Методические рекомендации

«ОТВЕТСТВЕННОЕ ПОВЕДЕНИЕ УЧИТЕЛЕЙ В СЕТИ»

Дети в интернете

Содержание

ВВЕДЕНИЕ

Сеть интернет изначально развивалась как средство коммуникации и обмена информацией. Основная функция сети была в осуществлении связи между пользователями, находящимися в разных точках планеты. Процесс стремительного развития информационно-коммуникационных технологий (далее – ИКТ) позволил значительно расширить функциональные возможности сети интернет, при этом использование ИКТ на протяжении всего времени существования, несмотря на появление новых возможностей, сопровождается возникновением частично осознанных рисков и угроз.

Результаты различных исследований и опросов показали, что каждый второй ребенок считает, что в сети интернет располагается информация, негативно влияющая на него, а каждый пятый хотя бы раз сталкивался с такой информацией. В ситуации, когда дети не способны справиться с чем-либо в сети интернет, они обращаются за помощью к родителям и друзьям. Учителя стоят в этом ряду на последнем месте. Как показали многие исследования, даже высококомпетентные в сфере ИКТ педагоги далеко не всегда являются безусловными авторитетами для школьников и имеют адекватные представления о том, чем занимаются их ученики в сети интернет и с какими опасностями могут столкнуться.

К основным наиболее актуальным типам интернет-рисков для детей принято относить:

– технические риски, которые определяются возможностями повреждения программного обеспечения персонального компьютера (далее – ПК), хранящейся на нем информации, нарушения ее конфиденциальности или взлома аккаунтов, хищения паролей и персональной информации посредство вредоносных программ (вирусов, червей, троянских коней, шпионских программ, ботов и др.);

– риски в сфере потребления, возникающие в процессе приобретения товаров и услуг через сеть интернет, включающие в себя риск приобретения товара низкого качества, контрафактной и фальсифицированной продукции, риск потери денежных средств без приобретения товара или услуги, хищения финансовой информации с целью мошенничества;

– риски в информационной среде, которые возникают в процессе использования находящихся в сети интернет материалов (текстов, изображений, аудио- и видеофайлов, ссылок на различные ресурсы), содержащих противозаконную, неэтичную и вредоносную информацию;

– риски в сфере коммуникации, возникающие в процессе общения и межличностного взаимодействия пользователей в сети интернет (например, кибербуллинг, незаконные контакты, груминг, сексуальные домогательства, знакомства в сети интернет и последующие встречи с интернет-знакомыми в реальной жизни), с которыми можно столкнуться при общении в чатах, онлайн-мессенджерах, социальных сетях, сайтах знакомств, форумах, блогах.

На основе перечисленных рисков рассмотрим области сети интернет, наиболее подверженные рискам (таблица 1).

Таблица 1 – Классификация областей сети Интернет, наиболее подверженных рискам

Направления	Характеристика	Риски для пользователя
Техносфера	техническая безопасность и базовая техническая грамотность пользователей	заражение ПК либо мобильного устройства вирусом, потеря информации
Сфера потребления	заказы, услуги, покупки, совершаемые онлайн	безопасность личных данных (пароли доступа к банковской карте, аккаунту), мошенничество, финансовые потери
Информационная среда	создание, поиск, отбор, критическая оценка контента	потребление незаконного и непредназначенного для детей контента (неэтичного и вредоносного содержания[1])
Сфера коммуникации	создание, развитие, поддержание отношений, самопрезентация, идентичность, репутация	разглашение личной и/или конфиденциальной информации, троллинг, кибербуллинг[2]

Техносфера и сфера потребления в большей степени связаны с безопасностью интернет-пользователей. Информационная среда и сфера коммуникации — это важные факторы социализации. Они влияют на формирование личности, нравственных ценностей, культуру поведения.

Стоит отметить, что в Республике Беларусь проблемы интернет-рисков затронуты в том числе и на законодательном уровне. 11 мая 2016 г вступил в силу Закон Республики Беларусь №362-З О внесении изменений и дополнений в некоторые законы Республики Беларусь. Одним из изменений и дополнений в Закон Республики Беларусь от 19 ноября 1993 года «О правах ребенка» в редакции Закона Республики Беларусь от 25 октября 2000 года стало внесение в Закон главы «Защита детей от информации, причиняющей вред их здоровью и развитию».

Также при Правительстве Республики Беларусь был создан общественно-консультативный совет по защите детей от информации, причиняющей вред их здоровью и развитию. В стране существуют консультационные центры и телефоны доверия экстренной психологической помощи для детей и подростков и их родителей.

Министерства образования Республики Беларусь от №82 от 15 июля 2015 г., согласно которой, одной из основных составляющих воспитания является информационная культура обучающегося, которая определяется как качественная, динамичная характеристика жизнедеятельности человека в области передачи, хранения и применения информации, основанная на информационно-коммуникационной компетентности личности.

[1] – насилие, эротика и порнография, нецензурная лексика, информация, разжигающая расовую ненависть, экстремизм, пропаганда анорексии и булимии, суицида, азартных игр и наркотических веществ и другое.

[2] – преследование сообщениями, содержащими оскорбления, агрессию, запугивание, хулиганство, социальное бойкотирование с помощью различных интернет-сервисов.

