Дата поступления рукописи в редакцию: 20.03.2026 г.
Дата принятия рукописи в печать: 14.05.2026 г.
DOI: 10.24412/2224-9133-2026-4-325-329

ГАУЖАЕВА Виктория Александровна,
кандидат юридических наук, доцент кафедры информационных технологий и специальной техники органов внутренних дел Северо-Кавказского института повышения квалификации (филиал) Краснодарского университета МВД России,
e-mail: mail@law-books.ru

БЖИЕВ Роман Борисович,
кандидат юридических наук,
доцент института стоматологии и челюстно-лицевой хирургии ФГБОУ ВО «Кабардино-Балкарский государственный университет им. Х.М. Бербекова»,
e-mail: mail@law-books.ru

БОРИСОВА Мария Игоревна,
преподаватель кафедры тактико-специальной подготовки Волгоградской академии МВД России,
e-mail: mail@law-books.ru

ЦИФРОВИЗАЦИЯ ПРЕСТУПНОСТИ: ПРОБЛЕМЫ УГОЛОВНО-ПРАВОВОЙ КВАЛИФИКАЦИИ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ И ПЕРСПЕКТИВЫ РАЗВИТИЯ ЗАКОНОДАТЕЛЬСТВА

Аннотация. *В статье исследуются актуальные проблемы применения норм главы 28 Уголовного кодекса Российской Федерации, регламентирующих ответственность за преступления в сфере компьютерной информации. Автор анализирует судебную практику, выявляет коллизии и пробелы действующего законодательства в условиях стремительной цифровизации общественных отношений. Особое внимание уделяется проблемам разграничения смежных составов преступлений, определению предмета и объекта преступного посягательства, установлению причинно-следственной связи между противоправными действиями и наступившими последствиями. Автор обосновывает необходимость системного реформирования уголовно-правовых норм о киберпреступности с учетом международного опыта и современных технологических реалий. В работе формулируются конкретные предложения по совершенствованию законодательства, направленные на повышение эффективности противодействия преступлениям в цифровой среде.*

Ключевые слова: *киберпреступность, компьютерная информация, цифровизация, уголовно-правовая квалификация, информационная безопасность, вредоносные программы, несанкционированный доступ, уголовная ответственность, объект преступления, совершенствование законодательства.*

GAUZHAEVA Victoria Aleksandrovna,
Candidate of Law Associate Professor, Department of Information Technology and Specialized Equipment of the Internal Affairs Agencies, North Caucasus Institute for Advanced Training (branch) of the Krasnodar University of the Ministry of Internal Affairs of Russia

BZHIEV Roman Borisovich,
Candidate of Law Associate Professor, Institute of Dentistry and Maxillofacial Surgery, Kabardino-Balkarian State University named after Kh.M. Berbekova,

BORISOVA Maria Igorevna,
Instructor,
Department of Tactical and Special Training
Volgograd Academy of the Ministry of Internal Affairs of Russia

DIGITALIZATION OF CRIME: PROBLEMS OF CRIMINAL-LAW CLASSIFICATION OF COMPUTER-RELATED CRIMES AND PROSPECTS FOR LEGISLATION DEVELOPMENT

Annotation. *This article examines current issues in the application of Chapter 28 of the Criminal Code of the Russian Federation, which regulates liability for cybercrimes. The author analyzes judicial practice and identifies conflicts and gaps in current legislation in the context of the rapid digitalization of social relations. Particular attention is paid to distinguishing between related offenses, determining the subject and object of criminal offenses, and establishing a causal relationship between illegal actions and the resulting consequences. The author substantiates the need for a systemic reform of criminal law regulations on cybercrime, taking into account international experience and modern technological realities. The paper formulates specific proposals for improving legislation aimed at increasing the effectiveness of combating crimes in the digital environment.*

Key words: *cybercrime, computer information, digitalization, criminal law classification, information security, malware, unauthorized access, criminal liability, object of crime, legislative improvement.*

Современный этап развития общества характеризуется беспрецедентным уровнем проникновения цифровых технологий во все сферы жизнедеятельности человека. По данным Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации, уровень цифровизации экономики России к 2024 году достиг 28%, что обуславливает необходимость адекватной правовой защиты складывающихся общественных отношений [1]. В этой сфере образуются менее защищенные социальные группы, которые требуют дополнительной защиты и поддержки, в том числе правовыми методами.

Одновременно с расширением цифрового пространства наблюдается трансформация преступности: традиционные криминальные практики переносятся в виртуальную среду, возникают принципиально новые способы совершения общественно опасных деяний, демонстрируя уверенный рост [2].

