Наталья Николаевна БУГЕРА,
кандидат юридических наук, доцент, ORCID 0000-0002-2459-7855
Волгоградская академия МВД России (г. Волгоград)
начальник кафедры уголовного права учебно-научного комплекса
по предварительному следствию в органах внутренних дел
knn.76@mail.ru

Научная статья
УДК 343.34:[004.6+004.9]

УГОЛОВНАЯ ОТВЕТСТВЕННОСТЬ ЗА НЕПРАВОМЕРНЫЙ ДОСТУП К КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ: РЕТРОСПЕКТИВНЫЙ СРАВНИТЕЛЬНО-ПРАВОВОЙ АНАЛИЗ

КЛЮЧЕВЫЕ СЛОВА. Информация, неправомерный доступ, информационные технологии, «компьютерные» преступления, уголовное законодательство, уголовная ответственность.

АННОТАЦИЯ. ***Введение.*** *В нашей стране продолжается период преобразований в экономике. С каждым годом возрастает число акционерных, совместных и частных предприятий, фермерских хозяйств, представительств иностранных компаний. Эта динамика, соответствующая росту экономической активности, тесно переплетается с быстрым развитием информационных технологий, что формирует новую реальность, в которой угрозы кибербезопасности приобретают значительный масштаб. Развитие банковского сектора, активное внедрение современных вычислительных и коммуникационных технологий в деятельность государственных структур приводит к увеличению объемов хранимой и обрабатываемой информации. Неправомерный доступ к информации является одним из наиболее распространенных видов «компьютерных» преступлений. Такой доступ осуществляется с применением различных методов, в том числе посредством технологий социальной инженерии, взлома паролей, а также использования уязвимостей в программном обеспечении. Последствия неправомерного доступа могут быть весьма серьезными: утечка конфиденциальных данных, финансовые потери, репутационный ущерб, нарушение деятельности организаций и государственных учреждений.* ***Методы.*** *При проведении исследования оказался востребован общенаучный диалектический метод познания окружающей действительности, предполагающий полное и всестороннее изучение явлений, рассмотрение связей и противоречий между ними. Кроме того, были использованы методы описания, сравнительно-правового анализа, логического осмысления, абстрагирования и обобщения. Проведено изучение динамики показателей, характеризующих количество зарегистрированных преступлений, квалифицированных по ст. 272 УК РФ.* ***Результаты.*** *Сравнительный анализ законодательства разных стран позволил установить, что существует значительная вариативность в подходах к определению состава преступления рассматриваемого нами вида, критериям их квалификации и мерам наказания за их совершение. Некоторые страны акцентируют внимание на материальном ущербе, другие – на нарушении конфиденциальности данных, третьи – на несанкционированности доступа. Унификация терминологии и критериев квалификации во всемирном масштабе, по нашему мнению, является необходимым условием для эффективного международного сотрудничества в сфере противодействия неправомерному доступ к информации.*

ВВЕДЕНИЕ

Научно-технический прогресс, развитие компьютерных технологий, глобальных информационных сетей в условиях рыночной экономики привели к появлению таких общественно опасных деяний, как «компьютерные» преступления. Информатизация, телекоммуникационные системы охватили все сферы государственной и общественной жизни. Общественная угроза, исходящая от «компьютерных» преступлений, заключается в том, что виновные применяют современные технологии для реализации своих преступных намерений, совершая нередко тяжкие и особо тяжкие уголовно наказуемые деяния. Использование безбумажных технологий и вычислительных средств в управленческой и про-

Natalia N. BUGERA,
Cand. Sci. (Jurisprudence), Associate Professor, ORCID 0000-0002-2459-7855
Volgograd Academy of the Ministry of Interior of Russia (Volgograd, Russia)
Head of the Department of Criminal Law of the Educational and Scientific
Complex for Preliminary Investigation in the Internal Affairs Bodies
knn.76@mail.ru

CRIMINAL LIABILITY FOR UNLAWFUL ACCESS TO COMPUTER INFORMATION: A RETROSPECTIVE COMPARATIVE LEGAL ANALYSIS

KEYWORDS. Information, unlawful access, information technology, «computer» crimes, criminal legislation, criminal liability.

