Министерство просвещения и воспитания Ульяновской области

ОГБНОУ Центр ППМС «Развитие»

Центр информационной безопасности детей

Методические рекомендации по основам информационной безопасности для обучающихся общеобразовательных организаций

Ульяновск, 2021 г.

Методические рекомендации направлены на организацию преподавания основ информационной безопасности в общеобразовательных организациях.

Задачи методических рекомендаций:

1. Оказание методической поддержки педагогических работников и сотрудников образовательных организаций России с целью организации обучения детей и их родителей (законных представителей) информационной безопасности;
2. Использование современных технологий и методик в организации обучения детей, в частности в рамках межпредметного обучения, внеурочной деятельности и других форм обучения;
3. Повышение уровня информационной грамотности педагогических работников и сотрудников администрации общеобразовательных организаций Российской Федерации в части тематических положений приказа Министерства труда и социальной защиты РФ от 18 октября 2013 г. N 544н"Об утверждении профессионального стандарта "Педагог (педагогическая деятельность в сфере дошкольного, начального общего, основного общего, среднего общего образования) (воспитатель, учитель)", ФГОС ООО, ФГОС НОО и ФГОС СОО;
4. Оказать методическую помощь администрациям образовательных организаций в организации обучения детей, их родителей (законных представителей) и педагогических работников информационной безопасности;
5. Формирование тем и вопросов по вопросам информационной безопасности для включения в тематические учебники, учебные пособия и другие учебно-методические материалы.

Методические рекомендации направлены на организацию обучения детей по следующим направлениям:

1. Организация обучения в рамках действующих учебных предметов и(или) использования межпредметного обучения;
2. Организация обучения в рамках части основной образовательной программы, формируемой участниками образовательного процесса, включая организацию отдельных учебных предметов, учебных курсов и внеурочную деятельность;
3. Организация обучения в рамках дополнительного образования.

Методические рекомендации ориентированы на следующие аудитории (далее - педагогические работники):

1. Учителя, преподаватели и классные руководители;
2. Сотрудники администрации образовательных организаций по учебно-воспитательной работе, по воспитательной работе и безопасности образовательного процесса и обучающихся;
3. Ответственные лица в штате образовательных организаций в части психологического и воспитательного взаимодействия с обучающимися и педагогами (педагоги-организаторы, психологи, методисты и другие сотрудники образовательных организаций);
4. Ответственные лица в штате образовательных организаций в части дополнительного образования обучающихся и организации внеурочной деятельности.

Кроме этого, данные методические рекомендации могут быть использованы:

1. администрациями учреждений для детей-сирот и детей, оставшихся без попечения родителей;
2. организациями дополнительного образования;
3. профессиональными образовательными организациями;
4. и другими организациями, осуществляющими образовательную деятельность для несовершеннолетних обучающихся.

Методические рекомендации содержат общие представления о сферах безопасности в информационном пространстве и мерах, которые реализуются в образовательной среде для обеспечения информационной безопасности обучающихся.

Методические рекомендации имеют следующую структуру:

1. Раздел «Актуальность информационной безопасности детей» направлен на ознакомление педагогических работников основными причинами актуальности информационной безопасности детей, действующим законодательством и положениями нормативно-правовых актов, затрагивающих данную сферу;
2. Раздел «Основные аспекты информационной безопасности» содержит описание всех аспектов информационной безопасности, и некоторые вопросы обеспечения информационной безопасности детей для родителей (законных представителей);
3. Раздел «Организация обучения детей и родителей (законных представителей)» направлен на предоставление педагогическим

работникам и сотрудникам образовательных организаций информации о различных механизмах организации обучения обучающихся и их родителей (законных представителей).

В приложении к методическим рекомендациям представлен перечень источников, используемых при подготовке методических рекомендаций, а также методические разработки для организации и проведения мероприятий с обучающимися разных возрастов.

Актуальность информационной безопасности детей

Дети и подростки — активные пользователи интернета как в мире, так в Российской Федерации.

Доступ несовершеннолетних к сайтам в сети «Интернет» дает им возможность изучать образовательный контент, общаться с ровесниками, самостоятельно обучаться, узнавать о проводимых конкурсах, олимпиадах, принимая в них участие, и использовать сеть «Интернет» в качестве источника для собственного развития.

Однако использование Интернета вместе с возможностями несет и риски, такие как:

1. Издевательство ровесниками и незнакомцами в сети над ребенком;
2. Воровство его аккаунтов, денег и личных данных;
3. Втягивание ребенка в асоциальную деятельность (группы смерти, группы с рекламой наркотиков и т.д);
4. Прочтение детьми информации, вредящей их мировоззрению и психотическому состоянию.

По данным исследования Центра информационной безопасности детей Ульяновской области «Изучение сфер жизнедеятельности несовершеннолетних в сети «Интернет», более половины учащихся сталкиваются с негативной информацией и травлей в сети Интернет.

По данным исследования «Образ жизни российских подростков в сети» у 87% процентов детей возникали различные проблемы в сети «Интернет» только за последний год, однако только 17% рассказали о них своим родителям по следующим причинам:

1. Уверенность детей в незнании родителями решения их проблем;
2. Страх перед родителями;
3. Отсутствие возможности рассказать и поделиться с родителями своими проблемами.

По этой причине образовательные организации должны осуществлять профилактику и обучение детей навыкам безопасного использования сети Интернет и информирование их родителей (законных представителей) о возможных сетевых рисках.

Формирование информационной и цифровой грамотности населения, а особенно детей как одной из самых социально незащищенных категорий населения, является одним из важнейших факторов не только для сохранения информационного суверенитета нашей страны и формирования всех сфер информационного общества, но и для обеспечения развития цифровой экономики.

В настоящее время различные федеральные законы, нормативно-правовые акты и их положения, затрагивают вопросы обеспечения безопасности детей в информационном пространстве.

Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации" определяет механизм физического ограничения доступа к запрещенной информации в сети «Интернет». Данный механизм предусматривает создание федерального реестра сетевых адресов, доменных имен и указателей страниц, содержащих информацию, распространение которой в России запрещено - Единый реестр доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено.

Федеральный закон от 29.12.2010 N 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» регулирует отношения, связанные с защитой детей от информации, причиняющей вред их здоровью и (или) развитию, в том числе от такой информации, содержащейся в информационной продукции.

Федеральный закон №436 определяет перечень запрещенной для детей информации, возрастные категории детей и виды информации, разрешенной для той или иной категории, а также требования к обороту информационной продукции.

