Научная статья
УДК 343.85:[343.72:004]

СОВЕРШЕНСТВОВАНИЕ ЗАКОНОДАТЕЛЬСТВА В СФЕРЕ ПРОТИВОДЕЙСТВИЯ КИБЕРУГРОЗАМ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

Константин Борисович Толкачев
Государственное Собрание – Курултай Республики Башкортостан
Уфа, Россия, gskrb@bashkortostan.ru

Аннотация. Статья посвящена исследованию состояния законодательства в сфере противодействия киберугрозам различного характера – от интернет-мошенничества до кибервойны. Дается обзор киберрисков в современном обществе за последние несколько лет, анализируется эффективность как уже принятых, так и только еще разрабатывающихся законодательных решений в сфере цифровых взаимоотношений и борьбы с киберугрозами. На основе анализа правоприменения соответствующих федеральных законов автором выработаны собственные предложения по дальнейшему совершенствованию соответствующей области права, а также сделан вывод о необходимости и неизбежности разработки и принятия в обозримом будущем Цифрового (Информационного) кодекса Российской Федерации.

Ключевые слова: национальная безопасность, киберугрозы, киберпреступность, кибермошенничество, кибервойна, интернет-мошенничество, цифровое право, информационное право, цифровой кодекс, информационный кодекс, инфокодекс, информация, IT, финансы, цифровая трансформация.

Для цитирования: Толкачев К. Б. Совершенствование законодательства в сфере противодействия киберугрозам национальной безопасности // Вестник Уфимского юридического института МВД России. 2025. № 3 (109). С. 102–115.

Original article

IMPROVING LEGISLATION IN THE FIELD OF COUNTERING CYBER THREATS TO NATIONAL SECURITY

Konstantin B. Tolkachev
The State Assembly – the Kurultay of the Republic of Bashkortostan
Ufa, Russia, gskrb@bashkortostan.ru

Abstract. The article is devoted to the study of the state of legislation in the field of countering cyber threats of various types – from Internet fraud to cyber warfare. An overview of cyber risks in modern society over the past few years is given, and the effectiveness of both already adopted and newly developed legislative decisions in the field of digital relationships and combating cyber threats is analyzed. Based on the analysis of the enforcement of relevant federal laws, the author has developed his own proposals for further improvement of the relevant area of law, and concluded that it is necessary and inevitable to develop and adopt a Digital (Information) Code of the Russian Federation in the foreseeable future.

Keywords: national security, cyber threats, cybercrime, cyber fraud, cyberwar, internet fraud, digital law, information law, digital code, information code, infocodex, information, IT, finance, digital transformation.

For citation: Tolkachev K. B. Improving legislation in the field of countering cyber threats to national security // Bulletin of Ufa Law Institute of the Ministry of Internal Affairs of Russia. 2025. No. 3 (109). P. 102–115. (In Russ.)

Введение

Проблема киберугроз и тех рисков, которые они несут с собой для национальной безопасности, с каждым годом обретает все большую популярность в реалиях современной цифровой эпохи.

По данным МВД России за последние пять лет число правонарушений в цифровой среде выросло более чем в два раза. Сегодня их доля в общем массиве всех преступлений составляет около 40 %, а среди тяжких и особо тяжких преступлений этот показатель достигает 60 %[1]. За 2023 год ущерб от кибермошенничеств превысил 156 миллиардов рублей, а по итогам 2024 года озвучена уже сумма в 200 миллиардов рублей. При этом надо понимать, что даже такие внушительные показатели не отражают в действительности всей полноты проблемы и того колоссального материального урона, который наносят действия киберпреступников частным лицам, хозяйствующим субъектам и национальной экономике в целом. Это лишь верхушка айсберга, поскольку огромное количество киберпреступлений, особенно совершенных против граждан, остается неучтенным и не фигурирует в официальной статистике. При этом и сами по себе официальные данные зачастую оказываются довольно противоречивы, что также сигнализирует о фактически более значимом ущербе от действий мошенников. Так, если по данным МВД России в 2024 году ущерб от киберпреступлений составил обозначенные выше 200 миллиардов рублей, то по данным Сбербанка только с помощью телефонного мошенничества преступники похитили со счетов россиян в 2024 году не менее 295 миллиардов рублей[2]. Также большую тревогу вызывает такая негативная тенденция, как ежегодно снижающийся уровень раскрываемости киберпреступлений на фоне взрывного роста их количества – в 2024 году раскрываемость составила всего 23 %[3].

С учетом того, что киберпреступления достаточно разноплановы по своему характеру, угрозу национальной безопасности, которую они несут, следует также понимать достаточно широко. Речь в данном случае не только о безопасности функционирования военных объектов, предприятий оборонно-промышленного комплекса и в целом стратегически важных производств. С учетом надежной защиты их баз данных и постоянной готовности к кибератакам в данном направлении обозначенная проблема здесь хоть и не сходит с повестки, но носит частный характер, атаки единичны, а удачное их число и вовсе сведено к минимуму. Поэтому угрозу национальной безопасности со стороны кибермошенников следует понимать и как угрозу безопасности функционирования всех цифровых ресурсов органов государственной власти разного уровня, органов местного самоуправления, где уровень защиты уже существенно ниже, риски выше, атаки чаще, а также как угрозу цифровой безопасности каждого отдельно взятого гражданина страны, связанные с ней не только риски финансовых потерь, но и в первую очередь возможную опасность для жизни и здоровья. Именно последняя категория потенциальных жертв наиболее уязвима, и именно по ней наносят основной удар кибермошенники.

Результаты исследования

Наиболее прогрессирующим видом киберпреступлений (более 90 % от общего количества) в настоящее время является телефонное мошенничество. Это наиболее распространенный способ хищения денежных средств у граждан. Другая тревожная тенденция – рост утечек персональных данных. По информации Роскомнадзора, в 2022 году в России произошло 150 крупных уте-

[1] Ущерб от IT-преступлений в России превысил 116 миллиардов рублей // РИА Новости. URL: https://ria.ru/20240925/it-1974584213.html (дата обращения: 14.03.2025).