ANNOTATION. ***Introduction.*** *Our country continues to undergo economic transformations. The number of joint-stock, joint and private enterprises, farms, and representative offices of foreign companies increases every year. This dynamic, which corresponds to the growth of economic activity, is closely intertwined with the rapid development of information technology, which forms a new reality in which cybersecurity threats are acquiring a significant scale. The development of the banking sector, the active introduction of modern computing and communication technologies in the activities of government agencies leads to an increase in the volume of stored and processed information. Unlawful access to information is one of the most common types of «computer» crimes. Such access is carried out using various methods, including social engineering technologies, password cracking, and the use of software vulnerabilities. The consequences of unlawful access can be very serious: leakage of confidential data, financial losses, damage to reputation, disruption of the activities of organizations and government agencies.* ***Methods.*** *When conducting the study, the general scientific dialectical method of cognition of the surrounding reality was in demand, which involves a complete and comprehensive study of phenomena, consideration of the connections and contradictions between them. In addition, the methods of description, comparative legal analysis, logical comprehension, abstraction and generalization were used. The dynamics of indicators characterizing crimes classified under Article 272 of the Criminal Code of the Russian Federation was studied.* ***Results.*** *A comparative analysis of the legislation of different countries allowed us to establish that there is significant variability in approaches to defining the elements of the crime of the type under consideration, the criteria for their qualification and penalties for committing them. Some countries focus on material damage, others – on violation of data confidentiality, others – on unlawful access. Unification of terminology and criteria for qualification on an international scale, in our opinion, is a prerequisite for effective international cooperation in the field of counteracting unlawful access to information.*

изводственной сферах создает возможности для совершения преступлений.

МЕТОДЫ

В ходе исследования применялся общенаучный диалектический метод познания окружающей действительности, предполагающий полное и всестороннее изучение явлений, рассмотрение связей и противоречий между ними. Кроме того, были использованы общенаучные методы: анализ и синтез – для детального изучения отличий, имеющих место в описании объективных и субъективных признаков «компьютерных» преступлений; с помощью метода обобщения был сделан вывод о сходстве и различиях некоторых признаков «компьютерных» преступлений в зарубежных странах. Среди частнонаучных методов оказались востребованы: формально-юридический метод (для более точного правоприменения), сравнительно-правовой метод (способствовал анализу предусмотренных в разных странах санкций за совершение «компьютерных» преступлений).

РЕЗУЛЬТАТЫ

Преступления в области компьютерной информации, хотя и занимают относительно небольшую долю в общей структуре преступности по сравнению с другими видами преступлений, особенно связанными с посягательствами на собственность, представляют собой серьезную угрозу как для отдельных пользователей электронно-вычислительной техники, так и для национальной безопасности в целом. На это обращали внимание многие исследователи, изучавшие соответсвующую проблематику [1, 2, 3]. Такие преступления всё чаще принимают организованный транснациональный характер, а наносимый ими вред порой с трудом поддается подсчету. Согласно статистическим данным, количество зарегистрированных преступлений, квалифицированных по ст. 272 УК РФ (неправомерный доступ к компьютерной информации), ежегодно растет. Так, в 2019 году их было 242, в 2020 – 4105, в 2021 – 6392, в 2022 – 9308, в 2023 – 36788. В 2024 году их число достигло 105311[1].

В России неоднократно в разные годы рассматривались законопроекты, касающиеся ответственности за «компьютерные» преступления. Однако огромные масштабы наносимого такими преступлениями ущерба и практическое отсутствие возможности возмещения причиненного ими вреда свидетельствуют о том, что действующая в нашей стране нормативная правовая база, регламентирующая уголовную ответственность за преступления рассматриваемого нами вида, по-прежнему требует совершенствования. Инициирование законопроектов еще до принятия Уго-

[1] Состояние преступности // МВД России: сайт // URL: https://мвд.рф/folder/101762 (дата обращения: 28.01.2025).

