Методические рекомендации
«Защита детей в цифровом пространстве»

Стремительное развитие и распространение новых информационных и телекоммуникационных технологий оказывает противоречивое влияние на все сферы жизнедеятельности социума: интернет-пространство характеризуется доступностью в получении информации, оперативностью ее передачи, способствует массовой коммуникации, но с другой стороны, одновременно, оно способно оказывать и негативное влияние как на отдельных людей, так и на общество в целом: вовлечение в нежелательные контакты социальных сетей, пропаганда насилия и экстремизма, игромания и интернет-зависимость, обман и вымогательство денег, склонению к суициду и совершению насильственных действий.

В современном мире с бурно развивающейся цифровой средой все большую актуальность приобретает проблема отрицательного влияния информационного общества, отличающегося насыщенностью и многообразием контента[1], на детей, чья способность адекватно перерабатывать информацию только формируется. Исследование рисков, с которыми сталкиваются в сети несовершеннолетние, а также технологий их защиты как никогда актуально сейчас, в эпоху, когда весь мир перешел в онлайн. В силу возраста и отсутствия опыта дети особенно уязвимы для различного рода киберпреступников, поэтому их безопасности в Интернете уделяется повышенное внимание. Сегодняшние риски трансформируются, раскрываются и усиливаются под влиянием технологических трендов и глобальных изменений в обществе. Проведенный мониторинг информационного пространства выявил следующие группы киберрисков[2]:

1. Криминализация: вовлечение детей в криминальные сообщества, продажа запрещенных товаров и услуг, радикализация и экстремизм, траффикинг (торговля людьми);

2. Маркетинговое давление, рискованные денежные отношения: интернет как канал сбыта товаров, опасных для жизни и здоровья людей, продвинутые методики маркетинга (таргет), темные паттерны (склонение пользователя к действиям, которые он считает нежелательными) и онлайн-мошенничество;

3. Личностная атака, психологическое насилие: кибербуллинг, сталкинг (преследование), груминг (установление взрослыми дружеских отношений с несовершеннолетними через Интернет для вступления с ними в интимную связь, запугивания и шантажа), сексуальные домогательства;

[1] содержимое веб-страниц, социальных сетей, каналов в мессенджерах и видеохостингах.

[2] Исследование ПАО «Ростелеком» «Технологии защиты детей в интернете» (https://www.company.rt.ru/social/kids-safety).

4. Цифровая эксплуатация, использование ребенка для создания цифрового контента: доксинг (поиск и открытая публикация персональной информации о человеке со злым умыслом), создание и распространение материалов с детской порнографией, кража сбор и эксплуатация персональных данных, шерентинг (размещение родителями контента, связанного с их детьми);

5. Информационное давление, информация, не предназначенная для детей и подростков: контент, содержащий сцены насилия, порнографический контент, дезинформация, опасные тренды и челленджи (вызовы);

6. Аддикция (злоупотребление), формирование зависимости от интернет-среды: алгоритмы удержания внимания, игровая зависимость, избыточное использование Интернета.

Обеспечение информационной безопасности личности и государства, является одним из национальных приоритетов современной государственной политик России и обеспечивается во взаимодействии законодательной, правоприменительной, правоохранительной, судебной, контрольной и других форм деятельности государственных органов при участии организаций и граждан.

Основу нормативно-правовой базы Российской Федерации, регулирующей общественные отношения, связанные в том числе с защитой детей от информации, причиняющей вред их здоровью и развитию, составляют:

1. Федеральный закон Российской Федерации от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации»[3];

2. Федеральный закон Российской Федерации от 27.07.2006 N 152-ФЗ «О персональных данных»;

3. Федеральный закон Российской Федерации от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»;

4. Указ Президента Российской Федерации от 05.12.2016 N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации".

Также, на законодательном уровне в Российской Федерации закреплены виды информации, запрещенной для распространения среди детей:

1) побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству, либо жизни и (или) здоровью иных лиц, либо направленная на склонение или иное вовлечение детей в совершение таких действий;

2) способная вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, никотинсодержащую продукцию, алкогольную и спиртосодержащую

[3] Далее – Федеральный закон № 149-ФЗ.

продукцию, принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством;

3) обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям или животным;

4) содержащая изображение или описание сексуального насилия;

5) отрицающая семейные ценности, пропагандирующая нетрадиционные сексуальные отношения и формирующая неуважение к родителям и (или) другим членам семьи;

6) оправдывающая противоправное поведение;

7) содержащая нецензурную брань;

8) содержащая информацию порнографического характера.

В сферах жизнедеятельности, где инновационный процесс проявился в большей степени (экономика, средства массовой коммуникации, образование и т.д.), основным инструментом-регулятором государства выступает уголовно-правовой механизм. Так, Уголовным кодексом Российской Федерации предусмотрена ответственность за преступления, совершенные в публичном выступлении, в средствах массовой информации или информационно-телекоммуникационных сетях:

1. Преступления против жизни и здоровья (гл. 16): доведение до самоубийства (ст. 110), склонение к совершению самоубийства или содействие совершению самоубийства (ст. 110.1), организация деятельности, направленной на побуждение к совершению самоубийства (ст. 110.2);

2. Преступления против свободы, чести и достоинства личности (гл. 17): клевета (ст. 128.1);

3. Преступления против половой неприкосновенности и половой свободы личности (гл. 18): развратные действия (ст. 135);

4. Преступления против семьи и несовершеннолетних (гл. 20): вовлечение несовершеннолетнего в совершение действий, представляющих опасность для жизни несовершеннолетнего (ст. 151.2);

5. Преступления против собственности (гл. 21): кража (ст. 158), мошенничество в сфере компьютерной информации (ст. 159.6);

