ФОНД
НАЦИОНАЛЬНЫЕ
РЕСУРСЫ
ОБРАЗОВАНИЯ

При поддержке

КОМИТЕТ
ОБЩЕСТВЕННЫХ СВЯЗЕЙ
И МОЛОДЁЖНОЙ ПОЛИТИКИ
ГОРОДА МОСКВЫ

ИНТЕРНЕТ-БЕЗОПАСНОСТЬ ДЕТЕЙ: МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

Разработаны в рамках проекта
«Безопасная интернет-среда — детям»

ОГЛАВЛЕНИЕ

Введение

За последние годы сеть Интернет вошла в нашу жизнь и стала важным современным источником информации и средством общения. Сегодняшние дети уже не представляют себе мир без смартфона и планшета, браузера и онлайн-игр. И так же, как мы учим малышей чистить зубы и правильно переходить дорогу, мы стараемся рассказывать им об основных правилах безопасного использования сети Интернет.

Сегодня, по данным Института развития Интернета, им пользуются 76% россиян. Растет и число школьников, ежедневно использующих социальные сети. Результаты мониторинга Фонда «Национальные ресурсы образования», проведенного среди 2 500 школьников от 13 до 18 лет в 84 регионах России, показывают, что 50% ребят заходят в социальные сети более девяти раз в день. Чаще всего школьники используют социальные сети для переписки с друзьями — 83%, для чтения постов и просмотра новостной ленты — 74%, для прослушивания музыки — 70%, для размещения фотографий — 26%.

Технический прогресс делает информацию все более доступной. В начале 2000-х годов одна музыкальная композиция могла скачиваться на жесткий диск в течение полутора часов. Сегодня мы за несколько минут загружаем на планшет целый сезон любимого телешоу, чтобы смотреть его по дороге на работу. И если раньше основными угрозами, которые таит в себе увлечение компьютером и Интернетом, взрослые считали нарушение зрения, осанки, развитие зависимости и нежелательный контент, то сегодня все чаще называются такие явления, как потеря конфиденциальности, кибербуллинг, фейк-ньюз, финансовое мошенничество. По данным индекса цифровой культуры Microsoft за 2018 год, Россия заняла 19-е место в мире из 22 возможных по уровню подверженности рискам — в 2018 году онлайн-рискам подверглись 74%

россиян. Второй год подряд самым распространенным стал риск нежелательной коммуникации (67%). Часто риски проявлялись в форме оскорблений и недостоверной информации в Сети. Две трети россиян сталкивались с оскорблениями, практически 40% — с недостоверной информацией и фейк-ньюз; каждый пятый пострадал от действий финансовых мошенников. Чаще всего источниками рисков в Сети становились незнакомые люди.

Этим рискам подвержены не только взрослые, но и подростки и даже дети младшего школьного возраста. В 2017 году в ходе опроса Фонда «Национальные ресурсы образования» о наличии в сети Интернет угроз для несовершеннолетних высказались 93% из 5 тысяч респондентов. По их мнению, подростки становятся жертвами мошеннических действий, сталкиваются с нежелательным для психологического развития содержанием, принимают за истину ложную информацию, а также порой неумышленно, по незнанию, сами совершают в сети противоправные действия.

Эти данные подтверждаются и статистикой МВД. Только за период с января по ноябрь 2018 года было зарегистрировано более 156 тысяч преступлений, совершенных с использованием компьютерных и телекоммуникационных технологий. Среди них более 38 тысяч преступлений совершены самими несовершеннолетними, около 1,5 тысяч несовершеннолетних были вовлечены в совершение преступлений или антиобщественных действий.

Безусловно, проведение комплексной работы с детьми остается в первую очередь за родителями. При этом сложно переоценить и тот вклад, который может внести школа. Для современных школьников именно учитель, а не интернет и компьютер, остается центральной фигурой в учебной и внеучебной деятельности — только 1,5% подростков считают, что учеба стала бы интересней, если бы преподавателя полностью заменили компьютерные

технологии. Цифровое обучение приветствуют 47% школьников, но только в том случае, если будут использоваться современные увлекательные программы, а вторую половину урока будет интересно вести учитель. Каждый пятый подросток считает, что компьютер уместен не на всех предметах и не на каждом уроке, а 7% учащихся полностью отказались бы от компьютера в пользу занятий с учителем, способным организовать разные формы работы для всего класса. Половина подростков от 13 до 18 лет считают, что для положительного воздействия школы на учеников нужны доверительные отношения между учителями и учащимися, а 41% школьников полагает, что педагоги должны быть авторитетами для своих учеников. Почти половина школьников (42%) считают, что в случае нарушения их прав нужно обратиться к учителю.

Как сообщил в феврале 2019 года портал Mel.fm, в сентябре 2019 года в расписании британских школ появятся уроки, где ученикам расскажут об особенностях взаимоотношений между людьми, безопасном общении в Сети и заботе о своем психическом здоровье. Занятия будут обязательными. Подобные занятия проводятся и в школах России.

Эти материалы отобраны для помощи в обучении подростков безопасному использованию Интернета и повышения их цифровой грамотности.

Основные понятия

Блогер — человек, который ведет собственный электронный дневник в сети Интернет и администрирует его, в том числе на одной из популярных платформ (Instagram, LiveJournal, Facebook и т. д.).

Вредоносный код — компьютерный код или веб-скрипт, разработанный для создания уязвимостей в системе, с помощью которых выполняются несанкционированные вредоносные действия, такие как кража информации и данных и другие потенциальные повреждения файлов и вычислительных систем.

Контент-фильтр — устройство или программное обеспечение для фильтрации сайтов по их содержимому, не позволяющее получить доступ к определенным сайтам или услугам сети Интернет. Система позволяет блокировать веб-сайты с содержимым, не предназначенным для просмотра.

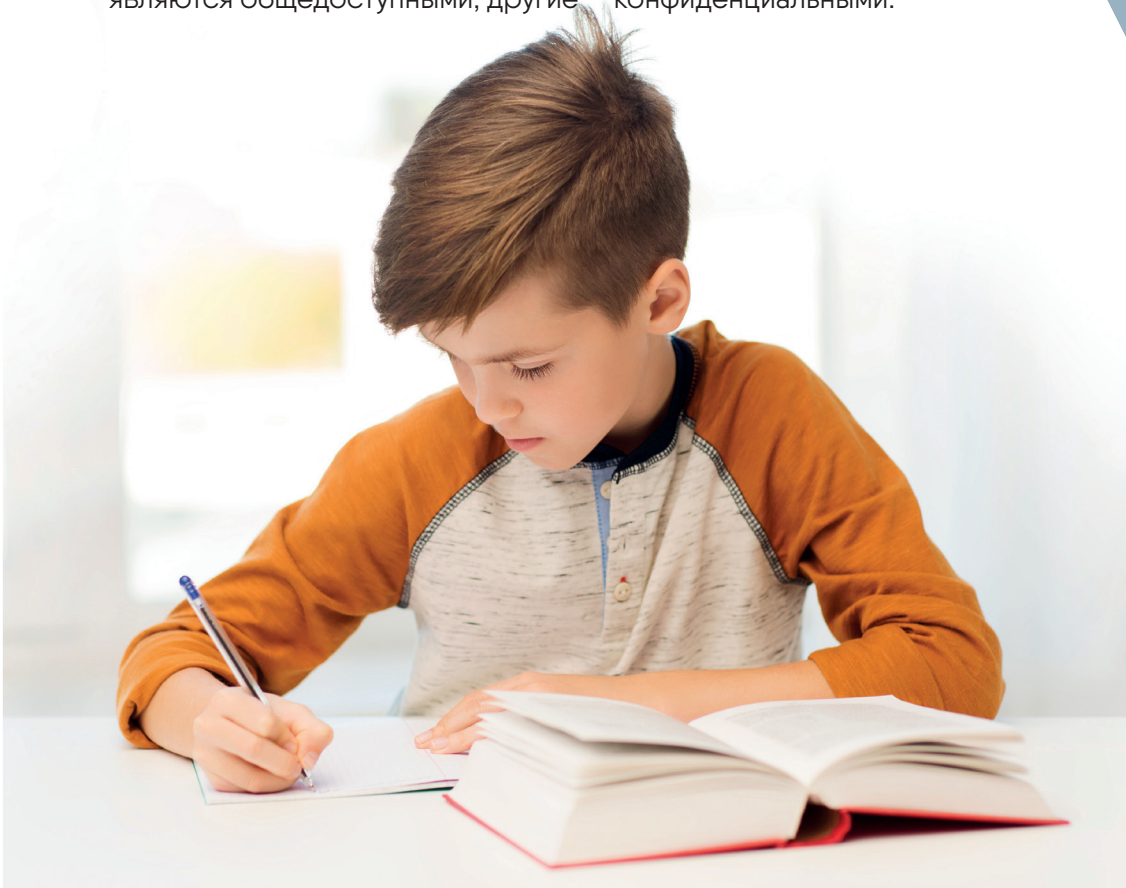
Персональные данные — любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных).

