ДЕПАРТАМЕНТ ЦИФРОВОГО РАЗВИТИЯ ВОЛОГОДСКОЙ ОБЛАСТИ

УПОЛНОМОЧЕННЫЙ ПО ПРАВАМ РЕБЕНКА В ВОЛОГОДСКОЙ ОБЛАСТИ

УГРОЗЫ ДЕТСКОЙ КИБЕРБЕЗОПАСНОСТИ

Методическое пособие для педагогов

Вологда, 2022 год

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Интернет позволяет получать большое количество информации в одно мгновение. Но есть и обратная сторона медали – контент в сети не всегда безопасен для ребёнка, поэтому нужно принимать меры по обеспечению безопасности детей в сети Интернете.

В России действует Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию». Закон запрещает распространение нежелательной информации среди детей в зависимости от их возраста. Это относится не только к интернету – фильмы в кино и книги, например, тоже попадают под ограничения.

Преступления и правонарушения совершаемые несовершеннолетними в сети Интернет, в последнее время становятся все более распространенными. Изменяется социальная ситуация, особенности взаимодействия подростков с внешним миром и, в свою очередь, преступность несовершеннолетних меняет свою специфику. Зачастую преступления в интернет-пространстве совершаются подростками в силу недостаточного понимания социальных норм, разделения реальной и виртуальной жизни, при этом у них возникает ощущение своей полной анонимности, а также снижается волевой контроль поведения.

Ключевые определения:

Вирус – это вид вредоносного программного обеспечения, способного создавать копии самого себя и внедряться в код других программ, системные области памяти, загрузочные секторы, а также распространять свои копии по разнообразным каналам связи.

Троян – разновидность вредоносной программы, проникающая в компьютер под видом легитимного программного обеспечения, в отличие от вирусов и червей, которые распространяются самопроизвольно.

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 – относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных).

Кибербуллинг – это запугивание и травля с использованием цифровых технологий, повторяющиеся эпизоды, цель которых - напугать, разозлить или опозорить тех, кого преследуют.

Цифровой след – это данные, которые вы оставляете при использовании интернета. Эти данные включают посещаемые веб-сайты, отправляемые электронные письма и информацию, указываемую в онлайн-формах.

Мессенждер – это программа для мгновенного обмена текстовыми сообщениями, аудиозаписями, фотографиями и другими мультимедиа.

НОРМАТИВНО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ

- Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» от 29.12.2010 N 436-ФЗ.
- Федеральный закон «О персональных данных» от 27.07.2006 N 152-ФЗ.
- Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ.
- Федеральный закон от 3 июля 1998 г. № 124-ФЗ «Об основных гарантиях прав ребенка в Российской Федерации».
- Распоряжение Правительства Российской Федерации от 02.12.2015 N 2471-р «Об утверждении Концепции информационной безопасности детей».
- Приказ Минцифры России от 22.03.2022 N 226 «О перечне федеральных мероприятий, направленных на обеспечение информационной безопасности детей, производство информационной продукции для детей и оборот информационной продукции, на 2022 - 2027 годы».
- Письмо Минобрнауки России от 28.04.2014 № ДЛ-115/03 «О направлении методических материалов для обеспечения информационной безопасности детей при использовании ресурсов сети Интернет».
- Письмо Минобрнауки России от 14.05.2018 № 08-1184 «О направлении информации».

ПРИОРИТЕТНЫЕ ЗАДАЧИ ГОСУДАРСТВЕННОЙ ПОЛИТИКИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЕТЕЙ

Семья, государство и заинтересованные в обеспечении информационной безопасности детей общественные организации имеют следующие приоритетные задачи:

- Формирование у детей навыков самостоятельного и ответственного потребления информационной продукции.
- Повышение уровня медиаграмотности детей.
- Формирование у детей позитивной картины мира и адекватных базисных представлений об окружающем мире и человеке.
- Ценностное, моральное и нравственно-этическое развитие детей.
- Воспитание у детей ответственности за свою жизнь, здоровье и судьбу, изживание социального потребительства и инфантилизма.
- Усвоение детьми системы семейных ценностей и представлений о семье.
- Развитие системы социальных и межличностных отношений и общения детей.
- Удовлетворение и развитие познавательных потребностей и интересов ребенка, детской любознательности и исследовательской активности.
- Развитие творческих способностей детей.
- Воспитание у детей толерантности.
- Развитие у детей идентичности (гражданской, этнической и гендерной).
- Формирование здоровых представлений о сексуальной жизни человека.
- Эмоционально-личностное развитие детей.
- Формирование у детей чувства ответственности за свои действия в информационном пространстве.
- Воспитание детей как независимых, ответственных и самостоятельно мыслящих личностей с целью изживания социального иждивенчества.

