

Оригинальная статья / Original article

<https://doi.org/10.21869/2223-1501-2023-13-3-156-168>

Правовое обеспечение предупреждения киберпреступности в Российской Федерации и Республике Казахстан

К. О. Карабеков¹ ✉

¹Омская академия Министерства внутренних дел России
пр. Комарова, д. 7, г. Омск 644092, Российская Федерация

✉ e-mail: KarabekovK@mail.ru

Резюме

Актуальность. Большое значение в предупреждении преступности, в том числе киберпреступности в России и Казахстане, имеет содержание их правового обеспечения. Законодательство о киберпреступности в России и Казахстане разнообразно и имеет свои особенности. Актуальным является изучение содержания и системы правовых мер по предупреждению киберпреступности в России и Казахстане и выработка единого подхода к систематизации нормативных правовых актов, направленные на обеспечение кибербезопасности и предупреждение киберпреступности.

Целью является выявление недостатков и разработка предложений по повышению эффективности правового обеспечения предупреждения киберпреступности в Российской Федерации и Республике Казахстан.

Задачи: изучить и провести сравнение содержания международно-правовых актов, нормативных правовых актов Российской Федерации и Республики Казахстан по предупреждению киберпреступности и обеспечению кибербезопасности.

Методология. Основу научного исследования составил всеобщий диалектический метод. Также использован общенаучный метод анализа, который позволил провести систематизацию нормативных правовых актов по предупреждению киберпреступности. Метод научного синтеза использовался для авторского представления правового обеспечения предупреждения киберпреступности. Метод сравнительного правоведения стал основой для характеристики правового обеспечения предупреждения киберпреступности в юридической науке и в законодательстве Российской Федерации и Республики Казахстан.

Результаты. В ходе исследования выявлены недостатки систематизации законодательства по предупреждению киберпреступности в Российской Федерации и Республике Казахстан, предложена классификация соответствующих нормативных правовых актов по признаку субъектов, которые их принимают.

Выводы. Для более глубокого раскрытия системы нормативных правовых актов, касающихся кибербезопасности и предупреждения киберпреступности в России и Казахстане, исключения пробелов правового регулирования, а также их дублирования необходима их полная классификация по признаку субъектов, которые их принимают.

Ключевые слова: киберпреступность; правовое обеспечение; информационная безопасность; международные договоры.

Конфликт интересов: Автор декларирует отсутствие явных и потенциальных конфликтов интересов, связанных с публикацией настоящей статьи.

Для цитирования: Карабеков К. О. Правовое обеспечение предупреждения киберпреступности в Российской Федерации и Республике Казахстан // Известия Юго-Западного государственного университета. Серия: История и право. 2023. Т. 13, № 3. С.156–168. <https://doi.org/10.21869/2223-1501-2023-13-3-156-168>.

Поступила в редакцию 21.04.2023

Принята к публикации 26.05.2023

Опубликована 30.06.2023

Legal Support for the Prevention of Cybercrime in the Russian Federation and the Republic of Kazakhstan

Kanatbek O. Karabekov¹ ✉

¹Omsk Academy of the Ministry of Internal Affairs of Russia
7 Komarova Str., Omsk 644092, Russian Federation

✉ e-mail: KarabekovK@mail.ru

Abstract

Relevance. The content of their legal support is of great importance in the prevention of crime, including cybercrime in Russia and Kazakhstan. Cybercrime legislation in Russia and Kazakhstan is diverse and has its own peculiarities. It is relevant to study the content and system of legal measures to prevent cybercrime in Russia and Kazakhstan and to develop a unified approach to the systematization of regulatory legal acts aimed at ensuring cybersecurity and preventing cybercrime.

Purpose. The aim is to identify shortcomings and develop proposals to improve the effectiveness of legal support for the prevention of cybercrime in the Russian Federation and the Republic of Kazakhstan.

Objectives. to study and compare the content of international legal acts, regulatory legal acts of the Russian Federation and the Republic of Kazakhstan on the prevention of cybercrime and cybersecurity.

Methodology. The basis of scientific research was the universal dialectical method. A general scientific method of analysis was also used, which made it possible to systematize regulatory legal acts on the prevention of cybercrime. The method of scientific synthesis was used for the author's presentation of legal support for the prevention of cybercrime. The method of comparative jurisprudence has become the basis for the characterization of legal support for the prevention of cybercrime in legal science and in the legislation of the Russian Federation and the Republic of Kazakhstan.

Results. In the course of the study, the shortcomings of the systematization of legislation on the prevention of cybercrime in the Russian Federation and the Republic of Kazakhstan were identified, the classification of relevant regulatory legal acts on the basis of the subjects that adopt them was proposed.

Conclusion. For a deeper disclosure of the system of regulatory legal acts related to cybersecurity and the prevention of cybercrime in Russia and Kazakhstan, the exclusion of gaps in legal regulation, as well as their duplication, their complete classification is necessary on the basis of the entities that accept them.

Keywords: cybercrime; legal support; cybersecurity; information security; international treaties.

Conflict of interest: The Author declare the absence of obvious and potential conflicts of interest related to the publication of this article.

