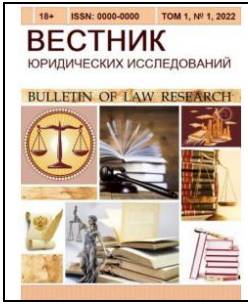

*Научно-исследовательский журнал «**Вестник юридических исследований / Bulletin of Law Research**»*
https://blr-journal.ru
2025, Том 4, № 3 / 2025, Vol. 4, Iss. 3 https://blr-journal.ru/archives/category/publications
Научная статья / Original article
УДК 343.983

Цифровые преступления: проблемы квалификации и ответственности

[1] Гереев З.Г., [1] Киселева Т.А., [1] Далоев А.Т.,
[1] Ростовский институт, филиал Всероссийского государственного университета юстиции (РПА Минюста России)

Аннотация: в статье рассматриваются актуальные проблемы квалификации и ответственности за цифровые преступления в российском законодательстве в условиях повсеместного развития информационных технологий. Подчеркивается, что стремительное развитие технологий создает значительные трудности для квалификации таких деяний и привлечения виновных к ответственности, что подтверждается международной статистикой о росте киберпреступности. Рассматривается правовое регулирование цифровой преступности, основанное на международных соглашениях в рамках ООН и СНГ, а также нормы уголовного законодательства Российской Федерации, в частности статьи 159.6 и 272 УК РФ. Детально анализируются проблемы квалификации мошенничества в сфере компьютерной информации, в том числе при фишинговых атаках, где возникает неопределенность в разграничении составов общего мошенничества и мошенничества в сфере компьютерной информации. Приводится пример из судебной практики, иллюстрирующий данную проблему. В статье указаны проблемы квалификации, как сложность установления причинно-следственной связи между действиями виновного и наступившими последствиями, особенно при наличии множественных факторов, а также трудности, возникающие при квалификации преступлений, совершаемых с использованием новых технологий, требующих постоянного обновления законодательства. Отдельное внимание уделяется проблеме квалификации трансграничных преступлений и необходимости международного сотрудничества в данной сфере. В качестве дополнительных мер предлагается усиление образовательной работы, пересмотр судебной практики с акцентом на фактический вред от цифровых преступлений и создание специализированного национального агентства по борьбе с цифровой преступностью.

Ключевые слова: цифровые преступления, квалификация, ответственность, мошенничество в сфере компьютерной информации, киберпреступность, информационные технологии

Для цитирования: Гереев З.Г., Киселева Т.А., Далоев А.Т. Цифровые преступления: проблемы квалификации и ответственности // Вестник юридических исследований. 2025. Том 4. № 3. С. 97 – 105.

Поступила в редакцию: 9 февраля 2025 г.; Одобрена после рецензирования: 6 апреля 2025 г.; Принята к публикации: 22 мая 2025 г.

Digital crimes: problems of qualification and responsibility

[1] Gereev Z.G., [1] Kiseleva T.A., [1] Daloev A.T.,
[1] Rostov Institute branch of the All-Russian State University of Justice (RPA of the Ministry of Justice of Russia)

Abstract: the article examines current problems of qualification and responsibility for digital crimes in Russian legislation in the context of the widespread development of information technology. It is emphasized that the rapid

development of technology creates significant difficulties for the qualification of such acts and bringing the perpetrators to justice, which is confirmed by international statistics on the growth of cybercrime. The legal regulation of digital crime at the international and national levels is considered, including international agreements within the UN and the CIS, as well as the norms of the criminal legislation of the Russian Federation, in particular Articles 159.6 and 272 of the Criminal Code of the Russian Federation. The problems of qualification of fraud in the field of computer information are analyzed in detail, including in phishing attacks, where there is uncertainty in the distinction between the elements of general fraud and fraud in the field of computer information. An example from judicial practice is given illustrating this problem. The article identifies the problems of qualification, such as the difficulty of establishing a causal relationship between the actions of the perpetrator and the consequences that have occurred, especially in the presence of multiple factors, as well as the difficulties that arise when qualifying crimes committed using new technologies that require constant updating of legislation. Special attention is paid to the problem of qualifying cross-border crimes and the need for international cooperation in this area. As additional measures, it is proposed to strengthen educational work, revise judicial practice with an emphasis on the actual harm from digital crimes and create a specialized national agency to combat digital crime.