Травля (жарг. буллинг) — агрессивное преследование одного из членов коллектива (чаще – школьников и студентов, в некоторых случаях и взрослых) со стороны другого члена коллектива. Травлю организует лидер, иногда вместе с сообщниками, а большинство остаются свидетелями. Жертва травли оказывается не в состоянии защитить себя от нападок — этим травля и отличается от конфликта, где силы сторон примерно равны. Травля может быть как физической, так и психологической. Проявляется во всех возрастных и социальных группах. В сложных случаях может принять некоторые черты групповой преступности.

Фишинг — один из видов интернет-мошенничества, целью которого является получение доступа

к конфиденциальным данным пользователей: логинам, паролям, лицевым счетам и банковским картам. В основном используется метод проведения массовых рассылок от имени популярных компаний или организаций, содержащих ссылки на ложные сайты, внешне неотличимые от настоящих.

Цифровой след — совокупность информации о посещениях и вкладе пользователя в цифровое пространство. Может включать в себя информацию, полученную из мобильного Интернета, веб-пространства и телевидения. Это могут быть личные профили и учетные записи в социальных сетях, информация о посещаемых веб-сайтах, открытые и созданные файлы, личные сообщения и комментарии, видео, фотографии и другая виртуальная активность, в том числе ввод персональных данных пользователя. Некоторые из этих материалов являются общедоступными, другие — конфиденциальными.



1. Сетевые угрозы безопасности детей

1.1. Мошенничество в отношении детей

Признаки интернет-мошенничества бывает непросто распознать даже взрослым. Совершать противоправные действия в сети преступники могут как через Интернет, так и через локальное подключение. Хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации определяется законодательством как «Мошенничество в сфере компьютерной информации». Данный вид противоправных действий рассматривается в ст. 159.6 УК РФ. Ответственность по указанной статье наступает с 16 лет.

Возможные схемы мошенничества:

1) Фишинг (получение доступа к логинам, паролям, банковским данным).

Мошенники организуют рассылку сообщений якобы от имени банка со ссылками на поддельные страницы официальных сайтов. Вводя свои персональные данные (номера банковских карт, логины, пароли), жертва неосознанно передает конфиденциальную информацию мошенникам. А те, в свою очередь, используют сведения для завладения денежными средствами.

Для предупреждения школьников о подобных схемах мошенничества можно:

- рассказать о специализированных интернет-ресурсах проверки сайтов на факты совершения мошеннических действий (например, сайт https://довериевсети.рф/) и других сервисах контроля репутации сайта на предмет мошеннических действий (негативные отзывы, жалобы на сайт, проверка на вирусы). Напомнить, что достоверный сайт обязательно содержит сведения об авторах и их контактные данные;

- обратить внимание детей на то, что нельзя вводить данные банковских карт на сомнительных сайтах интернет-магазинов (cvc/cvv-код, срок действия, номер карты);

- напомнить, что никому не стоит передавать или выкладывать в Сеть конфиденциальные данные (логин, пароль), свидетельство о рождении, паспортные данные, адрес прописки и фактического места жительства, слишком личные фотографии.

2) Поддельные интернет-магазины. В интернете существует большое количество поддельных магазинов, недобросовестных продавцов и лжепредпринимателей, которые могут обмануть, не предоставить товар или завладеть персональными данными для мошеннических действий.

Пример. В апреле 2019 года женщина из города Кинель Самарской области перевела 62 000 рублей мошенникам, торговавшим шубами на поддельном сайте. Шубу она не получила, а сайт на следующий день был заблокирован. На сайте размещали поддельные отзывы и ссылки на контакты в социальных сетях, и перед оплатой женщина писала, как думала, реальным людям, которые все как один дали положительные отзывы.

При заказе через Интернет нужно руководствоваться некоторыми правилами:

- обязательно нужно проверить интернет-магазин перед совершением покупки: на официальном сайте должны быть приведены сведения о правоустанавливающих документах (свидетельство о регистрации в налоговом органе, код ОКВЭД, ИНН, ОГРН), соглашение на использование и обработку персональных данных, адрес фактического расположения, данные о потребительских свойствах товара.

– не сообщать свои персональные данные и не переводить денежные средства лицам, которые не являются сторонами сайта.

Развитие интернет-торговли нередко вызывает у ребят желание не только купить, но и начать продавать товары. Некоторые школьники организуют группы продаж товаров из Китая, например, с площадок Aliexpress, некоторые выставляют на продажу свои поделки, творческие работы, личные вещи, размещают объявления об оказании услуг. Посоветуйте детям не продавать товары через неспециализированные интернет-сайты, социальные сети, рассылку рекламных сообщений. Для этого существуют специализированные сайты, например, https://www.avito.ru, https://youla.ru. За регулярное распространение товаров и услуг, осуществляемое с нарушениями, можно быть обвиненным в незаконном предпринимательстве.

Примечание. Систематическое получение прибыли от продажи товаров без регистрации ИП является незаконным предпринимательством. В соответствии со статьей 2 Гражданского кодекса Российской Федерации предпринимательской является самостоятельная, осуществляемая на свой риск деятельность, направленная на систематическое получение прибыли от пользования имуществом, продажи товаров, выполнения работ или оказания услуг лицами, зарегистрированными в этом качестве в установленном законом порядке.

Для практической отработки рекомендуется использовать кейс № 12 (стр. 25).

3) Сборы средств на «благотворительность».

В социальных сетях все шире распространяется практика сбора средств на лечение, питание, покупку медикаментов и оборудование, помощь в трудной жизненной ситуации как для людей, так и для животных. Желание помочь – очень благородный порыв, но лучше убедиться, что эта помощь достигнет адресата. Злоумышленники могут

сымитировать официальную страницу по сбору средств для благотворительных целей, указав при этом свой расчетный счет. Часто это происходит во время ликвидаций последствий аварий и катастроф, терактов с большим количеством пострадавших: люди торопятся оказать помощь нуждающимся, не тратят времени на проверку информации, а потому иногда переводят деньги мошенникам.

Что можно сделать?

- проверить источник: для какой группы в социальных сетях происходит сбор пожертвований;
- проверить через поисковик, существуют ли аналогичные группы, направленные на поддержку этому же человеку, животному, организации — иногда мошенники делают страницу-клон в надежде перехватить часть посетителей сообщества с хорошей репутацией;
- связаться с администраторами группы для уточнения деталей, задавая им при этом как можно больше вопросов, позволяющих определить их причастность к этому сбору средств;
- постараться связаться с родственниками/представителями лица или лиц, для которых организован сбор средств.