For citation: Karabekov K. O. Legal Support for the Prevention of Cybercrime in the Russian Federation and the Republic of Kazakhstan. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta. Seriya: Istoriya i pravo = Proceedings of the Southwest State University. Series: History and Law.* 2023; 13(3): 156–168. (In Russ.) <https://doi.org/10.21869/2223-1501-2023-13-3-156-168>.

Received 21.04.2023

Accepted 26.05.2023

Published 30.06.2023

Введение

Вопросами предупреждения киберпреступности, обеспечения кибербезопасности или информационной безопасности в Российской Федерации занимались такие ученые, как Д. М. Апкаев, А. С. Логозинский [1], В. Р. Атнашев, С. Н. Яхъеева [2], Т. А. Гончарова, Л. В. Набоков [3],

В. Ф. Джафарли [4], К. Н. Евдокимов [5], П. Н. Кобец [6], А. Л. Осипенко [7], С. С. Симонова [8]. В Республике Казахстан вышеуказанные проблемы стали предметами обсуждения и анализа таких ученых, как Н. А. Биекенов [9], Р. Е. Джансареева, К. Аратулы [10], Р. Т. Дыбыс [11], А. Н. Камбаров, Н. А. Тулаганов [12],

А. Махмутов [13], А. Д. Мухамеджанова [14], А. А. Мырзахмет [15], К. К. Саби-ров, Ф. Р. Ахмеджанов [16]. Ученые России и Казахстана проявляют активный научный интерес к проблемам киберпреступности. По нашему мнению, это связано не только с ростом киберпреступлений и огромным материальным вредом, причиняемым киберпреступлениями, но и в целом с беспрецедентным масштабом киберугроз, возникающих для наших государств.

Киберпреступность стала новым глобальным вызовом для всего современного мира, но особенно для прогрессивно развивающихся государств, повсеместно внедряющих современные информационно-телекоммуникационные технологии. Параллельно с ростом внедрения этих технологий, и даже опережающими темпами, растет основанная на этих технологиях преступность. И чем активнее государства внедряют современные ИТ-технологии, тем больше они сталкиваются с проблемами киберпреступности.

В России и Казахстане Интернетом пользуются более 90% от общей численности населения, и статистика показывает, что с ростом количества интернет-пользователей параллельно регистрируется рост киберпреступлений и объем причиняемого ими ущерба. Так, в России размер ущерба, причиненного киберпреступлениями, в 2021 г. оценивается в 90 млрд рублей против порядка 70 млрд рублей годом ранее¹, а в Казахстане в 2022 г. ущерб составил 7 млрд тенге (это примерно 1 млрд 57 млн 700 тыс. рублей)².

¹ Эксперт оценил ущерб от киберпреступлений в России в 2021 году // РИА Новости. URL: https://ria.ru/20211222/kiberprestupleniya-1764_832102.html/ (дата обращения: 13.04.2023).

² Машаев А. Что стало причиной роста киберкриминала в Казахстане // Курсив. URL: [https://kz.kursiv.media/2022-12-15/chto-](https://kz.kursiv.media/2022-12-15/chto-stalo-prichinoj-rosta-kiberkriminala-v-kazahstane/)

Проблему борьбы с данным видом преступности осложняет, прежде всего, новизна и динамичность способов совершения этих преступлений. Конечно, в каждом государстве существуют свои давно разработанные системы мер профилактики и предупреждения преступности, однако способы совершения киберпреступлений так быстро обновляются, что предупредить их традиционными мерами не всегда удастся. Особенно отставание сказывается на правовом регулировании и закреплении содержания и порядка применения предупредительных мер борьбы с киберпреступностью. Все это требует повышенного внимания наших государств к разработке системы и содержанию нормативных правовых актов, касающихся как обеспечения кибербезопасности (информационной безопасности), так и борьбы с конкретными видами киберпреступлений.

Методология

Основу научного исследования составил всеобщий диалектический метод. Также использован общенаучный метод анализа, который позволил провести систематизацию нормативных правовых актов по предупреждению киберпреступности. Метод научного синтеза использовался для авторского представления правового обеспечения предупреждения киберпреступности. Метод сравнительного правоведения стал основой для характеристики правового обеспечения предупреждения киберпреступности в юридической науке и в законодательстве Российской Федерации и Республики Казахстан.

Результаты и их обсуждение

Киберпреступность, имея трансграничную сущность, представляет собой большую опасность для всех стран, для

stalo-prichinoj-rosta-kiberkriminala-v-kazahstane/ (дата обращения: 13.04.2023).

всех граждан, независимо от их местонахождения и гражданства. Такая глобальная угроза для всех людей в мире требует не только усилий отдельных государств по борьбе с киберпреступностью на своей территории, но и адекватного государственного реагирования на мировом уровне, объединения усилий всех государств мира в организации борьбы с киберпреступностью. Решением этих вопросов, предполагается, должны заниматься международные организации, объединяющие несколько стран мира, такие как Организация Объединенных Наций (далее – ООН), Совет Европы (далее – СЕ), Организация по безопасности и сотрудничеству в Европе (далее – ОБСЕ), Шанхайская организация сотрудничества (далее – ШОС), Содружество Независимых Государств (далее – СНГ). При этом большое значение должны иметь нормативные правовые акты таких международных организаций, позволяющие скоординировать и объединить усилия всех государств в борьбе с киберпреступностью.