В дополнении к этому в стране принята Концепция непрерывного воспитания детей и учащейся молодежи в Республике Беларусь, утвержденная постановлением На ряду с тем, что информационная культура способствует овладению знаниями, умениями, навыками в области информационных технологий и позволяет эффективно использовать имеющиеся в распоряжении общества информационные ресурсы и средства информационных коммуникаций в личностном и профессиональном становлении, она также предполагает воспитание личной ответственности за распространение информации.

К условиям формирования информационной культуры относят:

– создание в учреждениях образования информационно–образовательной среды, направленной на формирование системно–информационной картины мира и информационной компетентности обучающихся;

– наличие и совершенствование в учреждениях образования необходимой информационно–технической базы;

– наличие у педагогических работников и обучающихся знаний в области современных информационно–коммуникационных технологий;

– использование в воспитательном процессе ресурсов «медиаобразования» (средств массовой информации: прессы, радио, телевидения, интернета, социальных сетей);

– системность, качественный отбор информации и адресность информационного воздействия;

– стимулирование активности и проявление творческой инициативы обучающихся в практической деятельности;

– систематическую рефлексивную оценку обучающимися результатов своей деятельности.

С учетом перечисленных условий одним из важных аспектов формирования информационной культуры является обеспечение информационной безопасности, которая понимается как состояние защищенности детей и учащейся молодежи, при котором минимизирован риск, связанный с причинением информацией вреда здоровью, нормальному физическому, интеллектуальному, психическому, духовному и социальному развитию детей и учащейся молодежи.

В связи с этим, а также стремительным увеличением числа пользователей сети интернет среди детей и подростков растет необходимость повышать уровень информационной культуры школьных учителей и практических психологов, расширять их представления о возможностях сети интернет, образе жизни и особенностях цифрового поколения, влиянии онлайн–рисков на развитие детей.

Одним из основных показателей информационной культуры субъекта образовательных отношений является его ответственное поведение в сети интернет.

Данные исследований показывают:

– 90% детей ежедневно заходят в интернет;

– каждый 3–ий из них находится в сети от 3 до 5 часов;

– каждый 6–ой ребенок – от 5 до 8 часов.

Данная статистика демонстрирует, что время, проводимое подростками–пользователями в сети интернет, становится значимой частью их распорядка дня, а интернет – тем фактором, который определяет новый образ жизни. Учитывая высокую интенсивность потока информации и коммуникации в течение интернет–сеансов, нельзя недооценивать их влияние на психическое развитие и формирование личности ребенка. Сеть интернет становится одним из значимых источников социокультурного развития.

Настоящее методическое пособие предполагает решение следующих задач:

– повышение информационной культуры учителей и сокращение существующего цифрового разрыва между взрослыми и детьми;

– расширение представлений педагогов о возможностях сети интернет как источника информации, инструмента коммуникации, сферы потребления;

– расширение представлений педагогов о влиянии контентных, коммуникационных, потребительских и технических рисков и угроз, с которыми сталкиваются в глобальной сети дети и подростки, на их здоровье, развитие личности и процессы социализации.

1. УГРОЗЫ, ВОЗНИКАЮЩИЕ ПРИ НЕКОРРЕКТНОМ ФУНКЦИОНИРОВАНИИ ОСНОВНЫХ КОМПОНЕНТОВ/ЭЛЕМЕНТОВ СЕТИ ИНТЕРНЕТ И МЕРЫ ПРЕДОСТОРОЖНОСТИ

Использование сети интернет невозможно без обеспечения корректной работы трех составляющих:

– аппаратных средств – устройств, позволяющих осуществлять подключение к сети интернет;

– программного обеспечения для использования сети интернет;

– подключения (физического) к сети интернет.

1.1 Риски и угрозы, вызванные сбоем в работе аппаратных средств

Персональный компьютер представляет собой сложное электронное устройство. Работа ПК и всех компонентов подвержена сбоям. Последствия от незначительных сбоев не оказывают влияние на работу пользователя, т.к. программное обеспечение самостоятельно устраняет эти последствия. Однако в работе аппаратных средств могут возникать и более серьезные ошибки, в результате которых появляются уязвимости в информационной безопасности системы, а именно в целостности и доступности информации.

Причины возникновения угроз информационной безопасности, в результате ошибок работы аппаратных средств, подразделяются на:

– естественные причины, вызванные воздействием на аппаратные средства объективных физических процессов или стихийных природных явлений, независящих от человека. Например, при работе электронных устройств возможны перепады напряжения, вызванные грозой. В результате таких перепадов, оборудование подвергается усиленной нагрузке и может выйти из строя. Также широко известны частые случаи обрыва сети электропередачи при падении деревьев из–за сильного ветра.

– искусственные причины, вызванные деятельностью человека, которые классифицируют по степени преднамеренности проявления на:

– непреднамеренные, вызванные ошибками при разработке аппаратных средств, ошибками в действиях пользователя. К ним относятся: неумышленные действия, приводящие к частичному или полному отказу, или разрушению аппаратных средств; неправомерное отключение оборудования или изменения режимов работы устройств. Например, рядом с модулями ПК расположена жидкость и пользователь случайно пролил ее на клавиатуру или системный блок, в результате чего произошло короткое замыкание, которое вывело из строя ПК.

Приведенные типы угроз приводят к утрате работоспособности отдельных подсистем или всего устройства, и как следствие к потере или нарушению целостности

и доступности информации, хранящейся на ПК.