Keywords: digital crimes, qualification, liability, fraud in the field of computer information, cybercrime, information technology

For citation: Gereev Z.G., Kiseleva T.A., Daloev A.T. Digital crimes: problems of qualification and responsibility. Bulletin of Law Research. 2025. 4 (3). P. 97 – 105.

The article was submitted: February 9, 2025; Approved after reviewing: April 6, 2025; Accepted for publication: May 22, 2025.

Введение

Развитие информационных технологий и повсеместное проникновение цифровой среды в различные сферы общественной жизни порождают новые виды противоправных деяний, получивших общее название «цифровые преступления». Данные деяния представляют собой серьезную угрозу для безопасности личности, общества и государства, что обуславливает необходимость их эффективного правового регулирования. Однако квалификация и привлечение к ответственности за цифровые преступления сопряжены с рядом специфических проблем, требующих детального изучения и поиска оптимальных решений в рамках российского законодательства.

Одним из вопросов является определение самого понятия «цифровое преступление» в российском праве. Несмотря на отсутствие легального закрепления данного термина, под ним принято понимать противоправные деяния, совершаемые с использованием информационно-коммуникаци-онных технологий, компьютерной техники и сети Интернет, направленные против информационной безопасности, собственности, личности и других охраняемых законом объектов. К наиболее распространенным видам цифровых преступлений относятся неправомерный доступ к компьютерной информации, создание, использование и распространение вредоносных программ, мошенничество в сфере компьютерной информации, нарушение авторских и смежных прав в цифровой среде, а также кибербуллинг и распространение запрещенной информации.

Борьба с цифровой преступностью является главным приоритетом внутренней политической безопасности, однако стремительное развитие технологий создает серьезные проблемы для квалификации таких деяний и привлечения виновных к ответственности. Международные статистические данные свидетельствуют о неуклонном росте киберпреступности [13]. Так, в 2023 году на Тайване было зарегистрировано 35 000 случаев мошенничества, а имущественные потери достигли 8,878 млрд. долл. США. Только в августе 2024 года сумма мошенничества составила 137 млн. долл. США, что превышает общую сумму за весь предыдущий год [12]. В настоящее время до 60% дел, расследуемых местными прокуратурами и судами, связаны с цифровой преступностью, что подчеркивает масштаб проблемы и нагрузку на правоохранительную систему.

Международные тенденции также указывают на эскалацию цифровой преступности. Например, в США количество случаев мошенничества с кредитными картами увеличилось на 53% с 2020 по 2023 год. В Европейском союзе объем мошенничества с кредитными картами достиг 1,53 млрд евро, причем 84% пришлось на онлайн-мошенничество. В Великобритании в период с 2011 по 2020 год мошенничество с платежами по кредитным картам выросло на 68%, а количество жертв онлайн-мошенничества превысило 1,2 млрд фунтов стерлингов [12]. Данные демонстрируют, что мошенничество, совершаемое с использованием

цифровых сетей, представляет собой не только серьезную проблему, но и устойчивую международную преступную тенденцию, требующую адекватных мер реагирования.

Текущая ситуация с неконтролируемой цифровой преступностью, с точки зрения криминологии, может быть охарактеризована как ситуация «социального беспорядка», в которой существующая система социальных норм оказывается недостаточной для регулирования поведения в цифровой среде. Это приводит к ослаблению социального контроля и способствует распространению преступной активности. Однако, помимо вопросов социального контроля, остро стоят проблемы квалификации цифровых преступлений и определения ответственных лиц.

Е.А. Русскевич отмечает, что цифровая преступность часто возникает в периоды трансформации социальной структуры, включая переход к информационному и современному цифровому обществу [8]. Новые трансформации создают возможности для преступников и одновременно порождают сложности для правоохранительных органов. Одной из проблем является квалификация новых видов преступлений, которые не всегда вписываются в существующие правовые рамки.

Кроме того, определение ответственности в цифровой среде представляет собой серьезный вызов. Анонимность в интернете, использование сложных технических средств для совершения преступлений, а также трансграничный характер многих киберпреступлений существенно осложняют идентификацию и привлечение к ответственности виновных. Возникают вопросы о юрисдикции, о сотрудничестве между правоохранительными органами разных стран, а также об ответственности провайдеров интернет-услуг и платформ за действия пользователей.

Таким образом, борьба с цифровой преступностью требует не только усиления мер по предотвращению и пресечению таких деяний, но и совершенствования законодательства, разработки четких критериев квалификации различных видов цифровых преступлений, а также развития механизмов установления и привлечения к ответственности лиц, их совершающих. Только комплексный подход, учитывающий как технические, так и правовые аспекты проблемы, поможет эффективно противостоять растущей угрозе цифровой преступности.