Иногда в ходе длительного онлайн-общения собеседник начинает ссылаться на наличие проблем, решение которых требует финансовых средств. Расскажите ученикам, что не следует без обсуждения со взрослыми переводить деньги малознакомому человеку, с которым общались только в режиме онлайн, какие бы причины ни называл собеседник (операции, долги, «проблемы, о которых не расскажешь родителям»).

4) Вирусный контент.

Меняет или полностью блокирует доступ к персональному компьютеру. В такой ситуации пользователю часто приходит требование осуществить перевод или отправить СМС на предлагаемый номер для восстановления пароля. В других случаях компьютер может подвергнуться заражению «трояном», который делает доступными для злоумышленников личные данные.

Пример. Новый вирус троян-вымогатель Trojan-Ransom.Win32.Vkont.a появился в социальной сети «ВКонтакте», предупреждают эксперты «Лаборатории Касперского». Алгоритм работы троянцев-вымогателей прост и заключается в блокировании работы компьютера с целью получения денег злоумышленниками. Для этого пользователю предлагается отправить СМС-сообщение на короткий номер в обмен на пароль для восстановления данных или нормальной работоспособности компьютера. Для России проблема «блокеров» является очень актуальной: по данным «Лаборатории Касперского», ежедневно с такими вредоносными программами сталкиваются несколько тысяч российских пользователей и не только при пользовании соцсетью, но и при скачивании сомнительных фильмов.

В сети «ВКонтакте» это обычно выглядит так: пользователю предлагают пройти по ссылке на сайт, который на самом деле является мошенническим, и там узнать все интересующие его тайны. На этом сайте предлагается скачать ПО для взлома учетных записей в социальной сети «ВКонтакте». Однако после клика на кнопку загрузки под видом «программы-взломщика» начинается скачивание троянца-вымогателя. После этого на рабочем столе компьютера появляется окно с предложением отправить СМС-сообщение на короткий номер, чтобы

получить программу для доступа к личным данным пользователей сети «ВКонтакте». Одновременно троянец блокирует работу системы до тех пор, пока вымогатели не получат выкуп в виде СМС.

Но после отправке СМС троянец скачивает архив VK-Hack.zip, в котором находятся программа для подбора паролей к аккаунтам в популярных почтовых сервисах, а также ПО класса ShareWare, за полноценное использование которого необходимо заплатить дополнительно. Таким образом, жертва уловки мошенников не только оплачивает отправку дорогостоящей эсэмэски, но и получает совсем не бесплатные программы сомнительного функционала. «Лаборатория Касперского» рекомендует при обнаружении СМС-блокера на компьютере не идти на поводу у мошенников и не отправлять сообщения, а удалить назойливый баннер с рабочего стола с помощью бесплатного сервиса на сайте «Лаборатории Касперского». Данная услуга доступна также и через мобильное устройство.

Обсудите с ребятами, что нельзя переходить по опасным ссылкам, принимать какие-либо сомнительные соглашения. Для защиты компьютера нужно устанавливать специальные защитные программы и фильтры. Для надежной защиты лучше использовать лицензионное программное обеспечение с актуальными обновлениями. Устанавливать необходимо все обновления, как только они становятся доступными. Нельзя допускать истечения срока действия антивируса.

Стоит относиться с осторожностью к скачиванию программных продуктов из файлообменных сетей и торрентов. Подозрительные файлы не открывайте и не сохраняйте. Не отвечайте на сомнительные рассылки. И главное — не посещайте ресурсы с неоднозначной репутацией, которые вызывают у вас (или у вашей

антивирусной программы) любые подозрения.

Аналогичные рекомендации целесообразно дать подросткам для соблюдения интернет-безопасности вне образовательной организации.

При проведении уроков по Интернет-безопасности и занятий в рамках внеурочной деятельности можно использовать кейсы № 2 и № 10 (стр. 22 и 24).

5) Информация о легком заработке.

Сейчас в Сети набирают популярность объявления о легком и высоком заработке для подростков. Зачастую такая работа связана с вовлечением ребят в мошеннические или преступные схемы. Как правило, речь идет о распространении наркотических средств: подростки делают «закладки» в назначенных куратором местах, а затем их забирают клиенты. Стоимость такой подработки для школьников весьма привлекательна — от 60 000 до 160 000 рублей. Нередко ребята соглашаются, не догадываясь о характере доставляемого товара. Но иногда желание заработать перевешивает здравый смысл, и некоторые подростки соглашаются участвовать в распространении наркотиков, рассчитывая остаться безнаказанными.

В рамках мероприятий по интернет-безопасности подросткам можно рекомендовать:

- анализировать любые «привлекательные» объявления на адекватность;
- всегда проверять информацию о работодателе, а проверив — настаивать на оформлении официальных трудовых отношений (с 14 лет) или договора гражданско-правового характера (с 15 лет). Если речь не идет ни о чем незаконном, работодатель должен согласиться;
- выяснять содержание и условия подработки

до мелочей (почему так оценивается, что конкретно нужно делать, что нужно везти, какой товар доставлять);

- если что-то смущает – не стесняться спрашивать и выяснять любые подробности;

- всегда помнить, что за легкую работу ни один работодатель не будет расплачиваться крупной суммой денег;

- обращать внимание на предложения сделать что-то анонимно. Это один из маркеров того, что вас вовлекают в мошенническую схему.

При проведении бесед на эту тему можно использовать кейс № 4 (стр. 23).

1.2. Недостоверная информация и deepfake

Большинству подростков сложно оценивать сайты с точки зрения достоверности информации. В рамках уроков и внеурочной деятельности по интернет-безопасности целесообразно объяснить обучающимся, что **не все, что они видят в Интернете, является правдой.**

При проведении практических занятий можно представить школьникам несколько источников с разным содержанием информации по той или иной проблеме и спросить, что они думают о проблеме, как это мнение соотносится с информацией, представленной в источниках. Объясните учащимся, что в случаях столкновения с сомнительным содержанием нужно поискать дополнительную информацию или посоветоваться с родителями и учителями.

Необходимо объяснить школьникам, что информация, выложенная в Интернете, может не соответствовать действительности, ведь опубликовать ее может абсолютно любой человек.

Целесообразно при проведении уроков по интернет-безопасности и в рамках внеурочной деятельности дать школьникам следующие рекомендации:

1) Не скачивать информацию для выполнения работ по учебе с непроверенных источников. Важно уметь давать адекватную оценку информации в неструктурированном потоке. Например, в банк рефератов, курсовых и дипломов работы выкладываются такими же школьниками и студентами, а сделать вывод о том, как такая работа была оценена, невозможно. Можно обратить внимание школьников на факт, что достойная работа стоит существенных временных и интеллектуальных затрат, и автор не будет распространять такую работу в свободном доступе для общего пользования.

2) Пользоваться официальными энциклопедиями и словарями.

3) Проверять сайт, с которого будет использована информация. Сайт должен содержать сведения об авторстве сайта, контактные данные, ссылки на источники информации. Самым лучшим доказательством надежности сведений является наличие ссылок на авторитетные источники информации. Это могут быть агентства по сбору статистических данных, научно-исследовательские институты, другие официальные источники.

Часто в Интернете идет перепечатка данных с одного сайта на другие. Чем больше ссылок на исходный материал находится в Сети, тем выше его авторитет в глазах других ресурсов. Это, как правило, говорит о том, что данному источнику информации доверяют. Тем не менее его тоже лучше проверить, иногда большое количество сайтов ссылаются на один и тот же источник недостоверной информации.

Пример. В 2010 году во время матча чемпионата мира по футболу между Бразилией и КНДР многие заметили баннер в руках бразильских болельщиков, на котором было написано: Cala Boca Galvão. Те, кто во время просмотра матча привык строчить твиты, заметили, что тысячи бразильских болельщиков ретвитят эту фразу. Через четыре дня Cala Boca Galvão вышел в топ трендов Twitter, состоящий из слов или фраз, которые чаще всего ретвитят пользователи сервиса по всему миру.

