Необходимость проводить соответствующее обучение сотрудников для повышения у них навыка противостояния социоинженерным атакам отмечена и в работе Dina Aladawy, Kristian Beckers, Sebastian Pape [2]. Указанные авторы считают, что наиболее эффективными в данной области могут стать деловые игры, в процессе которых сотрудники учатся противостоять мошенникам. Соответственно, сегодня назрела острая необходимость обеспечить обучение сотрудников компаний умению распознавать риски, связанные с социоинженерными атаками, и противостоять им. Практика показывает, что осведомленность сотрудников о возможных угрозах является лучшей защитой от утечки данных [3].

Таким образом, можно констатировать, что обучение сотрудников компании методам противодействия социоинженерным атакам является наиболее эффективным средством защиты от такого типа угроз.

Список литературы

1. Sanders, C. A. (2018). *Social Engineering Knowledge Measured as a Security Countermeasure*. (Master's thesis). – URL: https://scholarcommons.sc.edu/etd/4567

2. Aladawy, D., Beckers, K., & Pape, S. (2018). PERSUADED: Fighting Social Engineering Attacks with a Serious Game. In *Lecture notes in computer science* (Pp. 103–118). – DOI: https://doi.org/10.1007/978-3-319-98385-1_8

3. Hussain Ali Aldawood, Geoffrey SkinnerA Critical Appraisal of Contemporary Cyber Security Social Engineering Solutions: Measures, Policies, Tools and Applications.

Г. А. Грищенко,
кандидат юридических наук, доцент,
Московский государственный юридический
университет имени О. Е. Кутафина (МГЮА)

ПРАВОВЫЕ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЕТЕЙ В ЦИФРОВОЙ СРЕДЕ

Аннотация. В современном цифровом мире дети являются наиболее уязвимой аудиторией пользователей в сети Интернет. Чрезмерное доверие несовершеннолетних к популярным блогерам (инфлюенсерам) приводят к тому, что зачастую размываются границы реальной и виртуальной жизни, и, как следствие, может привести к причинению вреда жизни и (или) здоровью себе и окружающим. Целью статьи является проведение анализа законодательства, правоприменительной практики, общественного мнения и научной литературы в области регулирования информационной безопасности детей, и выработка рекомендаций по совершенствованию правовой регламентации соответствующих отношений с учетом новых вызовов и угроз в условиях цифровизации. Проведенный анализ показал недостаточность и неэффективность регулирования некоторых аспектов обеспечения информационной безопасности детей в цифровой среде. В качестве

выводов предложены рекомендации по реализации правовых решений, которые помогут достичь должного уровня регламентации отдельных направлений по обеспечению информационной безопасности детей в цифровой среде.

Ключевые слова: информационная безопасность детей, угрозы в цифровой среде, сеть Интернет, цифровые технологии, деструктивный «вредный» контент, правовые проблемы, совершенствование законодательства

LEGAL PROBLEMS OF ENSURING THE INFORMATION SECURITY OF CHILDREN IN THE DIGITAL ENVIRONMENT

Abstract. In today's digital world, children are the most vulnerable audience of Internet users. Excessive trust of minors in popular bloggers (influencers) leads to the fact that the boundaries of real and virtual life are often blurred, and, as a result, can lead to harm to life and (or) health to oneself and others. The purpose of the article is to analyze legislation, law enforcement practice, public opinion and scientific literature in the field of regulating information security of children, and to develop recommendations for improving the legal regulation of relevant relations, taking into account new challenges and threats in the context of digitalization. The conducted analysis showed the insufficiency and inefficiency of regulation of some aspects of ensuring information security of children in the digital environment. As conclusions, recommendations are proposed for the implementation of legal solutions that will help achieve the proper level of regulation of certain areas to ensure the information security of children in the digital environment.

Keywords: information security of children, threats in the digital environment, the Internet, digital technologies, destructive "harmful" content, legal problems, improvement of legislation

Введение. В современных цифровых реалиях одной из самых уязвимых категорий с позиции обеспечения информационной безопасности являются дети. Учитывая постоянное совершенствование цифровых технологий и расширение сферы их применения, дети наиболее подвержены не всегда положительному влиянию сети Интернет. При этом зачастую выявить информационные угрозы цифровой среды достаточно сложно и взрослым, и специалистам в сфере информационной безопасности (особенно это касается так называемой «фейковой» информации, когда, например, дипфейки способны подделать не только изображение человека, но и его голос).

