Оригинальная статья / Original article

https://doi.org/10.21869/2223-1501-2022-12-5-94-102

(cc) BY 4.0

Понятие киберпреступности в Российской Федерации и Республике Казахстан

К. О. Карабеков[1] ✉

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

✉ e-mail: KarabekovK@mail.ru

Резюме

***Актуальность**. Статья посвящена одному из актуальных современных вопросов – киберпреступности. Понятие «киберпреступность» широко используется в криминологии и практической деятельности полиции в Российской Федерации и Республике Казахстан. Однако вопрос о точном и полном понимании киберпреступности, а также о его законодательном закреплении до сегодняшнего дня остается открытым. Сущность данной проблемы заключается в том, что от правильного понимания киберпреступности зависит эффективность работы правоохранительных органов по предупреждению такого рода преступлений. В настоящее время в период бурного развития информационных технологий количество преступлений, совершаемых в киберпространстве, растет пропорционально числу пользователей компьютерных сетей.*

***Целью** является точное и полное определение понятия «киберпреступность» в Российской Федерации и Республике Казахстан.*

***Задачи**: на основе имеющихся в юридической литературе определений выявить главные признаки киберпреступности и провести систематизацию этого понятия.*

***Методология**. В процессе работы над исследованием использовались методы теоретического исследования (анализ и синтез, индукция и дедукция, мысленное моделирование), сравнительно-правовой подход.*

***Результаты**. В ходе исследования предложено понимание киберпреступности как исторически изменчивого, латентного социального и уголовно-правового негативного явления, представляющего собой систему преступлений, совершённых дистанционно в информационном пространстве с использованием средств информационно-коммуникационных технологий.*

***Выводы**. Исследование позволило прийти к выводу, что анализ доктринальных подходов не показывает единого мнения среди ученых в определении киберпреступности. Это обусловлено различными трактовками киберпространства и способов использования компьютерных систем при совершении противоправных действий. Несмотря на различия ученые ставят вопрос о соотношении международного законодательства и законодательства России относительно перечня противоправных действий, которые отнесены к преступлениям, совершаемым в киберсфере.*

По нашему мнению, понятие «киберпреступность» может применяться к преступлениям, которые совершаются с использованием любых средств информационно-коммуникационных технологий. Киберпреступность – это более широкое понятие, чем «интернет-преступность», так как оно включает в себя возможность совершения преступлений с использованием любых информационных или телекоммуникационных сетей.

***Ключевые слова**: киберпреступления; киберпреступность; кибербезопасность; информационно-коммуникационные технологии; информационное пространство.*

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

Для цитирования: Карабеков К. О. Понятие киберпреступности в Российской Федерации и Республике Казахстан // Известия Юго-Западного государственного университета. Серия: История и право. 2022. Т. 12, № 5. С. 94–102. https://doi.org/10.21869/2223-1501-2022-12-5-94-102.

Поступила в редакцию 11.08.2022 Принята к публикации 09.09.2022 Опубликована 12.10.2022

© Карабеков К. О., 2022

The Concept of Cybercrime in the Russian Federation and the Republic of Kazakhstan

Kanatbek O. Karabekov[1] ✉

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

✉ e-mail: KarabekovK@mail.ru

Abstract

Relevance. *The article is devoted to one of the current topical issues - the concept of cybercrime in the Russian Federation and the Republic of Kazakhstan. The concept of cybercrime is widely used in criminology and practical activities of the police of the two countries. However, an accurate and complete understanding of cybercrime, as well as its legislative consolidation, remains open to this day. The essence of this problem lies in the fact that the effectiveness of law enforcement agencies in preventing such crimes depends on the correct understanding of cybercrime. Currently, during the rapid development of information technology, the number of crimes committed in cyberspace is growing in proportion to the number of users of computer networks.*

The purpose *is to give an accurate and complete definition of the concept of cybercrime in the Russian Federation and the Republic of Kazakhstan.*

