Чеверикин Сергей Анатольевич

методист

МКУ «Отдел образования»

пгт Аксубаево, Республика Татарстан

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ДЕТЕЙ: СОЦИАЛЬНЫЕ И ТЕХНОЛОГИЧЕСКИЕ АСПЕКТЫ

***Аннотация**: информационная безопасность детей и подростков в цифровом пространстве – это состояние защищенности детей, в котором минимизирован риск причинения психологического вреда здоровью детей, их духовному, нравственному, физическому и психическому развитию. При этом информационная безопасность в образовательном учреждении может быть достигнута только при успешной реализации ряда педагогических условий, одним из которых является высокий уровень информационно-коммуникационных компетенций педагогов. Предлагаемая программа повышения информационно-коммуникационной компетенции учителя предусматривает повышение уровня компетентности педагогов в сфере информационной безопасности детей и подростков через изучение таких тематических модулей, как: Государственная политика в образовании; Социальные угрозы сети Интернет; Технологические угрозы сети Интернет; Психологические и техно-психологические угрозы сети Интернет; Социально-технологические угрозы сети Интернет; Социально-психологические угрозы сети Интернет.*

***Ключевые слова**: кибербезопасность, интернет-ресурсы, информационная безопасность детей, информационная безопасность подростков, ИКТ-компетентность педагогов, фишинг, спам, кибербуллинг, вредоносные программы, сетевая гигиена, психологическое здоровье, безопасное использование сети Интернет детьми, безопасное использование сети Интернет подростками.*

Стремительные темпы развития и распространения информационных технологий приводят к формированию качественно иной картины мира, транслируя ценности, задавая новые нормы, паттерны поведения и стратегии социального

взаимодействия. Плоскость общения упрощается, перемещаясь из традиционной в виртуальную, благодаря чему формируется информационно-коммуникативная среда, подразумевающая особую систему социальных коммуникаций современного общества, в котором социальные субъекты становятся взаимозависимыми за счет объединения в коммуникационную сеть, способствующую координации и согласованию совместной деятельности путем общения с использованием интернет-технологий, и новые формы построения социальных взаимоотношений, приводящих к качественно новым сдвигам во всех сферах жизнедеятельности.

Давно уже известный факт, что Интернет – величайшая в мире образовательная и художественная платформа, научные и культурные учреждения и организации всего мира открывают свои виртуальные двери, в том числе и для детей. Интернет предлагает детям широкий спектр возможностей для выражения их индивидуальности, образования и обучения, поэтому дети являются одной из наиболее быстрорастущих групп пользователей Интернета. Однако, одновременно с положительными моментами возникают вопросы информационной безопасности детей. Защита несовершеннолетних от интернет-угроз является важной задачей, однако недостаточно контролируемый характер сети Интернет создает много нерешенных проблем.

В Интернете представлены сайты, где все чаще стала появляться «вредная» информация, к которой можно отнести: призыв к войне; информация, возбуждающая социальную, расовую, информационную или религиозную ненависть и вражду; пропаганда ненависти, вражды и превосходства; распространение порнографии; посягательство на честь, доброе имя и деловую репутацию людей; рекламу (недостоверную, неэтичную, скрытую); информацию, оказывающую деструктивное воздействие на психику людей, и, особенно, детей и подростков.

Важно отметить, что сеть Интернет пока никому в целом не принадлежит, как и не существует на сегодняшний день единых законов, регулирующих Интернет по всему миру, но борьба за кибербезопасность и, в первую очередь, за безопасность детей в Интернете – основной вызов времени в развитии глобального сетевого пространства, и Россия здесь не исключение.

В Российской Федерации на уровне государственных органов и федеральных служб ведется постоянная и целенаправленная работа по противодействию угрозам информационной безопасности. Создан реестр экстремистских сайтов; осуществляют мероприятия антисуицидальной интернет-профилактики; закрывается доступ к ресурсам, способным спровоцировать опасное для жизни и здоровья поведение детей, сайты, содержащие призывы к суициду, участию в массовых публичных мероприятиях, фанатских движениях и пр.; блокируются ксенофобские сайты, направленные на возбуждение ненависти, либо вражды, а также на унижение достоинства человека, либо группы лиц.

