Научная статья
УДК 343.3/.7
DOI: 10.47475/2311-696X-2024-42-3-75-79

С. 75–79

СОВЕРШЕНСТВОВАНИЕ ПРАВОВЫХ СРЕДСТВ ПРОТИВОДЕЙСТВИЯ УГРОЗАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Аркадий Борисович Гриненко
Генеральная прокуратура Российской Федерации, Москва, Россия
a.b.grinenko@mail.ru
https://orcid.org/0009-0007-5733-9063

Аннотация. Развитие и глубокое проникновение в повседневную жизнь человека информационно-телекоммуникационных технологий и продуктов не только является фактором ускорения экономического развития государства и формирования информационного общества, но и создает условия повышенного уголовного интереса к их использованию. Анализ данных о преступности и правоприменительная практика подтверждают вывод о негативных тенденциях, свидетельствующих о масштабировании криминального использования телекоммуникаций, особенно при совершении преступлений против собственности. Отмечается специализация противоправной деятельности, преследующей цель ухода от ответственности за содеянное. Констатируется активное использование в преступной деятельности метода «социальной инженерии», для которого весьма важны персональные данные. Выделяются повышающие общественную опасность незаконного использования средств коммуникации признаки, в том числе, анонимность и трансграничность.

С учетом выявленных криминологических условий приводятся данные о некоторых реализуемых законодательных инициативах и имеющих целесообразность с точки зрения потребности правового регулирования предложениях по совершенствованию правовых средств противодействия угрозам информационной безопасности Российской Федерации.

Ключевые слова: информационная безопасность, информационно-телекоммуникационные технологии, незаконный оборот персональных данных, метод «социальной инженерии», фишинг

Для цитирования: Гриненко А. Б. Совершенствование правовых средств противодействия угрозам информационной безопасности Российской Федерации // Правопорядок: история, теория, практика. 2024. № 3 (42). С. 75–79. DOI: 10.47475/2311-696X-2024-42-3-75-79

Reseach article

IMPROVEMENT OF LEGAL REMEDIES OF COUNTERING THREATS TO INFORMATION SECURITY OF THE RUSSIAN FEDERATION

Arkadiy B. Grinenko
Prosecutor General's Office of the Russian Federation, Moscow, Russia
a.b.grinenko@mail.ru
https://orcid.org/0009-0007-5733-9063

Abstract. The development and deep penetration of information and communication technologies and products into our daily lives not only accelerates the economic development of the state and the establishment of information society, but also creates conditions for increased criminal interest in the use thereof. Analysis of crime data and law enforcement practice confirm the supposed negative trends showing magnification of criminal use of telecommunications, especially when committing crimes against property. Notable is the spread of illegal activities that pursue the goal of evading responsibility for crimes committed. The thesis draws attention to the active use in criminal activities of "social engineering" techniques, that are largely dependent on the personal data. Identified in the paper as well are the features that serve to increase the public danger of illegal use of communication means, such as anonymity and cross-border elements, among others.

Given the identified criminological conditions, data is provided on some ongoing legislative initiatives and proposals, feasible from the point of view of the need for legal regulation aimed at improving the legal means of countering threats to the information security of the Russian Federation.

Keywords: information security, information and communication technologies, illegal circulation of personal data, "social engineering" techniques, phishing

For citation: Grinenko AB. Improvement of legal remedies of countering threats to information security of the Russian Federation.*Pravoporyadok: istoriya, teoriya, praktika* [Legal and Order: History, Theory, Practice]. 2024;(3):75-79. (In Russ.) DOI: 10.47475/2311-696X-2024-42-3-75-79

Введение

В пункте 25 Указа Президента Российской Федерации от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации»[1] определены национальные интересы Российской Федерации на современном этапе. Ими в числе иных названы защита граждан и всех форм собственности от противоправных посягательств.

В соответствии со Стратегией обеспечение национальных интересов Российской Федерации осуществляется за счет концентрации усилий и ресурсов органов публичной власти, организаций и институтов гражданского общества на реализации стратегических национальных приоритетов, к которым отнесена информационная безопасность (п. 26 указа).

В комплексе решаемых при реализации государственной политики по обеспечению информационной безопасности задач главой государства выделена необходимость создания условий для эффективного предупреждения, выявления и пресечения преступлений и иных правонарушений, совершаемых с использованием информационно-коммуникационных технологий, и обеспечение защиты конституционных прав и свобод человека и гражданина при обработке персональных данных, в том числе с использованием информационных технологий (п. 57 указа).