УГРОЗЫ ИНТЕРНЕТА ДЛЯ ДЕТЕЙ

1. Мошенничество в отношении детей

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:

1.1 Фишинг – получение доступа к логинам, паролям, банковским данным.

1.2 Поддельные интернет магазины.

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

1.3 Сборы средств на «благотворительность».

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.

Детям необходимо объяснить, 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»).

1.4 Вирусы

Вирус может полностью блокировать 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.

1.5 Приватность данных

Чтобы разобраться, как персональная информация может стать общеступной, нужно понять, как информация попадает в Интернет.

Есть несколько вариантов:

- Заполняем анкету при регистрации на ненадежном сайте.

- Участвуем в сомнительных онлайн-опросах, конкурсах, викторинах.
- Оплачиваем покупки в Сети на фишинговом сайте.
- Выкладываем фотографии, на которые случайно попадает персональная информация, например, табличка с названием улицы и номером дома.

Но это не единственные способы. Перечисленные выше варианты, касаются конкретных действий самого пользователя, но важно понимать, что влиять на приватность может то, что мы не контролируем напрямую, например:

- Публикации других людей о нас. Например, друзья размещают совместную с вами фотографию без разрешения.
- История наших поисковых запросов и посещенных сайтов. Ее обычно собирают поисковые системы, чтобы предложить вам более подходящую рекламу.
- Установка и использование сомнительных приложений. Например, приложению «Фонарик» нужен доступ только ко вспышке, но если такое приложение просит доступ к контактам и сообщениям, это повод задуматься. Под видом благонадежного приложения, может на самом деле оказаться зловредное программное обеспечение или рекламный софт.

Как обезопасить детей от мошенничества?

- Установите антивирус. Он будет блокировать подозрительные программы, которые ребёнок может нечаянно скачать на компьютер. Ими нередко пользуются хакеры, чтобы получить доступ к персональным данным. Кроме того, антивирус предупредит ребёнка о переходе по подозрительной ссылке, которая может позволить мошеннику дистанционно управлять устройством пользователя.
- Учите ребёнка здравому смыслу. Он должен понимать, что некоторые вещи – например, имена и должности родителей, адрес, пароль от социальной сети и так далее – нельзя никому раскрывать. Объясните, что интернет позволяет любому человеку выдавать себя за кого угодно. Перед тем как встретиться с другом, которого нашёл в Сети, лучше поговорить со взрослыми. Здравый смысл — одно из главных правил безопасности.
- Обсудите правила пользования интернетом и ограничьте время присутствия в Сети. Согласитесь, что вы не сможете все время контролировать своего ребенка и постоянно находиться рядом с ним. Но вы сможете установить правила, при которых обе стороны останутся довольны: например, назначить время онлайн-присутствия и установить нормы на загрузку тех или иных файлов, фильмов и программ.
- Важно объяснить детям, что бесплатный сыр бывает только в мышеловке. Чтобы получить что-то стоящее, нужно вкладывать силы и не рассчитывать на удачу.

Уточните, что данные вашей карты – это информация, делиться которой нельзя и использовать можно только под вашим контролем.

- Расскажите ребенку, что можно рассказать о себе, а что нет при регистрации на различных сайтах.
- Используйте в социальных сетях ребенка «Настройки приватности».
- Контролируйте списки друзей в социальных сетях ребенка.

2. Нежелательный контент

Это могут быть жестокие сцены насилия, причинение вреда живым существам, порнографические материалы и другое. Нужно понимать, что рано или поздно ребёнок столкнётся с подобным контентом, как бы вы ни старались это предотвратить. Важно сделать то, что в ваших силах, чтобы это не оставило сильного травмирующего отпечатка на психике сына или дочери.

Большинству подростков сложно оценивать сайты с точки зрения достоверности информации. Важно объяснить ребенку, что не все, что они видят в Интернете, является правдой.

Объясните, что в случаях столкновения с сомнительным содержанием нужно поискать дополнительную информацию или посоветоваться с родителями и учителями. Необходимо объяснить школьникам, что информация, размещенная в Интернете, может не соответствовать действительности, ведь опубликовать ее может абсолютно любой человек.