Согласно пункту 1 статьи 14 Федерального закона от 24.07.1998 N 124-ФЗ "Об основных гарантиях прав ребенка в Российской Федерации" органы государственной власти Российской Федерации принимают меры по защите ребенка от информации, пропаганды и агитации, наносящих вред его здоровью, нравственному и духовному развитию, в том числе от национальной, классовой, социальной нетерпимости, от рекламы алкогольной продукции и табачных изделий, от пропаганды социального, расового, национального и религиозного неравенства, от информации порнографического характера, от информации, пропагандирующей нетрадиционные сексуальные отношения, а также от распространения печатной продукции, аудио- и видеопродукции, пропагандирующей насилие и жестокость, наркоманию, токсикоманию, антиобщественное поведение.

В области образования вопросы обучения детей информационной безопасности также нашли свое отражение.

Федеральный государственный образовательный стандарт основного общего образования в части результатов освоения основной образовательной программы подчеркивает важность обучения детей навыкам и знаниям обучающихся в сфере информационной безопасности.

Основные аспекты информационной безопасности

В данном разделе будут рассмотрены аспекты информационной безопасности, разделенные на блоки:

1. Безопасность в цифровой среде
2. Опасные программы и явления цифровой среды
3. Опасный контент и опасные персоны
4. Деструктивные течения и защита от них
5. Безопасное поведение

1. Безопасность в цифровой среде

Пользуясь различными гаджетами, подключаясь к и Интернету, мы погружаемся в цифровую среду - быстро меняющееся и динамично реагирующее на наши запросы пространство, которое формируют интернет-сайты, поисковые машины, социальные сети и форумы, мессенджеры, компьютерные игры, мобильные приложения, электронные почтовые сервисы, видеохостинги и т.д.

Цифровая среда - пространство, доступ в которое осуществляется посредством электронных устройств и в котором с помощью программных средств происходит активное взаимодействие людей между собой и ли людей с электронными сервисами: создание поисковых запросов и получение информации по ним, публикация постов, фото- и видеоматериалов, отправка сообщений.

В цифровой среде люди выступают как цифровые сущности - аккаунты и профили (анонимные или персональные). Пользователь цифровой среды действует в ней, с одной стороны, как активный потребитель информации (выбирает контент, формирует поисковые запросы), а с другой стороны, как создатель и распространитель контента (размещает сообщения, комментарии, фото и видео и т.д.).

Большинство интернет-пользователей чувствуют себя в цифровой среде достаточно защищёнными, однако, несмотря на то что в виртуальном пространстве действуют государственные законы, общепринятые нормы поведения и даже формируются новые правила (сетевой этикет), гарантий полной безопасности не существует.

Это обусловлено совокупностью факторов:

1. В цифровом пространстве отсутствует контакт «лицом к лицу». Замена его взаимодействием цифровых сущностей создаёт иллюзию анонимности, что снижает у некоторых людей степень ответственности за свои поступки и вызывает желание нарушить правила поведения и этические нормы, которые в реальной жизни они, как правило, соблюдают.
2. Другое заблуждение, свойственное пользователям цифровой среды, - иллюзия приватности - необоснованная уверенность пользователя в том, что он полностью контролирует размещённую в цифровом пространстве им самим информацию, включая персональную. Многие беспечно относятся к необходимости защитить свои персональные данные или данные, по которым его можно идентифицировать, а затем получить и другую информацию: узнать адрес, режим жизни, хобби и т.д. сведениями личного характера могут воспользоваться злоумышленники в корыстных целях.
3. При работе в цифровом пространстве каждый должен помнить о реально существующей угрозе заражения цифровых устройств вредоносными программами, которые могут вывести технику из строя и ли привести к потере пользователем важных для него данных.

4. В цифровом пространстве присутствуют опасные персоны, противоправную деятельность которых полностью предотвратить не возможно.

Об обеспечении безопасности в цифровой среде заботятся как на индивидуальном, так и на общественном и государственном уровнях: принимаются специальные цифровые законы, выпускаются антивирусные программы, владельцы социальных сетей разрабатывают и регулярно обновляют правила поведения в них. Но эти меры не могут гарантировать полной защищенности в цифровой среде, и каждый пользователь должен лично принимать участие в обеспечении собственной безопасности. Для защиты от каждого вида опасности разработаны свои приёмы, а если избежать ее не удалось, применяют специальные механизмы/ алгоритмы решения проблемы.

Основные опасности цифровой среды

Риски, присущие цифровому пространству и так или иначе воздействующие на находящегося в этом пространстве человека, можно разделить на две большие группы:

1. Электронные риски, или кибер-риски, угрожающие самому устройству (смартфону, планшету, ноутбуку), установленным на нем программам, банковским счетам, паролям (программы-трояны, вирусы, кибератаки) и т.п.
2. Информационные риски, угрожающие сознанию владельца цифрового устройства (определённый контент может вызвать у человека цифровую зависимость, привести к разрушению его когнетивных способностей и даже произвести прямые атакующие действия на сознание), фальшивые новости (фейкньюс), опасный контент.

Наибольшую опасность представляют информационные риски, угрожающие целостности сознания и здоровью пользователей цифровой среды.

Развитие и широкое распространение информационных технологий сформировало серьёзную социальную и медицинскую проблему - цифровую зависимость. В большинстве случаев формирование цифровой зависимости долгое время не осознаётся самим человеком и он предпочитает не замечать ее, считая постоянную погруженность в цифровую среду нормой современной жизни.

Многие из описанных ниже проявлений цифровой зависимости присущи большинству наших современников, однако это свидетельствует не о норме, а о степени распространенности этого явления. Обратите внимание, если человек:

- часто бесцельно и хаотично ищет что-то в Интернете;
- постоянно и подолгу переписывается в мессенджерах и чатах;
- много времени (более 7-8 часов каждый день) проводит за компьютерной игрой (или игрой на смартфоне), интернет-серфингом и общением в социальных сетях;
- беспрерывно смотрит видеоролики/ фильмы/ сериалы через Интернет;
- совершает множество бесконтрольных покупок в Интернете (оформляет множество платных подписок);
- имеет пристрастие к постоянному чтению новостей, отдавая предпочтение «горячим» и негативным новостям.

Это повод задуматься о здоровье человека, его психологическом и социальном благополучии.

Безусловно, автоматически объявлять зависимым человека, который пользуется смартфоном или получает информацию в Интернете, не стоит, но следует иметь ввиду, что чрезмерное погружение в цифровую реальность чревато привыканием к такому времяпрепровождению.

Основные признаки цифровой зависимости:

1. Придание сверхзначимости постоянному присутствию и общению в социальных сетях, непрерывному ознакомлению с лентами новостей и т.п.
2. Формирование эмоциональной зависимости, колебания настроения в зависимости от возможности присутствия в Интернете.
3. Потребность в увеличении времени присутствия в Интернете и частоты использования разнообразных устройств доступа в цифровую среду.
4. Возникновение «синдрома отмены» - ухудшение самочувствия при отсутствии возможности доступа в цифровую среду.
5. Возникновение нарушений (недоразумений и конфликтов) в общении в обычной жизни.
6. Потеря самоконтроля, возникновение срывов и рецидивов при попытках отрегулировать время присутствия в цифровой среде.