По результатам различных социологических исследований (ВЦИОМ, Лига безопасного Интернета, Лаборатория Касперского и др.), более половины несовершеннолетних детей практически постоянно находятся в сети Интернет (более 60 % лиц возраста 13–16 лет), при этом количество проводимого времени в данном виртуальном пространстве с каждым годом увеличивается (до 8–10 часов в сутки). Доля детей дошкольного и младшего школьного возраста в общей статистике по количеству проводимому времени в Интернете тоже с каждым годом возрастает, что свидетельствует о повышении значимости данной формы коммуникации в современном обществе [2; 3; 5; 8].

Таким образом, проблема обеспечения информационной безопасности усложняется тем, что с каждым годом количество детей, проводящих время в цифровой среде, увеличивается, а возраст знакомства с виртуальным пространством снижается, о чем свидетельствуют различные опросы общественного мнения.

Основная часть. Погруженность детей с самого раннего возраста в информационную среду Интернета отражается на дальнейшей социализации ребенка дошкольного возраста и может создавать определенную трудность при вхождении ребенка, например, в образовательное пространство, именно поэтому с малых лет важно обеспечить безопасность детей относительно информации, полученной из сети Интернет, и научить извлекать полезное и познавательное самостоятельно [1. С. 38–40; 4].

Выработка эффективных механизмов по вопросам обеспечения информационной безопасности детей в контексте ее правовой регламентации на протяжении последних лет является одной из наиболее обсуждаемых тем не только в масштабах отдельной страны, но и всего мирового сообщества, что подтверждается соответствующими концептуальными и стратегическими нормативными правовыми актами (например, указы Президента Российской Федерации от 17 мая 2023 г. № 358 «О Стратегии комплексной безопасности детей в Российской Федерации на период до 2030 года», от 9 ноября 2022 г. № 809 «Об утверждении Основ государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей», от 2 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации», от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации», Распоряжение Правительства Российской Федерации от 22 декабря 2022 г. № 4088-р «Об утверждении Концепции формирования и развития культуры информационной безопасности граждан Российской Федерации»).

Анализ вышеуказанных документов показывает, что основное внимание государства нацелено на формирование у детей и взрослых знаний (навыков, умений) по всему спектру вопросов обеспечения информационной безопасности (распознавание дипфейков, различных форм цифрового мошенничества, создание и систематическое обновление надежных паролей, критическая оценка получаемой информации, владение мерами противодействия распространению «вредной» информации и т. д.).

При этом, несмотря на все принимаемые государством меры, существующая ситуация свидетельствует о наличии определенных проблем по созданию эффективных механизмов по предотвращению (минимизации) распространения «вредного» деструктивного контента среди детей в цифровой среде (прежде всего, это касается социальных сетей, мессенджеров и иных каналов активного взаимодействия пользователей сети Интернет). Статистика обращений в государственные и общественные структуры по вопросам обеспечения информационной безопасности, рассматриваемых споров, рост объема распространения незаконного контента в Интернете и цели втягивания в соответствующие сообщества де-

тей свидетельствуют о том, что правовое регулирование не успевает за слишком активным развитием общественных отношений в рассматриваемом контексте.

Конечно, в Российской Федерации приняты определенные нормативные правовые акты, целью которых является защита детей от информации, причиняющей вред их здоровью и развитию. Среди таких актов, прежде всего, следует отметить Конституцию Российской Федерации, федеральные законы от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» (далее – ФЗ о защите детей от информации) и от 24 июля 1998 г. № 124-ФЗ «Об основных гарантиях прав ребенка в Российской Федерации» (далее – ФЗ об основных гарантиях прав ребенка), устанавливающие базовые принципы обеспечения безопасности детей в интернет-среде.