[2] Ущерб от киберпреступлений в 2024 году составил порядка 200 млрд рублей // Коммерсантъ. URL: https://www.kommersant.ru/doc/7552645 (дата обращения: 14.03.2025).

[3] Там же.

чек, в 2023 году – 168. В итоге в открытый доступ попало более 510 миллионов записей о гражданах России. Это мощное оружие в руках преступников. По чужим персональным данным оформляются кредиты, осуществляется рассылка жертвам телефонных мошенничеств поддельных квитанций на оплату услуг ЖКХ, штрафов от госорганов и т. п.

По оценкам Сбербанка, в открытом доступе находятся персональные данные уже около 90 % взрослого населения страны[1]. В 2024 году службой безопасности Сбербанка зафиксировано рекордное количество звонков от мошенников. В пиковые моменты их число доходило до 20 миллионов в сутки. Общий ущерб отечественной экономике от таких действий преступников по итогам 2024 года оценивается в один триллион рублей.

С каждым днем действия киберпреступников становятся все более изощренными, злоумышленники активно используют методы социальной инженерии (мошеннические действия совершаются от имени сотрудников правоохранительных органов или банков, с помощью фиктивных аккаунтов в социальных сетях либо фиктивных мобильных приложений финансовых организаций, в телефонных разговорах осуществляются манипуляции персональными данными жертвы). Так, осенью 2024 года в Республике Башкортостан было зафиксировано резкое увеличение количества звонков от мошенников, представляющихся сотрудниками энергосбытовой компании. С помощью настойчивых предложений об оформлении заявок на замену электросчетчиков преступники пытались получить доступ к аккаунтам граждан на портале «Госуслуги». Аналогичных примеров немало и в других регионах.

Одна из наиболее уязвимых перед киберпреступниками категорий граждан – это пенсионеры. По данным, озвученным на заседании коллегии МВД России Президентом России В. В. Путиным, доля пожилых граждан в общем числе пострадавших составляет не менее 25 %[2]. Представители старшего поколения в силу своей доверчивости, невысокого уровня цифровой и правовой грамотности, как правило, наиболее легко поддаются психологическому и технологическому воздействию мошенников. При этом суммы финансовых потерь зачастую оказываются достаточно крупными. Так, в Архангельской области пенсионерка потеряла 3,5 миллиона рублей, просто ответив мошенникам по телефону, а 72-летний житель Омска перевел мошенникам 8 миллионов рублей.

Успешные удары киберпреступники наносят не только по пенсионерам. Современные технологии позволяют воспроизводить документы и подписи, голос и видео любого человека. В итоге можно наблюдать, как жертвами мошенников регулярно становятся звезды эстрады, депутаты разного уровня, руководители государственных органов и другие категории граждан, которые на первый взгляд в силу своей правовой и технологической грамотности не должны попадаться на подобные провокации.

В последние годы одна из наиболее часто попадающих под удары киберпреступников категорий граждан – это участники СВО и их родственники. Выбор преступниками соответствующих жертв обусловлен, во-первых, существенными в случае удавшегося мошенничества перспективами финансового обогащения с учетом высокой социальной защищенности данных категорий граждан, в том числе достаточно крупных выплат им в ряде случаев, во-вторых, идейными соображениями нанести болезненный удар в наиболее уязвимое место, попытавшись тем самым дестабилизировать общественно-политическую ситуацию в стране. Манипуляции в отношении родственников

[1] Сбербанк: в открытый доступ попали персональные данные 90 % россиян // Коммерсантъ. URL: https://www.kommersant.ru/doc/7283274 (дата обращения: 14.03.2025).

[2] Ущерб от киберпреступлений в 2024 году составил порядка 200 млрд рублей // Коммерсантъ. URL: https://www.kommersant.ru/doc/7552645 (дата обращения: 14.03.2025).

участников СВО осуществляются, как правило, с помощью телефонных звонков либо через мессенджеры – мошенники от имени руководства воинской части или госпиталя сообщают, что военнослужащий ранен и срочно нужны деньги на лечение. Либо информируют о гибели и необходимости перевода денег для транспортировки тела на родину. Третий распространенный вариант – сообщение о том, что военнослужащий попал в плен, и требование выкупа. Преступных схем много, они постоянно совершенствуются.

С учетом того, что большинство киберпреступников находятся на территории недружественных государств и фактически не просто осуществляют мошеннические действия, а ведут полномасштабную кибервойну против России в целом, и их цель не только похитить денежные средства россиян, но и посеять панику, нанести ущерб здоровью и жизням людей, следующим видом киберпреступлений, уже не таким «безобидным», как простой отъем денег у населения, является вовлечение граждан в противоправную деятельность. Чаще всего при этом используются шантаж и запугивание, в том числе угроза расправы над родственниками жертвы. Зачастую мошенники представляются сотрудниками правоохранительных органов, спецслужб и отдают поручения от их имени. Популярен также метод, когда злоумышленники сперва обманными действиями заставляют жертву перевести им крупную сумму денег, нередко взятую в кредит, а потом, когда человек понимает, что перечислил деньги мошенникам, оказывают на него психологическое давление с требованиями выполнить определенные «поручения» за возврат денежных средств. В итоге человек поджигает здание банка, военкомата или льет зеленку в избирательную урну, закладывает взрывное устройство, совершает иные противоправные деяния. При этом речь, как правило, об изначально законопослушных гражданах, которые в одних случаях сознательно идут на преступление под воздействием страха, а в других случаях даже не осознают, что делают. Например, в сентябре 2024 года 77-летнего жителя Санкт-Петербурга мошенники убедили поджечь военкомат с помощью коктейля Молотова. При этом дистанционно управляемый мошенниками по телефону пенсионер искренне считал, что помогает своими действиями правоохранительным органам в борьбе с терроризмом[1]. Другой подобный случай также произошел в Санкт-Петербурге: в январе 2025 года 76-летнюю пенсионерку приговорили к 10 годам лишения свободы за поджог автомобиля у здания военкомата, совершенный под психологическим воздействием кибермошенников в 2023 году[2]. И третий яркий пример из Санкт-Петербурга – мошенники вынудили 46-летнюю женщину оформить кредит на 1,7 миллиона рублей и перевести им всю эту сумму, после чего спровоцировали ее поджечь несколько автомобилей в разных районах города, обещая вернуть за это деньги[3]. Аналогичным образом в Москве женщина, чтобы вернуть похищенные у нее мошенниками из Украины деньги, подожгла по их заданию номер в отеле[4]. Еще один житель Москвы, попавший под влияние кибермошенников, осуществлял по их заданию видеосъемку позиций систем ПВО. Похожих примеров немало и в других регионах. При этом для лиц, ставших жертвами

