DOI: https://doi.org/10.24833/0869-0049-2021-4-123-135

Исследовательская статья
Поступила в редакцию: 12.07.2021
Принята к публикации: 27.10.2021

Ляйсян Маратовна СТАРКОВА
Астраханский государственный университет,
Татищева ул., д. 20а, Астрахань, 414056, Российская Федерация,
5leska5@mail.ru
ORCID: 0000-0002-4411-6510

ПОДХОДЫ К ПОНИМАНИЮ И НОРМАТИВНОМУ ОПРЕДЕЛЕНИЮ КАТЕГОРИИ «КИБЕРПРЕСТУПНОСТЬ» И СМЕЖНЫХ ПОНЯТИЙ В ПРАКТИКЕ РЕГИОНАЛЬНЫХ МЕЖДУНАРОДНЫХ ОРГАНИЗАЦИЙ

ВВЕДЕНИЕ. *На фоне развернувшейся эпидемии коронавируса наметившиеся в предыдущие годы тенденции киберпреступности достигли небывалых масштабов. Стремительный перевод многих базовых сфер общественного функционирования на цифровую платформу в условиях фактического правового вакуума предоставил преступникам практически безграничные возможности. В этих условиях задача совершенствования и унификации базовых категорий в сфере борьбы с «новой формой преступности» представляет первостепенный интерес не только с позиций запросов теории, но и для создания эффективного международно-правового механизма противодействия данной угрозе.*

МАТЕРИАЛЫ И МЕТОДЫ. *Материалом для исследования послужили правовые документы, разработанные под эгидой 14 региональных международных организаций, представляющих собой ту или иную региональную группу, научные труды зарубежных и отечественных ученых. Методологическую основу исследования составили традиционные для юридических работ общенаучные и частнонаучные методы познания.*

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ. *В результате проведенного исследования были выявлены несогласованность терминологии, отсутствие единообразно понимаемого и применяемого нормативно-закрепленного определения «новой формы преступности» и смежных понятий, которые соответствовали бы критерию аутентичности. Региональные международные организации оперируют такими понятиями, как «киберпреступность», «атаки против информационных систем», «преступления в сфере компьютерной информации», «преступления в сфере информационных технологий», «информационная преступность», «преступления, относящиеся к компьютерам и сетям», «риски цифровой безопасности», «использование информационно-коммуникационных технологий (ИКТ) в террористических и преступных целях». Все это свидетельствует об отсутствии единых подходов к пониманию самой сущности и специфических особенностей данного криминального явления.*

ОБСУЖДЕНИЕ И ВЫВОДЫ. *Автор обращает внимание, что термин «киберпреступность» используется в 7 из 14 групп международных документов регионального характера. Анализ работ отечественных и зарубежных исследователей подтверждает обоснованность применения термина «киберпреступность», как наиболее полно и точно отражающего уникальные свойства данного вида преступности, его техническую составляющую. На*

основе соотнесения и сравнительного исследования терминов «информационная преступность», «компьютерная преступность», «киберпреступность» автор формулирует базовые положения, которые возможно учесть при попытках разработки унифицированного понятия. Автор обращает внимание на тот факт, что с учетом специфического характера объекта, предмета и виртуальной среды совершения данных преступлений, любая правовая норма должна быть сформулирована и соотнесена с объективной возможностью ее практической реализации с учетом технических особенностей.

КЛЮЧЕВЫЕ СЛОВА: *киберпреступность, компьютерная преступность, информационная преступность, технотронная преступность, международные региональные организации, международно-правовая система противодействия киберпреступности, унификация понятийного аппарата*

ДЛЯ ЦИТИРОВАНИЯ: Старкова Л.М. 2021. Подходы к пониманию и нормативному определению категории «киберпреступность» и смежных понятий в практике региональных международных организаций. – *Московский журнал международного права.* №4. С. 123–135. DOI: https://doi.org/10.24833/0869-0049-2021-4-123-135

Автор заявляет об отсутствии конфликта интересов.

Research article
Received 12 July 2021
Approved 27 October 2021

DOI: https://doi.org/10.24833/0869-0049-2021-4-123-135

Lyasyan M. STARKOVA
Astrakhan State University
20A, ul. Tatishcheva, Astrakhan, Russian Federation, 414056
5leska5@mail.ru
ORCID: 0000-0002-4411-6510

APPROACHES TO UNDERSTANDING AND NORMATIVE DEFINITION OF THE CATEGORY OF "CYBERCRIME" AND RELATED CONCEPTS IN THE PRACTICE OF REGIONAL INTERNATIONAL ORGANIZATIONS

INTRODUCTION. *Against the background of the unfolding epidemic of coronavirus, the trends in cybercrime that appeared in previous years have reached unprecedented magnitudes. The rapid transfer of many basic spheres of social functioning to a digital platform in an actual legal vacuum provided criminals with almost unlimited opportunities. In these circumstances, the task of improving and unifying the basic categories in the field of combating the «new form of crime» is of paramount interest not only from the point of view of theory, but also in order to create an effective international legal mechanism to counter this threat.*

MATERIALS AND METHODS. *The material for the study were legal documents developed under the auspices*

of 14 regional international organizations, which represent one or another regional group, scientific works of foreign and domestic scientists. The methodological basis of the study was the general scientific and private scientific methods of cognition, traditional for legal work.

RESEARCH RESULTS. *The study revealed inconsistencies in terminology, the absence of a uniformly understood and applied normative definition of a «new form of crime» and related concepts that would meet the criterion of authenticity. Regional international organizations operate with such concepts as "cybercrime", "attacks against information systems", "crimes in the field of computer information", "crimes in the field of information technology", "information crime", "crimes related to computers and networks", "digital security risks", "the use of information and communication technologies (ICTs) for terrorist and criminal purposes". All this indicates the absence of common approaches to understanding the very essence and specific features of this criminal phenomenon.*

DISCUSSION AND CONCLUSIONS. *The author draws attention to the fact that the term "cybercrime" is used in 7 out of 14 groups of international documents of a regional nature. Analysis of the work of domestic and foreign researchers confirms the validity of the use of the term "cybercrime", as most fully and accurately reflecting the unique properties of this type of crime, its technical component. Based on the correlation and comparative study of the terms "information crime", "computer crime", "cybercrime", the author formulates basic provisions that can be taken into account when trying to develop a unified concept. The author draws attention to the fact that, taking into account the specific nature of the object, subject and virtual environment of committing these crimes, any legal norm should be formulated and correlated with the objective possibility of its practical implementation, taking into account technical characteristics.*

KEYWORDS: *cybercrime, computer crime, information crime, technotronic crime, international regional organizations, international legal system against cybercrime, unification of the conceptual apparatus*

FOR CITATION: Starkova L.M. Approaches to Understanding and Normative Definition of the Category “Cybercrime” and Related Concepts in the Practice of Regional International Organizations. – *Moscow Journal of International Law.* 2021. No. 4. P. 123–135. DOI: https://doi.org/10.24833/0869-0049-2021-4-123-135

The author declares the absence of conflict of interest.

