Дата поступления рукописи в редакцию: 17.05.2026 г. DOI: 10.24412/2782-3830-2026-6-293-299
Дата принятия рукописи в печать: 02.07.2026 г.

АКАПЬЕВ Виктор Львович,
кандидат педагогических наук,
доцент кафедры информационно-компьютерных
технологий в деятельности органов внутренних дел
Белгородского юридического института МВД России
имени И.Д. Путилина,
e-mail: akapevv@yandex.ru

БОРИСЕНКО Александр Васильевич,
кандидат физико-математических наук,
старший преподаватель кафедры информационно-компьютерных
технологий в деятельности органов внутренних дел
Белгородского юридического института
МВД России имени И.Д. Путилина,
e-mail: borisenko02.94@mail.ru

КОВАЛЕВА Екатерина Геннадьевна,
кандидат технических наук,
доцент кафедры информационно-компьютерных
технологий в деятельности органов внутренних дел
Белгородского юридического института МВД России
имени И.Д. Путилина,
e-mail: kovalevazchs@yandex.ru

ПИРОЖЕНКО Юрий Анатольевич,
преподаватель кафедры информационно-компьютерных
технологий в деятельности органов внутренних дел
Белгородского юридического института
МВД России имени И.Д. Путилина,
e-mail: pieibex@yandex.ru

ИНТЕРНЕТ-МОШЕННИЧЕСТВО (ФИШИНГ): ПРОБЛЕМЫ КВАЛИФИКАЦИИ

Аннотация. *Цифровизация общества в области финансово-экономических отношений и возрастающая негативная роль кибермошенничества актуализируют необходимость совершенствования правовой регламентации указанной сферы общественных отношений. Однако, решение указанной задачи осложняется отсутствием четкой терминологически-правовой регламентации ключевых понятий в российском законодательстве. Предметом рассмотрения в данной статье является фишинг, представляющий собой одну из наиболее распространенных форм кибермошенничества, анализируются проблемы правовой квалификации данного деяния в российском законодательстве, связанные с отсутствием легального определения и сложностью разграничения смежных составов преступлений. На основе изучения научных подходов, статистических данных и судебной практики обосновывается необходимость выделения фишинга в самостоятельный состав преступления, которая будет направлена на повышение эффективности противодействия данному виду киберпреступлений.*

Ключевые слова: *кибермошенничество, киберпреступления, киберпреступник, фишинг, финансово-экономические отношения, правовая квалификация.*

AKAPYEV Viktor Lvovich,
Candidate of Pedagogical Sciences,
Docent of the Department ICT in Law Enforcement Agencies
Belgorod Law Institute The Ministry of Internal Affairs of Russia
named after I.D. Putilin

BORISENKO Alexander Vasilyevich,
Candidate of Physico-mathematical Sciences,
Senior lecturer of the Department ICT in Law Enforcement Agencies
Belgorod Law Institute The Ministry of Internal Affairs of Russia
named after I.D. Putilin

KOVALEVA Ekaterina Gennadievna,
Candidate of Technical Sciences,
Associate Professor of the Department ICT in Law Enforcement Agencies
Belgorod Law Institute The Ministry of Internal Affairs of Russia
named after I.D. Putilin

PIROZHENKO Yuri Anatolyevich,
lecturer of the Department ICT in Law Enforcement Agencies
Belgorod Law Institute The Ministry of Internal Affairs of Russia
named after I.D. Putilin

INTERNET FRAUD (PHISHING): QUALIFICATION ISSUES

Annotation. *The digitalization of society in the sphere of financial and economic relations, combined with the growing adverse impact of cyber fraud, has made it necessary to refine the legal regulation of this area of social relations.. However, the solution of this problem is complicated by the lack of clear terminological and legal regulation of key concepts in Russian legislation. This article examines phishing as one of the most common forms of cyberbullying, analyzes the problems of legal qualification of this act in Russian legislation related to the lack of a legal definition and the difficulty of distinguishing related crimes. Based on the study of scientific approaches, statistical data and judicial practice, the necessity of identifying phishing as an independent crime is substantiated, which will be aimed at improving the effectiveness of countering this type of cybercrime.*