Дополнительные признаки цифровой зависимости:

1. Ухудшение состояния здоровья (набор или потеря веса, мышечные боли и т.д.), психологическая нестабильность (апатия, тревога, депрессия).

2. Нарушение привычного ритма жизни, пренебрежение семейным и дружеским общением, отказ от ранее любимых увлечений.

3. Использование различных ухищрений и обмана с целью получения доступа в Интернет.

Одной из разновидностей цифровой зависимости является игромания.

Игромания - патологическая склонность к играм (как к видеоиграм, так и азартным играм), в цифровой среде выражается в навязчивой потребности играть в онлайн-, видеоигры и другие игры.

По мнению экспертов в области психического здоровья, чрезмерное увлечение видеоиграми, особенно жестокими, не обязательно приведёт к расстройству, но с большей вероятностью сможет оказать негативное влияние на психику.

К информационным рискам, помимо цифровой зависимости, относится *опасный контент* - информационные материалы, способные причинить моральные страдания человеку, нанести урон его психике. Некоторые виды такой информации законодательно запрещены, а где-то допускаются к распространению с возрастными ограничениями.

В цифровой среде, особенно в социальных сетях можно столкнуться с хищными персонами (манипуляторами, мошенниками, интернет-тролями и даже просто неуравновешенными людьми), которые, прячась за аватарками и никами, создают фальшивые профили, причиняют вред пользователям Интернета.

Другой формой информационных рисков является *опасное поведение* в Интернете, способное привести к правонарушению. Необходимо помнить о том, что при необдуманном поведении в Сети можно незаметным для себя образом превратиться в нарушителя закона. Это может произойти как по неосмотрительности, так и в результате чьей-либо провокации.

Электронные риски наносят человеку не столь значимый урон, как информационные (поскольку угрожают не благополучию личности, а материальной составляющей жизни), тем не менее их нельзя не учитывать при взаимодействии с цифровой средой.

Существует ряд *опасных программ*, которые могут нанести вред электронному устройству, установленному на нем программному обеспечению или облегчают мошенникам доступ к данным пользователя, хранящимся на устройстве. Противостоять рискам заражения компьютера или гаджета опасными программами поможет соблюдение правил кибергигиены.

Помимо опасных программ, существуют опасные явления, такие ка к взлом аккаунта, спам, фишинг и другие виды мошенничества в цифровой среде. В своей преступной деятельности мошенники активно применяют знание психологии и могут сыграть в некоторых человеческих слабостях (интерес к скидкам, сомнительным способам обогащения, различным выгодным предложениям) либо вызвать чувство тревоги (угрозой блокировки банковских карт или сообщением о том, что близкий попал в беду и ему необходима помощь и т.п.). Противостоять таким угрозам поможет критическое отношение ко всем входящим сообщениям по электронной почте, телефону, в социальных сетях. Прежде чем предпринять какие-либо действия (перевести средства, заблокировать аккаунт и т.д.), следует удостовериться в истинности информации (перезвонить в банк, родственнику, другу).

2. Опасные программы и явления цифровой среды

Современные электронные устройства (компьютеры, планшеты, смартфоны, смарт-часы, телевизоры, подключаемые к Интернету, умные колонки и прочие устройства «умного дома») требуют не только подзарядки аккумуляторов, но и постоянного скачивания обновлений для установленных на них операционных систем, программ и приложений. Существует множество полезных программ, которые помогают в работе с текстовыми документами, таблицами, в обработке фото- и видеофайлов. Тем не менее важно знать, что скачивая программы и приложения, пересылая друзьям и получая от них фотографии, забавные картинки, новостные материалы, тексты контрольной работы (домашнего задания), пользователь может запустить в свое устройство вредоносную программу, которая будет собирать данные о пользователе или нарушит работу устройства.

Программами принято называть программное обеспечение (ПО), используемое на компьютере.

Приложениями принято называть ПО, используемое на смартфонах и планшетах.

Вредоносное программное обеспечение - программы, предназначенные для осуществления несанкционированного доступа к информации или ресурсам информационной системы и/или воздействия на них.

Наиболее распространёнными видами вредоносного ПО являются:

- *вирусы* - внедряются в программы и распространяются по каналам связи, могут удалять как отдельные файлы, так и всю операционную систему,

блокировать работу пользователей; кроме того, вирусы потребляют ресурсы системы и занимают место на накопителях информации;

- *троянские программы (или трояны)* - проникают в компьютер под видом легального ПО, могут собирать данные банковских карт, нарушать работоспособность компьютера и даже использовать IP-адрес пользователя.

Самой коварной вредоносной программой является троян: он способен имитировать не только имя, но и иконку любой программы или файла, предлагая себя для запуска пользователем и скрывая присутствие в системе.

В бытовом общении понятия «вредоносное ПО» и «вирусы» употребляются как синонимы, однако следует иметь ввиду, что вирусы - одна из разновидностей вредоносных программ.

Не всегда вредоносные программы и приложения создаются с целью получить несанкционированный доступ чужому устройству. Главный вред от них заключается в расфокусировке внимания пользователя. Осуществляется это таким образом: программы собирают информацию о вашей активности, запоминают, какие сайты вы посещаете, какими темами интересуетесь, а затем основываясь на этих данных, показывают ненужную рекламу, вызывающий контент (например, «желтые новости» - новости, основанные на слухах, сенсациях, скандалах, зачастую не имеющие ничего общего с реальностью).

Опасные явления: фишинг, мошенники, спамеры

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

Социальная инженерия - совокупность приёмов, направленных на получение несанкционированного доступа к конфиденциальной информации и основанных на знании особенностей психологии людей.

Мошеннические схемы и технологии постоянно совершенствуются. Так, например, преступникам ничего не стоит, подменив отображающийся у вас на экране номер или взломав аккаунт вашего друга, позвонить вам от его лица и попросить о чем-то, что повлечёт для вас неприятности.

Лучшей защитой от технологий социальной инженерии является критическое отношение ко всем входящим сообщениям. Если вас просят перевести деньги, сообщить какой-либо пароль, код, пришедший по смс, и т.п., то предпринимать действия рекомендуется только после проверки подлинности сообщения и его источника.

Нередки случаи, когда интернет-пользователь получает письмо (или сообщение в социальной сети) от банка, в котором у него оформлена карта (или интернет-магазина, в котором он делал заказ), содержащее ссылку на сайт этого банка (интернет-магазина). Адрес в ссылке будет практически не отличим от реального, визуально знакомого. Пройдя по этой ссылке, потенциальная жертва мошенничества попадает на страницу, где ей будет предложено заполнить специальную форму - ввести личные данные, данные банковской карты (номер, логин и пароль), номер телефона и др. Подобная мошенническая технология называется фишинг.