1. Введение

На всем протяжении развития и становления информационного общества информация как базовый ресурс представляла интерес для криминальных структур, использующих достижения технологической революции как в качестве средства, так и в качестве объекта преступлений. Появление глобальной сети Интернет выводит проблему киберпреступности за рамки временных, пространственных и даже политических границ. Киберпреступность приобретает характер транснациональной угрозы, требующей эффективных и своевременных действий со стороны международного сообщества. Элемент транснациональности делает международное сотрудничество ключевым фактором принятия эффективных мер противодействия новой угрозе. На этом этапе начинается формирование международной системы противодействия киберпреступности, в основу которой закладываются правовые источники международного характера. На протяжении последних 20 лет в ряде регионов были реализованы различные подходы, направленные на правовую регламентацию борьбы с киберпреступностью и приняты соответствующие региональные соглашения.

Стоит отметить, что проблема киберпреступности, безусловно носит комплексный многоаспектный характер, что определяет многообразие направлений и подходов к ее исследованию. Поэтому в данной работе полагаем необходимым сузить рамки исследования. Таким образом, целью данной работы является анализ понятийного аппарата в сфере борьбы с киберпреступностью (понятия «киберпреступность», «информационная преступность», «компьютерная преступность»), разработанного и применяемого в рамках международных нормативных источников регионального характера и выработка на основе проведенного сравнительного анализа рекомендаций и доктринального обоснования применимости рассмотренных правовых категорий.

2. Нормативное определение понятия «киберпреступность», применяемое в документах региональных международных организаций

В основу исследования заложен анализ правовых документов, разработанных в контексте или под эгидой 14 региональных международных организаций, представляющих собой ту или иную региональную группу согласно принципу географического распределения. Стоит отметить, что документы различаются по юридической силе и соответствующим правовым последствиям. Исходя из критерия обязательности, данные документы разделены на две группы: обязательные и рекомендательного характера. Так, ряд документов (Конвенция Совета Европы о киберпреступности 2001г., Конвенция Африканского союза о кибербезопасности и защите персональных данных 2014 г., Конвенция Лиги арабских государств о борьбе с преступлениями в области информационных технологий 2010 г., Соглашение о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере информационных технологий 2018 г. и др.) имеют характер межгосударственных соглашений, что влечет наложение определенных юридических обязательств на государство-участника в соответствии с принципом добросовестного выполнения обязательств, принятых на себя в соответствии с международным соглашением[1]. Другие документы (Типовые законы Содружества Наций о компьютерных преступлениях и электронных доказательствах 2002 г., Типовой закон о компьютерных преступлениях и киберпреступности Сообщества развития Юга Африки (САДК) 2012 г., Декларация G7 об ответственном поведении государств в киберпространстве, Лука, 2017 г. и др.) носят рекомендательный характер и выступают в качестве общих правовых рамок и типовых моделей законодательства в сфере противодействия киберпреступности, что, в свою очередь, не предполагает установление каких-либо юридических обязательств для государств. В таблице содержится полный перечень указанных документов:

Обязательные	Рекомендательного характера
Совет Европы: Конвенция Совета Европы о киберпреступности 2001 г. (Будапештская Конвенция)	**Сообщество развития Юга Африки (САДК):** Типовой закон о компьютерных преступлениях и киберпреступности Сообщества развития Юга Африки (САДК) 2012 г.
Европейский Союз (ЕС): Директива 2013 / 40 / ЕС Европейского парламента и Совета от 12 августа 2013 г. о нападениях на информационные системы и замене Рамочного решения Совета 2005 / 222 / ЈНА	**Организация экономического сотрудничества и развития (ОЭСР):** – «Рекомендация ОЭСР 2015 г. по управлению рисками цифровой безопасности для экономического и социального процветания», заменившая действовавшие ранее «Руководящие принципы ОЭСР по обеспечению безопасности информационных систем и сетей: На пути к культуре безопасности» 2002 г. – «Рекомендация по цифровой безопасности критически важных видов деятельности была принята Советом ОЭСР 2019 г.», заменившая «Рекомендацию ОЭСР о защите критической информационной инфраструктуры 2008 г.» – «Рекомендации, касающиеся Руководящих принципов, регулирующих защиту конфиденциальности и трансграничные потоки персональных данных 1980 г.» (обновлены в 2013 г.) – «Рекомендации о принципах формирования политики в области Интернета 2011 г.» – «Рекомендация Совета по цифровой безопасности критически важных видов деятельности 2019 г.», заменившая «Рекомендации Совета по защите критически важных информационных инфраструктур 2008 г.» – Декларация о цифровой экономике: инновации, экономический рост и социальное процветание (Канкунская декларация) 2016 г.
Содружество независимых государств (СНГ): – Соглашение о сотрудничестве в борьбе с преступлениями в сфере компьютерной информации (Соглашение Содружества Независимых Государств 2001 г.); – Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий 2018 г.	**Содружество наций (Британское содружество наций):** – Типовой закон о компьютерах и преступлениях, связанных с компьютерами 2002 г. – Типовой закон об электронных доказательствах 2002 г.

[1] Декларация о принципах международного права, касающихся дружественных отношений и сотрудничества между государствами в соответствии с Уставом Организации Объединенных Наций, принята Резолюцией Генеральной Ассамблеи ООН 1970 г. Доступ: https://www.un.org/ru/documents/decl_conv/declarations/intlaw_principles.shtml (дата обращения 04.07.2021).