Особенно остро в настоящий момент встает вопрос обеспечения информационной безопасности аудитории от нежелательного воздействия на нее интернет-ресурсов, содержащих нежелательный, вредный, а зачастую и откровенно опасный контент. Отсюда возникает достаточно сложная задача: научить людей разобраться в потоках информации, выявить информационные угрозы и защититься от них. И, конечно, в первую очередь, подрастающее поколение, как наиболее уязвимое в силу своей психологической, социальной и физиологической незрелости.

В самом широком смысле, информационная безопасность детей и подростков в цифровом пространстве – это состояние защищенности детей, в котором минимизирован риск причинения психологического вреда здоровью детей, их духовному, нравственному, физическому и психическому развитию. И основная, самая важная работа по противодействию угрозам информационной безопасности должна начинаться, конечно же, в семье и школе. А поскольку законные представители обучающихся зачастую сами не обладают достаточным уровнем необходимых знаний, основная нагрузка по обеспечению цифровой безопасности учеников ложится на общеобразовательные организации. Но информационная безопасность в образовательном учреждении может быть достигнута только при успешной реализации ряда педагогических условий, одним из которых является высокий уровень информационно-коммуникационных компетенций педагогов.

Предлагаемая программа повышения информационно-коммуникационной компетенции учителя предусматривает повышение уровня компетентности педагогов в сфере информационной безопасности детей и подростков через изучение различных тематических модулей.

Цели и задачи данной программы определены следующим образом.

Цель: формирование и совершенствование профессиональных компетенций педагогов в области информационной безопасности детей.

Задачи.

1. Определить уровень ИКТ компетентности педагогов.

2. Повысить компетентность педагогов в вопросах существующих интернет-рисков и способах противодействия им.

3. Расширить профессиональные возможности педагогов в части обеспечения информационной безопасности обучающихся.

Таким образом, адресная направленность программы – это учителя-предметники и классные руководители общеобразовательных организаций, заместители руководителей по воспитательной работе общеобразовательных организаций. Освоение программы рассчитано на одно полугодие учебного года, и общая трудоемкость ее составляет 48 часов. Форма обучения – заочная, с применением электронного обучения, дистанционных образовательных технологий.

Что касается ожидаемых результатов освоения данной программы, то ее содержание построено таким образом, что их можно сформулировать следующим образом. Педагогические работники по итогам прохождения программы должны:

– знать: приоритетные направления развития образовательной системы российской федерации; действующие нормативные документы в области информационной безопасности детей; управленческие подходы по организации защиты детей от информационных угроз; основные информационные угрозы; основные механизмы защиты детей от информационных угроз;

– уметь: организовывать деятельность по выявлению и защите детей от основных социальных угроз; организовывать деятельность по защите детей от воз-

никающих угроз при работе с персональными устройствами; организовывать деятельность по защите детей от фишинга; организовывать деятельность по защите детей от угроз, связанных с кибербуллингом; организовывать деятельность по защите детей от угроз, связанных с экстремизмом, группами смерти и АУЕ.

Текущий контроль освоения программы осуществляется по итогам изучения модулей в виде выполнения практических работ и решения кейсов.

Среди рисков освоения программы следует выделить низкую мотивацию педагогических работников к обучению, большую занятость педагогов, стереотипы педагогического поведения и недостаточный уровень информационно-коммуникативной компетентности педагогов. Однако, через использование системы морального и материального стимулирования, управленческое регулирование; через осознание педагогами исключительной важности изучаемого материала и способность применить полученные знания в практической деятельности, а также при помощи дополнительные занятий по повышению ИКТ-грамотности риски эти можно нивелировать.

Содержание самой программы представлено следующими модулями.

Во-первых, это входящее тестирование, позволяющее определить уровень информационно-коммуникационной компетентности педагогов, степень осведомленности о существующих интернет-угрозах и мерах их профилактики.

Модуль 1. Государственная политика в образовании.

1. Государственная политика в сфере общего образования Российской Федерации. 2. Нормативное регулирование в области информационной безопасности детей. 3. Цифровая трансформация образования.

Модуль 2. Социальные угрозы сети Интернет.

1. Информационная безопасность. 2. Коллективная интернет-истерия. 3. Подростковый суицид как соцсетевой феномен. 4. Скулшутинг. 5. Опасный досуг.

Модуль 3. Технологические угрозы сети Интернет.

1. Вредоносные программы. 2. Сетевая гигиена. 3. Безопасное использование авторского контента.

Модуль 4. Психологические и техно-психологические угрозы сети Интернет.

1. Феномен онлайн игровой зависимости. 2. Фрейпинг, скам, псевдоблаготворительность. 3. Фишинг.