Материалы и методы исследований

В рамках данного исследования проблем квалификации и ответственности за цифровые преступления в российском законодательстве применялся комплексный методологический подход. Основу исследования составил анализ действующих норм УК РФ (ст. 159, 159.6, 272, 273 и др.), регламентирующих ответственность за преступления в сфере информационных технологий. Проведен анализ научной и юридической литературы, посвященной вопросам квалификации и ответственности за киберпреступления. Особое внимание уделялось изучению судебной практики по уголовным делам о цифровых преступлениях с целью выявления проблем правоприменения и тенденций судебных решений.

Результаты и обсуждения

Правовое регулирование цифровой преступности основано на международных соглашениях, так и российском законодательстве, направленном на противодействие данному виду противоправной деятельности [4]. На международном уровне вопросы борьбы с цифровой преступностью обсуждаются в рамках Организации Объединенных Наций, и нашло отражение в Докладе XI Конгресса ООН по предупреждению преступности и уголовному правосудию, состоявшемся в Бангкоке в 2005 году [1]. Данный документ подчеркивает необходимость международного сотрудничества и обмена информацией между государствами для эффективного противодействия транснациональным формам киберпреступности. Развитие сотрудничества в этой сфере также является предметом Соглашения между правительствами государств – членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности, заключенного в 2009 году [9]. Данное соглашение направлено на координацию усилий стран-участниц в борьбе с угрозами в информационном пространстве, а также преступления, совершаемые с использованием информационных технологий.

В рамках Содружества Независимых Государств также предпринимаются шаги по гармонизации законодательства и налаживанию взаимодействия в сфере противодействия цифровой преступности. Об этом свидетельствуют Соглашение о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере компьютерной информации и Соглашение о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере информационных технологий [10, 11]. Указанные документы определяют основные направления сотрудничества между странами СНГ в выявлении, пресечении и расследовании преступлений, связанных с использованием информационных технологий, а также обмен опытом и проведение совместных операций.

Несмотря на наличие ряда международных соглашений, в научном сообществе отмечается отсутствие единого комплексного подхода к определению понятия «цифровые преступления», что затрудняет унификацию правового регулирования на глобальном уровне. Как отмечается в Руководстве для дискуссий, подготовленном в рамках Четырнадцатого Конгресса ООН по предупреждению преступности и уголовному правосудию, разнообразие технологических средств, используемых при совершении преступлений, порождает различные классификации и определения в доктрине уголовного права [7].

В России правовое регулирование цифровой преступности осуществляется посредством соответствующих норм в уголовное законодательство. В Российской Федерации, как следует из упоминания УК РФ, ответственность за преступления в сфере компьютерной информации, а также мошенничество, предусмотрена отдельными статьями [4]. При этом отмечается тенденция к расширению перечня деяний, признаваемых преступными в связи с развитием новых технологий, таких как беспилотные транспортные средства и искусственный интеллект, которые могут быть использованы в преступных целях, что требует постоянной адаптации правовых норм к возникающим угрозам.

Статья 159.6 УК РФ устанавливает ответственность за мошенничество в сфере компьютерной информации, то есть хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

Несмотря на наличие специальной нормы, квалификация мошенничества в сфере компьютерной информации сопряжена с рядом проблем, обусловленных как спецификой предмета преступления (компьютерная информация), так и динамичностью развития информационных технологий. Рассмотрим основные проблемы квалификации ст. 159.6 УК АРФ.

Основным отличием ст. 159.6 УК РФ от общего состава мошенничества (ст. 159 УК РФ) является способ совершения преступления. Если общее мошенничество предполагает обман или злоупотребление доверием, то мошенничество в сфере компьютерной информации совершается посредством манипуляций с компьютерной информацией или вмешательства в работу информационных систем. На практике бывает сложно провести четкую границу между этими составами. Например, при фишинге потерпевший добровольно передает свои данные, введенный в заблуждение ложным сообщением (классический обман) [5]. Однако для получения доступа к этим данным преступник использует компьютерную информацию и информационно-телекоммуникационные сети. Возникает вопрос: квалифицировать ли это как общее мошенничество или как мошенничество в сфере компьютерной информации? Судебная практика по данному вопросу не всегда единообразна, что создает неопределенность при квалификации.