Objectives: *based on the available definitions in the legal literature, to identify the main signs of cybercrime and to systematize the concept of "cybercrime".*

Methodology. *In the process of working on the study, methods of theoretical research (analysis and synthesis, induction and deduction, mental modeling), a comparative legal approach were used.*

Results. *The study suggests an understanding of cybercrime as a historically volatile, latent, social and criminal-legal negative phenomenon, which is a system of crimes committed virtually in the information space using information and communication technologies.*

Conclusions. *The study concluded that the analysis of doctrinal approaches does not show a consensus among scientists in the definition of cybercrime. This is due to different interpretations of cyberspace and ways of using computer systems when committing illegal actions. Despite the differences, scientists raise the question of the relationship between international legislation and Russian legislation, regarding the list of illegal actions that are attributed to crimes committed in the cybersphere.*

In our opinion, the concept of "cybercrime" can be applied to crimes that are committed using any means of information and communication technologies. Cybercrime is a broader concept than "Internet crime", as it includes the possibility of committing crimes using any information or telecommunications networks.

Keywords: *cybercrime; cybercrime; cybersecurity; information and communication technologies; information space.*

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. The Concept 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*. 2022; 12(5): 94–102. (In Russ.) https://doi.org/10.21869/2223-1501-2022-12-5-94-102.

Received 11.08.2022 Accepted 09.09.2022 Published 12.10.2022

***

Введение

С появлением компьютерных технологий общество вышло на новый виток своего развития. Мир поделился на две части: реальную и виртуальную. За относительно короткий период своего существования век информационных технологий кардинально изменил общество и самого человека. Перед человечеством стала новая угроза безопасности – киберпреступность [1, с. 79].

Киберпреступления − это новый вид преступных действий, который появился под влиянием процессов модернизации и улучшения компьютерной техники, глобальных информационных сетей [2, с. 63].

Одной из причин ускоренного роста киберпреступности являются технологические тренды. К 2022 г. к глобальной сети Интернет будет подключен 1 трлн устройств. К 2023 г. у 80% людей появится аватар в цифровом мире [3, с. 166−167].

Актуальность изучения киберпреступлений обусловлена тем, что современное постиндустриальное, информационное общество находится в состоянии постоянного развития: в экономике наличествует инновационный сектор с высокопроизводительной промышленностью, индустрией знаний, где часто совершаются и киберпреступления [4, с. 94].

Определение понятия киберпреступности уже давно стало злободневной темой. С течением времени она не теряет своей актуальности, более того, приобретает новые аспекты. Это происходит потому, что, во-первых, методы совершения киберпреступлений быстро развиваются, соответственно признаки киберпреступности тоже меняются, во-вторых, регулярно возникают новые киберугрозы для безопасности населения, в-третьих, темпы законодательного регулирования не соответствуют темпам роста преступной деятельности в киберпространстве, в-четвертых, назрела потребность прогнозирования киберпреступности и выработки адекватных мер противодействия ей.

Методология

Основу научного исследования составил всеобщий диалектический метод. Также использован общенаучный метод анализа, который позволил провести систематизацию признаков киберпреступности. Метод научного синтеза использовался для авторского формулирования понятия киберпреступности. Метод сравнительного правоведения стал основой для характеристики понятий киберпреступности в юридической науке и в законодательстве Российской Федерации и Республики Казахстан.

Результаты и их обсуждение

Борьба с преступлениями, которые совершаются в электронной среде, осложняется аспектами: во-первых, общество сталкивается с правонарушителями нового формата; во-вторых, для раскрытия данных преступлений требуются специализированные сотрудники, обладающие особыми знаниями и опытом; в-третьих, контролировать киберпреступность и бороться с ней на уровне отдельного государства практически невозможно [3, с. 376].