Изучение действующего международного законодательства в этом направлении свидетельствует о наличии определенных достижений. Например, ООН принял несколько нормативных актов, в которых определены задачи законодательства в области кибербезопасности, включая:

- защиту прав человека;
- установление стандартов допустимого поведения для пользователей информационно-коммуникационных технологий (далее – ИКТ);
- установление социально-правовых санкций за совершение киберпреступлений;
- обеспечение защиты пользователей ИКТ и предотвращение вреда, наносимого людям, данным, системам, сервисам и инфраструктуре;
- обеспечение возможностей для расследования и уголовного преследова-

ния в отношении преступлений, совершаемых в сети Интернет;

– содействие международному сотрудничеству по вопросам, связанным с киберпреступностью¹.

Реализация этих задач должна находить отражение в содержании нормативных правовых актов по предупреждению и противодействию киберпреступности всех государств, в том числе России и Казахстана. Учитывая территориальную близость, исторически длительный характер общения между нашими народами, а также дружественный характер взаимоотношений между нашими государствами, большой интерес представляет изучение реального состояния правового регулирования и обеспечения вопросов кибербезопасности и опыта борьбы с киберпреступностью.

Приступая к изучению такого опыта, следует учесть особенности и достижения научных школ и направлений, разные подходы ученых наших стран к характеристике понятия и содержания правового обеспечения предупреждения преступности.

Чтобы предупредить преступления, необходимо развивать экономику, политику, идеологию, культуру и быт таким образом, чтобы исключить или уменьшить негативные аспекты общественной жизни, которые могут стать причиной или условием для преступности. Для этого необходимо создать правовую базу, которая обеспечит такую организацию общественной жизни [17, с. 140]. Поэтому правовое регулирование является определяющим фактором в борьбе с киберпреступностью, и комплексные нормативные правовые акты, учитывающие реалии криминогенной ситуации в сете-

¹ Киберпреступность. Модуль 3. Правовая база и права человека // ООН. Вена, 2019. С. 4. URL: [Cybercrime_Module_3_Legal_Frameworks_and_Human_Rights_RU.pdf](#) / (дата обращения: 13.04.2023).

вом информационном пространстве, являются необходимыми для эффективной борьбы [18, с. 132–133].

Согласно мнению А. Л. Осипенко, «в правовом регулировании сетевых процессов можно выделить как минимум два направления: во-первых, развитие общих правовых механизмов, обеспечивающих безопасность информационного пространства глобальных компьютерных сетей, и, во-вторых, создание системы правовых норм, непосредственно регламентирующих борьбу с преступностью в глобальных сетях» [17, с. 314].

В. Ф. Джафарли в своих исследованиях на тему «Криминология кибербезопасности» выстраивает, по нашему мнению, правильное представление о том, что комплексное обеспечение кибербезопасности предполагает систему нормативных правовых актов, в том числе и в некриминальной сфере [4, с. 13].

Д. А. Шестаков отмечает, что «контроль общества за преступностью без надлежащей нормативной базы (основополагающего закона и систематизации прочих законов и подзаконных актов в данной области) в силу хаотичности, необеспеченности государственной поддержкой оказывается предельно неэффективным, что имеет место в современной России» [19, с. 147–148].

Также, по мнению И. М. Мацкевича, «криминологическое законодательство – это система нормативных правовых актов, которые регулируют общественные отношения, касающиеся причин, условий преступлений и преступности, предупреждения преступлений и преступности, лиц, совершивших преступления, и их жертв, а также применения иных мер по борьбе с преступлениями и преступностью» [20, с. 13–14].

Таким образом, каждое государство должно быть обеспечено системой мер по профилактике и предупреждению преступности, которые регламентированы законодательством. Под правовым обеспечением предупреждения преступности

понимается комплекс нормативных правовых актов, принимаемых государством, в которых определяются общие политические, социальные, экономические задачи государства и правоохранительных органов по предупреждению преступности.

Наличие большого числа нормативных правовых актов объективно создает трудности не только в их применении, но даже в ориентации в них. Конечно, это требует их упорядоченности, систематизации, классификации, которую необходимо проводить на определенной основе. Так, В. Ф. Джафарли предлагает вариант систематизации нормативных правовых актов по обеспечению кибербезопасности в Российской Федерации на три уровня: «первый уровень – правовые основы обеспечения национальной безопасности; второй уровень – правовые основы обеспечения национальной и международной кибербезопасности; третий уровень – правовые основы обеспечения криминологической безопасности, в том числе и в сфере информационно-коммуникационных технологий» [4, с. 20].