[1] Мошенник, заставивший пожилого петербуржца поджечь военкомат, попал на видео // Газета.ru. URL: https://www.gazeta.ru/social/news/2024/09/30/24042769.shtml (дата обращения: 14.03.2025).

[2] В Петербурге пенсионерке дали 10 лет за поджог машины у военкомата // РБК. URL: https://www.rbc.ru/politics/29/01/2025/67997bcf9a7947a1f934d360 (дата обращения: 14.03.2025).

[3] В Петербурге мошенники заставили женщину поджечь пять автомобилей. RG.RU. URL: https://rg.ru/2024/08/26/reg-szfo/v-peterburge-moshenniki-zastavili-zhenshchinu-podzhech-piat-avtomobilej.html (дата обращения: 14.03.2025).

[4] SHOT: украинские мошенники заставили москвичку поджечь номер в отеле // Аргументы и факты. URL: https://aif.ru/incidents/shot-ukrainskie-moshenniki-zastavili-moskvichku-podzhech-nomer-v-otele (дата обращения: 14.03.2025).

киберпреступников, такие истории зачастую заканчиваются не только потерей денег, но и реальными сроками лишения свободы.

Особую тревогу вызывает тот факт, что в подобные правонарушения кибермошенники целенаправленно в большом количестве вовлекают несовершеннолетних. Наряду с пожилыми гражданами это одна из целевых групп при выборе преступниками жертвы, что вполне объяснимо, поскольку, если деньги проще всего выманить у доверчивого пенсионера, то на преступление легче всего толкнуть психологически незрелого подростка. Это максимально внушаемая и легко управляемая категория, к тому же это самая интернет-активная категория. Кроме того, у подростков неустойчивая психика, они зачастую не отдают полного отчета в последствиях своих действий. Таким образом, это идеальная жертва для киберпреступника, цель которого – совершение на территории России диверсий и других противоправных действий руками местного населения.

Вербовка несовершеннолетних осуществляется с помощью социальных сетей, телеграмм-каналов, а также в чатах онлайн-игр. Преступники втираются в доверие к подростку, сулят деньги за выполнение их поручений, а также «гарантируют» полную безнаказанность за соответствующие действия. Наряду с обещанием материального вознаграждения для склонения детей к совершению преступлений используются также манипуляции их психикой, эмоциями, в том числе угрозы расправы над близкими. Нередко подростки идут на противоправные действия и для поддержания своего авторитета среди сверстников.

Правонарушения, совершенные подростками под давлением кибермошенников, наносят значительный материальный ущерб, представляют большую угрозу для общественной безопасности, а также имеют крайне негативные последствия для судьбы самих малолетних правонарушителей. Так, в апреле 2024 года в Самаре задержали двух 16-летних подростков на территории военного аэродрома «Кряж» при попытке осуществить поджог вертолета Ми-8. До задержания этими же подростками под оказанным на них через Интернет давлением спецслужб Украины была совершена серия других терактов на территории Самарской области, в том числе поджог вышки мобильной связи, двух релейных шкафов на железнодорожных путях и поезда[1]. В сентябре 2024 года в городе Ноябрьске Ямало-Ненецкого автономного округа двое школьников в возрасте 13 и 14 лет, управляемые киберпреступниками, совершили поджог вышки мобильной связи и вертолета Ми-8. Имущество было полностью уничтожено, сумма ущерба составила более 300 миллионов рублей[2]. Аналогичный случай произошел и в Омске, где двое школьников в возрасте 16 лет осуществили успешный поджог вертолета Ми-8[3]. Как в Омске, так и в Ноябрьске при совершении поджогов пострадали сами малолетние правонарушители. При этом в обоих случаях подросткам грозит серьезная ответственность. В приведенных выше в качестве примера и в других аналогичных случаях управление действиями подростков овеществлялось киберпреступниками через мессенджеры с территории Украины. За противоправные действия несовершеннолетним были обещаны крупные суммы денег, которые они так и не получили.

Для вербовки детей и молодежи действующие с территории Украины киберпреступники наиболее активно используют такие инструменты коммуникации, как мессенджеры и сетевые компьютерные игры. Так, осенью 2024 года в результате опера-

[1] В Самаре задержали двух старшеклассников по делу о попытке поджога Ми-8. Коммерсантъ. URL: https://www.kommersant.ru/doc/6662061 (дата обращения: 14.03.2025).

[2] «Ими управляли извне». Губернатор Ямала прокомментировал поджог вертолета школьниками Газета.ru. URL: https://www.gazeta.ru/social/2024/09/12/19735429.shtml (дата обращения: 14.03.2025).

[3] Суд продлил арест подросткам из Омска, которые подожгли вертолет. РИА Новости. URL: https://ria.ru/20241122/arest--1985241272.html (дата обращения: 14.03.2025).