Для того чтобы обезопасить детей от нежелательного контента рекомендуется установить родительский контроль. Существуют различные программы, которые ограничивают доступ к подозрительным сайтам, помогают контролировать действия и безопасность детей в Сети и лимитируют время пребывания в интернете.

3. Кибербуллинг

Помимо правонарушений, относящихся к уголовно наказуемым деяниям и подпадающих под действие Уголовного кодекса РФ, в фокус внимания взрослых попадает широкий круг деструктивно направленных действий, обозначаемых понятием «кибернасилие». Этим термином принято обозначать электронную травлю, проявления жестокости онлайн, то есть преднамеренные агрессивные действия, систематически осуществляемые против жертвы, которая не может себя защитить, с использованием электронных средств: социальных сетей, электронных писем, сетевых игр и т.д.

Кибербуллинг детей – острая проблема. В интернете легче сохранить кажущуюся анонимность и это, в свою очередь, порождает вседозволенность вкупе с сопутствующими проблемами. Важно вовремя отследить, что у ребёнка проблемы в Сети. Об этом говорят некоторые симптомы: подавленность, постоянное использование гаджетов, злость или непривычная замкнутость.

Виды кибербуллинга:

Троллинг – написание в Интернете провокационных сообщений с целью вызвать гнев, конфликты между участниками, пустой трёп, оскорбления и т. п.

Флейминг – единоразовые оскорбительные и/или вульгарные комментарии, сообщения и т.д. направлены на дальнейшее разжигание ссоры. Иногда применяется в контексте троллинга, но чаще флейм вспыхивает просто из-за обиды на виртуального собеседника.

Хейт – это открытое выражение свей ненависти к кому/чему-либо, т.е. полноценная травля человека в сети.

Подделка личности – путём взлома страницы пользователя или создания её копии начинается распространение ложной информации и очернение человека. От лица жертвы рассылаются оскорбительные сообщения в адрес знакомых, учителей и т.п.

Разглашение данных – публикация в интернете любых сведений о человеке, которые не являются достоянием общественности, может повлечь за собой тяжёлые последствия для жертвы.

Кибersталкинг – длительное преследование в сети, сопровождающееся угрозами расправы и сексуальным домогательством. Агрессор буквально везде следует за своей жертвой – отмечается на фотографиях, комментирует любую активность в интернете, вступает в те же группы, пытается узнать информацию у друзей жертвы.

Как помочь ребенку, если он стал жертвой киберпреследования:

- окажите ребенку необходимую поддержку и внимание;
- установите положительный эмоциональный контакт;
- внимательно выслушайте рассказ ребенка;
- сохраните подтверждение фактов нападения;
- заблокируйте пользователя, присылающего угрозы или оскорбления;
- сообщите о нападениях или преследовании администрации сайта;
- обратитесь на горячую линию детского телефона доверия 8 800 2000 122;
- обратитесь в правоохранительные органы.

4. Побуждение детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, самоубийству

В настоящее время все больше и больше детей с восхищением смотрят на взрослых, которые делают экстремальные селфи, забираются на крыши поездов, прыгают с моста, перебегают улицу перед проезжающими машинами и делают «вызов» всем, кто подписан в социальных сетях на них. Для ребенка это вызов, и вызов он принимает, так как в силу возрастных особенностей ему любая задача по плечу - «море по колено».

5. Вовлечение детей в противоправные действия

К большому сожалению, сегодня распространение незаконного оборота наркотиков достигло той стадии, когда широкие массы молодёжи направленно и интенсивно втягиваются в их употребление. Подростки и молодежь активно используют виртуальное общение в социальных сетях, поэтому данная группа населения в первую очередь подвержена влиянию агрессивной рекламе потребления наркотических средств и веществ. У детей такая информация способна вызвать желание употребить наркотические средства, психотропные одурманивающие вещества, желание покурить или выпить.

Причем родители не всегда вовремя могут заметить, что ребенок попал в эти сети. Зачастую поведение ребенка, отличающееся от нормы проявляется когда возникает уже зависимость от психотропных веществ, алкоголя. Тем самым будет труднее подростка вылечить от этой зависимости.

Тревожной общемировой тенденцией является активное проникновение идей экстремизма и терроризма в молодежную среду. Многие несовершеннолетние, которые в силу определенных жизненных обстоятельств, попадая под влияние взрослых в интернете, например, пойдут с ружьем в школу и будут обстреливать сверстников и т.д. Такие примеры, к сожалению, у нас все еще на слуху.