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

Другое распространённое явление в Интернете, которое можно назвать условно мошенническим, - спам.

Спам - массовая рассылка не запрошенных пользователем электронных писем и сообщений в мессенджерах.

Как правило, спам-сообщения носят рекламный или агитационный характер. Например, это может быть, как реклама новой акции в каком-либо магазине, так и жалостливое письмо с просьбой помочь человеку, попавшему в беду. Спам может нанести вред компьютеру и причинить неудобства его пользователю, так как на очистку почтово ящика уходит значительное количество времени, а открытие некоторых сообщений может повлечь за собой установку вредоносного ПО. Если попасть в базу рассылки спамеров, сообщения от них будут поступать постоянно.

Спам и фишинг - лишь две из множества разновидностей интернет-мошенничества. Несмотря на огромные усилия и финансовые вложения властей, руководителей компаний и частных пользователей, большее количество мошенников всевозможных мастей процветает в Интернете; они присутствуют во всех без исключения социальных сетях, онлайн-сервисах частных объявлений и мессенджерах.

Правила кибергигиены

Соблюдение ряда простых правил поможет вам если не полностью обезопасить компьютер и мобильное устройство, то по крайней мере снизить риск их заражения, а так же сохранить ваши средства и персональные данные.

Как и что скачивать:

- по возможности постоянно пользуйтесь антивирусным программным обеспечением, регулярно обновляйте его и не отключайте его;
- скачивайте только проверенные программы и приложения из надежных источников, читайте отзывы о них (вас должно насторожить, если при установке приложение запрашивает слишком много прав, максимально урежьте их);
- скачивайте только те программы и приложения, которые вам действительно нужны;
- избегайте скачивания различных «расширений» и «улучшителей» функционала для широко распространённых приложений (WhatsApp, Instagram и др.).

Как защититься от вредного и вредоносного ПО:

- проверьте права установленных у вас приложений, поставьте ограничения, если вы забыли это сделать при установке;
- избегайте подписки на пуш-уведомления сайтов в браузерах (это наделит владельцев этих сайтов обширными возможностями).

Пуш-уведомления - небольшие всплывающие окна на экране вашего устройства. Уведомления могут выводиться на экран любого устройства, имеющего область оповещения.

Как защититься от мошенников, стремящихся воспользоваться личными данными:

- не рекомендуется переходить по ссылкам и заполнять формы, в которых необходимо указывать личные данные. Если Вам нужно выполнить какие-либо операции с банковской картой, самостоятельно сделайте это с помощью официального сайта банковского учреждения;
- номер и пин-код банковской карты, логины и пароли от личных кабинетов должны знать только вы и на всякий случай ваши родители (соответственно на письма, сообщения или звонки с просьбой уточнить/перепроверить/подтвердить личные данные отвечайте отказом, а о поступившем предложении сообщите взрослым);

- не храните пин-коды от карт рядом с самими картами. Запишите в мобильный телефон номер службы поддержки банка или установите мобильное приложение от банка, чтобы в случае утери/кражи карты можно было сразу же обратиться в банк и заблокировать ее;
- не разрешайте фотографировать ваши документы и банковские карты, если кто-то предпринимал такие попытки, сообщите об этом взрослым;
- относитесь к копиям ваших документов (электронным и бумажным) также внимательно, как и к самим документам, не оставляйте их навиду и постарайтесь не пересылать их по электронной почте и через мессенджеры;
- относитесь критически к электронным письмам с незнакомых адресов, не открывайте их;
- если вам на почту/мессенджер пришло письмо/ сообщение от имени финансового учреждения с просьбой перейти по определённой ссылке и заполнить некоторую форму, перенаправьте это письмо в службу безопасности финансового учреждения (как правило, контакты таких учреждений находятся в открытом доступе); таким образом вы поможете предотвратить мошеннические действия в отношении как себя, так и других пользователей;
- если не хотите получать уведомления от компаний/интернет-магазинов и т.д., будьте внимательны и не соглашайтесь на рассылку от них (если это всё же произошло, попробуйте отписаться самостоятельно или направьте администраторам сайта письмо с просьбой исключить вас из списка рассылки).

Правила создания и хранения паролей:

- всегда придумывайте сложные пароли - комбинации различных символов, букв разного регистра, цифр;
- используйте разные пароли для разных устройств;
- периодически меняйте пароли;
- старайтесь не записывать пароли на листочках бумаги и не хранить их рядом с банковскими картами;
- используйте программы для хранения паролей.

Как защититься от спам-рассылки:

- если вам приходят письма/сообщения от неизвестных факторов, заблокируйте этих авторов, письма переместите в папку под названием «Спам» или удалите;
- постарайтесь без крайней необходимости не оставлять свои ФИО, номер телефона и адрес электронной почты при совершении покупок и прочих действий в Сети (это сократит количество ненужных звонков и спам-сообщений).

Одним из наиболее надежных способов защиты от спама является наличие двух адресов электронной почты. Первый e-mail следует использовать исключительно для ведения деловой переписки, а второй применять для подписок на различные сайты, каналы и т.п. именно такие адреса чаще всего подвергаются спам-атакам.

Как обезопасить себя при совершении операций на электронных торговых площадках:

- не вносите предоплату и не сообщайте данные своей карты, даже если покупка кажется вам очень выгодной (вас должно насторожить, если продавец создаёт иллюзию ажиотажного спроса на его товар, побуждая вас внести предоплату);
- внимательно читайте правила и условия пользования сайтами, если оставляете на нем свои персональные данные.

3. Опасный контент и опасные персоны

Для определения запрещенной или непозволительной с точки зрения общества содержательной составляющей информационного ресурса введено специальное понятие - шок-контент. К шок-контенту относятся сцены драк и избиения людей, жестокого обращения с животными, материалы, содержащие описание или визуализацию подобных событий. Шок-контент способен оказать разрушительное воздействие на психику человека: нанести психическую травму, вызвать чувство отчаяния, одиночества, страха, привести к длительному стрессу и т.д.

Шок-контент может присутствовать в кинофильмах и документальных фильмах, книгах и журналах, рекламе и других видах информационной продукции, включая интернет сайты и социальное сети. Как правило, его применение продиктовано желанием вызвать сильную эмоциональную реакцию зрителя (читателя), привлечь внимание, побудить к определенным действиям.

Просмотр шок-контента может стать причиной психического неблагополучия вплоть до психического расстройства личности.

Для защиты психического здоровья граждан правительство нашей страны на законодательном уровне ограничивает демонстрацию и распространение шок-

контента. С этой целью все информационные материалы классифицируются в соответствии с возрастными категориями аудитории.