Например, В 2012 году Чертановским районным судом города Москвы указанные лица были признаны виновными в хищении 13 миллионов рублей и приговорены к условному лишению свободы сроком на шесть лет с испытательным сроком в пять лет, однако до истечения испытательного срока совершили новые преступления. Но злоумышленники не стали ждать окончания условного срока и продолжили фишинговую деятельность. Савеловским районным судом города Москвы был вынесен обвинительный приговор в отношении братьев Евгения и Дмитрия Попелышей, а также их соучастников, признанных виновными в совершении кибермошенничества. Согласно судебному решению, братья Попелыши были приговорены к восьми годам лишения свободы с отбыванием наказания в исправительной колонии общего режима, а также к штрафу в размере 900 тысяч рублей каждый. Пресс-секретарем суда было сообщено, что остальные фигуранты уголовного дела получили наказание в виде лишения свободы на срок от четырех с половиной до шести лет и штрафы в размере до 700 тысяч рублей, за исключением одного лица, которому было назначено условное осуждение с последующей амнистией и снятием судимости [6].

Установлено, что преступные действия квалифицированы по ч. 2 ст. 273, ч. 3 ст. 272 и ч. 4 ст. 159.6 УК РФ, предусматривающих ответственность за создание, использование и распространение вредоносных компьютерных программ, неправомерный доступ к компьютерной информации и мошенничество в сфере компьютерной информации, совершенное органи-зованной группой либо в особо крупном размере. Следствием было установлено, что Попелыши использовали фишинговые методы для получения аутентификационных данных от личных кабинетов клиентов российских кредитных организаций. Злоумышленники осуществляли распространение вредоносного программного обеспечения, которое обеспечивало перенаправ-ление пользователей на фиктивные веб-страницы, имитирующие формы ввода конфиденциальной информации. В дальнейшем соучастники преступной группы осуществляли телефонные звонки потерпевшим, представляясь сотрудниками банков и убеждая их сообщать коды подтверждения банковских операций.

В ходе судебного разбирательства было установлено, что под руководством братьев Попелышей действовала организованная преступ-ная группа, включавшая лиц, ответственных за осуществление телефонных звонков, распростра-нение вредоносных программ, разработку и модернизацию вредоносного программного обеспечения, а также лиц, занимавшихся обналичиванием похищенных денежных средств. В результате преступной деятельности, осуществлявшейся с марта 2013 года по май 2015 года, банде удалось получить доступ к приблизительно семи тысячам банковских счетов и вывести более 12,5 миллионов рублей. При задержании обвиняемые предприняли попытку уничтожить вещественные доказательства, однако их действия были пресечены. Несмотря на представленные стороной обвинения доказательства, защита подсудимых настаивала на их невиновности, указывая на отдельные обстоятельства, вызывающие сомнения в обоснованности обвинения. Следует отметить, что братья Попелыши и один из их соучастников ранее уже привлекались к уголовной ответственности за совершение аналогичных преступлений в сфере компьютерной информации.

Как уже упоминалось, квалификация фишинга может быть неоднозначной. Некоторые суды квалифицируют его по ст. 159 УК РФ (обман), другие – по ст. 159.6 УК РФ (вмешательство в функционирование информационно-телекоммуникаци-онных сетей путем получения доступа к учетным данным). Перенаправление пользователя на поддельный сайт также может квалифицироваться как вмешательство в функционирование информационно-телекоммуникационных сетей. Хищение денежных средств с банковских карт с использованием троянских программ или программ-вымогателей однозначно подпадает под ст. 159.6 УК РФ, так как происходит вмешательство в работу средств хранения и обработки компьютерной информации. Хищение виртуальных ценностей, аккаунтов или денежных средств в онлайн-играх и социальных сетях также может квалифицироваться по ст. 159.6 УК РФ, если хищение происходит путем неправомерного доступа или манипуляций с компьютерной информацией. Несанкционированные переводы денежных средств с электронных кошельков или банковских счетов, совершенные путем взлома или обмана платежных систем, также подпадают под действие ст. 159.6 УК РФ.