Отдельные вопросы реализации общественных отношений, связанных с оборотом разного рода информации, регулируются федеральными законами от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее – ФЗ об информации) и от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

Особое внимания заслуживает новая Концепция информационной безопасности детей в Российской Федерации, утвержденная Распоряжением Правительства Российской Федерации от 28 апреля 2023 г. № 1105-р, которая определяет принципы обеспечения информационной безопасности детей и приоритетные задачи, а также механизмы реализации государственной политики в данной сфере (предыдущая Концепция действовала с 2015 по 2020 гг.).

На региональном уровне также принимаются нормативные документы, направленные на регламентацию различных аспектов обеспечения информационной безопасности детей в цифровой среде. Например, во многих субъектах Российской Федерации действует проект «КиберПатруль», главной целью которого является формирование безопасного интернет-пространства для несовершеннолетних, поиск «вредной» деструктивной информации, проведение информационной работы по безопасности в сети с несовершеннолетними и их родителями (Красноярск, Тюмень, Курск, Иркутск и др.). Деятельность подобных проектов, несомненно, способствует повышению эффективности противодействия киберпреступности среди детей разных возрастных категорий и обеспечения информационной безопасности.

Регулирование вопросов обеспечения информационной безопасности детей осуществляется также на отраслевом уровне (например, Приказ Минцифры России от 1 декабря 2020 г. № 644 «О плане мероприятий, направленных на обеспечение информационной безопасности детей, на 2021 – 2027 годы», Письмо Минобрнауки России от 28 апреля 2014 г. № ДЛ-115/03 «О направлении методических материалов для обеспечения информационной безопасности детей при использовании ресурсов сети Интернет»).

Несмотря на сформировавшуюся в целом нормативно-правовую базу регулирования обеспечения информационной безопасности детей в цифровой среде, остается еще много нерешенных вопросов в данной области. Появляются новые условия и возможности для совершения новых правонарушений, не всегда охватываемых действующими составами уголовного и административного зако-

нодательства или недостаточно четко и однозначно их определяемые (например, кибербуллинг, треш-стрим); когнитивные возможности детей и особенности психологического развития данной возрастной группы не всегда готовы правильно оценить ситуацию и среагировать на возможные угрозы из сети Интернет.

В связи с этим представляется целесообразным изменить подход к понятийному аппарату данной сферы и расширить трактовку информационной безопасности детей, сделав акцент именно на информационно-психологической безопасности детей, включив соответствующие изменения в ФЗ о защите детей от информации.

Наличие пробелов (коллизий) в праве, стремительное развитие информационных (цифровых) технологий, недостаточный уровень цифровой грамотности, игнорирование правил безопасной работы в цифровой среде обусловливают необходимость совершенствования российского законодательства в сфере обеспечения информационной безопасности детей.

Очевидно, что со временем степень вызовов, угроз и рисков в цифровой среде будет только возрастать, будут появляться новые категории (сущности) общественных отношений, требующих тщательной проработки и правового регулирования. Трагические события в учебных заведениях, связанные с применением насилия в отношении учащихся и педагогов («колумбайны»), порождают в обществе дискуссии не только по поводу ужесточения мер по обороту оружия, но и по поводу интернет-контента, влияющего на сознание ребенка, повышающего уровень его агрессивности, снабжающего опасными знаниями. Последнее дело в Челябинской области, когда мальчик принес в школу самодельное взрывное устройство, которое смастерил по видеоурокам в Интернете (причем родители не препятствовали таким занятиям, поощряя научный потенциал сына), демонстрирует, что изменения в российском законодательстве просто необходимы [6].

В Интернете существует огромное количество разнообразных сообществ, которые представляют собой аккумуляцию молодежных субкультур и которые могут распространять «вредную» информацию, хотя изначально они позиционируют себя как тематические группы, созданные с целью объединения единомышленников, никак не противоречащей законодательству (фурри, слэш, ауе, аниме и др.).

Подобные интернет-сообщества могут знакомить сразу со всеми видами деструктивной информации (пропаганда наркотиков, суицидов, школьных расстрелов, нетрадиционных отношений и т. д.), которая всегда подается с юмором, лишая возможности ребенку критически оценить возможную опасность от потребляемого контента. Со временем ребенок подписывается на узкотематические группы и попадает под негативное влияние руководителей (кураторов) соответствующих сообществ.

