Северо-Кавказский юридический вестник. 2025. № 2. С. 112–124
North Caucasus Legal Vestnik. 2025;(2):112–124

Проблемы, процессуального, уголовного права и криминологии

Научная статья
УДК 343.721
EDN HTHQAA

Мошенничество в цифровом пространстве и его особенности

Светлана Ивановна Кузина[1], Марина Олеговна Пухкалова[2], Анна Владимировна Цыкора[3]

[1]Южно-Российский институт управления – филиал Российской академии народного хозяйства и государственной службы при Президенте РФ, Ростов-на-Дону, Россия, svivk@yandex.ru
[1]Филиал Московского университета имени С. Ю. Витте, Ростов-на-Дону, Россия
[2]Южный университет (ИУБиП), Ростов-на-Дону, Россия, mop_76@mail.ru
[3]Донской государственный технический университет, Ростов-на-Дону, Россия, ttanneta@mail.ru

Аннотация

Введение. Научно-технический прогресс, определяя соответствующую «новую ступень развития», которая улучшает жизнь людей в части доступности достижений для широкого круга, порождает использование информационных технологий криминальными элементами общества. В этой связи неизбежен рост преступности, основанной на использовании возможностей цифровых технологий, что подтверждается соответствующими отчетами правоохранительной системы. Актуальность рассматриваемой проблемы ежедневно подтверждается публикациями в средствах массовой информации о количестве совершенных в отношении граждан краж и мошенничеств с использованием информационно-телекоммуникационных технологий.

Цель. Охарактеризовать особенности мошенничества в компьютерной сфере, определить ключевые аспекты развития законодательства в отношении киберпреступности.

Теоретические основы. Методы. Теоретическую основу исследования составили научные статьи, статистические отчеты государственных ведомственных структур, материалы судебной и следственной практик. Методологическую основу составляют обще используемые методы научного исследования, применение которых обуславливает выбор системного, деятельностного, функционального и междисциплинарного подходов в изучении актуальной проблемы.

Результаты. В статье раскрываются понятия и обозначаются соответствующие введенные нормы, которые охраняются законодательством в области защиты информации, обозначаются причины необходимости дифференциации ответственности за мошеннические действия, связанные с персональными данными. Кроме того, проведён системный анализ основных видов мошенничества в сети Интернет, который подтвердил актуальность и востребованность рассматриваемой темы.

Выводы. Современное российское уголовное законодательство стоит перед серьезнейшей задачей: необходимостью быстрой разработки и внедрения эффективного механизма пресечения и предупреждения киберпреступлений, которые неизбежно появятся в связи с бурным развитием технологий. На сегодняшний день в России уже реализован широкий спектр мер, направленных на борьбу с киберпреступностью, но при этом данные меры, как правило, сосредоточены на «физической» составляющей – на контроле курьеров, обслуживающей инфраструктуры и оборудования. Однако мир киберпреступлений гораздо сложнее и многограннее, чем просто «железо» и «провода».

Создание специализированных государственных органов и кибервойск, несомненно, является важным шагом на пути к становлению безопасного государства. В этом направлении работы значимым этапом стало создание 11 октября 2022 г. Управления по организации борьбы с противоправным использованием информационно-коммуникационных технологий.

Однако, важно помнить, что это лишь часть решения проблемы, так как для работы указанного ведомства необходимо постоянное совершенствование законодательства, апробация его в правоприменительной практике и адаптация к быстро меняющимся условиям киберпространства, а также тесное взаимодействие между государственными органами, банковским сектором и международным сообществом для быстрого обмена информацией и совместной плодотворной работы над предотвращением киберугроз (кибератак). Без всестороннего подхода, объединяющего технологические, правовые и кадровые аспекты, достижение реальной кибербезопасности останется сложной и долгосрочной задачей нашего государства.

Ключевые слова: киберпреступность, искусственный интеллект, мошенничество в сети Интернет, фишинг, вишинг, схема финансовой пирамиды, фарминг

Для цитирования: Кузина С. И., Пухкалова М. О., Цыкора А. В. Мошенничество в цифровом пространстве и его особенности // Северо-Кавказский юридический вестник. 2025. № 2. С. 112–124. EDN HTHQAA

Problems of Procedural, Criminal Law and Criminology

Original article

Fraud in the digital space and its features

Svetlana I. Kuzina[1], Marina O. Pukhkalova[2], Anna V. Tsykora[3]

[1]South-Russian Institute of Management of Russian Presidential Academy of National Economy and Public Administration, Rostov-on-Don, Russia, svivk@yandex.ru

[1]Branch of the Moscow University named after S. Yu. Vitte, Rostov-on-Don, Russia

[2]Southern University (IMBL), Rostov-on-Don, Russia, mop_76@mail.ru

[3]Don State Technical University, Rostov-on-Don, Russia, ttanneta@mail.ru

Abstract

Introduction. Scientific and technological progress, defining an appropriate "new stage of development" that improves people's lives in terms of accessibility of achievements to a wide range, generates the use of information technology by criminal elements of society. In this regard, the growth of crime based on the use of digital technologies is inevitable, which is confirmed by the relevant reports of the law enforcement system. The relevance of the problem under consideration is confirmed daily by publications in the media about the number of thefts and frauds committed against citizens using information and telecommunication technologies.

Purpose. To characterize the features of fraud in the computer sphere, to identify key aspects of the development of legislation on cybercrime.

Theoretical foundations. Methods. The theoretical basis of the research was made up of scientific articles, statistical reports of government departmental structures, materials of judicial and investigative practices. The methodological basis is made up of commonly used scientific research methods, the application of which determines the choice of systemic, activity-based, functional and interdisciplinary approaches to the study of an urgent problem.