Twitter сообщил своим пользователям, что Cala Boca Galvão – популярный твит, однако это не помогло им понять значение этой фразы. На помощь пришли бразильские пользователи сервиса. Они объяснили, что Galvão – это птица, оказавшаяся на грани исчезновения из за того, что ее яркими перьями украшают головные уборы исполнительниц самбы, которые танцуют на карнавальных парадах. Для распространения информации о бедственном положении этого вида пернатых был создан Институт Galvão, и с каждого ретвита Cala Boca Galvão – «Спасите птицу Galvão», институт

получает пожертвование в 10 центов. От имени Института Galvão на YouTube появился ролик на английском языке, в котором рассказывали о бедственном положении птицы Galvão и настоятельно призвали к участию в кампании Twitter под лозунгом: «Секундное дело – сделать ретвит, секундное дело – спасти жизнь».

Кампания набирала обороты. После того как на защиту птицы Galvão встали пользователи Twitter, за дело принялись знаменитости. Леди Гага, по слухам, собиралась выпустить сингл под названием Cala Boca Galvão, на YouTube появились десятки версий новой песни. Многие версии звучали как переделка ее же композиции Alejandro, но были, как ни странно, и совершенно другие мелодии. Фонд птицы Galvão, дочерняя организация Института Galvão, раскрыл темную сторону этого вопроса, опубликовав фото тренера аргентинской сборной по футболу Диего Марадоны с торчащим из ноздри зеленым пером. Оказалось, что птиц истребляют еще из-за галлюциногенных свойств содержащегося в оперении вещества.

Для тех, кто еще не набрал эту фразу в Google переводчике, 15 июня 2010 года газета New York Times раскрыла карты: Cala Boca Galvão переводится как «Замолчи, Гальвао». Карлос Эдуардо душ Сантуш Гальвао Буэно – ведущий футбольный комментатор телеканала Rede Globo, транслирующего игры Кубка мира в Бразилии. Его полные штампов и общих мест комментарии были не по душе многим бразильским фанатам. Фраза разошлась, когда тысячи бразильских болельщиков, смотря первые матчи турнира по Rede Globo, дали выход своему раздражению. Когда же фраза вошла в топ трендов Twitter, поддержание ее на пике популярности стало своеобразной игрой. Призывая ничего не подозревающих благонамеренных иностранцев ретвитить эту фразу, сетевые бразильцы сыграли со всем остальным миром гигантскую шутку.

4) Не доверять расплывчатым ссылкам на источники информации, таким как «по исследованиям ученых», «как утверждают специалисты». **Любое утверждение имеет**

автора. Поэтому для того, чтобы ссылка была корректна, нужно упоминать дату, автора и метод проведения исследования (опрос, наблюдение, рейд и т. д.), а в случае с высказываниями отдельных экспертов — их полное имя, место работы, звания и т. д.

Очень важным является вопрос о компетентности автора информации. Стоит выяснить его статус, должность, ознакомиться с другими работами, материалами, комментариями, отзывами. Возможно, автор ведет свой блог, у него есть страница в социальной сети, он имеет научную степень, журналистский опыт и пр. Также можно выяснить рейтинг ресурса, на котором исходно была размещена информация: насколько он популярен, пользуется или не пользуется авторитетом, какие отзывы существуют о данном ресурсе в Сети. В этом могут помочь известные информационно-поисковые системы, например, «Яндекс». Он покажет и индекс цитирования ресурса, и выдаст через поисковый запрос информацию о нем, а также по различным комбинациям поисковых запросов предоставит аналогичную информацию, которая поможет сравнить данные, оценить их достоверность.

Обращайте внимание на наличие у интернет-ресурса свидетельства о регистрации в качестве СМИ — он несет особую ответственность за любую опубликованную информацию. Также можно доверять официальным информационным агентствам, таким как ИТАР-ТАСС, Интерфакс, РИА «Новости» и другие.

5) Новость, окрашенная в яркие эмоциональные тона, но не имеющая ссылок на достоверные источники, не подтвержденная фотографиями или видеосъемками, носит явно пропагандистский характер. Сомнительные же фотографии следует проверять с помощью поиска по картинкам (в системах «Яндекс» или Google). Часто случается, что при освещении событий СМИ используют более старые фотографии похожих (но не тех, о которых пишут) событий.

20 овчарок подлежат усыплению

«В связи с расформированием отдела охраны ВОХР РЖД подлежат усыплению 20 воспитанных, ученых, умных овчарок. Отдадут даром!».

Это – один из первых массовых фейков. Он появился в 2011 году в Новосибирске. В объявлении были номера личных телефонов реальных людей, ни сном ни духом не ведающих ни о каких собаках. Позже фейк публиковался в разных городах, с различными телефонами. Дозвониться на них не удавалось, но говорили, что телефоны мошеннические, и при попытке дозвониться на них снимаются деньги.

Позже появился аналогичный фейк про далматинцев. «Овчарки» и «далматинцы» в виде фотографий несколько лет странствовали по Сети, утратив телефоны и остатки логики, но репосты попадались вплоть до 2016 года, а это значит, что находились люди, которые, поддавшись эмоциям, репостили объявление без контактов, даже не думая о смысле такого репоста.

Новостную аналитику (особенно политизированных событий) без ссылок на надежные источники нужно воспринимать как недостоверную.

В последние годы в Сети набирает обороты такое явление, как deep fake – поддельное видео, созданное компьютерным алгоритмом из большого числа изображений одного человека. Это управляемый искусственным интеллектом механизм замещения на видео лица одного человека лицом другого человека. При этом «дипфейк» – уже устоявшееся явление, примеры замены лиц можно встретить в сюжетах различных кинофильмах. Процесс создания deep fake в настоящее

время является очень дорогостоящим, кроме того, для действительно качественного копирования целевой модели необходимо большое количество фотоснимков (более 2-3 тысяч). Сейчас не каждый сможет позволить себе воспользоваться этой технологией, но в будущем наличие в Сети большого количества ваших фотографий может стать базой для создания такого ложного видео.

Пример. В мае 2018 года в Интернете появился видеоролик, в котором Дональд Трамп давал совет Бельгии по проблеме изменения климата. Видео создала бельгийская политическая партия Socialistische Partij Anders (Фламандская социалистическая партия) и разместила его в Twitter и Facebook. Это вызвало сотни комментариев пользователей Сети, многие из которых выразили возмущение, что американский президент осмелился оказывать влияние на политику Бельгии. Задача партии состояла в использовании фейкового видео для привлечения внимания людей. После просмотра пользователей перенаправляли на онлайн-петицию, в которой призывали бельгийское правительство предпринять более срочные действия в вопросе климата.

А британская компания Synthesia сняла социальную рекламу с участием бывшего футболиста Дэвида Бекхэма, который рассказывает об опасности малярии. Бекхэма не просто озвучивают девять актеров. Благодаря ИИ-обработке он будто сам произносит слова на девяти разных языках, и выглядит это очень убедительно.

Недостоверная информация может содержаться не только на информационных сайтах. Ежедневно в социальных сетях школьники видят фотографии дорогостоящего отдыха, красивых мест, брендовых вещей. Пользователи соцсетей показывают только лучшие стороны своей жизни, самые яркие ее моменты. Подобный контент формирует у подростков искаженное впечатление об успешности. Проводя параллель со своей повседневной жизнью, дети пытаются

стремиться к такому же формату успешности, не всегда имея на это средства.

На занятиях или классных часах можно обсудить со школьниками, что отдельные посты в социальных сетях никогда не отражают полную картину реальной жизни.

1) Фотографии, выкладываемые в социальные сети, тщательно редактируются при помощи современных программ. Для сравнения можно взять фотографии публичных людей — снимки в реальной жизни и промо-фотографии, обработанные в редакторах.

