

УДК 343.9

DOI 10.33184/vest-law-bsu-2021.11.8

Е. В. Сандальникова

**ТЕОРЕТИКО-ПРАВОВАЯ ИДЕНТИФИКАЦИЯ
КИБЕРПРЕСТУПНОСТИ В СИСТЕМЕ РОССИЙСКОГО ПРАВА
И СИСТЕМЕ РОССИЙСКОГО ЗАКОНОДАТЕЛЬСТВА**

Дата поступления 21 сентября 2021 г.

В статье обосновывается целесообразность теоретико-правовой идентификации киберпреступности в системе российского права и системе российского законодательства. В связи с этим поднимается вопрос более общего характера: об адаптации новой категории в теории права, критериях и основаниях ее включения в теоретико-категориальный аппарат теории государства и права. В результате проведенного исследования делается вывод о необходимости нормативной детализации понятия киберпреступности, отграничения ее от смежных правовых категорий, определяются место и роль новой категории киберпреступности в понятийно-категориальном аппарате российского права и законодательства.

Ключевые слова и фразы: теория государства и права; понятийно-категориальный аппарат; киберпреступность; цифровая преступность; ответственность за киберпреступления.

E. V. Sandalnikova

**LEGAL AND THEORETICAL IDENTIFICATION OF CYBERCRIME
IN THE RUSSIAN LAW SYSTEM
AND IN THE RUSSIAN LEGISLATION SYSTEM**

The article justifies the usefulness of a theoretical and legal identification of cybercrime in the system of Russian law and the system of Russian legislation. This raises the question of a more general nature: the adaptation of the new category in the theory of law, the criteria and the grounds for its inclusion in the theoretical-categorical apparatus of State and law. The study concludes that there is a need for normative detail on the concept of cybercrime, distinguishing it from related legal categories, and defining the place and role of the new category of cybercrime in of cybercrime in its conceptual and categorical apparatus.

Keywords and phrases: theory of state and law; conceptual and categorical apparatus; cybercrime; digital crime; responsibility for cybercrime.

Правовая наука в целом и общая теория государства и права в частности испытывают потребность в решении вопроса о критериях включения той или иной новой категории в число юридических и теоретико-правовых. На примере теоретико-правовой идентификации киберпреступности постараемся в этой статье данную проблематику поставить как вопрос для обсуждения.

Киберпреступность в настоящее время вышла далеко за рамки национальных проблем и занимает свое место среди актуальных проблем международного, транснационального уровня. По данным исследователей, в современный период пользователями сети Интернет в мире являются более 4,5 млрд человек, что составляет более половины населения всего земного шара¹. Естественно, что вместе с ростом пользователей сети Интернет растет интерес криминального мира к ее использованию для извлечения прибыли и иных результатов преступной деятельности.

О том, что в настоящее время киберпреступность «прогрессирует», свидетельствуют статистические данные Министерства внутренних дел РФ, согласно которым в 2020 г. на 1,6 % был отмечен рост всех зарегистрированных преступлений по причине того, что преступления все чаще совершаются с применением IT-технологий. Непосредственно криминальных деяний, совершенных в информационной сфере, с января по май 2021 г. зарегистрировано на 25,7 % больше, чем в этот же период 2020 г., в том числе на 48,4 % больше преступлений совершено в Сети и при помощи сети Интернет и на 40,1 % больше преступлений с использованием компьютерной техники. Если с января по май 2020 г. удельный вес преступлений в сфере высоких технологий составлял 21,7 %, то за аналогичный период этого года – уже 26,8 %². При этом в России, по данным Генеральной прокуратуры, раскрывается меньше 25 % киберпреступлений, и это следует трактовать крайне негативно, учитывая тот факт, что количество таких преступлений за последние пять лет увеличилось в 25 раз³.

¹ Сергеева Ю. Вся статистика интернета на 2020 год – цифры и тренды в мире и в России [Электронный ресурс]. URL: <https://www.web-canape.ru/business/internet-2020-globalnaya-statistika-i-trendy/> (дата обращения: 18.09.2021).