тивно-розыскных мероприятий Федеральной службы безопасности в регионах России были задержаны 39 молодых людей в возрасте от 14 до 35 лет, которые по заданию киберпреступников из Украины осуществляли изготовление взрывных устройств, готовили нападения на школы и религиозные учреждения, склоняли несовершеннолетних к совершению насильственных действий в отношении сверстников и представителей органов государственной власти[1]. При этом коммуникация с украинскими кураторами осуществлялась через кроссплатформенную проприетарную систему мгновенного обмена сообщениями Discord[2], ранее уже неоднократно использовавшуюся для распространения дискриминационного контента в разных странах. После указанной выше волны задержаний Discord был 8 октября 2024 года заблокирован на территории России и Турции. Данная система заблокирована также в Китае[3].

Сообщения о противоправных действиях детей и молодежи, совершенных в результате психологических манипуляций киберпреступников, поступают регулярно из разных регионов. Опасность данной ситуации заключается не только в том, что в результате таких деяний наносится ущерб жизням и здоровью граждан, объектам инфраструктуры, но и в том, что страна теряет молодое поколение, поскольку киберпреступники толкают его прямиком в тюрьму.

Как мы видим, спектр видов киберпреступности достаточно разнообразен, арсенал средств преступников широк и обновляется с каждым днем, урон от данной деструктивной деятельности весьма ощутим и разнопланов – от прямого экономического ущерба, угрозы жизням и здоровью граждан до дестабилизации социально-политической обстановки в обществе и проблем с воспитанием подрастающего поколения. Очевидно, что киберпреступность в разных ее проявлениях – это серьезная угроза национальной безопасности, целенаправленная подрывная деятельность, поэтому необходимы эффективные методы борьбы с ней.

С учетом широты проблемы ее решение требует серьезных законодательных разработок, а кроме того, консолидации усилий всего силового блока, банковского сектора, поставщиков услуг Интернета и сотовой связи. Важны также повышение правовой и финансовой грамотности населения, просветительская и воспитательная работа с молодежью, что автоматически требует вовлечения в этот процесс органов государственной власти всех уровней, органов МСУ, институтов гражданского общества.

Нельзя сказать, что борьба с обозначенным явлением не ведется. Если рассматривать, например, мошенничества, связанные с попытками хищения денежных средств россиян, то за последние несколько лет был принят целый блок законов, нацеленных на противодействие преступлениям в данной сфере. В качестве наиболее эффективного законодательного решения необходимо упомянуть вступивший в силу с 1 декабря 2021 года Федеральный закон от 1 июля 2021 г. № 250-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации», которым внесены поправки в федеральные законы «О банках и банковской деятельности», «О рынке ценных бумаг», «О Центральном банке Российской Федерации (Банке России)», «Об информации, информационных технологиях и о защите информации» и в ряд других законодательных актов. Принципиальной новацией данного федерального закона стало существенное расширение полномочий Банка России по противодействию финансовому

[1] ФСБ: задержаны 39 проукраинских радикалов, склонявших подростков к насилию // Коммерсантъ. URL: https://www.kommersant.ru/doc/7197560 (дата обращения: 14.03.2025).

[2] Discord – мессенджер, разработанный компанией Discord Inc. (ранее — Hammer & Chisel), 8 октября 2024 г. заблокирован Роскомнадзором из-за нарушений требования российского законодательства.

[3] Discord // Википедия. URL: https://ru.wikipedia.org/wiki/Discord (дата обращения: 14.03.2025).

мошенничеству в Интернете. Если раньше регулятор мог блокировать мошеннические сайты только через прокуратуру и суд, то после принятия закона он получил право ограничивать доступ к ресурсам, созданным с заведомо мошенническими целями (сайты финансовых пирамид, нелицензированных компаний либо маскирующих свои ресурсы под сайты лицензированных организаций и т. п.), в досудебном порядке[1]. Вступление в силу закона и его реализация на практике в течение более трех лет позволила существенно ограничить действия мошенников, защитить денежные средства большого количества россиян.

С 1 августа 2023 года вступил в силу Федеральный закон от 24 июля 2023 г. № 340-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации», закрепивший, наряду с прочими изменениями, обязанность банков проверять все денежные переводы физических лиц, приостанавливать подозрительные операции на двое суток, а также возмещать средства, переведенные без согласия клиентов на счета мошенников[2]. Дальнейшим развитием данной правовой новации стал Федеральный закон от 24 июля 2023 г. № 369-ФЗ «О внесении изменений в Федеральный закон «О национальной платежной системе», подписанный Президентом России одновременно с вышеуказанным законом и вступивший в силу спустя год – в июле 2024 года. В данном документе, наряду с обязанностью банков проверять все денежные переводы и блокировать те из них, которые имеют признаки мошенничества, прописан алгоритм осуществления такой проверки и приостановки сомнительных переводов, сам порядок отнесения переводов к имеющим признаки мошеннических, а также условия, схема и сроки возврата денежных средств банком обманутому мошенниками клиенту в зависимости от ситуации, выполнила ли финансовая организация установленные законом обязательства по блокировке подозрительного платежа или уклонилась от них, и был ли платеж осуществлен клиентом добровольно после уточняющего запроса банка[3].

Исполнение перечисленных правовых норм на практике существенно урезало возможности кибермошенничества в финансовой сфере, помогло спасти средства граждан на триллионы рублей. Так, по данным Центрального Банка Российской Федерации, в 2024 году банками было отражено более 72 миллионов попыток хищения денежных средств со счетов клиентов на сумму 13,5 триллиона рублей. Для сравнения в 2023 году отражено 34 миллиона атак, спасено 5,8 триллиона рублей[4]. Данная динамика свидетельствует как о более чем двукратном увеличении активности киберпреступников, так и о значительном повышении эффективности работы антифрод-систем кредитных организаций, а главное, о результативности принятых законов. При этом важно отметить, что, несмотря на значительный рост количества кибератак на счета граждан, общее число проведенных операций без добровольного согласия клиентов в 2024 году удалось сдержать примерно на уровне 2023 года (1,197 млн и 1,165 млн случаев соответственно), хотя общий объем таких операций в рублевом выражении и вырос (27,534 млрд в 2024 г. и 15,791 млрд рублей в 2023 г.). Из указанной суммы банки в итоге вернули кли-

[1] О внесении изменений в отдельные законодательные акты Российской Федерации: федеральный закон от 1 июля 2021 г. № 250-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

[2] О внесении изменений в отдельные законодательные акты Российской Федерации: федеральный закон от 24 июля 2023 г. № 340-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

[3] О внесении изменений в Федеральный закон «О национальной платежной системе»: федеральный закон от 24 июля 2023 г. № 369-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс»

[4] Обзор операций, совершенных без добровольного согласия клиентов финансовых организаций // Центральный банк Российской Федерации. URL: https://cbr.ru/analytics/ib/operations_survey/2024/ (дата обращения: 14.03.2025).

