государственное бюджетное общеобразовательное учреждение Самарской области средняя общеобразовательная школа имени полного кавалера ордена Славы Петра Васильевича Кравцова с. Старопохвистнево муниципального района Похвистневский Самарской области

Алгоритм реагирования на запрещенный информационный контент

Общие положения

В соответствии с пунктом 6, пп.2 статьи 28 «Компетенция, права, обязанности и ответственность образовательной организации» Федерального закона от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации» дошкольные образовательные учреждения и общеобразовательные организации обязаны создавать безопасные условия обучения, в том числе при проведении практической подготовки обучающихся, а также безопасные условия воспитания обучающихся, присмотра и ухода за обучающимися, их содержания в соответствии с установленными нормами, обеспечивающими жизнь и здоровье обучающихся, работников образовательной организации.

Под информационной безопасностью детей (далее – Безопасность) Правительство РФ понимает состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и физическому, психическому, духовному, нравственному развитию (Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»).

В разделе первом распоряжения Правительства РФ от 28.04.2023 № 1105-р «О концепции информационной безопасности детей в Российской Федерации» (далее – Концепция) отмечается, что современные дети - первое поколение, чье взросление происходит на фоне стремительно развивающихся информационно-коммуникационных технологий. В своих привычках, ценностях и поведении в сети «Интернет» эта группа принципиально отличается от представителей более старшей аудитории (18-45 лет). Их основными интересами являются общение в социальных сетях, просмотр видео и онлайн-игры.

Вместе с тем указанная аудитория является крайне уязвимой с точки зрения информационной безопасности. В связи с высокой степенью анонимности интернет-пространства и возможностью выстраивания общения с использованием нескольких профилей и псевдонимов риск проявления

асоциальных форм поведения в цифровой среде увеличивается.

Нестабильность эмоциональной сферы и низкий уровень критичности восприятия и обработки информационного потока детьми и подростками свидетельствуют о том, что именно дети и подростки находятся в группе потенциального риска для негативного воздействия и интернет-манипуляций с последующим вовлечением в деструктивную деятельность.

Деструктивное информационное воздействие способствует развитию формирования у детей и подростков неправильного восприятия традиционных российских духовно-нравственных ценностей, провоцирующего «психологический слом», следствием которого могут стать как депрессивное состояние, так и проявление девиантного поведения, повышенной агрессии к окружающим.

В области виртуальной коммуникации дети подвержены рискам стать жертвой компьютерного мошенничества и вымогательства, вовлечения в сексуальную эксплуатацию, террористическую и экстремистскую деятельность, распространение наркотических средств, психотропных веществ и их прекурсоров, аналогов наркотических средств и психотропных веществ и новых потенциально опасных психотропных веществ посредством игровых активностей, а также в сообщества с нарушением общепринятых норм морали.

Действия руководителя организации и педагогических работников по созданию условия для обеспечения безопасности детей

В соответствии с Концепцией образовательные организации обязаны обеспечить безопасность детей. Ответственность за ее обеспечение несет руководитель образовательной организации (далее – Руководитель). Кроме этого, в обеспечении безопасности должны принимать участие все работники образовательной организации в пределах своей компетенции.

Руководитель:

- ✓ утверждает приказ об организации безопасности в образовательной организации с указанием ответственного за ее обеспечение;
- ✓ ведет общий контроль исполнения поручений в сфере инфобезопасности; утверждает локальные акты по вопросам инфобезопасности;
- ✓ организует взаимодействие с социальными партнерами, госорганами, общественными организациями по вопросам инфобезопасности.

Заместитель Руководителя:

- ✓ организует мониторинг соблюдения работниками законодательства в сфере инфобезопасности и защиты прав детей;
- ✓ предлагает проекты планов мероприятий в сфере обеспечения

инфобезопасности в образовательной организации.

Ответственный за безопасность:

- ✓ контролирует исправность работы системы контент-фильтрации ресурсов сети Интернет;
- ✓ организовывает мониторинг исполнения мероприятий, направленных на защиту детей от негативной информации – причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования, в том числе включенных в план мероприятий по обеспечению безопасности обучающихся образовательной организации;
- ✓ организовывает просветительские мероприятия с социальными партнерами и (или) обеспечивает участие работников образовательной организации в таких мероприятиях;
- ✓ готовит списки педагогических работников, которым необходимо пройти профессиональное обучение в сфере защиты детей от видов информации, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования;

Учитель и воспитатель:

- ✓ контролирует, чтобы содержание частей ООП и их реализация обеспечивали комфортную атмосферу для детей, позволяли обучить детей вопросам информационной безопасности;
- ✓ подбирает средства обучения и воспитания, которые соответствуют законодательству, в том числе с позиции информационной безопасности.

Классный руководитель:

- ✓ реализует воспитательные мероприятия, в том числе по вопросам безопасности;
- ✓ взаимодействует с родителями, чтобы углубить их знания в сфере инфобезопасности, объясняет, как обучить этому детей.