² Краткая характеристика состояния преступности в Российской Федерации за январь – май 2021 г. [Электронный ресурс] // Офиц. сайт МВД России. URL: <https://xn--b1aew.xn--p1ai/reports/item/24742236> (дата обращения: 20.09.2021).

³ Егоров И. Генпрокурор рассказал о росте числа киберпреступлений в России [Электронный ресурс] // Российская газета. 2020. 17 июля. URL: <https://rg.ru/2020/07/17/genprokuror-rasskazal-o-roste-chisla-kiberprestuplenij-v-rossii-v-25-raz.html> (дата обращения: 20.09.2021).

В то же время, несмотря на остроту проблемы противодействия киберпреступности, в современной международной и российской практике имеются противоречия и трудности в выработке единых подходов к определению самого понятия киберпреступности.

Разработка государственной политики в области противодействия киберпреступности в современный период активно продвигается, хотя налицо немало проблем, связанных с реализацией мероприятий, предусмотренных в рамках ее продвижения. Это проблемы обеспечения информационной безопасности различных категорий граждан, организаций, органов власти в сети Интернет, а также проблемы обеспечения защиты персональных данных и противодействия преступности в области цифровой экономики.

Сложность, которую осознает власть, состоит в том, что информация – ресурс, объект, имеющий свою специфику и в силу этого отличающийся особенностями защиты при ее распространении, обеспечении доступа к ней или, наоборот, ограничении доступа к ней. Как верно пишет М.А. Маслиенко, концентрация информационных ресурсов для хранения в электронных системах еще более усугубляет проблемы противодействия киберпреступности, соответственно, цифровизация требует повышения оптимизации механизма борьбы с противоправными действиями в информационной сфере [1, с. 29].

Механизм государственной политики России по противодействию киберпреступности, полагаем, безусловно, строится на основе системы официальных документов, в которых определены основные положения обеспечения информационной безопасности. Так, в Доктрине информационной безопасности России¹, принятой, в 2016 г. и действующей в современный период без изменений и принятия новых редакций, содержатся указания:

– на национальные интересы в информационной среде (основной из них – обеспечение конституционных прав и свобод граждан, гарантирование частной неприкосновенности и т. д.);

– на информационные угрозы и состояние информационной безопасности (основной угрозой называется наращивание зарубежными странами давления на информационную инфраструктуру России);

– на стратегические цели и тактические задачи обеспечения информационной безопасности (включая задачи по пресечению, противодействию, профилактике противоправных действий в области информационных технологий, в том числе криминальных);

– на организационные условия обеспечения информационной безопасности (они строятся на законотворческих, правоприменительных, право-

¹ Об утверждении Доктрины информационной безопасности РФ : указ Президента РФ от 05.12.2016 № 646 // Собрание законодательства РФ. 2016. № 50, ст. 7074.

охранительных, контрольных и судебных основах организации различных форм деятельности уполномоченных органов власти, а также коммерческих, некоммерческих организаций, граждан в сфере противодействия противоправным действиям в информационной среде).

Однако перечня мероприятий, планируемых к реализации в рамках исследуемого механизма государственной политики противодействия киберпреступности, в Доктрине информационной безопасности России не содержится. При этом со стороны уполномоченных органов власти, в частности МВД России, в последнее время делаются заявления о необходимости внедрения в ближайшее время новейших методов борьбы с киберпреступностью и создания специального органа государственной власти – киберполиции¹.

По словам министра внутренних дел России В.А. Колокольцева, создание киберполиции еще только планируется, так как для этого нужно подготовить документационное сопровождение, переквалифицировать или существенно изменить квалификацию сотрудников, приобрести и освоить новую современную технику отслеживания преступных деяний в сети Интернет. Однако необходимо ускориться, поскольку в период распространения коронавирусной инфекции и принятия государством мер по минимизации рисков от ее распространения и одновременной цифровизации российской экономики значительно увеличилось число преступлений, совершаемых с использованием информационных ресурсов, за счет повышения криминальными субъектами уровня знаний из сети Интернет. Планируется, что в МВД России будут сформированы специальные управления по борьбе с киберпреступлениями, но без значительного расширения штатной численности министерства. Хотя при этом запланировано увеличение штатного состава Бюро специальных технических мероприятий МВД России, расширение его представительства во всех субъектах Российской Федерации и значительное расширение финансирования на противодействие киберпреступности².

