УДК 342.7

ОТДЕЛЬНЫЕ ТЕОРЕТИКО-ПРАВОВЫЕ АСПЕКТЫ КИБЕРБЕЗОПАСНОСТИ ЛИЧНОСТИ

Т. Н. Кузьменкова
старший преподаватель
Могилевский государственный университет имени А. А. Кулешова
аспирант
Белорусский государственный университет

В статье обосновывается необходимость теоретической разработки категории «кибербезопасность личности» и развития нормативно-правового регулирования в соответствующем контексте. Исследуется место кибербезопасности личности в общей системе обеспечения информационной безопасности, а также выделяются основные элементы данного понятия. Отдельное внимание уделено теме правового сопровождения кибербезопасности личности, изложены предложения по совершенствованию национального законодательства.

Ключевые слова: информационная безопасность, кибербезопасность, киберпространство, кибератака, онлайн-груминг, Интернет, искусственный интеллект.

Введение

Повышение роли средств массовой информации и массовых коммуникаций, особенно информационно-телекоммуникационной сети «Интернет», в жизни современного социума привело к усилению значимости сферы информационной безопасности и принятию соответствующих нормативных правовых актов. В качестве одной из составляющих информационной безопасности выделяют кибербезопасность – «состояние защищенности информационной инфраструктуры и содержащейся в ней информации от внешних и внутренних угроз» (п. 3 Приложения 2 Указа Президента Республики Беларусь 14.02.2023 г. № 40) [1].

Следует сказать, что законодатель делает акцент на информационной безопасности, кибербезопасности именно государства и общества. В юридической науке поднимается вопрос о необходимости обособления и более тщательной теоретико-правовой проработке информационной безопасности личности, в качестве элемента которой, по мнению автора, стоит выделить и кибербезопасность. Анализ законодательства позволяет сделать вывод о значимости кибербезопасности в структуре правового статуса личности и нормативно-правовом регулировании отдельных аспектов. Тем не менее, отсутствие теоретической разработки и специального правового сопровождения ряда вопросов, приводит к пробелам в праве и потенциальной допустимости противоправных деяний, а также негативного информационного воздействия в обход существующего законодательства.

Таким образом, актуальность настоящего исследования обусловлена значимостью сферы информационной безопасности в целом и кибербезопасности, в частности, как в системе обеспечения национальной безопасности, так и для отдельной личности. Цель исследования: раскрыть отдельные теоретико-правовые аспекты кибербезопасности личности, наметить вектор совершенствования законодательства в соответствующей сфере.

Основная часть

Сложно не согласиться с мнением, что последние десятилетия стали революционными в развитии информационного пространства. Информация, являясь основным ресурсом и опорой общественного прогресса, выступила еще и «…эффективным инструментом для преобразования окружающей социальной действительности» [2, с. 5]. «Производитель не просто делает информацию доступной для каждого члена информационного общества, но активно использует все возможные каналы информационной коммуникации, воздействуя на личность. Каналы информационной коммуникации совершенствуются, расширяя выбор средств и технологий воздействия» [3, с. 54]. При этом механизмы деструктивного информационного воздействия на личность, общество и государство также постоянно совершенствуются. Например, «новая реальность породила феномены фейкинга и фейковизации информационного пространства как элемента новой гибридной войны со всеми ее отличительными особенностями… К таковым можно отнести новые виды информационных продуктов, которые создаются с активным использованием компьютерных технологий, в том числе искусственного интеллекта (нейросетей)» [2, с. 13–14].

Именно поэтому особое внимание на сегодняшний день уделяется сфере информационной безопасности. В качестве одной из составляющих информационной безопасности выделяют кибербезопасность, которая в соответствии с Указом Президента Республики Беларусь 14 февраля 2023 г. № 40 «О кибербезопасности» определяется как состояние защищенности информационной инфраструктуры и содержащейся в ней информации от внешних и внутренних угроз [1]. Отражение отдельных вопросов по защите технических средств, систем и технологий создания, преобразования, передачи, использования и хранения информации от кибератак в законодательстве предопределяет вектор дальнейшего нормативно-правового регулирования исследуемой области. Вместе с тем имеется ряд проблемных или неразрешенных моментов, которые требуют теоретической разработки и последующего правового сопровождения в рамках заданного вектора. Одним из таких моментов является сфера кибербезопасности личности.