Проблемы квалификации цифровых преступлений обусловлены рядом факторов. Во-первых, динамичный характер развития информационных технологий приводит к появлению новых способов совершения преступлений, которые зачастую не в полной мере охватываются существующими составами преступлений, предусмотренными УК РФ [2]. Например, квалификация действий, связанных с использованием криптовалют в преступных целях или с атаками на объекты критической информационной инфраструктуры, может вызывать затруднения у правоприменителей. Во-вторых, специфика цифровой среды, характеризующаяся трансграничностью, анонимностью и возможностью удаленного совершения действий, затрудняет установление места и времени совершения преступления, а также идентификацию лиц, причастных к его совершению. В-третьих, квалификация отдельных составов преступлений, таких как мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ) или неправомерный доступ к компьютерной информации (ст. 272 УК РФ), требует глубокого понимания технических аспектов функционирования информационных систем и технологий, что не всегда возможно без привлечения специалистов.

Не менее актуальной является проблема определения ответственности за цифровые преступления. Установление виновности лица, совершившего преступление в цифровой среде, может быть затруднено в связи с использованием различных средств анонимизации, прокси-серверов, VPN-соединений и других технологических ухищрений [3]. Кроме того, сложность может представлять доказывание умысла и мотива преступления, особенно в случаях, когда действия носят автоматизированный характер или осуществляются с использованием вредоносного программного обеспечения. Еще одной проблемой является определение размера причиненного ущерба, который в цифровой среде может носить нематериальный характер или быть распределен между большим количеством потерпевших.

Продолжая рассмотрение проблем квалификации и ответственности за цифровые преступления в российском законодательстве, необходимо детально остановиться на отдельных аспектах, вызывающих особые трудности у правоприменителей.

Одной из значимых проблем является установление причинно-следственной связи между действиями виновного и наступившими общественно опасными последствиями. В соответствии с общими принципами уголовного права, привлечение к ответственности возможно лишь при установлении прямой причинной связи между противоправным деянием и причиненным вредом. В контексте цифровых преступлений данное требование нередко вызывает затруднения. Так, при хищении денежных средств путем фишинга (статья 159 УК РФ «Мошенничество») несмотря на то, что потерпевший самостоятельно вводит свои данные на подложном сайте, следствию необходимо доказать, что именно действия злоумышленника по созданию и распространению фишинговой ссылки стали непосредственной причиной утраты денежных средств.

Сложность заключается в том, что потерпевший мог допустить ошибку, не распознать поддельный ресурс или стать жертвой социальной инженерии, что может опосредовать причинно-следственную связь.

Кроме того, в цифровой среде на наступление негативного результата могут влиять множественные факторы. Например, при неправомерном доступе к компьютерной информации (статья 272 УК РФ) утечка данных может произойти не только в результате действий хакера, но и вследствие уязвимостей в программном обеспечении, ошибок администрирования или неосторожных действий самого пользователя. Установление однозначной причинно-следственной связи в таких случаях требует проведения сложных технических экспертиз и анализа всего комплекса обстоятельств дела. Данная проблема осложняет квалификацию преступления и может служить основанием для оспаривания виновности лица.

Другой существенной проблемой является квалификация преступлений, совершаемых с использованием новых технологий. Сфера информационных технологий развивается чрезвычайно быстро, постоянно появляются новые способы совершения противоправных деяний, которые зачастую не находят прямого отражения в действующих нормах уголовного законодательства. Например, использование технологий искусственного интеллекта для создания дипфейков, распространение вредоносного программного обеспечения, использующего новейшие уязвимости, или совершение мошеннических действий с использованием криптовалют могут представлять сложности для квалификации по существующим статьям УК РФ.

Для эффективной борьбы с киберпреступностью необходимо постоянное совершенствование уголовного законодательства и разъяснение его положений с учетом новых технологических реалий. Необходимо внесение изменений и дополнений в действующие статьи УК РФ, так и в принятии новых законодательных актов, направленных на противодействие конкретным видам киберпреступлений. Кроме того, важную роль играют разъяснения высших судебных инстанций, которые позволяют унифицировать практику применения уголовного закона в условиях быстрого развития технологий.

Особую сложность представляет квалификация трансграничных преступлений. В случаях, когда преступление совершается с использованием серверов, расположенных на территории иностранного государства, или злоумышленник находится за пределами Российской Федерации, возникают юрисдикционные вопросы. Действие ст. 12 УК РФ распространяется на преступления, совершенные на территории Российской Федерации. Однако в цифровой среде определение места совершения преступления затруднено, поскольку противоправные действия могут инициироваться в одной стране, а последствия наступать в другой. Ст. 11 УК РФ предусматривает ответственность граждан Российской Федерации и лиц без гражданства, постоянно проживающих в Российской Федерации, совершивших преступление за пределами Российской Федерации. Однако привлечение таких лиц к ответственности может быть затруднено без эффективного международного сотрудничества.