Совершенствование существующего механизма реализации государственной политики в сфере противодействия киберпреступности, считаем, должно осуществляться путем:

– повышения общей правовой грамотности населения при получении информации, информационных услуг в сети Интернет и его взаимодействия

¹ Петров И. В структуре МВД создается киберполиция [Электронный ресурс] // Российская газета. 2020. 18 дек. URL: <https://rg.ru/2020/12/18/v-strukture-mvd-sozdaetsia-kiberpoliciia.html> (дата обращения: 17.09.2021).

² Дело в шифре: траты на информбезопасность в России увеличат в восемь раз [Электронный ресурс] // Известия. 2020. 2 окт. URL: <https://iz.ru/1068209/anna-ustanova/delo-v-shifre-traty-na-informbezopasnost-v-rossii-uvelichat-v-vosem-raz> (дата обращения: 18.09.2021).

с правоохранительными органами, даже при незначительном ущербе, по выявлению и раскрытию киберпреступлений;

- создания на постоянной основе специальных мониторинговых центров по пресечению кибератак;

- укрепления правовой базы, определяющей меры противодействия киберпреступности;

- внедрения в России международных стандартов противодействия киберпреступности (в том числе стандартов о присвоении индикатора компроментации киберпреступника);

- разработки и внедрения национальных стандартов защиты отраслей цифровой экономики;

- повышения уровня использования новейшего программного оборудования, специально создаваемого в современный период для пресечения кибератак;

- повышения квалификации сотрудников правоохранительных органов, осуществляющих противодействие киберпреступности, за счет повышения уровня их специальных знаний в области IT-технологий, получения зарубежного опыта выявления и расследования киберпреступлений;

- разработки актуальных методических рекомендаций по противодействию (выявлению, раскрытию, расследованию) киберпреступлениям, которые были бы подготовлены с учетом международных стандартов в этой области, складывающейся за рубежом и у нас в стране судебно-следственной практики, меняющейся криминогенной обстановки в сфере компьютерной информации и способов, механизмов совершения киберпреступлений;

- сплочения институтов гражданского общества, коммерческих организаций, ведущих специалистов в IT-сфере и правоохранительных органов в сотрудничестве по выявлению и раскрытию криминальных действий в данной сфере.

В то же время разработка понятийно-категориального аппарата о киберпреступности необходима в части определения ее понятия, отличий от смежных правовых категорий и выявления особенностей построения системы правового регулирования противодействия киберпреступности и, главное, если говорить в аспекте нашего исследования, ее теоретико-правовой идентификации как категории права, занимающей свое место в системе российского права.

Термин «киберпреступность», и в этом мы согласны с мнением В.Н. Цимбал и С.Г. Ключева, до настоящего времени не получил единообразного толкования как в международных документах, так и в российском законодательстве [2, с. 129], хотя в 2000 г. по итогам работы сессии X Конгресса ООН по предупреждению преступности и уголовному правосудию было

сформулировано его определение как любого преступного деяния в электронной среде, а в 2005 г. в рамках XI Конгресса ООН по предупреждению преступности и уголовному правосудию оно было сформулировано по-иному: все преступления с использованием компьютеров [3, с. 19].

Причиной того, что нормативного определения киберпреступности до сих пор нет в национальных системах законодательства, исследователи называют юрисдикционную дилемму, поскольку в разных странах и в их системах законодательства понятие киберпреступности определяется по-разному [3, с. 18]. К тому же нет точных данных о ежегодно совершаемых киберпреступлениях как новых видов преступлений, нет четкого законодательного определения, в том числе и в России, понятий «цифровая преступность» и «киберпреступность», нет полного и признаваемого единодушно всем научным сообществом научного обоснования этих понятий.