ловного кодекса Российской Федерации 1996 года позволило акцентировать внимание на необходимости решения вопросов, связанных с неправомерным доступом к компьютерной информации, на законодательном уровне. Но, к сожалению, разработанные в то время нормативные акты не были лишены недостатков, возникла необходимость во внесении в них существенных изменений для уточнения объективных и субъективных признаков «компьютерных» преступлений. Позитивный момент подготовки тех законопроектов заключался в том, что удалось определить основные направления совершенствования законодательства, регламентирующего ответственность за «компьютерные» преступления, а некоторые их положения были использованы законодателем в дальнейшем. Разработчики новых законопроектов отказались от ранее высказанных предложений ограничиться дополнением уже имеющихся в УК РСФСР составов преступлений квалифицирующими обстоятельствами по признаку использования компьютерной техники. И первый (появившийся до принятия УК РФ 1996 года), и второй (представленный в период принятия УК РФ 1996 года) законопроекты были ориентированы на введение в уголовное законодательство отдельных норм, содержащих составы самостоятельных «компьютерных» преступлений.

Авторы законопроектов, используя законотворческий опыт зарубежных стран, положения, содержавшиеся в международных соглашениях, предлагали сформировать в УК РФ отдельную самостоятельную главу 29 «Компьютерные преступления». В итоге в кодексе 1996 года появилась глава 28 «Преступления в сфере компьютерной информации». Вместе с тем сфера обработки информации и информационного обмена была регламентирована не только УК РФ, но и федеральными законами от 16 февраля 1995 г. № 15-ФЗ «О связи» и от 20 февраля 1995 г. № 24-ФЗ «Об информации, информатизации и защите информации» (оба документа утратили силу). В указанных нормативных актах были даны определения объектов правовой защиты в сфере информационных технологий, устанавливались категории доступа отдельных субъектов к конкретным видам информации, регламентировались права и обязанности владельцев этих объектов. Юридическая значимость данных законов заключалась еще и в том, что они содержали определение понятия «конфиденциальная информация», а также устанавливали пределы его правового применения и указывали конкретных лиц, ответственных за защиту такой информации от воздействия тех или иных факторов [4, с. 62].

3 апреля 1995 года был подписан Указ Президента Российской Федерации № 334 «О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации». Это событие имело большое значение для формирования комплекса мер, направленных на улучшение безопасности информационных и телекоммуникационных систем государственных учреждений, российских финансовых организаций, а также различных компаний и учреждений. В целях реализации этих мер Правительство Российской Федерации 26 июня 1995 года приняло постановление № 608 «О сертификации средств защиты информации», в соответствии с которым планировалось создать механизмы фиксации сведений о системе сертификации, а также о средствах защиты информации, подлежащих лицензированию, о порядке оплаты услуг, связанных с их разработкой, установкой, эксплуатацией, и т.д.

Таким образом, законодательство Российской Федерации, регламентирующее отношения, связанные с доступом к компьютерной информации, начало постепенно формироваться примерно с 1991 года. Однако, несмотря на все достоинства принятых в период с 1991 по 1997 год нормативных актов, в российской правовой системе в то время не существовало уголовно-правовых мер защиты компьютерной информации от несанкционированного доступа [5, с. 111]. И потому важнейшим событием, связанным с организацией борьбы с «компьютерными» преступлениями, включая неправомерный доступ к компьютерной информации, оказалось вступление в силу с 1 января 1997 года нового Уголовного кодекса. Ключевым моментом стала криминализация общественно опасных деяний в сфере компьютерной информации [6, с. 43]. Дальнейшее развитие законодательства, регламентирующего ответственность за неправомерный доступ к компьютерной информации, связано с принятием Федерального закона от 8 декабря 2003 г. № 162-ФЗ «О внесении изменений и дополнений в Уголовный кодекс Российской Федерации». В положения гл. 28 УК РФ были внесены изменения и дополнения. Редакция диспозиции рассматриваемой нами нормы (ст. 272 УК РФ) осталась прежней, корректировке подверглась лишь ее санкция.