ентам в 2024 году 9,9 % (2,713 млрд рублей), в 2023 году – 8,7 % (1,378 млрд рублей). Кроме того, в рамках исполнения Федерального закона от 1 июля 2021 г. № 250-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» Банк России инициировал блокировку 46 тысяч мошеннических сайтов и аккаунтов в соцсетях, а также 172 тысячи используемых мошенниками телефонных номеров[1].

Очередным шагом на пути дальнейшего совершенствования законодательной базы в целях противодействия киберпреступности стало принятие Федерального закона от 26 февраля 2024 г. № 31-ФЗ «О внесении изменений в Федеральный закон «О кредитных историях» и Федеральный закон «О потребительском кредите (займе)», вступившего в силу с 1 марта 2025 года. Данным законом закреплено право граждан устанавливать так называемый самозапрет на получение кредитов путем направления заявки через МФЦ или портал «Госуслуги». Одновременно для кредитных организаций этим же законом закреплена обязанность проверять факт наличия такого самозапрета при оформлении кредитов[2]. А одной из ключевых новаций уже 2025 года в сфере укрепления правовых основ для борьбы с финансовым мошенничеством в Интернете стало принятие Федерального закона от 13 февраля 2025 г. № 9-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации», ключевые положения которого вступят в силу с 1 сентября 2025 года. Речь, в частности, о норме, которой вводится «период охлаждения» по кредитам и займам – деньги по ним в размере от 50 тысяч до 200 тысяч рублей можно будет получить не ранее чем через четыре часа после заключения договора кредитования, а более крупные суммы – не ранее чем через 48 часов. Этим же законом закреплена обязанность микрофинансовых организаций зачислять денежные средства по договору потребительского займа только при условии совпадения сведений о реквизитах заемщика денежных средств и их получателя[3]. Нормы данного закона значительно сужают перечень возможных лазеек, которые используются киберпреступниками для хищения средств.

Несмотря на все принимаемые усилия по совершенствованию правовых механизмов противодействия киберпреступности, проблема не сходит с повестки. Более того, ее масштаб ширится с каждым годом. По данным МВД России, за последние пять лет число киберпреступлений в стране выросло более чем вдвое[4] и сегодня составляет 40 % от общего числа преступлений[5]. Поэтому данный вопрос регулярно поднимается на уровне Государственной Думы, Правительства, федеральных ведомств, слышны и голоса регионов. Каждое из перечисленных нами выше законодательных решений, безусловно, важно, было принято своевременно и помогло предотвратить массу негативных процессов. Однако все они решают лишь одну из граней обозначенной проблемы, а этих граней много. В силу точечности работы в данном направлении и по объективным причинам определенной инертности зако-

[1] Обзор операций, совершенных без добровольного согласия клиентов финансовых организаций // Центральный банк Российской Федерации. URL: https://cbr.ru/analytics/ib/operations_survey/2024/ (дата обращения: 14.03.2025)..

[2] О внесении изменений в Федеральный закон «О кредитных историях» и Федеральный закон «О потребительском кредите (займе)»: федеральный закон от 26 февраля 2024 г. № 31-ФЗ. «Доступ из справ.-правовой системы «КонсультантПлюс».

[3] О внесении изменений в отдельные законодательные акты Российской Федерации: федеральный закон от 13 февраля 2025 г. № 9-ФЗ. URL: http://publication.pravo.gov.ru/document/0001202502130045 (дата обращения: 14.03.2025).

[4] За пять лет число киберпреступлений увеличилось более чем вдвое // RG.RU. URL: https://rg.ru/2024/09/25/policiia-v-seti.html (дата обращения: 14.03.2025).

[5] МВД назвало число преступлений, совершенных с использованием IT-технологий // РИА Новости. URL: https://ria.ru/20250120/mvd-1994678968.html (дата обращения: 14.03.2025).

нодательного процесса в целом реальная ситуация в сфере борьбы с киберпреступностью сегодня далека от желаемого результата. Следует признать, что методы работы преступников совершенствуются гораздо быстрее, чем правовые механизмы противодействия им. Очевидно, что данная область права никогда не угонится за киберпреступниками, если не произойдет смена тактики и не будут выработаны более широкие, кардинальные решения, позволяющие предусмотреть методы развития цифровых технологий и социальной инженерии на десятилетия вперед и предотвратить их безнаказанное использование злоумышленниками. С учетом масштаба проблемы необходимы разработка и принятие целого комплекса федеральных законов, которые обеспечили бы взвешенный, выверенный подход к всестороннему решению такого негативного явления, как киберпреступность.