Отметим, что и в правовой науке по этому вопросу сложилась такая же ситуация. Причем подходы к определению понятия «киберпреступность» могут использоваться (впрочем, как и к другим правовым понятиям, например, юридической ответственности) разные: культурологический, социологический, лингвистический, идеологический, экономический, политический, криминалистический и др., как могут использоваться и разные подходы к отграничению понятия «киберпреступность» от схожих понятий (информационная преступность, преступность высоких технологий, компьютерная преступность, цифровая преступность и др.), классификации киберпреступности, пониманию причин и условий ее появления и распространения, решению правоприменительных проблем, возникающих при противодействии и предупреждении киберпреступлений, их выявлении, расследовании и раскрытии. К тому же нужно учитывать, что разнообразие преступлений в киберпространстве ежегодно только возрастает, на что было обращено особое внимание на XIV Конгрессе ООН по предупреждению преступности и уголовному правосудию, состоявшемся в 2000 г.¹ Соответственно, актуальным представляется сначала определение понятия киберпреступности, а затем установление ее видов, инструментов, инфраструктуры, современного состояния.

Для того чтобы определить понятие киберпреступности, учитывая, что его нет не только в правовой науке, необходимо выявить ее признаки, установить соотношение со смежными правовыми категориями и только затем определить ее место как категории права в системе российского права.

Так, Т.Л. Тропина определяет понятие киберпреступности через совокупность преступлений, которые совершаются в киберпространстве с приме-

¹ Руководство для дискуссий. XIV Конгресс ООН по предупреждению преступности и уголовному правосудию (Киото, 20–27 апреля 2000 г.) [Электронный ресурс]. URL: <https://docviewer.yandex.ru/view/327544614/?page=1&> (дата обращения: 14.08.2021).

нением компьютерных систем или сетей, разнообразных средств, обеспечивающих доступ в киберпространство, но против них самих, а также против компьютерных данных [4, с. 8]. Аналогичное определение она дала совместно с В.А. Номоконовым, акцентировав внимание на любых проявлениях преступной деятельности в киберпространстве посредством компьютерных систем или сетей, других средств, применяемых в этом пространстве и направленных против них самих же, а также против компьютерных данных [5, с. 45].

Один из руководителей «Лаборатории Касперского» и сотрудник Московского университета МВД России И.Г. Чекунов аргументирует свое мнение о понимании киберпреступлений (отметим, что в его исследовании понятие киберпреступности не употребляется) тем, что эти преступные деяния для понимания их таковыми обязательно должны совершаться в сети Интернет или с ее использованием, а мобильные средства связи, компьютеры при этом выступают орудиями или предметами их осуществления [6, с. 182].

По мнению Т.В. Пинкевич и Е.Н. Рахмановой, понятие «киберпреступность» уже понятия «цифровая преступность» по содержанию. Ученые трактуют цифровую преступность как противоправное и одновременно социальное явление, которое включает в себя целую совокупность преступлений в сфере цифровых технологий или с использованием (незаконным завладением, незаконным предложением, незаконным распространением информации в виртуальной среде, информационно-телекоммуникационных сетях) таких технологий [7, с. 193].

Схожими по содержанию с понятием «киберпреступность» можно назвать не только понятие «цифровая преступность», но и понятия «информационная преступность», «преступность высоких технологий», «компьютерная преступность». Определим их, чтобы понять, как соотносятся они по объему своего содержания, можно ли их считать синонимами.

Помимо указанных понятий в правовой науке используются и иные понятия в исследуемой сфере. Например, Н.В. Летёлкин использует понятие «преступления, совершаемые с использованием информационно-телекоммуникационных сетей» и включает в его смысл все преступные деяния, совершаемые в области охраны правомерного пользования информационно-телекоммуникационными сетями при использовании технологических систем [8, с. 8].