Results. The article reveals the concepts and designates the relevant introduced norms, which are protected by legislation in the field of information protection, and explains the reasons for the need to differentiate responsibility for fraudulent actions related to personal data. In addition, a systematic analysis of the main types of fraud on the Internet was carried out, which confirmed the relevance and relevance of the topic under consideration.

Conclusions. Modern Russian criminal legislation is facing a major challenge: the need to quickly develop and implement an effective mechanism for the suppression and prevention of cybercrimes, which will inevitably appear due to the rapid development of technology. To date, Russia has already implemented a wide range of measures aimed at combating cybercrime, but these measures, as a rule, focus on the "physical" component – on the control of couriers, service infrastructure and equipment. However, the world of cybercrime is much more complex and multifaceted than just hardware and wires. The creation of specialized government agencies and cyber forces is undoubtedly an important step towards becoming a secure State. An important stage in this area of work was the creation on October 11, 2022 of the Office for the Organization of the Fight against the Illegal Use of Information and Communication Technologies. However, it is important to remember that this is only part of the solution to the problem, since the work of this department requires continuous improvement of legislation, its testing in law

enforcement practice and adaptation to the rapidly changing conditions of cyberspace, as well as close cooperation between government agencies, the banking sector and the international community for the rapid exchange of information and joint, fruitful work on prevention cyber threats (cyber-attacks). Without a comprehensive approach combining technological, legal and human aspects, achieving real cybersecurity will remain a difficult and long-term task for our state.

Keywords: cybercrime, artificial intelligence, Internet fraud, phishing, vishing, pyramid scheme, pharming

For citation: Kuzina S. I. , Pukhkalova M. O. Tsykora A. V. Fraud in the digital space and its features. *North Caucasus Legal Vestnik.* 2025;(2):112–124. (In Russ.). EDN HTHQAA

Введение

Интернет-пространство формирует новую сферу для жизни и взаимодействия современного общества. По данным Российской ассоциации электронных коммуникаций и Интернета (РАЭК), в 2020 году число россиян, пользующихся Интернетом, превысило 95 миллионов человек, а на начало 2023 года в РФ насчитывалось 127,6 млн интернет-пользователей, что составляет около 88,2% населения страны. В связи с чем «количество преступных деяний в сети «Интернет» значительно повышается с каждым годом, а уровень раскрываемости киберпреступлений, по данным Генеральной прокуратуры РФ, составляет 4,4%»[1].

Таким образом, одной из важных задач отечественного уголовного законодательства на данном этапе является создание механизма для эффективного пресечения и предупреждения уже существующих киберпреступлений, а также разработка мер по противодействию и контролю новых видов преступлений в рамках киберпространства, такие как преступления с использованием нейронных технологий и искусственного интеллекта.

Авторы статьи при проведении своего исследования ставили **целью** охарактеризовать особенности мошенничества в компьютерной сфере, а также определить ключевые аспекты развития законодательства в отношении киберпреступности.

Теоретические основы. Методы

Теоретическую основу исследования составили научные статьи и публикации. Эмпирическую основу исследования – статистические отчеты государственных ведомственных структур, материалы судебной и следственной практик. Методологическую основу составляют обще используемые методы научного исследования, применение которых обуславливает выбор системного, деятельностного, функционального и междисциплинарного подходов в изучении обозначенной проблемы.

Результаты и обсуждение

Современный прогресс в области цифровых технологий не стоит на месте. Именно эта динамичность и практически безграничные возможности киберпространства создают колоссальные трудности для правоохранительных органов. Требуется фундаментальное изменение подхода к подготовке кадров, включающее не только теоретическую базу, но и практическую отработку методик расследования, использование новейших технологий анализа данных и понимание тонкостей работы нейронных сетей и искусственного интеллекта, использующихся уже в повседневной жизни, бизнесе и государстве.

Интернет играет ключевую роль в современном мире, позволяя людям многое в онлайн-сфере – общение, покупку товаров и услуг, образование, работу и т.п. Также он является платформой для современного бизнеса и банком хранения неограниченного количества данных – конфиденциальных, финансовые и персональные. Федеральным законом от 29.11.2012 № 207-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» в российское уголовное законодательство было внесено несколько изменений, касающихся главы 21 «Преступления против собственности» УК РФ, а именно помимо основной статьи 159 «Мошенничество» УК РФ, были добавлены специальные нормы предусматривающие ответственность за мошенничество совершенные различными способами или в разных областях и сферах общества[2].

[1] О преступлениях, совершаемых с использованием современных информационно-коммуникационных технологий // Официальный сайт Генеральной Прокуратуры Режим доступа: https://genproc.gov.ru/smi/news/genproc/news-1431104/ Загл. с экрана. (Дата обращения: 03.12.2024).

[2] Федеральный закон «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» от 29.11.2012 N 207-ФЗ- // Официальный интернет–портал правовой информации Режим доступа: http://www.pravo.gov.ru. Загл. с экрана. (Дата обращения: 03.12.2024).

После изменения законодательства перед права примирителями встал ряд вопросов относительно того, какие именно объекты охраняются в соответствии с новыми нормами в области защиты данных. Для начала необходимо прояснить причины предложенной дифференциации ответственности за мошеннические действия и рассмотреть какие именно изменения были внесены в законодательство. Предлагается разобрать статью 159.6 «Мошенничество в сфере компьютерной информации» УК РФ как наиболее часто совершаемый состав[1], которая предусматривает состав мошенничества, когда люди добровольно перечисляют деньги злоумышленникам или предоставляют данные своих банковских карт под влиянием заблуждения относительно содержимого веб-сайта. Мошенничество в сфере компьютерной информации предусматривает совершения мошенничества через информационно-телекоммуникационные сети. Указанные мошеннические схемы, разворачивающиеся в сети, целью которых является хищение денежных средств с банковских счетов, мобильных телефонов и электронных кошельков пользователей, отличаются высокой степенью изощренности и масштабируемости, что значительно затрудняет работу правоохранительных органов по их предотвращению и раскрытию.