– преднамеренные, связанные с корыстными, идейными устремлениями злоумышленников. К таким угрозам относятся: вывод из строя всех или отдельных наиболее важных компонентов ПК; отключение или вывод из строя подсистем функционирования вычислительных систем (электропитания, охлаждения, линий связи). Также к данному типу угроз можно отнести атаки, направленные на сбой работы аппаратных средств или маскирующие деятельность злоумышленника, путем имитирования сбоев в работе ПК. Данный тип угроз приводит к нарушению не только целостности и доступности, а также конфиденциальности и достоверности информации.

1.2 Риски и угрозы, возникающие вследствие ошибок в работе программного обеспечения

При процессе работы с ПО возможно возникновение ошибок, которые могут привести к некорректному функционированию программы, утрате или искажению данных, уязвимостям в безопасности. В результате некорректного функционирования ПО, пользователь подвергается рискам и угрозам безопасности, среди которых к наиболее распространенным относят:

– несанкционированный доступ (НСД) – самый распространенный вид компьютерных нарушений, который заключается в получении пользователем доступа к ресурсу, на который у него нет разрешения в соответствии с принятой в организации политикой безопасности;

– незаконное использование привилегий, которое заключается в применении злоумышленниками программного обеспечения, функционирующее в нештатном (нестандартном) режиме. Незаконный захват привилегий возможен либо при наличии ошибок в самой системе, либо в случае халатности при управлении системой. Строгое соблюдение правил управления системой защиты, соблюдение принципа минимума привилегий позволяет избежать таких нарушений;

– использование «скрытых каналов», представляющих собой пути передачи информации между процессами системы и нарушающих системную политику безопасности. В среде с разделением доступа к информации пользователь может не получить разрешение на обработку интересующих его данных, однако может придумать для этого обходные пути. «Скрытые каналы» могут быть реализованы различными путями, в частности при помощи программных закладок (троянских коней);

– выполнение каких–либо действий одним пользователем от имени другого пользователя (так называемый «маскарад»). Такие действия другому пользователю могут быть разрешены. Нарушение заключается в присвоении прав и привилегий;

– скрытую, недокументированную точку входа в программный модуль, так называемые «люки», которые относятся к категории угроз, возникающих вследствие ошибок реализации какого–либо проекта (системы в целом, комплекса программ и т. д.). Поэтому в большинстве случаев обнаружение «люков» – результат случайного поиска;

– вредоносные программы. В последнее время участились случаи воздействия на вычислительную систему специально созданными программами. Для обозначения всех программ такого рода был предложен термин «вредоносные программы». Эти программы прямо или косвенно дезорганизуют процесс обработки информации или способствуют утечке и/или искажению информации.

К самым распространенным видам подобных программ относятся:

Вирус — это программа, которая способна заражать другие программы, модифицируя их так, чтобы они включали в себя копию вируса.

Троянский конь — программа, которая содержит скрытый или явный программный код, при исполнении которого нарушается функционирование системы безопасности. Троянские кони способны раскрыть, изменить или уничтожить данные, или файлы. Их встраивают в программы широкого пользования, например, в программы обслуживания сети, электронной почты.

«Червяк» — программа, распространяемая в системах и сетях по линиям связи. Такие программы подобны вирусам: заражают другие программы, а отличаются от вирусов тем, что не способны самовоспроизводиться.

«Жадная» программа — программа, которая захватывает (монополизирует) отдельные ресурсы вычислительной системы, не давая другим программам возможности их использовать.

«Бактерия» — программа, которая делает копии самой себя и становится паразитом, перегружая память ПК и процессор.

«Логическая бомба» — программа, приводящая к повреждению файлов или компьютеров (от искажения данных – до полного уничтожения данных). «Логическую бомбу» вставляют, как правило, во время разработки программы, а срабатывает она при выполнении некоторого условия (время, дата, ввод кодового слова).

«Лазейки» — точка входа в программу, благодаря которой открывается доступ к некоторым системным функциям. Обнаруживается путем анализа работы программы.

Также к классу вредоносных программ можно отнести **снифферы** (программы, перехватывающие сетевые пакеты), программы подбора паролей, атаки на переполнение буфера, в некоторых приложениях – дизассемблеры и отладчики.

Перечисленные атаки зачастую используются совместно для реализации комплексных атак. Так, например, троянская программа может использоваться для сбора информации о пользователях на удаленном компьютере и ее пересылки злоумышленнику, после чего последний может осуществить атаку методом «маскарада».

1.3 Угрозы, вызванные нарушениями в работе сети

Нарушения в работе сети приводят к негативным изменениям использования сети интернет: пользователь может потерять доступ к данным, хранящимся на распределенных серверах (в «облаке»), информации в сети интернет, общению с коллегами и друзьями.

Наиболее важными угрозами, вызванными нарушениями в работе сети интернет, являются кража конфиденциальных данных и заражение устройства вредоносным ПО.

Кража личных данных – вид мошенничества, в результате которого происходит хищение личной информации, к примеру, паролей, имен пользователей, банковских данных, номеров кредитных карточек и т.д. Кража данных доступа к счету пользователей является наиболее распространенным видом мошенничества в сети интернет. Злоумышленники чаще всего используют фишинг–атаки для кражи персональной информации (подробно будет рассмотрено в следующем разделе).