2) Некоторые пользователи соцсетей в погоне за онлайн-популярностью используют чужие изображения для создания поддельного видеоролика.

1.3. Общение в Сети

Сегодня, когда можно моментально сделать снимок и отправить его, более тесным стало не только общение. И оказаться в неприятной ситуации, отправив неосторожно сделанную фотографию, очень легко. Не только детям, но и взрослым следует внимательно оценивать изображения, которые они выкладывают в Сеть.

Обсудите с ребятами, насколько может быть опасно отправлять личные, а тем более — интимные фото и видео, с помощью которых можно установить, где и с кем живет ребенок, где и в какое время часто бывает. Подростки недооценивают эти риски. Сеть воспринимается ребятами как пространство безопасного общения. Многие считают, что при общении в Интернете их никто не найдет и не увидит. Тем временем специалисты советуют: не выкладывай в Интернет ничего, что не хотел бы однажды увидеть на Кремлевской стене. Главная угроза в том, что приватные фотографии, видео или сообщения могут стать не столь приватными.

Случается, что социальные сети в корыстных целях используют злоумышленники. Это могут быть педофилы,

которые, ищут новые жертвы, выдавая себя за сверстника, искать личной встречи, а также мошенники, которые пользуясь доверчивостью подростков, выведывают конфиденциальную информацию. Предупредите ребенка, что опасность невольно может исходить даже от знакомых людей. Например, человек, которому отправили сообщение, может выложить фотографии в Интернет или переслать друзьям. Или же злоумышленники могут получить доступ к облачному хранилищу, куда автоматически отправляется медиаконтент со смартфона. Есть вероятность того, что подросток потеряет смартфон или забудет его в общественном месте. Этот телефон может подобрать посторонний человек и получить таким образом доступ к медиафайлам.

Попав в чужие руки, эротические фотографии или видео могут стать инструментом шантажа. Кроме того, подобные материалы, размещенные в социальных сетях, могут «перекочевать» на порносайты. Это может не только сказаться на репутации жертвы в Сети, но и создать серьезные проблемы уже в реальной жизни. Сложности могут вызвать и выложенные в социальные сети фотографии билетов в семейный отпуск — они могут стать сигналом для злоумышленников, что квартира останется без присмотра.

Еще одним последствием публичного распространения приватных фотографий может стать кибербуллинг — это особенно часто встречается в подростковой среде. При этом стоит понимать, что человека на фотографии можно идентифицировать, даже если в кадре не видны никакие особые приметы, такие как родинки или татуировки. Определить, кто изображен на фотографии, можно по разным деталям, в том числе и по интерьеру. Кроме того, в свойствах фотографии зачастую остаются данные автора, дата съемки, сведения о камере, на которую делался снимок, вплоть до ее серийного номера. Смартфон также сохраняет геометку того места, где сделана фотография. По этим косвенным уликам часто можно вычислить владельца снимка.

Вот несколько основных правил, которые следует сформулировать вместе с детьми:

1. Не стоит отправлять интимные фотографии незнакомцам даже после долгих уговоров.
2. Не следует таким образом пытаться привлечь внимание парня или девушки.
3. Не стоит публиковать у себя на страничке в социальной сети откровенную фотографию или даже кадр с намеком на откровенность с целью собрать побольше «лайков».

Если кто-то из ребят уже стал жертвой, вы можете помочь им связаться с администрацией ресурса, где появилось фото, и сообщить, что персональные данные несовершеннолетнего размещены в открытом доступе. Администрация должна эту информацию удалить. Если такое обращение не поможет, стоит прибегнуть к юридической помощи: в нашей стране действуют законы относительно защиты персональных данных и незаконного распространения порнографии.

В рамках занятий по интернет-безопасности можно:

- рассказать о том, почему не стоит выкладывать подробную информацию о себе, номер телефона и электронной почты;
- напомнить, что не нужно часто «чекиниться», то есть проставлять привязки к месту действия, выкладывая фотографии;
- можно провести инструктаж по поводу общения с незнакомыми людьми в Сети, научить говорить четкое «нет» на предложения списаться по электронной почте, созвониться, а тем более встретиться;
- провести разъяснительную работу о том, что нельзя раскрывать информацию о себе незнакомым людям, доверять сведения личного характера человеку, которого никогда не видел вживую;

- рекомендовать подросткам не рассказывать в Сети ничего такого, чего они могут стесняться;
- обсудить с ребенком возможные угрозы и опасности от встреч и онлайн-общения с незнакомцами и договориться о том, как он будет вести себя в той или иной ситуации;
- разъяснить обучающимся, что в Интернете человек может представиться кем угодно;
- сформировать у обучающихся настороженную позицию к вопросам с финансовым подтекстом;
- провести беседу с детьми и подростками о нецелесообразности публикации своих геолокаций, по которым злоумышленники смогут определить их местоположение.

При проведении соответствующих уроков и мероприятий внеурочной деятельности рекомендуется использовать кейсы № 13 и № 14 (стр. 26).

2. Опасности, которым дети подвергают себя и других при использовании сети Интернет

2.1. Съемка фото и видео для размещения в сети Интернет, сопряженная с опасностью для жизни и здоровья

В последнее время среди интернет-пользователей набирает популярность фото- и видеосъемка как повседневных, так и ярких жизненных моментов, и размещение данного контента в сети Интернет. Некоторые примеры такого поведения детей:

1) Подросток становится невольным свидетелем вооруженного конфликта, стрельбы, взрыва и первым делом снимает происходящее на мобильный телефон. Вместо того чтобы предпринять необходимые меры безопасности (убежать, вызвать полицию), он снимает «уникальное видео» ради популярности в Сети, рискуя жизнью и здоровьем.

2) Выбор подростком опасных или экстремальных увлечений. Например, «руфинг» (прогулки по крышам), «скайуокинг» (покорение самых высоких точек в городе без специального снаряжения) или «зацепинг» (проезд вне салона электропоезда, трамвая – на крыше или подножке). Ради популярности в Интернете дети стремятся заснять свои «подвиги», что ведет к негативным последствиям. Такие увлечения сами по себе представляют смертельную опасность, а использование камеры только увеличивает риск оступиться, потерять равновесие или не заметить угрозу.

3) Стремление поразить интернет-друзей яркими или опасными фотографиями, сделанными в формате селфи. Как в России, так и в мире зафиксирована масса смертельных исходов при попытке сделать собственную фотографию в опасных местах, которые уже получили название «селфиубийства». Селфи на воде, на краях

обрывов или скал, на железных и автомобильных дорогах, на крышах домов или промышленных объектов, вблизи линий электропередач могут привести к крайне негативным последствиям для жизни и здоровья ребенка.

Предотвратить подобные ситуации можно через формирование у обучающихся культуры личной безопасности. Она состоит в готовности защитить себя и окружающих от неблагоприятного воздействия, угроз и наступления нежелательных последствий. Подростку можно объяснить, что при возникновении опасных ситуаций необходимо в первую очередь, позаботиться о безопасности себя и других людей, а затем вызвать полицию. При беседе на тему опасных увлечений нужно постараться принять точку зрения ребенка, услышать от него аргументы в пользу его хобби. Главное — занять доброжелательную позицию со своей стороны, ненавязчиво предложить альтернативные виды деятельности, проходящие в безопасных условиях. Важно не переусердствовать, но при этом донести до ребенка посыл, что он не безразличен вам, своей семье, близким и друзьям.

2.2. Игнорирование опасности в виртуальной среде

Зачастую происходящее в сети Интернет не воспринимается подростками как часть реальной жизни. В большинстве случаев дети воспринимают сетевое общение как игру, не понимая, что за экраном — живые люди со своими представлениями, мнением, реакциями на то или иное явление.

Например, школьник публикует в социальных сетях сообщения, призывающие к физической расправе с учителями, родителями, одноклассниками. Но друзья учащегося или ребята из его класса не воспринимают такие публикации всерьез и оставляют данный факт без внимания.