Key words: *cyberbullying, cybercrime, cybercriminal, phishing, financial and economic relations, legal qualifications.*

В связи с многообразием способов и приёмов совершения преступлений при помощи гаджетов и новейших технологий возникает необходимость выделить кибермошенничество в особый вид в структуре преступлений в сфере компьютерной информации. Главной площадкой для него выступает интернет. Интенсивное использование глобальной сети вызывает у правоохранительных органов тревогу, поскольку расширяются возможности для применения интернета и цифровых технологий в противоправных целях, в том числе для обмана [1].

Повышенное внимание к указанной проблеме подтверждено высказыванием Владимира Путина на совещании с членами Правительства 5 марта 2025 года: «Ущерб для граждан, а значит и для государства, со стороны телефонных и интернет-мошенников приобрел просто недопустимые размеры, очень большие. Поэтому действовать нужно быстро». На совещании также отмечено, что почти 90% россиян сталкивались с подобными правонарушениями в сфере информационно-коммуникационных технологий. Число преступлений с использованием средств связи в прошлом году выросло на 13%, однако раскрываемость киберпреступлений снизилась до 23% по сравнению с предыдущим годом [2].

Председатель Государственной Думы Вячеслав Володин не раз отмечал, что «кибермошенники пытаются изобрести все новые способы, чтобы обмануть граждан и завладеть их денежными средствами. Депутаты последовательно работают над совершенствованием законодательства в этой сфере: противодействие мошенничеству было и остается одним из основных приоритетов в работе Государственной Думы» [3].

Одной из современных форм мошенничества является фишинг. Этот метод основан на недостаточной осведомленности пользователей о нормах сетевой безопасности и направлен на получение доступа к конфиденциальной информации, часто финансового характера [4]. Главное отличие фишеров от хакеров заключается в том, что они используют обман доверия граждан для получения паролей, номеров кредитных карт и другой конфиденциальной информации [5].

Согласно отчетам организаций Fraud.org и Национальной лиги потребителей (NCL), фишинг является самым распространенным видом мошенничества. В 2025 году он занял первое место по всем зарегистрированным жалобам, составив около 35% от общего числа инцидентов

[6]. Примечательно, что по сравнению с 2024 годом количество жалоб на фишинг выросло на 85-86% [7].

В России зафиксирована положительная динамика снижения доли фишинга. Если в 2024 году на него приходилось 85,7% всех кибератак, то за 10 месяцев 2025 года этот показатель снизился до 69%. Несмотря на снижение доли, общее число атак продолжает расти. В 2025 году решения «Лаборатории Касперского» остановили 554 миллиона кликов по мошенническим ссылкам. Если в предыдущие годы фишинговая активность обычно достигала пиков в определенные сезоны, то в этот раз она оставалась на одном уровне все двенадцать месяцев с единственным заметным спадом в декабре [8].

Лидером среди отраслей, против которых направлен фишинг, стал ритейл (онлайн-покупки) – 50% атак. Далее следуют финансовый сектор (32%) и инвестиционные порталы (33%) [9]. В инвестиционной сфере мошенники активно имитируют брокерские платформы и криптобиржи [10].

Приведенные показатели указывают на важность противодействия данному виду мошенничества, однако в российском правовом поле термин «фишинг» не является обособленным составом преступления, что порождает терминологические проблемы и вызывает бурные научные дискуссии [11].

Хотя в Уголовном кодексе Российской Федерации (УК РФ) нет статьи «Фишинг», существует официальное (ведомственное) определение. Согласно документам, фишинг – это: «Действия... в целях введения в заблуждение и реализации угрозы... незаконного получения и разглашения сведений, составляющих коммерческую и банковскую тайну...» [21].