По мнению автора, теоретико-правовая разработка кибербезопасности личности в первую очередь должна быть связана с определением ее места в системе информационной безопасности в общем. Здесь следует учитывать, что категория информационная безопасность является безусловным атрибутом интересов государства, однако данный феномен можно рассматривать и с позиции интересов отдельной личности. Вопрос о необходимости обособления и более тщательной правовой проработке информационной безопасности личности поднимался в трудах А. С. Жарова, Н. А. Збруевой, Т. Д. Логиновой, Е. Ю. Митрохиной, А. А. Тамодлиной, А. В. Туликова. Например, Т. Д. Логинова предлагает выделить право личности на информационную безопасность, которое «представляет собой законодательно закрепленную возможность каждому свободно пользоваться доступной информацией с использованием информационно-коммуникационных технологий, а также комплекс мер государственно-правового характера, направленный на обеспечение защиты личности от негативной информации, способной причинить ей вред» [4].

На наш взгляд, информационная безопасность личности выступает одним из компонентов информационной безопасности государства. В структуре конституционно-правового статуса личности она может быть выражена посредством права личности на безопасность в информационной сфере, которое является «комплексным понятием, включающим: право на защиту персональных данных и иной личной информации, право на защиту от деструктивного информационного воздействия, право на кибербезопасность» [5, с. 100]. Тем самым кибербезопасность личности является более узким по смыслу понятием и охватывается понятием информационная безопасность личности.

Следующим этапом теоретико-правового развития категории «кибербезопасность личности» должно стать ее содержательное наполнение, выделение составных элементов.

Когда речь идет о кибербезопасности (в науке вместо термина кибербезопасность можно встретить понятия безопасность в киберпространстве, цифровая безопасность), как правило, ее связывают с защитой информационной инфраструктуры, то есть «совокупности технических средств, систем и технологий создания, преобразования, передачи, использования и хранения информации от кибератак» (п. 5 Приложения 2 Указа Президента Республики Беларусь 14.02.2023 г. № 40) [1]. Под кибератакой, в свою очередь понимается «целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации» (п. 2 Приложения 2 Указа Президента Республики Беларусь 14.02.2023 г. № 40) [1].

Безусловно, заметен акцент на технической стороне рассматриваемого вопроса. Большая часть положений зарубежного законодательства также обращена к технической составляющей при определении понятий «информационная безопасность», «кибербезопасность», «киберпространство». Вместе с тем, как справедливо отмечает Т. А. Бражник, «интересы личности, связанные с обеспечением безопасности в киберпространстве, значительно шире, чем технические принципы работы оборудования и обработки данных. Особенно это касается несовершеннолетних, их здоровья и морального развития» [6].

Содержательное наполнение кибербезопасности личности является сложным и многокомпонентным и связано с защитой личности от различных видов негативных проявлений в виртуальной сфере, например, манипулятивного и (или) деструктивного информационного воздействия, кибербуллинга, онлайн груминга, нежелательной рекламы, интернет-мошенничества, компьютерных вирусов, взлома аккаунта и иных кибератак.

С учетом выделения нами кибербезопасности личности в качестве одного из элементов информационной безопасности личности, наряду с защитой личности от деструктивного информационного воздействия, защитой персональных данных и иной личной информации, полагаем, что содержательное наполнение исследуемой категории прежде всего должно описывать техническую сторону безопасности в киберпространстве, а прочие угрозы в цифровой сфере могут охватываться иными элементами. Однако установить четкие границы в содержательном наполнении рассматриваемых категорий сложно. Например, использование манипулятивных технологий в Интернете, сочетает в себе как технические, так и смысловые аспекты информационного воздействия на личность. Поэтому в настоящем исследовании будем рассматривать как элементы кибербезопасности черты, присущие только для данного понятия, так и комплексные, сочетающие вопросы нескольких аспектов информационной безопасности личности.

Предлагаем выделить следующие составляющие кибербезопасности личности:

- состояние защищенности от кибератак, непосредственно воздействующих на технические средства, системы и технологии создания, преобразования, передачи, использования и хранения информации (например, использование вредоносных программ, организация ботнетов, несанкционированный доступ к компьютерной информации);

- состояние защищенности личности от иных негативных деяний, при которых Интернет выступает в качестве способа или средства их совершения (например, интернет-мошенничество, кибербуллинг, онлайн груминг);

- состояние защищенности личности от манипулятивного, деструктивного информационного воздействия в киберпространстве, которое, прежде всего, связано с предупреждением негативного мировоззренческого и информационно-психологического влияния.