Исследователи выделяют несколько групп собственности, которые наиболее часто подвергается кражам с ПК пользователей: параметры доступа к финансовым системам, интернет–пейджерам и сайтам, адресам электронной почты, пароли к онлайн–играм. Для осуществления кражи чаще всего используются вредоносные программы или методы социального инжиниринга.

1.4 Меры предосторожности во избежание возникновения угроз безопасности

Для наглядности смоделируем ситуацию.

Педагог из-за низкого уровня информационной культуры или по неосторожности перешел на подозрительный сайт. При переходе по ссылке, на ПК произвелась загрузка вредоносного программного обеспечения (троянский конь). В результате злоумышленник с помощью программы «троянский конь» осуществляет сбор данных с ПК пользователя и как следствие получает закрытую информацию о пользователе (доступ к банковскому аккаунту, доступ к электронной почте, к аккаунтам в социальных сетях и т.д.). В частности, для педагога «заражение» компьютера приведет к более серьезным последствиям. Злоумышленник с помощью вредоносного ПО может получить доступ не только к личной информации учителя, но и к персональным данным детей и их родителей, нарушить функционирование системы безопасности учреждения образования. Во избежание таких последствий всем педагогам при работе в сети интернет рекомендуется выполнять следующие действия:

1. При загрузке интернет-сайта удостовериться, что адрес сайта начинается с комбинации https:// – это значит, что соединение с веб-сайтом зашифровано.
2. При подключении через общедоступную сеть Wi-Fi нельзя пользуйться платежными системами и другими важными сервисами.
3. Необходимо использовать надежные пароли – это важный элемент защиты, позволяющий значительно повысить безопасность онлайн-транзакций. Ключевые элементы надежности пароля – длина и сложность. Идеальный пароль – это длинная комбинация различных знаков, которая включает в себя буквы и цифры, а также знаки пунктуации и символы.
4. Не использовать один и тот же пароль для доступа в различные аккаунты.
5. Регулярно изменять свои пароли.
6. Важно обеспечить защиту для записанных паролей. Быть внимательным к тому, где хранятся или записываются пароли.
7. Регулярно обновлять браузер и операционную систему.
8. Внимательно следить за тем, какие веб-сайты открываются и что загружается Это относится к музыке, фильмам, файлам, плагинам и дополнениям для браузера и т. д.
9. Остерегаться всплывающих окон, которые предлагают установить ПО или устранить неполадки.
10. Устанавливать ПО только из надежных источников.
11. Пользоваться только авторитетными ресурсами, такими как встроенный магазин приложений или сайт разработчика, а не сторонними сайтами для загрузки ПО.
12. В случае обнаружения подозрительных признаков работы ПК после загрузки из сети интернет (устройство медленно работает, появляются всплывающие окна), нужно немедленно удалить ПО и проверить систему с помощью последней версии антивирусной программы.

2. СФЕРА ПОТРЕБЛЕНИЯ. ВОЗМОЖНОСТИ И РИСКИ

Стремительное развитие интернет-технологий способствовало возникновению интернет-торговли. В настоящее время существует огромный ассортимент товаров и услуг, предоставляемых в сети интернет.

2.1 Потребительские риски

Основной угрозой, с которой пользователь может столкнуться при осуществлении

покупки в сети интернет, является интернет-мошенничество.

Под мошенничеством принято понимать хищение чужого имущества или приобретение права на чужое имущество путём обмана или злоупотребления доверием.

Наиболее популярным видом мошенничества в сети интернет является фишинг, целью которого является получение доступа к конфиденциальным данным пользователей – логинам и паролям. Это достигается путём проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов, например, от имени банков или внутри социальных сетей. В письме часто содержится прямая ссылка на сайт, внешне неотличимый от настоящего, либо на сайт с редиректом. После перехода пользователем на поддельную страницу мошенники с помощью различных психологических приёмов побуждают пользователя ввести на поддельной странице свои логин и пароль, которые он использует для доступа к определённому сайту, что позволяет злоумышленникам получить доступ к аккаунтам и банковским счетам.

Мошенников, использующих техники фишинга для достижения своих целей, называют фишерами.

Различают следующие методы (техники) фишинга:

Социальная инженерия – метод, основанный на использовании слабостей человеческого фактора. Поэтому фишеры стараются своими действиями встревожить пользователя и вызвать его немедленную реакцию. Например, электронное письмо с заголовком «чтобы восстановить доступ к своему банковскому счёту», как правило, привлекает внимание и заставляет пользователя пройти по веб-ссылке для получения более подробной информации.

Веб-ссылки. Большинство методов фишинга сводится к маскировке поддельных ссылок на фишинговые сайты под ссылки настоящих организаций. Адреса с опечатками или субдомены часто используются мошенниками.

Например, http://www.yourbank.example.com/ похож на адрес банка Yourbank, а на самом деле он ссылается на фишинговую составляющую сайта example.com. Также имеет место уловка, которая заключается в использовании внешне правильных ссылок, в реальности ведущих на фишинговый сайт. Например, http://ru.wikipedia.org/wiki/Правда приведёт не на статью «Правда», а на статью «Ложь».

Один из старых методов обмана заключается в использовании ссылок, содержащих символ «@», который применяется для включения в ссылку имени пользователя и пароля. Например, ссылка http://www.google.com@members.tripod.com/ приведёт не на www.google.com, а на members.tripod.com от имени пользователя www.google.com.