Это определение используется для методической работы правоохранительных органов, а на практике фишинг понимается как вид мошенничества, при котором злоумышленники используют поддельные сайты или сообщения для хищения данных [12].

В свою очередь, Н.В. Ралдугина определяет фишинг как вид интернет-мошенничества, целью которого завладеть конфиденциальными данными пользователя, например, логинами и паролями для входа в сервисы, данными банковской карты и лицевого счёта [13].

По мнению А.Н. Завьялова «фишинг - это один из способов мошенничества, целью которого является формирование поддельного сайта, неправомерное получение паролей, номеров банковских счетов и т.д. для получения конфиденциальной информации пользователей» [14].

При данном подходе к интерпретации фишинга как мошенничества с применением компьютерных технологий можно выделить три разновидности ответственности: административную как самый исходный и базовый уровень наказания, уголовную как наиболее обширный пласт воздействия на лиц, совершающих преступные деяния, а также гражданско-правовую как направление юридических последствий [15].

Выбор конкретной формы зависит от размера причиненного ущерба, способа совершения деяния и наступивших последствий. Это свидетельствует о высокой общественной опасности фишинга, посягающего как на отношения собственности, так и на безопасность в сфере компьютерной информации [16].

Несмотря на наличие формальных оснований для привлечения к административной ответственности по статьям 7.27 и 7.27.1 Кодекса Российской Федерации об административных правонарушениях (КоАП РФ) за мелкое хищение (наказание назначается за мелкое хищение на сумму до 2500 рублей) или причинение ущерба путем обмана, на практике эта мера применяется крайне редко [22]. Это обусловлено тем, что фишинг, как правило, является либо способом подготовки к более тяжкому преступлению, либо частью серии мошеннических действий, что автоматически переводит деяние в плоскость уголовного права [17].

Статья 159.6 Уголовного кодекса Российской Федерации (УК РФ), призванная стать эффективным инструментом борьбы с компьютерным мошенничеством, с момента своего появления стала объектом обоснованной научной критики. Основные дискуссии разворачиваются вокруг неоднозначности законодательной формулировки, в частности - определения адресата обмана, и разграничения данного состава со смежными преступлениями, предусмотренными главой 28 УК РФ. Также основной проблемой является определение момента, когда фишинг считается завершённым преступлением: это происходит, когда злоумышленник получает доступ к данным пользователя, когда он начинает их использовать, или только после того, как были украдены денежные средства? Этот вопрос имеет непосредственное влияние на возможность привлечения виновных к ответственности и на квалификацию деяний.

В соответствии со статьей 159.6 мошенничество в сфере компьютерной информации представляет собой 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. Но также мошенничество в сфере компьютерной информации требует дополнительной квалификации по статье 272, 273, предполагающие неправомерный доступ к компьютерной информации - получение доступа к кон-

фиденциальным данным пользователей, а также создание, использование и распространение вредоносных компьютерных программ - производство реализация фишинговых сайтов и рассылка вредоносных писем [23].

Основная сложность заключается в выборе между несколькими статьями УК РФ, которые часто пересекаются. Квалификация деяния зависит от того, как именно преступник завладел имуществом: через обман человека или через вмешательство в работу программ.

На практике судам и следствию сложно определить грань, где заканчивается «обман человека» (ст. 159) и начинается «вмешательство в работу сети» (ст. 159.6). Особенно это касается поддельных сайтов-двойников (фишинг). Если сайт просто собирает данные, а преступник потом сам вводит их в приложение банка – это вмешательство. Если данные ввела сама жертва – это общий обман [18].

Как было отмечено, в российском законодательстве отсутствует само понятие «фишинг». Это технический, а не юридический термин, из-за чего одни и те же действия могут трактоваться по-разному: от мошенничества до неправомерного доступа к компьютерной информации (ст. 272 УК РФ) или даже административного правонарушения, если не доказан умысел на хищение [19].