Один из наиболее распространенных методов – создание поддельных веб-сайтов, практически неотличимых от оригинальных ресурсов банков, платежных систем или популярных онлайн-сервисов. Злоумышленники мастерски копируют дизайн, логотипы, адреса и даже используют SSL-сертификаты, чтобы внушить пользователю доверие и заставить его ввести конфиденциальную информацию: номера банковских карт, пароли, CVV-коды, данные для доступа к онлайн-банкингу и прочее. Получив доступ к этим данным, преступники могут осуществить несанкционированные транзакции, похитив значительные суммы денег. При этом географическая дистанция не является препятствием – мошенничество может быть совершено из любой точки планеты, что делает расследование и преследование виновных невероятно сложным процессом, требующим международного сотрудничества правоохранительных структур. В настоящее время данный способ становится актуальным в период все возможных аукционных распродаж, скидок и предложений дополнительного заработка.

Основные виды мошенничества в сети Интернет представлены на рис. 1.

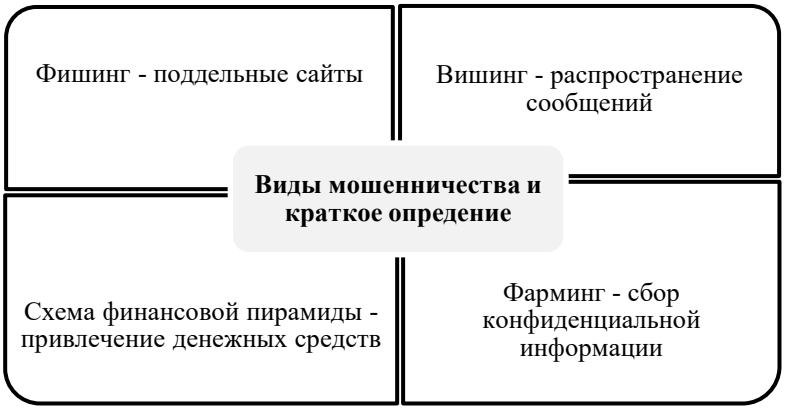

Рис. 1. Основные виды мошенничества в сети интернет
Fig. 1. The main types of fraud on the Internet

Фишинг (англ. phishing, от fishing – рыбная ловля, выуживание) – «вид интернет-мошенничества, который заключается в направлении жертве электронного письма от известного юридического лица» [1, с. 68]. Метод фишинга, который представляет собой рассылку электронных писем, SMS-сообщений или сообщений в мессенджерах, содержащих ссылки на поддельные веб-ресурсы и (или) приложения. Эти сообщения часто маскируются под официальные уведомления от банков, государственных организаций или интернет-магазинов, содержат срочные просьбы о подтверждении данных, угрозы блокировки счетов или обещания получения выгодных предложений. Наживка в таких

[1] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 28.12.2024)) // Собрание законодательства РФ. 17.06.1996, № 25, ст. 2954.

сообщениях зачастую настолько убедительна, что даже опытные пользователи могут стать жертвами обмана.

Вишинг – (англ. vishing – voice phishing – голосовой фишинг) – является распространенной разновидностью сетевого мошенничества. Вишинг схож с фишингом. Отличие вишинга от фишинга состоит в том, что при вишинге используется телефонная связь. Злоумышленники звонят своим жертвам, представляясь сотрудниками банков, служб поддержки, правоохранительных органов или других организаций, и выманивают конфиденциальную информацию под различными предлогами. Они могут использовать психологическое давление, угрозы или манипуляции, чтобы заставить человека раскрыть свои личные данные. «Такими конфиденциальными данными могут являться: номер банковской карты, пароли от личного кабинета мобильного банка, PIN-коды, приходящие в смс, коды доступа или другую личную информацию в тоновом наборе» [2, с. 118]. Такие сообщения могут распространяться и через игры, акцентируя внимание на подростковом поколении, и социальные сети, мессенджеры.

Схема финансовой пирамиды, применяемая в настоящее время в сфере интернет-инвестиций и быстрого заработка, полностью аналогична классической финансовой пирамиде. Обещания быстрой и высокой прибыли привлекают множество жертв, которые вкладывают свои средства и заемные в том числе, полагаясь на ложные обещания организаторов пирамиды. В конечном итоге, большинство участников таких схем терпят убытки, а организаторы уносят с собой украденные деньги.

Фарминг (англ. farming – фермерство), однако «здесь пользователя компьютера обманывают программным способом, как правило, путем применения вредоносного программного обеспечения, способного изменять навигационную систему компьютера» [3, с. 25]. Это более изощренный вид мошенничества, при котором злоумышленники перенаправляют трафик с легитимных веб-сайтов на свои поддельные ресурсы. Это осуществляется путем подмены DNS-записей или инфицирования компьютера зловредным программным обеспечением. Жертва, введя в адресной строке браузера правильный адрес, попадает на поддельный сайт, где может быть обманута и лишена своих средств. Такие программы рассылаются в мессенджерах, на электронные почты. Сейчас распространен такой вид фарминга в форме сообщений «Это ты на фото посмотри» и ссылка на вредоносное программное обеспечение, жертва переходит по ссылке, далее уже работает прикрепленный вирус, он получает доступ ко всем данным телефона – к банковским приложениям и контактам. Когда достигнута последняя цель вирус начинает рассылать сообщение с такой же информацией всем контактам первоочередной жертвы.

В борьбе с киберпреступностью крайне важно повышать осведомленность пользователей о существующих методах мошенничества. Необходимо быть внимательными при получении подозрительных электронных писем, SMS-сообщений и телефонных звонков, не переходить по ссылкам из неизвестных источников, не раскрывать конфиденциальную информацию третьим лицам и использовать только надежные антивирусные программы и средства защиты от киберугроз. Только совместными усилиями пользователей и правоохранительных органов можно эффективно противостоять распространению киберпреступности и защитить себя от мошеннических действий в интернете.