Для профилактики подобных ситуаций можно предпринять следующее:

- объяснить обучающимся, что такие публикации могут представлять реальную опасность;
- донести до подростков, что сообщить о таких публикациях учителям и родителям — осознанный поступок взрослого человека;
- напомнить, что все случаи стрельбы или вооруженного нападения в школах начинаются с публикаций в социальных сетях, которые никто не воспринимает всерьез;
- объяснить ребятам, что лучше лишний раз перестраховаться и сообщить об угрозе, чем рисковать своей жизнью и жизнью своих одноклассников;
- по возможности лично обращать внимание на содержание контента, размещаемого учениками в социальных сетях;
- провести аналогичные мероприятия с родителями обучающихся, ознакомить их с информацией, сообщенной ранее подросткам.

2.3. Противоправные действия детей в сети Интернет

Какие действия подростков в сети Интернет могут привести к негативным последствиям:

1) Оскорбление личности в Интернете.

Важно проводить работу с подростками, направленную на повышение их правовой сознательности. **Обучающиеся несут ответственность за то, что пишут в сети Интернет, и должны об этом знать.** Ученикам можно рекомендовать:

- не вступать в перепалку с теми людьми, целью которых является осознанная провокация другого человека на проявление эмоций;

– не реагировать на оскорбительные сообщения, прекратить общение и закрыть страницу от посторонних лиц.

Следует разъяснить школьникам, что не стоит стесняться рассказывать учителям и родителям об угрозах, полученных через Интернет. В таком случае есть шанс наиболее достойного выхода из ситуации. Цель интернет-провокаторов – специально запугать человека, но сами они очень боятся ответственности.

Важно обратить внимание подростков, что если они сами являются агрессорами в интернет-среде, ошибочно думать, что об этом никто не узнает. Переписка может очень быстро распространиться в Сети и служить доказательством действий, противоречащих нормам права.

При проведении соответствующих уроков и мероприятий внеурочной деятельности рекомендуется использовать кейсы № 5 и № 6 (стр. 23).

2) Травля в Интернете: кибербуллинг.

Изменение психологической обстановки в классе может являться свидетельством начала травли одного или нескольких учеников. Об этом могут говорить насмешки одноклассников над сверстником, чрезмерное увлечение неопределенными видео в телефонах.

Если вам кажется, что в детском коллективе негативная обстановка, но еще неясно, кто является жертвой, необходимо установить лидера и аутсайдера группы. Также полезно понимать, кто в классе является интровертом, а кто — экстравертом. Как правило, больше страдают интроверты — они чувствительнее к нарушению границ, и их проще ранить. Определение социальных ролей в классе поможет понять, кому необходима помощь, а чьи границы лучше не нарушать.

Переход травли в активную фазу нельзя оставлять без внимания. Оскорбления, драки, неуместные шутки

необходимо пресекать. Важно провести беседу со всеми участниками конфликта. Бездействие в подобной ситуации невозможно, иначе конфликт может зайти очень далеко, а его последствия могут быть очень печальными для всех его участников. Важно, не осуждать только зачинщика травли. Скорее всего он действует так, потому что его поддерживает весь класс. Целесообразно привлекать к разбору ситуации педагога-психолога. Специалист сможет поддержать жертву травли, организовать беседу с участниками конфликта и дать рекомендации о необходимости подключения родителей и других одноклассников к разрешению проблемы.

Подросткам, ставшим жертвами буллинга в Интернете, необходимо рекомендовать обращаться к родителям и педагогам в случаях продолжения агрессии в свою сторону даже после ограничения доступа к своему аккаунту. Взрослые помогут принять адекватное и взвешенное решение.

Родители представляют интересы несовершеннолетних детей, поэтому должны быть в курсе происходящего с ними. Информацию до них необходимо доносить аккуратно, но настойчиво. Родителям стоит рекомендовать следить за эмоциональным состоянием ребенка. В том случае, если ребенок явно подавлен и напуган, родителям целесообразно получить доступ к его аккаунтам в социальных сетях, чтобы определить, исходит ли угроза от тех людей, с которыми он общается в Сети.

Следует обратить внимание обучающихся на следующие моменты:

- в интернет-травле они могут оказаться как по одну, так и по другую сторону;
- любая переписка может храниться очень долго (минимум полгода), к тому же любые материалы сейчас можно сохранить, создав архив;
- даже при использовании VPN-сервисов, предотвращающих отслеживание активности в Интернете,

есть другие способы установления зачинщика интернет-травли.

При проведении соответствующих уроков и мероприятий внеурочной деятельности рекомендуется использовать кейсы № 13 и № 14 (стр. 26).

3) Майнинг криптовалюты.

Заработок в Интернете обрел большую популярность, особенно среди подростков. Новым видом деятельности, приносящей доход посредством использования интернет-технологий, стала добыча виртуальной криптовалюты (майнинг). Вместе с тем такой заработок представляет собой опасность как для жизни и здоровья детей, так и для окружающих людей. Ведь для этой деятельности необходима «майнинг ферма» – большое количество специального оборудования, сосредоточенного в одном помещении. Электропроводка в жилых домах не рассчитана на такие нагрузки. Поэтому при майнинге риск пожара в домах существенно увеличивается. Случаи возгорания из-за работы «майнинг ферм» уже имели место. Например, в городе Артем Приморского края пожар разгорелся на площади 500 квадратных метров, в результате чего выгорели полностью восемь квартир. Похожий инцидент произошел в Томской области, когда проводка домов не выдержала нагрузки, в результате случилось короткое замыкание.

Помимо этого «майнинговые фермы» создают повышенный уровень шума. Чаще всего это связано с работой системного оборудования, но также сильный шум могут создавать кондиционеры, круглосуточно работающие для охлаждения помещений. Регулярное шумовое воздействие неблагоприятно сказывается как на нервной системе, так и на ходе сна. Для восстановления и отдыха человеку необходима спокойная бесшумная обстановка. После длительного нахождения в шумном помещении человек может испытывать

повышенную раздражительность и утомляемость, качество сна ухудшается.

В настоящее время в Государственной Думе Федерального Собрания Российской Федерации рассматривается законопроект, в котором закрепляются такие понятия, как «майнинг», «криптовалюта», «токен», «смарт-контракт», а также предлагается отнести добычу криптовалют к предпринимательской деятельности. Это означает, что с такого заработка необходимо будет заплатить налог.

Примечание. Отстоять свое право на достойную репутацию в сети Интернет возможно. С 1 января 2016 года в Российской Федерации действует закон о «праве на забвение».

Вы имеете право потребовать у поисковой системы удалить из результатов поиска ссылки на материалы, в которых речь идет о вас. При этом информация должна быть недостоверной, устаревшей (трехлетней давности или более ранней) или противоречить законам РФ.

Важный нюанс: *контент не смогут удалить с сайта, на котором он размещен, но информация пропадет из поисковой выдачи.* Чтобы выйти на нее, понадобится знать точный адрес прямой ссылки. Контент, который вы просите удалить, должен иметь прямое отношение лично к вам: Ф. И. О. или внешность (если речь идет о фотографиях и видео) того, о ком идет речь в публикациях, должны совпадать с вашими.

Нельзя требовать удаления материалов, в которых есть признаки уголовных преступлений, если срок привлечения к ответственности по ним еще не вышел. То есть если о вас написали, что

вы украли велосипед из магазина игрушек, ссылки на статьи об этом можно будет удалить только после того как (и если) вы докажете свою невиновность. Также нельзя требовать удаления материалов, где говорится о вашей судимости, если она не снята и не погашена.