По нашему мнению, основные средства борьбы с киберпреступностью определяются национальным законодательством конкретной страны, которое дополняется международно-правовыми предписаниями, содержащимися в международных документах, учитывая также специфику киберпреступности (повышенная скрытность, международный, трансграничный, дистанционный характер и т. д.), поэтому нельзя недооценивать важную роль международных правовых актов.

В целом для лучшего раскрытия содержания и системы, поиска пробелов правового регулирования, исключения дублирования нормативных правовых актов, касающихся кибербезопасности (информационной безопасности) и киберпреступности в России и Казахстане, можно предложить следующую классификацию по уровню статуса субъектов,

которые принимают эти нормативные правовые акты:

1. Международно-правовые акты *глобальных субъектов* мирового уровня.

2. Международно-правовые акты *межрегиональных субъектов* межгосударственного (*межнационального*) уровня.

3. Национальные нормативные правовые акты *национальных субъектов* уровня отдельных государств (*государственного*) уровня.

В соответствии с этой классификацией нормативные правовые акты делятся на три уровня.

Учитывая трансграничный (транснациональный) характер киберпреступлений, при котором преступник, объект преступного посягательства, жертва могут находиться под юрисдикцией разных государств, к *первой группе* необходимо относить международно-правовые акты ООН по обеспечению кибербезопасности (информационной безопасности) и сотрудничеству по борьбе с киберпреступностью, т. к. в ООН входят 193 государства.

К таким источникам среди документов ООН, посвященных вопросам международной информационной безопасности (кибербезопасности) и борьбы с киберпреступностью, относятся:

– Резолюция Генеральной Ассамблеи ООН 53/70 от 4 января 1999 г. «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности»;

– Резолюция Генеральной Ассамблеи ООН 73/27 от 5 декабря 2018 г. «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности»;

– Резолюция Генеральной Ассамблеи ООН 73/264 от 22 декабря 2018 г. «Поощрение ответственного поведения государств в киберпространстве в контексте международной безопасности»;

– Конвенция ООН против транснациональной организованной преступности, 2000 г.;

– Факультативный протокол к Конвенции ООН о правах ребенка, касающийся торговли детьми, детской проституции и детской порнографии, 2000 г.;

– Элементы для создания глобальной культуры кибербезопасности (приняты резолюцией 57/239 Генеральной Ассамблеи ООН от 20 декабря 2002 г.).

В таких документах, как Глобальная программа кибербезопасности Международного союза электросвязи или Резолюция Генеральной Ассамблеи ООН «Создание глобальной культуры кибербезопасности и оценка национальных усилий по защите важнейших информационных инфраструктур», содержатся подходы к пониманию кибербезопасности, охватывающие сферу безопасного использования ИКТ и защиты критической информационно-коммуникационной инфраструктуры. Это включает в себя защиту информационных систем, аппаратно-программных комплексов, телекоммуникационных систем, сетей телекоммуникаций, систем защиты информации и программного обеспечения от вредоносного воздействия программно-техническими методами.

Вместе с тем следует отметить, что в содержании международно-правовых актов не раскрыты производные термина кибербезопасности, такие понятия, как киберпреступность, киберпространство, киберзащита, кибератаки, кибернападение. В целом это затрудняет общее восприятие этих терминов на глобальном международном уровне и создает определенные проблемы в международном сотрудничестве по обеспечению кибербезопасности и противодействию киберпреступности.

К международно-правовым актам *регионального* (межнационального, межгосударственного) уровня следует отнести акты таких организаций, как СЕ (47 государств), ОБСЕ (57 государств), ШОС

(9 государств), СНГ (10 государств). В частности, к международно-правовым актам *регионального* уровня, посвященным вопросам международной информационной безопасности (кибербезопасности) и борьбе с киберпреступностью, относятся:

- на уровне *СЕ*: Конвенция СЕ о компьютерных преступлениях и Дополнительный протокол к Конвенции о компьютерных преступлениях, касающийся уголовной ответственности за акты расистского и ксенофобского характера, совершаемые через компьютерные системы, 2001 г.; Конвенция СЕ о защите детей от эксплуатации и надругательств сексуального характера, 2007 г.;

- на уровне *ОБСЕ*: Меры укрепления доверия в рамках ОБСЕ с целью сокращения рисков возникновения конфликтов в результате использования информационных и коммуникационных технологий (Решение РС.DEC/1202 от 10 марта 2016 г.);

- на уровне *ШОС*: Соглашение ШОС о сотрудничестве в области обеспечения международной информационной безопасности, 2010 г.

Соглашения в рамках СНГ по борьбе с киберпреступлениями:

- Соглашение о сотрудничестве в борьбе с преступлениями в сфере компьютерной информации от 1 июня 2001 г.;

- модельный Информационный кодекс для государств – участников СНГ от 23 ноября 2012 г.;

- Рекомендации Межпарламентской ассамблеи государств СНГ по совершенствованию и гармонизации национального законодательства государств – участников СНГ в сфере обеспечения информационной безопасности от 23 ноября 2012 г.;

- Рекомендации Межпарламентской ассамблеи государств СНГ по правовому регулированию эксплуатации открытых телекоммуникационных сетей для предупреждения их использования в террористических и иных противоправных целях от 29 ноября 2013 г.;

- модельный закон СНГ о критически важных объектах информационно-коммуникационной инфраструктуры от 28 ноября 2014 г.;

- модельный Регламент административных процедур, осуществляемых уполномоченными органами в сфере обеспечения информационной безопасности государств – участников СНГ от 28 ноября 2014 г.;

- Рекомендации Межпарламентской ассамблеи государств СНГ по совершенствованию законодательства государств – участников СНГ в сфере противодействия технологическому терроризму от 16 апреля 2015 г.