Ключевым этапом разработки кибербезопасности личности с учетом указанных выше элементов должна стать работа по совершенствованию ее нормативного правового сопровождения. ***Во-первых***, по мнению автора, свое место в законодательстве должно найти право человека на кибербезопасность, в том числе допустимо рассмотреть возможность его закрепления в Законе Республики Беларусь «Об информации информатизации и защите информации» и в перспективе – Информационном кодексе. С учетом всей значимости рассматриваемого права для несовершеннолетних, целесообразно включение соответствующих формулировок в Закон Республики Беларусь «О правах ребенка», а также разработка самостоятельного документа: «Концепции кибербезопасности несовершеннолетних», содержащего базовые положения взаимодействия детей с киберпространством. Здесь можно ориентироваться на опыт Российской Федерации. Так, 28 апреля 2023 года Распоряжением Правительства Российской Федерации № 1105-р была принята обновленная Концепция информационной безопасности детей, главная цель которой – защита несовершеннолетних от угроз и рисков в цифровой среде [7].

Во-вторых, совершенствование законодательства в сфере обеспечения кибербезопасности личности целесообразно вести и в направлении закрепления составов преступлений, отражающих специфику совершения отдельных деяний с использованием киберпространства. Ряд противоправных деяний, связанных со сферой функционирования киберпространства, уже криминализирован в белорусском законодательстве: Статья 198[1]. «Нарушение законодательства о средствах массовой информации», ст. 212 «Хищение имущества путем модификации компьютерной информации» и в целом глава 31 «Преступления против компьютерной безопасности» Уголовного кодекса Республики Беларусь [8]. Вместе с тем развитие общественных отношений, цифровизация многих сфер, требует пристального внимания к анализу и последующему отражению в праве мер по защите от новых негативных явлений. Речь идет, например, о таких деяниях, как различные формы интернет-мошенничества, кибербуллинг, онлайн-грумминг.

Так, особого внимания заслуживает также тема сексуальной эксплуатации детей в форме онлайн-груминга (сексуальное домогательство в социальных сетях). «В иностранной научной литературе это явление изучается уже длительное время и получило относительно подробное описание. Домогательство в варианте онлайн груминга, включается в качестве частного случая в более широкую категорию «онлайн сексуальная эксплуатация ребенка», к которой также относятся «секстинг», или создание и распространение сексуальных обнаженных или полуобнаженных изображений посредством мобильных телефонов и/или Интернета, и сексуальное вымогательство (“sexual extortion”, или “sextortion”) у детей таких сексуальных изображений, в том числе с помощью угроз или шантажа» [9]. Согласно Уголовному кодексу Республики Беларусь подобные деяния могут подпадать под действия статей 169 «Развратные действия», 170 «Понуждение к действиям сексуального характера» [8], однако эти составы преступлений не охватывают всю специфику онлайн-груминга.

По мнению Е. Г. Дозорцевой, А. С. Медведевой, сексуальный онлайн груминг должен стать «объектом пристального внимания не только правоохранительных органов, но и исследователей – юристов, психологов, лингвистов. Необходим правовой анализ данного состава преступления и определение того, насколько полно он отражен в существующем законодательстве» [9]. В контексте сказанного заслуживает внимания

предложение, высказанное в российской юридической науке, о «включении в Уголовный кодекс Российской Федерации статьи 135.1, предусматривающей ответственность за любое умышленное предложение о встрече, с которым лицо, достигшее 18-летнего возраста, при помощи сети Интернет или иных информационно-коммуникационных технологий обращается к несовершеннолетнему с целью совершения против него полового преступления» [9].

В-третьих, свое дальнейшее развитие в законодательстве должны найти меры по защите личности в киберпространстве от манипулятивного, в том числе деструктивного, воздействия на мировозренческую, нравственно-ценностную и идеологическую сферу, а также правовое регулирование использования искусственного интеллекта (нейросетей) в соответствующем контексте. Данное направление совершенствования национального права напрямую вытекает из положений Основного Закона Республики Беларусь. Так, возможность ограничения конституционных прав и свобод, в том числе свободы слова и права на информацию, в интересах национальной безопасности (одним из компонентов которой выступает информационная безопасность), общественного порядка, защиты нравственности, здоровья населения, прав и свобод других лиц, предусмотрена статьей 23 Конституции [10].

