ненормативной лексики;
- преследование — рассылка неприятных писем своей жертве продолжительное время, которая в дальнейшем может вылиться в шантаж какими-либо фактами её жизни;

- 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

Сегодня существует некий рейтинг наиболее распространённых в Интернете афер за последние 5 лет. Эти 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.



«Нигерийская афера». Обычно пользователю приходит электронное письмо от незнакомца, которому срочно нужно перевести большую сумму денег из одной страны в другую (чаще всего 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 около 1000 долларов США, 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 компенсаций жертвам «нигерийской аферы» 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.

Признаки негативного воздействия

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 (номеров банковских счетов, логинов и паролей, кодов, паспортных данных и др.).

ВАЖНО! Объясните ребёнку, что сайты, запрашивающие слишком много информации о пользователе при совершении покупок в Интернете (данные счетов, пароли, домашние адреса и номера телефонов), могут оказаться

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 на себя, или сделать так, чтобы он шёл в вашем присутствии и под вашим контролем. Так вы будете в курсе того, на что и как ваш ребёнок тратит деньги, и сможете предостеречь его от киберпреступников.

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

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

Создайте отдельную учётную запись и ограничьте права пользователя. Пусть у ребёнка не будет возможности удалять и устанавливать программы без вашего ведома. Заходить в учётную запись родителей он тоже не должен.

Активируйте функцию родительского контроля и включите безопасный поиск в браузере. Можно составить список разрешённых сайтов или заблокировать нежелательные. Лучше не допускать ребёнка к интернет-аукционам, платёжным системам и онлайн-банкингу.

Установите специальный детский поисковик, например «Гогуль» или «Спутник.дети». Популярность этих ресурсов, несмотря на их безопасность и ориентированность именно на детскую аудиторию, сегодня крайне низкая. Ими пользуются лишь 2% опрошенных. Самыми востребованными браузерами среди детей являются Google Chrome (42%), «Яндекс.Браузер» (19%) и Safari (17%).

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.

Поговорите с ребёнком и объясните 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.

Предупредите, что за всё сказанное и сделанное в Интернете придётся отвечать. Все действия можно отследить, поэтому не стоит совершать необдуманных поступков. Постарайтесь установить доверительные отношения, чтобы ребёнок не боялся делиться с вами своими сомнениями. Скажите, что, если он увидит что-то непонятное или неприятное, столкнётся с агрессией или повышенным вниманием со стороны незнакомых, пусть приходит к вам за советом.

Поговорите об интересах и о том, какие сервисы и сайты можно посещать, а какие не стоит. Расскажите, что нельзя скачивать файлы с подозрительных сайтов, из писем и сообщений неизвестных отправителей.

Научите использовать настройки конфиденциальности и посоветуйте 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.

Научите не реагировать на киберагрессию. Спокойно и доходчиво объясните, что хамство и троллинг в Интернете — признак скверного воспитания и неуверенности в себе. Если кто-то будет писать ему оскорбительные сообщения или угрожать, пусть расскажет об этом вам, 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).

Предупредите об опасностях. Объясните, почему 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.

Расскажите о мошенниках. Объясните ребёнку, что администрация сервиса никогда не станет требовать конфиденциальную информацию: полные данные счетов, пароли или ПИН-коды. Расскажите об основных видах мошенничества и научите отличать поддельные сайты.

Если он захочет что-то купить онлайн, пусть предварительно посоветуется с вами. Подключите виртуальную карту и ежемесячно вносите на неё сумму, которую ребёнок может тратить онлайн по своему усмотрению.

Научите правилам безопасности в Интернете, расскажите, что нельзя скачивать файлы с подозрительных сайтов, открывать письма и сообщения от неизвестных отправителей. Попросите никогда не отключать антивирусные программы. Научите его выходить из своих аккаунтов, если он пользовался чужим устройством.

Выбирайте смартфон, который не привязан к сим-карте одного оператора. Не полагайтесь 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.

