Научная статья
УДК 343
doi 10.46741/2713-2811.2024.25.1.015

Преступления в сфере компьютерной информации: реальное состояние и перспективы реализации

АЛЛА ВАЛЕРЬЕВНА ПЕЛЕВИНА

Национальный исследовательский Нижегородский государственный университет им. Н. И. Лобачевского, Нижний Новгород, Россия, allochka_90@bk.ru

Аннотация. В статье рассматриваются преступления в сфере компьютерной информации, исследуется их эволюция, дается доктринальная оценка реального состояния, выявляются юридико-технические изъяны в конструировании уголовно-правовых положений, формулируются предложения по их устроению. Отмечается особая роль Уголовного кодекса Российской Федерации в правовой защите информации (гл. 28).

Ключевые слова: Конституция Российской Федерации; Уголовный кодекс Российской Федерации; закон; преступления в сфере компьютерной информации; информация; информационные отношения; статья; должностное лицо; примечание; терминологический инструментарий; законодательная ошибка; коллизии.

5.1.4. Уголовно-правовые науки.

Для цитирования: Пелевина А. В. Преступления в сфере компьютерной информации: реальное состояние и перспективы реализации // Ius publicum et privatum: сетевой научно-практический журнал частного и публичного права. 2024. № 1 (25). С. 120–128. doi 10.46741/2713-2811.2024.25.1.015.

Original article

Computer Crime: Problems of Identifying the Corpus Delicti and Exercising Criminal Liability

ALLA V. PELEVINA

Lobachevsky State University of Nizhny Novgorod, Nizhny Novgorod, Russia, allochka_90@bk.ru

Abstract. The article considers computer crimes, studies their evolution, gives a doctrinal assessment of the real state, identifies legal and technical flaws in the construction of criminal law provisions, and formulates proposals for their correction. The special role of the Criminal Code of the Russian Federation in the legal protection of information is noted.

Keywords: Constitution of the Russian Federation; Criminal Code of the Russian Federation; law; computer crimes; information; information relations; article; official; note; terminological tools; legislative error; collisions.

5.1.4. Criminal law sciences.

For citation: Pelevina A.V. Computer crime: problems of identifying the corpus delicti and exercising criminal liability. *Ius publicum et privatum: online scientific and practical journal of private and public law*, 2024, no. 1 (25), pp. 120–128. doi 10.46741/2713-2811.2024.25.1.015.

Эволюция современного мира характеризуется массовым внедрением информационных технологий во все сферы человеческого бытия. Информационные отношения стали его неотъемлемой частью, важнейшим направлением деятельности законодательных и исполнительных органов государственной власти, учреждений и организаций, граждан, значимым фактором общественной жизни, определяющим стратегию и тактику развития мировой цивилизации [1, с. 75].

Изложенное выше положение нашло свое реальное воплощение в принятой 12 декабря 1993 г. Конституции Российской Федерации. Так, в Основном законе закреплено право на информацию, позволяющую обеспечить развитие свободного демократического общества. Регламентированное право на информацию принадлежит любому лицу, независимо от пола, расы, национальности, языка, происхождения, имущественного и должностного положения, места жительства, отношения к религии, убеждений, принадлежности к общественным объединениям, а также другим обстоятельствам, если оно находится на территории Российской Федерации.

Конкретизация указанного положения нашла свое подтверждение в п. 4 ст. 29 Конституции Российской Федерации, где провозглашается свобода информации, то есть право каждого свободно искать, получать, передавать, производить и распространять информацию любым законным способом – посредством межличностного общения, средств массовой информации, материальных носителей информации. Кроме того, в п. 5 ст. 29 устанавливается запрет на цензуру массовой информации, а в п. 1 ст. 24 содержится запрет на сбор, хранение, использование и распространение информации о частной жизни без согласия лица.

В различных национальных законодательных источниках конституционное положение закрепляет право на обладание, пользование, воспроизведение, защиту, уничтожение ненужной информации.

Особую роль в правовой защите информации играет Уголовный кодекс Российской Федерации. Свидетельством этому являются уголовно-правовые нормы об ответственности за преступления в сфере компьютерной информации (гл. 28), включенные в разд. IX «Преступления против общественной безопасности и общественного порядка». Такой подход подтверждает стремление законодателя адекватно отразить потребности общества в уголовно-правовой охране информационных отношений [2, с. 635].