Эффективная борьба с трансграничной киберпреступностью требует активного международного сотрудничества в сфере обмена информацией, оказания правовой помощи и выдачи преступников. Необходимо заключение и реализация международных договоров и соглашений, направленных на противодействие киберпреступности, а также развитие взаимодействия между правоохранительными органами различных государств. Отсутствие эффективного международного сотрудничества может привести к безнаказанности лиц, совершающих преступления в цифровой среде, что подрывает усилия по обеспечению кибербезопасности на национальном и международном уровнях.

Таким образом, проблемы установления причинно-следственной связи, квалификации преступлений с использованием новых технологий и трансграничных преступлений являются ключевыми вызовами для российского законодательства в сфере борьбы с цифровой преступностью. Их решение требует комплексного подхода, включающего совершенствование уголовного законодательства, развитие международного сотрудничества, повышение квалификации правоприменителей и активное использование возможностей современных информационных технологий для выявления и пресечения киберпреступлений.

Российское законодательство предпринимает шаги по совершенствованию правового регулирования в сфере борьбы с цифровыми преступлениями. В УК РФ введены специальные составы преступлений, направленные на противодействие киберпреступности (ст. 272-274.1). Принимаются федеральные законы, регулирующие вопросы информационной безопасности и защиты критической информационной инфраструктуры. Однако, несмотря на предпринимаемые меры, существующая правовая база нуждается в дальнейшем развитии и адаптации к быстро меняющимся реалиям цифровой среды.

Для реализации единой стратегии охраны правопорядка правительству недостаточно полагаться исключительно на правовые санкции. Например, в Китае приняты «Четыре закона о борьбе с мошенничеством» в июле 2024 года. Несмотря на столь громкое заявление и конкретную реализацию законодательства о борь-

бе с мошенничеством в Тайване достиг пика в 13,7 млрд. долл. в августе 2024 года, что превысило общий объем мошенничества за все предыдущие годы.

Поскольку российское общество вступает в цифровую эпоху, ему необходима системная и комплексная стратегия общественной безопасности для усиления социального контроля и регулирования цифровой преступности на законодательном уровне. В целях повышения эффективности борьбы с цифровыми преступлениями необходимо комплексное решение проблем квалификации и ответственности. Необходимо совершенствование уголовного законодательства путем введения новых составов преступлений, учитывающих специфику цифровых технологий, а также внесения изменений в существующие нормы для четкого их применения к цифровым правонарушениям. Кроме того, назрела необходимость в дополнении статьи 273 УК РФ. Следует рассмотреть возможность расширения понятия «вредоносная компьютерная программа» с учетом появления новых видов вредоносного программного обеспечения и способов их распространения, а также предусмотреть ответственность за разработку и распространение инструментов, заведомо предназначенных для совершения киберпреступлений.

Важным направлением является повышение квалификации сотрудников правоохранительных органов в области информационных технологий и кибербезопасности, а также развитие международного сотрудничества в сфере борьбы с трансграничными цифровыми преступлениями. Кроме того, необходимо уделять внимание вопросам профилактики цифровой преступности, повышения уровня цифровой грамотности населения и формирования ответственного поведения в онлайн-среде.

Рекомендуется, укорениться в системе образования и придавать большое значение образованию и обучению от дошкольного до старшего школьного возраста, чтобы улучшить индивидуальный самоконтроль, развить прочные социальные знания и устойчивость в жизни, чтобы избежать преступлений, вызванных искушением, и жертв, вызванных невежеством в будущем. Судебная система должна отойти от традиционного менталитета наказания за физические преступления и сосредоточиться на фактическом вреде, причиненном обществу современными цифровыми преступлениями. Назначаемое наказание должно превышать реальную степень вреда, ощущаемого жертвой. Также необходимо создать специализированное агентство, «Национальный механизм по борьбе с цифровой преступностью», в котором цифровые регулирующие агентства будут основным ответственным подразделением, с полномочиями командовать, планировать, координировать и бороться с цифровой преступностью по всей стране. Только таким образом можно будет по-настоящему и эффективно разрушить барьеры соответствующих агентств, основанные на их собственных интересах, и в полной мере реализовать эффективность современной профилактики цифровой преступности.