Согласимся с мнением Т.В. Пинкевич о том, что после VIII Конгресса ООН по предупреждению преступности и обращению с правонарушителями 1990 г., а также по результатам исследований Стэнфордского исследовательского института, который впервые в своем докладе использовал термин «компьютерная преступность», а позже по результатам проводимых исследований сущности компьютеров как субъектов, объектов, инструментов пре-

ступлений появилось узкое и широкое понимание киберпреступности. Узкое заключается в том, что всякое незаконное поведение, посягающее на безопасность компьютерных систем и данных, в форме электронных операций можно считать киберпреступностью. Широкое понимание основано на отнесении к киберпреступности любого противозаконного поведения, которое осуществлено с использованием или посредством компьютерных систем, в том числе незаконное распространение информации через сеть Интернет или с использованием компьютерной системы [3, с. 19].

Не только в специальной литературе, но и в международных документах можно найти определения киберпреступности и на их основе определить место этой категории в системе российского законодательства.

С 1992 г., когда впервые Организация экономического сотрудничества и развития (ОЭСР) издала Директиву по вопросам безопасности информационных систем¹, для обозначения преступности в информационной среде использовались разные термины, а затем в международных актах активно стал употребляться именно термин «киберпреступность», следуя выводам анализа Директив ОЭСР², Резолюций ООН (например, Резолюции ООН A/RES/53/70³). Хотя еще недавно, как обращалось внимание в вопроснике Всестороннего исследования проблем киберпреступности⁴ 2013 г., проведенного ООН, данное понятие употреблялось менее чем в 5 % принятых на тот момент 200 актов законодательства о преступности в информационной среде. Во Всестороннем исследовании отмечается, что можно дать много определений киберпреступлений, их содержание будет зависеть от целей употребления этого понятия. Однако в его основу может быть положен такой круг преступлений, совершение которых направлено против конфиденциальности, доступности, целостности компьютерных систем, программ, данных.

X Конгресс ООН по предупреждению преступности рекомендовал понимать под киберпреступностью любое преступление, которое совершается при помощи, в рамках или против компьютерной сети или системы и в

¹ Обзор Директивы ОЭСР по проблеме безопасности информационных систем и сетей: формирование культуры и обеспечение безопасности (2003) [Электронный ресурс]. URL: <https://docviewer.yandex.ru/view/327544614> (дата обращения: 14.08.2021).

² Директивы ОЭСР [Электронный ресурс]. URL: <https://www.oecd.org/sti/ieconomy/15582276.pdf> (дата обращения: 18.09.2021).

³ Резолюция ООН A/RES/53/70 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» от 04.01.1999 [Электронный ресурс]. URL: <https://www.ifap.ru/ofdocs/un/5753.pdf> (дата обращения: 17.09.2021).

⁴ Всестороннее исследование проблем преступности (Проект УНП ООН, Нью-Йорк, Вена, февраль 2013 г.) [Электронный ресурс]. URL: <https://docviewer.yandex.ru/view/327544614> (дата обращения: 14.08.2021).

принципе каждое преступление, совершаемое в электронной среде (то есть использующей все каналы связи по передаче данных посредством телекоммуникаций или компьютеров)¹. Тогда же было сформулировано узкое определение киберпреступности как противозаконного поведения, посягающего на безопасность компьютерных систем, их баз данных в форме электронных операций.

Широкое определение киберпреступности было сформулировано по итогам XI Конгресса ООН, проведенного в 2005 г.² Оно заключалось в том, что киберпреступлением следует считать преступление, совершенное с использованием компьютера, независимо от того, направлено ли оно на компьютерную сферу и технологии, или применение цифровых технологий, или использование компьютера в целом как инструмента, орудия преступления.

Стоит отметить, что Конвенция Совета Европы о преступности в сфере компьютерной информации 2001 г.³, которая в 2004 г. ратифицирована и Российской Федерацией, только единожды употребляет понятие «киберпреступность», но не раскрывает его. Полагаем, что здесь уместно привести мнение ученых:

во-первых, в действующем российском законодательстве не содержится нормативного определения понятий, связанных с преступлениями в сфере компьютерных технологий, и, как следствие, понятия «киберпреступность»;

во-вторых, составы преступлений в сфере компьютерной информации, которые закреплены в уголовном законодательстве России, не во всем соответствуют международным актам, принятым для унификации правовых механизмов по противодействию киберпреступности, в том числе Конвенции № 185;

в-третьих, российское уголовное законодательство современного периода не имеет достаточную правовую основу для реализации ответственности за совершение преступлений с использованием компьютерных технологий [9, с. 10].