Защитите смартфон ребёнка, сделав следующее:

- установите на устройство пароль и попросите ребёнка никому не сообщать его, даже лучшему другу;
- установите специальное приложение, которое поможет контролировать устройство удалённо, даже если его потеряют или украдут;
- объясните, что скачивать приложения и игры можно только в официальных магазинах приложений: App Store, Google Play и Windows Market;
- подключите аккаунт ребёнка к своей банковской карте и настройте предварительное одобрение на покупку контента.

Установите полезные приложения. Загрузите в смартфон ребёнка карты, чтобы он мог определить своё местоположение, если потеряется. Научите прокладывать маршрут и ориентироваться. Убедитесь, что он запомнил домашний адрес.

Установите 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?

Для защиты юных пользователей родители применяют специальные средства защиты. В числе популярных — установка антивируса (65%), просмотр истории браузера (32%) и фильтры родительского контроля (30%). Дети стараются обезопасить себя в Сети самостоятельно, а не только надеясь на родительскую помощь: устанавливают антивирус (29%), не посещают сомнительные сайты (23%) и не переходят по незнакомым ссылкам (20%).

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%.

Для того чтобы оградить ребёнка от противоправного контента (тексты, картинки, аудио, видеофайлы, ссылки на сторонние ресурсы), следует сформировать ряд легко выполнимых правил:

- договоритесь, чтобы ребёнок сообщал о нахождении нежелательной информации;

- расскажите, что не вся информация в Интернете достоверная, и приучите его советоваться с вами по любому непонятному вопросу;
- расспрашивайте ребёнка о том, какие сайты он посещал и какую информацию видел;
- включите программы родительского контроля, чтобы оградить ребёнка от нежелательного контента;
- не будет лишним напоминание правил безопасности в Сети.

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

Около 80% детей когда-либо сталкивались с опасностями в Интернете. Причём самая распространённая угроза — это компьютерные вирусы. О ней заявила сразу четверть опрошенных. Также 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 (24% опрошенных). 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 помочь ребёнку создать хороший и безопасный аккаунт в социальных сетях?

1. Придумайте вместе хорошее имя для аккаунта, но не используйте одновременно имя, фамилию и дату рождения. Это не очень креативно, а ещё такой никнейм может раскрыть слишком много личной информации.

2. Помощь родителей в создании уникального безопасного пароля.

3. Помогите определиться ребёнку с направленностью его блога и выставьте правильные настройки приватности.

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

Совет школьнику!

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.

4. Объясните ребёнку, что 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.

5. Если ребёнок хочет иметь больше подписчиков и у него открытый аккаунт, расскажите ему, что 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, #летний- фестиваль), 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.

6. 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.

7. Объясните ребёнку, что необходимо следить за тем, чтобы на него не подписывалось слишком много ботов. Для этого можно использовать специальные программы для оценки подписчиков, например hypeauditor.com.

ПРАВИЛА РАБОТЫ В СОЦИАЛЬНЫХ СЕТЯХ

- Создать уникальный надежный пароль
- Не разглашать персональные данные
- Контролировать личную информацию
- Не осуществлять покупки в социальных сетях
- В случае покупки товара, не осуществлять предоплату

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

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.

Что делать, если … ?

Что делать, если аккаунт взломали?

1. Заблокируйте банковские карты
2. Поменяйте пароль на почте, к которой привязан ваш аккаунт
3. Обратитесь к службе поддержки социальной сети
4. Отправьте информацию по другим каналам коммуникаций вашим друзьям, чтобы они знали о взломе страницы и не стали жертвами мошенников

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 «игнор-лист».
- 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.