Эксперты отмечают, что компьютер (в отличие от человека) нельзя «обмануть» в классическом понимании, так как у него нет психики. Поэтому применение термина «мошенничество» к компьютерным атакам вызывает споры, хотя это и удобно для следствия [20].

Гражданско-правовая ответственность, реализуемая через механизмы статей 15, 1064 и особенно 1102 ГК РФ (о неосновательном обогащении), предоставляет потерпевшим действенный, хотя и непростой, механизм возврата похищенных средств. Значимой тенденцией в судебной практике становится право потерпевших требовать возмещения ущерба не только напрямую с преступников, но и с владельцев банковских счетов. Это заметно расширяет инструменты защиты прав пострадавших и одновременно повышает уровень ответственности для соучастников противоправных схем.

Действующая нормативная база, регламентирующая ответственность за фишинг, характеризуется фрагментарностью и содержит существенные правовые лакуны. Дефицит унифицированной терминологии и отсутствие отдельного состава преступления создают сложности при квалификации деяний, что заставляет правоприменительные органы использовать целый комплекс разнородных правовых норм. В подобных обстоятельствах потерпевшим остаётся полагаться в основном на гражданское право: именно оно нередко позволяет вернуть потерянное, тогда как привлечь виновных к уголовной ответственности мешают сложности со сбором доказательств.

Помимо этого, возникают технологические и доказательные сложности, так как киберпреступления обладают высокой латентностью и анонимностью. Фишинговые сайты часто хостятся на серверах за рубежом, а преступники используют VPN, прокси и анонимные сети. Это вызывает проблемы с международным сотрудничеством и юрисдикцией (невозможно экстрадировать подозреваемого или получить логи с иностранного сервера)

Чтобы признать человека виновным, нужно доказать, что он создал поддельный сайт именно для кражи, а не ради эксперимента или теста. Также трудно установить причинно-следственную связь между действиями хакера и конкретным ущербом (например, если потерпевший сообщил пароль добровольно) [15].

Можно утверждать, что законодательство часто не успевает за технологиями, так как такие современные методы совершения преступления как голосовые дипфейки и использование нейросетей усложняют квалификацию.

Новым вызовом для правоприменения стало разъяснение Верховного Суда, согласно которому компании могут нести ответственность за мошенничество, совершенное от их имени фишерами. Раньше клиент должен был проверять подлинность сайта. Теперь компания обязана доказывать, что сайт-двойник не имеет к ней отношения, иначе суд может обязать бизнес возместить ущерб пострадавшим. Это создает риск двойных штрафов и репутационных потерь [16].

Системный характер проблем правовой квалификации фишинга в Российской Федерации объясняется совокупностью двух факторов: несовершенством законодательной техники и технологической спецификой указанных противоправных деяний. Несмотря на закрепление соответствующих норм в УК РФ, правоприменительная практика демонстрирует устойчивые трудности при разграничении смежных составов преступлений, доказывании вины, а также при преодолении анонимности, обусловленной трансграничным характером совершаемых атак.

Ключевой проблемой квалификации фишинга в Российской Федерации выступает дисбаланс между стремительной эволюцией технологических способов совершения преступлений и статичностью уголовно-правовых норм. Действующие положения УК РФ (в частности, ст. 159 и 159.6) не в полной мере отвечают вызовам, связанным с применением социальной инженерии и современных цифровых инструментов. Вместе с тем в период 2025–2026 гг. государством были инициированы меры, направленные на преодоление указанных недостатков:

1. Пилотный проект Генпрокуратуры (июнь 2025 – март 2026) по внесудебной блокировке фишинговых сайтов [24].
2. Законопроект о блокировках (вступление в силу с 01.03.2026), упрощающий процедуру закрытия мошеннических ресурсов [25].