Шанхайская организация сотрудничества (ШОС): Соглашение о сотрудничестве в области обеспечения международной информационной безопасности, принятое Шанхайской организацией сотрудничества в 2010 г.	**Организация американских государств (ОАГ):** – Рекомендации, принимаемые по итогам совещаний Министров юстиции и Генеральных прокуроров Америки (REMJA) 1999–2016; – Рекомендации Межправительственной группы экспертов по киберпреступности 1999–2016 гг.; – Глобальная межамериканская стратегия по кибербезопасности, утверждена резолюцией AG/RES 2004 (XXXIV-O / 04) Генеральной Ассамблеи ОАГ.
Африканский Союз: Конвенция Африканского союза о кибербезопасности и защите персональных данных 2014 г.	**Группа 7 (8) / G7 (8):** – Принципы и план действий по борьбе с высокотехнологичными преступлениями, утвержден на совещании Министров юстиции и внутренних дел 1997г. – Учреждение международной круглосуточной сети реагирования на киберинциденты в формате 24 / 7 – Декларация G7 об ответственном поведении государств в киберпространстве, Лука, 2017 г. – Динарская декларация об инициативе Киберправа 2019 г.
Экономическое сообщество Западноафриканских государств (ЭКОВАС): Директива Экономического сообщества Западноафриканских государств (ЭКОВАС) C/DIR. 1 / 08 / 11 о борьбе с киберпреступностью в рамках ЭКОВАС от 19 августа 2011 г.	**Организация по безопасности и сотрудничеству в Европе (ОБСЕ):** – Решение Постоянного совета ОБСЕ № 1039 от 26 апреля 2012г. «Разработка мер укрепления доверия с целью сокращения рисков возникновения конфликтов в результате использования информационных и коммуникационных технологий (ИКТ)» (2012, Неофициальная рабочая группа) – Решение Постоянного совета ОБСЕ № 1106 от 3 декабря 2013 г. «Первоначальный перечень мер укрепления доверия в рамках ОБСЕ с целью сокращения рисков возникновения конфликтов в результате использования ИКТ» (2013 – первый набор из 11 МД) – Решение Постоянного совета ОБСЕ № 1202 от 10 марта 2016 г. «Меры укрепления доверия в рамках ОБСЕ с целью сокращения рисков возникновения конфликтов в результате использования ИКТ» (2016 – второй набор дополнительных 5 МД) – Постановление Совета министров № 5 / 16 «Усилия ОБСЕ по сокращению рисков возникновения конфликтов в результате использования ИКТ» от 9 декабря 2016 г. (2016 – одобрены принятые 16 МД) – Постановление Совета министров № 5 / 17 «Наращивание усилий ОБСЕ по сокращению рисков возникновения конфликтов в результате использования ИКТ» от 8 декабря 2017г. (2017 – сосредоточиться на реализации 16 МД)
Лига арабских государств (ЛАГ): Конвенция Лиги арабских государств о борьбе с преступлениями в области информационных технологий, принята Лигой арабских государств в 2010 г.	**Организация Североатлантического договора (НАТО):** Таллиннское руководство по международному праву, применимому к кибервойне, Центр передового опыта совместной киберзащиты НАТО, 2013 г.; Таллиннское руководство по международному праву, применимому к кибервойне 2.0, обновленная версия 2017 г. Центр передового опыта совместной киберзащиты НАТО.

Анализ указанных документов выявил несогласованность терминологии, отсутствие единообразно понимаемого и применяемого нормативно-закрепленного определения «новой формы преступности» и смежных понятий, которые соответствовали бы критерию аутентичности. В качестве исходного определения «новой формы преступности» используются такие понятия, как *«киберпреступность», «атаки против информационных систем», «преступления в сфере компьютерной информации», «преступления в сфере информационных технологий», «информационная преступность», «преступления, относящиеся к компьютерам и сетям», «риски цифровой безопасности», «использование информационно-коммуникационных технологий (ИКТ) в террористических и преступных целях»*.

Термин «киберпреступность» используется в 7 из 14 групп международных документов регионального характера. При этом использование данного термина в названии, преамбуле и основной части документа не подкреплено нормативным определением данной категории в разделе, содержащем термины и понятия.

Так, в Конвенции Совета Европы О киберпреступности 2001 г. термин cybercrime («киберпреступность») вынесен в название документа и используется в преамбуле, между тем, конкретное содержание данного понятия не приведено. Преамбула: «Будучи убеждены в том, что настоящая Конвенция необходима для сдерживания действий, направленных против конфиденциальности, целостности и доступности компьютерных систем и сетей и компьютерных данных, а также против злоупотребления такими системами, сетями и данными, путем обеспечения уголовной наказуемости таких деяний, описываемых в настоящей Конвенции»[2].

[2] Convention on Cybercrime Council of Europe. 2001. URL: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185?module=treaty-detail&treatynum=185 (accessed 25.06.2021).

Конвенция Африканского союза о кибербезопасности и защите персональных данных 2014 г. не содержит определение понятия «киберпреступность». Между тем в Главе 3 «Обеспечение кибербезопасности и борьба с киберпреступностью» в ст. 25 «Законодательство против киберпреступности» указано, что «государствам-членам при принятии законодательных и организационных мер в сфере борьбы с киберпреступностью следует рассматривать в качестве киберпреступлений такие уголовно наказуемые деяния, которые посягают на конфиденциальность, целостность, доступность и сохранность информационных и коммуникационно-технологических систем, обрабатываемых ими данных, и базовой сетевой инфраструктуры».[3]

В Директиве Экономического сообщества Западноафриканских государств (ЭКОВАС) о борьбе с киберпреступностью в рамках ЭКОВАС 2011 г. нет конкретного определения понятия «киберпреступление», применен распространенный подход закрепления конкретного перечня деяний, подлежащих криминализации и образующих состав киберпреступления. Кроме того, следует отметить, что сфера действия документа охватывает категории общеуголовных преступлений (таких, как кража, мошенничество, обращение денежных средств и имущества, добытых преступным путем, шантаж), совершенных с использованием Интернета. Еще одна группа включенных деяний – преступления, связанные с киберпреступностью, а именно общеуголовные преступления, для обнаружения и расследования которых необходимы электронные доказательства.[4]

Типовой закон Содружества наций 2002 г. о компьютерах и преступлениях, связанных с компьютерами. В преамбуле документа содержится указание на то, что он не определяет правовую категорию «киберпреступность», учитывая, что последняя включает в себя «а) правонарушения, направленные на компьютеры, компьютерные и коммуникационные сети и системы, данные пользователей, которые в них содержатся; и б) традиционные общеуголовные составы преступлений, совершенных с использованием компьютеров, компьютерных и коммуникационных сетей и систем, а также если применение технологий имеет большое значение для расследования данных преступлений».[5]

Типовой закон о компьютерных преступлениях и киберпреступности Сообщества развития Юга Африки (САДК) 2012 г. говорит о the Computer Crime and Cybercrime Act / «Компьютерных преступлениях и киберпреступлениях»; computer and network related crime / «преступлениях, относящихся к компьютерам и сетям». Определение данных преступных деяний осуществляется через перечень конкретных составов, подлежащих криминализации.[6]

Документы Организации Американских Государств (ОАГ) используют понятие «киберпреступность» и смежные понятия с приставкой «кибер». Документы не содержат нормативных определений данных понятий, но в качестве базовых рекомендаций для разработки правовой сферы обеспечения кибербезопасности обозначена, в частности, «криминализация неправомерного использования компьютеров и компьютерных сетей»[7].