Понимание необходимости подобных решений есть как у законодателей, так и у исполнительной власти, и ряд соответствующих мер уже даже был анонсирован в конце 2024 – начале 2025 гг. Так, в октябре 2024 года в рамках форума Finopolis 2024 в Сочи заместитель Председателя Правительства – Руководитель Аппарата Правительства Российской Федерации Д. Ю. Григоренко заявил о совместной разработке Правительством России и Центробанком проекта федерального закона, нацеленного на повышение уровня защиты финансовых операций, совершаемых с использованием биометрии[1]. Речь, по всей вероятности, идет о законодательном закреплении за банками обязательства использования системы двойной аутентификации, что позволит защитить средства клиентов даже в случае кражи кибермошенниками биометрических данных. По состоянию на март 2025 года данные о внесении соответствующего проекта закона на рассмотрение в нижнюю палату Федерального Собрания отсутствовали, но, очевидно, работа по его подготовке ведется. Можно предположить, что данный законопроект войдет одной из составных частей в комплекс масштабных поправок в законодательство для борьбы с киберпреступностью, анонсированных в феврале 2025 года Правительством России. Данные поправки позиционируются экспертами как самые значительные за последние годы меры реагирования со стороны государства на проблему киберпреступности. Предполагается, что соответствующий пакет документов, который рассматривает Комиссия Правительства Российской Федерации по законопроектной деятельности, затронет изменение нескольких десятков федеральных законов и иных нормативных актов. Подготовка данного пакета документов была подтверждена в том числе и Д. Ю. Григоренко[2]. По его словам, началу работы над предложениями по соответствующему комплексному изменению законодательства предшествовал детальный анализ наиболее распространенных мошеннических схем и методов работы преступников, включая взломы аккаунтов, кражу персональных данных, психологические манипуляции с помощью телефонных звонков и переписки в мессенджерах и другие способы совершения мошенничеств. На основе полученных данных были разработаны комплексные меры максимальной защиты граждан от потенциальных киберугроз.

В данный комплекс мер, предложенных к закреплению на законодательном уровне, войдут:

– обязательная маркировка международных звонков, а также звонков с виртуальных АТС;

– право блокировки спам-звонков и рассылок абонентами сотовых операторов;

– обязательство оператора мобильной связи присылать сообщения с кодом для

[1] Усложнить жизнь мошенникам: какие меры предлагают правительство и ЦБ для защиты биометрических данных // RG.RU. URL: https://rg.ru/2024/10/16/kak-sohraniat-lico.html (дата обращения: 14.03.2025).

[2] Власти готовят самые большие за последние годы поправки против кибермошенников // Газета.ru. URL: https://www.gazeta.ru/tech/2025/02/10/20525708.shtml (дата обращения: 14.03.2025).

идентификации в ЕСИА в случае соответствующего запроса абонента во время телефонного разговора только после завершения вызова;

– право госорганов, занимающихся оперативно-розыскной деятельностью, получать сведения из информационных систем операторов связи;

– запрет на ввоз, реализацию и использование на территории России абонентских терминалов иностранных спутниковых систем, чья работа запрещена или ограничена в России или ЕврАзЭС, возможность досудебной блокировки сайтов, распространяющих информацию о реализации таких устройств;

– обязательная биометрическая идентификация при оформлении выписок из бюро кредитных историй и дистанционного оформления микрозаймов;

– возможность граждан устанавливать через портал «Госуслуги» блокировку дистанционного заключения договора на оказание услуг сотовой связи;

– обязанность кредитных организаций, маркетплейсов, социальных сетей, агрегаторов обеспечить возможность добровольного использования биометрии при авторизации пользователей.

Внесение необходимых изменений в законодательство и внедрение указанных мер на практике планируются уже в 2025–2026 гг.[1] При этом Минцифры России рассчитывает в результате реализации комплекса этих и ряда других правовых мер «закрыть» проблему кибермошенничества в России уже в 2025 году. Такую позицию, в частности, озвучил в марте 2025 года в ходе выступления в Совете Федерации замглавы ведомства И. В. Лебедев[2].

На наш взгляд, предложенные Правительством России в феврале 2025 года меры законодательного реагирования, действительно, представляются комплексными и эффективными. Это как раз-таки та самая смена тактики, которая позволит федеральному законодателю догнать до сих пор постоянно оказывавшуюся на шаг впереди киберпреступность и эффективно противодействовать ей правовыми методами. Вместе с тем на данный момент видится преждевременным говорить о масштабном решении проблемы кибермошенничества и тем более о полном «закрытии» данного вопроса.

Предложенный комплекс законодательных решений в целом соответствует общемировым тенденциям совершенствования законодательства в сфере кибербезопасности и нацелен преимущественно на повышение безопасности финансовых операций, усиление идентификации пользователей, минимизацию возможного использования интернет-мошенниками зарубежных мессенджеров и подменных телефонных номеров, усложнение оформления кредитов по поддельным документам.

Вместе с тем при всей своей комплексности, обоснованности и предполагаемой эффективности реализации на практике данные меры не представляются исчерпывающими для полноценного противодействия киберпреступности. В частности, они направлены на противодействие уже известным схемам работы преступников, не учитывают их постоянное обновление, регулярное приспособление злоумышленников к действующим защитным механизмам и внедрение новых технологий для их обхода. На практике это может привести к тому, что уже на момент вступления предложенных законодательных норм в силу преступники адаптируются к новым реалиям и изобретут способы обхода новых, кажущихся в настоящий момент непреодолимыми систем защиты.

Следует также отметить, что предложенный комплекс мер сосредоточен преимущественно на противодействии использу-

[1] Правительство изменит десятки законов для борьбы с кибермошенниками. РБК. URL: https://www.rbc.ru/technology_and_media/10/02/2025/67a752bb9a7947c806896597 (дата обращения: 14.03.2025).

[2] Минцифры рассчитывает в этом году «закрыть» проблему кибермошенничеств. Коммерсантъ. URL: https://www.kommersant.ru/doc/7551641 (дата обращения: 14.03.2025).

емым мошенниками техническим средствам и мало учитывает широко применяемые киберпреступниками методы социальной инженерии, с помощью которых совершается значительное количество преступлений. На наш взгляд, предложенный комплекс законодательных мер необходимо дополнить нормами о противодействии именно методам психологических манипуляций, осуществляемых преступниками в отношении жертвы и усилением ответственности за подобные действия. Одновременно видится целесообразным и ужесточение ответственности за использование мошенниками отдельных видов технологий, например, так называемых дипфейков. В 2024 году частота использования киберпреступниками дипфейков выросла на 13 % и достигла 5 тысяч случаев. Тенденция тревожная, и на ее фоне предложение рассматривать дипфейки как отягчающее обстоятельство при совершении киберпреступлений уже озвучивалось со стороны Минцифры России[1].