Некоторые вида информации относятся к категории запрещённых для создания и распространения по причине их вредоносного воздействия на граждан и общество.

Основные виды опасного и запрещённого контента в Интернете:

1. Пропаганда экстремизма (экстремизм - противоправная деятельность, основанная на приверженности крайним взглядам и сопровождаемая публичными действиями, которые могут иметь насильственный характер, отрицать конституционные принципы, законные интересы человека, общества и государства).
2. Пропаганда наркотиков (распространение в различной форме сведений о наркотических средствах).
3. Демонстрация насилия над людьми (сцены причинения людям физического и эмоционального вреда, оправдание насилия и противоправного поведения).
4. Демонстрация жестокого обращения с животными (сцены причинения боли и/или страдания животному из хулиганских или корыстных побуждений, влекущих их увечье или гибель).
5. Вербовка в террористические организации (целенаправленное склонение, привлечение к участию в деятельности террористических организаций; среди молодёжи вербовка ведётся преимущественно в соцсетях).
6. Пропаганда нацистской символики (нацизм - идеология, ставящая во главу угла определённую нацию (национальность, расу) и призывающая к использованию репрессий по отношению к остальной части человечества).
7. Информация, отрицающая семейные ценности, традиционные представления о семье, способах семейного уклада.
8. Сквернословие (применение непристойных и бранных слов).

Полностью исключить опасный и запрещённый контент в Интернете сложно, но, соблюдая несложные принципы цифровой гигиены, может снизить риск столкновения с запрещённым и шок-контентом.

«Хищные персоны» в Сети: как распознать их и защититься от них

К Интернету имеют доступ более 4 млрд жителей планеты, и среди них есть люди, страдающие психическими расстройствами, тягой к насилию, имеющие преступные наклонности или злые намерения. Некоторые из них используют Сеть в качестве площадки для реализации своих замыслов или получения

эмоциональной разрядки. Люди, действующие таким образом, являются своего рода хищниками, и в Интернете, как и в живой природе, от хищников надо держаться подальше, а при вынужденном общении с ними быть начеку.

Самыми распространенными преступными приемами сетевых хищников являются мошенничество, кибербуллинг (кибербуллинг - понятие, пришедшее к нам из английского языка, калька слова cyberbullying, означающего «травля в Сети») и даже вербовка в деструктивные группы.

Кибербуллинг - агрессивное поведение в цифровом пространстве (киберпространстве) по отношению к кому-либо, осуществляемое, как правило, в течении продолжительного времени. Жертвой кибербуллинга чаще всего становятся подростки, самые активные и при этом наиболее уязвимые пользователи Сети. Травля может происходить посредством размещения агрессивных и нелицеприятных комментариев, постов, унижающих фото- и видеоматериалов в соцсетях.

Предотвратить травлю в соцсетях можно несколькими способами:

- заблокируйте учётные записи пользователей, ведущих себя агрессивно по отношению к другим посетителям;
- об известных вам фактах травли сообщите в администрацию используемой вами социальной сети.

Если вас вовлекают в конфликт, не спешите сразу блокировать свой аккаунт или аккаунт потенциального провокатора. Для начала попробуйте применить любые из указанных методов:

- *игнорируйте агрессора* (отсутствие реакции на его выпады лишит его возможности развивать агрессивный сценарий);
- *будьте подчёркнуто вежливы* (при вынужденном общении на любые выпады отвечайте вежливо, соблюдая правила речевого этике, - это поможет снизить градус агрессии);
- *переключите внимание собеседника* (задайте неожиданный вопрос, смените тему разговора, вспомните интересную или смешную историю - это поможет изменить тон и направление беседы);
- *положительно оцените личностные качества собеседника, точность его высказываний* (найдите, за что его поблагодарить, например, за подсказку, согласитесь с его высказыванием, хорошо отзовитесь о его речевых навыках), только не допускайте насмешек и подшучивания со своей стороны, чтобы не давать конфликту дальнейшего развития;
- *используйте позитивные смайлы* в ответ на агрессию;
- *предложите обидчику почувствовать себя на вашем месте* (возможно, он осознает некорректность своего поведения).

Очень часто травлей в сети занимаются дети и подростки с заниженной самооценкой или повергшиеся насилию (испытавшие на себе жестокое обращение). Как правило, агрессивное поведение является привычным и неосознаваемым способом защиты. Именно поэтому агрессор очень часто заслуживает жалости, а не того, чтобы перед ним трепетали от страха.

Другим опасным явлением в Сети является вербовка в различные организации и группы, чаще всего запрещённые, пребывание в которых может плачевно закончится для детей и подростков. Вербовщики никогда не действуют открыто и напрямую, поэтому их деятельность особенно опасна.

Осознать истинный размах деятельности вербовщиков тяжело, и чтобы не стать их случайной жертвой, важно быть внимательным и обращать внимание на некоторые характерные особенности поведения таких аккаунтов.

Что должно насторожить в поведении незнакомца:

- вне зависимости от расположения к нему пытается установить с вами дружеские отношения;
- настойчиво рекомендует изучить материалы по какой-то определённой тематике, присылает ссылки на книги, видео- и аудиозаписи, фотографии и т.п.
- пытается получить личную информацию: ФИО, адрес проживания, место учебы, хобби и др.;
- стремится ограничить общение с другими людьми, хочет стать избранным собеседником («Другие тебя не понимают, но я вижу, что ты - уникальная личность»);
- знает обо всем и может ответить на любой вопрос, но ответы чаще всего однообразны;
- пытается объяснить ваши чувства и эмоции;
- часто упоминает определённую группу (организацию), хвалит ее, говорит, что, вступив в неё, появится возможность реализоваться в интересующей области (как художник/писатель/спортсмен и т. д.).

Технологии защиты от опасных персон и плохого контента. Правила информационной гигиены

Размещая контент в Интернете, помните о том, что:

- за персональными данными могут охотиться мошенники и преступники (не размещайте их в открытом доступе, не отправляйте незнакомцам);
- даже личная переписка по тем или иным причинам может быть обнародована (следите за тем, что вы пишите);

- облачные сервисы хранения данных не дают полной гарантии их сохранности и защищенности от утечек информации;
- смелые фотографии, неосторожные высказывания и т. п., даже размещённые в закрытых (подзамочных) областях, могут быть вынесены на всеобщее обозрение и остаться в Сети навсегда (подумайте, может ли это как-то навредить вам сейчас или в будущем; как это скажется на вашей репутации).

Общаясь в цифровом пространстве, помните о том, что:

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

4. Деструктивные течения и защита от них

Деструктивное поведение - это разрушительное поведение, направленное вовне или на самого себя, препятствующее достижению позитивного решения задач и приводящее к нарушению физического, психического и социального благополучия.