Другой распространенный способ мошенничества – «рассылка ложных сведений от лица финансовых, кредитных и других организаций. Мошенники общаются с жертвой, выдавая себя за сотрудников указанных организаций, и требуют передачи ими определенных сведений, в том числе финансовых. Это дает возможность мошенникам получить доступ к денежным средствам жертвы или иным ее финансовым инструментам. Еще один распространенный способ мошенничества - размещение в сети «Интернет» несуществующих предложений о продаже товаров или услуг на выгодных условиях. Жертве предлагается внести определенную сумму денежных средств в качестве предоплаты, но после их получения все контакты прекращаются, сайты и интернет-страницы блокируются или удаляются, телефоны аннулируются» [4, с. 90-91].

Профессор Е. Р. Россинская указывает на то, что: «способы компьютерных преступлений являются полно структурными, причем могут быть выбраны различные технологии подготовки, совершения и сокрытия, слабо коррелирующие с видом преступления» [5, с. 195]. Вместе с тем необходимо учитывать, что «указанные виды преступного поведения достаточно латентны, развиты, а потому принять своевременное решение о том, что в отношении конкретного лица было совершено преступление не всегда представляется возможным» [6, с. 290]. Что говорит нам о еще одной стороне рассматриваемых деяний – это их латентности в обществе, не все потерпевшие обращаются

к правоохранительным органам с целью поиска преступников, так как считают, что вернуть свои средства не представляется возможным. Латентны преступления с наименьшим ущербом, но если мы посчитаем комплексный ущерб от мошенничеств небольшой тяжести в сумме, то официальная статистика увеличится еще в несколько раз.

Для каждого способа мошенничества в сети Интернет будут свои способы предупреждения, профилактики и избегания мошеннических уловок.

Некоторые из них включают: «Установка антивирусных программ и firewall (рус. межсетевой экран) на компьютере. Эти программы помогают обнаружить и предотвратить атаки злоумышленников, которые пытаются получить доступ к компьютеру и украсть личные данные. Использование сложных паролей и двухфакторной аутентификации. Это поможет защитить ваш аккаунт от взлома. Никогда не используйте один и тот же пароль для нескольких аккаунтов. Осторожность при нажатии на ссылки и скачивании файлов. Никогда не открывайте вложения от незнакомых отправителей и не переходите по ссылкам, которые кажутся подозрительными. Использование защищенных соединений. При покупках онлайн убедитесь, что сайт использует защищенное соединение и имеет SSL-сертификат. Цифровой сертификат (SSL-сертификат) – это электронный или печатный документ, подтверждающий принадлежность владельцу открытого ключа или каких-либо атрибутов» [7, с. 32]. Предоставление личных данных только на доверенных сайтах, детальное изучение реквизитов вебстраниц, которые размещаются на хостинге, уникального доменного имени и иных технических данных, с целью обезопасить свои личные сведения на сайтах, которые кажутся ненадежными. Подача заявления в правоохранительные органы, если становишься жертвой мошенничества в сети Интернет. Проведение образовательной работы по повышению уровня информированности людей об опасностях в Интернете и методах защиты от мошенничества. Курсы по информационной безопасности, семинары и мероприятия, проводимые правительственными и частными организациями, могут помочь людям узнать о различных видах мошенничества и научиться защищаться от них.

В свою очередь особенности видов мошенничества в сети Интернет разграничиваются по сфере общественных отношений, в которой совершаются преступления, предмет и способ совершения преступления. Особенность состава преступления заключается в том, что при модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки, передачи компьютерной информации или информационно-телекоммуникационных сетей, а именно в банковский счет и таким обманным путем будут похищены безналичные средства платежа.

Уголовное деяние в сфере информационно-телекоммуникационных технологий считается оконченным с момента похищения денежных средств или электронных денег, а не с момента их использования.

Работа правоохранительных органов часто сталкивается со сложными случаями, где преступные действия демонстрируют признаки, характерные для мошенничества, но одновременно обладают и другими, не позволяющими однозначно квалифицировать их именно как мошенничество. Это создает значительные трудности для следователей и оперативных сотрудников, требуя от них глубокого анализа всех обстоятельств дела, кропотливого изучения деталей и тщательного сопоставления фактов с нормами действующего законодательства. Отсутствие четкой, однозначной квалификации влечет за собой риск неправильного применения закона, что может привести к несправедливому осуждению или, наоборот, к безнаказанности преступника. Подобные ситуации требуют не только высокого профессионализма, но и огромного опыта, способности к логическому мышлению и умения разбирать сложные, запутанные цепочки событий. В частности, любая ошибка в квалификации может иметь далеко идущие последствия, в том числе и для жертвы преступления.

Особую сложность представляет мошенничество в сфере компьютерной информации. Хотя включение ответственности за него в главу 21 УК РФ (посягательства на собственность) указывает на основной объект преступного посягательства – имущественные отношения, реальность оказывается значительно сложнее. Дело в том, что компьютерные преступления часто затрагивают и другие правоотношения, например, связанные с информационной безопасностью. Здесь мы сталкиваемся не только с посягательством на имущество, но и с нарушением конфиденциальности, несанкционированным доступом к информации, повреждением данных и другими видами вреда, не всегда поддающимися простой денежной оценке.

Мошенничество в компьютерной сфере характеризуется активными действиями со стороны преступника. В отличие от традиционных способов мошенничества, основанных на обмане или злоупотреблении доверием, киберпреступления имеют свои специфические черты, проявляющиеся

в объективной стороне преступления. Статья 159.6 УК РФ описывает эти особенности, упоминая такие действия, как введение, удаление, блокирование или модификация компьютерной информации, а также «иное вмешательство»[1]. Рассмотрим подробнее каждый из этих терминов, чтобы полнее понять суть и сложность квалификации подобных преступлений.