Безусловно, все перечисленные международно-правовые акты регионального уровня при необходимости решения вопросов по борьбе с киберпреступностью признаются основополагающими актами, но не всегда в таких документах учитывается суверенитет и независимость стран-участников. Например, к Конвенции СЕ о компьютерных преступлениях и к Дополнительному протоколу к Конвенции о компьютерных преступлениях, касающихся уголовной ответственности за акты расистского и ксенофобского характера, совершаемые через компьютерные системы (2001 г.), Россия не присоединилась, поскольку положения ст. 32b противоречат российскому законодательству и нарушают суверенитет государства, т. к. предусмотренные в ней действия могут совершаться без предварительного уведомления и согласия стороны, на территории которой эти действия совершаются. Кроме того, «в УК РФ отсутствуют нормы, устанавливающие уголовную ответственность юридических лиц за преступления в сфере компьютерной информации» [5, с. 27]. По нашему мнению, в международно-правовых актах должен быть закреплён комплекс правовых мер, учитывающих суверенитет и независимость отдельных государств.

К нормативным правовым актам (*национальное законодательство*), обес-

печивающим кибербезопасность (информационную безопасность) отдельных стран, по нашему мнению, следует отнести законы, подзаконные и локальные нормативные правовые акты, в том числе и Российской Федерации и Республики Казахстан.

Безусловно, главным источником государства для защиты прав граждан и обеспечения кибербезопасности является Конституция. Согласно ст. 23 Конституции РФ каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени (п. 1). Также каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений (п. 2). В ст. 24 сказано, что сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются (п. 1). Аналогичные статьи (17, 18) имеются и в Конституции Республики Казахстан. Это говорит о том, что государство гарантирует защиту личных неимущественных прав граждан от противоправных посягательств с использованием ИКТ.

К основным нормативным правовым актам, обеспечивающим кибербезопасность (информационную безопасность) наших стран, следует отнести: Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (Постановление Правительства Республики Казахстан от 8 сентября 2016 г. № 529 «Об утверждении Правил и критериев отнесения объектов информационно-коммуникационной инфраструктуры к критически важным объектам информационно-коммуникационной инфраструктуры»), Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации» (Закон Республики Казахстан от 16 ноября 2015 г. № 401-V ЗРК «О доступе к информации»), Доктрину информационной безопасности

Российской Федерации (Постановление Правительства Республики Казахстан от 30 июня 2017 г. № 407 «Об утверждении Концепции кибербезопасности»), Стратегию развития информационного общества в Российской Федерации на 2017–2030 гг., национальную программу «Цифровая экономика Российской Федерации» (Постановление Правительства Республики Казахстан от 30 декабря 2021 г. № 961 «Об утверждении Концепции развития отрасли информационно-коммуникационных технологий и цифровой сферы»), Национальную стратегию развития искусственного интеллекта на период до 2030 г., Концепцию развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 г., Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (Уголовный кодекс Республики Казахстан от 3 июля 2014 г. № 226-V ЗРК), Кодекс Российской Федерации об административных правонарушениях от 30 дек. 2001 г. № 195-ФЗ (Кодекс Республики Казахстан от 5 июля 2014 г. № 235-V ЗРК «Об административных правонарушениях»).

Характеризуя содержание указанных нормативных правовых актов, нельзя не отметить их значительную разноплановость. По нашему мнению, для качественного и системного правового регулирования вопросов кибербезопасности нужна определенная концепция. В качестве примера можно обратиться к содержанию Постановления Правительства Республики Казахстан от 30 июня 2017 г. № 407, которым была утверждена Концепция кибербезопасности¹. Данная Концепция определяет основные направления реализации государственной политики в сфере защиты электронных информационных ресурсов, информационных

¹ Об утверждении Концепции кибербезопасности ("Киберщит Казахстана"): Постановление Правительства Республики Казахстан от 30 июня 2017 г. № 407 // Эділет : сайт. URL: <https://adilet.zan.kz/rus/docs/P1700000407> (дата обращения: 24.03.2023).

систем и сетей телекоммуникаций, обеспечения безопасного использования ИКТ, также призвана обеспечить единство подходов к мониторингу обеспечения информационной безопасности государственных органов, физических и юридических лиц, а также выработку механизмов предупреждения и оперативного реагирования на инциденты информационной безопасности, в том числе в условиях чрезвычайных ситуаций социального, природного и техногенного характера, введения чрезвычайного или военного положения.