Изучение зарубежного законодательства, регламентирующего ответственность за несанкционированный доступ к компьютерной информации, позволило выявить разнообразие подходов иностранных законодателей к определению родового объекта исследуемого нами преступления. Таковым признаются различные группы общественных отношений. В качестве родового объекта незаконного доступа к компьютерной информации в большинстве европейских стран определены общественная безопасность и общественный порядок (в Латвии, Нидерландах и др.). В некоторых государствах, например во Франции и Бельгии, родовым объектом такого преступления признается неприкосновенность системы автоматизированной обработки информации, в ФРГ и Австрии – частная и профессиональная сфера.

По нашему мнению, можно выделить три группы зарубежных стран, различающихся подходами законодателя к криминализации неправомерного доступа к компьютерной информации. В первую группу входят государства, в уголовных законах которых имеются отдельные самостоятельные нормы, устанавливающие ответственность за несанкционированный доступ к компьютерной информации. Это Австрия, Дания, Бельгия, Латвия,

Франция. Вторая группа стран включает в себя те государства, где неправомерный доступ к компьютерной информации криминализирован лишь в качестве способа совершения иных преступлений, а самостоятельной статьи, посвященной данному преступлению, в уголовных кодексах нет. К этой группе относятся Испания и Швеция. Третью группу составляют страны, в уголовном законодательстве которых ответственность за неправомерный доступ к компьютерной информации предусмотрена как в отдельной самостоятельной норме, так и в качестве квалифицирующего признака в составах других преступлений. Здесь речь идет о Польше, ФРГ, Нидерландах.

Анализ включенных в иностранные кодексы уголовно-правовых норм, касающихся ответственности за неправомерный доступ к компьютерной информации, выявил ряд характерных черт, относящихся к объективной стороне данного преступления. В связи с этим выделяются два подхода законодателей к формулированию состава рассматриваемого нами преступления. Первый связан с криминализацией доступа именно к компьютерной информации (как в Дании и Польше), либо сведениям (в ФРГ) или электронным данным (в Австрии). Второй подход обусловливает установление ответственности за неправомерный доступ в саму систему обработки информации, то есть в информационное или компьютерное устройство, электронную систему (как сделано, например, в Латвии, Австрии, Нидерландах, Бельгии, Франции).

Еще одной характерной для зарубежного уголовного права чертой является иное восприятие способов совершения рассматриваемого нами преступления и других связанных с ним обстоятельств [7, с. 313]. Например, в Уголовном кодексе Бельгии упоминается такой признак общественно опасного деяния, как «доступ без разрешения». В Уголовном кодексе Дании законодатель указал, что подобный доступ является незаконным и несанкционированным. В уголовных кодексах Нидерландов и Польши при описании способа совершения преступления в качестве обязательного признака указывается «с нарушением мер (системы) защиты». В кодексах некоторых стран делается указание на специальный предмет преступления, а именно «сведения, имеющие особо охраняемый характер» (например в ФРГ). Поразному в зарубежных уголовных кодексах определено содержание самого общественно опасного деяния. Так, в ФРГ это «разведывание сведений», а в Австрии – «противозаконный доступ».

Различия наблюдаются также и в подходах законодателей к конструкции состава преступления. В большинстве уголовных кодексов зарубежных стран состав неправомерного доступа к компьютерной информации сформулирован по типу формального [8, с. 126], то есть общественно опасные последствия не включены в качестве конструктивных признаков в состав рассматриваемого преступления (в Дании, Нидерландах, Бельгии и др.)[1].

