Дата поступления рукописи в редакцию: 09.04.2026 г.
Дата принятия рукописи в печать: 14.05.2026 г.
DOI: 10.24412/2224-9133-2026-4-470-474

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

ПРОКОФЬЕВА Елена Васильевна
кандидат физико-математических наук,
доцент, доцент кафедры исследования документов
учебно-научного комплекса экспертно-
криминалистической деятельности
Волгоградской академии МВД России,
e-mail: mail@law-books.ru

ОТДЕЛЬНЫЕ АСПЕКТЫ ЭВОЛЮЦИИ ПРОТИВОДЕЙСТВИЯ КИБЕРМОШЕННИЧЕСТВУ

Аннотация. *В статье рассматриваются этапы эволюции законодательства в части противодействия мошенничеству в кибепространстве в рамках уголовного, административного и гражданского законодательства. Рассматриваются четыре этапа развития: от первых норм уголовного законодательства до качественно нового уровня институционализации противодействия кибермошенничеству, обеспечивающего преодоление информационной разрозненности и создание единого информационного пространства безопасности с принятием нормативно-правовых актов, регулирующих отдельные правоотношения, возникающие в сфере информационного права.*

Ключевые слова: *кибермошенничество, киберпреступность, развитие законодательства, мошенничество, информационное пространство, преступления в сфере компьютерной информации.*

GAUZHAEVA Victoria Aleksandrovna,
Candidate of Legal Sciences 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

PROKOFIEVA Elena Vasilievna
Candidate of Physical and Mathematical Sciences,
Associate Professor Associate Professor,
Department of Document Research, Educational and
Scientific Complex of Forensic Science,
Volgograd Academy of the Ministry of Internal Affairs of Russia

SELECTED ASPECTS OF THE EVOLUTION OF COUNTERING CYBERFRAUD

Annotation. *This article examines the stages of legislative evolution in combating cyberfraud within the framework of criminal, administrative, and civil law. Four stages of development are examined: from the first*

provisions of criminal law to a qualitatively new level of institutionalization of countering cyberfraud, which ensures the overcoming of information fragmentation and the creation of a unified information security space with the adoption of legal acts governing certain legal relations arising in the field of information law.

Key words: *cyberfraud, cybercrime, legislative development, fraud, information space, computer crimes.*

Стремительная цифровизация социально-экономических процессов, будучи неоспоримым благом цивилизационного развития, одновременно обнажила уязвимость традиционных правовых конструкций перед вызовами высокотехнологичной преступности. Кибермошенничество, трансформировавшееся из точечных девиаций в структурированную индустрию с глобальными трансграничными связями, сегодня представляет собой сложнейший объект для правовой регламентации. Законодатель оказался перед дилеммой: сохранить инерционность нормотворчества, свойственную континентальной правовой семье, либо перейти к превентивной (проактивной) модели регулирования, способной опережать появление новых криминальных схем. Эволюция подходов в этой сфере демонстрирует постепенный отход от сугубо карательной парадигмы к комплексной экосистеме защиты, где центральное место занимает не только неотвратимость наказания, но и создание условий, исключающих сам факт возможности хищения средств.

Ключевым вектором развития законодательного массива становится переход от фрагментарного реагирования к системному межотраслевому регулированию. Современная правовая архитектура противодействия кибермошенничеству аккумулирует в себе инструменты гражданского, финансового и уголовного права, формируя симбиоз публично-правовых запретов с частноправовыми механизмами защиты. В фокусе внимания законодателя сегодня находятся такие аспекты, как внедрение механизма «периода охлаждения» (anti-fraud cooling-off) для финансовых транзакций, ужесточение требований к идентификации пользователей в сетях связи, а также имплементация института возмещения вреда финансовыми организациями без признания их виновными. Такая конвергенция позволяет сместить акцент с посткриминального воздействия на предупредительное формирование среды, где совершение преступления становится технологически затруднительным.