Модуль 5. Социально-технологические угрозы сети Интернет.

1. Что такое Darknet. 2. Наркоторговля в Darknet. 3. Правила безопасности соцсетей. 4. Кибербуллинг.

Модуль 6. Социально-психологические угрозы сети Интернет.

1. Радикальные группы. 2. Экстремизм, терроризм. 3. Группы смерти и ARG. 4. АУЕ и нонконформистские субкультуры.

По итогам прохождения теоретических модулей предусмотрены практические задания. Практическая работа выполняется онлайн на занятии, обучающиеся проверяют правильность выполнения работы в соответствии с листом самопроверки, размещенном в цифровой среде.

В заключение проводится итоговое тестирование для определения степени освоения программы и актуального уровня компетентности педагогов в сфере обеспечения информационной безопасности обучающихся.

Таким образом, результатом освоения данной программы педагогами стать повышение информационно-коммуникационной компетентности педагога, знание основных информационных угроз и умение строить алгоритмы безопасного использования сети Интернет детьми и подростками. И, как следствие, создание организационных и методических условий для обеспечения информационной безопасности обучающихся образовательных организаций. Учителя смогут применять на практике знания, полученные на лекциях и практических занятиях; организовать направления своей педагогической работы по реализации информационной безопасности; применять методы профилактики Интернет-зависимости учащихся.

Педагогические работники будут владеть информацией о правовой защите детей от влияния негативной информации и быть способным оградить их от факторов влияния; методами и формами защиты от негативной и разрушающей информации в сети Интернет; педагогической компетентностью в сфере информационной безопасности.

Список литературы

1. Бирюков А.А. Информационная безопасность: защита и нападение / А.А. Бирюков. – М.: ДМК-Пресс, 2017.

2. Хломов К.Д. Кибербуллинг в опыте российских подростков / К.Д. Хломов, Д.Г. Давыдов, А.А. Бочавер // Психология и право. – 2019.

3. Международная информационная безопасность. Теория и практика: учебник для вузов / под общ. ред. А.В. Крутских. – в 3 т. – М.: Аспект Пресс, 2019.

4. Ефимова Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: монография / Л.Л. Ефимова, СА. Кочерга. – М.: Юнити, 2016. – 239 с.

5. Курс «Безопасность в интернете» от Яндекса [Электронный ресурс]. – Режим доступа: https://yandex.ru/yaintern/schools/shkib (дата обращения: 18.01.2024).

6. Журнал для педагогов, психологов и родителей «Дети в информационном обществе» [Электронный ресурс]. – Режим доступа: http://www.fid.su/projects/journal (дата обращения: 18.01.2024).

7. Солдатова Г. Интернет: возможности, компетенции, безопасность: методическое пособие / Г. Солдатова, Е. Зотова, М. Лебешева, В. Шляпников [Электронный ресурс]. – Режим доступа: http://detionline.com/internet-project/training-aids (дата обращения: 18.01.2024).

8. «Урок полезного и безопасного Интернета» от компании МТС [Электронный ресурс]. – Режим доступа: http://detionline.com/mts/lessons (дата обращения: 18.01.2024).

9. Защита детей. Лаборатория Касперского [Электронный ресурс]. – Режим доступа: https://kids.kaspersky.ru/ (дата обращения: 18.01.2024).

10. Проект «Разбираем Интернет вместе с Google» [Электронный ресурс]. – Режим доступа: http://www.razbiraeminternet.ru/ (дата обращения: 18.01.2024).

11. Think with Google. Новое поколение интернет-пользователей: исследование привычек и поведения российской молодежи онлайн [Электронный ресурс]. – Режим доступа: https://clck.ru/382otb (дата обращения: 18.01.2024).

12. PricewaterhouseCoopers: аналитический обзор по теме информационной безопасности (2018) [Электронный ресурс]. – Режим доступа: https://www.pwc.ru/ru/publications/global-informationsecurity-survey-2018.html$ (дата обращения: 18.01.2024).

13. «Исследования» от Mail.ru Group [Электронный ресурс]. – Режим доступа: https://corp.mail.ru/ru/press/infograph/ (дата обращения: 18.01.2024).

14. Мальцева В.А. Защита детей от кибербуллинга. вопросы уголовноправового регулирования / В.А. Мальцева [Электронный ресурс]. – Режим доступа: https://clck.ru/382pFK (дата обращения: 18.01.2024).