Документы Группы 7(8) / G7(8), в частности, Декларация G7 об ответственном поведении государств в киберпространстве (Лука, 2017 г.), Динарская декларация об инициативе Киберправа 2019 г., содержат понятия «высокотехнологичные преступления», «киберпреступность», «кибербезопасность», «киберзащита», объединенные общей формулировкой «вредоносное использование ИКТ», которое может создавать угрозу безопасности и стабильности киберпространства.[8]

---

[3] African Union Convention on Cyber Security and Personal Data Protection. 2014. URL: https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection (accessed 25.06.2021).

[4] The Economic Community of West African States (ECOWAS) Directive on Fighting Cyber Crime within ECOWAS. 2011 URL: https://issafrica.org/ctafrica/uploads/Directive%201:08:11%20on%20Fighting%20Cyber%20Crime%20within%20ECOWAS.pdf (accessed 25.06.2021).

[5] The Commonwealth Model law on computer and computer-related crime and electronic evidence. 2011 URL: https://thecommonwealth.org/sites/default/files/key_reform_pdfs/P15370_7_ROL_Model_Bill_Electronic_Evidence_0.pdf (accessed 25.06.2021)

[6] Southern African Development Community (SADC) Model Law on Computer Crime and Cybercrime. 2012. URL: https://www.itu.int/en/ITU/Cybersecurity/Documents/SADC%20Model%20Law%20Cybercrime.pdf (accessed 25.06.2021).

[7] OAS: Comprehensive Inter-American Strategy to Combat Threats to Cybersecurity: a multidimensional and multidisciplinary approach to creating a culture of cybersecurity. 2004. URL: http://www.oas.org/en/sms/cicte/documents/oas_ag/agres_2004_(xxxiv-o-04)_en.pdf (accessed 25.06.2021)

[8] G7 Declaration on responsible states behavior in cyberspace. 2017 URL: https://www.mofa.go.jp/files/000246367.pdf (accessed 25.06.2021); G7 Dinard Declaration on the Cyber Norm Initiative. 2019 URL: http://www.g7.utoronto.ca/foreign/190406-cyber.html (accessed 25.06.2021)

Термин «киберпреступность» получил более широкое распространение в зарубежной доктрине и соглашениях, принятых в европейском, американском, африканском регионах. Так, официально название Будапештской конвенции 2001 г. на языке оригинала звучит как Convention on Cybercrime. Во многих источниках (как нормативных, так и теоретических, а также при упоминании в средствах массовой информации) документ носит название Конвенции Совета Европы о борьбе с киберпреступностью. Российская Федерация не является участницей данной Конвенции, в связи с чем отсутствует официальный текст перевода на русский язык. Между тем Правовое управление Государственной Думы ФС РФ при переводе указанного документа трактует его название как «Конвенция о преступности в сфере компьютерной информации»[9], что, по мнению автора, можно расценивать не как неточность перевода, а скорее, как намеренное «приведение» международного документа в соответствие с принятой национальной концепцией в сфере обеспечения информационной безопасности.

Стоит отметить, что в российском законодательстве термин «киберпреступность» не находит своего закрепления. Для определения данного вида преступлений применяются понятия «преступления в сфере компьютерной информации», «информационные преступления», «преступления в сфере ИКТ (информационно-коммуникационных технологий)», что отражается не только в национальном законодательстве, но и в международных документах, разрабатываемых и реализуемых по инициативе и при участии Российской Федерации: Соглашении о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации 2001 г.[10]; Соглашении о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий 2018 г.[11]; Соглашении о сотрудничестве в области обеспечения международной информационной безопасности, принятом Шанхайской организацией сотрудничества в 2010 г.[12]; Проекте Конвенции Организации Объединенных Наций о сотрудничестве в сфере противодействия информационной преступности 2018 г. (инициатива РФ)[13].

3. Анализ доктринальных подходов к пониманию категории «киберпреступность» и смежных понятий

В научной литературе также отсутствует единообразие мнений относительно определения «новой формы преступности». Здесь можно обнаружить те же различия в подходах зарубежных и отечественных исследователей, что и в нормативно-правовых источниках. Так, представители зарубежной науки в большинстве своем оперируют термином «киберпреступность» и связанными с ним понятиями с ключевой приставкой «кибер». Следует отметить, что проблема «компьютерной преступности» стала объектом научных исследований в зарубежных странах с 70-х годов прошлого века. Возникновение данного криминального явления, расследование первых инцидентов компьютерных преступлений потребовали разработки соответствующей теоретической и нормативной базы. Соответственно, именно западные исследователи впервые предприняли попытки сформулировать понятие «компьютерная преступность». Данный термин был введен в оборот в научных кругах в начале 1960-х гг. исследователем Д.Б. Паркер [Parker

[9] Конвенция о преступности в сфере компьютерной информации 2001 г. – *Справочно-правовая система Гарант*. Доступ: https://base.garant.ru/4089723/ (дата обращения: 18.06.2021).

[10] «Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации» 2001 г. – *Справочно-правовая система КонсультантПлюс*. Доступ: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=INT&n=9210#045128599939795544 (дата обращения: 18.06.2021). Документ прекращает действие в отношениях между государствами – участниками Соглашения от 28.09.2018 с даты вступления в силу указанного Соглашения.

[11] Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий 2018 г. Доступ: http://cis.minsk.by/ (дата обращения: 12.06.2021)

[12] Соглашение между Правительствами государств – членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности 2019 г. – *Справочно-правовая система КонсультантПлюс*. Доступ: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=INT&n=51984#041486154092490657 (дата обращения: 18.06.2021).

[13] ООН: Резолюция, принятая Генеральной Ассамблеей ООН 5 декабря 2018 г. № 73/27 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». Доступ: https://undocs.org/ru/A/RES/73/27 (дата обращения 04.07.2021 г.).

1998:2– 5], которая впервые обозначила, что «электронно-вычислительная машина (ЭВМ) является как объектом преступления, так и орудием, используемым для получения политических или деловых преимуществ».

Этот подход был положен в основу многих более поздних исследований, в ходе которых, независимо от обоснования применимости того или иного термина (компьютерные преступления, преступления, относящиеся к компьютеру, электронные преступления, высокотехнологичные преступления, Интернет-преступления, киберпреступления), авторы исходят из двойственной природы данного рода деяний, которые так или иначе охватывают противоправные действия в киберпространстве, в частности, в рамках компьютерной сети. Несмотря на неоднократные попытки исследователей описать сущность явления киберпреступности и дать определение данного понятия, до сегодняшнего момента в зарубежной науке остается множество неопределенностей и дебатов относительно различных аспектов киберпреступности, включая типологию и истинную природу нового криминального явления. Одним из ключевых спорных положений является вопрос корреляции между «новой формой преступности» (киберпреступностью) и традиционной преступностью физического мира. Ряд исследователей полагает, что, хотя киберпреступность может рассматриваться в качестве новой специфической формы преступности, она сохраняет сущностные признаки традиционной преступности [Grabosky 2001: 243–249], [Yar 2005:407–427; Bosler, Berenblum 2019: 495–499; Ilievski 2016:30–47]. Среди аргументов приводится положение о том, что киберпреступники не более чем корректируют и совершенствуют традиционные способы преступных деяний преступлений, используя безграничные возможности киберпространства. Технологии, по мнению этих исследователей, – инструмент в руках пользователя, который может применять его как в позитивных, так и в преступных целях.