Многие специалисты, занимающиеся анализом практики вовлечения детей в деструктивные сообщества, говорят о так называемых «воронках вовлечения» [7], которые отражают последовательность действий ребенка и рост его зависимости от выполнения разнообразных опасных заданий.

Так, изначально информация по различным темам (суицид, травля, наркотики) размещается в открытой группе, в которую ребенок может вступить, вы-

полнив определенное простое задание. Усложняя задания, куратор сообщества постепенно переключает внимание ребенка на его важность и значимость в данной группе, находясь в которой можно только соблюдая некоторые правила, характерные для данной субкультуры. Со временем ребенок переходит в закрытые группы, в которых общение происходит в основном посредством личных сообщений, и заканчивается такая «игра» выполнением заданий в реальном времени.

Отдельно стоит отметить необходимость донесения до детей информации о возможности попадания в такие зависимые группы и о правильности реагирования на получение соответствующих приглашений по вступлению в подобные интернет-сообщества.

В связи с этим считаем необходимым продолжить работу по просвещению детей, а также их родителей и учителей в сфере обеспечения информационной безопасности, проводя в образовательных учреждениях специальные уроки по знакомству с новыми формами мошенничества в цифровой среде, с новыми техническими решениями (программами, сервисами, платформами) по выявлению информации, не соответствующей действительности (сайты по распознаванию дипфейков) и т. д.

Хотелось бы обратить внимание еще на одну проблему обеспечения информационной безопасности, которая затрагивает в целом всех субъектов интернет-пространства – обеспечение защиты персональных данных, когда незаконная обработка личной информации может использоваться злоумышленниками в противоправных целях.

Статистика свидетельствует, что дети зачастую не осознают все потенциальную опасность размещения в Интернете личной информации о себе и членах своей семьи:

– 58 % указывают свой домашний адрес и мобильный телефон;
– 39 % указывают номер школы;
– 29 % выкладывают фото, на которых видна обстановка в квартире;
– 23 % размещают информацию о родителях и родственниках;
– 10 % указывают свой реальный возраст;
– 7 % публикуют геолокацию [7].

Очевидно, что дети должны знать, какие персональные данные существуют (к которым, помимо общеизвестных фамилии, имени, отчества, относятся также изображение, голос, отпечатки пальцев и др.), кому и как их можно предоставлять и в каких случаях следует обратиться за помощью к взрослым.

Учитывая вышеизложенное, представляется целесообразным дальнейшую работу по совершенствованию российского законодательства в сфере обеспечения информационной безопасности детей выстраивать по следующим направлениям:

1) следует унифицировать понятийный аппарат в рассматриваемой сфере, определить особенности распространения информации в сети Интернет, ориентированной на детскую аудиторию (особенно в социальных сетях), осмыслить и сформулировать новые составы правонарушений, к которым может привести распространение деструктивного контента, и внести соответствующие изменения в нормативные правовые акты;

В связи с этим целесообразно в ФЗ о защите детей от информации ввести дефиницию вредной (вредоносной) информации, определить ее критерии, и в целом расширить трактовку самой категории «информационная безопасность детей», определив ее как «информационно-психологическую безопасность детей».

2) учитывая, что контент в сети Интернет может быть как положительным, так и негативным (деструктивным), необходимо привить детям навыки по его анализу и конструктивной оценке. В связи с этим представляется необходимым включение в образовательный процесс уроков информационной безопасности, цифровой грамотности (цифровой гигиены) и проведение просветительских мероприятий для родителей и работников сферы образования;

Необходимо усилить работу по методической поддержке образовательных учреждений в сфере информационной безопасности детей, разработать понятные и доступные учебно-просветительские материалы.