Уголовно-правовое обеспечение информационных отношений в современных условиях является одним из важнейших направлений деятельности субъектов уголовной политики [3]. Неслучайно за последнее время преступные элементы стали активно использовать средства коммуникации и массовой информации в своих противоправных целях. По различным оценкам, в мире получили возможность пользоваться Интернетом более четырех миллиардов лиц, в Российской Федерации количество пользователей превышает

87 млн. Доступность в использовании, мобильность и простота, оперативность, минимальность материальных затрат, быстрота и масштабы распространения информации, высокий уровень закрытости делают ее привлекательной для криминальных элементов [4, с. 237; 5, с. 4].

Глава 28 «Преступления в сфере компьютерной информации» в первоначальной редакции УК РФ включала в себя три статьи: «Неправомерный доступ к компьютерной информации» (ст. 272), «Создание, использование и распространение вредоносных программ для ЭВМ» (ст. 273), «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети» (ст. 274).

Продолжая законотворческую работу по совершенствованию нормы об ответственности за преступления в сфере компьютерной информации, законодатель внес изменение в названия ст. 273 и 274. В настоящее время они получили новую редакцию: «Создание, использование и распространение вредоносных компьютерных программ» (ст. 273 УК РФ); «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей» (ст. 274 УК РФ) [6].

Одновременно с этим законодатель внес изменение в диспозиции указанных статей, а также включил две новые статьи об ответственности: за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ) [7], нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования (ст. 274.2 УК РФ) [8].

Таким образом, в указанных статьях содержится описание шестнадцати составов преступлений. В частности, в ст. 272 УК РФ – четыре состава преступления, ст. 273 УК РФ – три, ст. 274 УК РФ – два, ст. 274.1 УК РФ – пять и ст. 274.2 УК РФ – два.

С учетом квалифицированных видов из числа преступлений в сфере компьютерной информации (16 составов) шесть деяний относятся к числу преступлений небольшой тяжести (ч. 1, 2, 3 ст. 272, ч. 1 ст. 274, ч. 1, 2 ст. 274.2 УК РФ), четыре средней тяжести (ч. 1, 2 ст. 273, ч. 2 ст. 274, ч. 1 ст. 274.1 УК РФ) и шесть тяжкие (ч. 4 ст. 272, ч. 3 ст. 273, ч. 2, 3, 4, 5 ст. 274.1 УК РФ).

Применение такого юридико-технического приема конструирования составов преступлений позволило более точно установить степень общественной опасности посягательств, личности виновного и, исходя из этого, дифференцировать ответственность.

Вносимые в конструкции статей юридико-технические изменения законодатель снабдил тремя примечаниями. Так, в ст. 272 в примечании 1 сформулировано понятие компьютерной информации, под которой понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

В примечании 2 определены стоимостные критерии, позволяющие установить причиненный вред в результате совершения преступления (крупным ущербом признается ущерб, сумма которого превышает один миллион рублей). Одновременно с этим в примечании к ст. 274.2 УК РФ законодатель сформулировал дефиницию должностного лица [9].

Включенные в уголовный закон юридико-технические новации нельзя признать совершенными, отвечающими требованиям, предъявляемым к конструированию криминообразующих признаков, в связи с чем они породили следующие проблемы в их применении.

1. Проблемы использования понятия «должностное лицо». Согласно уголовно-правовой доктрине субъектом преступления признается лицо, обладающее юридически закре-

пленными в законе признаками: во-первых, совершенное деяние должно быть запрещено уголовным законом и обладать общественной опасностью; во-вторых, лицо, совершившее общественно опасное деяние, должно быть способно нести уголовную ответственность.

В ст. 19 УК РФ уголовную ответственность законодатель связывает с тремя обязательными признаками: физическое лицо, возраст, вменяемость. В некоторых случаях, кроме указанных выше признаков, характеризующих субъект преступления, он может обладать дополнительными признаками, влияющими на квалификацию совершенного лицом деяния.

Признаки специального субъекта в конструкциях диспозиций довольно часто закрепляются в уголовно-правовых нормах, где устанавливаются дополнительные признаки субъекта, включая ответственность должностных лиц.

Однако, несмотря на указанные выше положения, в ряде случаев принятые законодательные решения следует признать юридически не вполне обоснованными с точки зрения законодательной техники, противоречащими правовой логике, что ставит их под сомнение. Все это в полной мере следует отнести к установлению уголовной ответственности за преступления в сфере компьютерной информации должностного лица.