Выводы

Проблема квалификации и ответственности за цифровые преступления в российском законодательстве обусловлена стремительным развитием информационных технологий и их повсеместным проникновением в общественные отношения. Несмотря на предпринимаемые государством меры по совершенствованию правового регулирования, введение специальных составов преступлений в УК РФ, сохраняется ряд существенных проблем. Основными из них являются проблемы в разграничении смежных составов преступлений, таких как общее мошенничество и мошенничество в сфере компьютерной информации, особенно при квалификации деяний, связанных с фишингом. Кроме того, стремительное появление новых технологий, таких как искусственный интеллект и криптовалюты, создает потребность в постоянной адаптации уголовного законодательства и введении новых правовых норм, способных эффективно противодействовать возникающим угрозам. Особую сложность представляет квалификация и расследование трансграничных цифровых преступлений, которая обусловлена вопросами юрисдикции и необходимостью активизации международного сотрудничества в сфере обмена информацией и выдачи преступников.

Для повышения эффективности борьбы с цифровой преступностью необходимо реализация комплексного подхода, дальнейшее совершенствование уголовного законодательства путем введения новых составов преступлений и внесения изменений в существующие нормы. Но, и повышение уровня цифровой грамотности населения, усиление мер профилактики, а также развитие специализированных подразделений в правоохранительных органах, обладающих необходимыми техническими знаниями и компетенциями. Важным аспектом является переосмысление подходов к назначению наказания за цифровые преступления с акцентом на реальный ущерб, причиненный обществу и потерпевшим. Представляется целесообразным рассмотрение вопроса о создании специализированного национального органа, координирующего деятельность различных ведомств в сфере противодействия цифровой преступности, чтобы эффективно планировать и реализовывать меры по борьбе с данным видом

противоправной деятельности. Только системные и скоординированные усилия государства, общества и образовательных институтов могут обеспечить должный уровень безопасности в цифровом пространстве и эффективно противостоять растущей угрозе цифровой преступности в современных условиях.

Дальнейшее развитие российского законодательства в этой сфере, основанное на анализе существующих проблем и передовом международном опыте, будет способствовать эффективной борьбе с цифровой преступностью и созданию безопасной и доверительной цифровой среды.

Список источников

1. Доклад XI Конгресса Организации Объединенных Наций по предупреждению преступности и уголовному правосудию. Бангкок, 18-25 апреля 2005 [Электронный ресурс]. URL: https://www.unodc.org/ https://www.unodc.org/documents/congress/Documentation/11Congress/A_CONF.203.18_V0584411_r.pdf (дата обращения: 01.07.2021)

2. Капинус О.С. Цифровизация преступности и уголовного права // Байкальский научный журнал. 2022. Т. 13. № 1. С. 1 – 7.

3. Ображиев К.В. Преступные посягательства на цифровые финансовые активы и цифровую валюту: проблемы квалификации и законодательной регламентации // Журнал российского права. 2022. № 2. С. 71 – 87.

4. Перина А.С. «Цифровые преступления»: понятие, типология, признаки // Юридический вестник Самарского университета. 2023. Т. 9. № 3. С. 106 – 115. DOI: https://doi.org/10.18287/2542-047X-2023-9-3-106-115

5. Потемкина А.Ю. Фишинг как разновидность интернет-мошенничества // Молодой ученый. 2022. № 28 (423). С. 187 – 189.

6. Приговор Чертановского районного суда г. Москвы от 7 сентября 2012 г. по уголовному делу № 1-486/12. // СудАкт: Судебные и нормативные правовые акты РФ. URL: https://sudact.ru/regular/doc/j4eDxuKkqebt/?regular-txt=Попелыши®ular-case_doc=®ular-lawchunkinfo=272+УК+РФ+®ular-date_from=®ular-date_to=®ular-workflow_stage=®ular-area=®ular-court=®ular-judge=&_=1657025602537. (дата обращения: 19.12.2024)

7. Руководство для дискуссий, подготовленное в рамках Четырнадцатого Конгресса ООН по предупреждению преступности и уголовному правосудию. Киото, Япония, 20-27 апреля 2020 года [Электронный ресурс]. URL: https://www.unodc.org/documents/congress/Documentation/14thCongress/DiscussionGuide/A_CONF.234_PMI_V1806331_r.pdf. С. 50 – 56.

8. Русскевич Е.А. Уголовное право и «цифровая преступность»: проблемы и решения. 2-е изд. Москва: Издательский Дом «Инфра-М», 2022. 351 с.

9. Соглашение между правительствами государств – членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности (заключено в Екатеринбурге 16.06.2009). Доступ из справ.-правовой системы «КонсультантПлюс».