Основой для формирования государственной политики и развития общественных отношений в области обеспечения информационной безопасности, а также для выработки мер по совершенствованию системы обеспечения информационной безопасности является Доктрина информационной безопасности Российской Федерации, утвержденная Указом Президента Российской Федерации от 05.12.2016 № 646[2].

Названные документы стратегического планирования определяют не только сферу национальных интересов, цели и направления обеспечения безопасности, но формулируют перечень угроз, на противодействии которым требуется концентрировать усилия в рамках реализации государственной политики.

Отмечая разноплановость угроз информационной безопасности, в рамках настоящей статьи полагаем целесообразным обратиться к анализу некоторых аспектов состояния противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий, а также реализуемым и предлагаемым мерам правового характера в целях снижения остроты проблематики.

Материал и методы

При подготовке публикации использованы сведения государственной статистики о состоянии преступности в Российской Федерации и статистические данные о результатах рассмотрения судами дел об административных правонарушениях Судебного департамента при Верховном Суде Российской Федерации, результаты анализа практики расследования фактов совершения с использованием информационно-телекоммуникационных преступлений, данные системы обеспечения законодательной деятельности Государственной Думы, а также нормативные правовые источники. Основу настоящего исследования составили диалектический метод познания социальных явлений, общенаучные и частнонаучные методы познания.

Описание исследования

Как показало время, включение в документы стратегического планирования в качестве одной из угроз национальной безопасности Российской Федерации указанной выше категории преступлений, а также прогнозирование их роста, были вполне обоснованными. Более того, такая угроза национальным интересам в информационной сфере в настоящее время является доминирующей.

Проанализированные в рамках исследования с 2018 года, т. е. с момента, когда начат углубленный статистический учет фактов криминального использования информационно-телекоммуникационных технологий, показатели государственной статистики о состоянии преступности в Российской Федерации не только подтверждают негативные тенденции, но позволяют выявить направленность криминальных устремлений, распространенность способов совершения преступлений [1; 2].

Так, в 2023 году зарегистрировано 1947,2 тыс. преступлений, из числа которых почти 677 тысяч совершены с использованием информационно-телекоммуникационных технологий (+29,7 % к 2022 году). Примечательно, что шесть лет назад (в 2018 году) таких деяний было установлено немногим менее 175 тысяч, или почти в четыре раза меньше.

В структуре совершенных с использованием информационно-телекоммуникационных технологий криминальных деяний более 70 % — преступления против собственности (свыше 370 тысяч в абсолютных цифрах). Доля этих преступлений стабильно высокая.

Анализ структуры информационно-телекоммуникационной преступности указывает на увеличение за последние шесть лет преступлений в сфере компьютерной информации (в четырнадцать раз — с 2,5 тыс. до 37,1 тысяч).

За тот же период отмечается четырехкратный рост в регистрации наркосбытов (с 18,8 тыс. до 81,5 тыс.), мошенничеств — в 3,8 раза (с 91,6 до 353,2 тыс.),

[1] Собрание законодательства Российской Федерации. 2021. № 27 (часть II). Ст.5351.

[2] Собрание законодательства Российской Федерации. 2016. № 50. Ст.7074.

а краж — в 3,6 раза (с 32,6 до 119,2 тыс.). Существенно возросло число вымогательств с использованием информационно-телекоммуникационных технологий — с 1621 до 6495[1].

Статистический учет также свидетельствует, что наиболее активно при совершении преступлений с использованием информационно-коммуникационных технологий применяется сеть Интернет и средства мобильной связи.

При определении потребности совершенствования правовых средств противодействия им, представляется небезынтересной характеристика общественно опасных способов применения сети Интернет и средств мобильной связи применительно к таким деяниям, которые направлены на завладение собственностью граждан.

Эксплуатация средств телекоммуникаций в самом широком смысле слова кроет в себе значительные риски обращения потенциала технологий против пользователя. Совершенных мер защиты не бывает, особенно если это связано с человеческим фактором. Именно этот фактор употребляется для достижения преступного результата.