Вместе с тем, динамика нормотворчества в исследуемой сфере неизбежно сталкивается с экстерриториальностью киберпространства и асинхронностью обновления законодательств разных юрисдикций. Дальнейшее совершенствование правовых механизмов видится не столько в увеличении санкционного давления, сколько в гармонизации процедур оперативного обмена данными между банковским сектором, правоохранительными органами и операторами связи. Перспективным направлением также является внедрение риск-ориентированного подхода, при котором степень правовой защиты дифференцируется в зависимости от уровня уязвимости конкретных общественных отношений. Формирование устойчивой законодательной модели противодействия кибермошенничеству — это процесс непрерывной адаптации, требующий от юристов не только ретроспективного анализа судебной практики, но и прогностического моделирования возможных угроз.

Быстрое и не всегда поступательное развитие информационных технологий в планетарном масштабе и существенная цифровизация экономики повлекли возникновение новых способов совершения преступлений и правонарушений, в том числе наиболее распространенной его преступной формы - кибермошенничества. Цифровая трансформация, как феномен и один из наиболее вероятных путей развития преступной деятельности создает беспрецедентные вызовы для правоохранительных органов, которые не имеют достаточно возможностей, в том числе, и необходимый кадровый потенциал для широкомасштабного противодействия. Распространение кибермошенничества, сложность его выявления и сбора доказательственной базы требуют совершенствования деятельности по противодействию преступлениям этой группы.

Проблемой выступает не только сложность правовой оценки новых форм мошеннических действий и правонарушений, совершаемых с использованием информационных технологий, но и противоречия в нормативно-правовых актах, регламентирующих информационную сферу деятельности.

Противодействие кибермошенничеству требует применения норм уголовного права (установление ответственности за совершение преступлений) [1], административного права (регулирование деятельности кредитных организаций и операторов связи), гражданского права (возмещение ущерба, защита прав потребителей), финансового права (регулирование национальной платёжной системы) [2], информационного права (защита персональных данных и банковской тайны) [3].

Эволюция законодательства о противодействии кибермошенничеству в сфере финансовых технологий [4 , с.4-7] прошла несколько качественно различных этапов, каждый из которых характеризовался определёнными приоритетами и особенностями правовой политики.

Первый этап (конец 1990-х — начало 2000-х годов) связан с появлением первых норм уголовного законодательства, устанавливающих ответственность за преступления в сфере компьютерной информации. Федеральный закон от 25.05.1998 № 89-ФЗ «О внесении изменений и дополнений в Уголовный кодекс Российской Федерации» ввёл в систему УК РФ главу 28 «Преступления в сфере компьютерной информации», предусмотрев ответственность за неправомерный доступ к компьютерной информации, создание и распространение вредоносных программ. Данный этап характеризовался преимущественно технократическим подходом, когда правовое регулирование было ориентировано на защиту самой информации как объекта, а не на защиту интересов субъектов, использующих информационные системы для осуществления финансовых операций.

Второй этап (середина 2000-х — начало 2010-х годов) ознаменовался формированием института национальной платёжной системы и правовым регулированием электронных денежных средств. Федеральный закон от 27.06.2011 № 161-ФЗ «О национальной платёжной системе» [2] установил правовые и организационные основы функционирования национальной платёжной системы, определил статус операторов платёжных систем, эмитентов электронных денежных средств, ввёл требования к обеспечению безопасности платёжных операций. Данный этап характеризовался переходом от технократического подхода к защите информации к комплексному регулированию финансовых отношений в цифровой среде.

Третий этап (середина 2010-х — начало 2020-х годов) связан с массовым распространением дистанционного банковского обслуживания и возникновением новых форм кибермошенничества, прежде всего социальной инженерии. Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации» в части регулирования дистанционных технологий, а также многочисленные подзаконные акты Банка России создали правовую основу для развития дистанционных финансовых сервисов. Однако стремительное развитие технологий опередило законодательное регулирование, что привело к формированию значительных правовых пробелов и росту масштабов кибермошенничества.