Представители другого направления настаивают на том, что сущностные признаки и специфические особенности самого киберпространства как особой среды, где совершаются эти преступления, а также возможности информационно-технических средств создают ключевые различия в природе киберпреступности и традиционной преступности [Furnell 2001:35–44; Cross, Shinder 2008:50–55; Choi, Lee 2017: 394–402; Bosler, Berenblum 2019: 495–499].

Рассмотрим некоторые из определений киберпреступности, формулируемые в рамках различных западных школ. «Киберпреступление – это противоправное действие, совершаемое посредством использования информационных или коммуникационных технологий либо для атаки на сеть, компьютерную систему, данные, веб-сайты, либо для содействия совершению других преступлений» [Goodman, Brenner 2002: 139–223]. Гордон и Форд [Gordon, Ford 2006: 13–20] определяют киберпреступление как любое преступление, для совершения которого были использованы компьютер, сеть или техническое оборудование. Роберт Мур [Moore 2011:45–50] обращает внимание на тот факт, что киберпреступление может быть определено как любое преступление, использующее компьютер и сеть, в то время как «компьютерное преступление» включает применение только компьютеров. Несмотря на крайнюю обобщенность подобных дефиниций, они отражают идею о необходимости разграничения понятий «киберпреступление» и «компьютерное преступление».

Интересна типология киберпреступлений, согласно которой выделяют три категории киберпреступлений: преступление в самом устройстве, преступление с использованием устройства и преступление против устройства [Wall 2007:60–75; Madriaza et al. 2018]. Данный подход к классификации и определению киберпреступлений полностью соотносится с рекомендациями экспертов ООН, сформулированными в рамках работы Десятого Конгресса ООН по предупреждению преступности и обращению с правонарушителями, согласно которым термин «киберпреступность» охватывает любое преступление, которое может совершаться с помощью компьютерной системы или сети, в рамках компьютерной системы или сети или против компьютерной системы или сети. Термин охватывает любое преступление, совершенное в электронной среде[14].

Отечественные ученые в большей степени используют терминологию, соответствующую официальному подходу, закрепленному в уголовном законодательстве РФ, где данный вид преступлений определен через родовой объект

[14] Десятый Конгресс ООН по предупреждению преступности и обращению с правонарушителями. 10–17 апреля 2000 г. Доступ: https://undocs.org/pdf?symbol=ru/A/CONF.187/15 (дата обращения: 12.07.2021).

как «преступления в сфере компьютерной информации».

Так А.В. Суслопаров под «информационными преступлениями» понимает «общественно-опасные противоправные деяния, причиняющие вред общественным отношениям по обеспечению информационной безопасности личности, общества и государства, способом совершения которых является информационное воздействие или (и) предметом которых является информация как особый нематериальный объект». При этом автор рассматривает информационные преступления в качестве самостоятельной правовой категории, которая включает компьютерные преступления, но не ограничивается ими, поскольку предметом информационных преступлений является любая социально-значимая информация, независимо от формы материального носителя (не только машинный носитель, но и бумажный)[15]. А.Н. Попов отмечает, что понятие «информационного преступления» охватывает не только действия, совершаемые с использованием современных технических средств, но и разнообразные формы психологического информационного воздействия, которое может осуществляться как с использованием современных ИКТ, так и через традиционные каналы СМИ[16]. Д.О. Крылов и А.В. Малюгина [Крылов, Малюгина 2017] отмечают, что при анализе различных правовых оценок противоправных действий в сфере информации (вне зависимости от ее формы – компьютерная, документированная и иная), становится очевидно, что законодатель в качестве основания для отнесения того или иного деяния к категории «информационных преступлений», выделяет информацию как главную охраняемую ценность, при этом механизм и характер совершаемых с информацией действий имеет второстепенное значение. Тем самым обосновывается применимость термина «информационные преступления» как наиболее полно отражающего сущность данной формы преступности через объект посягательства. Между тем, следует предположить, что «информационные преступления» – крайне широкая и неконкретная категория, которая охватывает значительный круг разнородных деяний в сфере информационного обмена.

Ряд отечественных исследователей при определении «новой формы преступности» обращается к так называемому техническому аспекту. Здесь используется термин «компьютерные преступления», что позволяет акцентировать внимание на компьютерах как на объектах и средствах совершения данных преступлений. При этом мнения ученых относительно возможности формулирования правовых категорий через технический аспект не совпадают. Ряд авторов (М.С. Гаджиев[17], А.И. Долгова [Организованный терроризм…2002:50–65], Т.Л. Тропина[18]) выступает против применения термина «компьютерная преступность», поскольку в науке уголовного права не применяется классификация преступлений, основанная на определении вида технического средства, с помощью которого они совершаются. В этом значении скорее стоит говорить не об отдельной специфической форме преступности в юридическом смысле, а о компьютерных аспектах традиционных преступлений (Ю.М. Батурин, А.М. Жодзишский [Батурин, Жодзишский 1991:14–27]). Другие авторы отстаивают самостоятельность категории «компьютерная преступность» для обозначения новой формы преступности (В.Б. Вехов [Вехов 1996:27–45], Н.А. Селиванов [Селиванов 1993: 36–40], А.А. Жмыхов[19], Т.М. Лопатина[20], Д.В. Добровольский[21]).

Между тем при анализе работ отечественных исследователей за последние пять лет отмечается тенденция выделения понятия «преступле-

[15] Суслопаров А.В. Компьютерные преступления как разновидность преступлений информационного характера. Дисс. … канд. юрид. наук. Владивосток. 2010. С. 32–56.

[16] Попов А.Н. *Преступления в сфере компьютерной информации. Учебное пособие.* Санкт-Петербург: Санкт-Петербургский юридический институт (филиал) Университета прокуратуры Российской Федерации, 2018. С. 4–11.

[17] Гаджиев М.С. Криминологический анализ преступности в сфере компьютерной информации (по материалам республики Дагестан). Дисс. … канд. юрид. наук. Махачкала. 2004. С. 12–20.

[18] Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы. Дисс. … канд. юрид. наук. Владивосток. 2005. С. 17–44.