В первоначальной редакции законодатель в УК РФ выделил две группы субъекта преступления: должностное лицо и лицо, выполняющее управленческие функции в коммерческой и иной организации. Так, согласно примечаниям 1–4 к ст. 285 УК РФ «Злоупотребление должностными полномочиями» законодатель сформулировал дефиниции должностного лица применительно к лицу, занимающему государственные должности Российской Федерации, занимающему государственные должности субъекта Российской Федерации, а также государственных служащих и служащих в органах местного самоуправления.

Одновременно с этим в примечании 1 к ст. 201 УК РФ «Злоупотребление полномочиями» дано определение лицу, выполняющему управленческие функции в коммерческой и иной организации. Такой подход в конструировании признаков специальных субъектов позволил четко провести их разграничение исходя их выполнения ими служебных обязанностей в различных юридических образованиях.

Федеральным законом от 14.07.2022 № 260-ФЗ законодатель включил в УК РФ ст. 274.2, в которой предусмотрел ответственность за нарушение порядка установки, эксплуатации и модернизации в сети связи, технических средств, противодействию угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования, либо несоблюдение технических условий их установки или требований к сетям связи при использовании указанных технических средств, совершенный *должностным лицом* (курсив наш. – *А. П.*) или *индивидуальным предпринимателем* (курсив наш. – *А. П.*), подвергнутыми административному наказанию за деяние, предусмотренное ч. 2 ст. 13.42 Кодекса Российской Федерации об административных правонарушениях». В примечании к ст. 274.2 УК РФ указывается, что «под должностным лицом в настоящей статье понимается лицо, постоянно, временно либо по специальному полномочию выполняющее управленческие, организационно-распорядительные или административно-хозяйственные функции в коммерческой или иной организации». В данном случае в примечании к ст. 274.2 УК РФ законодатель формулирует понятие должностного лица применительно к осуществлению выполняемой функции в коммерческой и иной организации, что противоречит ранее сформулированным положениям в примечании 1 к ст. 285 УК РФ.

Согласно примечанию 1 к ст. 285 УК РФ под должностным лицом понимается лицо, постоянно, временно либо по специальному полномочию осуществляющее функции предста-

вителя власти либо выполняющее организационно-распорядительные, административно-хозяйственные функции в государственных органах, органах местного самоуправления, государственных и муниципальных учреждениях, государственных внебюджетных фондах, государственных корпорациях, государственных компаниях, публично-правовых компаниях, на государственных и муниципальных унитарных предприятиях, в хозяйственных обществах, в высшем органе управления которых Российская Федерация, субъект Российской Федерации или муниципальное образование имеет право прямо или косвенно (через подконтрольных им лиц) распоряжаться более чем пятьюдесятью процентами голосов либо в которых Российская Федерация, субъект Российской Федерации или муниципальное образование имеет право назначать (избирать) единоличный исполнительный орган и (или) более пятидесяти процентов состава коллегиального органа управления, в акционерных обществах, в отношении которых используется специальное право на участие в Российской Федерации, субъектов Российской Федерации или муниципальных образований в управлении такими акционерными обществами («золотая акция»), а также в Вооруженных Силах Российской Федерации, других войсках и воинских формированиях Российской Федерации.

Кроме того, оно противоречит и примечанию 1 к ст. 201 УК РФ, в котором говорится о том, что «лицом, выполняющим управленческие функции в коммерческой или иной организации, за исключением организаций, указанных в п. 1 примечаний к статье 285 настоящего Кодекса, либо в некоммерческой организации, не являющимся государственным органом, органом местного самоуправления либо государственным или муниципальным учреждением, признается лицо, выполняющее функции единоличного исполнительного органа, либо члена совета директоров или иного коллегиального исполнительного органа, или лицо постоянно, временно либо по специальному полномочию, выполняющее организационно-распорядительные или административно-хозяйственные функции в этих организациях» [9].

Изложенное выше положение свидетельствует о допущенных юридико-технических ошибках в определении специального субъекта в указанных примечаниях. Примененный юридико-технический прием в конструировании общей и специальной уголовно-правовой нормы свидетельствует о том, что специальная норма (ст. 274.2 УК РФ) не может содержать меньше криминообразующих признаков, чем общая (ст. 285 УК РФ).

Кроме того, возникает определенное сомнение в установлении ответственности и их несоразмерности в исследуемых статьях. Так, за совершение деяния, указанного в ст. 274.2 УК РФ, предусматривается наказание до трех лет лишения свободы, а в ст. 285 УК РФ – до четырех лет свободы.