Четвёртый этап (с 2018 года по настоящее время) характеризуется системным подходом к противодействию кибермошенничеству и институциональным строительством в сфере информационной безопасности финансового сектора. Федеральный закон от 11.06.2018 № 167-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части противодействия хищению денежных средств» [5] стал переломным в развитии законодательства, создав правовую основу для механизма приостановки незаконных платежей, легализовав деятельность по антифрод-мониторингу, сформировав правовую базу для информационного обмена об участниках схем хищений [6]. Расширены полномочия Банка России по регулированию информационной безопасности не только в кредитных организациях, но и во всех некредитных финансовых организациях - микрофинансовых организациях, сельскохозяйственных кредитных потребительских кооперативах, ломбардах, страховых и инвестиционных компаниях [6].

Принятие Федерального закона от 01.04.2025 № 41-ФЗ «О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации» [7] знаменует собой переход к принципиально новой модели правового регулирования противодействия кибермошенничеству, основанной на синергетическом взаимодействии всех заинтересованных субъектов в режиме реального времени.

Закон, вступивший в силу 1 июня 2025 года, направлен на комплексное решение проблемы киберпреступности и содержит три взаимосвязанных блока мер, формирующих единую систему противодействия.

Первый блок связан с созданием государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационно-коммуникационных технологий. Система предназначена для обеспечения информационного взаимодействия в режиме реального времени между органами государственной власти, кредитными организациями, операторами связи и иными субъектами. Из обозначенной системы правоохранители могут получить сведения об абонентских номерах, используемых для совершения противоправных действий, а также информация о лицах, причастных к киберпреступлениям [7]. Создание системы представляет собой качественно новый уровень институционализации противодействия кибермошенничеству, обеспечивающий преодоление информационной разрозненности и создание единого информационного пространства безопасности.

Второй блок регулирует деятельность операторов связи и направлен на противодействия спам-рассылкам и обзвонам, являющимися основными каналами мошеннических действий на основе социальной инженерии. Нормативный акт предусматривает обязанность операторов связи маркировать звонки индивидуальных предпринимателей и юридических лиц информацией о категории вызова и наименовании звонящего (до 32 символов) [7]. Вводится запрет на передачу смс-сообщений во время текущего разговора по сотовой связи, что должно препятствовать передаче различных кодов-подтверждений и пресечения схем мошенничества такого типа, которые основаны на психологическом воздействии на жертву.

Третий из представленных блоков содержит специальные требования к кредитным организациям по обеспечению безопасности операций с наличными денежными средствами. Банки обязаны осуществлять контроль за законностью операций при снятии наличных через банкоматы. При выявлении признаков принуждения клиента к операции банк вправе установить лимит снятия наличных в размере 50 тыс. рублей в сутки на срок до 48 часов с обязательным уведомлением клиента. Вводится ограничение на снятие наличных в размере 100 тыс. рублей в месяц для лиц, включённых в базу данных Банка России о случаях осуществления переводов без добровольного согласия клиента [7].

Закон также устанавливает запрет на использование иностранных мессенджеров для органов государственной власти, Банка России, кредитных организаций, страховых компаний, инвестиционных фондов и других субъектов финансового рынка [7], что обусловлено необходимостью обеспечения информационной безопасности и защиты конфиденциальной информации [8, с. 93-96].

Эволюция законодательства в данной сфере прошла путь от технократического подхода к защите информации к комплексной модели, основанной на синергетическом взаимодействии государственных органов, кредитных организаций, операторов связи и иных субъектов. Принятие Федерального закона от 01.04.2025 № 41-ФЗ [7] знаменует собой переход к системному регулированию, основанному на создании единого информационного пространства безопасности и институциональном взаимодействии в режиме реального времени, предупреждение и пресечения киберугроз [9].

Эффективность правового регулирования в значительной степени зависит от преодоления выявленных проблем: устранения пробелов в квалификации киберпреступлений [10, с.34-36], 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.

Список литературы:

[1] Уголовный кодекс Российской Федерации: федер. закон от 13.06.1996 № 63-ФЗ (ред. от 20.02.2026) // Собрание законодательства РФ. 1996. № 25. Ст. 2954.

[2] О национальной платёжной системе: федер. закон от 27.06.2011 №161-ФЗ (ред. от 20.02.2026) // Собрание законодательства РФ. 2011. № 27. Ст. 3872.

