

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ЗАЩИТЫ НЕСОВЕРШЕННОЛЕТНИХ ОТ ДЕСТРУКТИВНОЙ ИНФОРМАЦИОННОЙ СРЕДЫ НА ПРИМЕРЕ АВСТРАЛИИ

С.В. Черкасова, П.Н. Сафоненков

Москва, Государственный университет управления

Проблема деструктивного влияния информационного пространства на несовершеннолетних стоит достаточно остро во всех государствах, где средства интернет-коммуникации широко популярны и доступны вследствие высокого уровня развития коммуникационных технологий, наличия инфраструктуры и всеобщего перехода к информационному обществу. В связи с острой необходимостью контроля за данной сферой общественных отношений многие государства нормативно урегулировали вопросы, касающиеся защиты несовершеннолетних граждан от деструктивной информационной среды, ярким примером является Австралия, где законодательная база в области информационной безопасности находится на высоком уровне.

В Глобальном индексе кибербезопасности в мировом рейтинге по состоянию на 2020 год Австралия занимает 12 позицию [2]. В стране недавно был принят Закон о безопасности в Интернете № 76 от 23 июля 2021 г. (Online Safety Act 2021) [3], сам законопроект был разработан ещё в 2019 году, но в ходе рассмотрения вносилось большое количество поправок, в связи с чем процесс принятия занял достаточно много времени.

Закон предусматривает введение должности уполномоченного по электронной безопасности (eSafety Commissioner), в компетенцию которого входит:

- обеспечение функционирования системы подачи жалоб на материалы, содержащие элементы киберзапугивания в адрес несовершеннолетних, содержащие интимные изображения граждан без их согласия;
- координация деятельности министерств, органов и агентств в целях обеспечения информационной безопасности граждан Австралии;
- поддержка, аккредитация, оценка деятельности организаций, рекламных и информационных программ, которые занимаются Интернет-безопасностью граждан;
- поддержка, проведение, оценивание исследований уровня Интернет-безопасности австралийцев;
- предоставление министру регулярных отчётов по уровню кибербезопасности граждан, консультирование по вопросам информационной безопасности;
- обеспечение функционирования Закона о безопасности в Интернете и пр.

Основные требования к безопасности Интернет-контента определяет министр. Закон предусматривает ответственность для лиц, которые не только публикуют интимные изображения гражданина без его согласия, но и для лиц, которые угрожают опубликовать такие изображения (ст. 4).

В Законе предусмотрены критерии, по которым определяют, какой цифровой контент считать вредным для несовершеннолетних. Так, вредоносной считается информация, размещённая в свободном доступе на Интернет-площадках, которую обычный человек счел бы негативно воздействующей для детей (ст. 6). Также определены критерии признания контента агрессивным, оскорбительным. Объектом Закона является любая информация в открытом доступе.

В Австралии законодательно конкретизированы основные требования к безопасности в Интернете, среди которых:

- информация не может содержать материалы киберзапугивания детей и взрослых, интимные изображения граждан без их согласия, материалы, пропагандирующие насилие;

- при публикации информации 2 класса важно обеспечить принятие технических мер для предотвращения детей доступа к контенту (Ст. 107 Закона о безопасности в Интернете №76 к материалам 2 класса относит контент, предназначенный, по оценкам Квалификационной комиссии, для возрастной группы граждан старше 18 лет, а также контент, не классифицированный комиссией, но который в случае оценки, вероятно, получил бы ограничение 18 +);

- поставщик услуги обязан принимать и рассматривать жалобы на контент от пользователей по запросу уполномоченного по электронной безопасности, предоставлять ему отчёт по количеству жалоб и их природе, а также принятым мерам по поступившим обращениям (часть 4 Закона № 76).

В случае если установлен факт опубликования неправомерной информации, служба социальных сетей/ электронная службе/ Интернет-служба направляет автору уведомление с требованием удалить материал из всеобщего доступа, извиниться за публикацию, а также официальное предупреждение воздержаться от публикации любых подобных неправомерных материалов в будущем (ст. 64). Если за 12 месяцев виновное лицо нарушило положения действующего законодательства 2 и более раз, уполномоченный по электронной безопасности может обратиться в Федеральный суд с требованием прекратить деятельность по предоставлению услуг в Интернет-пространстве (ст. 156).

Закон позволяет органам и ассоциациям, осуществляющим деятельность в сфере онлайн-индустрии, разрабатывать отраслевые кодексы. Уполномоченный по электронной безопасности вправе установить отраслевой стандарт в сфере Интернет-безопасности (ст. 105). Отраслевые кодексы и стандарты могут регулировать круг следующих вопросов:

- процедуры работы с материалами 1 и 2 класса;
- процедуры информирования администраторов и провайдеров об ответственности, предусмотренной за размещение неправомерной информации;
- информирование пользователей о наличии, использовании и применении программного обеспечения для фильтрации Интернет-контента и пр.

Кроме того, в стране ведётся чёрный список сайтов, блокируют за распространение запрещённой законом информации. Сформированный

единый чёрный список доступен для всех провайдеров, которые осуществляют демонстрацию материалов через фильтр заблокированного контента.

На данный момент в стране разрабатывается Австралийская стратегия кибербезопасности 2023-2030, она предусматривает создание «киберщитов» по всей стране, которые включают в себя обучение граждан и работников предприятий противодействию киберугрозам, разработку новых глобальных стандартов цифровой безопасности, создание системы обмена информацией об угрозах и блокировке мирового масштаба и пр. [1]

Таким образом, в Австралии существует всеобъемлющая и масштабная нормативно-правовая база, направленная на законодательное противодействие современным информационным угрозам.

Список литературы

1. Australia's new cybersecurity strategy: Build "cyber shields" around the country [Electronic resource]. – Mode of access: <https://www.csoonline.com/article/652708/australias-new-cybersecurity-strategy-to-build-6-cyber-shields-around-the-country.html>. – Date of access: 11.10.2023.
2. Global Cybersecurity Index 2020 [Electronic resource]. – Mode of access: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf. – Date of access: 11.10.2023.
3. Online Safety Act 2021 No. 76 [Electronic resource]. – Mode of access: <https://www.legislation.gov.au/Details/C2021A00076>. – Date of access: 11.10.2023.

НЕКОТОРЫЕ ВОПРОСЫ ОРГАНИЗАЦИИ ПОЛИКУЛЬТУРНОГО ВОСПИТАНИЯ В СТАВРОПОЛЬСКОМ КРАЕ

О.Н. Шалыгина

Ставрополь, Ставропольский государственный педагогический институт

Ю.В. Королькова, А.Г. Лазарева

*Ставрополь, Ставропольский краевой институт
развития образования, повышения квалификации и переподготовки
работников образования*

В последние годы в российском обществе четко наметилась тенденция понимания необходимости объединяющих российских граждан ориентиров и ценностей, потребность поликультурного воспитания подрастающего поколения, обучения его цивилизованным нормам взаимоотношений в вопросах, затрагивающих интересы отдельного человека, коллектива, общества, государства и требующих обязательных для всех решений при взаимодействии институтов гражданского общества. Об этом неоднократно в своих посланиях Федеральному Собранию говорил Президент России В.В. Путин, подчеркивая важность духовного единства народа России и объединяющие его моральные ценности.

В научной литературе и практике появилось понятие «российский патриотизм» [2], важной характеристикой которого является идентификация