На сегодняшний день законодатель не определил, кто именно признается в них должностным лицом, а кто – выполняющим управленческие функции в коммерческой или иной организации.

Решить возникшую проблему, по нашему мнению, позволит проведение унификации указанных понятий, используемых в ст. 201, 285 и 274.2 УК РФ.

2. Проблемы использования терминологического инструментария. Законодатель в процессе правотворческой деятельности при конструировании криминообразующих признаков диспозиции статей гл. 28 использует разнообразный терминологический инструментарий.

Важным при этом является исключение как юридико-технических, так и сущностно-содержательных ошибок, направленных на реализацию принципа унификации правовых

норм, то есть приведение их к единой форме. В процессе унификации как юридико-технического приема в уголовном законе обеспечивается единообразие конструирования уголовно-правовых положений, их четкость и строгость в описании, логичность, что позволяет упростить их, уменьшить в объеме. Все это будет способствовать правильному его применению, устранит неоправданные случаи дифференциации [10, с. 19–20].

Однако, несмотря на очевидность и бесспорность данных положений и на предпринимаемые меры, законодателю не удалось избежать ошибок. Примером может служить конструирование криминообразующих признаков в процессе законотворческой деятельности уголовно-правовых норм гл. 28 УК РФ, в частности терминов иностранного происхождения, таких как «блокирование», «модификация», «инфраструктура» и др., которые требуют в процессе применения определенности, ясности, доступности понимания сущностно-содержательных признаков, закрепленных в них [11, с. 116].

Такой юридико-технический прием при описании признаков противоправных деяний создает определенные трудности при квалификации преступлений в сфере компьютерной информации правоприменителем. При уяснении тех или иных многочисленных терминов, сущностно-содержательных признаков в конструкциях диспозиций у правоприменителя в процессе их реализации возникает потребность в их уяснении. Подтверждением этому могут служить понятия, их юридико-техническая характеристика, содержащиеся в статьях, определяющих ответственность за неправомерный доступ к компьютерной информации (ст. 272 УК РФ), создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ), неправомерное воздействие на критическую информационную инфраструктуру (ст. 274.1 УК РФ), нарушение правил централизованного управления техническими средствами, противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования (ст. 274.2 УК РФ). Например, «компьютерная программа», «несанкционированное уничтожение, блокирование, модификация, копирование компьютерной информации», «нейтрализация средств защиты компьютерной информации», «средства хранения, обработки или передачи охраняемой компьютерной информации», «критическая информационная инфраструктура Российской Федерации» и т. д.

Указанный правовой терминологический инструментарий законодателем по понятным причинам не определяется. По мнению некоторых ученых, правоприменитель вынужден обращаться к текстам комментариев к УК РФ, которые даются научными, практическими работниками, которые в большей своей части носят субъективный, порой и противоречивый, а в ряде случаев взаимоисключающий характер [12, с. 464]. Применение данного приема в конструировании не может служить улучшением понимания закона, повышением его качества и в конечном не усилит ее превентивную силу.

В этих условиях высшая судебная инстанция также не дает каких-либо толкований данных терминов, что в определенной степени влияет на качество и эффективность правоприменительной деятельности при квалификации преступлений в сфере компьютерной информации.

Обращение к нормативно-правовым актам не решает возникающих проблем. В частности, используемая в них терминология в сфере информационных отношений унифицирована недостаточно, а в ряде случаев носит противоречивый характер. Так, в Федеральном законе от 27.06.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» законодатель в различных вариантах использует термин "информация": это

сведения (сообщения, данные) независимо от форм их представления; «информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств»; информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

Однако в уголовном законодательстве используемые криминообразующие признаки трактуются по-разному. Так, в ст. 280 и 282 УК РФ данный криминообразующий признак сформулирован как с «*использованием средств массовой информации либо информационно телекоммуникационных сетей, в том числе сети "Интернет"*», а в ст. 280.1 УК РФ – *«с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей (включая сеть "Интернет")»* (выд. авт.). Примененный юридико-технический подход при формулировании криминообразующих признаков не только не свидетельствует о их единообразии, но и противоречит принципу унификации, что расширяет возможности его толкования в процессе правоприменительной деятельности.