Эти меры направлены на борьбу с инфраструктурой фишеров, но не решают пока главной дилеммы: как правильно квалифицировать сам факт обмана в цифровой среде.

Современные реалии требуют внесения изменений в законодательство для более действенного и адекватного противодействия актуальным преступлениям. В связи с этим, целесообразно на законодательном уровне ввести определение и юридическую квалификацию фишинга в отдельной статье 159.7 УК РФ, представив ее в следующей редакции:

«1. Фишинг, то есть создание, использование или распространение вредоносных компьютерных программ либо иная деятельность, направленная на получение неправомерного доступа к охраняемой законом информации, содержащей персональные данные, банковские реквизиты, логины, пароли или иные конфиденциальные сведения, совершенные в целях хищения чужого имущества или приобретения права на чужое имущество, - наказываются штрафом в размере от трехсот тысяч до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет, либо исправительными работами на срок до двух лет, либо лишением свободы на срок до трех лет.

2. Те же деяния, совершенные:

– группой лиц по предварительному сговору;
– в крупном размере, - наказываются штрафом в размере от пятисот тысяч до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период от двух до трех лет, либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет, либо принудительными работами на срок до пяти лет, либо лишением свободы на срок до пяти лет».

Введение специализированной статьи позволит: устранить пробел в законодательном определении фишинга, преодолеть конкуренцию норм и необходимость квалификации по совокупности преступлений, унифицировать правоприменительную практику, повысить эффективность уголовного преследования и, как следствие, усилить защиту прав и законных интересов граждан в цифровой среде.

Таким образом, проведенное исследование позволяет заключить, что фишинг представляет собой одну из наиболее распространенных и общественно опасных форм кибермошенничества, требующую адекватного правового реагирования. Анализ российского законодательства выявил ключевые проблемы квалификации данного деяния: отсутствие легального определения фишинга и сложность разграничения смежных составов преступлений (ст. 159.6, 272, 273 УК РФ). Изучение научных подходов, статистических данных и судебной практики подтверждает необходимость выделения фишинга в самостоятельный состав преступления. В связи с этим предлагается новая редакция статьи Уголовного кодекса РФ (ст. 159.7), направленная на устранение правовой неопределенности и повышение эффективности противодействия данному виду киберпреступлений.

Список литературы:

[1] Гаркавая В. Искусственный интеллект как инструмент предотвращения экономических преступлений и борьбы с мошенничеством на финансовом рынке / В. Гаркавая, Е.А. Смирнова, П.А. Созинов [и др.] // Экономика и управление: проблемы, решения. – 2026. – Т. 4. № 1 (166). – С. 74-82.

[2] Тревожные звонки: Путин заявил о недопустимых масштабах мошенничества в РФ. - URL: https://iz.ru/1849375/alena-nefedova-natalia-ilina/trevozhnye-zvonki-putin-zayavil-o-nedopustimyh-masshtabah-moshennichestva-v-rf (дата обращения 11.05.2026).

[3] Как законодательство защищает граждан от кибермошенников. - URL: http://duma.gov.ru/news/61988 (дата обращения 01.05.2026).

[4] Хамит Е.Е. Особенности квалификации интернет-хищений, совершаемых посредством «фишинга» // Вестник Академии правоохранительных органов при Генеральной прокуратуре Республики Казахстан. – 2023. – № 3 (29). – С. 67-75.

[5] Бячкова Н.Б. Современные виды фишинга в киберпреступлениях / Н.Б. Бячкова // Неделя науки, посвященная 25-летию ФКОУ во Пермский институт ФСИН России: сборник материалов, Пермь, 03–07 февраля 2025 года. – Пермь: Пермский институт Федеральной службы исполнения наказаний, 2025. – С. 21-23.

[6] New Report: Top Ten Scams of 2025. – URL: fraud.org›new-report-top-ten-scams-of-2025 (дата обращения 05.05.2026).