Как помочь жертвам

Дети и подростки, которые регулярно становятся жертвами оскорблений и угроз в сети, гораздо чаще склонны быть в депрессии и испытывать тревогу. В некоторых случаях дело доходит до суицида

- **Трансакционный анализ**

  Этот тип помощи представляет собой анализ старых психологических травм и сопоставление их с текущей ситуацией. Дети и взрослые, которые до сих пор цепляются за страх и чувства, которые они пережили из-за оскорблений и задирок, могут нуждаться в помощи с их преодолением, чтобы разобраться с настоящим

- **Научить стоять за себя**

  Люди подвергающиеся нападкам и оскорблениям часто нуждаются в помощи для приобретения уверенности в себе, чтобы противостоять обидчикам

- **Когнитивно-поведенческая терапия**

  Данная терапия эффективна при изменении поведения или мыслей человека, с целью добиться позитивных изменений в его повседневной жизни. Часто дети, которых обижают, развивают свои защитные поведенческие привычки ,чтобы справиться с депрессией и тревогой. Когнитивно-поведенческая терапия помогает им преодолеть это.

Как помочь обидчикам

Дети и взрослые, которые обижают других часто нуждаются в помощи со своей неуместной агрессией. В некоторых случаях, они сами переживают некую форму оскорблений от других обидчиков или члена семьи.

- **Управление гневом**

  Многие агрессивные люди просто не могут выражать свой гнев адекватным путем. Добраться до корня их гнева и научить их технике расслабления, вот что должно им помочь.

- **Психотерапия**

  Некоторые обидчики таким образом справляются со своими старыми или нынешними травмами. Психотерапия может помочь узнать откуда берутся эти гнев и обида.

- **Вмешательство**

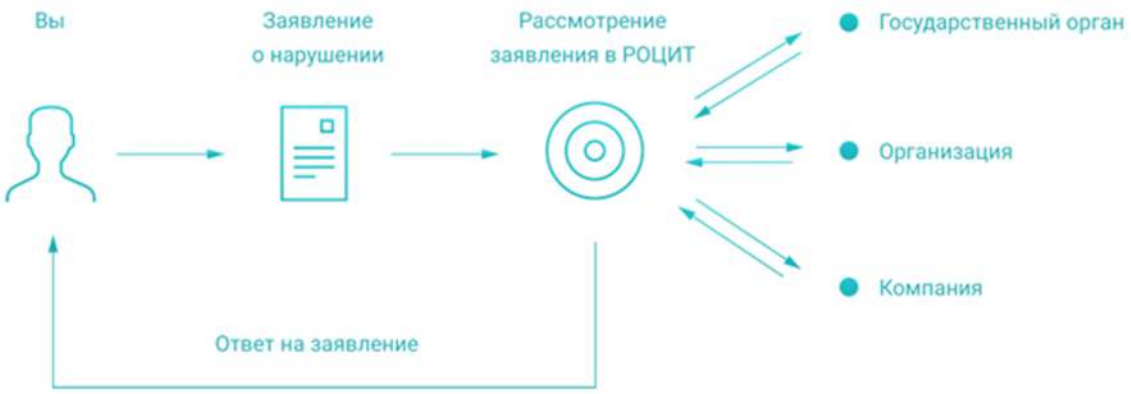
  Вмешательство в поведение обидчика чаще всего является самым эффективным способом объяснить им, какой урон они причиняют своими поступками. Иногда это включает в себя его семью или даже жертву.

Как работает горячая линия?

1. Заполните заявку на сайте РОЦИТ rocit.ru/hotline.

2. Приложите нужные ссылки и документы.

3. Специалисты горячей линии РОЦИТ проконсультируют вас и при необходимости свяжутся с профильными организациями и госорганами, которые могут решить проблему.



ВАЖНО! Горячая линия Центра экстренной психологической помощи МЧС России (Москва) +7 (495) 626-37-07, www.psi.mchs.gov.ru

Список литературы

Вангородский С.Н. Основы кибербезопасности. 5–11 классы: учебно-методическое пособие. – М.: ДРОФА, 2019.

Поляков В.В., Кузнецов М.И., Марков В.В., Латчук В.Н. Основы безопасности жизнедеятельности. 5 класс: учебник. – М.: ДРОФА, 2019.

Учебные материалы Региональной общественной организации «Центр интернет-технологий» (РОЦИТ), 1996–2019.