10. Соглашение о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере компьютерной информации. 2001. Доступ из справ.-правовой системы «КонсультантПлюс».

11. Соглашение о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере информационных технологий. 2018. URL: http://publication.pravo.gov.ru/Document/View/0001202207180005(дата обращения: 15.12.2024)

12. Kuo J. The Global State of Scams – 2023. URL: https://recorder.ro/wp-content/uploads/2024/07/State-of-Scams-Report-2023.pdf(дата обращения: 15.12.2024)

13. Zarmsky S. Is International Criminal Law Ready to Accommodate Online Harm? Challenges and Opportunities // Journal of International Criminal Justice. 2022. Vol. 22 (1). P. 169 – 184. Doi: https://doi.org/10.1093/jicj/mqae013

References

1. Report of the XI United Nations Congress on Crime Prevention and Criminal Justice. Bangkok, 18-25 April 2005 [Electronic resource]. URL: https://www.unodc.org/ https://www.unodc.org/documents/congress/Documentation/11Congress/A_CONF.203.18_V0584411_r.pdf (date of access: 01.07.2021)

2. Kapinus O.S. Digitalization of Crime and Criminal Law. Baikal Scientific Journal. 2022. Vol. 13. No. 1. P. 1 – 7.

3. Obraziev K.V. Criminal Attacks on Digital Financial Assets and Digital Currency: Problems of Qualification and Legislative Regulation. Journal of Russian Law. 2022. No. 2. P. 71 – 87.

4. Perina A.S. "Digital crimes": concept, typology, features. Legal Bulletin of Samara University. 2023. Vol. 9. No. 3. P. 106 – 115. DOI: https://doi.org/10.18287/2542-047X-2023-9-3-106-115

5. Potemkina A.Yu. Phishing as a type of Internet fraud. Young scientist. 2022. No. 28 (423). P. 187 – 189.

6. Verdict of the Chertanovsky District Court of Moscow dated September 7, 2012 in criminal case No. 1-486/12. SudAkt: Judicial and regulatory legal acts of the Russian Federation. URL: https://sudact.ru/regular/doc/j4eDxuKkqebt/?regular-txt=Поплеыши®ular-case_doc=®ular-lawchunkinfo=272+УК+РФ+®ular-date_from=®ular-date_to=®ular-workflow_stage=®ular-area=®ular-court=®ular-judge=&_=1657025602537 (date of access: 19.12.2024)

7. Discussion Guide prepared within the framework of the Fourteenth United Nations Congress on Crime Prevention and Criminal Justice. Kyoto, Japan, 20-27 April 2020 [Electronic resource]. URL: https://www.unodc.org/documents/congress/Documentation/14thCongress/DiscussionGuide/A_CONF.234_PMI_V1806331_r.pdf. P. 50 – 56.

8. Russkevich E.A. Criminal law and “digital crime”: problems and solutions. 2nd ed. Moscow: Publishing House “Infra-M”, 2022. 351 p.

9. Agreement between the governments of the member states of the Shanghai Cooperation Organization on cooperation in the field of international information security (concluded in Yekaterinburg on 16.06.2009). Access from the reference and legal system “ConsultantPlus”.

10. Agreement on cooperation of the CIS member states in combating crimes in the field of computer information. 2001. Access from the reference and legal system “ConsultantPlus”.

11. Agreement on Cooperation between the CIS Member States in Combating Crimes in the Sphere of Information Technology. 2018. URL: http://publication.pravo.gov.ru/Document/View/0001202207180005 (date of access:: 15.12.2024)

12. Kuo J. The Global State of Scams – 2023. URL: https://recorder.ro/wp-content/uploads/2024/07/State-of-Scams-Report-2023.pdf (date of access: 15.12.2024)

13. Zarmsky S. Is International Criminal Law Ready to Accommodate Online Harm? Challenges and Opportunities. Journal of International Criminal Justice. 2022. Vol. 22 (1). P. 169 – 184. Doi: https://doi.org/10.1093/jicj/mqae013

Информация об авторах

Гереев З.Г., директор колледжа, Ростовский институт, филиал Всероссийского государственного университета юстиции (РПА Минюста России)

Киселева Т.А., заместитель директора колледжа, Ростовский институт, филиал Всероссийского государственного университета юстиции (РПА Минюста России)

Далоев А.Т., преподаватель колледжа, Ростовский институт филиал, Всероссийского государственного университета юстиции (РПА Минюста России)