Исследование особенностей субъекта неправомерного доступа к компьютерной информации показало, что в большинстве зарубежных стран им признается физическое вменяемое лицо, достигшее установленного законом возраста [9, с. 75]. Отличительной особенностью УК Франции является возможность привлечения к уголовной ответственности не только физического, но и юридического лица. Причем это касается и ряда других преступлений (например экологических или коррупционной направленности). Французский законодатель не только указал юридических лиц в качестве субъектов рассматриваемого нами преступления, но и подробно регламентировал виды и сроки наказаний, применяемых к юридическим лицам в случае совершения таких преступлений. Уголовная ответственность юридических лиц предусмотрена также в Дании и Бельгии [10, с. 82].

Следует отметить разнообразие подходов зарубежных законодателей к возрасту субъекта рассматриваемого нами преступления. В отличие от российского законодательства, согласно которому субъектом является лицо, достигшее 16-летнего возраста, в некоторых зарубежных странах предусмотрена возможность привлечения к ответственности за неправомерный доступ к компьютерной информации в более раннем возрасте. 12-летний возраст субъекта такого преступления установлен в Нидерландах. В Швеции и Дании субъектом признается лицо, достигшее 15 лет. Так же как и в России, ответственность с 16 лет предусмотрена в Латвии. А вот в Польше минимальный возраст субъекта данного преступления – 17 лет.

Исследование особенностей признаков субъективной стороны неправомерного доступа к компьютерной информации показало единообразный подход зарубежных законодателей к определению формы вины [11, с. 102]. Во всех изученных нами иностранных уголовных кодексах субъективная сторона в данном случае выражается в вине в виде прямого умысла. Неосторожная форма вины указывается как признак квалифицированных составов неправомерного доступа к компьютерной информации. В некоторых кодексах (например в Бельгии) предусмотрена альтернативная форма вины (умысел или неосторожность).

Две группы государств можно выделить, рассматривая позиции их законодателей относительно обстоятельств, отягчающих уголовную ответственность за неправомерный доступ к компьютерной информации. К первой относятся страны, в уголовных кодексах которых представлен только основной состав несанкционированного доступа, без квалифицирующих признаков (как, например, в Австрии). Вторую группу составляют государства, в уголовных кодексах которых предусмотрены квалифицирующие признаки неправомерного доступа к компьютерной информации. Среди них самыми распространенными являются: совершение деяния с использованием служебного положения; незаконный доступ, совершенный повторно, совершенный организованной группой,

[1] Ястребов Д.А. Уголовная ответственность за преступления в сфере компьютерной информации за рубежом: Лекция / под общ. ред. Р.А. Каламкаряна. 2-е изд., перераб. и доп. М., 2004. С. 16.

совершенный по приказу; неправомерный доступ, повлекший ухудшение функционирования компьютерной системы[1]. Кроме того, в качестве квалифицированных составов преступлений выделены: неправомерный доступ, причинивший определенный ущерб; неправомерный доступ, повлекший изменение или уничтожение данных; неправомерный доступ, совершенный с целью изъятия (копирования) данных; несанкционированный доступ с намерением совершить обманную операцию (с целью получить незаконный доход) [12, с. 129]. Таким образом, есть основания говорить о том, что законодательство большинства зарубежных стран отличается многообразием квалифицированных видов незаконного доступа к компьютерной информации.