Формально подобная Концепция кибербезопасности в Российской Федерации отсутствует, хотя в 2010 г. был опубликован проект подобной концепции, но в итоге такой стратегический документ не был принят. В качестве аналогов стратегии кибербезопасности в Российской Федерации возможно привести следующие нормативные правовые акты: Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации¹ и Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26 июля 2017 г. № 187-ФЗ², а также Концепцию государ-

ственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, выписка из которой опубликована на сайте Совета безопасности³. Учитывая опыт Республики Казахстан по систематизации государственной политики в области кибербезопасности, необходимо все-таки принять Концепцию кибербезопасности Российской Федерации.

По нашему мнению, предлагаемая систематизация законодательства в сфере обеспечения интересов кибербезопасности поможет нашим государствам правильно выстроить систему мер предупреждения, найти пробелы правового регулирования, исключить дублирование нормативных правовых актов, касающихся кибербезопасности (информационной безопасности) и киберпреступности в России и Казахстане.

Выводы

Проанализировав международные акты, нормативные правовые акты Российской Федерации и Республики Казахстан и мнения ученых о системе, роли и значении законодательства по предупреждению и противодействию киберпреступности, можно делать следующие выводы:

– в законодательстве Российской Федерации и Республики Казахстан отсутствует единая система нормативных правовых актов по предупреждению киберпреступности;

¹ Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации: [утв. Президентом РФ 3 февр. 2012 г. № 803] // КонсультантПлюс. URL: https://www.consultant.ru/document/cons_doc_LAW_150730/ (дата обращения: 24.03.2023).

² О безопасности критической информационной инфраструктуры Российской Федерации»: Федер. закон от 26 июля 2017 г. № 187-ФЗ // КонсультантПлюс. URL: https://www.consultant.ru/document/cons_doc_LAW_18734/

www.consultant.ru/document/cons_doc_LAW_220885/ (дата обращения: 24.03.2023).

³ Выписка из Концепции государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации : [утв. Президентом РФ 12 дек. 2014 г. № К 1274] // Совет Безопасности Российской Федерации. URL: <http://www.scrf.gov.ru/security/information/document131/> (дата обращения: 24.03.2023).

– в содержании глобальных международных правовых актов нет правильного закрепления прав и обязанностей государств в отношении вопросов международной кибербезопасности;

– в содержании глобальных международных правовых актов не раскрыты основные термины, касающиеся понятий «кибербезопасность», «киберпреступность», «киберпространство»;

– в документах ООН не закреплён комплекс правовых мер, учитывающих суверенитет отдельных государств.

Для лучшего понимания системы и содержания, поиска пробелов правового регулирования, исключения дублирования нормативных правовых актов, касающихся кибербезопасности (информационной безопасности) и киберпреступности в России и Казахстане можно предложить следующую классификацию по признаку субъектов, которые принимают эти нормативные правовые акты: первое – международно-правовые акты *глобального* уровня; второе – международно-правовые акты *регионального (межнационального, межгосударственного)* уровня;

третье – нормативные правовые акты (*национальное законодательство*) отдельных государств.

Также на основе опыта Республики Казахстан для систематизации государственной политики в области кибербезопасности представляется возможным принятие Концепции кибербезопасности Российской Федерации.

Стратегии кибербезопасности России и Казахстана схожи по целям, поскольку обеспечение кибербезопасности (информационной безопасности) стало приоритетным направлением обеспечения национальной безопасности государств и их критически важных отраслей. Обе страны обеспокоены безопасностью киберпространства, включающего в себя критическую информационную инфраструктуру. В рамках СНГ поднимаются вопросы сотрудничества в борьбе с киберпреступностью, единодушно отмечается эволюция киберугроз, а также отмечается необходимость совместной работы и глобального международного регулирования действий в киберпространстве.

Список литературы

1. Апкаев Д. М., Логозинский А. С. Некоторые аспекты предупреждения киберпреступности // Пенитенциарное право: юридическая теория и правоприменительная практика. 2022. № 3 (33). С. 63–67.
2. Атнашев В. Р., Яхъеева С. Н. Международное сотрудничество в борьбе с киберпреступностью и кибертерроризмом // Евразийская интеграция: экономика, право, политика. 2019. № 3 (29). С. 37–42.
3. Гончарова Т. А., Набоков Л. В. Киберпреступность в России: проблемные аспекты и предупреждение преступности // Инновационная экономика и право. 2022. № 1 (20). С. 118–124.
4. Джафарли В. Ф. Криминология кибербезопасности: в 5 т. Т. 1: Криминологическая кибербезопасность: теоретические, правовые и технологические основы. М.: Проспект, 2021. 288 с.
5. Евдокимов К. Н. Актуальные вопросы предупреждения преступлений в сфере компьютерной информации в Российской Федерации // Академический юридический журнал. 2015. № 1 (59). С. 21–31.
6. Кобец П. Н. Киберпреступность: современные виды, причины, ее порождающие, и особенности предупреждения // Вестник Самарского юридического института. 2022. № 1 (47). С. 52–58.