Что касается технической стороны вопроса, то актуальным видится введение на законодательном уровне полного контроля со стороны государства за чатами онлайн-игр, в том числе оперативная блокировка таких ресурсов, поскольку именно с помощью данного сегмента цифровых коммуникаций, а не традиционных мессенджеров, киберпреступники, как правило, осуществляют вербовку молодежи, толкают ее на противоправные действия. Выше мы упоминали осуществленную на территории России осенью 2024 года блокировку Discord – одного из наиболее популярных инструментов в геймерском сообществе. Однако это точечное решение, не решающее проблему во всей ее полноте – геймеры, а следом за ними и кибермошенники уже адаптировались к ситуации блокировки Discord и нашли альтернативы данному ресурсу. Соответственно, вопрос необходимо решать комплексно в отношении всех подобных платформ. Возможность их анонимного использования и применения для склонения детей и молодежи к противоправным действия должна быть полностью исключена.

Необходимо также принять во внимание тот факт, что раскрытие значительной части кибермошенничеств усложняется организованностью данного вида преступности. Кибермошенничеством сегодня занимаются не единичные преступники, а крупные колл-центры, в которых задействованы тысячи людей. Большинство таких центров расположены, как правило, за пределами страны, на территории недружественных государств. Соответственно, возможности борьбы с подобного рода трансграничной организованной преступностью, особенно в современных геополитических реалиях, у правоохранительных органов ограничены.

Выработка решений обозначенной проблемы ведется руководством страны на самом высоком уровне. Вопрос попал в том числе в поле зрения Президента России В. В. Путина. В опубликованном в феврале 2025 года Перечне поручений по итогам заседания Совета по развитию гражданского общества и правам человека поставлена задача Правительству Российской Федерации совместно с ФСБ России и МВД России о выработке дополнительных мер по блокировке телефонных вызовов, осуществляемых с территорий Украины и других недружественных иностранных государств в преступных целях. Срок исполнения поручения обозначен 1 июля 2025 года[2].

Ранее, в декабре 2024 года Президент В. В. Путин также обращал внимание на тот факт, что интернет-мошенничество по выманиванию денег у россиян на территории Украины возведено в ранг государственной

[1] Гонка голосовых вооружений // Коммерсантъ. URL: https://www.kommersant.ru/doc/7516456 (дата обращения: 14.03.2025).

[2] Перечень поручений по итогам заседания Совета по развитию гражданского общества и правам человека // Официальный сайт Президента России. URL: http://kremlin.ru/acts/assignments/orders/76233 (дата обращения: 14.03.2025).

политики и осуществляется при полномасштабной поддержке украинских спецслужб созданными специально для этих целей крупными центрами[1].

В такой ситуации, когда действия преступников, осуществляемые профессиональными хакерскими группировками и колл-центрами, инициируются и контролируются неонацистским киевским режимом при финансовой и технологической поддержке других недружественных государств, уместно говорить уже не столько даже о киберпреступности, сколько о полномасштабной кибервойне, ведущейся против Российской Федерации и ее граждан. А это означает, что и меры правового реагирования на ситуацию должны быть соответствующими. При этом следует принимать во внимание, что само понятие «кибермошенничество» в целом как явление, если не под этим, то под иными терминами, относительно четко описано в российском и международном праве, на законодательном уровне регламентированы меры противодействия данному явлению, а также нормы ответственности за соответствующие деяния преступников (например, в статьях 159.6, 187, 272, 272.1, 273, 274, 274.1, 274.2 Уголовного кодекса Российской Федерации и ряде других)[2]. В то же время понятие «кибервойна» в правовом отношении до сих пор остается достаточно зыбким. Более того, четкого определения как в научной литературе, так и в законодательстве не нашел даже термин «информационная война», одной из частных разновидностей которой, несомненно, является кибервойна [1]. В результате возникает правовая коллизия, более того, парадокс, когда такое явление, как кибервойна, существует, на уровне органов государственной власти и в обществе в целом имеется адекватное понимание того, что собой представляет данное явление, кибервойны активно ведутся в современном мире как государствами, так и частными структурами, в том числе против нашей страны, компетентными ведомствами принимаются меры по противодействию данному явлению, однако в законодательстве отсутствуют четкое определение данного явления и нормы ответственности за ведение кибервойны против Российской Федерации и ее граждан.

Целесообразным видится первоначально устранить этот пробел в правовом поле, дать в законодательстве прозрачное определение кибервойне, разграничив понятия «кибервойна» и «киберпреступность», охарактеризовав признаки тех противоправных действий, которые позволяют отнести их к кибервойне, и определив меры реагирования государства на такие действия. Очевидно, что ответственность за ведение кибервойны должна при этом быть выше, чем за обычное кибермошенничество. Если меры ответственности за киберпреступления, прописанные преимущественно в главе 28, а также в статьях 159.6 и 187 Уголовного кодекса Российской Федерации, предусматривают наказание в виде штрафов и относительно незначительных сроков лишения свободы, то деяния лиц, ведущих кибервойну, в случае закрепления такого понятия в законодательстве, станет возможным уже расценивать как действия военных преступников со всеми вытекающими из этого последствиями. Кроме того, места расположения на территориях, контролируемых неонацистским киевским режимом, баз хакерских группировок и колл-центров, осуществляющих против Российской Федерации и ее граждан действия с признаками кибервойны, станут в таком случае законными целями Вооруженных Сил Российской Федерации с вытекающим из этого нанесением по ним ударов доступными средствами поражения, как по любым другим украинским воинским формированиям. Де-факто кибервойска в современных реа-

[1] Мошенничество против россиян контролируют спецслужбы Украины, заявил Путин // РИА Новости. URL: https://ria.ru/20241219/putin-1990154728.html (дата обращения: 14.03.2025).