Аппаратные и программные системы защиты основаны на использовании конфиденциальных, или, как их еще называют, «чувствительных» данных: логины, пароли, идентификаторы, простая электронная подпись (имея в виду пароль из SMS) и т. п. Утрата конфиденциальных данных становится возможной как в результате небрежного отношения к сохранности втайне от третьих лиц такого рода данных, так и злонамеренных действий. В силу взаимосвязи между успешным прохождением защитных процедур и возможностью совершения пользователем телекоммуникаций тех или иных юридически значимых действий, особенно в отношении электронных денежных средств, такие чувствительные данные становятся криминальной целью.

В числе наиболее распространенных способов незаконного получения конфиденциальных данных — методы «социальной инженерии» [3; 4]. Не вдаваясь в описание конкретных моделей этого метода, отметим, что их криминальная «эффективность» зависит в том числе от получения максимального объема персональных данных (о личности, местоположении, номерах телефона, отдельных банковских сведений и т. п.), совокупность которых в значительной мере облегчает совершение соответствующих преступлений, оказывая нужное злоумышленнику психологическое воздействие на волю жертвы.

Наряду с этим наблюдаются устойчивые признаки уголовной специализации, когда похищение информационных баз, в том числе персональных данных, их обработка, создание и обслуживание фишинговых ресурсов, дроповодство и последующая легализация преступных доходов осуществляется на возмездной основе разными субъектами, зачастую, не имеющими единого умысла на совершение конкретного, например корыстного, преступления. При этом такого рода услуги пользуются спросом в криминальной сфере, что обуславливает утечки персональных данных, увеличение фишинговых сайтов, рост числа эмитированных одному физическому лицу кредитных карт, с помощью которых выводятся похищенные электронные денежные средства.

В то же время правовая оценка с точки зрения уголовного закона перечисленных «подготовительных» действий на практике вызывает затруднения как при определении направленности умысла лиц, осуществляющих их, так и квалификации совершаемого субъектом деяния в соответствии с конкретной формой информационно-телекоммуникационного преступления. Самостоятельная стоимостная оценка рассматриваемых «криминальных услуг», как правило, снижает заинтересованность участия соответствующего лица в конкретном преступлении.

В этой связи представляется резонным разрешение вопроса о необходимости криминализации незаконного оборота персональных данных, коль скоро они (эти данные) способствуют реализации устоявшихся форм преступного использования средств коммуникации. Отправной точкой в этом направлении является выявление криминологических условий.

Так, по данным открытых источников, в 2023 году Роскомнадзор зарегистрировал 168 утечек персональных данных, в свободный доступ попало больше 300 млн записей о физических лицах. В 2022 году «утекли» более 1130 млн записей, а за 2021 год — более 100 млн записей[2]. Незаконно полученные персональные данные так или иначе становятся предметом торговли, преимущественно через даркнет. Примечательно, что по оценкам IT-специалистов, в несанкционированном доступе имеются персональные данные о 80 % населения России.

Как уже отмечалось, возможность незаконной обработки персональных данных несет вполне конкретную угрозу охраняемым общественным отношениям. Это выражается, прежде всего, в том, что в силу анонимности «оператор» не несет никакой ответственности за свои действия, которые к тому же им монетизируются.

Другим немаловажным аспектом общественной опасности незаконного оборота персональных данных является трансграничность, которая, с одной стороны, позволяет совершать неправомерные действия не из юрисдикции Российской Федерации, а с другой — весьма осложняет работу компетентным органам по ее пресечению.

Незаконный оборот персональных данных (если такие действия не посягают на охраняемую законом тайну) преследуется в соответствии с законодательством об административных правонарушениях (ст. 13.11 Кодекса

[1] Краткая характеристика состояния преступности в Российской Федерации за январь — декабрь 2023 года // Министерство внутренних дел Российской Федерации : [сайт]. URL: https://мвд.рф/reports/item/47055751/ (дата обращения: 21.02.2024).

[2] В 2023 году в сеть утекло более 300 млн записей о россиянах // ТАСС. URL: https://tass.ru/obschestvo/19693845 (дата обращения: 21.02.2024).

Российской Федерации об административных правонарушениях (далее — КоАП РФ)). В то же время влияние результатов административной практики на состояние и профилактику преступности в рассматриваемой сфере малозаметно.