7. Осипенко А. Л. Сетевая компьютерная преступность: теория и практика борьбы: монография. Омск: Омск. акад. МВД России, 2009. 480 с.
8. Симонова С. С. Противодействие киберпреступности в России и зарубежных странах: криминологический и виктимологический аспекты // Вестник Российского нового университета. Серия: Человек и общество. 2022. Вып. 3. С. 58–61.
9. Биекенов Н. А. Некоторые проблемы обеспечения кибербезопасности в Республике Казахстан // Вестник Института законодательства Республики Казахстан. 2014. № 1 (33). С. 16–20.
10. Джансараева Р. Е., Аратулы К. Борьба с киберпреступлениями: сравнительный анализ законодательства стран СНГ // Криминологический журнал Байкальского государственного университета экономики и права. 2012. № 3. С. 95–99.
11. Дыбыс Р. Т. Административно-правовые средства обеспечения информационной безопасности в Республике Казахстан // Казахская цивилизация. 2017. № 3. С. 47–54.
12. Камбаров А. Н., Тулаганов Н. А. Проблемы обеспечения информационной безопасности Республики Казахстан // Физика. Технологии. Инновации: сборник научных трудов / под ред. В. Н. Рычкова. Екатеринбург: Урал. федер. ун-т, 2015. Вып. 1. С. 257–262.
13. Махмутов А. Концепция национальной безопасности Казахстана в контексте современных внешнеполитических реалий // Внешнеполитические перспективы и новые концепты международной стратегии Казахстана: материалы круглого стола. Алматы: Жибек жолы, 2012. С. 14–15.
14. Мухамеджанова А. Д. Особенности динамики киберпреступности в Республике Казахстан и ее влияние на вопросы её предупреждения // Российско-азиатский правовой журнал. 2022. № 2. С. 49–55.
15. Мырзахмет А. А. Правовое обеспечение информационной безопасности Республики Казахстан // Молодой ученый. 2019. № 15 (253) С. 119–122.
16. Сабиров К. К., Ахмеджанов Ф. Р. Некоторые вопросы законодательного укрепления кибербезопасности в Республике Казахстан // Вопросы кибербезопасности. 2017. № 3 (21). С. 55–62.
17. Криминология / под ред. В. Д. Малкова. М.: Юстицинформ, 2004. 524 с.
18. Прокументов Л. М. Криминализация и декриминализация как средства выражения уголовно-правовой политики // Вопросы развития российского законодательства: сборник материалов региональной научно-практической конференции. Томск: Изд-во науч.-техн. лит., 2005. С. 132–133.
19. Шестаков Д. А. Криминология: Преступность как свойство общества. Краткий курс. СПб.: Лань, 2001. 259 с.
20. Мацкевич И. М. Криминология. М.: Норма, 2017. 368 с.

References

1. Apkaev D. M., Logozinskij A. S. Nekotorye aspekty preduprezhdeniya kiberprestupnosti [Some aspects of cybercrime prevention]. *Penitenciarnoe pravo: yuridicheskaya teoriya i pravoprimeritel'naya praktika* = *Penitentiary law: legal theory and law enforcement practice*, 2022, no. 3 (33), pp. 63–67.
2. Atnashev V. R., Yah"eeva S. N. Mezhdunarodnoe sotrudnichestvo v bor'be s kiberprestupnost'yu i kiberterrorizmom [International cooperation in the fight against cybercrime and cyberterrorism]. *Evrazijskaya integraciya: ekonomika, pravo, politika* = *Eurasian integration: Economics, law, Politics*, 2019, no. 3 (29), pp. 37–42.

3. Goncharova T. A., Nabokov L. V. Kiberprestupnost' v Rossii: problemnye aspekty i preduprezhdenie prestupnosti [Cybercrime in Russia: problematic aspects and crime prevention]. *Innovacionnaya ekonomika i pravo = Innovative Economics and Law*, 2022, no. 1 (20), pp. 118–124.

4. Dzhafarli V. F. Kriminologiya kiberbezopasnosti. T. 1: Kriminologicheskaya kiberbezopasnost': teoreticheskie, pravovye i tekhnologicheskie osnovy [Cybersecurity Criminology. Vol. 1. Criminological Cyberbullying: Theoretical, truthful and Technological foundations]. Moscow, Prospekt Publ., 2021. 288 p.

5. Evdokimov K. N. Aktual'nye voprosy preduprezhdeniya prestuplenij v sfere komp'yuternoj informacii v Rossijskoj Federacii [Topical issues of crime prevention in the field of computer information in the Russian Federation]. *Akademicheskij yuridicheskij zhurnal = Academic Law Journal*, 2015, no. 1 (59), pp. 21–31.

6. Kobec P. N. Kiberprestupnost': sovremennye vidy, prichiny, ee porozhdayushchie, i osobennosti preduprezhdeniya [Cybercrime: modern types, causes, its generating, and features of prevention]. *Vestnik Samarskogo yuridicheskogo instituta = Bulletin of the Samara Law Institute*, 2022, no. 1 (47), pp. 52–58.

7. Osipenko A. L. Setevaya komp'yuternaya prestupnost': teoriya i praktika bor'by [Network computer crime: theory and practice of struggle]. Omsk, Omsk. akad. MVD Rossii, 2009. 480 p.