¹ Aconf.187/10. Справочный документ для семинара-практикума по преступлениям, связанным с использованием компьютерной сети [Электронный ресурс]. URL: https://mgimo.ru/upload/iblock/11d/11d26239824de2cccfb2_68b6ba2caa20.pdf (дата обращения: 18.09.2021).

² Предварительные итоги Одиннадцатого Конгресса ООН по предупреждению преступности и уголовному правосудию (Бангкок, 18–25 апреля 2005 г.) [Электронный ресурс]. URL: http://www.crime-research.ru/analytics/crime_bangkok (дата обращения: 14.08.2021).

³ Конвенция о преступности в сфере компьютерной информации (EST № 185) (прин. в г. Будапеште 23.11.2001, с изм. от 28.01.2003) [Электронный ресурс] // Доступ из справ.-правовой системы «КонсультантПлюс». URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base_13526#jAY95gSyWVhIGOJ12 (дата обращения: 14.08.2021).

На XIV Конгрессе ООН по предупреждению преступности и уголовному правосудию, проходившем с 7 по 12 марта 2021 г. в Киото, министр внутренних дел России В.А. Колокольцев использовал термин «информационная преступность», пояснив позицию России о том, что наша страна усматривает решение проблем с преступлениями в компьютерной сфере в разработке под эгидой ООН универсальной конвенции о противодействии информационной преступности¹. Отсюда становится понятным, что понятия «киберпреступность», «цифровая преступность», «компьютерная преступность» близки по смыслу. Также следует различать понятия «киберпреступность» и «киберпреступление». Несмотря на схожесть в словообразовании, это разные понятия. Первое по содержанию шире второго. И здесь, конечно, важно понимать, опираясь на норму ст. УК РФ, что киберпреступление есть общественно опасное виновное деяние, запрещенное УК РФ под угрозой наказания, которое совершается в информационном или киберпространстве. Данное преступление сложное по объектному составу. При его совершении субъект (или субъекты), согласимся с позицией И.В. Романова, посягает как на общественную безопасность, так и на собственность, права человека, иные охраняемые законом интересы и отношения [10, с. 107–108]. Не зря законодатель выделил в отдельную главу преступления в сфере компьютерной информации (гл. 28 УК РФ).

Совершенно очевидно, что понятие «киберпреступность» имеет более широкую сферу применения, им охватываются не только преступления, указанные в гл. 28 УК РФ, но и другие преступления, которые также можно совершить с использованием информационных технологий.

В Доктрине информационной безопасности понятие «киберпреступность» не употребляется. В ней используется понятие «угроза информационной безопасности», раскрываемое как действия и факторы в своей совокупности, которые несут опасность ущерба для интересов российского государства в информационной сфере.

Учитывая изложенное, постараемся резюмировать основные и важные положения о киберпреступности.

Однозначного понимания понятия киберпреступления на национальном и международном уровнях, в российском и международном законодательстве не сложилось, хотя оно в нем и содержится. Со своей стороны считаю, что киберпреступность – криминальное и одновременное негативное социальное правовое явление, появление которого связано с информационными технологиями, а точнее, с их широким распространением в бытовой,

¹ Владимир Колокольцев выступил на XIV Конгрессе ООН по предупреждению преступности и уголовному правосудию [Электронный ресурс]. URL: <https://xn--b1aew.xn--p1ai/news/item/23344408> (дата обращения: 13.09.2021).

предпринимательской, государственной и иных областях, сферах деятельности, с повышением их доступности, универсальности, использованием во всем мире.