Деструктивное поведение в Интернете может сформироваться под влиянием как отдельно взятых аккаунтов в социальных сетях, так и деструктивных течений, сообществ и субкультур, распространяющихся сегодня в Сети.

Деструктивные течения в Интернете - объединения, группы и сообщества прямо или косвенно задействованные в распространении деструктивного поведения и материалов (текстов, картинок, видеороликов), которые:

- запрещены на территории России;
- потенциально опасны для психического здоровья и благополучия;
- призывают к совершению действий, опасных для психического, физического и социального благополучия человека.

Деструктивные течения напрямую влияют на самих участников течений, а также опосредованно и на всех пользователей Интернета.

Как распознать деструктивную группу в социальных сетях

ЛЮБОЙ ИЗ ПРИЗНАКОВ ГОВОРИТ О ДЕСТРУКТИВНОСТИ	**Вас должно насторожить если...**	**Например**
	Сама группа признает свои материалы деструктивными или, наоборот, предупреждает о том, что не пропагандирует деструктив	«Мы не пропагандируем насилие. Группа носит информационный характер»
	В группе призывают к поведению, которое может негативно повлиять на психофизическое и социальное благополучие	Призывают к употреблению запрещённых препаратов или медицинских препаратов без рецепта врача
	В группе распространяют деструктивные материалы (текст, фото, видео и др.)	«Как изготовить оружие дома»
	Распространяют ссылки на источники деструктивных материалов	Ссылки на запрещённое видео с кадрами насилия
	Переносят общение из открытого пространства в закрытые чаты и личные сообщения в целях сокрытия обсуждения вопросов, прямо или косвенно являющихся нарушением законодательства, общепринятых норм и правил, не соответствующих возрастным ограничениям аудитории группы	«Если хотите обсудить, переходите в этот чат, пока Роскомнадзор на заблокировал»

	Если осознание того, что содержание группы не одобряется окружающими	«Это самая жуткая группа из тех, что я видел»
	Администрация скрыта, ее контакты не указаны или на ее открытых аккаунтах проявляются признаки деструктивного поведения	Администратор группы, посвящённой юмористическим картинкам, является сатанистом
	У разных групп со схожей тематикой одни и те же администраторы, и хотя бы одна из этих групп имеет признаки деструктивного поведения	Администратор групп, направленных на помощь бездомным животным, также является администратором группы, посвящённой жестокому обращению с животными
	Организуются конкурсы и флешмобы дестрктивного содержания или имеющие деструктивные цели	Флешмобы, задания в которых - употребить в пищу предметы, не являющиеся продуктами питания
	В группе осуществляется информирование о деструктивном поведении, его мотивированиие, сопровождение или контроль	«Хочешь сделать себе больно? Я расскажу о нескольких способах, как это сделать»
	Распространяются специфические правила поведения, противоречащие общепринятым нормам морали и общечеловеческим ценностям	Правила призывают называть плохими словами взрослых или обижать малышей
	Происходит формирование культа личности лидера/кумира/идола, у которого есть признаки деструктивного поведения	Серийный убийца как герой
	Группе приписываются романтизм, красота и эстетичность; на контент негативного содержания накладывается позитивный фон	Группа, посвящена культуре наркомании, публикует изображение красивых людей, употребляющих запрещённые вещества

Кроме того, группа может содержать признаки деструктивности в разных вариациях, в одной группе может быть только один признак, в другой - множество. Зачастую одного признака не достаточно для признания группы

деструктивной, наличие единовременно нескольких признаков с большей точностью определяет деструктивную группу.

Некоторые признаки вовлечения в деструктивные сообщества

- Снижение самостоятельности и критического мышления
- Стремление к асоциальному поведению
- Нарушение правовых норм и дисциплин
- Нарушение социальных и этических норм
- Уход в виртуальную реальность
- Проявление агрессии к окружающим
- Снижение мотивации и воли
- Формирование фанатизма по отношению к человеку, группе, идее
- Отрицание авторитета взрослых и общечеловеческих ценностей
- Симпатия к антигероям и различным злодеям
- Мрачное видение будущего
- Отказ от ответственности
- Формирование радикальных взглядов

Правила гигиены по защите от деструктивного влияния в Интернете:

1. Группы, которые прямо признают, что они являются/ не являются деструктивными, намеренно распространяют информацию о деструктивном поведении. Избегайте контакта с ними, а в случае если вы наткнулись на них, обратитесь к администратору Сети, чтобы остановить распространение деструктивного влияния.
2. Аккаунты, у которых есть признаки демонстрации деструктивного поведения, могут оказаться злоумышленниками. Будьте осторожны с ними, не раскрывайте им личных данных, не открывайте присланные от них материалы, избегайте вовлечения в деструктивную тему.
3. Группы, посвящённые культу личности персоны, имеющей признаки деструктивного поведения, могут распространять радикальные взгляды и призывать к деструктивному поведению. Постарайтесь взглянуть на эту персону критически, избегайте радикальных идей и взглядов, возможно, вами хотят воспользоваться в своих целях.
4. Оставленный лайк, комментарий или репост под материалом, прямо или косвенно связанным с деструктивным поведением (пугающие изображения, грустные надписи), может привлечь внимание злоумышленников. Такие материалы могут оказать негативное влияние на вашу психику, а также стать сигналом для вербовщиков и кураторов.
5. Конкурсы, которые могут нанести вред физическому, психическому или социальному благополучию, часто имеют опасные последствия. Берегите

себя и своих близких, участвуйте только в проверенных конкурсах, в ходе которых вы можете освоить позитивный полезный навык или помочь кому-то без вреда для себя и окружающих.

Выход из деструктивной группы возможен, но иногда этому могут помешать различные причины, последствий которых боится подросток:

- страх потерять недавно приобретённых друзей и знакомых;
- угрозы физической расправы со стороны участников деструктивной группы;
- шантаж материалами, компрометирующими пользователя, со стороны участников группы;
- боязнь потерять популярность и какой-либо статус в деструктивной группе;
- возникшая материальная, социальная, психологическая или иная зависимость от участников движения.

Примерная схема выхода из деструктивного сообщества

Шаг 1 ➡	**Шаг 2** ➡	**Шаг 3** ➡	**Шаг 4** ➡	**Шаг 5** ➡
Немедленно откажитесь выполнять деструктивные практики	Перестаньте потреблять деструктивный контент	Сократите или оборвите контакты с участниками течения	Поделитесь переживаниями с тем, кому доверяете	Начните общение в положительной группе
➡ **Шаг 6** ➡	**Шаг 7** ➡	**Шаг 8** ➡	**Шаг 9** ➡	**Шаг 10**
Сделайте скриншоты сообщений с угрозами, предупредите о передаче их в полицию	Если угрозы поступили в ваш адрес, незамедлительно обратитесь в полицию	Даже если на вас есть какая-либо компромент-рующая информация, обязательно обращайтесь в полицию	Обратитесь за профессио-нальной психологической помощью	Никогда не стесняйтесь обращаться за помощью, не думайте, что вы остались с проблемой один на один

5. Безопасное поведение

Из-за того что в Интернете обмен информацией происходит очень быстро, а также есть возможность общаться анонимно с большим количеством самых разных и часто совершенно не знакомых людей, у пользователей могут возникнуть опасные иллюзии нереальности происходящего и отсутствия ответственности за свои слова и действия.