В настоящее время большое количество научных публикаций в России, Казахстане и в других странах посвящено борьбе с компьютерной преступностью и обеспечению кибербезопасности. В университетах вводятся новые академические дисциплины, рассматривающие вопросы кибербезопасности. Исследованиями киберпреступности занимаются представители разных направлений научного сообщества, но больше всего – IT-специалисты и юристы. Именно они наиболее активно пытаются понять и описать содержание этого постоянно развивающегося явления.

Несмотря на то, что информация о киберпреступности быстро и впечатляюще накапливается, в юридической науке еще не выработано единое полное определение данного явления. В этом можно убедиться, проанализировав понятия киберпреступности, которые даны различными учеными.

Так, согласно мнению А. В. Федорова, киберпреступность – это преступность в информационном пространстве, моделируемом при помощи компьютера, в котором находятся сведения о лицах, предметах, фактах, событиях, явлениях и процессах, представленных в математи-

ческом, символьном или в любом другом выражении и находящихся в движении по локальным и глобальным компьютерным сетям, либо сведения, хранящиеся в памяти любого физического или виртуального устройства, а также другого носителя, специально предназначенного для их хранения, обработки и передачи [6, с. 111].

С точки зрения В. А. Номоконова, киберпреступность охватывает как преступность, в которой компьютер является предметом, а информационная безопасность – объектом преступления, так и иные деяния, где компьютеры используются как орудия или средства совершения преступлений против собственности, авторских прав, общественной безопасности или нравственности [7, с. 105].

По мнению Т. Л. Тропиной, киберпреступность образуют деяния, совершенные в киберпространстве, представляющие собой виновные противоправные вмешательства в функционирование компьютеров, компьютерных программ, компьютерных сетей; несанкционированные модификации компьютерных данных, а также иные противоправные общественно опасные действия, совершенные с помощью или посредством компьютеров, компьютерных сетей и программ [8, с. 141].

Вышеуказанные ученые (А. В. Федоров, В. А. Номоконов, Т. Л. Тропина), по нашему мнению, в своих определениях не раскрывают все признаки киберпреступности, делая акцент на предмет киберпреступления и обобщая киберпреступность как преступность в информационном пространстве или киберпространстве.

По определению И. Г. Чекунова, киберпреступность – это самостоятельный вид преступности, который определяется посредством применения признаков объективной стороны, таких как средство совершения преступления и орудие совершения преступления. В качестве них выступают вредоносная программа или техническое средство, подключенное к сети Интернет, использование которого направлено на причинение ущерба физическому или юридическому лицу. По его мнению, понятие «киберпреступность» охватывает все преступные деяния, которые совершаются с использованием средств информационно-коммуникационных технологий [9, с. 185]. По нашему мнению, этот автор шире охватил понятие киберпреступности в современных реалиях, учитывая совершение киберпреступлений с использованием средств информационно-коммуникационных технологий.

Т. Н. Шарыпова и А. А. Сидоренко считают, что термин «киберпреступность» сочетает в себе «любое преступление, которое может совершаться с помощью компьютерной системы или сети, в рамках компьютерной системы или сети, против компьютерной системы или сети» [10, с. 975]. Но при этом они не учитывают использование других средств информационно-коммуникационных технологий (например, различных носителей информации или средств связи) при совершений киберпреступлений.

Наиболее полный перечень обстоятельств, характерных для большинства преступлений, совершаемых в глобальных компьютерных сетях, дает А. Л. Осипенко (особая подготовленность преступников, повышенная скрытность, трансграничный, дистанционный характер и многообразие способов совершения преступлений т.д.) [10, с. 109–110]. Аналогичные особенности киберпреступления отмечают также А. А. Коновалов, С. А. Наумов, Д. Д. Колесникова [12, с. 23]. Безусловно, все это характеризует ситуации, в которых совершаются киберпреступления, однако когда речь идет о признаках, необходимо выделять только наиболее существенные обстоятельства.