[3] Об информации, информационных технологиях и о защите информации: федер. закон от 27.07.2006 № 149-ФЗ (ред. от 29.12.2025) // Собрание законодательства РФ. 2006. № 31 (ч. I). Ст. 3448.

[4] Рябухин С.В. Финансовая безопасность: взгляд законодателя // Финансовая безопасность. 2025. № 1. С. 4-7.

[5] О внесении изменений в отдельные законодательные акты Российской Федерации в части противодействия хищению денежных средств: федер. закон от 11.06.2018 № 167-ФЗ // Собрание законодательства РФ. 2018. № 24. Ст. 3409.

[6] Обеспечение кибербезопасности в кредитно-финансовой сфере / П. Ревенков // Банковское дело. 2019. 6 ноября. - URL: https://www.secuteck.ru/articles/obespechenie-kiberbezopasnosti-v-kreditno-finansovoj-sfere (дата обращения: 18.02.2026).

[7] О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации: федер. закон от 01.04.2025 № 41-ФЗ (ред. от 31.07.2025) // Собрание законодательства РФ. 2025. № 14. Ст. 1542.

[8] Романенко Е.А., Казарцева В.А. Проблемы совершенствования уголовного законодательства и практики его применения в сфере противодействия кибермошенничеству // Синергия. 2025. № 5. С. 93-96.

[9] Киберугрозы финансовой отрасли: прогноз на 2025–2026 гг. / Positive Technologies. 2025. - URL: https://ptsecurity.com/research/analytics/kiberugrozy-finansovoi-otrasli--prognoz-na-2025-2026-g/ (дата обращения: 18.02.2026)

[10] Пикалов П.А. Правовые основы систематизации кибермошенничества по законодательству Российской Федерации // Евразийский юридический журнал. 2025. № 7 (206). С. 34-36.

References:

[1] Criminal Code of the Russian Federation: feder. Law of 13.06.1996 No. 63-FZ (as amended by 20.02.2026) //Collection of Legislation of the Russian Federation. 1996. № 25. Art. 2954.

[2] On the national payment system: feder. Law No. 161-FZ dated 27.06.2011 (as amended on 20.02.2026) //Collection of Legislation of the Russian Federation. 2011. № 27. Art. 3872.

[3] About Information, Information Technology, and Information Security: Feder. Law of 27.07.2006 No. 149-FZ (as amended by 29.12.2025) //Collection of Legislation of the Russian Federation. 2006. No. 31 (part I). Art. 3448.

[4] Ryabukhin S.V. Financial security: legislator's view//Financial security. 2025. № 1. S. 4-7.

[5] On amendments to certain legislative acts of the Russian Federation in terms of countering theft of funds: feder. Law of 11.06.2018 No. 167-FZ//Collection of Legislation of the Russian Federation. 2018. № 24. Art. 3409.

[6] Ensuring cybersecurity in the credit and financial sector/P. Revenkov//Banking. 2019. November 6. - URL: https://www.secuteck.ru/articles/obespechenie-kiberbezopasnosti-v-kreditno-finansovoj-sfere (дата обращения: 18.02.2026).

[7] On the creation of a state information system for countering offenses committed using information and communication technologies, and on amending certain legislative acts of the Russian Federation: feder. Law of 01.04.2025 No. 41-FZ (as amended by 31.07.2025) //Collection of Legislation of the Russian Federation. 2025. № 14. Art. 1542.

[8] Romanenko E.A., Kazartseva V.A. Problems of improving criminal legislation and the practice of its application in the field of countering cyber fraud// Synergy. 2025. № 5. S. 93-96.

[9] Financial Industry Cyber Threats: Forecast 2025-2026/Positive Technologies 2025. - URL: https://ptsecurity.com/research/analytics/kiberugrozy-finansovoi-otrasli--prognoz-na-2025-2026-g/ (дата обращения: 18.02.2026)

[10] P.A. Pikalov. Legal Basis for Systematization of Cyber Fraud under the Legislation of the Russian Federation//Eurasian Legal Journal. 2025. № 7 (206). S. 34-36.