В действительности грань между дозволенным и недозволенным в интернете гораздо тоньше, чем можно было бы себе представить, а наказание за, казалось бы, невинные детские шалости может быть вполне взрослым. Общение в Интернете, размещаемая информация, репосты могут выйти за рамки не только правил приличия, но и закона.

Наиболее распространённые правонарушения в Интернете

1. Возбуждение ненависти, вражды между людьми, унижение человеческого достоинства, совершенные публично.

Виновнику непременно придётся отвечать по закону, если его публичные высказывания в адрес какого-то человека, касающееся его пола, расы, национальности, языка, происхождения, религии или принадлежности к какой-либо группе, будет признано судом противоправным. Прежде чем отправлять/размещать сообщение, комментарий и т.д., задумайтесь, как они могут быть приняты адресатом.

2. Побуждение к самоубийству.

Травля в Сети может иметь множество негативных последствий. Если же издевательства над человеком подтолкнули его к мысли о причинении вреда своему здоровью, соответствующая переписка будет изучена представителями правоохранительных органов, и агрессора в обязательном порядке привлекут к ответственности.

3. Пропаганда (публичное демонстрирование) нацистской символики.

Размещая (распространяя) в Интернете фотографии, рисунки, видеоролики и материалы в других форматах, содержащие нацистскую символику или атрибутику (или символику и атрибутику нацистских организаций), пользователь совершает правонарушение. Решение о том, является ли конкретный материал пропагандой или публичным демонстрированием нацистской (экстремистской) символики, принимается судом на основе заключений экспертов. *Основной причиной правонарушений в цифровом*

пространстве со стороны пользователей является неверная оценка ими законности содержания контента.

4. Распространение заведомо ложной информации, создавшей угрозу для чьей-то жизни и/или здоровья (причинившей вред).

Создателя и распространителя (или его родителей) заведомо ложного сообщения общественно значимого характера, повлёкшего за собой угрозу причинения вреда жизни и здоровью граждан, их имуществу, угрозу нарушения общественного порядка или приведшего к негативным последствиям, могут оштрафовать на крупную сумму. Распространителю ложной информации о предполагаемом теракте угрожает реальный тюремный срок. Уголовный Кодекс РФ за заведомо ложное сообщение об атаке терроризма предусматривает наказание в виде лишения свободы на срок до десяти лет.

5. Вовлечение в распространение наркотиков.

Вовлечение в распространение наркотиков - деятельность по привлечению человека к участию в процессе распространения наркотиков с помощью различных приёмов (просьбы, угрозы, обман, шантаж и т. д.).

Примеры манипулятивных приёмов используемых для вовлечение подростков в процесс распространения наркотиков:

- в сети запускают серию роликов/постов о «последних медицинских исследованиях», которые доказали пользу того или иного препарата для активизации умственной деятельности, расширения сознания, увеличения физически показателей. Это делается для разрушения тезиса о безусловном вреде наркотиков и формировании из положительного образа;
- популяризация и романтизация наркотиков и образа жизни наркоманов в массовой культуре через распространение объектов массовой культуры (фильмов, сериалов, книг, музыки), содержащих упоминания о наркотиках;
- попытки в личном общении привлечь к употребление или распространению наркотиков. При этом подростка чаще всего пытаются убедить, что в силу его возраста проблемы с законом ему не грозят;
- размещение объявлений о работе распространителем наркотиков. Подростков пытаются завлечь высокой оплатой труда, что, впрочем далеко от реальности, а если даже кому-то и удаётся заработать, то длится это недолго и заканчивается многолетним тюремным заключением.

Правонарушением является размещение/пересылка сообщений о закладках/тайниках и прочих местах хранения наркотиков.

В представленной ниже таблице даны ответы на наиболее распространённые вопросы, касающиеся юридически правильного поведения в Сети.

Вопрос	Ответ
Правда ли, что мне ещё нет 16 лет, меня не привлекут к ответственности за преступления?	Нет. Уголовная ответственность наступает в 16 лет (а иногда с 14 лет), но к несовершеннолетним могут применяться меры воспитательного воздействия, в отношении них может быть назначено наказание, их могут поместить в специальное учебно-воспитательное учреждение закрытого типа или привлечь к административной ответственности и выплате штрафа
Правда ли, что я сам решаю, говорю/пишу я что-либо экстремистское и пропагандирую ли я нацизм?	Нет. Характеризовать материалы будут эксперты, назначенные судом, а их выводы могут сильно отличаться от мнения автора.
Правда ли, что, если я спрячусь под ником, меня не узнают ни другие пользователи, ни правоохранительные органы?	Частично правда. Для других пользователей можно остаться инкогнито, но, если встанет вопрос об определении личности в рамках расследования преступления, правоохранительным органам не составит труда найти виновника.
Так ли это, что, если я не знаю, насколько противозаконны мои действия, меня не будут наказывать?	Нет. Если человек не знает, что его поступок или высказывание можно будет квалифицировать как нарушение закона, от юридических последствий его это не убережёт. В этом случае сработает общий принцип правосудия: незнание закона не освобождает от ответственности.

Организация обучения детей и родителей (законных представителей)

Образовательные организации с учетом актуальности информационной безопасности детей, описанной в соответствующем разделе данных

рекомендаций должны предпринимать различные меры по повышению уровня знаний обучающихся в сфере информационной безопасности, а для реализации данной функции также взаимодействовать с родителями и законными представителями обучающихся для повышения их уровня знаний в данной сфере.

Организация обучения информационной безопасности обучающихся

Образовательная организация может организовать обучение своих обучающихся информационной безопасности путем:

1. Обращения внимания вопросам обеспечения информационной безопасности в рамках действующих в образовательной организации учебных дисциплин;
2. Внедрения в образовательную программу самостоятельной учебной дисциплины или увеличение количества учебных часов на изучение данной проблематики при изучении учебных предметов в рамках вариантовой части учебного плана образовательной программы;
3. Организации соответствующих мероприятий или обучения в рамках тематической внеурочной деятельности и дополнительного образования;
4. Организации соответствующих мероприятий или обучения в рамках программ воспитания и социализации обучающихся.