Также можно выделить работы казахстанских исследователей, которые занимались проблемами киберпреступности:

Б. Х. Толеубекова [13], Т. Б. Сеитов [14], А. К. Нурпеисова [15], К. Аратулы [16].

Ученые Казахстана рассматривают киберпреступность как компьютерную преступность, в основном (Б. Х. Толеубекова, Т. Б. Сеитов, А. К. Нурпеисова) в уголовно-правовом, уголовно-процессуальном, криминалистическом аспекте. Однако заслуживают отдельного внимания научные труды К. Аратулы, который занимался исследованием компьютерной преступности в криминологическом аспекте. Согласно результатам его научных исследований законодательной практики различных государств, а также международного сообщества, к числу компьютерных преступлений можно отнести преступления в сфере компьютерной информации и преступления, совершаемые с использованием информационных технологий [17]. По мнению К. Аратулы, в зависимости от объекта и предмета посягательства все компьютерные преступления, предусмотренные как в отечественном, так и в зарубежном уголовном праве, можно разделить на две группы:

1) преступления в сфере компьютерной информации;

2) преступления, где компьютерная информация является орудием или средством совершения другого преступления.

Согласно мнениям казахстанских исследователей К. К. Сабирова, Ф. Р. Ахмеджанова, на сегодняшний день в Казахстане наблюдаются все признаки институционализации киберпреступности: формируются правовые нормы в борьбе с киберпреступниками, создаются международные институты по кибербезопасности, развиваются новые сферы деятельности, ориентированные на противодействие киберпреступности, и др. Также в Республике Казахстан существует как техническая, так и правовая база для создания системы безопасности киберпространства и сетей телекоммуникаций [18, с. 56].

Из этого следует, что понятие киберпреступности в Республике Казахстан широко используется в комплексном его понимании. Однако полное и точное определение киберпреступности казахстанские исследователи не дают, и этот вопрос также не регламентирован в нормативных правовых актах.

В век цифровизации за информацией разворачивается настоящая охота, хакеры придумывают все более сложные вирусы, а те, кто с ними борются, наращивают все более сложную защиту. 90% от всех киберпреступных замыслов – это массовые угрозы, с которыми сталкиваются пользователи каждый день: черви, трояны, фишинговые письма, 9,9% – это целевые атаки, ориентированные на конкретных людей и компании, а последние 0,1% – это новинка нашего столетия – кибероружие [19, с. 49].

Сегодня существует много способов совершения киберпреступлений, но не все из них актуальны на данный момент – некоторые устарели, другие требуют от хакера большого опыта, а третьи просто не подходят для достижения цели преступника. Поэтому злоумышленники очень серьезно подходят к выбору способа совершения киберпреступления.

Под способом совершения преступления ученые объясняют как объективно и субъективно обусловленные правила поведения субъекта до, в момент и после совершения преступления, которые оставляют разного рода характерные следы, позволяющие с помощью криминалистических приемов и средств получить представление о сущности происшедшего, своеобразии криминального поведения правонарушителя, его личных данных и, соответственно, найти более рациональные методы решения задач раскрытия преступления.

Проанализировав научные труды ученых, можно выделить следующие способы совершения киберпреступлений [20, с. 43]:

– похищение компьютерной техники;

– перехват информации;

– несанкционированный доступ к информации;

– манипуляция данными и управляющими командами;

– компьютерный саботаж;

– комплексные методы.

В результате работы на основе исследования основных методов совершения киберпреступлений была проведена систематизация признаков понятия «киберпреступность».

Выводы

Подводя итоги, необходимо отметить, что анализ доктринальных подходов не показывает единого мнения среди ученых в определении киберпреступности. Это обусловлено различными трактовками киберпространства и способов использования компьютерных систем при совершении противоправных действий. Несмотря на различия, ученые ставят вопрос о соотношении международного законодательства и законодательства России относительно перечня противоправных действий, которые отнесены к преступлениям, совершаемым в киберсфере.