[7] 8 Crypto Scams to Watch Out for in 2025. – URL: tatum.io›blog/8-crypto-scams-2025 (дата обращения 12.04.2026).

[8] В России зафиксировано снижение доли фишинга, но киберпреступники усилили атаки на Telegram и распространяют больше вредоносного ПО. – URL: // https://cisoclub.ru/v-rossii-zafiksirovano-snizhenie-doli-fishinga-no-

kiberprestupniki-usilili-ataki-na-telegram-i-rasprostranjajut-bolshe-vredonosnogo-po (дата обращения 17.04.2026).

[9] Ритейл обошел финансовый сектор по количеству фишинговых и скам-атак в 2025. – URL: https://anrt.info/news/proish/70209-riteyl-oboshel-finsektor-po-chislu (дата обращения 05.04.2026).

[10] Краснова В.А. Проблемы фишинга в цифровом пространстве современного общества / В.А. Краснова, А.С. Пьянченко // Проблемы научно-практической деятельности. Поиск и выбор инновационных решений: сборник статей по итогам Международной научно-практической конференции, Саратов, 14 апреля 2025 года. – Стерлитамак: Агентство международных исследований, 2025. – С. 261-264.

[11] Официальный сайт МВД России. – URL: https://news.ru/amp/society/v-mvd-nazvali-samye-populyarnye-onlajn-sfery-dlya-fishinga-u-moshennikov (дата обращения 30.03.2026).

[12] Прокурор разъясняет. – URL: // https://epp.genproc.gov.ru/ru/mmtp/activity/legal-education/explain/e85554 (дата обращения 15.04.2026).

[13] Ралдугина, Н.В. «Письмо счастья» от мошенников: как не клюнуть на фишинг / Н.В. Ралдугина // Альфа-Банк: Альфа-Курс. – 2025. – URL: https://kurs.alfaba№k.ru/articles/pismo-schastya-ot-moshe№№ikov-kak-№e-klyu№ut-№a-fishi№g-i-№e-poteryat-de№gi (дата обращения 05.04.2026).

[14] Завьялов А.Н. Интернет-мошенничество (фишинг): проблемы и предупреждения // Baikal Research Jour№al. 2022. №2. URL: https://cyberle№i№ka.ru/article/№/i№ter№et-moshe№№ichestvo-fishi№g-problemy-protivodeystviya-i-preduprezhde№iya (дата обращения 11.04.2026).

[15] Фишинг: понятие, правовая регламентация и проблемы квалификации // https://gppart66.ru/articles/fishing-ponyatie-pravovaya-reglamentatsiya-i-problemy-kvalifikatsii (дата обращения 27.03.2026).

[16] Зайцева Э.Д. Социальная инженерия в финансовой сфере: что такое фишинг и как с этим бороться / Э.Д. Зайцева, Я.М. Дорощенков // Современные тенденции развития среднего профессионального образования России в эпоху цифровизации: перспективы и тренды: Сборник статей Всероссийской научно-практической конференции, Брянск, 08 октября 2025 года. – Брянск: ИП Усова И.Н., 2025. – С. 48-50.

[17] Фролов М.Д. О некоторых проблемах квалификации мошенничества в сфере компьютерной информации // Адвокат. – 2016. – № 6. – С. 53-58.

[18] Хисамова З.И. Об особенностях квалификации преступлений, совершаемых в сфере использования информационно-коммуникационных технологий // Общество и право. – 2016. – № 1 (55). – С. 117-120.

[19] Баранов А.Н. Уголовно-правовое и криминологическое противодействие мошенничеству в сфере компьютерной информации // Молодой ученый. – 2025. – № 38 (589). – С. 55-58.

[20] Бедеров И. Первые 72 часа – это окно для спасения репутации и снижения ущерба - Tom Hunter. – URL: https://tomhunter.ru/press-center/press-releases/pervye-72-chasa-eto-okno-dlya-spaseniya-reputaczii-i-snizheniya-ushherba.html (дата обращения 07.05.2026).