Как следует из статистики Судебного департамента при Верховном Суде Российской Федерации, количество привлеченных за совершение правонарушений, предусмотренных вышеуказанной, а также статьями 13.11.1 (Распространение информации о свободных рабочих местах или вакантных должностях, содержащей ограничения дискриминационного характера), 13.12 чч. 2, 4 (Нарушение правил защиты информации), 13.14 (Разглашение информации с ограниченным доступом) КоАП РФ, снижается (с 1736 в 2018 году до 431 в 2022 году) при возрастании сумм административного штрафа с 6,8 млн рублей в 2018 году до 59,4 млн рублей в 2022 году[1].

Установленные действующим Уголовным кодексом Российской Федерации (далее — УК РФ) меры ответственности не выделяют персональные данные в качестве предмета преступления. В зависимости от объекта преступного посягательства и формы запрещенных уголовным законом действий, персональные данные попадают под уголовно-правовую защиту, предусмотренную ст. 137 (Нарушение неприкосновенности частной жизни) и ст. 272 (Неправомерный доступ к компьютерной информации) УК РФ.

Однако если принять во внимание, что не все категории персональных данных могут быть отнесены к личной и семейной тайне, а обработка уже находящихся в несанкционированном доступе персональных данных вопреки требованиям Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» не всегда связана с неправомерным доступом к компьютерной информации, вполне обоснованным представляется вывод о возможности воздействия на рассматриваемый вид поведения уголовно-правовыми средствами[2].

При этом масштабы такой противоправной деятельности, системная связь с преступлениями, совершаемыми с использованием информационно-телекоммуникационных технологий, анонимность и трансграничность наряду с низким уровнем профилактического воздействия соответствующих мер административной ответственности и объективной затруднительностью удаления соответствующих сведений из сетевого доступа, указывают на общественную опасность рассмотренных выше действий, связанных с незаконным оборотом персональных данных.

Одним из вариантов снижения остроты выявленных негативных факторов является выработка правового механизма противодействия утечкам баз персональных данных и последующей противоправной их обработке. Отчасти на это направлен подготовленный и принятый в первом чтении проект федерального закона № 502113-8 «О внесении изменений в Уголовный кодекс Российской Федерации».

Субъектами права законодательной инициативы предлагается признать преступлением незаконное использование и (или) передачу, сбор и (или) хранение компьютерной информации, содержащей персональные данные, а равно создание и (или) обеспечение функционирования информационных ресурсов, предназначенных для ее незаконного хранения и (или) распространения (проект ст. 272.1 УК РФ)[3].

И хотя концептуальная направленность предлагаемых законодательных изменений в целом не вызывает возражений, примененный подход к определению некоторых признаков преступления, на наш взгляд, нуждается в осмыслении с точки зрения в том числе законодательства о персональных данных.

В частности, проектируемые в части первой новеллы определение предмета преступного посягательства в виде «компьютерной информации, содержащей персональные данные», а также признак, указывающий на неправомерный доступ к средствам ее обработки, хранения или иного вмешательства в их функционирование, либо иным незаконным путем, представляются казуистичными и сужают сферу применения предлагаемой ответственности.

Часть шестая проектируемой статьи 272.1 УК РФ направлена на установление ответственности за создание и (или) обеспечение функционирования информационных ресурсов (сайта в сети Интернет и (или) страницы сайта в сети Интернет, информационной системы, программы для электронных вычислительных машин), заведомо предназначенных для незаконного хранения, передачи (распространения, предоставления, доступа) компьютерной информации, содержащей персональные данные.

В то же время в отсутствие в диспозиции этой нормы таких действий, как незаконный сбор персональных данных, достижение цели защиты от вреда, причиняемого фишинговыми информационными ресурсами, будет затруднительным.

В системной взаимосвязи с указанным выше находится проект федерального закона № 502104-8 «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях», который также принят в первом чтении Государственной Думой[4].

Его положения предполагают введение, в частности, дополнительных мер ответственности за невыполнение и (или) несвоевременное выполнение оператором предусмотренной законодательством Российской Федерации в области персональных данных обязанности

[1] Судебный департамент при Верховном суде Российской Федерации : [сайт]. URL: http://cdep.ru/?id=79 (дата обращения: 21.02.2024).

[2] Собрание законодательства Российской Федерации. 2006. № 31 (1ч.). Ст.3451.

[3] Законопроект № 502113-8 // СОЗД ГАС «Законотворчество». URL: https://sozd.duma.gov.ru/bill/502113-8 (дата обращения: 21.02.2024).