По нашему мнению, понятие «киберпреступность» может применяться к преступлениям, которые совершаются с использованием любых средств информационно-коммуникационных технологий. Киберпреступность – это более широкое понятие, чем «интернет-преступность», т. к. оно включает в себя возможность совершения преступлений с использованием любых информационных или телекоммуникационных сетей. Сеть Интернет – самая популярная сеть, но существуют также и другие сети, которые могут быть использованы преступниками в качестве средства совершения преступления, например такие сети, как ANts P2, Bitmessage, Freenet, Gnutella, Manolito, MUTE, Nodezilla, OneSwarm, RShare, ZeroNet, TOR (The Onion Router), StealthNet, Hyperboria, JAP (Java Anonymous Proxy).

Изучив и оценив понятия киберпреступности, имеющиеся в трудах ученых России и Казахстана, точки зрения на содержание ее признаков, возможно, по нашему мнению, выделить основные признаки киберпреступности:

– это преступность в информационно-телекоммуникационном пространстве;

– объектом преступления является информационная безопасность;

– охват всех преступных деяний, которые совершаются с использованием средств информационно-телекоммуникационных технологий;

– повышенная скрытность совершения преступления, которая обеспечена спецификой сетевого информационно-телекоммуникационного пространства (развитые механизмы анонимности, сложность инфраструктуры и т.п.);

– возможность совершения преступления в автоматизированном режиме в нескольких местах одновременно;

– дистанционный характер преступных действий в условиях отсутствия физического контакта преступника и потерпевшего;

– невозможность предотвращения и пресечения преступлений данного вида традиционными средствами;

– очень высокий потенциал развития и нарастания неблагоприятных последствий;

– несоответствие темпа роста преступной деятельности в киберпространстве темпам законодательного регулирования и реализации отдельных средств противодействия такой деятельности.

На основании вышеизложенного можно дать следующее определение киберпреступности: *это исторически изменчивое, латентное социальное и уголовно-правовое негативное явление, представляющее собой систему преступлений, совершённых дистанционно в информационном пространстве с использованием средств информационно-коммуникационных технологий.*

Список литературы

1. Осташевская В. О. Борьба с киберпреступностью: внутринациональный и международный аспект // Вестник студенческого научного общества ГОУ ВПО «Донецкий национальный университет». 2020. Т. 4, № 12-2. С. 79–83.

2. Черепашкин А. С. Противодействие киберпреступности в России: уголовно-правовые и криминологические аспекты // Вестник Уральского института экономики, управления и права. 2021. № 3 (56). С. 63–66.

3. Жадан И. Э. Киберпреступность как угроза международной безопасности // Математическое и компьютерное моделирование в экономике, страховании и управлении рисками. 2020. № 5. С. 166–169.

4. Тулегенов В. В. Киберпреступность как форма выражения криминального профессионализма // Криминология: вчера, сегодня, завтра. 2014. № 2 (33). С. 95–97.

5. Евкина И. И. Киберпреступность как угроза информационной безопасности // Инновации. Наука. Образование. 2021. № 36. С. 375–377.

6. Федоров А. В. Информационная безопасность в мировом политическом процессе: М.: МГИМО Ун-т, 2006. 218 с.

7. Номоконов В.А. Актуальные проблемы борьбы с киберпреступностью // Информационные технологии и безопасность: сборник научных трудов Международной конференции. Киев: Национальная академия наук Украины, 2003. Вып. 3. С. 104–108.

8. Тропина Т. Л. Киберпреступность и кибертерроризм // Организованная преступность, терроризм и коррупция: криминологический ежеквартальный альманах. 2003. Вып. 2. С. 140–144.

9. Чекунов И. Г. Киберпреступность: понятие, классификация, современные вызовы и угрозы // Молодые ученые. 2012. № 3. С. 178–186.

10. Шарыпова Т. Н., Сидоренко А. А. Киберпреступность в XXI веке // Аллея науки. 2019. Т. 2, № 1 (28). С. 978–981.