[19] Жмыхов А. А. Компьютерная преступность за рубежом и ее предупреждение. Дисс. ... канд. юрид. наук. Москва, 2003. С. 14–37.

[20] Лопатина Т.М. Криминологические и уголовно-правовые основы противодействия компьютерной преступности. Дисс. … доктора. юрид. наук. Москва. 2004. С. 25–36.

[21] Добровольский Д. В. Актуальные проблемы борьбы с компьютерной преступностью: Уголовно-правовые и криминологические проблемы. Дисс. … канд. юрид. наук. Москва. 2006. С. 13–42.

ния в сфере компьютерной информации», что вполне соотносится с позицией российского законодателя, закрепленной в гл. 28 УК РФ «Преступления в сфере компьютерной информации». Отмечая излишнюю обобщенность и широту термина «компьютерные преступления», авторы обосновывают эффективность применения термина «преступления в сфере компьютерной информации», определяя их как «противоправное виновно-совершенное общественно-опасное деяние, наказуемое в уголовном порядке, посягающее на общественные отношения по безопасному производству, хранению, передаче, поиску, использованию, распространению или защите компьютерной информации, причинившее или создающее угрозу причинения вреда охраняемым законом права и интересам физических и (или) юридических лиц, общества, государства» [Петрова, Лобачев 2020:52–62].

Т.Л. Тропина в своей диссертации обосновывает применимость термина «киберпреступность», который рассматривается как более емкий и наиболее точно отражающий специфику «новой формы преступности», совершаемой в особо рода пространстве – киберпространстве. Представляется вполне обоснованным довод Т.Л. Тропиной, что термин «компьютерная преступность» следует рассматривать как более узкий, определяющий суть явления исключительно через преступления, совершенные с использованием компьютера. Между тем, стремительные темпы развития технологий делают неприменимым использование подобного узкого термина, поскольку в настоящее время уже само понятие «компьютер» становится размытым. Техническая составляющая «новой формы преступности» не сводится исключительно к применению компьютеров как технических средств. Компьютер выступает своего рода орудием, своеобразным физическим объектом воплощения виртуальной компьютерной системы, в которой хранится информация, которая и представляет интерес для преступного посягательства.

О.А. Бойко формулирует понятие «киберпреступность» крайне обобщенно, как «широкий спектр противоправных деяний, для совершения которых используются компьютерные технологии» [Бойко 2017:123–126].

С.И. Буз под «киберпреступлением» понимает любое преступление, совершенное с помощью информационных технологий, либо в информационном пространстве. При этом под информационными технологиями понимаются как технические средства (персональные компьютеры, ноутбуки, смартфоны), так и сама информация, и ее носители. Под информационным пространством подразумеваются информационно-телекоммуникационные сети (например, Интернет), компьютерные локальные сети и т. д. [Буз 2019:78–82].

Интересно, что в настоящий момент отечественные ученые высказывают мнение о «трансформации традиционной компьютерной преступности в новый вид высокотехнологичной преступности – технотронную преступность, представляющую собой систему взаимосвязанных и образующих единую целостность общественно опасных деяний, совершенных с использованием компьютерных, информационно-телекоммуникационных, когнитивных, космических, робототехнических и иных высоких технологий [Евдокимов 2020:26–33]. Данная концепция представляется вполне обоснованной в силу стремительных темпов развития информационных технологий, разработки новейших средств и систем искусственного интеллекта, Интернета вещей, облачных данных, проникающих в самые различные сферы человеческой деятельности, что, безусловно, не может не отразиться на характере преступных деяний, совершаемых в данной специфической среде.

4. Заключение

Таким образом, несмотря на отсутствие согласованной терминологии и подходов к определению и нормативному закреплению «новой формы преступности», следует исходить из базового положения, что данный вид преступности включает две категории преступлений:

1. В первом случае информационно-коммуникационные технологии (ИКТ) являются непосредственной целью преступления (в качестве объекта преступного посягательства выступает «Триада КЦД» – конфиденциальность, целостность, доступность как неотъемлемые свойства информации.

2. Во втором случае ИКТ являются неотъемлемой частью способа совершения преступления (эта группа преступлений охватывает традиционные общеуголовные составы преступлений, совершению которых тем или иным образом способствуют ИКТ, включая сеть Интернет).

В связи с выявленной крайней несогласованностью в подходах представляется, что для раз-

работки авторского определения «новой формы преступности» необходимо комплексное исследование, основанное на детальном анализе широкого перечня доктринальных источников, которое будет реализовано автором в последующих публикациях. Тем не менее, на основе проведенного анализа автор приходит к выводу о необходимости определения и вычленения той исходной детерминанты, которая отражает сущностные особенности и специфические свойства новой формы преступности, отличающие ее от других преступлений. При определении такой детерминанты необходимо учесть, что данные преступления совершаются в особо рода сложноорганизованной системе, осуществляющей получение, хранение, обработку, преобразование и передачу информации в качестве базового ресурса. То есть, разрабатываемое определение должно отражать два элемента:

1) указание на информацию, в качестве нематериального ресурса и объекта преступного посягательства;

2) указание на особого рода систему, в которой реализуются процессы обработки, хранения и передачи информации (в качестве такой системы выступает компьютерная сеть, Интернет и другие автоматизированные системы управления).

С учетом изложенного, автор приходит к выводу, что термин «киберпреступность» представляется наиболее обоснованным, поскольку приставка «кибер» содержит указание на связь с наукой кибернетикой в ее значении, предложенном и обоснованном в теории Норберта Винера [Винер 2019:25–27].

В заключение следует отметить, что задача совершенствования и унификации базовых категорий в сфере борьбы с киберпреступностью представляет первостепенный интерес не только с точки зрения теории, но главным образом для разработки и реализации эффективного международно-правового механизма противодействия данному виду преступности. Безусловно, для решения этой задачи требуется комплексный подход, в основу которого должны быть положены доктринальные обоснования и исследования специалистов не только юридической науки, но и представителей технических наук. Это обстоятельство часто упускается из виду при разработке правовых норм, между тем, принимая во внимание специфический характер объекта, предмета и виртуальной среды совершения данных преступлений, любая правовая норма должна быть сформулирована и соотнесена с объективной возможностью ее практической реализации с учетом технических особенностей.