8. Simonova S. S. Protivodejstvie kiberprestupnosti v Rossii i zarubezhnyh stranah: kriminologicheskij i viktimologicheskij aspekty [Countering cybercrime in Russia and abroad: criminological and victimological aspects]. *Vestnik Rossijskogo novogo universiteta. Seriya: Chelovek i obshchestvo = Bulletin of the Russian New University. Series: Man and Society*, 2022, is. 3, pp. 58–61.

9. Biekenov N. A. Nekotorye problemy obespecheniya kiberbezopasnosti v Respublike Kazahstan [Some problems of cybersecurity in the Republic of Kazakhstan]. *Vestnik Instituta zakonodatel'stva Respubliki Kazahstan = Bulletin of the Institute of Legislation of the Republic of Kazakhstan*, 2014, no. 1 (33), pp. 16–20.

10. Dzhansaraeva R. E., Aratuly K. Bor'ba s kiberprestupleniyami: sravnitel'nyj analiz zakonodatel'stva stran SNG [Combating cybercrime: a comparative analysis of the legislation of the CIS countries]. *Kriminologicheskij zhurnal Bajkal'skogo gosudarstvennogo universiteta ekonomiki i prava = Criminological Journal of the Baikal State University of Economics and Law*, 2012, no. 3, pp. 95–99.

11. Dybys R. T. Administrativno-pravovye sredstva obespecheniya informacionnoj bezopasnosti v Respublike Kazahstan [Administrative and legal means of ensuring information security in the Republic of Kazakhstan]. *Kazahskaya civilizaciya = Kazakh civilization*, 2017, no. 3, pp. 47–54.

12. Kambarov A. N., Tulaganov N. A. [Problems of ensuring information security of the Republic of Kazakhstan]. *Fizika. Tekhnologii. Innovacii. Sbornik nauchnyh trudov [Physics. Technologies. Innovations. Collection of scientific papers]*; ed. by V. N. Rychkova. Ekaterinburg, Ural. feder. Univ. Publ., is. 1, 2015, pp. 257–262.

13. Mahmutov A. [The concept of national security of Kazakhstan in the context of modern foreign policy realities]. *Vneshnopoliticheskie perspektivy i novye koncepty mezhdunarodnoj strategii Kazakhstana. Materialy kruglogo stola [Foreign policy prospects and new concepts of Kazakhstan's international strategy. Materials of the round table]*. Almaty, Zhibek zholy, 2012, pp. 14–15. (In Russ.)

14. Muhamedzhanova A. D. Osobennosti dinamiki kiberprestupnosti v Respublike Kazahstan i ee vliyanie na voprosy eyo preduprezhdeniya [Features of cybercrime dynamics in the Republic of Kazakhstan and its impact on AIDS prevention issues]. *Rossijsko-aziatskij pravovoj zhurnal = Russian-Asian Law Journal*, 2022, no. 2, pp. 49–55.

15. Myrzahmet A. A. Pravovoe obespechenie informacionnoj bezopasnosti Respubliki Kazahstan [Legal support of information security of the Republic of Kazakhstan]. *Molodoj uchenyj = Young scientist*, 2019, no. 15 (253), pp. 119–122.
16. Sabirov K. K., Ahmedzhanov F. R. Nekotorye voprosy zakonodatel'nogo ukrepleniya kiberbezopasnosti v Respublike Kazahstan [Some issues of legislative strengthening of cybersecurity in the Republic of Kazakhstan]. *Voprosy kiberbezopasnosti = Cybersecurity issues*, 2017, no. 3 (21), pp. 55–62.
17. Kriminologiya [Criminology]; ed. by V. D. Malkov. Moscow, Yusticinform Publ., 2004. 524 p.
18. Prozumentov L. M. [Criminalization and decriminalization as a means of expressing criminal law policy]. *Voprosy razvitiya rossijskogo zakonodatel'stva. Sbornik materialov regional'noj nauchno-prakticheskoy konferencii* [Issues of development of Russian legislation. Collection of materials of the regional scientific and practical conference]. Tomsk, Izd-vo nauch.-tekhn. lit., 2005, pp. 132–133. (In Russ.)
19. Shestakov D. A. Kriminologiya: Prestupnost' kak svojstvo obshchestva. Kratkij kurs [Criminology: Crime as a property of society. Short course]. St. Petersburg, Lan' Publ., 2001. 259 p.
20. Mackevich I. M. Kriminologiya [Criminology]. Moscow, Norma Publ., 2017. 368 p.

Информация об авторе / Information about the Author

Карабеков Канатбек Омирзакович, адъюнкт Омской академии Министерства внутренних дел России, г. Омск, Российская Федерация, e-mail: KarabekovK@mail.ru, ORCID: 0000-0001-7461-8215

Kanatbek O. Karabekov, Adjunkt, Omsk Academy of the Ministry of Internal Affairs of Russia, Omsk, Russian Federation, e-mail: KarabekovK@mail.ru, ORCID: 0000-0001-7461-8215