[4] СОЗД ГАС «Законотворчество». URL: https://sozd.duma.gov.ru/bill/502104-8 (дата обращения: 21.02.2024).

по уведомлению уполномоченного органа по защите прав субъектов персональных данных в случае установления факта неправомерной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных, а также за действия (бездействие) оператора, повлекшие неправомерную передачу (предоставление, распространение, доступ) информации (проектируемые чч. 10–17 ст. 13.11 КоАП РФ).

При этом действия (бездействие) оператора, повлекшие неправомерную передачу (предоставление, распространение, доступ) информации (и санкции за их совершение), предлагается дифференцировать в зависимости от количества записей о субъектах персональных данных и уникальных обозначений сведений о физических лицах, необходимых для определения таких лиц, либо если такие действия совершены в отношении специальной категории персональных данных (соответственно проектируемые чч. 12–14 и ч. 15 ст. 13.11 КоАП РФ).

В рамках настоящей статьи относительно данного законопроекта лишь отметим, что существенное увеличение размера административных штрафов (в абсолютном размере до 15 миллионов рублей), на наш взгляд, выглядит убедительным профилактическим стимулом для правомерного поведения операторов персональных данных в части недопущения и предотвращения утечек информационных баз с персональными данными, как и своевременное информирование уполномоченных органов о соответствующем инциденте.

Заключение и выводы

Несмотря на некоторую ясность в вопросе перспективы правового регулирования реакции государства на незаконный оборот персональных данных, проблематика противодействия юридическими средствами возмездному оформлению банковских карт для их последующей передачи и использования в преступных целях (как правило, с применением дистанционного банковского обслуживания), формированию нелегального рынка соответствующих услуг, с учетом обозначенной выше уголовной специализации криминальной деятельности требует внимания не только практических работников, но и представителей науки.

При этом юридические интересы в сфере противодействия информационно-телекоммуникационной преступности не ограничиваются обсуждением обозначенных выше вопросов. В повестке выработка на международном уровне оснований и порядка сотрудничества государств в сфере противодействия использованию информационно-коммуникационных технологий в преступных целях, юридическая проблематика регулирования применения искусственного интеллекта, противодействия дипфейкам, снижение спроса в даркнете на криминальные услуги и товары, используемые для совершения рассматриваемых деяний.

Также актуальными остаются вопросы неотвратимости наказания, совершенствования механизмов выявления (например, развитие системы Антифрод) и привлечения к ответственности лиц, совершивших преступления с использованием информационно-телекоммуникационных технологий, оперативной блокировки похищенных ими электронных денежных средств и возмещение причиненного преступлением в сфере телекоммуникации вреда.

Как представляется, отмеченные криминологические условия для совершенствования законодательства в сфере противодействия преступному использованию телекоммуникаций, могут представлять интерес для практикующих юристов и юристов-правоведов, а также специалистов в сфере IT-технологий.

Список источников

1. Батоев В. Б. Преступления, совершаемые с использованием или применением информационно-телекоммуникационных технологий: способы их совершения и количественные характеристики // Правопорядок: история, теория, практика. 2023. № 3 (38). С. 101–112. DOI: 10.47475/2311-696X-2023-38-3-101-112

2. Бегишев И. Р., Хисамова З. И. Криминологические риски применения искусственного интеллекта // Всероссийский криминологический журнал. 2018. Т. 12, № 6. С. 767–775. DOI: 10.17150/2500-4255.2018.12(6).767-775

3. Бегишев И. Р., Берсей Д. Д. Генезис криминальной социальной инженерии // Цифровые технологии и право : сборник научных трудов II Международной научно-практической конференции (Казань, 22 сентября 2023 г.) : в 6 т., т. 6. Казань : Познание, 2023. С. 24–34.

4. Никитин Е. В. Проблемы противодействия технологиям социальной инженерии как элементу преступной деятельности // Виктимология. 2023. Т. 10, № 4. С. 485–491. DOI: 10.47475/2411-0590-2023-10-4-485-491

КОНФЛИКТ ИНТЕРЕСОВ

Конфликт интересов отсутствует.

CONFLICT OF INTEREST

There is no conflict of interest.

Дата поступления статьи /Received: 30.03.2024.
Дата рецензирования /Revised: 27.05.2024.
Дата принятия статьи к публикации / Accepted: 15.07.2024.