Ещё одна проблема была обнаружена при обработке браузерами Интернациональных Доменных Имён: адреса, визуально идентичные официальным, могут вести на сайты мошенников.

Обход фильтров. Фишеры часто вместо текста используют изображения, что затрудняет обнаружение мошеннических электронных писем антифишинговыми фильтрами. Но специалисты научились бороться и с этим видом фишинга. Так, фильтры почтовых программ могут автоматически блокировать изображения, присланные с адресов, не входящих в адресную книгу. К тому же появились технологии, способные обрабатывать и сравнивать изображения с сигнатурами однотипных картинок, используемых для спама и фишинга.

Веб-сайты. Обман не заканчивается на посещении жертвой фишингового сайта. Некоторые фишеры используют JavaScript для изменения адресной строки. Это достигается либо путём размещения картинки с поддельным URL поверх адресной строки, либо закрытием настоящей адресной строки и открытием новой с поддельным URL.

Межсайтовый скриптинг. Злоумышленник может использовать уязвимости в скриптах подлинного сайта. Этот вид мошенничества наиболее опасен, так как пользователь авторизуется на настоящей странице официального сайта, где всё, – от веб-адреса до сертификатов, выглядит подлинным. Подобный фишинг очень сложно обнаружить без специальных навыков.

Вишинг (голосовой фишинг). Сегодня фишинг выходит за пределы интернет-мошенничества, а поддельные веб-сайты стали лишь одним из множества его направлений. Письма, которые якобы отправлены из банка, могут сообщать пользователям о необходимости позвонить по определённому номеру для решения проблем с их банковскими счетами. Эта техника называется вишинг (голосовой фишинг). Позвонив на указанный номер, пользователь заслушивает инструкции автоответчика, которые указывают на необходимость ввести номер своего счёта и PIN-код. К тому же фишеры могут сами звонить жертвам, убеждая их, что они общаются с представителями официальных организаций, используя фальшивые номера. В конечном счёте, человека также попросят сообщить его учётные данные.

Смишинг (SMS-фишинг). Набирает свои обороты и SMS-фишинг, также известный как смишинг (англ. SMiShing – от «SMS» и «фишинг»). Мошенники рассылают сообщения, содержащие ссылку на фишинговый сайт, – входя на него и вводя свои личные данные, жертва аналогичным образом передаёт их злоумышленникам. В сообщении также может говориться о необходимости позвонить мошенникам по определённому номеру для решения «возникших проблем». Встречается и следующий вид SMS-фишинга: на подставном сайте для получения какой-либо услуги просят отправить SMS на предложенный номер или ввести свой номер сотового телефона, чаще всего это фэйки файлообменных сервисов. В первом случае с телефонного счёта абонента списывается крупная (возможно, максимальная предусмотренная контрактом) сумма, во втором случае номер добавляется в базу адресов рассылки SMS-спама и может использоваться для дальнейших фишинговых действий.

Вывод.

Только ответственное отношение к собственной безопасности и понимание основных методов, используемых интернет-мошенниками, могут защитить пользователя от кражи личных данных. Критичное отношение к любым сообщениям, полученным в сети интернет, отказ от любых форм взаимодействия, инициированного незнакомыми пользователями, перепроверка информации по альтернативным каналам связи, защита персональной информации от третьих лиц – все это должно стать заповедями компетентного потребителя. Получив подозрительное сообщение, его нужно как следует обдумать, прежде чем предпринимать какие-либо действия.

Следует обратить внимание на источник сообщения: как правило, фишинговые сообщения приходят с незнакомых или подозрительных адресов.

Информацию всегда следует перепроверять, например, связаться с отправителем по телефону, посмотреть официальный веб-сайт или найти информацию об авторе сообщения при помощи общедоступных поисковых сервисов (Google, Yandex, Bing, Yahoo).

Если сообщение содержит угрозу для жизни и здоровья близких людей, которых сейчас нет рядом с вами, стоит подумать, где и с кем они могут сейчас быть, попытаться связаться тем, кто предположительно может дать точную информацию.

Имеет смысл обратить внимание на само сообщение: как правило, оно содержит грамматические и стилистические ошибки, недопустимые при деловой переписке.

Обычно фишинговое сообщение содержит в себе массу неточностей и противоречий, которые легко можно найти при спокойном и трезвом подходе.

2.2 Контентные риски в сети Интернет и способы защиты от негативной информации

С каждым годом информация приобретает все большую значимость в жизни человека и общества. В связи с ростом важности информации в развитии общества необходимо ее разделение на благоприятную и оказывающую негативное влияние.