6. Преступления против общественной безопасности (гл. 24): публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганда терроризма (ст. 205.2), публичное распространение заведомо ложной информации об обстоятельствах, представляющих угрозу жизни и безопасности граждан (ст. 207.1), публичное распространение заведомо ложной общественно значимой информации, повлекшее тяжкие последствия (ст. 207.2), публичное распространение заведомо ложной информации об использовании Вооруженных Сил Российской Федерации, исполнении государственными органами Российской Федерации своих полномочий (ст. 207.3), публичные призывы к осуществлению экстремистской деятельности (ст. 280), публичные призывы к осуществлению действий, направленных на нарушение территориальной целостности Российской Федерации (ст. 280.1), публичные действия, направленные на дискредитацию использования Вооруженных Сил Российской Федерации в

целях защиты интересов Российской Федерации и ее граждан, поддержания международного мира и безопасности или исполнения государственными органами Российской Федерации своих полномочий в указанных целях (ст. 280.3), публичные призывы к осуществлению деятельности, направленной против безопасности государства (ст.280.4), возбуждение ненависти либо вражды, а равно унижение человеческого достоинства (ст. 282);

7. Преступления против здоровья населения и общественной нравственности (гл. 25): незаконные изготовление и оборот порнографических материалов или предметов (ст. 242), изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних (ст. 242.1), использование несовершеннолетнего в целях изготовления порнографических материалов или предметов (ст. 242.2);

8. Преступления против мира и безопасности человечества (гл. 34): призывы к развязыванию агрессивной войны (ст. 354), реабилитация нацизма (ст. 354.1).

В Российской Федерации одним из технических инструментов, обеспечивающих безопасное функционирование пользователей в сфере IT-технологий, является институт блокировки Интренет-ресурсов, содержащих и распространяющих противоправный контент.

Порядок ограничения доступа к информации, распространяемой с нарушением закона определен статьями 15.1–15.6-1, 15.8, 15.9 Федерального закона № 149-ФЗ, функциями по контролю и надзору в сфере средств массовой информации, в том числе электронных, и массовых коммуникаций, информационных технологий и связи наделена Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)[4].

Также на Роскомнадзор возложена функция по приему сообщений от граждан, юридических лиц, индивидуальных предпринимателей, органов государственной власти, органов местного самоуправления о наличии на страницах сайтов в интернет-пространстве противоправной информации посредством направления соответствующих обращений в Общественную электронную приемную Роскомнадзора (https://rkn.gov.ru/treatments/ask-question/).

Эффективным методом борьбы с распространением запрещенного контента в социальных сетях и сообществах является модерация, т.е. регулярный мониторинг соблюдения правил общения на цифровой площадке, которые установил владелец или администратор ресурса, проверка и блокировка материалов, а также право пользователя обратиться к администратору ресурса с жалобой на незаконный контент.

К технологическим решениям по защите детей в киберпространстве относятся и инструменты родительского контроля, которые предоставляют родителям повышенную степень контроля над действиями детей в онлайн- и офлайн-среде посредством установки специального программного обеспечения

[4] Постановление Правительства Российской Федерации от 16.03.2009 N 228 «Об утверждении Положения о Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций».

на смартфоны, компьютеры и другие устройства, к которым ребенок имеет доступ. В базовый функционал инструментов родительского контроля входит блокирование доступа к интернету, приложениям и играм, ограничение экранного времени, защита от ненадлежащего контента путем его фильтрации, отслеживание онлайн-активности, контактов и местоположения ребенка. Эти функции заключаются в проактивной регуляции и мониторинге действий ребенка в интернете, поэтому такие программы позволяют выявлять и заблаговременно минимизировать киберриски для детей. Несмотря на широкий спектр функций подобных программ, полная изоляция ребенка от киберрисков не будет способствовать выработке необходимых компетенций в области кибербезопасности, которые понадобятся ему в будущем.

Стоит помнить, что инструменты родительского контроля, которые позволяют осуществлять постоянное наблюдение за ребенком, могут разрушить доверие к родителям, а в отдельных случаях даже могут повлечь психологические травмы и депрессию. В случае, когда ребенок или подросток испытывает отторжение и непринятие инструментов родительского контроля, он может найти способы обхода установленных правил.

Одним из способов защиты детей в интернете является использование Интернет-фильтров, которые блокируют доступ к нежелательным сайтам и скачивание файлов определенной тематики, ограничивают запуск приложений и игр. Также существуют специальные программы, которые обеспечивают фильтрацию интернет-ресурсов по встречающимся ключевым словам без необходимости внесения родителями вручную в черный список отдельных сайтов с неприемлемым для детей контентом. Такие фильтры не привязаны ко времени реагирования команды модераторов или нейросети, они защищают ребенка постоянно.

В современных реалиях особенно важно развивать у детей навыки цифровой гигиены, соблюдение базовых принципов которой позволит минимизировать уровень негативного влияния медиапространства[5]:

1. Обновление программного обеспечения, использование антивирусных программ и уникальных и сложных паролей, двухфакторной аутентификации;

2. Воздержаться от общения с неизвестными пользователями, от распространения информации личного характера о себе и своих близких, не ставить отметки о геолокации;

3. Относится с подозрением к электронным сообщениям, требующим немедленно перейти по ссылке, позвонить или открыть вложение, перевести деньги или оплатить выигрыш;

4. Помнить, что интернет — это публичное пространство, и вести себя в нем нужно точно также, как в любом другом общественном месте.

[5] С. Макаров Прекрасный, опасный, кибербезопасный мир. Всё, что важно знать детям и взрослым о безопасности в интернете – www.company.rt.ru/social/book_cybersecurity/files/_SMakarov_fullBook_light.pdf.