Одним их часто встречающихся видов противоправного поведения подростков в сети Интернет являются правонарушения сексуального характера - общение на сексуальные темы, инициирование обмена интимными фотографиями, в том числе с лицами младшего возраста, в некоторых случаях сопровождающееся угрозами, шантажом. Впоследствии полученные интимные изображения могут быть отправлены, в том числе без ведома того, кто на них представлен, одному или нескольким выбранным получателям по электронной почте, социальным сетям, а также быть опубликованными на различных онлайн-форумах, в результате чего они становятся общедоступными для всех посетителей сайта.

Жизнь не стоит на месте, и каждый день появляется новая возможность вовлечь несовершеннолетних в противоправные действия. Задача, прежде всего родителей состоит в том, что бы они всегда разговаривали со своими детьми. Необходимо наладить

дружественные, доверительные отношения. Именно этот фактор будет препятствием тому, что ребенок не будет искать поддержку в социальных сетях, и не попадет в руки нечестных взрослых.

РЕКОМЕНДАЦИИ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ

1. Общие рекомендации

- Повышение компетенций родителей (законных представителей) и работников организаций детства в области цифровой грамотности и информационной безопасности на портале «Учеба.онлайн».
- Рассказать ребёнку об опасностях, с которыми он может столкнуться в сети

Родители не только должны изучить вопрос безопасности детей в интернете, но и обучить самих детей правильному поведению в сети, чтобы исключить возможность возникновения опасных ситуаций. Обязательно рассказать ребенку о существовании онлайн-хищников, киберпреступности, вредоносных программ, кибербуллинга и что делать с этим. Мало того, что нужно научить ребёнка правильно переходить улицу и не разговаривать с незнакомцами, также требуется объяснить, что при неправильном использовании интернет может быть очень опасен.

- Показать ребёнку, что родители всегда готовы его выслушать

Важно, чтобы ребёнок понимал – родители открыты для разговора, когда речь идет о безопасности в интернете. Если у ребёнка появляются проблемы, связанные со всемирной паутиной, он должен осознавать, что в любой момент может поделиться ими с родителями.

- Использовать инструменты для реализации родительского контроля

Родительский контроль – это комплекс мер, которые гарантируют родителям, что их ребёнок не получит доступа к вредоносному контенту или неподходящим, по мнению родителей веб-сайтам.

- Использовать надежные пароли

Пояснить ребенку, что при регистрации на веб-сайте требуется придумать запоминающийся, но в то же время сложный пароль – это поможет снизить риск взлома учетной записи в Интернете.

- Научить ребёнка, что общение в сети с незнакомцем, так же опасно, как и в реальности.

Всем известное правило «Не говорите с незнакомцем на улице» актуально и в эпоху интернета. Обязательно донесите до своего ребёнка, что встречи с людьми, с которыми он знакомится в интернете, сопряжены с риском для его безопасности.

- Предупредите ребенка об информации, которую нельзя сообщать в интернете: домашний адрес, название школы, которую посещает ребенок, класс, электронный адрес, пароли, пин-коды.

- Расположите компьютер вашего ребенка в месте общей доступности: столовой или гостиной.
- Установите временные ограничения на компьютер (в какое время и как долго ребенок пользуется интернетом), средства фильтрации.
- Установите защиту от вирусов, регулярно обновляйте антивирусное программное обеспечение.
- Объясните ребенку о необходимости использования проверенных информационных ресурсов.
- Научите ребенка правилам общения с незнакомыми людьми в интернете.
- Разъясните ребенку об опасности встреч с теми, с кем он общается через интернет, если он не знаком с этими людьми.

2. Рекомендации по техническому ограничению доступа детей к нежелательному контенту в сети Интернет

Для ограничения доступа детей к нежелательному контенту существуют следующие способы:

1. Встроенные средства операционной системы. Создайте на компьютере учетную запись для ребенка, применив к ней функцию «Родительского контроля» С помощью данной функции можно:

1) регулировать время нахождения ребенка в Интернете;

2) блокировать доступ к некоторым сайтам;

3) запрещать запуск некоторых игр и программ;

2. Коммерческое программное обеспечение.

Установите лицензионное программное обеспечение, специально ориентированное на осуществление «Родительского контроля». Данные программы располагают более широким спектром возможностей по ограничению доступа детей в Интернет.

3. Свободно распространяемое программное обеспечение.

Данное программное обеспечение находится в свободном доступе и обеспечивает базовый набор функций для ограничения доступа детей к нежелательным сайтам.

4. Тарифные опции интернет – провайдеров.