К информации, причиняющей вред здоровью и развитию детей, способной оказать негативное влияние на здоровье, физическое, нравственное и духовное развитие детей определенной возрастной категории, относится информация:

– вызывающая желание употреблять алкогольные и слабоалкогольные напитки, потреблять наркотические средства, психотропные вещества, их аналоги, токсические или другие одурманивающие вещества, табачные изделия;

– побуждающая к совершению преступления или иного общественно опасного деяния, в том числе к занятию проституцией, попрошайничеством, бродяжничеством, участию в азартных играх, совершению действий, связанных с изготовлением, распространением порнографических материалов или предметов порнографического характера;

– положительно оценивающая преступление или идеализирующая преступников, поощряющая поведение, ущемляющее человеческое достоинство, в том числе совершение насильственных действий по отношению к людям или животным;

– отображающая издевательства над человеком или группой людей либо их унижение в связи с этническим происхождением, национальной, расовой, религиозной, языковой, половой принадлежностью, убеждениями или взглядами, социальным положением, заболеванием;

– поощряющая или положительно оценивающая жестокость, физическое, психическое, сексуальное насилие, сексуальную эксплуатацию, сексуальные отношения с участием детей;

– побуждающая к нанесению телесных повреждений или самоубийству, описывающая средства или обстоятельства самоубийства;

– содержащая методики либо иные материалы о способах изготовления опасных для жизни и здоровья людей предметов и их использования;

– поощряющая привычки, противоречащие формированию здорового образа жизни;

– содержащая нецензурные слова и выражения; дискредитирующая институт семьи и брачно–семейные отношения;

– устрашающего характера, в том числе представляемая в виде изображения или описания в унижающей человеческое достоинство форме смерти, несчастного случая, аварии, катастрофы, заболевания и (или) их последствий;

– содержащая порнографические материалы и (или) эротику.

В зависимости от тематики, жанра, содержания и художественного оформления информационной продукции, особенностей восприятия содержащейся в ней информации детьми определенного возраста, а также от возможности причинения содержащейся в ней информацией вреда здоровью и развитию детей информационной продукции присваиваются следующие знаки возрастной категории:

«0+» – без возрастных ограничений (универсальная);

«6+» – предназначена для лиц, достигших 6 лет;

«12+» – предназначена для лиц, достигших 12 лет;

«16+» – предназначена для лиц, достигших 16 лет;

«18+» – предназначена для лиц, достигших 18 лет.

Государственное регулирование.

Многие государства в той или иной мере ограничивают доступ к незаконной и неприемлемой информации в сети интернет для своих граждан, особенно несовершеннолетних. В Республике Беларусь принят Закон Республики Беларусь №362-З от 11 мая 2016 г «О внесении изменений и дополнений в некоторые законы Республики Беларусь.» Одним из изменений и дополнений в Закон Республики Беларусь от 19 ноября 1993 года «О правах ребенка» в редакции Закона Республики Беларусь от 25 октября 2000 года стало внесение в Закон главы «Защита детей от информации, причиняющей вред их здоровью и развитию».

Также при Правительстве Республики Беларусь был создан общественно-консультативный совет по защите детей от информации, причиняющей вред их здоровью и развитию. В стране существуют консультационные центры и телефоны доверия экстренной психологической помощи для детей и подростков и их родителей.

Программно-технические средства защиты от нежелательного контента.

Одним из решений по защите детей от негативной информации является безопасный поиск, который позволяет фильтровать результаты, содержащие изображения или ключевые слова, рассматриваемые как неподходящие для детей. Также для ограждения ребенка от негативной информации существует специальное ПО, которое позволяет ограничивать доступ детей в сеть интернет, времяпровождение в сети интернет и осуществлять контроль получаемой ребенком из сети информации.

Однако данные средства не позволяют полностью ограничить детей от негативной информации, находящейся в сети интернет. Для обеспечения безопасного использования детьми сети интернет важно формирование и развитие у них информационной культуры. В том числе способности и готовности оценивать основные риски, связанные с распространением в сети интернет противозаконной и негативной информации.

Например, при отсутствии у педагога понимания и содержания понятия нежелательного контента и не использования таких возможностей ПО или ОС как «родительский контроль», учащийся получает неограниченный и бесконтрольный доступ к любой информации, располагаемой в сети интернет.

3. СФЕРА КОММУНИКАЦИИ

Для оперативной и качественной передачи переработанной информации наряду с развитием средств её обработки идет непрерывный процесс совершенствования средств коммуникаций. Революционные изменения в области глобальных средств коммуникаций и становления «информационного общества» произошли с появлением сети интернет.

3.1 Виды, возможности и потенциальные риски интернет-коммуникации

В сети интернет присутствует большое разнообразие сервисов, предоставляющих возможность общения с другими людьми. Данные сервисы отличаются по функционалу и имеют свои преимущества и потенциальные риски.

Сервисы интернет-коммуникации делятся на два типа:

- сервисы для асинхронного общения (общения не в реальном времени), к ним относят: электронную почту, социальные сети, форумы, блоги.

- сервисы синхронной коммуникации - средства общения, позволяющие общаться в режиме реального времени: мессенджеры, IP-телефония, чаты и т.п.

3.1.1 Электронная почта

Электронная почта — технология и служба по пересылке и получению электронных сообщений (называемых «письма», «электронные письма» или «сообщения») между пользователями компьютерной сети (в том числе – сети интернет). Электронная почта по составу элементов и принципу работы практически повторяет систему обычной (бумажной) почты, заимствуя как термины (почта, письмо, конверт, вложение, ящик, доставка и другие), так и характерные особенности – простоту использования, задержки передачи сообщений, достаточную надёжность и в то же время отсутствие гарантии доставки.

3.1.2 Социальная сеть

Социальные сеть – платформа, онлайн–сервис и веб–сайт, предназначенные для построения, отражения и организации социальных взаимоотношений в сети интернет.