Введение информации – это не простое добавление данных, а целенаправленное внесение информации в конкретную базу данных, часто с использованием специальных программных средств или технических устройств. Это может быть введение ложных сведений, фальсификация данных, подмена информации или добавление информации, предназначенной для введения в заблуждение. Необходимо тщательно изучать методы, использованные преступником, для определения намерений и степени вреда, нанесенного жертве.

Удаление информации – это полное или частичное уничтожение данных. Здесь важно определить значимость удалённой информации, ее ценность для жертвы и цели преступника. Было ли удаление целенаправленным актом мошенничества, или это было случайным действием, не имеющим прямого отношения к мошенническим целям.

Блокирование информации – это ограничение доступа к информации. Это может быть временное или постоянное блокирование, полное или частичное. Цель такого действия – часто вымогательство, блокирование важной информации в обмен на выкуп. Важно установить цель преступника и ущерб, нанесенный жертве в результате блокирования информации.

Модификация информации – это изменение существующих данных. Это может быть изменение цифр на банковском счете, изменение персональных данных, подмена документов и т.д. Важно определить характер изменений и их влияние на правоотношения между участниками.

Иное вмешательство – это широкое понятие, охватывающее все прочие действия, связанные с неправомерным доступом и манипуляциями с компьютерной информацией. Это может быть вирусное поражение, несанкционированный доступ к системе, отказ в обслуживании и другие действия, направленные на нарушение нормального функционирования компьютерных систем и причинение вреда жертве.

Квалификация мошеннических действий в сфере компьютерной информации требует глубокого анализа всех обстоятельств дела, тщательного изучения действий преступника, целей преступления и нанесенного вреда. Только при учете всех нюансов можно принять обоснованное решение и правильно квалифицировать совершённое преступление.

Нашему законодателю также необходимо ввести новые правовые положения, регулирующие ответственность за «фишинг», а также более тщательно контролировать оборот биометрических данных. Биометрия может использоваться для множества целей, в том числе для общественно-опасных. В России уже действует система «Госуслуги.Биометрия», облегчающая такие действия, как получение банковских услуг, заключение договоров связи и оформление электронной подписи. Однако без надёжной защиты эти технологии могут стать целями для злоумышленников, пытающихся использовать личные данные жертв для совершения юридически значимых действий.

Подобно технологии «deepfake», о которой говорилось ранее, «фишинг» также «не имеет официального определения в российском законодательстве, что значительно затрудняет его квалификацию. Однако проблематика «фишинга» в нашем праве уже толковалась. В 2017 году Верховный суд Российской Федерации дал подробные разъяснения относительно правовых аспектов мошенничества в сфере компьютерной информации»[2]. Согласно этим разъяснениям, «фишинг» необходимо квалифицировать как кражу, а не как мошенничество.

Однако мы считаем, что верховному суду требовалось более подробно рассмотреть специфику «фишинга», поскольку деяние всегда проходит без непосредственного контакта между преступником и жертвой, но не обязательно совершается тайно, как кража. Поэтому, в науке предлагается «квалифицировать «фишинг» по статье 159.6 как мошенничество в сфере компьютерной информации» [8, с. 52–57], что представляется более разумным и рациональным, однако полностью не раскрывает суть явления.

[1] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 28.12.2024)) // Собрание законодательства РФ. 17.06.1996. № 25. Ст. 2954.

[2] Постановление Пленума Верховного Суда Российской Федерации о 30.11.2017 №48 «О судебной практике по делам о мошенничестве, присвоении и растрате» // Российская газета. 11.12.2017. № 280.

Под статью 159.6 подпадает вмешательство в работу информационных систем, но «фишинг» обычно строится на обмане пользователей через сообщения или звонки. Поэтому необходимо разрабатывать отдельную статью для наказания за «фишинг» и установить его описание в нормативных актах. Поэтому на данном этапе требуется предусмотреть отдельный уголовно-правовой состав для нового вида преступления – «фишинга» и ответственность за его совершение, а также в рамках других нормативных правовых актов установить описание его видов.

Мы считаем, что ключевой составляющей развития уголовного законодательства в сфере киберпреступности также должна стать формализация принципов стратегического противодействия этим видам преступлений с целью обеспечения успешного реагирования на ее проявления. «Важными составляющими такой стратегии могут стать создание в каждом регионе специализированных подразделений, непосредственно занимающихся детальной разработкой местного законодательства и внедрением различных программ по профилактике киберпреступлений, а также соответствующая подготовка и повышение квалификации правоохранительных и судебных органов в этой сфере» [9].

Мы убеждены, что ключевым аспектом развития законодательства в отношении киберпреступности должно стать создание стратегии противодействия таким преступлениям для обеспечения более эффективного ответа на их появление. Элементы этой стратегии могут включать создание специализированных подразделений в каждом регионе для детальной проработки местного законодательства, внедрение программ профилактики киберпреступлений и повышение квалификации сотрудников правоохранительных и судебных органов.

Также на данном этапе крайне важно опираться не только на собственный опыт борьбы с киберпреступностью, но и анализировать последние международные методики и лучшие практики, подходы к классификации и криминализации преступлений в сфере компьютерной информации. Международный обмен информацией по новым видам преступлениям может способствовать изменению или созданию законодателем нормативных правовых актов, касающихся информационной сети, поскольку каждая уголовная политика имеет свои уникальные элементы.

В этой связи необходимо провести анализ раздела обзора о состоянии преступности в Российской Федерации за январь-декабрь 2024 г., представленного ФКУ «Главным информационно-аналитическим центром» Министерства внутренних дел Российской Федерации, в ходе которого можно сделать вывод о том, что принимаемые государством меры по противодействию преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий приносят положительные результаты в одних складывающихся условиях и имеют некоторые сложности в других ситуациях. Сводную информацию можно видеть в табл. 1[1].