Вызывают определенные затруднения толкование термина в использовании сети Интернет оборота в одном случае «*в том числе*», в другом «*включая*», что свидетельствует о лексических противоречиях. По мнению А. А. Бережного, во-первых, «в том числе» предполагает как наличие, так и отсутствие данного средства. «Включая» может указывать на его обязательное присутствие [13, с. 19]». Во-вторых, термин «электронные сети», примененный в качестве квалифицирующего признака в ч. 2 ст. 280.1 УК РФ, не включен ни в основной квалифицированный состав ст. 282 УК РФ, ни в качестве квалифицированного состава ч. 2 ст. 280, ни в качестве основного и квалифицированного состава ст. 282 УК РФ.

Решение возникших внутриотраслевых коллизий видится в унификации формулировок, охватывающих все признаки характеризующих данное явление. Полагаем, что законодателю следует внести изменения в редакцию указанных статей и изложить ее аналогично имеющимся в ст. 280 УК РФ: с использованием средств массовой информации либо электронных или телекоммуникационных сетей (включая сеть «Интернет»).

В свою очередь в Доктрине информационной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 05.12.2016 № 646, определен термин «информационная инфраструктура» как совокупность объектов информатизации, информационных систем, сайтов в сети «Интернет» и сетей связи, расположенных на территории Российской Федерации, а также на территориях, находящихся под юрисдикцией Российской Федерации или используемых на основании международных договоров Российской Федерации.

Уголовный кодекс Российской Федерации при регламентации ответственности преступлений в сфере компьютерной информации использует понятие «информационно-телекоммуникационная сеть», сфера компьютерной информации.

СПИСОК ИСТОЧНИКОВ

1. Кузнецов А. П. Ответственность за преступления в сфере компьютерной информации : учеб.-практ. пособие. Н. Новгород, 2007. С. 75.
2. Полный курс Уголовного права : в 5 т. / под ред. А. И. Коробеева. СПб., 2008. Т. 4. Преступления против общественной безопасности. 672 с.
3. Хасамова З. И. Об особенностях квалификации преступлений, совершаемых с использованием информационно-коммуникативных технологий // Общество и право. 2016. № 1 (55). С. 117–120.

4. Петрянин А. В. Концептуальные основы противодействия преступлениям экстремистской направленности: теоретико-прикладное исследование : дис. … д-ра юрид. наук. Н. Новгород, 2015. 490 с.
5. Летелкин Н. В. Уголовно-правовое противодействие преступлениям, совершаемым с использованием информационно-телекоммуникационных сетей, включая сети «Интернет» : дис. … канд. юрид. наук. Н. Новгород, 2018. 218 с.
6. О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации : федер. закон от 07.12.2011 № 420-ФЗ // Собр. законодательства Рос. Федерации. 2011. № 50. Ст. 7362.
7. О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» : федер. закон от 26.07.2017 № 194-ФЗ // Собр. законодательства Рос. Федерации. 2017. № 31 (ч. I). Ст. 4743.
8. О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации : федер. закон от 14.07.2022 № 260-ФЗ // Собр. законодательства Рос. Федерации. 2022. № 29 (ч. II). Ст. 5227.
9. О внесении изменений в статьи 201 и 285 Уголовного кодекса Российской Федераци : федер. закон от 24.02.2021 № 16-ФЗ // Собр. законодательства Рос. Федерации. 2021. № 9. Ст. 1463.
10. Кругликов Л. Л. Смирнова Л. Е. Унификация в уголовном праве. СПб., 2008. 310 с.
11. Кузнецов А. П. Бацин И. В. Негативные парадигмы конструирования норм главы 22 УК РФ // Юридическая наука и практика. Вестник Нижегородской академии МВД России. 2015. № 1 (29). С. 112–116.
12. Актуальные проблемы Особенной части Уголовного права : учеб. / отв. ред. И. А. Подройкина, С. И. Улеська. М., 2019. С. 464.
13. Бережной А. А. Информационная безопасность как объект уголовно-правовой охраны в области противодействия преступлениям экстремистской направленности // Уголовное право: стратегия развития в XXI веке : материалы XVI Междунар. науч.-практ. конф. М., 2019. С. 17–21.