Что важно помнить:

- Закон о «праве на забвение» не позволяет удалить информацию, но помогает существенно затруднить ее поиск.
- Закон относится к российским поисковым системам и иностранным поисковикам, ведущим коммерческую деятельность на территории России.
- Собственные поисковые системы сайтов (например, блогов и социальных сетей) не попадают под действие закона. Исключение: сайты, в которые встроен поиск «Яндекса».
- Требовать у поисковика удалить нежелательный контент по закону о «праве на забвение» может только физическое лицо. Юридическим лицам придется сразу обращаться в суд.
- Если заявление хочет подать несовершеннолетний, ему нужно попросить об этом родителей или официального опекуна.
- Поисковик не имеет права разглашать информацию о том, что вы обратились с просьбой удалить информацию о себе.

3. Дополнительные материалы для проведения уроков по интернет-безопасности и внеурочной работы

Примерные правила поведения в сети для подростков (по версии портала Mel.fm):

1. Говори в Сети только то, что скажешь, глядя в глаза.
2. Не показывай информацию о себе никому, кроме близких друзей.
3. Не трави других.
4. Травят тебя — закрывай аккаунт.
5. Не рассказывай о себе незнакомцам.
6. Важно сказать «нет» предложениям о переписке, звонке, встрече.
7. Троллинг — не повод для нервных потрясений.
8. У шутки могут быть далеко идущие последствия.
9. За экраном такие же люди, как ты, помни об этом всегда.

Вы можете сформулировать собственные правила, используя в работе следующие кейсы.

№ 1. Ученица 5-го класса рассказала своему классному руководителю, что группа ее одноклассников снимает на фото и видео все, что происходит на перемене. Чтобы было, что снимать, они берут чей-нибудь рюкзак, оставленный в коридоре, выбрасывают его в урну для мусора и ждут, когда владелец рюкзака начнет его искать. Фото и видео ученики выкладывают в разные социальные сети.

Может ли подобное произойти с вами?[1]

[1] Методические рекомендации по обеспечению информационной безопасности обучающихся при работе в сети Интернет: [Электронный ресурс]. СПб: ГБУ ДПО «СПбЦОКОиИТ», 2018. URL: https://umr.rcokoit.ru/pages/methodical-cabinet-is-network.html.

№ 2. К психологу школы за советом обратился ученик 8-го класса. Школьник рассказал, что около двух недель назад по электронной почте он получил приглашение от своего друга поиграть в интернет-игру, доступ к которой открывается по прикрепленной ссылке. Перейдя по указанной в письме ссылке, в появившемся окне подросток подтвердил свое участие, нажав какую-то кнопку. Игра оказалась очень увлекательной, но спустя день на электронную почту пришло письмо с незнакомого адреса с требованием оплаты участия. Ученик его проигнорировал, письма, содержащие угрозы благополучию его семьи, стали появляться каждый день. Со слов ребенка, он должен уже около 100 000 рублей. Родителям рассказать боится. Что предпринять, не знает.

Как вы думаете, чего ему не следовало делать? Может ли это произойти с вами?[2]

№ 3. После первой четверти к директору школы обратилась мама новенькой девочки из 10-го класса. Мама сообщила, что в социальной сети появилась группа под названием «Ненавижу новенькую», к которой присоединилось 60% класса. В группе публикуются сведения, порочащие девочку. На телефон ребенку приходят СМС с угрозами и требованиями покинуть класс. Ребенок уходить из класса и из школы не хочет, однако эмоциональное состояние девочки беспокоит маму. Разговор с классным руководителем не привел к положительному результату.

Какой совет вы бы дали?[3]

---

[2] Методические рекомендации по обеспечению информационной безопасности обучающихся при работе в сети Интернет: [Электронный ресурс]. СПб: ГБУ ДПО «СПбЦОКОиИТ», 2018. URL: https://umr.rcokoit.ru/pages/methodical-cabinet-is-network.html.

[3] Методические рекомендации по актуализации (проектированию) содержания программ повышения квалификации педагогических и руководящих работников образовательных организаций по вопросам организации информационной безопасности обучающихся при работе в сети Интернет: [Электронный ресурс]. СПб: ГБУ ДПО «СПбЦОКОиИТ», 2018. URL: https://umr.rcokoit.ru/upload/editor/files/methodical_cabinet/information_security/2018/mr-new-2018.pdf.

№ 4. Однажды вечером Аня обнаружила, что кто-то взломал ее аккаунт, разместил на стене неприличные изображения и стал рассылать оскорбления ее друзьям в личной переписке. Аня восстановила доступ к аккаунту и поменяла пароль, но было уже поздно. Многие удалили ее из друзей и добавили в черный список, а кто-то даже перестал разговаривать в школе.

Что следует сделать Ане для того, чтобы восстановить свою репутацию? Как предотвратить подобную ситуацию?[4]

№ 5. Вадиму 14 лет, он хорошо учится, занимается карате, живет рядом со школой. Выходя из школы после уроков, он встретил свою бабушку, которая расспросила его о школе, поправила шарф, а на прощание поцеловала. Эту сцену сняли на видео его одноклассники, поместили в социальную сеть и подписали «у Вадима новая подружка!». Когда Вадим узнал, кто это сделал, он сильно избил одноклассника. Из-за этого его отстранили от участия в соревнованиях.

Кто пострадал в этой ситуации? Кто поступил неправильно? Как вы бы поступили в данной ситуации?

№ 6. В 9-м классе школы учились две подруги, Катя и Оля. Под большим секретом Катя рассказала Оле, что ей нравится Игорь из 11-го класса. Оля не удержалась и рассказала об этом одной знакомой в социальной сети, и скоро это стало известно всем. Над Катей стали смеяться, она очень разозлилась и стала писать про Олю всякие гадости в Интернете. Родители Оли обратились к классному руководителю и директору школы. В итоге Катя была вынуждена перейти в другую школу.

Кто пострадал в этой ситуации? Кто поступил неправильно? Как вы бы поступили в данной ситуации?

---

[4] Тест по теме: «Оценка уровня цифровой грамотности»: [Электронный ресурс] // ООО «Инфоурок». URL: https://infourok.ru/test-po-teme-ocenka-urovnya-cifrovoy-gramotnosti-2295839.html.

№ 7. Представьте, что у вашей младшей сестры появился собственный компьютер. Родители разрешили ей пользоваться им самостоятельно, но договорились, что она будет проводить за ним не более 30 минут в день. Вас попросили настроить домашний компьютер так, чтобы она могла им пользоваться максимально безопасно. Какие настройки вы будете использовать?[5]

№ 8. Вы были в гостях у знакомого и немного поработали за его компьютером — искали информацию, заходили в свой почтовый ящик и аккаунт социальной сети. Какие настройки браузера вы можете использовать, чтобы ваша информация осталась конфиденциальной?[6]

№ 9. Вы обнаружили бесплатную точку Wi-Fi и подключились к ней. Что вы можете не опасаясь делать в Интернете? Какие ваши действия могут оказаться опасными? На что нужно обращать внимание при работе в Интернете через общественное Wi-Fi-подключение?[7]

№ 10. Вы искали нужную книгу в Интернете, нашли и решили скачать, но тут возник баннер, заблокировавший весь экран, с надписью Microsoft Security. На баннере также написано, что необходимо пополнить счет, отправив СМС на номер NNNN, чтобы получить код разблокировки. Стоимость СМС — 600 рублей.

Что предпринять, чтобы решить проблему? Послать ли СМС на номер? Что нужно сделать, чтобы больше не попадать в такие неприятные ситуации?

---

[5] Интернет: возможности, компетенции, безопасность. Методическое пособие для работников общего образования. Часть 1. Практикум: [Электронный ресурс]. М.: Google, 2013. URL: https://26315s014.edusite.ru/DswMedia/internet_vozmojnosti-kompetencii-bezopasnost-chast-1.pdf.

[6] Там же.

[7] Там же.