Для ограничения доступа к нежелательному контенту с настольных компьютеров и мобильных устройств можно использовать дополнительные опции, предлагаемые Интернет-провайдерами. Для этого необходимо обратиться в службу технической поддержки провайдера. Телефон данной службы обычно указан в договоре.

5. Специальные возможности антивирусных программ.

Установите подходящую антивирусную программу на домашний компьютер. Выберите в настройках программы функцию родительского контроля или установите веб - фильтр.

6. Программное обеспечение мобильных устройств.

В самой операционной системе мобильного устройства имеются некоторые настройки, позволяющие создать профиль с ограниченным доступом в Интернет, запрещает покупки в приложениях, ограничивает запуск некоторых приложений. Установите специальное приложение, предлагающее множество способов ограничения доступа в Интернет.

7. Тарифные опции сотовых операторов.

Обратитесь к вашему мобильному оператору и установите функции «Черный список», функцию связи между номером родителя и ребенка, фильтрацию нежелательных звонков и СМС.

ЗАКЛЮЧЕНИЕ

Обеспечение безопасности детей в интернете так же важно, как и в реальном мире. Существует множество причин, по которым дети хотят и должны использовать интернет: от выполнения школьных заданий до посещения виртуальных мероприятий, внеклассного обучения и интерактивных игр с друзьями. Интернет – это богатый ресурс и интересное место для общения, если дети и подростки знают, как использовать его безопасно и избегать потенциальных угроз.

Безопасность в интернете достигается постоянными разговорами с детьми о том, как и для чего, используется интернет и знанием, как обеспечить их защиту. Понимание того, почему дети выходят в интернет, с кем они там взаимодействуют и какие сайты посещают, очень важно для обеспечения их безопасности. Также крайне важно информировать их о рисках, связанных интернетом, о безопасном и вежливом общении в интернете и о действиях в случае, если они столкнулись с чем-то неуместным.

Разговаривайте с детьми, используйте инструменты для их защиты и следите за их действиями. Защитить ребенка от всего на свете невозможно. Однако можно научить его, как правильно поступать, если все же ребенок попал в нехорошую ситуацию.

ССЫЛКИ НА ПОЛЕЗНЫЕ РЕСУРСЫ ПО ОБЕСПЕЧЕНИЮ ДЕТСКОЙ КИБЕРБЕЗОПАСНОСТИ

1. ВКонтакте: как настроить безопасность и приватность: https://www.kaspersky.ru/blog/vk-security-and-privacy-settings/22858/.
2. Урок цифры «Приватность в цифровом мире»: тренажеры для обучающихся с 1 по 11 класс: https://урокцифры.рф/lessons/cybersecurity.
3. Центр безопасного Интернета в России: https://www.saferunet.ru/.
4. Как защитить аккаунт в «Одноклассниках» на пять с плюсом: https://www.kaspersky.ru/blog/odnoklassniki-zashita-ot-vzloma/25960/.
5. Рекомендации для несовершеннолетних и родителей, наглядные информационные материалы по безопасному использованию сети «Интернет»: https://fcprc.ru/wp-content/uploads/2021/12/MR-po-bezopasnomu-ispolzovaniyu-seti-Internet-.pdf.
6. Перечень федеральных мероприятий, направленных на обеспечение информационной безопасности детей, производство информационной продукции для детей и оборот информационной продукции на 2022-2027 годы: https://www.edu.yar.ru/safety/docs/2022_03_perechen/pismo_vhodyashchee_vh_01-10292_22.pdf.
7. ФГБНУ «Центр защиты прав и интересов детей». Система консультативной помощи подросткам и родителям в области информационной безопасности в сети Интернет: https://fcprc.ru/tvoy-bezopasniy-kibermarshrut/.
8. Методические материалы для учителей. Рекомендации по проведению занятия «Основы безопасного общения в социальных сетях»: https://kids.kaspersky.ru/metodic.
9. Видеоролик о защите детских персональных данных: http://персональныеданные.дети/multimedia/videorolik_o_zawite_detskih_personalnyh_dannyh1/.
10. Лига безопасного интернета. Материалы к урокам безопасного интернета: http://www.ligainternet.ru/encyclopedia-of-security/parents-and-teachers/parents-and-teachers-detail.php?ID=3652.
11. Азбука информационной безопасности для младших школьников от Лаборатории Касперского: http://www.ligainternet.ru/encyclopedia-of-security/parents-and-teachers/parents-and-teachers-detail.php?ID=10340.