Действующее уголовное законодательство, несмотря на регулярные изменения и дополнения, не всегда успевает адаптироваться к стремительно меняющимся реалиям. Глава 28 Уголовного кодекса Российской Федерации (далее – УК РФ) «Преступления в сфере компьютерной информации» (статьи 272-274.2) была введена в 1996 году и с тех пор претерпела существенные изменения, однако многие проблемы правоприменения остаются нерешенными.

Ключевой теоретической проблемой остается определение родового и непосредственного объекта преступлений этой группы. По этому вопросу нет единого мнения. Часть исследователей полагает, что объектом выступают общественные отношения в сфере обеспечения безопасности информации и систем ее обработки [3, с.303]. Другие ученые акцентируют внимание на общественных отношениях по безопасному использованию компьютерной информации [4, с.454].

Мы склоняемся к мнению, что это те отношения, которые обеспечивают безопасность информационной среды и информационных систем. Такой подход согласуется с положениями Доктрины информационной безопасности Российской Федерации и позволяет более точно определить специфику посягательств в цифровой сфере.

Не менее дискуссионным является вопрос о предмете преступного посягательства. Законодатель использует термин «компьютерная информация», определяя ее в примечании к статье 272 УК РФ как информацию на машинном носителе, в электронно-вычислительной машине (далее - ЭВМ), системе ЭВМ или их сети. Однако данное определение не учитывает современные технологические реалии: облачные хранилища, распределенные системы, технологии блокчейн и т.д. [5, с.5-17].

Правоприменительная практика сталкивается с трудностями при квалификации деяний, связанных с воздействием на информацию, размещенную в облачных сервисах, принадлежащих иностранным компаниям, или при посягательствах на децентрализованные системы. Данная проблема требует законодательного решения путем расширения понятия компьютерной информации с учетом современных форм ее существования и хранения.

Статья 272 УК РФ устанавливает ответственность за неправомерный доступ к охраняе-

мой законом компьютерной информации. Анализ судебной практики демонстрирует существенные расхождения в толковании признаков состава данного преступления.

Во-первых, проблематичным является установление момента окончания преступления. Судебная практика исходит из того, что преступление окончено с момента получения лицом возможности ознакомиться с охраняемой законом информацией или распорядиться ею [6]. Однако при этом не учитывается, что современные системы защиты информации фиксируют многочисленные попытки несанкционированного доступа, которые автоматически блокируются. Возникает вопрос: следует ли квалифицировать такие действия как покушение на преступление или как оконченное деяние, если технически доступ был осуществлен, но информация не была получена в результате срабатывания защитных механизмов?

Во-вторых, сложности вызывает разграничение неправомерного доступа к компьютерной информации и смежных составов преступлений. Как справедливо отмечает А.В. Наумов, нередко одни и те же действия могут быть квалифицированы и по статье 272 УК РФ, и по статьям о хищении, нарушении неприкосновенности частной жизни и другим нормам [7, с.603]. Правоприменитель должен руководствоваться правилами квалификации при конкуренции норм, однако отсутствие четких разъяснений Пленума Верховного Суда РФ по данной категории дел порождает противоречивую практику.

В-третьих, дискуссионным остается вопрос об уголовной ответственности за использование стандартных учетных данных (логин/пароль), установленных производителем оборудования или программного обеспечения и не измененных пользователем. Некоторые суды признают такие действия неправомерным доступом, другие указывают на отсутствие преодоления системы защиты информации. Представляется необходимым законодательное закрепление понятия «преодоление системы защиты информации» для унификации судебной практики.

Статья 273 УК РФ предусматривает ответственность за создание, распространение или использование вредоносных компьютерных программ. Диспозиция данной нормы вызывает множество вопросов у правоприменителя.

Законодатель определяет вредоносные программы как программы, заведомо предназначенные для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты. Однако в современных условиях существует значительное количество программного обеспечения двойного назначения: инструменты тестирования на проникновение, программы для аудита информационной безопасности, средства удаленного администрирования и т.д. [8, с.54].

Правоприменительная практика сталкивается с необходимостью разграничения легитимного использования таких программ специалистами в области информационной безопасности и противоправной деятельности. Критерием должна выступать цель использования, однако установление субъективной стороны в таких делах представляет значительную сложность.

Кроме того, современные технологии позволяют создавать программы, которые формально не подпадают под определение вредоносных, но фактически причиняют существенный вред. Например, программы-майнеры, использующие вычислительные ресурсы чужих компьютеров без согласия их владельцев, или программы для DDoS-атак, построенные на принципе распределенных вычислений. Требуется расширение перечня признаков вредоносности программ с учетом новых технологических угроз [9, с.45-55].

Статья 274 УК РФ устанавливает ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования. Данная норма применяется крайне редко, что обусловлено целым рядом причин.