При всех плюсах научно-технического прогресса, стоит учитывать, что «современный Интернет – это не только неограниченная база знаний, объединяющая и заключающая все человечество в единое информационное поле, но и мощнейшее орудие пропаганды, средство для транслирования и распространения любых идеологий, продвижения интересов любых групп (в том числе преступных)… Многогранные в своих проявлениях фейки (информационные манипуляции) – это глобальный и реальный вызов социуму, государству и международному сообществу… Посредством фейковизации медиапространства насаждаются необходимые манипулятору мировоззренческие установки, формируется гиперреальность (гиперреальное как «реальное» без истока и без реальности), представляющее собой «царство симулякров» – псевдообразов явлений действительности» [2, с. 90–91]. Необходимо также отметить, что «алгоритмы социальных сетей и новостных агрегаторов (рекомендательные системы) предлагают интернет-пользователю контент той тематики и направленности, к которым уже ранее проявлялся интерес. Таким образом, пользователь может не видеть альтернативных точек зрения…. Основным критерием истинности информации становится ее виральность (т. е. сам факт ее широкого распространения)» [2, с. 61].

По мнению автора, правовое сопровождение видов и способов распространяемой в киберпространстве информации во многом связано с технической стороной вопроса, а также необходимостью установления четких критериев по определению вредоносного характера информационного воздействия, что в условиях процесса глобализации является весьма проблематичным. Однако с учетом значимости сферы информационной безопасности как для государства и общества, так и для отдельной личности, совершенствование законодательства в направлении защиты от деструктивного и манипулятивного воздействия должно стать ключевым в современных реалиях.

Примечателен в рассматриваемом контексте опыт Ирана и Китая. В Китае киберпространство рассматривается как часть государственной территории, в связи с чем государство «настаивает на исключительном праве на регулирование Интернета на территории страны, активно использует цензуру для фильтрации контента, запрещенного законодательством…» [11]. Основным отличием Иранской модели кибербезопасности является «создание национальной информационной сети, которая па замыслу разработчиков должна заменить в киберпространстве государства всемирную информационную сеть, а также активное применение в этом контексте программ фильтрации и блокировки интернет-контентов» [12].

Совершенствование законодательства в Республике Беларусь, на наш взгляд, также должно идти по пути создания действенного организационно-правового механизма регулирования транслируемого контента в Интернете, равно как и предупреждения отрицательного влияния деструктивной информации на нравственное, психическое, физическое и социальное благополучие отдельного человека, социальных групп и населения в целом путем повышения цифровой грамотности граждан, дальнейшего развития культуры безопасного поведения в киберпространстве.

Выводы

Сферу информационной безопасности в целом и кибербезопасности в частности целесообразно развивать, преломляя сквозь призму интересов не только государства и общества, но и отдельной личности.

Кибербезопасность личности представляет собой актуальное направление совершенствования национального законодательства, в том числе в сфере прав и свобод человека, если вести речь о праве личности на кибербезопасность.

Понятие «кибербезопасность личности» является более узким по смыслу и охватывается понятием «информационная безопасность личности».

При развитии отраслевого законодательства, прежде всего уголовного, следует учитывать угрозы информационно-коммуникационного мира. Особенная часть Уголовного кодекса Республики Беларусь может быть дополнена составами преступлений, отражающими специфику совершения отдельных деяний с использованием киберпространства.

Ключевым направлением обеспечения информационной безопасности личности должно стать создание действенного организационно-правового механизма регулирования видов и способов распространяемой информации в Интернете, а также принятие мер по развитию культуры безопасного поведения в киберпространстве (в первую очередь в отношении несовершеннолетних) в связи с чем предлагается разработка базового документа в соответствующей сфере – «Концепции кибербезопасности несовершеннолетних».

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. О кибербезопасности [Электронный ресурс]: Указ Президента Республики Беларусь, 14 февраля 2023 г., № 40 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

2. Фейковизация как средство информационной войны в интернет-медиа : научно-практическое пособие. – Москва : Блок-Принт, 2023. – 144 с.

3. ***Чеботарева, А. А.*** Правовое обеспечение информационной безопасности личности в глобальном информационном обществе: дис. …докт. юрид. наук: 12.00.13 / А. А. Чеботарева. – М, 2018. – 473 с.