3) очевидно, что влияние цифровых медиа (социальных сетей, форумов, блогов и проч.) на процессы формирования и проявления общественного мнения достаточно существенно, особенно среди детей. Это требует разработки принципиально новых механизмов реагирования на нарушения в цифровой среде, например, в рамках деятельности блогеров, тиктокеров и других лидеров молодежного мнения в цифровом пространстве России, в части досудебной блокировки неправомерного контента в сети Интернет. Необходимо усовершенствовать механизм подачи электронных жалоб на обнаруженный незаконный контент, особенно в различных мессенджерах;

4) также следует разделить угрозы информационной безопасности детей по степени их общественной опасности и возможных негативных последствий (аутодеструктивные, суицидальные, экстремистские и проч.), что должно найти отражение в уголовном и административном законодательстве в части выработки эффективного соотношения между наносимым вредом и уровнем ответственности, а также в части предупреждения совершения противоправных деяний в цифровой среде.

Заключение. Комплексная реализация представленных предложений позволит развить теоретические и практико-ориентированные положения по вопросам исключения (минимизации) угроз распространения деструктивного контента в сети Интернет, и выработать действенную эффективную систему принципов, приоритетных задач и механизмов, обеспечивающих реализацию государственной политики в области информационной безопасности детей.

Список литературы

1. Алексеенко А. А., Иванова М. М. Обеспечение информационной безопасности детей дошкольного возраста // Цифровая экономика: проблемы и перспективы развития: Сб. научных статей 4-й Всероссийской научно-практической конференции. – Курск, 2022. – С. 38–40.

2. Анненкова И. В., Залоило М. В. Новая культура коммуникаций в условиях цифровой и социокультурной глобализации: право, медиа и национальная идентичность // Журнал зарубежного законодательства и сравнительного правоведения. – 2019. – № 3. – С. 140–155.

3. ВЦИОМ: результаты опроса о восприятии россиянами интернета и о возможности его ограничения [Электронный ресурс] // Сайт Всероссийского центра изучения общественного мнения. 22.03.2021 [Электронный ресурс]. – URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/internet-i-deti-vozmozhnosti-i-ugrozy#:~:text=%D0%94%D0%B5%D1%82%D0%B8%20%D0%B2%20%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B5,%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8%20%D0%B2%20%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B5%20(81%25)

4. Магдилова Л. В. Правовые основы обеспечения информационной безопасности несовершеннолетних // Сайт научной электронной библиотеки КиберЛенинка. 2017. 10.21779/2224-0241-2017-23-3-104-108

5. Сколько времени в день ребенку можно проводить в Интернете? // Сайт Лиги безопасного Интернета. 13.02.2023. [Электронный ресурс]. – URL: https://ligainternet.ru/skolko-vremeni-v-den-rebenku-mozhno-provodit-v-internete/

6. Сустина Т. К вопросу об интернет-безопасности детей // «Адвокатская газета». – 2022. – № 5.

7. Угрозы для детей в цифровой среде [Электронный ресурс] // Сайт Центра правовой помощи гражданам в цифровой среде ФГУП «ГРЧЦ». 2023. – URL: https://4people.grfc.ru/faq/detskaya-bezopasnost-v-internete-na-chto-sleduet-obraschat-vnimanie/

8. 56 % детей постоянно находятся в Сети [Электронный ресурс] // По материалам сайта kaspersky.ru. [Электронный ресурс] – URL: http://security.mosmetod.ru/internet-zavisimosti/99-56-detej-postoyanno-nakhodyatsya-v-seti

Г. Г. Егоров,
кандидат юридических наук, доцент,
Волгоградский государственный университет
(Волжский филиал)

ИСПОЛЬЗОВАНИЕ НЕЙРОСЕТЕЙ ДЛЯ МОНИТОРИНГА ПРОТИВОПРАВНЫХ ОТНОШЕНИЙ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Аннотация. В статья рассматриваются перспективны использование современных машинных комплексов анализа правовых отношений на предмет соответствия современному действующему законодательству. Выделяются основные направление противоправных действий, выявление которых становится возможным при использовании графологических нейронных сетей (GNN) основанных на логике асинхронного анализа правонарушений основанных на нарушения финансового оборота. В качестве практической составляющей использовался опыт апробации данных комплексов в Китайской народной республики, при этом проводится анализ как технических так и правовых особенностей внедрения тождественных систем в контрольную сфере Российской Федерации. Определя-