Так, не наблюдается общее снижение рассматриваемого вида преступлений, всего количество деяний, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации увеличилось на 13,1% по сравнению с аналогичным периодом 2023 г., имеется снижение на 13,1% преступлений, совершенных с использованием или применением: расчетных (пластиковых) карт, на 61,8% с использованием фиктивных электронных платежей и значительное снижение мошенничества с использованием электронных средств платежа ст. 159.3 УК РФ на целых 88,9% и на 25,9 % – мошенничества в сфере компьютерной информации ст. 159.6 УК РФ, что подтверждает правильную и компетентную работу правоохранительной системы в данной сфере.

Возможно на динамику повлияло отключение трансграничных платежей по международным картам, а также нахождение существенной доли «бенефициаров» и исполнителей мошеннических схем за пределами Российской Федерации, которые на время потеряли возможность работать**, з**амедление общих темпов роста мошеннических атак на критические объекты инфраструктуры и банковские предприятия. Многие компании успели выработать и внедрить меры по защите своих ресурсов, адаптироваться к новым условиям работы**.** Переориентация мошенников на другие задачи, взаимодействие МВД России и Центральным Банком России, в рамках которого в режиме реального времени организован информационный обмен между госорганами, практически исключён пропуск иностранного трафика с использованием подмены телефонных номеров, также банкам предоставлено право на двое суток приостанавливать операции по переводу средств со счетов клиентов.

[1] Режим доступа: https://мвд.рф/reports/item/60248328/file:///C:/Users/An/Downloads/Sbornik_UOS_2024.pdf. Загл. с экрана. (Дата обращения: 20.03.2025).

Таблица 1 – Сведения о преступлениях, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации за 2024 год

Table 1 – Information on crimes committed using information and telecommunication technologies or in the field of computer information in 2024

Сведения о преступлениях, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации	Зарегистрировано (в отчетном периоде)		В том числе, выявленных сотрудниками		
	Всего	+,- в %	Следственных органов Следственного комитета Российской Федерации	Органов внутренних дел	Органов Федеральной службы безопасности
Всего преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации	765365	13,1	2862	755094	4890
из них тяжких и особо тяжких	369267	7,8	1847	363375	3060
в том числе совершенных с использованием или применением: расчетных (пластиковых) карт	115469	-13,1	339	114734	242
компьютерной техники	42347	16,4	225	40357	1197
программных средств	13461	10,6	82	13023	251
фиктивных электронных платежей	615	-61,8	4	536	63
сети «Интернет»	649064	23,2	2273	640897	4035
средств мобильной связи	346035	14,3	560	344070	980
в том числе кража ст. 158 УК РФ	105937	-11,1	454	105330	27
мошенничества ст. 159, 159.3, 1159.6 УК РФ	380344	6,8	222	379445	278
из них мошенничества ст. 159 УК РФ	379762	7,5	213	378887	267
мошенничества с использованием электронных средств платежа ст. 159.3 УК РФ	273	-88,9	6	261	2
мошенничества в сфере компьютерной информации ст. 159.6 УК РФ	309	-25,9	3	297	9

К положительным примерам также мы можем отнести, частичный рост уровня финансовой грамотности населения, граждане всё чаще распознают уловки мошенников и передают их номера для блокировки, осуществляется информировании о том, что денежные средства на счёте потерянной/найденной карты принадлежат её владельцу, а их незаконное использование влечёт уголовную ответственность, что необходимо уведомить о находке кредитную организацию (по телефону горячей линии или в отделении банка). Сообщения в информационном поле и на стендах кредитных организаций о том, что если поблизости есть офис финансовой организации, выпустившей найденную карту, можно отнести её туда - сотрудник банка заблокирует доступ к карте, утилизирует пластик и сообщит владельцу об этом. В научных трудах имеются обобщения данного вида криминальных явления, например, Д. Н. Ветровым предложены следующие способы совершения хищений:

«• Использование найденной и ли украденной карточки для оплаты товаров и услуг или/и получения наличных денег из банкоматов,

• Подделка самой пластиковой карты или ее оттисков,
• Получение незаконным путем оттисков настоящей пластиковой карты,
• Мошенничество с картами, не полученными законным держателем,
• Получение преступниками настоящих пластиковых карт путем оформления заявок на подставных лиц,
• Использование слабых мест технологии обработки платежей, совершенных с помощью «пластиковых» денег,
• Мошенничества, совершаемые законными держателями пластиковых карт» [10, с. 48-49].

Снижение на 11,1 % в категории кража ст. 158 УК РФ объективно объясняется изменением квалификации деяний в процессе предварительного следствия и судебного разбирательства, связанные с разъяснениями данными Верховным судом Российской Федерации, так как судебная практика по применению приведённых в отчете статей противоречива По остальным показателям имеется положительный рост. Также, как мы видим, большая доля мошенничеств в информационной среде выявляются сотрудниками органов внутренних и относятся к их компетенции, что подтверждает загруженность следователей указанным видом преступлений при значительном кадровом дефиците.

Заключение

Действующее российское законодательство в сфере киберпреступности нуждается в обновлении и совершенствовании. На данном этапе важно «разработать меры по предупреждению и пресечению киберпреступлений, повышению уровня их раскрываемости, а также на формирование эффективного законодательного механизма, направленного на совершенствование и регулирование проблемных или неурегулированных проблем данной сферы» [11].

Нельзя не обозначить проблему нехватки специализированных средств и современных методов расследования – одна из главных проблем. Ситуация осложняется недостаточной подготовкой сотрудников правоохранительных органов в сфере кибербезопасности. Многие специалисты, работающие в традиционных областях правоохранительной деятельности, просто не обладают необходимыми знаниями и навыками для эффективного расследования киберпреступлений. Также, необходимо серьезно усилить материально-техническое обеспечение подразделений, занимающихся расследованием киберпреступлений. Это касается как специального программного обеспечения для анализа данных и выявления преступной активности, так и современного оборудования для мониторинга сети и проведения оперативно-розыскных мероприятий. Без значительного увеличения финансирования этих направлений реально эффективная борьба с киберпреступностью будет невозможна.