11. Осипенко А. Л. Сетевая компьютерная преступность: теория и практика борьбы: монография. Омск: Омская акад. МВД России, 2009. 480 с.

12. Коновалов А. А., Наумов С. А., Колесникова Д. Д. Киберпреступность как глобальная угроза экономической безопасности: виды, особенности, проблемы воздействия // Ростовский научный журнал. 2018. № 1. С. 20–27.

13. Толеубекова Б. Х. Проблемы совершенствования борьбы с преступлениями, совершаемыми с использованием компьютерной техники: дис. ... д-ра юрид. наук. Алматы, 1998. 380 с.

14. Сеитов Т. Б. Международно-правовое сотрудничество государств в борьбе с компьютерной преступностью: дис. … канд. юрид. наук. Алматы, 2002. 120 с.

15. Нурпеисова А. К. Уголовно-правовые и криминалистические аспекты компьютерной преступности: автореф. дис. … канд. юрид. наук. Караганда, 2010. 33 с.

16. Аратулы К. Уголовная политика в борьбе с компьютерной преступностью в условиях глобализации (на казахском языке): дис. … д-ра философии. Алматы, 2013. 166 с.

17. Аратулы К. Преступления в сфере компьютерной информации в РК и зарубежных странах // Вестник КазНУ. Серия Юридическая. 2010. Т. 56, № 4. С. 105–109.

18. Сабиров К. К., Ахмеджанов Ф. Р. Некоторые вопросы законодательного укрепления кибербезопасности в Республике Казахстан // Вопросы кибербезопасности. 2017. № 3 (21). С. 55–62.

19. Магомедов Р. М. Анализ киберпреступности и борьба с ней // Экономика: вчера, сегодня, завтра. 2020. Т. 10, № 6-1. С. 48–54.

20. Мамцов К. Г. Киберпреступность как угроза национальной безопасности // Молодой исследователь Дона. 2022. № 1 (34). С. 42–45.

References

1. Ostashevskaya V. O. Bor'ba s kiberprestupnost'yu: vnutrinacional'nyj i mezhdunarodnyj aspekt [The fight against cybercrime: the domestic and international aspect]. *Vestnik studencheskogo nauchnogo obshchestva GOU VPO "Doneckij nacional'nyj universitet" = Bulletin of the Student Scientific Society of the Donetsk National University*, 2020, vol. 4, no. 12-2, pp. 79–83.

2. Cherepashkin A. S. Protivodejstvie kiberprestupnosti v Rossii: ugolovno-pravovye i kriminologicheskie aspekty [Countering cybercrime in Russia: criminal law and criminological aspects]. *Vestnik Ural'skogo instituta ekonomiki, upravleniya i prava = Bulletin of the Ural Institute of Economics, Management and Law*, 2021, no. 3 (56), pp. 63–66.

3. Zhadan I. E. Kiberprestupnost' kak ugroza mezhdunarodnoj bezopasnosti [Cybercrime as a threat to international security]. *Matematicheskoe i komp'yuternoe modelirovanie v ekonomike, strahovanii i upravlenii riskami = Mathematical and computer modeling in economics, insurance and risk management*, 2020, no. 5, pp. 166–169.

4. Tulegenov V. V. Kiberprestupnost' kak forma vyrazheniya kriminal'nogo professionalizma [Cybercrime as a form of expression of criminal professionalism]. *Kriminologiya: vchera, segodnya, zavtra = Criminology: yesterday, today, tomorro*w, 2014, no. 2 (33), pp. 95–97.

5. Evkina I. I. Kiberprestupnost' kak ugroza informacionnoj bezopasnosti [Cybercrime as a threat to information security]. *Innovacii. Nauka. Obrazovanie = Innovations. The science. Education*, 2021, no. 36, pp. 375–377.

6. Fedorov A. V. Informacionnaya bezopasnost' v mirovom politicheskom processe [Information security in the global political process]. Moscow, MGIMO Univ. Publ., 2006. 218 p.