Большое значение при проведении компаративистского исследования уголовного законодательства имеет сопоставление санкций за незаконный доступ к компьютерной информации, установленных в нормах кодексов зарубежных стран [13, с. 27]. В большинстве стран за совершение этого преступления предусмотрены альтернативные и относительно-определенные санкции, причем, как правило, указано два вида наказания. Самым распространенным видом наказания является штраф (в Австрии, Бельгии, в американском штате Техас). Во многих странах в санкцию включен и такой вид наказания, как лишение свободы. Минимальный срок лишения свободы – до 6 месяцев – предусмотрен в Дании, Норвегии, Австрии, Нидерландах; срок до 1 года установлен во Франции, Бельгии; до 3 лет – в ФРГ, Турции, КНР, Польше (то есть в этих странах общественная опасность данного преступления признается более высокой). Отличительной особенностью уголовного кодекса штата Техас является зависимость срока лишения свободы от размера ущерба, который был причинен виновным [14, с. 69]. Так, за совершение несанкционированного доступа к компьютерной информации в рамках основного состава преступления установлено наказание в виде лишения свободы на срок от 180 дней, а в случае особо квалифицированного состава – до 99 лет (при условии, что в результате совершения преступления был причинен ущерб на сумму свыше 200 тысяч долларов). В некоторых странах в санкции норм, предусматривающих ответственность за неправомерный доступ к компьютерной информации, включены такие виды наказания, как ограничение свободы (как в Польше) и арест (например в КНР). Таким образом, результаты изучения санкций, закрепленных в уголовных кодексах зарубежных стран, показывают, что в большинстве государств неправомерный доступ к компьютерной информации относится к числу преступлений небольшой тяжести (так же как и в Российской Федерации).

ЗАКЛЮЧЕНИЕ

Подводя итог, подчеркнем, что общественная опасность незаконного доступа к компьютерной информации давно признана международным сообществом, и это отразилось в отнесении деяний данного вида к группе транснациональных преступлений. Это обусловливает необходимость повышения эффективности самых репрессивных из всех имеющихся способов противодействия им, а именно уголовно-правовых средств [15, с. 551]. Несомненно, этому будет способствовать приведение к единообразию подходов законодателей разных стран к установлению оснований уголовной ответственности за незаконный доступ к компьютерной информации. Среди возможных путей решения обозначенной проблемы видится разработка единых критериев криминализации такого доступа. Причем это будет полезно для дальнейшей успешной борьбы с «компьютерными» преступлениями всех видов.

Проведенный нами анализ уголовно-правовых норм законодательства некоторых зарубежных государств показал, что незаконный доступ к компьютерной информации в том или ином виде криминализирован во всех развитых странах. Отмечаются различия в подходах к конструированию отдельных признаков состава исследуемого преступления, а также к его законодательной конструкции и определению его квалифицированных видов. Во всех странах установлен запрет на совершение несанкционированного доступа в целях защиты компьютерной информации и обеспечения безопасности ее использования.

Различия в основаниях уголовной ответственности за незаконный доступ к компьютерной информации в зарубежных странах могут носить существенный характер. В связи с этим представляется целесообразным унифицировать подход к определению признаков основного состава этого преступления, что значительно повысит эффективность противодействия данному виду транснациональной преступности. ■

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Семенова И.В. Цифровая информация как предмет посягательства преступлений в сфере компьютерной информации // Ученые записки Крымского федерального университета имени В.И. Вернадского. Юридические науки. 2022. Т. 8 (74). № 4. С. 158-165.

2. Сердюкова Е.В., Чуниха А.А., Зиновьева Е.О. Особенности уголовной ответственности за преступления в сфере компьютерной информации // Восточно-Европейский научный журнал. 2021. № 8-1 (72). С. 57-59.

3. Алексеева А.П., Анисимова Т.В. Законодательные инициативы в сфере установления уголовной ответственности за незаконные использование и передачу, сбор и хранение компьютерной информации, содержащей персональные данные: проблемы и перспективы // Уголовное законодательство: вчера, сегодня, завтра. Материалы международной научно-практической конференции. СПб: СПбУ МВД России, 2024. С. 13-15.

[1] Зинина У.В. Преступления в сфере компьютерной информации в российском и зарубежном уголовном праве: Автореф. дис. … канд. юрид. наук. М., 2007. С. 11.

4. Настоящий А.В. История появления и развития преступлений в сфере компьютерной информации // Студенческий вестник. 2020. № 7-1 (105). С. 62-63.