Во-первых, законодатель не конкретизирует, какие именно правила имеются в виду. В различных организациях действуют различные внутренние регламенты, стандарты, инструкции, что создает неопределенность бланкетной диспозиции. Как отмечается в юридической литературе, отсылка к неопределенному кругу нормативных актов и локальных документов противоречит принципу правовой определенности [10].

Во-вторых, установление причинно-следственной зависимости нарушением и наступившими последствиями возможно только экспертным путем со сложностями, связанными с методическим обеспечением этой деятельности.

В-третьих, субъектом данного преступления является лицо, имеющее доступ к средствам хранения, обработки или передачи охраняемой компьютерной информации. Однако законодатель не уточняет характер такого доступа (правомерный или неправомерный), что порождает споры в доктрине и правоприменительной практике.

Анализ зарубежного законодательства демонстрирует различные подходы к криминализации деяний в информационной сфере. Будапештская конвенция о киберпреступности 2001 года, к которой Российская Федерация не присоединилась, но положения которой активно

используются в международной практике, содержит более детальную классификацию компьютерных преступлений [11], что позволяет более дифференцированно подходить к установлению уголовной ответственности.

Законодательство Германии содержит специальные составы преступлений, связанных с компьютерным саботажем, шпионажем данных, фишингом. Уголовный кодекс Франции предусматривает ответственность за изготовление, продажу, хранение оборудования, программ или данных, предназначенных для совершения преступлений в информационной сфере. Этот опыт может использоваться в нашей законодательной практике в части, не противоречащей действующему законодательству [12, с.160-165].

На основании проведенного исследования представляется необходимым сформулировать наши предложения по вопросам совершенствования уголовно-правового регулирования ответственности за преступления в сфере компьютерной информации:

1. Расширить понятие «компьютерная информация» в примечании к статье 272 УК РФ, включив в него информацию, содержащуюся в распределенных информационных системах, облачных хранилищах и иных формах цифрового представления данных независимо от места физического расположения носителя.
2. Дополнить главу 28 УК РФ статьей об ответственности за организацию и проведение DDoS-атак, которые в настоящее время квалифицируются по различным нормам в зависимости от наступивших последствий, что не способствует единообразию практики.
3. Ввести в УК РФ норму об ответственности за незаконный оборот средств и программ, предназначенных для осуществления несанкционированного доступа к компьютерной информации.
4. Конкретизировать понятие «преодоление системы защиты информации» путем введения соответствующего примечания к статье 272 УК РФ, что позволит унифицировать судебную практику по делам о неправомерном доступе.
5. Внести изменения в статью 274 УК РФ, уточнив характер нарушаемых правил и установив, что речь идет о правилах, определенных федеральными законами, подзаконными нормативными актами или обязательными к применению стандартами.
6. Рассмотреть возможность введения в УК РФ специальной нормы об уголовной ответственности за компьютерное мошенничество как самостоятельного состава преступления, отличного от мошенничества в общем смысле, учитывая специфику способа совершения и характер причиняемого вреда.

Изучение уголовного законодательства, регламентирующего ответственность за деяния этой группы, приводит к выводу о необходимости продолжения его модернизации. Темпы цифровизации общества опережают развитие правовой базы и влекут сложности в противодействии киберпреступности. Сказываются и другие факторы, ключевым из которых выступает недостаток специалистов в этой сфере в сочетании с низким уровнем материально-технического обеспечения подразделений и сотрудников правоохранительных органов.

Основные проблемы правоприменения связаны с недостаточной определенностью ключевых понятий (компьютерная информация, вредоносная программа, преодоление системы защиты), сложностью разграничения смежных составов преступлений, отсутствием детальных разъяснений высших судебных инстанций по вопросам квалификации.

Эффективность правового регулирования в значительной степени зависит от преодоления выявленных проблем: устранения пробелов в квалификации киберпреступлений, развития международного сотрудничества, совершенствования механизмов защиты прав потерпевших. Дальнейшее развитие законодательства должно осуществляться с учётом баланса между обеспечением безопасности финансовых операций и сохранением доступности финансовых услуг, а также с соблюдением прав и свобод граждан в цифровой среде.

Перспективы дальнейших исследований связаны с разработкой концепции уголовно-правовой охраны информационной безопасности в условиях развития искусственного интеллекта, квантовых вычислений и других прорывных технологий, которые неизбежно потребуют переосмысления традиционных подходов к определению объекта, предмета и субъекта преступлений в цифровой среде и повлекут изменения в структуре и динамике преступности в разной степени в различных регионах страны.

Список литературы:

[1] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 29.12.2025) // Собрание законодательства РФ. 1996. № 25. Ст. 2954.

[2] Состояние преступности в России за январь-декабрь 2024 года. М.: ГИАЦ МВД России, 2025. - 52 с.