7. Nomokonov V. A. [Actual problems of combating cybercrime]. *Informacionnye tekhnologii i bezopasnost'. Sbornik nauchnyh trudov mezhdunarodnoj konferencii* [Information technologies and security. Collection of scientific papers of the international conference]. Kiev, Nacional'naya akademiya nauk Ukrainy, 2003, is. 3, pp. 104–108. (In Russ.)

8. Tropina T. L. Kiberprestupnost' i kiberterrorizm [Cybercrime and cyberterrorism]. *Organizovannaya prestupnost', terrorizm i korrupciya = Organized crime, terrorism and corruption,* 2003, is. 2, pp. 140–144.

9. Chekunov I. G. Kiberprestupnost': ponyatie, klassifikaciya, sovremennye vyzovy i ugrozy [Cybercrime: concept, classification, modern challenges and threats]. *Molodye uchenye = Young Scientists*, 2012, no. 3, pp. 178–186.

10. Sharypova T. N., Sidorenko A. A. Kiberprestupnost' v XXI veke [Cybercrime in the XXI century]. *Alleya nauki = Alley of Science*, 2019, vol. 2, no. 1 (28), pp. 978–981.

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

12. Konovalov A. A., Naumov S. A., Kolesnikova D. D. Kiberprestupnost' kak global'naya ugroza ekonomicheskoj bezopasnosti: vidy, osobennosti, problemy vozdejstviya [Cybercrime as a global threat to economic security: types, features, impact problems]. *Rostovskij nauchnyj zhurnal = Rostov Scientific Journal*, 2018, no. 1, pp. 20–27.

13. Toleubekova B. H. Problemy sovershenstvovaniya bor'by s prestupleniyami, sovershaemymi s ispol'zovaniem komp'yuternoj tekhniki. Diss. dokt. yurid. nauk [Problems of im-

proving the fight against crimes committed using computer technology. Dr. legal. sci. diss.]. Almaty, 1998. 380 p.

14. Seitov T. B. Mezhdunarodno-pravovoe sotrudnichestvo gosudarstv v bor'be s komp'yuternoj prestupnost'yu. Diss. kand. yurid. nauk [International legal cooperation of States in the fight against computer crime. Cand. legal. sci. diss.]. Almaty, 2002. 120 p.

15. Nurpeisova A. K. Ugolovno-pravovye i kriminalisticheskie aspekty komp'yuternoj prestupnosti. Avtoref. diss. kand. yurid. nauk [Criminal law and criminalistic aspects of computer crime. Cand. legal. sci. abstract diss.]. Karaganda, 2010. 33 p.

16. Aratuly K. Ugolovnaya politika v bor'be s komp'yuternoj prestupnost'yu v usloviyah globalizacii (na kazahskom yazyke). Diss. dokt. filosofii [Criminal policy in the fight against computer crime in the context of globalization (in Kazakh). Dr. Philos. sci. diss.]. Almaty, 2013. 166 p.

17. Aratuly K. Prestupleniya v sfere komp'yuternoj informacii v RK i zarubezhnyh stranah [Crimes in the field of computer information in the Republic of Kazakhstan and foreign countries]. Available at: https://articlekz.com/article/10037 (accessed 14.09.2022).

18. 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.

19. Magomedov R. M. Analiz kiberprestupnosti i bor'ba s nej [Cybercrime analysis and fight against it]. *Ekonomika: vchera, segodnya, zavtra = Economy: yesterday, today, tomorrow*, 2020, vol. 10, no. 6-1, pp. 48–54.

20. Mamcov K. G. Kiberprestupnost' kak ugroza nacional'noj bezopasnosti [Cybercrime as a threat to national security]. *Molodoj issledovatel' Dona = Young researcher of the Don*, 2022, no. 1 (34), pp. 42–45.

Информация об авторе / Information about the Author

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

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