5. Кочкина Э.Л., Сутурин М.А. Уголовная ответственность за преступления в сфере компьютерной информации: история становления и обзор нормативных документов // Актуальные вопросы совершенствования уголовной политики Российской Федерации. Сборник научных статей научно-практической конференции. Ростов-на-Дону, 2019. С. 111-116.

6. Ханмагамедова Ф.А. Методы борьбы с преступлениями в сфере компьютерной информации // Вестник Социально-педагогического института. 2011. № 1 (2). С. 43-44.

7. Канубриков В.А., Османов М.М. Способ совершения преступления как составообразующий признак преступлений в сфере компьютерной информации // Образование и право. 2021. № 5. С. 312-315.

8. Дворецкий М.Ю. Квалификация преступлений в сфере компьютерной информации в контексте эффективной реализации уголовной ответственности // Уголовное право: стратегия развития в XXI веке. 2023. № 3. С. 126-131.

9. Каримов А.М. Преступления в сфере компьютерной информации и преступления, совершаемые с использованием информационно-коммуникационных технологий: сравнительно-правовой аспект // Вестник Казанского юридического института МВД России. 2023. Т. 14. № 1 (51). С. 75-82.

10. Додонов В.Н., Капинус О.С., Щерба С.П. Сравнительное уголовное право. Особенная часть: Монография. М., 2010. 544 с.

11. Ульянов М.В. Преступления в сфере компьютерной информации: возможности уголовно-правового воздействия и предупреждения // Правопорядок: история, теория, практика. 2022. № 4 (35). С. 102-108.

12. Дремлюга Р.И. Компьютерная информация как предмет посягательства при неправомерном доступе: сравнительный анализ законодательства США и России // Журнал зарубежного законодательства и сравнительного правоведения. 2018. № 6 (73). С. 129-133.

13. Алексеева А.П., Белокобыльская О.И., Третьяков Ю.В. Возможности унификации критериев соотношения терминов, включенных в понятийный аппарат в сфере превенции преступности и преступлений // Вестник Волгоградской академии МВД России. 2023. № 3 (66). С. 25-30.

14. Фатьянов А.А., Григорьева М.А. Преступления в сфере компьютерной информации по законодательству Российской Федерации и штата Луизиана (США): сравнительно-правовой анализ // Российский следователь. 2022. № 8. С. 69-74.

15. Алексеева А.П. Профилактика правонарушений в России: законодательные основы и перспективы реализации // Преступность, уголовная политика, уголовный закон. Сборник научных трудов. Саратов: Саратовская государственная юридическая академия, 2013. С. 549-551.

REFERENCES

1. Semenova I.V. Tsifrovaya informatsiya kak predmet posyagatel'stva prestupleniy v sfere komp'yuternoy informatsii // Uchenyye zapiski Krymskogo federal'nogo universiteta imeni V.I. Vernadskogo. Yuridicheskiye nauki. 2022. T. 8 (74). № 4. S. 158-165.

2. Serdyukova Ye.V., Chunikha A.A., Zinov'yeva Ye.O. Osobennosti ugolovnoy otvetstvennosti za prestupleniya v sfere komp'yuternoy informatsii // Vostochno-Yevropeyskiy nauchnyy zhurnal. 2021. № 8-1 (72). S. 57-59.

3. Alekseyeva A.P., Anisimova T.V. Zakonodatel'nyye initsiativy v sfere ustanovleniya ugolovnoy otvetstvennosti za nezakonnyye ispol'zovaniye i peredachu, sbor i khraneniye komp'yuternoy informatsii, soderzhashchey personal'nyye dannyye: problemy i perspektivy // Ugolovnoye zakonodatel'stvo: vchera, segodnya, zavtra. Materialy mezhdunarodnoy nauchno-prakticheskoy konferentsii. SPb: SPbU MVD Rossii, 2024. S. 13-15.

4. Nastoyashchiy A.V. Istoriya poyavleniya i razvitiya prestupleniy v sfere komp'yuternoy informatsii // Studencheskiy vestnik. 2020. № 7-1 (105). S. 62-63.