В результате рассмотренных и новых постоянно обновляющихся опасностей в киберпространстве необходимо реализовать комплексную стратегию противодействия киберпреступности как на национальном, так и на международном уровне, а также разработать конкретные методы борьбы с этой проблемой.

По результатам исследования и анализа статистических данных относительно числа кибератак за начало 2023 г., численности интернет-пользователей, наиболее популярных социальных сетей в РФ, расценок на услуги киберпреступников в Telegram, были сделаны следующие выводы: происходит непрерывный рост числа интернет-пользователей, в том числе хакеров, в связи с чем расценки на их услуги понижаются, и растет количество совершаемых кибератак, однако в данной ситуации число таких атак может зависеть и от других факторов, например, международная обстановка, процесс совершенствования IT-технологий, репутация юридических лиц и другое[1].

По результатам изучения данных статистики МВД РФ за 2023 год, исходя из которых наблюдался стабильный рост киберпреступности, были сформулированы следующие причины: в качестве положительных выступает возможное повышение качества работы правоохранительных органов, однако, можно назвать и ряд негативных причин. В их число входит достаточно сложная система киберпространства, а также широкий масштаб распространения киберпреступлений.

Из этих двух причин вытекает третья – достаточно долгий процесс расследования данного вида преступлений. Также стоит отметить, что большинство из них латентны в виду факта сокрытия

[1] DIGITAL 2023: Глобальный обзорный отчет // DataReportal: сайт. Режим доступа: https://datareportal.com/reports/digital-2023-global-overview-report. Загл. с экрана. (Дата обращения: 03.12.2024).

либо профессиональных навыков преступников и др. Зачастую, ввиду строгой «палочной системы» в органах МВД РФ, ввиду бесперспективности дела, сотрудники в статистических карточках указывают другую квалификацию совершенного преступления (обычное мошенничество вместо кибермошенничества – 159 УК РФ вместо 159.6 УК РФ и др.)

Одним из достаточно проблемных аспектов раскрытия подобного вида преступлений является анонимизация интернет-пространства (мессенджер Telegram). Участились случаи мошенничества с использованием усовершенствованных мошеннических схем. По результатам анализа данных уровня защищенности крупнейших российских компаний от кибератак, было установлено, что порядка 96 % компаний имеют уязвимости в своих IT-системах, что говорит о высоком риске атак на их кибербезопасность, а затем и на конфиденциальные данные и счета в банках[1]. Следует подчеркнуть, что регулирование информационной сферы, с учетом сложившейся современной обстановки и мощной активизации преступной деятельности, требует особого внимания.

Также стоит отметить, что создание специализированных государственных органов и киберв войск является важным шагом на пути к становлению безопасного государства. Как показывает практика, без правильного и эффективного правового регулирования целесообразность любых нововведений теряется, поэтому, считаем необходимым, провести пересмотр действующего законодательства и внести соответствующие изменения, для защиты национальных интересов и борьбы с постоянно растущими киберугрозами.

В эпоху цифровизации решение о том, как организовать подобное подразделение – создать отдельное ведомство или включить его в состав уже существующих силовых структур, таких как ФСБ, МВД или Росгвардия, требует детального анализа задач, возможностей и особенностей данных служб.

Создание отдельного самостоятельного ведомства («Кибервойска») конечно же имеет ряд преимуществ:

- отдельное ведомство будет полностью сосредоточено на предотвращении и расследовании киберугроз, включая как внешние (хакерские атаки из-за рубежа), так и внутренние.

- сможет координировать усилия между различными государственными структурами, включая министерства, силовые ведомства и другие органы, то есть иметь высшую степень координационной деятельности.

- позволит объединить человеческие ресурсы различных специалистов по кибербезопасности из разных ведомств, возможно стран, что обеспечит единый подход к поставленным задачам с использованием передовых технологий.

В этом контексте стоит отметить, что привлечение экспертов и специалистов из гражданских отраслей IT может проходить более лояльнее нежели при приеме на службу в традиционных силовых структурах.

- двойственность возложенных функций (оборона и нападение) - защита критической инфраструктуры/предотвращение атак и ответная реакция в отношении противников в рамках национальной стратегии.

Но не стоит забывать, что формирование нового ведомства потребует значительных ресурсов, включая инфраструктуру, штат сотрудников и материально-техническую базу, увеличение бюрократической нагрузки на систему госуправления.

Создание специализированной службы в рамках существующих ведомств представляется более экономически эффективным решением, так как, например, ФСБ уже отвечает за защиту национальной безопасности, включая кибербезопасность, и имеет соответствующий опыт и ресурсы, при сосредоточении только на внутренней безопасности, что может уменьшить внимание к международным аспектам киберугроз; МВД активно занимается расследованием киберпреступлений и уже имеет подразделения, отвечающие за борьбу с киберпреступностью в уголовном направлении; Росгвардия обеспечивает защиту стратегически значимых объектов, что можно дополнить задачами защиты критической информационной инфраструктуры, но служба ориентирована на физическую безопасность, и кибер-фокус для ведомства полностью не соответствует профилю.

В связи с этим, авторам представляется оптимальным вариантам создание гибридной модели: создание службы в одном из существующих ведомств с усиленной координацией и автономией.

[1] Positive Technologies: 96% крупнейших компаний России уязвимы к кибератакам // Режим доступа: https://habr.com/ru/news/699628/. Загл. с экрана. (Дата обращения: 20.03.2025).