Список литературы

1. Батурин Ю.М., Жодзишский А.М. 1991. *Компьютерная преступность и компьютерная безопасность.* М.: Юридическая литература.160 с.
2. Бойко О.А. 2017. Понятие «киберпреступность»: основные дефиниции. – *Уголовная юстиция: законодательство, теория и практика. Сборник материалов VIII Республиканской научно-практической конференции студентов, магистрантов и аспирантов.* Брест: БрГУ имени А.С. Пушкина. С. 123–126.
3. Буз С. И. 2019. Киберпреступления: понятие, сущность и общая характеристика. – *Юрист-Правоведъ.* №4. С.78–82.
4. Вехов В. Б. 1996. *Компьютерные преступления: Способы совершения, методики расследования.* М.: Право и закон. 182 с.
5. *Организованный терроризм и организованная преступность.* Отв. ред. А.И. Долгова. 2002. М.: Российская криминологическая ассоциация. 128 с.
6. Евдокимов, К. Н. 2020. Самодетерминация компьютерной преступности в условиях ее трансформации в технотронную преступность. – *Правовые средства обеспечения национальной безопасности Российской Федерации: история и современность. Материалы международной научно-практической конференции.* Отв. редактор Е.М. Якимова. Иркутск: Байкальский государственный университет. С. 26–33.
7. Крылов Д.О., Малюгина А.В. 2017. К вопросу о терминологии в сфере киберпреступности (на материале английского языка). – *Международный студенческий научный вестник.* № 1. Доступ: https://eduherald.ru/ru/article/view?id=16836 (дата обращения: 15.05.2021).
8. Винер Н. 2019. *Кибернетика и общество.* М.: Издательство АСТ. 228 с.
9. Петрова И.А., Лобачев И.А. 2020. Преступления в сфере компьютерной (цифровой) информации: дискуссионные вопросы определения понятия, объекта уголовно-правовой охраны и предмета посягательств. – *Журнал прикладных исследований.* №1. С.52–62.
10. Скляров С.В., Евдокимов К.Н. 2016. Современные подходы к определению понятия, структуры и сущности компьютерной преступности в Российской Федерации. – *Криминологический журнал Байкальского государственного университета экономики и права.* Т. 10. №2. С. 322–330. DOI: 10.17150/1996-7756.2016.10(2).322-330
11. Селиванов Н. А. 1993. Проблемы борьбы с компьютерной преступностью. – *Законность.* № 8. С. 36–40.
12. Bosler A.M., Berenblum T. 2019. Introduction: new directions in cybercrime research. – *Journal of Crime and Justice.* Vol. 42. Issue 5. P. 495–499. DOI: https://doi.org/10.1080/0735648X.2019.1692426
13. Choi K.S., Lee J.R. 2017. Theoretical analysis of cyber-interpersonal violence victimization and offending using cyber-routine activities theory. – *Computers in Human Be-*

havior. Vol. 73 P. 394–402. DOI: 10.1016/j.chb.2017.03.061
14. DiMasi J.A., Hansen R.W., Grabowski H.G. 2003. The Price of Innovation: New Estimates of Drug Development Costs. – *Journal of Health Economics.* Vol. 22. Issue 2. P. 151–185. DOI:10.1016/S0167-6296(02)00126-1
15. Furnell S.M. 2001. Categorising cybercrime and cybercriminals: The problem and potential approaches. – *Journal of Information Warfare.* Vol. 1. Issue 2. P. 35–44.
16. Goodman M.D., Brenner S.W. 2002. The Emerging Consensus on Criminal Conduct in Cyberspace. – *International Journal of Law and Information Technology.* Vol. 10. Issue 2. P. 139–223. DOI: 10.1093/ijlit/10.2.139
17. Gordon S., Ford R. 2006. On the Definition and Classification of Cybercrime. – *Journal in Computer Virology.* Vol. 2. Issue 1. P. 139–223. DOI: 10.1007/s11416-006-0015-z
18. Grabosky P.N. 2001.Virtual Criminality: Old Wine in New Bottles. – *Social & Legal Studies.* Vol. 10. Issue 2. P. 243-249. DOI: https://doi.org/10.1177/a017405
19. Ilievski A. 2016. An Explanation of the Cybercrime Victimisation: Self-Control and Lifestyle/ Routine Activity Theory. – *Innovative Issues and Approaches in Social Sciences.* Vol. 9. Issue 1. P. 30–47. DOI: 10.12959/issn.1855-0541.IIASS-2016- № 1-art02
20. Madriaza P. [et al.]. 2018. *6th International Report on Crime Prevention and Community Safety: Preventing Cybercrime.* Montréal: International Centre for Prevention of Crime. 161 p.
21. Moore R. 2014. *Cybercrime: Investigating High-Technology Computer Crime.* New York: Routledge Publ. 312 p. DOI: https://doi.org/10.4324/9781315721767
22. Parker D.B. 1983. *Fighting Computer Crime: A New Framework for Protecting Information.* New York: John Wiley & Sons, Inc. 512 p.
23. Parker D.B. 1989. *Computer crime Criminal Justice Resource Manual.* Cambridge, Mass.; Department of Justice. 223 p.
24. Shinder D.L. Cross M. 2008. *Scene of the Cybercrime.* 2nd ed. Burlington, MA : Syngress Pub. 732 p.
25. Wall D. 2007. *Cybercrime: The Transphormation of Crime in the Information Age.* Cambridge: Polity Press. 288 p.
26. Yar M. 2005. The Novelty of «Cybercrime»: an Assessment in Light of Routine Activity Theory. – *European Journal of Criminology.* Vol. 2. Issue 4. P. 407–427. DOI: https://doi.org/10.1177/147737080556056