[21] Приказ Минцифры России от 28.02.2022 № 143 (ред. от 10.12.2024) «Об утверждении методик расчета показателей федеральных проектов национальной программы «Цифровая экономика Российской Федерации» и признании утратившими силу некоторых приказов Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации об утверждении методик расчета показателей федеральных проектов национальной программы «Цифровая экономика Российской Федерации» // СПС «КонсультантПлюс».

[22] Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (ред. от 02.05.2026) // СПС «КонсультантПлюс».

[23] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 09.04.2026) // СПС «КонсультантПлюс».

[24] Сайт: https://epp.genproc.gov.ru/ru/proc_41/activity/legal-education/explain/e5874898/ (дата доступа 10.05.2026).

[25] Проект Федерального закона «О внесении изменений в отдельные законодательные акты Российской Федерации (в части противодействия правонарушениям, совершаемым с использованием информационно-коммуникационных технологий)» (не внесен в ГД ФС РФ) // СПС «КонсультантПлюс».

References:

[1] Garkavaya, V. Artificial Intelligence as a Tool for Preventing Economic Crimes and Combating Fraud in the Financial Market / V. Garkavaya, E.A. Smirnova, P.A. Sozinov [et al.] // Economics and Management: Problems and Solutions. – 2026. – Vol. 4. No. 1 (166). – Pp. 74-82.

[2] Alarming Calls: Putin Announces Unacceptable Scale of Fraud in Russia. - URL: https://iz.ru/1849375/alena-nefedova-natalia-ilina/trevozhnye-zvonki-putin-zayavil-o-nedopustimyh-masshtabah-moshennichestva-v-rf (accessed on 11.05.2026).

[3] How the legislation protects citizens from cybercriminals. - URL: http://duma.gov.ru/news/61988 (accessed on 01.05.2026).

[4] Khamit E.E. Features of the qualification of Internet thefts committed by means of “phishing” // Bulletin of the Academy of Law Enforcement Agencies under the Prosecutor General’s Office of the Republic of Kazakhstan. – 2023. – No. 3 (29). – Pp. 67-75.

[5] Byachkova N.B. Modern Types of Phishing in Cybercrimes / N.B. Byachkova // Science Week Dedicated to the 25th Anniversary of the Federal Penitentiary Service of Russia at the Perm Institute of the Federal Penitentiary Service of Russia: Collection of Materials, Perm, February 03–07, 2025. – Perm: Perm Institute of the Federal Penitentiary Service, 2025. – Pp. 21-23.

[6] New Report: Top Ten Scams of 2025. – URL: fraud.org “new-report-top-ten-scams-of-2025 (accessed 05.05.2026).

[7] 8 Crypto Scams to Watch Out for in 2025. – URL: tatum.io “blog/8-crypto-scams-2025 (accessed 04/12/2026).

[8] A decrease in the share of phishing has been recorded in Russia, but cybercriminals have intensified attacks on Telegram and are spreading more malware. – URL: // https://cisoclub.ru/v-rossii-zafiksirovano-snizhenie-doli-fishinga-no-kiberprestupniki-usilili-ataki-na-telegram-i-rasprostranjajut-bolshe-vredonosnogo-po (accessed 04/17/2026).

[9] Retail surpassed the financial sector in the number of phishing and scam attacks in 2025. – URL: https://anrt.info/news/proish/70209-riteyl-oboshel-finsektor-po-chislu (accessed 04/05/2026).

[10] Krasnova V.A. Problems of phishing in the digital space of modern society / V.A. Krasnova, A.S. Pyanchenko // Problems of scientific and practical activity. Search and selection of innovative solutions: collection of articles based on the results of the International Scientific and Practical Conference, Saratov, April 14, 2025. – Sterlitamak: Agency for International Research, 2025. – Pp. 261-264.