Само понятие «киберпреступность» имеет широкую сферу применения, включает в себя всю совокупность преступных деяний, совершаемых с использованием информационно-коммуникационных технологий, является по сравнению с другими понятиями, обозначающими преступления в сфере информационно-телекоммуникационных сетей, наиболее оптимальным, отвечающим современным реалиям, а его базисной основой выступает киберпространство как сфера деятельности в информационном пространстве. Вместе с совершенствованием информационных технологий совершенствуются способы и орудия преступления, что обуславливает появление новых видов преступлений, требующих новых теоретических рекомендаций по их расследованию и раскрытию. В связи с этим необходимо выработать единый подход в доктрине права к содержательному аспекту термина «киберпреступность», дать его законодательное определение, проработать нормы уголовного права, закрепляющие составы преступлений, совершаемых в киберпространстве.

Юридическими признаками киберпреступности, определяющими ее сложную правовую природу и возможность ее теоретико-правовой идентификации как самостоятельной правовой категории в системе российского права и системе российского законодательства, можно назвать:

- прямую связь с информационной средой и нарушениями законодательства об информации;
- высокий уровень латентности;
- отсутствие географических границ, в которых совершаются киберпреступления, и, как следствие, их трансграничный характер;
- сложность расследования;
- крайне ограниченную оперативность в возможности пресечения совершения киберпреступлений;
- эффективное противодействие киберпреступности реально только при условии межнационального заинтересованного взаимодействия субъектов правоохранительных органов власти, государственного и частного секторов экономики, иных субъектов.

Список использованной литературы

1. Маслиенко М.А. Киберпреступность на современном этапе // Проблемы правоохранительной деятельности. 2021. № 2. С. 28–32.

2. Цимбал В.Н., Ключев С. Г. Понятие киберпреступления и его содержательная часть // Вестник Московск. ун-та МВД России. 2021. № 1. С. 129–132.
3. Ищук Я.Г., Пинкевич Т.В., Смольянинов Е.С. Цифровая криминология : учеб. пособие. М. : Акад. упр. МВД России, 2021. 244 с.
4. Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы : дис. ... канд. юрид. наук. Владивосток, 2005. 235 с.
5. Номоконов В.А., Тропина Т.Л. Киберпреступность как новая криминальная угроза // Криминология вчера, сегодня, завтра. 2012. № 1 (24). С. 45–55.
6. Чекунов И.Г. Киберпреступность: понятие, классификация, современные вызовы и угрозы // Молодые ученые. 2012. № 3. С. 178–186.
7. Пинкевич Т.В., Рахманова Е.Н. Понятие цифровой преступности // Современные тенденции управления и цифровая экономика: от регионального развития к глобальному экономическому росту : матер. 2-й Междунар. науч.-практ. конф. М., 2020. С. 193.
8. Летёлкин Н.В. Уголовно-правовое противодействие преступлениям, совершаемым с использованием информационно-телекоммуникационных сетей, включая сеть Интернет : автореф. дис. ... канд. юрид. наук. Н. Новгород, 2018. 24 с.
9. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий : учеб. пособие : в 2 ч. / А.В. Аносов [и др.]. М. : Акад. упр. МВД России, 2019. Ч. 1. 208 с.
10. Романов И.В. Понятие киберпреступлений и его значение для расследования // Сибирские уголовно-процессуальные и криминалистические чтения. 2016. № 5 (13). С. 105–109.

References

1. Maslienko M.A. Cybercrime at the present stage. *Problemy pravoohranitel'noj deyatel'nosti = Problems of law enforcement activity*, 2021, no. 2, pp. 28–32. (In Russian).
2. Tsimbal V.N., Klyuev S.G. Concept of cyber crime and its content. *Vestnik Moskovskogo universiteta MVD Rossii = Vestnik of Moscow University of the Ministry of Internal Affairs of Russia*, 2021, no. 1, pp. 129–132. (In Russian).
3. Ishchuk YA.G., Pinkevich T.V., Smol'yaninov E.S. *Cifrovaya kriminologiya* [Digital Criminology]. Ministry of Internal Affairs of the Russian Federation, 2021. 244 p.
4. Tropina T.L. *Kiberprestupnost': ponyatie, sostoyanie, ugovovno-pravovye меры bor'by Kand. Diss.* [Cybercrime: Concept, Conditions, Criminal Law Responses. Cand. Diss.]. Vladivostok, 2005. 235 p.