№ 11. Паша подготовил доклад об игуанах для выступления на уроке биологии. Для своей презентации ученик скопировал несколько фотографий с сайтов, где искал информацию, а также несколько найденных с помощью поиска Google среди картинок фотографий игуан. Паша дал ссылки на изображения в презентации. Кроме того, мальчик включил в презентацию несколько фотографий домашней игуаны своего друга Васи, которые скопировал из Васиного профиля в социальной сети, попросив у него разрешения на использование фотографий. В презентации школьник использовал книгу известного ученого-исследователя, жившего в XIX веке, а именно: взял отрывки с описанием исследования игуан, живших в неволе, а также процитировал слова ученого. Чтобы соблюсти правила цитирования, Паша указал имя и фамилию ученого, оформил текст кавычками, а книгу добавил в список использованной литературы. Презентация настолько понравилась учителю биологии, что он помог Паше опубликовать ее в школьном журнале «Биология глазами школьника».

Нарушил ли Паша чьи-то авторские права при подготовке презентации? Если да, то каким образом? В каких случаях Паше стоит быть более внимательным?

№ 12. Илья хочет приобрести в подарок своему отцу новый смартфон. Полчаса поисков наиболее выгодного по стоимости смартфона привели Илью на сайт интернет-магазина, предлагающего современные устройства по низкой цене.

О магазине. Мы находимся в г. Калининград и успешно работаем с 2005 года! Аппараты были изъяты у различных фирм и предпринимателей при попытке контрабандного ввоза в Россию, без уплаты таможенной пошлины и соответствующих налогов. Наша цель - максимально быстро реализовать товар, поэтому мы устанавливаем столь доступные цены. На весь товар предоставляется гарантия 1 год. Мы всегда отправляем заказы своим клиентам посылкой с описью вложения содержимого. В этом

случае сотрудники почты обязаны в Вашем присутствии вскрыть посылку до оплаты наложенного платежа, чтобы сверить содержимое посылки с описью. Таким образом, Вы сможете убедиться, что в посылке действительно находится мобильный телефон или планшетный компьютер надлежащего качества. Данные условия гарантируют отсутствие в изделии дефектов и удовлетворяют законным требованиям Потребителя в течение гарантийного срока с момента передачи товара потребителю.

Доставка и оплата. Доставка осуществляется Почтой России или курьером службы экспресс-доставки DHL по всей территории РФ и СНГ. Самовывоза нет. Оплата только через QIWI кошелек (VISA QIWI Wallet).

СПОСОБЫ ДОСТАВКИ:

1. Доставка курьером экспресс-почты DHL: 1-3 дня (только при условии полной предоплаты заказа).

2. Доставка бандеролью наложенным платежом: 7-20 дней (требуется оплата гарантийного взноса 500 рублей). Гарантийный взнос — это обязательное и неоспоримое условие, которое гарантирует серьезность Вашего намерения приобрести товар. Экспресс-доставка курьером DHL также осуществляется бесплатно, но только после полной предоплаты заказа.*

3. Если Вы выбрали способ «доставка наложенным платежом», то при получении посылки Вас попросят оплатить наложенный платеж в кассе почтового отделения. Для чего требуется гарантийный взнос: это вынужденная мера с нашей стороны, поскольку у нас часто бывают случаи, когда заказчик по независящим от нас причинам не является на почту и не выкупает посылку с заказом, в результате чего нам приходится платить за пересылку посылки в оба конца + почтовый сбор за хранение посылки на почте сверх установленного срока. В связи с этим, чтобы избежать лишних финансовых потерь, мы просим Вас оплатить гарантийный взнос. Схема здесь действует следующая: если Вы не являетесь на почту и не выкупаете посылку, то сумма гарантийного взноса покрывает наши расходы, затраченные на пересылку товара в оба конца. Никакого перерасхода с Вашей стороны не будет, так как при отправке заказа

сумма гарантийного взноса вычитается из его стоимости. Просим Вас с пониманием отнестись к данным условиям.

Какая информация на сайте не вызывает вашего доверия? Каким образом можно проверить добросовестность интернет-магазина?[8]

№ 13. Маша (14 лет) очень переживала, когда рассталась со своим молодым человеком. Чтобы разобраться в причинах расставания, она искала в Интернете информацию об отношениях и на одном из форумов увидела историю девушки, как две капли воды похожую на то, что произошло с ней. Маша написала этой девушке (ее звали Вика), и Вика ей ответила. Они вместе обсуждали произошедшее, делились чувствами и переживаниями, обсуждали темы, которые больше ни с кем не решались обсудить. В одном из сообщений Вика написала, что, чтобы забыть их несчастную любовь, им нужно найти себе какое-то занятие, увлечение. Вика сказала, что недавно нашла очень хорошую студию танцев, и предложила Маше пойти туда вместе.

Стоит ли Маше согласиться на встречу? Что вас настораживает в ситуации? Доверяете ли вы Вике? Какие могут быть последствия встречи? Какими способами Маша могла бы себя обезопасить?

№ 14. Неделю назад в социальной сети к Наде (12 лет) в друзья добавился Саша, 13 лет. Надя не знала его лично, но видела, что он есть в друзьях у шести ее близких знакомых, поэтому подтвердила заявку Саши. Он написал, что ему очень понравилась Надя на какой-то из фотографий в профиле их общих друзей, и хотел бы познакомиться с ней поближе. Саша прислал Наде множество сообщений, и она рассказала ему многое о себе: чем она увлекается, про свою школу и семью, где она живет и где любит отдыхать. Они даже обменялись номерами телефонов и несколько раз созванивались. Саша

[8] Методические рекомендации по организации и проведению в общеобразовательных организациях Российской Федерации Всероссийского урока безопасности школьников в сети Интернет. М.: ФГАОУ АПК и ППРО, 2015.

кажется Наде очень внимательным и заботливым молодым человеком, ей нравится, что он в нее влюблен. Вчера Саша наконец пригласил Надю на свидание: предложил сходить в кино на вечерний сеанс. Надя очень обрадовалась.

Стоит ли Наде согласиться на встречу? Что вас настораживает в ситуации? Доверяете ли вы Саше? Какие могут быть последствия встречи? Какими способами Надя могла бы себя обезопасить?

Полезные материалы для подготовки уроков и мероприятий, посвященных Интернет-безопасности школьников.

1.https://xn--b1aew.xn--p1ai/Internet_for_kids– Официальный портал МВД России «Безопасный Интернет – детям».

2.https://www.saferunet.ru/ – Центр безопасного Интернета в России.

3.http://i-deti.org/ – Безопасный Интернет для детей: законодательство, советы, мнения, международный опыт.

4.http://www.fid.su/ – Фонд развития Интернет.

5.http://www.ifap.ru/library/book099.pdf– «Безопасность детей в Интернете», компания Microsoft.

6.http://www.oszone.net/6213/ – «Обеспечение безопасности детей при работе в Интернет».

7.https://www.google.ru/safetycenter/families/start/basics/ – Центр безопасности Google.

8.http://shperk.ru/sovety/avtoritet.html – Как отличить фейк от настоящего материала? Дело о летающем дьяке Крякутном.

9.http://habrahabr.ru/company/mailru/blog/252091/ – «Безопасность в интернете: готовы ли пользователи противостоять киберугрозам?».

10.https://pandia.ru/text/78/639/36613.php – Урок безопасности «Правила общения в Интернете!» (для подростков 12-15 лет).

11.https://lenvhtl.edumsko.ru/uploads/2000/1188/doc_norm/perechen_meropriyatij_bezopasnost_v_internete.pdf – Программа мероприятий по безопасности в сети Интернет. Муниципальное автономное общеобразовательное учреждение «Видновский художественно-технический лицей».

12.https://proshkolu.ru/user/litvinatm59/blog/144290/ – Тренинг «Безопасность в сети Интернет».

ДЛЯ ЗАМЕТОК

ДЛЯ ЗАМЕТОК

ФОНД
НАЦИОНАЛЬНЫЕ
РЕСУРСЫ
ОБРАЗОВАНИЯ

www.nro.center