Вопросы обеспечения информационной безопасности могут быть изучены во время различных учебных дисциплин как в рамках курса «Информатика», «Основы безопасности жизнедеятельности», так и других предметных областей, и иной учебной деятельности с учетом межпредметных и метапредметных связей.

При преподавании и изучении обучающимися вопросов информационной безопасности рекомендуется не только рассмотреть различные аспекты информационной безопасности, но и вопросы практического использования сети «Интернет» для собственного развития и образования.

Образовательные организации организуют в рамках своей компетенции и проводят классные часы, внеклассные мероприятия и другие различные тематические мероприятия, в частности Единый урок по безопасности в сети «Интернет», квест по цифровой грамотности «Сетевичок» и другие.

Для повышения эффективности занятий могут быть проведены межпредметные и внутрикурсовые уроки: одновременно по двум предметам, одновременно для учащихся разных возрастов и т.д.

Обучение детей по ступеням обучения имеют следующие цели:

1. Для обучающихся начальной школы рекомендуется рассмотреть основные аспекты осуществления деятельности в сети «Интернет» и мерах собственной защиты, в частности с учетом отсутствия у многих детей в данном возрасте собственной электронной почты.
2. Для обучающихся средней школы вопросы информационной безопасности могут быть расширены за счет изучения психологических и технических аспектов информационной безопасности, вопросов законодательства и ответственности, правил и условий получения, изготовления и распространения информации и других аспектов, позволяющих обучающимся не только знать меры защиты, но и знание источников и принципов работы сетевых рисков.
3. Для обучающихся старшей школы вопросы информационной безопасности должны быть изучены в той мере, которая позволит самому обучающему стать источником достоверной информации по вопросам информационной безопасности для своих ровесников и младших.

Непосредственно уроки и занятия по вопросам информационной безопасности возможно организовать в следующих формах, которые могут быть использованы как отдельно, так и совместно:

1. Дискуссии или дебаты;
2. Деловые игры;
3. Подготовка обучающимися тематических буклетов, листовок и других материалов;
4. Квесты, премии, конкурсы и олимпиады;
5. Анкетирование, исследования и опросы;
6. Тесты и викторины;
7. Демонстрация мультфильмов и (или) видеоурока;
8. Семинар, вебинар или занятие с приглашенным экспертом.

При проведении уроков и занятий можно использовать следующие игровые методики:

1. Уроки, напоминающие публичные формы общения: пресс-конференция, брифинг, аукцион, бенефис, регламентированная дискуссия, панорама, телемост, репортаж, диалог, «живая газета», устный журнал и т.д.
2. Уроки, основанные на имитации деятельности учреждений и организаций: следствие, органы власти, патентное бюро, ученый совет и т.д.

3. Уроки, основанные на имитации деятельности при проведении общественно-культурных мероприятий: заочная экскурсия, экскурсия в прошлое, путешествие, прогулки и т.д.

Самостоятельным направлением работы является воспитание у детей культуры информационной безопасности при работе в сети Интернет вне образовательной организации:

1. Вовлечение обучающихся в деятельность детских общественных организаций, реализующих свою деятельность дистанционно, например, детская общественная организация "Страна молодых", Российское движение школьников и другие.
2. Организация и проведение дистанционных мероприятий, посвященных информационной безопасности, например, Всероссийская контрольная работа по информационной безопасности, квест «Сетевичок» и другие, для повышения уровня знаний обучающихся в сфере информационной безопасности и повышения общего уровня ИКТ-компетентности.

Организация обучения информационной безопасности родителей и законных представителей обучающихся

Образовательная организация может для повышения уровня знаний родителей и законных представителей обучающихся в вопросах обеспечения информационной безопасности детей предпринимать различные регулярные меры информационного и организационного характера, в частности:

1. Освещение вопросов информационной безопасности детей в рамках проводимых родительских собраний и проведение тематических собраний для родителей с участием педагогических работников и представителей администрации образовательной организации, в частности для демонстрации видеоматериалов по данным вопросам.

2. Организация индивидуальных и групповых консультаций родителей и законных представителей обучающихся классными руководителями, специалистами психологической службы и администрации образовательной организации для обеспокоенных родителей и законных представителей обучающихся и родителей и законных представителей обучающихся, находящихся в группе риска.

3. Проведение семинаров, лекций и вебинаров с участием экспертов и сотрудников правоохранительных органов для родителей и законных представителей обучающихся.

4. Раздача информационных материалов об обеспечении безопасности детей в сети «Интернет», в частности памятки, флаеры и другие материалы.
5. Проведение анкетирования родителей и законных представителей обучающихся по вопросам организации дома мер по обеспечению защиты детей в информационном пространстве.
6. Размещение на сайте образовательной организации, средствах массовой информации образовательной организации, сообществах в социальной сети и сервисе электронных дневников для родителей и законных представителей обучающихся информации по обеспечению информационной безопасности детей.

В ходе мероприятий для родителей и законных представителей обучающихся рекомендуется отметить следующие темы:

1. Важность обеспечения цифровой и информационной грамотности детей и подростков;
2. Рекомендации и советы по обеспечению информационной безопасности личности и детей как особо незащищенных пользователей сети «Интернет»;
3. Методы и функции родительского контроля.

При подготовке методических рекомендаций были использованы следующие источники:

1. Методические рекомендации по основам информационной безопасности для обучающихся общеобразовательных организаций с учётом информационных, потребительских, технических и коммуникативных аспектов информационной безопасности;
2. Учебно-методический комплект "Основы безопасности жизнедеятельности" для 8-9 классов под научной редакцией Ю.С. Шойгу;
3. http://сетевичок.рф;
4. http://Единыйурок.рф.

Методические разработки для организации и проведения мероприятий с обучающимися разных возрастов.

Материалы включают в себя конспекты занятий, презентации, видеоматериалы, изображения и тд, которые педагоги могут скачать по приложенным ссылкам.

Для каждой возрастной группы предусмотрена возможность выбора темы на усмотрение педагогов. Уроки-беседы возможно использовать для проведения в дистанционном формате посредством видеосвязи.

	Формат проведения	Тема проведения
1 группа старшие дошкольные группы – 1 класс	Урок-беседа	«Правила безопасности в сети Интернет»
2 группа 2 – 5 классы	викторина	«Информационная безопасность и защита персональных данных»,
	урок-беседа	«Безопасность при использовании современных гаджетов»
3 группа 6 – 9 классы	классный час	«Этика сетевого общения»
	урок-беседа	«Безопасность при использовании современных гаджетов»
4 группа 10 – 11 классы	классный час по методике case-study	«Цифровая гигиена»
	час изучения законодательства	«Законодательные меры за противоправные действия в сфере информационных технологий»

Ссылка для скачивания разработок

https://cloud.mail.ru/public/4SVB/2cKRq3HP3