[11] Official website of the Russian Ministry of Internal Affairs. – URL: https://news.ru/amp/society/v-mvd-nazvali-samye-populyarnye-onlajn-sfery-dlya-fishinga-u-moshennikov (date of application 30.03.2026).

[12] The Prosecutor clarifies. – URL: // https://epp.genproc.gov.ru/ru/mmtp/activity/legal-education/explain/e85554 (accessed 04/15/2026).

[13] Raldugina, N.V. “Letter of happiness” from scammers: how not to fall for phishing / N.V. Raldugina // Alfa-Bank: Alpha Course. – 2025. – URL: https://kurs.alfaba№k.ru/articles/pismo-schastya-ot-moshe№№ikov-kak-№e-klyu№ut-№a-fishi№g-i-№e-poteryat-de№ gi (accessed 04/05/2026).

[14] Zavyalov A.N. Internet fraud (phishing): problems and warnings // Baikal Research JourNo. al. 2022. No.2. URL: https://cyberle№i№ka.ru/article/№/i№ter№et-moshe№№ichestvo-fishi№g-problemy-protivodeystviya-i-preduprezhde№ iya (accessed 04/11/2026).

[15] Phishing: the concept, legal regulation and qualification issues // https://gppart66.ru/articles/fishing-ponyatie-pravovaya-reglamentatsiya-i-problemy-kvalifikatsii (accessed 03/27/2026).

[16] Zaitseva E.D. Social engineering in the financial sector: what is phishing and how to deal with it / E.D. Zaitseva, Ya.M. Doroshchenkov // Modern trends in the development of secondary vocational education in Russia in the era of Digitalization: prospects and trends: Collection of articles of the All-Russian Scientific and Practical Conference, Bryansk, October 08, 2025.On the Features of the Qualification of Crimes Committed in the Sphere of the Use of Information and Communication Technologies // Society and Law. – 2016. – No. 1 (55). – Pp. 117-120.

[19] Baranov A.N. Criminal and Criminological Counteraction to Fraud in the Sphere of Computer Information // Young Scientist. – 2025. – № 38 (589). – Pp. 55-58.

[20] Bederov I. The first 72 hours is a window to save reputation and reduce damage - Tom Hunter. – URL: https://tomhunter.ru/press-center/press-releases/pervye-72-chasa-eto-okno-dlya-spaseniya-reputaczii-i-snizheniya-ushherba.html (accessed 05/07/2026).d reduce damage - Tom Hunter. – URL: https://tomhunter.ru/press-center/press-releases/pervye-72-chasa-eto-okno-dlya-spaseniya-reputaczii-i-snizheniya-ushherba.html (accessed 05/07/2026).

[21] Order of the Ministry of Digital Affairs of Russia dated 28.02.2022 No. 143 (ed. 10.12.2024) “ On approval of methods for calculating indicators of federal projects of the national program “Digital Economy of the Russian Federation” and invalidating some orders of the Ministry of Digital Development, Communications and Mass Media of the Russian Federation on approval of methods for calculating indicators of federal projects of the national program “Digital Economy of the Russian Federation “//SPS” ConsultantPlus. “

[22] Code of Administrative Offenses of the Russian Federation No. 30.12.2001 dated 195-FZ (as amended by 02.05.2026) //SPS ConsultantPlus.

[23] The Criminal Code of the Russian Federation of 13.06.1996 No. 63-FZ (as amended by 09.04.2026) //SPS ConsultantPlus.

[24] Site: https://epp.genproc.gov.ru/ru/proc_41/activity/legal-education/explain/e5874898/ (access date 10.05.2026).

[25] Draft Federal Law “On Amendments to Certain Legislative Acts of the Russian Federation (in terms of countering offenses committed using information and communication technologies)” (not included in the State Duma of the Federal Assembly of the Russian Federation)//SPS “ConsultantPlus.”