Создание отдельного ведомства («Кибервойска») выглядит перспективно, но на данном этапе может быть слишком затратным и избыточным. Оптимальным решением является создание специализированной автономной службы в рамках ФСБ, которая будет сосредоточена на защите критической инфраструктуры и данных, предотвращении международных атак, а также на проведении наступательных кибероперациий. Это также обусловлено тем, что ФСБ уже играет ключевую роль в сфере национальной безопасности, а защита в цифровой сфере является её неотъемлемой частью.

Список источников

1. Дерюгин Р. А. О современных способах совершения мошенничества, связанного с использованием персональных данных пользователей сети интернет // Криминалистика: вчера, сегодня, завтра. 2023. №1 (25). С. 65–74.
2. Фадина Ю. П. Уголовно-правовая характеристика мошенничества в сети Интернет // Вестник Югорского государственного университета. 2017. № 1-2 (44). С. 117–121.
3. Бахтеев Д. В. О некоторых современных способах совершения мошенничества в отношении имущества физических лиц // Российское право: образование, практика, наука. 2016. № 3 (93). С. 24–26.
4. Милованова М. М., Шурухнов В. А. О способах мошенничества в сети «Интернет» // Имущественные отношения в РФ. 2021. №10 (241). С. 86–92.
5. Россинская Е. Р. Концепция учения об информационно-компьютерных криминалистических моделях как основе методик расследования компьютерных преступлений // Вестник Восточно-Сибирского института МВД России. 2021. № 2 (97). С. 190–200.
6. Каражеляскоов Б. А., Карпушева Л. Н., Юнусов М. Ф. Проблемы уголовной ответственности в сети интернет // Образование и право. 2022. № 11. С. 289–292.
7. Зубишин С. А. Роль SSL сертификатов в безопасной передаче данных // Молодой исследователь Дона. 2021. № 3 (30). С. 32–36.
8. Тарапанова Е.Л., Добкач Л.Я. Информационная безопасность личности // Вектор науки Тольяттинского государственного университета. Серия: Юридические науки. 2019. №3 (38). С. 52–57.
9. Крицкая Е. В. Цифровое мошенничество: современные тенденции, способы защиты и превенции // Молодой ученый. 2020. № 50 (340). С. 258–263.
10. Ветров Д. Н. Предупреждение хищений при использовании пластиковых денег в современных банковских системах (криминологический аспект): дис. … канд юрид наук. М., 1998. 185 с.
11. Кузнецов П. С. Проблемы расследования преступлений в сфере компьютерной информации // Молодой ученый. 2020. № 15 (305). С. 210–212.

References

1. Deryugin R. A. On modern methods of committing fraud related to the use of personal data of Internet users. *Criminalistics: yesterday, today, tomorrow.* 2023;1(25):65–74. (In Russ.)
2. Fadina Yu. P. Criminal and legal characteristics of fraud on the Internet. *Bulletin of Ugra State University*. 2017;1-2 (44):117–121. (In Russ.)
3. Bakhteev D. V. On some modern methods of fraud against the property of individuals. *Russian law: education, practice, science.* 2016;3(93):24–26. (In Russ.)
4. Milovanova M. M., Shurukhnov V. A. On the methods of fraud on the Internet. *Property relations in the Russian Federation.* 2021;10(241):86–92. (In Russ.)
5. Rossinskaya E. R. The concept of the doctrine of information and computer forensic models as the basis of methods for investigating computer crimes. *Bulletin of the East Siberian Institute of the Ministry of Internal Affairs of Russia.* 2021;2(97):190–200. (In Russ.)
6. Karazhelyaskov B. A., Karpusheva L. N., Yunusov M.F. Problems of criminal liability on the Internet. *Education and Law.* 2022;(11):289–292. (In Russ.)
7. Zubishin S. A. The role of SSL certificates in secure data transmission. *Young Researcher of the Don.* 2021;3(30):32–36. (In Russ.)
8. Tarapanova E. L., Dobkach L. Ya. Information security of personality. *Vector of Science of Tolyatti State University. Series: Legal Sciences.* 2019;3(38):52–57. (In Russ.)
9. Kritskaya E. V. Digital fraud: current trends, methods of protection and prevention. *Young Scientist.* 2020;50(340):258–263. (In Russ.)

10. Vetrov D. N. *Prevention of theft when using plastic money in modern banking systems (criminological aspect):* dis. ... Candidate of Law. Moscow; 1998. 185 p. (In Russ.)

11. Kuznetsov P. S. Problems of investigation of crimes in the field of computer information. *Young scientist.* 2020;15(305):210–212. (In Russ.)

Информация об авторах

С. И. Кузина, – доктор политических наук, профессор, ЮРИУ РАНХиГС; профессор, филиал Московского университета имени С.Ю. Витте в г. Ростове-на-Дону.

М. О. Пухкалова – кандидат юридических наук, доцент кафедры уголовно-правовых дисциплин, Южный университет (ИУБиП), судья в отставке.

А. В. Цыкора – кандидат юридических наук, доцент, ДГТУ.

Information about the authors

S. I. Kuzina – Dr. Sci. (Polit.), Professor, South-Russian Institute of Management of Russian Presidential Academy of National Economy and Public Administration; Professor, Branch of the Moscow University named after S. Yu. Vitte in Rostov-on-Don.

M. O. Pukhkalova – Cand. Sci. (Law), Associate Professor of the Department of Criminal Law Sciences, Southern University (IMBL).

A. V. Tsykora – Cand. Sci. (Law), Associate Professor, Don State Technical University.

Вклад авторов: все авторы сделали эквивалентный вклад в подготовку публикации. Авторы заявляют об отсутствии конфликта интересов.

Contribution of the authors: the authors contributed equally to this article. The authors declare no conflicts of interests.

Статья поступила в редакцию 24.03.2025; одобрена после рецензирования 14.05.2025; принята к публикации 16.05.2025.
The article was submitted 24.03.2025; approved after reviewing 14.05.2025; accepted for publication 16.05.2025.