Основными преимуществами социальных сетей являются:

– возможность общения с коллегами по работе, родственниками и друзьями, вне зависимости от их места проживания;

– использование социальных сетей как инструмента для саморазвития (просмотр познавательных фильмов, прослушивание музыки, чтение интересных книг, изучение иностранных языков);

– легкость в поиске интересующей информации, благодаря созданным в социальных сетях группам по интересам;

– возможность применения в образовательном процессе. Например, можно обмениваться конспектами лекций, заданиями по лабораторным работам и другой полезной информацией. Созданные сообщества позволяют пользователям детально изучить вопросы определенной тематики и обсудить проблемные вопросы с другими членами группы;

– социальные сети – это площадка для развития бизнеса. Здесь можно прорекламировать свой интернет–магазин, студию веб–дизайна или рок–школу. Реклама может быть направлена на целевую аудиторию и о вашем бизнесе узнают люди, которых могли бы заинтересовать предоставляемые вами продукция или услуги. Можно отыскать здесь новых клиентов, приумножить лояльность постоянных покупателей.

Главные недостатки использования социальных сетей:

– обилие развлекательной, поверхностной и зачастую ненужной информации;

– утрата человеком навыка реального общения, т.к. сформирована привычка к общению в режиме онлайн. Осуществляя общение в социальных сетях, пользователи часто не соблюдают правила грамматики и пунктуации, используют скудный словарный запас, эмоции заменяются смайликами – все это отрицательно сказывается на общении в реальном мире;

– зависимость от социальных сетей.

Угрозы безопасности пользователей в социальных сетях.

1. Проблемы конфиденциальности. При размещении личной информации в социальных медиа она становится публичной и как следствие частная жизнь пользователя, становится достоянием общественности.

2. Хакерство и взлом паролей. Для получения доступа к аккаунту и пользователя и кражи его конфиденциальных данных, в социальных сетях, хакеры используют различные методы: фишинг, социальная инженерия, размещение вредоносного ПО и подбор пароля с помощью специализированного ПО.

3. Виртуальные двойники. Большинство пользователей в социальных сетях

размещают личную информацию: дату рождения, информацию о семье, род занятий, предпочтения в области литературы и кинематографа, информацию о коллегах и друзьях, место жительство и т.д. Вся предоставляемая информация собирается злоумышленниками воедино и впоследствии они создают виртуального двойника пользователя. С помощью созданного двойника мошенники могут воздействовать на семью, друзей и коллег пользователя с целью получения денег, при этом пользователи, вступающие в общение с виртуальным двойником, полагают, что это реальный человек.

4. **Интернет-зависимость.** Простота применения и огромное количество информации, содержащейся в социальных сетях, в большинстве случаев способствует развитию зависимости – сформированной потребности активно использовать интернет для получения любой информации, общения и времяпрепровождения. Пользователь может много раз в день заходить на свои страницы в «Вконтакте», «Одноклассниках», Facebook и проводить большое количество времени, проверяя свои аккаунты или просто читая о том, что происходит в жизни других пользователей. При этом зависимые пользователи тратят на это рабочее время и уделяют меньше времени семье и друзьям.

3.1.3 Форумы

Форум — класс веб-приложений для организации общения посетителей веб-сайта. Суть работы форума заключается в размещении пользователями (посетителями форума) интересующих вопросов и проблем с их последующим обсуждением. Отдельно взятый предмет обсуждения, по сути, представляет собой тематическую гостевую книгу. Пользователи могут оставлять свои комментарии по заявленной проблеме, задавать вопросы по ней и получать ответы, а также сами отвечать на вопросы других пользователей форума и давать им советы. Вопросы и ответы сохраняются в базе данных форума, и в дальнейшем могут быть полезны как участникам форума, так и любым пользователям сети интернет, которые могут зайти на форум, зная адрес сайта, или получив его от поисковых систем при поиске информации.

3.1.4 Мобильная связь (SMS и MMS)

SMS – сервис коротких сообщений (Short Messaging Service), осуществляющий передачу небольшого объема данных в сети сотовой связи.

Одним сообщением в SMS можно передать 160 символов в 7-битной кодировке (арабские цифры и латинский алфавит), 140 символов в 8-битной кодировке (алфавит французского и немецкого языков) и 67 символов в 16-битной кодировке (кириллица и иероглифы). Вместе с текстом в SMS передается другая информация: время отправки, номера получателя и отправителя, схема кодировки, идентификатор протокола, сообщение о доставке и прочее. Эти данные позволяют адресовать сообщение верному адресату и обеспечить читабельность сообщения.

MMS – сервис мультимедийных сообщений (Multimedia Messaging Service). С его помощью можно отправлять на телефоны или электронную почту фотографии, видео или звуковые файлы. MMS-сообщение состоит из двух частей: SMS стандартной длины и мультимедийного файла, который сохраняется на WAP-сервере оператора. Если телефон получателя не поддерживает загрузку мультимедиа, будет показана ссылка на файл. Спецификации MMS ограничивают размер отправляемого вложения 999 килобайтами, российские операторы установили лимит в 300 килобайт.

3.1.5 Мессенджеры и IP-телефония

Основные сервисы синхронной коммуникации в сети интернет – это мессенджеры, IP-телефония и чаты.