[3] Уголовное право. Общая часть: учебник для вузов / ответственные редакторы А. В. Нау-

мов, А. Г. Кибальник. - 6-е изд., перераб. и доп. – М.: Издательство Юрайт, 2025. - 448 с.

[4] Комментарий к Уголовному кодексу Российской Федерации / под ред. А.И. Рарога. М.: Проспект, 2023.- 912 с.

[5] Талапина Э.В. Право и цифровизация: новые вызовы и перспективы // Журнал российского права. 2018. № 2. С. 5-17.

[6] Обзор судебной практики Верховного Суда Российской Федерации №2 (2019) (утв. Президиумом Верховного Суда РФ 17.07.2019) // Бюллетень Верховного Суда РФ. 2020. № 3.

[7] Наумов А.В. Практика применения Уголовного кодекса Российской Федерации: комментарий судебной практики и доктринальное толкование / под ред. Г.М. Резника. М.: Волтерс Клувер, 2005. - 926 с.

[8] Степанов-Егиянц В.Г. Ответственность за преступления против компьютерной информации по уголовному законодательству России: монография. М.: Статут, 2018. - 238 с.

[9] Номоконов В.А., Тропина Т.Л. Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра. 2012. № 1 (24). С.45-55.

[10] Ежова Е.В., Зимасова А.А. Соблюдение принципа правовой определенности при применении бланкетной нормы в уголовном праве как важная гарантия обеспечения конституционных прав человека // Вестник СГЮА. 2025. №1 (162). URL: https://cyberleninka.ru/article/n/soblyudenie-printsipa-pravovoy-opredelennosti-pri-primenenii-blanketnoy-normy-v-ugolovnom-prave-kak-vazhnaya-garantiya (дата обращения: 05.11.2025).

[11] Convention on Cybercrime (Budapest, 23.11.2001) // European Treaty Series. No. 185.

[12] Локнов А.И. Уголовно-правовая оценка неправомерного доступа к компьютерной информации // Уголовное законодательство: вчера, сегодня, завтра: материалы ежегодной международной научно-практической конференции, Санкт-Петербург, 09-10 июня 2023 года. СПб: Санкт-Петербургский университет Министерства внутренних дел Российской Федерации, 2023. С. 160-165.

References:

[1] The Criminal Code of the Russian Federation of 13.06.1996 No. 63-FZ (as amended on 29.12.2025) //Collection of Legislation of the Russian Federation. 1996. № 25. Art. 2954.

[2] The state of crime in Russia in January-December 2024. M.: GIAC Ministry of Internal Affairs of Russia, 2025. - 52 s.

[3] Criminal law. General part: textbook for universities/responsible editors A. V. Naumov, A. G. Kibalnik. - 6th ed., Revised. and add. - M.: Yuright Publishing House, 2025. - 448 s.

[4] Commentary to the Criminal Code of the Russian Federation/ed. A.I. Raroga. M.: Prospect, 2023.- 912 p.

[5] E.V. Talapina. Law and Digitalization: New Challenges and Prospects//Journal of Russian Law. 2018. № 2. S. 5-17.

[6] Review of judicial practice of the Supreme Court of the Russian Federation No. 2 (2019) (approved by Presidium of the Supreme Court of the Russian Federation 17.07.2019) //Bulletin of the Supreme Court of the Russian Federation. 2020. № 3.

[7] A.V. Naumov. Practice of application of the Criminal Code of the Russian Federation: commentary on judicial practice and doctrinal interpretation/ed. G.M. Reznik. M.: Wolters Kluver, 2005. - 926 p.

[8] Stepanov-Egiyants V.G. Responsibility for crimes against computer information under the criminal legislation of Russia: monograph. M.: Statute, 2018. - 238 p.

[9] Nomokonov VA, Tropina TL Cybercrime as a new criminal threat//Criminology: yesterday, today, tomorrow. 2012. № 1 (24). S.45-55.

[10] Yezhova E.V., Zimasova A.A. Observance of the principle of legal certainty when applying the blanket norm in criminal law as an important guarantee of ensuring constitutional human rights//Vestnik SSLA. 2025. №1 (162). URL: https://cyberleninka.ru/article/n/soblyudenie-printsipa-pravovoy-opredelennosti-pri-primenenii-blanketnoy-normy-v-ugolovnom-prave-kak-vazhnaya-garantiya (дата обращения: 05.11.2025).

[11] Convention on Cybercrime (Budapest, 23.11.2001) // European Treaty Series. No. 185.

[12] Loknov A.I. Criminal law assessment of illegal access to computer information//Criminal law: yesterday, today, tomorrow: materials of the annual international scientific and practical conference, St. Petersburg, June 09-10, 2023. St. Petersburg: St. Petersburg University of the Ministry of Internal Affairs of the Russian Federation, 2023. S. 160-165.