[2] Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

лиях – такой же род войск, как и любой другой, угроза национальной безопасности от кибервойск противника, как и наносимый ими урон колоссальны, соответственно, и подавление таких подразделений Вооруженными Силами Российской Федерации должно осуществляться аналогично тому, как это происходит в отношении военной техники, личного состава противника, эшелонов с вооружениями, пунктов дислокации наемников.

Заключение

С учетом возрастающей с каждым днем актуальности совершенствования законодательства в области противодействия киберугрозам разного характера, а также с учетом проникновения цифровых технологий практически во все сферы современного общественного устройства и необходимости в связи с этим постоянно расширять правовые нормы, регулирующие использование интернет-коммуникаций, нейросетей и IT-ресурсов в целом, в перспективе видится уместной более полная систематизация и кодификация соответствующего раздела права. Речь может идти о создании в обозримом будущем условного Цифрового (либо Информационного) кодекса Российской Федерации. Нормы, прописывающие меры противодействия киберугрозам в таком случае войдут в него одной из составных частей. Дальнейшее развитие системы права в Российской Федерации в любом случае рано или поздно неизбежно приведет к появлению такого кодекса. В России законодательство, регулирующее правоотношения в сфере цифровых технологий, существует с начала 1990-х годов. За более чем три десятилетия накопилась масса нормативных актов в данной сфере, большинство из которых менялись многократно. Только в Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ изменения вносились более 70 раз[1]. Экспертами в сфере IT и законодателями вопрос о создании цифрового кодекса поднимался уже неоднократно. Еще в 2014 году Институтом государства и права РАН была разработана и опубликована концепция Информационного кодекса Российской Федерации, большинство положений которой являются актуальными и сегодня [2].

В пользу необходимости кодификации цифрового законодательства свидетельствуют и общемировые тенденции развития права. Перспективы создания своих цифровых кодексов рассматриваются не только в России, но и в Индии, Узбекистане, Кыргызстане, Казахстане, Азербайджане, Молдове и ряде других государств. Межпарламентская Ассамблея государств – участников СНГ еще в 2008 году приняла модельный Информационный кодекс для государств – участников СНГ[2]. Впоследствии его редакция обновлялась в 2012 и 2022 годах[3]. К созданию цифровых кодексов сегодня стремятся даже те государства, для которых традиции кодификации законодательства в целом не характерны.

В сложившихся условиях появление цифрового кодекса в России, на наш взгляд, представляется лишь вопросом времени. В 2021 году на необходимость создания такого кодекса указывал Совет при Президенте Российской Федерации по развитию гражданского общества и правам человека[4]. А в 2023 году о необходимости разработки

[1] Об информации, информационных технологиях и о защите информации : федеральный закон от 27 июля 2006 г. № 149-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

[2] Модельный Информационный кодекс для государств – участников СНГ (ред. 2008 г.). // Электронный фонд нормативно-технической и нормативно-правовой информации Консорциума «Кодекс». URL: https://docs.cntd.ru/document/902124603 (дата обращения: 14.03.2025).

[3] Модельный Информационный кодекс для государств – участников СНГ (ред. 2022 г.). Доступ из справ.-правовой системы «КонсультантПлюс».

[4] Свести законы воедино: что такое Цифровой кодекс и для чего он нужен в России // Forbes. URL: https://www.forbes.ru/tekhnologii/499753-svesti-zakony-voedino-cto-takoe-cifrovoj-kodeks-i-dla-cego-on-nuzen-v-rossii (дата обращения: 14.03.2025).

Инфокодекса в очередной раз заявило Минцифры России[1].

Цифровой кодекс Российской Федерации, если (а точнее, когда) он будет принят, вместит в себя всю систему гарантий по защите прав граждан в современном цифровом мире, права и обязанности органов государственной власти, организаций по использованию цифровых технологий, весь комплекс мер по обеспечению сетевой безопасности, противодействию киберугрозам любого характера. Это позволит полноценно, комплексно решить все связанные с цифровой сферой вопросы социально-экономического развития общества и национальной безопасности.

СПИСОК ИСТОЧНИКОВ

1. Третьякова Е. С., Михайлова Е. М., Ширинкина А. А. Понятие и правовой статус информационной войны // Международное сотрудничество евразийских государств: политика, экономика, право. 2023. № 4. С. 40–44.

2. Концепция Информационного кодекса Российской Федерации / под ред. И. Л. Бачило. М.: ИГП РАН – Изд-во «Канон+» РООИ «Реабилитация», 2014. 192 с.

REFERENCES

1. Tretyakova E. S., Mikhailova E. M., Shirinkina A. A. The concept and legal status of information warfare // International cooperation of the Eurasian states: politics, economics, law. 2023. No. 4. P. 40–44. (In Russ.).

2. The concept of the Information Code of the Russian Federation / edited by I. L. Bachilo. M.: IGP RAS – Publishing house «Canon+» ROOI «Rehabilitation», 2014. 192 p. (In Russ.).

Сведения об авторе:

К. Б. Толкачев, доктор юридических наук, профессор, заслуженный юрист Российской Федерации.

Information about the author:

K. B. Tolkachev, Doctor of Law, Professor, Honored Lawyer of the Russian Federation.

Статья поступила в редакцию 29.06.2025; одобрена после рецензирования 30.06.2025; принята к публикации 26.09.2025.

The article was submitted 29.06.2025; approved after reviewing 30.06.2025; accepted for publication 26.09.2025.

[1] Минцифры предлагает вернуться к разработке кодекса для телекома // Forbes.. URL: https://www.forbes.ru/tekhnologii/490165-mincifry-predlagaet-vernut-sa-k-razrabotke-kodeksa-dla-telekoma (дата обращения: 14.03.2025).