Мессенджеры (от англ. messengers -посланники, посыльный) – программа или веб-сервис для мгновенного обмена сообщениями между людьми, включенными в список контактов друг у друга. Одна из наиболее популярных программ – ICQ, или, как ее называют пользователи Рунета, «аська», была создана в 1996 году и стала прообразом для разработки многих подобных программ. IP-телефония, или VoIP (Voice over IP), – приложения, которые позволяют не только обмениваться текстовыми сообщениями, но и совершать голосовые звонки по всему миру (например, Skype).

Мессенджеры и программы IP-телефонии позволяют своим пользователям видеть, кто из списка контактов находится онлайн, и общаться с помощью текста. В отличие от чатов, мессенджеры более закрыты и позволяют общаться только с людьми из своего списка контактов

Чат – средство обмена сообщениям в сети интернет в режиме реального времени. Сейчас в сети интернет существует множество чатов. Обычно они организованы тематически, в зависимости от интересов или возраста. Помимо возможностей текстового общения, некоторые чаты позволяют поддерживать голосовые разговоры в режиме реального времени. Чаты предоставляют возможность знакомиться и общаться с людьми со всего мира. В тематических чатах легко можно найти единомышленников. В то же время это открытое пространство для общения, в котором легко можно притвориться другим человеком. С одной стороны, это позволяет избежать влияния стереотипов реального мира, с другой – несет определенные риски (нецензурная лексика, буллинг, «троллинг», фишинг).

3.2 Возможности обучения в сети интернет

В требованиях основной образовательной программы указывается организация сетевого взаимодействия общеобразовательных учреждений, а выпускник школы должен уметь взаимодействовать в информационном пространстве образовательного учреждения. Педагог в этой системе рассматривается как проводник, в диалоге с которым школьники приобретают коммуникативную компетентность и получают навыки обучения на протяжении всей жизни.

Исследования Лаборатории Касперского[3] свидетельствуют о том, что:

- 96% учителей используют социальные сети в личных целях;
- у 67% опрошенных педагогов открытый аккаунт в социальных сетях;
- 73% опрошенных педагогов добавляют своих учеников в «друзья»;
- 25% учителей, добавляющих своих учеников в «друзья», не проводят с ними никакой педагогической работы на этих площадках.

Для эффективного использования сетевых возможностей в обучении педагог должен повышать свою информационную культуру. Коммуникационные сервисы позволяют выстроить взаимодействие с учениками и коллегами, поддерживать сотрудничество школьников на онлайн-площадках. В социальных сетях подростки могут выступать в роли исследователей, творцов и обучающихся. Каждый пользователь формирует в сети интернет свое личное пространство, в рамках которого он представляет себя и свои интересы. Сообщества объединяют людей со схожими интересами, которые могут делиться своими знаниями, идеями, находками и таким образом углублять знания друг друга, расширять горизонты, демонстрировать различные точки зрения на интересующие вопросы и проблемы.

[3] Информация получена из открытых интернет-источников.

3.3 Рекомендации использования интернет-средств коммуникации для педагогов

Для коммуникации в сети интернет учитель должен грамотно выстроить собственное сетевое пространство: правильно презентовать себя в сети интернет, выстраивать и поддерживать отношения с учащимися, создавать и развивать сообщества. Это подразумевает высокую ответственность при использовании социальных сетей.

Поведение педагога в социальных сетях может проявляться в виде:

Отказа от общения в социальной сети с учениками.

При таком поведении педагога в социальных сетях уменьшается эффективность воспитания учащихся, однако оно способствует обучению детей уважению личного пространства учителя и демонстрирует возможность использования социальных сетей, не выставляя личную жизнь напоказ.

Включения учеников в «друзья», общение с ними в социальных сетях.

Данный инструмент воспитания является наиболее эффективным, т. к. непосредственно затрагивает безопасность детей в сети интернет и вопросы учительской репутации и авторитета. Соответствие образа педагога в реальной и виртуальной жизни способствует повышению доверия среди учеников.

Главными направлениями, которым необходимо уделить особое внимание педагогам, активным в сети, являются:

– культура поведения и речи;

– размещаемая информация, в том числе фото– и видеоконтент;

– степень открытости информации о себе и своих друзьях;

– контроль включения в группы посторонних пользователей;

– самоконтроль вступления в группы с сомнительным и/или порочащим имя содержанием;

– педагогическая работа.

Наблюдая за активностью педагога в социальной сети и просматривая размещенные им материалы, ученики воспринимают эту информации как допустимую и приемлемую. Педагог должен поддерживать свою репутацию, заработанную среди учеников.

Репутация педагога в сети интернет напрямую зависит от:

– самопрезентации пользователя,

– его поведения в виртуальном пространстве,

– уровня культуры общения и размещаемого контента.

Во избежание потери педагогом репутации и для поддержания своего авторитета среди учеников и их родителей, следует соблюдать некоторые правила:

– не размещать в своем аккаунте фото и видео сомнительного содержания;

– не использовать ненормативную лексику и нецензурную брань;

– не оскорблять/подшучивать («троллить») других пользователей.

Для обеспечения безопасности учеников в сети педагогу рекомендуется придерживаться следующих правил:

– личный профиль должен быть открыт только для друзей;

– ученики в списке друзей скрыть ото всех;

– группа класса приватная – вступить в нее можно только по приглашению администрации.

Социально ответственный учитель может целенаправленно проводить с детьми педагогическую работу в сети.