REFERENCES

1. Kuznetsov A.P. *Otvetstvennost' za prestupleniya v sfere komp'yuternoi informatsii: ucheb.-prakt. posobie* [Responsibility for crimes in the field of computer information: textbook and practical guide]. Nizhny Novgorod, 2007. 127 p.
2. *Polnyi kurs Ugolovnogo prava: v 5 t. T. 4. Prestupleniya protiv obshchestvennoi bezopasnosti* [Complete course of criminal law: in 5 volumes. Volume 4. Crimes against public safety]. Ed. by Korobeev A.I. Saint Petersburg, 2008. 672 p.
3. Khasamova Z.I. On the specifics of qualifying crimes committed with the help of information and communication technologies. *Obshchestvo i pravo* = *Society and Law*, 2016, no. 1 (55), pp. 117–120. (In Russ.).
4. Petryanin A.V. *Kontseptual'nye osnovy protivodeistviya prestupleniyam ehkstremistskoi napravlennosti: teoretiko-prikladnoe issledovanie: dis. … d-ra yurid. nauk* [Conceptual foundations of countering extremist crimes: theoretical and applied research: Doctor of Sciences (Law) dissertation]. Nizhny Novgorod, 2015. 490 p.
5. Letelkin N.V. *Ugolovno-pravovoe protivodeistvie prestupleniyam, sovershaemym s ispol'zovaniem informatsionno-telekommunikatsionnykh setei, vklyuchaya seti "Internet": dis. … kand. yurid. nauk* [Criminal law counteraction to crimes committed using information and telecommunication networks, including the Internet: Candidate of Sciences (Law) dissertation]. Nizhny Novgorod, 2018. 218 p.
6. On Amendments to the Criminal Code of the Russian Federation and Certain Legislative Acts of the Russian Federation: Federal Law No. 420-FZ of December 7, 2011. In: *Sobr.*

zakonodatel'stva Ros. Federatsii [Collection of legislation of the Russian Federation]. 2011. No. 50. Art. 7,362. (In Russ.).
7. On Amendments to the Criminal Code of the Russian Federation and Article 151 of the Criminal Procedural Code of the Russian Federation in connection with the Adoption of the Federal Law "On the Security of the Critical Information Infrastructure of the Russian Federation": Federal Law No. 194-FZ of July 26, 2017. In: *Sobr. zakonodatel'stva Ros. Federatsii* [Collection of legislation of the Russian Federation]. 2017. No. 31 (Part I). Art. 4,743. (In Russ.).
8. On Amendments to the Criminal Code of the Russian Federation and the Criminal Procedural Code of the Russian Federation: Federal Law No. 260-FZ of July14, 2022. In: *Sobr. zakonodatel'stva Ros. Federatsii* [Collection of legislation of the Russian Federation]. 2022. No. 29 (Part II). Art. 5,227. (In Russ.).
9. On Amendments to Articles 201 and 285 of the Criminal Code of the Russian Federation: Federal Law No. 16-FZ of February 24, 2021. In: *Sobr. zakonodatel'stva Ros. Federatsii* [Collection of legislation of the Russian Federation]. 2021. No. 9. Art. 1,463. (In Russ.).
10. Kruglikov L.L., Smirnova L.E. *Unifikatsiya v ugolovnom prave* [Unification in criminal law]. Saint Petersburg, 2008. 310 p.
11. Kuznetsov A.P., Batsin I.V. Negative paradigms of designing of standards of Chapter 22 of the Criminal Code of the Russian Federation. *Yuridicheskaya nauka i praktika. Vestnik Nizhegorodskoi akademii MVD Rossii = Legal Science and Practice. Bulletin of the Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia*, 2015, no. 1 (29), pp. 112–116. (In Russ.).
12. *Aktual'nye problemy Osobennoi chasti Ugolovnogo prava: ucheb.* [Actual problems of the Special Part of Criminal Law: textbook]. Ed. by Podroikin I.A., Ules'k S.I. Moscow, 2019. 768 p.
13. Berezhnoi A.A. Information security as an object of criminal law protection in the field of countering extremist crimes. In: *Ugolovnoe pravo: strategiya razvitiya v XXI veke: materialy XVI Mezhdunar. nauch.-prakt. konf.* [Criminal law: development strategy in the 21st century: proceedings of the 16th International Scientific and Practice Conference]. Moscow, 2019. Pp. 17–21. (In Russ.).

СВЕДЕНИЯ ОБ АВТОРЕ / INFORMATION ABOUT THE AUTHOR

АЛЛА ВАЛЕРЬЕВНА ПЕЛЕВИНА – ассистент кафедры уголовного права и процесса юридического факультета Национального исследовательского Нижегородского государственного университета им. Н. И. Лобачевского, Нижний Новгород, Россия, allochka_90@bk.ru

ALLA V. PELEVINA – Assistant at the Department of Criminal Law and Procedure of the Law Faculty of the Lobachevsky State University of Nizhny Novgorod, Nizhny Novgorod, Russia, allochka_90@bk.ru

Статья поступила 05.10.2023