Педагог-психолог:

- ✓ проводит просветительскую и профилактическую работу по вопросам психологической уязвимости в цифровой среде;
- ✓ проводит индивидуальную работу с детьми и родителями, если они пострадали от действий в интернете: мошенничества, буллинга и т. д.

Администратор сайта образовательной организации:

- ✓ осуществляет мониторинг наполнения сайта школы, в том числе на соответствие законодательства о защите прав детей;
- ✓ контролирует, чтобы наполнение госпабликов соответствовало правилам инфобезопасности, в том числе создает просветительский контент по этим вопросам.

Педагог-библиотекарь:

- ✓ контролирует безопасность использования цифровых ресурсов библиотеки;
- ✓ осуществляет мониторинг состава библиотечного фонда на предмет отсутствия литературы экстремистского характера и другой, способной причинить вред психике детей.

Алгоритм реагирования на запрещенный информационный контент

В соответствии с Федеральным законом от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации», разработан механизм внесудебного блокирования запрещенной информации, что позволяет оперативно исключить к ней доступ в любой мобильной или проводной сети.

В целях оперативного реагирования на появление в сети «Интернет» запрещенной информации, Роскомнадзор предлагает направлять заявки в единую автоматизированную информационную систему (далее – ЕАИС) «Единый реестр» посредством заполнения формы, размещенной по адресу https://eais.rkn.gov.ru/feedback/

Процедура рассмотрения заявок в ЕАИС «Единый реестр» представлено на рисунке 1.

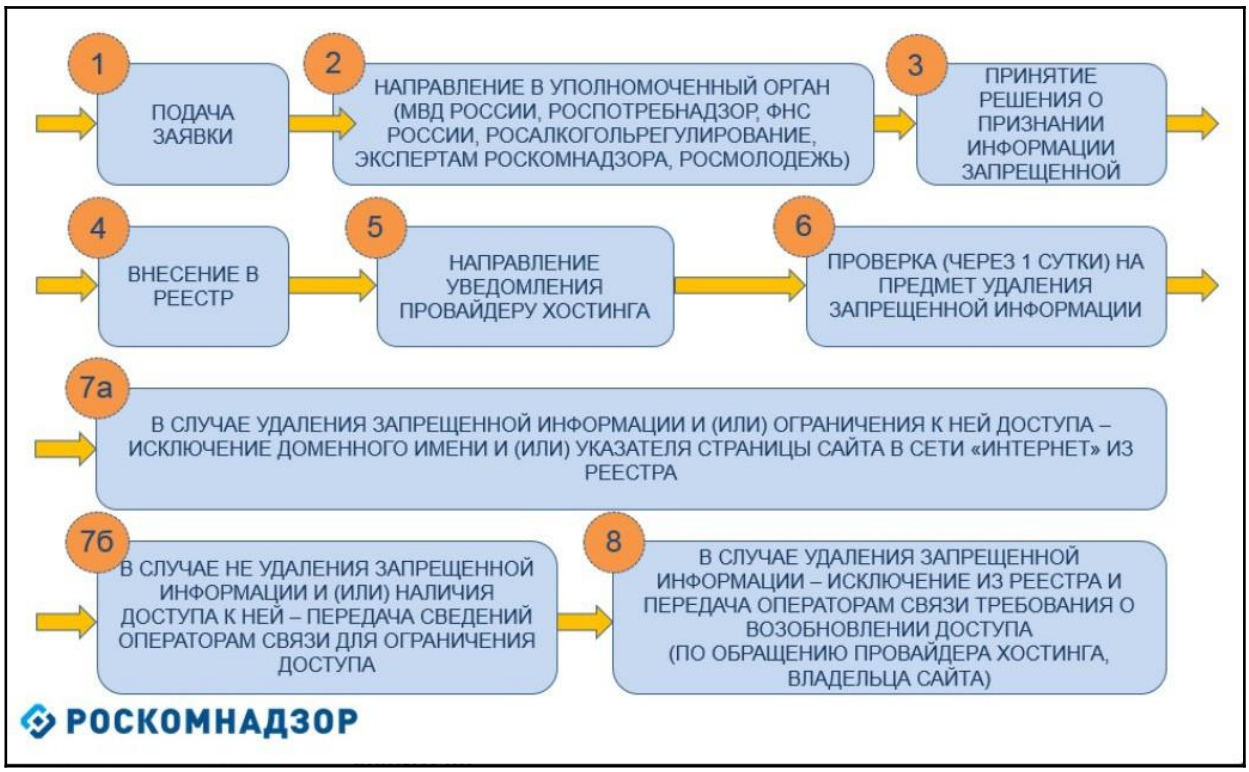

Рисунок 1. Рассмотрение заявок в ЕАИС «Единый реестр»