5. Kochkina E.L., Suturin M.A. Ugolovnaya otvetstvennost' za prestupleniya v sfere komp'yuternoy informatsii: istoriya stanovleniya i obzor normativnykh dokumentov // Aktual'nyye voprosy sovershenstvovaniya ugolovnoy politiki Rossiyskoy Federatsii. Sbornik nauchnykh statey nauchno-prakticheskoy konferentsii. Rostov-na-Donu, 2019. S. 111-116.

6. Khanmagamedova F.A. Metody bor'by s prestupleniyami v sfere komp'yuternoy informatsii // Vestnik Sotsial'no-pedagogicheskogo instituta. 2011. № 1 (2). S. 43-44.

7. Kanubrikov V.A., Osmanov M.M. Sposob sovershen'iya prestupleniya kak sostavoobrazuyushchiy priznak prestupleniy v sfere komp'yuternoy informatsii // Obrazovaniye i pravo. 2021. № 5. S. 312-315.

8. Dvoretskiy M.Yu. Kvalifikatsiya prestupleniy v sfere komp'yuternoy informatsii v kontekste effektivnoy realizatsii ugolovnoy otvetstvennosti // Ugolovnoye pravo: strategiya razvitiya v XXI veke. 2023. № 3. S. 126-131.

9. Karimov A.M. Prestupleniya v sfere komp'yuternoy informatsii i prestupleniya, sovershayemyye s ispol'zovaniyem informatsionno-kommunikatsionnykh tekhnologiy: sravnitel'no-pravovoy aspekt // Vestnik Kazanskogo yuridicheskogo instituta MVD Rossii. 2023. T. 14. № 1 (51). S. 75-82.

10. Dodonov V.N., Kapinus O.S., Shcherba S.P. Sravnitel'noye ugolovnoye pravo. Osobennaya chast': Monografiya. M., 2010. 544 s.

11. Ul'yanov M.V. Prestupleniya v sfere komp'yuternoy informatsii: vozmozhnosti ugolovno-pravovogo vozdeystviya i preduprezhdeniya // Pravoporyadok: istoriya, teoriya, praktika. 2022. № 4 (35). S. 102-108.

12. Dremlyuga R.I. Komp'yuternaya informatsiya kak predmet posyagatel'stva pri nepravomernom dostupe: sravnitel'nyy analiz zakonodatel'stva SSHA i Rossii // Zhurnal zarubezhnogo zakonodatel'stva i sravnitel'nogo pravovedeniya. 2018. № 6 (73). S. 129-133.

13. Alekseyeva A.P., Belokobyl'skaya O.I., Tret'yakov Yu.V. Vozmozhnosti unifikatsii kriteriyev sootnosheniya terminov, vklyuchennykh v ponyatiynyy apparat v sfere preventsii prestupnosti i prestupleniy // Vestnik Volgogradskoy akademii MVD Rossii. 2023. № 3 (66). S. 25-30.

14. Fat'yanov A.A., Grigor'yeva M.A. Prestupleniya v sfere komp'yuternoy informatsii po zakonodatel'stvu Rossiyskoy Federatsii i shtata Luiziana (SShA): sravnitel'no-pravovoy analiz // Rossiyskiy sledovatel'. 2022. № 8. S. 69-74.

15. Alekseyeva A.P. Profilaktika pravonarusheniy v Rossii: zakonodatel'nyye osnovy i perspektivy realizatsii // Prestupnost', ugolovnaya politika, ugolovnyy zakon. Sbornik nauchnykh trudov. Saratov: Saratovskaya gosudarstvennaya yuridicheskaya akademiya, 2013. S. 549-551.

ССЫЛКА ДЛЯ ЦИТИРОВАНИЯ

Бугера Н.Н. Уголовная ответственность за неправомерный доступ к компьютерной информации: ретроспективный сравнительно-правовой анализ // Вестник Калининградского филиала Санкт-Петербургского университета МВД России. 2025. № 1 (79). С. 16-22.