5. Nomokonov V.A., Tropina T.L. Cybercrime as a new criminal threat. *Kriminologiya vchera, segodnya, zavtra = Criminology: yesterday, today, tomorrow*, 2012, no. 1 (24), pp. 45–55. (In Russian).

6. Chekunov I.G. Cybercrime: Concept, Classification, Modern Challenges and Threats. *Young Scientists = Molodye uchenye*, 2012, no. 3, pp. 178–186. (In Russian).

7. Pinkevich T.V., Rakhmanova E.N. Digital Crime Concept. *Sovremennye tendencii upravleniya i cifrovaya ekonomika: ot regional'nogo razvitiya k global'nomu ekonomicheskomu rostu. Materialy 2-j Mezhdunarodnoj nauchno-prakticheskoy konferencii* [Modern Management Trends and the Digital Economy: from Regional Development to Global Economic Growth. Materials of the 2nd International Scientific and Practical Conference]. Moscow, 2020, p. 193. (In Russian).

8. Letyolkin N.V. *Ugolovno-pravovoe protivodejstvie prestupleniyam, sovershaemym s ispol'zovaniem informacii-onno-telekommunikacionnyh setej, vključaya set' Internet. Avtoref. Kand. Diss.* [Criminal Law responses to Crimes Committed through the Use of Information and Telecommunications Networks, including the Internet. Cand. Diss. Thesis]. Nizhny Novgorod, 2018. 24 p.

9. Gavrilin YU.V., Anosov A.V., Baranov V.V., Vasilchenko D.A., Golyandin N.P., Grinchenko V.S., Desyatov M.S., Kuzmin N.A., Lapunova YU.A., Lyuban V.G., Malakhov A.S., Parfenov A.V., Prokhorov E.S., Rjasov A.V., Smolyaninov E.S., Tretyakov M.A., Filippov A.N. *Deyatel'nost' organov vnutrennih del po bor'be s prestupleniyami, sovershennymi s ispol'zovaniem informacionnyh, kommunikacionnyh i vysokih tekhnologij* [The Activities of the Internal Affairs Bodies to Combat Crimes Committed Using Information, Communication and High Technologies]. Ministry of Internal Affairs of the Russian Federation, 2019, pt. 1. 208 p.

10. Romanov I.V. The concept of cybercrime and its implications for the investigation. *Sibirskie ugolovno-processual'nye i kriminalisticheskie chteniya = Siberian criminal process and criminalistic readings*, 2016, no. 5 (13), pp. 105–109. (In Russian).

Информация об авторе

Сандальникова Елена Владимировна – кандидат юридических наук, доцент кафедры таможенного дела и правового обеспечения Ульяновского государственного университета, г. Ульяновск;
sandalnikova.elena@yandex.ru

Information about the Author

Sandalnikova Elena Vladimirovna – Candidate of Sciences (Law), Assistant Professor of the Chair of Customs and Legal Support, Ulyanovsk State University, Ulyanovsk;
sandalnikova.elena@yandex.ru

Для цитирования

Сандальникова Е.В. Теоретико-правовая идентификация киберпреступности в системе российского права и системе российского законодательства // Вестник Института права Башкирского государственного университета. 2021. № 3. С. 58–71. DOI 10.33184/vest-law-bsu-2021.11.8.

For citation

Sandalnikova E.V. Legal and Theoretical Identification of Cybercrime in the Russian Law System and in the Russian Legislation System. *Vestnik Instituta prava Bashkirskogo gosudarstvennogo universiteta* = *Bulletin of the Institute of Law of the Bashkir State University*, 2021, no. 2, pp. 58–71. DOI 10.33184/vest-law-bsu-2021.11.8. (In Russian).