References

1. Baturin Yu.M., Zhodzishskii A.M. *Komp'yuternaya prestupnost' i komp'yuternaya bezopasnost'* [Computer Crime and Computer Security]. Moscow: Yuridicheskaya literature Publ. 1991. 160 p. (In Russ.)
2. Boiko O.A. Ponyatie "kiberprestupnost'": osnovnye definitsii [The Concept of Cybercrime: the main definitions]. – *Ugolovnaya yustitsiya: zakonodatel'stvo, teoriya i praktika. Sbornik materialov VIII Respublikanskoi nauchno-prakticheskoi konferentsii studentov, magistrantov i aspirantov* [Criminal Justice: legislation, theory and practice. Collection of materials of the VIII Republican Scientific and Practical Conference of students, undergraduates and postgraduates]. Brest: BrGU imeni A.S. Pushkina. 2017. P. 123–126. (In Russ.)
3. Bosler A.M., Berenblum T. Introduction: new directions in cybercrime research. – *Journal of Crime and Justice.* 2019. Vol. 42. Issue 5. P. 495–499. DOI: https://doi.org/10.1080/0735648X.2019.1692426
4. Buz S. I. Kiberprestupleniya: ponyatie, sushchnost' i obshchaya kharakteristika [Cyber crimes: concept, essence and general characteristic]. – *Yurist-Pravoved.* 2019. No. 4. P.78–82. (In Russ.)
5. Choi K.S., Lee J.R. Theoretical analysis of cyber-interpersonal violence victimization and offending using cyber-routine activities theory. – *Computers in Human Behavior.* 2017. Vol. 73 P. 394–402. DOI: 10.1016/j.chb.2017.03.061
6. DiMasi J.A., Hansen R.W., Grabowski H.G. The Price of Innovation: New Estimates of Drug Development Costs. – *Journal of Health Economics.* 2003. Vol. 22. Issue 2. P. 151–185. DOI:10.1016/S0167-6296(02)00126-1
7. Evdokimov, K. N. Samodeterminatsiya komp'yuternoi prestupnosti v usloviyakh ee transformatsii v tekhnotronnuyu prestupnost' [Self-determination of Computer Crime in the Conditions of its Transformation into Technotronic Vrime]. – *Pravovye sredstva obespecheniya natsional'noi bezopasnosti Rossiiskoi Federatsii: istoriya i sovremennost'. Materialy mezhdunarodnoi nauchno-prakticheskoi konferentsii.* Otv. redaktor E.M. Yakimova [Legal Means of Ensuring the National Security of the Russian Federation: history and modernity. Materials of the international scientific and practical conference. Ed. by E.M. Yakimova]. Irkutsk: Baikal'skii gosudarstvennyi universitet Publ. 2020. P. 26–33. (In Russ.)
8. Furnell S.M. Categorising cybercrime and cybercriminals: The problem and potential approaches. – *Journal of Information Warfare.* 2001. Vol. 1. Issue 2. P. 35–44.
9. Goodman M.D., Brenner S.W. The Emerging Consensus on Criminal Conduct in Cyberspace. – *International Journal of Law and Information Technology.* 2002. Vol. 10. Issue 2. P. 139–223. DOI: 10.1093/ijlit/10.2.139
10. Gordon S., Ford R. On the Definition and Classification of Cybercrime. – *Journal in Computer Virology.* 2006. Vol. 2. Issue 1. P. 139–223. DOI: 10.1007/s11416-006-0015-z
11. Grabosky P.N. Virtual Criminality: Old Wine in New Bottles. – *Social & Legal Studies.* 2001.Vol. 10. Issue 2. P. 243-249. DOI: https://doi.org/10.1177/a017405
12. Ilievski A. An Explanation of the Cybercrime Victimisation: Self-Control and Lifestyle/ Routine Activity Theory. – *Innovative Issues and Approaches in Social Sciences.* 2016. Vol. 9. Issue 1. P. 30–47. DOI: 10.12959/issn.1855-0541. IIASS-2016- № 1-art02
13. Krylov D.O., Malyugina A.V. K voprosu o terminologii v sfere kiberprestupnosti (na materiale angliiskogo yazyka) [On the Issue of Terminology in the Field of Cybercrime (based on the material of the English language)]. – *Mezhdunarodnyi studencheskii nauchnyi vestnik.* 2017. No. 1. (In Russ.). URL: https://eduherald.ru/ru/article/view?id=16836 (accessed 15.05.2021)
14. Madriaza P. [et al.]. *6th International Report on Crime Prevention and Community Safety: Preventing Cybercrime.* Montréal: International Centre for Prevention of Crime. 2018. 161 p.
15. Moore R. *Cybercrime: Investigating High-Technology Computer Crime.* New York: Routledge Publ. 2014. 312 p. DOI: https://doi.org/10.4324/9781315721767
16. *Organizovannyi terrorizm i organizovannaya prestupnost'.* Otv. red. A.I. Dolgova [Organized Terrorism and Organized Crime. Ed. by A.I. Dolgova]. Moscow: Rossiiskaya kriminologicheskaya assotsiatsiya Publ. 2002. 128 p. (In Russ.)
17. Parker D.B. *Computer crime Criminal Justice Resource Manual.* Cambridge, Mass.; Department of Justice. 1989. 223 p.

18. Parker D.B. *Fighting Computer Crime: A New Framework for Protecting Information*. New York: John Wiley & Sons, Inc. 1983. 512 p.
19. Petrova I.A., Lobachev I.A. Prestupleniya v sfere komp'yuternoi (tsifrovoi) informatsii: diskussionnye voprosy opredeleniya ponyatiya, ob"ekta ugolovno-pravovoi okhrany i predmeta posyagatel'stv [Crimes in Sphere of Computer (Digital) Information: debatable issues of definition of the concept, object of criminal legal protection and subject of encroachments]. – *Zhurnal prikladnykh issledovanii*. 2020. No. 1. P. 52-62. (In Russ.)
20. Selivanov N. A. Problemy bor'by s komp'yuternoi prestupnost'yu [Problems of Combating Computer Crimes]. – *Zakonnost'*. 1993. No. 8. P. 36-40. (In Russ.)
21. Shinder D.L. Cross M. *Scene of the Cybercrime*. 2nd ed. Burlington, MA : Syngress Pub. 2008. 732 p.
22. Sklyarov S.V., Evdokimov K.N. Sovremennye podkhody k opredeleniyu ponyatiya, struktury i sushchnosti komp'yuternoi prestupnosti v Rossiiskoi Federatsii [Modern Approaches to the Concept, Structure and Nature of Computer Crime in the Russian Federation]. – *Criminology Journal of Baikal National University of Economics and Law*. 2016. Vol. 10. No. 2. P. 322-330. (In Russ.). DOI: 10.17150/1996-7756.2016.10(2).322–330
23. Vekhov V. B. *Komp'yuternye prestupleniya: Sposoby sovershеniya, metodiki rassledovaniya* [Computer crimes: methods of commission, methods of investigation]. Moscow: Pravo i zakon Publ. 1996. 182 p. (In Russ.)
24. Wall D. *Cybercrime: The Transphormation of Crime in the Information Age*. Cambridge: Polity Press. 2007. 288 p.
25. Wiener N. The Human Use of Human Beings (Russ. ed.: Wiener N. *Kibernetika i obshchestvo*. Moscow: Izdatel'stvo AST Publ. 228 p.)
26. Yar M. The Novelty of «Cybercrime»: an Assessment in Light of Routine Activity Theory. – *European Journal of Criminology*. 2005. Vol. 2. Issue 4. P. 407-427. DOI: https://doi.org/10.1177/147737080556056

Информация об авторе

Ляйсян Маратовна Старкова,
ассистент кафедры международного права,
Астраханский государственный университет

414056, Российская Федерация, Астрахань, ул. Татищева, д. 20а

5leska5@mail.ru
ORCID: 0000-0002-4411-6510

About the Author

Lyasyan M. Starkova,
Assistant at the Department of International Law,
Astrakhan State University

20 A, Tatishchev street, Astrakhan, Russian Federation, 414056

5leska5@mail.ru
ORCID: 0000-0002-4411-6510