4. ***Логинова, Т. Д.*** Обеспечение права личности на информационную безопасность (теоретико-правовой аспект) [Электронный ресурс] : автореф. дис…. канд. юрид. наук: 12.00.01 / Т. Д. Логинова. – Омск, 2019. – Режим доступа: https://files.omsu.ru/about/structure/science/ont/dissovet/dm-212-179.pdf. – Дата доступа: 03.08.2023.

5. ***Кузьменкова, Т. Н.*** Право на безопасность в информационной сфере в системе прав и свобод человека / Т. Н. Кузьменкова // Веснік Магілёўскага дзяржаўнага ўніверсітэта імя А. А. Куляшова. Сер. D. Эканоміка, сацыялогія, права. – 2022. – № 2 (60). – С. 97–103.

6. ***Бражник, Т. А.*** Отдельные аспекты правового регулирования информационной безопасности личности [Электронный ресурс] / Т. А. Бражник // Вестник ВГУ. Сер. Право. – 2019. – № 3. – Режим доступа: https://cyberleninka.ru/article/n/otdelnye-aspekty-pravovogo-regulirovaniya-informatsionnoy-bezopasnosti-lichnosti/viewer. – Дата доступа: 01.08.2023.

7. Концепция информационной безопасности детей в Российской Федерации [Электронный ресурс]. – Режим доступа: https://www.vedomosti.ru/society/articles/2023/05/10/974297-pravitelstvo-utverdilo-kontseptsiyu-informatsionnoi-bezopasnosti-detei – Дата доступа: 09.08.2023.

8. Уголовный Кодекс Республики Беларусь [Электронный ресурс] : 9 июля 1999 г., № 275-З : принят Палатой представителей 2 июня 1999 г. : одобр. Советом Респ. 24 июня 1999 г. : в ред. Закона Респ.

Беларусь от 09.03.2023 г. № 256-З // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

9. ***Дозорцева, Е. Г.*** Сексуальный онлайн груминг как объект психологического исследования [Электронный ресурс] / Е. Г. Дозорцева, А. С. Медведева // Психология и право. – 2019. – Т. 9, № 2. – Режим доступа: https://psyjournals.ru/journals/psylaw/archive/2019_n2/107176. – Дата доступа: 01.08.2023.

10. Конституция Республики Беларусь [Электронный ресурс] : с изм. и доп., принятыми на респ. референдумах 24 нояб. 1996 г., 17 окт. 2004 г., 27 февр. 2022 г. // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

11. ***Горян, Э. В.*** Нормативно-правовая основа обеспечения национальной безопасности в киберпространстве: опыт Китайской Народной Республики [Электронный ресурс] / Э. В. Горян // Территория новых возможностей. Вестник Владивостокского государственного университета экономики и сервиса. – 2021. – № 1. – Режим доступа: https://cyberleninka.ru/article/n/normativno-pravovaya-osnova-obespecheniya-natsionalnoy-bezopasnosti-v-kiberprostranstve-opyt-kitayskoy-narodnoy-respubliki/viewer. – Дата доступа: 01.08.2023.

12. ***Ковалев, О. Г.*** Кибербезопасность в условиях национального Интернета (Иранский опыт противодействия киберугрозам) [Электронный ресурс] / О. Г. Ковалев, А. А. Скипидаров // Столыпинский вестник. – 2021. – Режим доступа: https://cyberleninka.ru/article/n/kiberbezopasnost-v-usloviyah-natsionalnogo-interneta-iranskiy-opyt-protivodeystviya-kiberugrozam/viewer. – Дата доступа: 01.08.2023.

Поступила в редакцию 8.11.2023 г.

Контакты: kuzmenkova@msu.by (Кузьменкова Татьяна Николаевна)

Kuzmenkova T. N. **SOME THEORETICAL AND JURIDICAL ASPECTS OF PERSONAL CYBERSECURITY**

The article proves the necessity of theoretical development of the category "personal cybersecurity" and the development of legal regulation in the relevant context. The place of personal cybersecurity in the general information security system is investigated, and the main elements of this concept are highlighted. Special attention is paid to the topic of legal support of personal cybersecurity, and suggestions for the national legislation improvement are outlined.

Keywords: information security, cybersecurity, cyberspace, cyberattack, online grooming, Internet, artificial intelligence.