Оригинальная статья / Original article

https://doi.org/10.21869/2223-1501-2023-13-3-90-101

Криминологические риски персональных данных: основные тенденции и прогнозы

И. С. Алихаджиева[1] ✉

[1]Российская криминологическая ассоциация имени Азалии Ивановны Долговой
г. Москва 117624, Российская Федерация

✉ e-mail: Alins1@yandex.ru

Резюме

Актуальность *статьи обусловлена глобальным ростом во всем мире преступлений, совершаемых в отношении персональных данных человека или с их использованием. По количеству утечек в Глобальную сеть личной конфиденциальной информации Россия занимает второе место в мире, а потому одной из серьезных проблем в нашей стране может стать преступность, связанная с незаконным оборотом персональных данных. В статье представлен оригинальный анализ основных тенденций и криминологических рисков этого вида преступности как нового сегмента российской преступности. На примерах следственно-судебной практики, статистических данных, экспертных оценок показаны основные тренды этого вида преступности и строится прогноз ее дальнейшего развития.*

Цель *исследования состоит в выявлении и формулировании основных тенденций и криминологических рисков, связанных с незаконным получением и (или) использованием личной конфиденциальной информации.*

Задачи*: на основе материалов криминологических исследований, статистических данных, следственно-судебной практики выявить и подвергнуть последующему осмыслению основные тенденции и криминологические риски незаконного оборота персональных данных.*

Методология*. В процессе работы использовались методы теоретического исследования (анализ, синтез, индукция и дедукция), а также статистический, документальный и формально-логический методы.*

Результаты*. На основе экспертных оценок, статистических данных и следственно-судебной практики установлены основные тренды развития преступности с персональными данными, оказывающие влияние на качественную и количественную трансформацию всей российской преступности в целом. Восполнен определенный пробел криминологической науки в части формулирования криминологических рисков, развитие которых может привести к росту латентного криминального насилия, мошеннических действий, коррупции, вымогательства, нарушения прав и свобод человека и др.*

Вывод*. До настоящего времени государством и законодателем до конца не осмыслены социально опасные последствия совершения преступлений с персональными данными. Их незаконный оборот обладает значительным криминогенным потенциалом, минимизировать который способны меры предупреждения, разработанные наукой и законодателем.*

Ключевые слова*: персональные данные; преступность; криминологические риски; конфиденциальная информация; хакерские атаки.*

Конфликт интересов*: Автор декларирует отсутствие явных и потенциальных конфликтов интересов, связанных с публикацией настоящей статьи.*

Для цитирования: Алихаджиева И. С. Криминологические риски персональных данных: основные тенденции и прогнозы // Известия Юго-Западного государственного университета. Серия: История и право. 2023. Т. 13, № 3. С. 90–101. https://doi.org/10.21869/2223-1501-2023-13-3-90-101.

Поступила в редакцию 10.04.2023 Принята к публикации 12.05.2023 Опубликована 30.06.2023

Criminological Risks of Personal Data: Main Trends and Forecasts

Inna S. Alikhadzhiyeva[1] ✉

[1]Russian Criminological Association named after Azalea Ivanovna Dolgova
Moscow 117624, Russian Federation

✉ e-mail: Alins1@yandex.ru

Abstract

Relevance *of the article is due to the global growth worldwide of crimes committed against or using human personal data. In terms of the number of leaks to the Global Network of Personal Confidential Information, Russia ranks second in the world, and therefore one of the serious problems in our country can be crime associated with the illegal trafficking of personal data. The article presents an original analysis of the main trends and criminological risks of this type of crime as a new segment of Russian crime. Using examples of investigative and judicial practice, statistical data, expert assessments, the main trends of this type of crime are shown and a forecast of its further development is based.*

The purpose *of the study is to identify and formulate the main trends and criminological risks associated with the illegal receipt and/or use of personal confidential information.*

Objectives: *on the basis of materials of criminological research, statistical data, investigative and judicial practice, to identify and subject to subsequent comprehension the main trends and criminological risks of illegal trafficking in personal data.*

Methodology*. In the process of work, methods of theoretical research (analysis, synthesis, induction and deduction), as well as statistical, documentary and formal-logical methods were used.*

The results*. Based on expert assessments, statistical data and investigative and judicial practice, the main trends in the development of crime with personal data have been established, which affect the qualitative and quantitative transformation of all Russian crime as a whole. A certain gap in criminological science has been filled in terms of the formulation of criminological risks, the development of which can lead to an increase in latent criminal violence, fraudulent actions, corruption, extortion, violation of human rights and freedoms, etc.*

Conclusion*. Until now, the state and the legislator have not fully understood the socially dangerous consequences of committing crimes with personal data. Their illegal trafficking has significant criminogenic potential, which is minimized by the prevention measures developed by science and the legislator.*

Keywords*: personal data; crime; criminological risks; confidential information; hacker attacks.*

Conflict of interest: *The Author declare the absence of obvious and potential conflicts of interest related to the publication of this article.*

For citation: Alikhadzhiyeva I. S. Criminological Risks of Personal Data: Main Trends and Forecasts. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta. Seriya: Istoriya i pravo = Proceedings of the Southwest State University. Series: History and Law*. 2023; 13(3): 90–101. (In Russ.) https://doi.org/10.21869/2223-1501-2023-13-3-90-101

Received 10.04.2023 Accepted 12.05.2023 Published 30.06.2023

***

Введение

В мировых масштабах утечек цифровых данных пользователей Россия занимает второе после США место в мире. За 2022 г. доля нашей страны составляет 2 млрд из 3 млрд «слитых» записей в Глобальную сеть во всем мире. В прошлом году в России случилось более 40 крупных цифровых инцидентов с персональными данными. Самые значимые из них по количеству были связаны с утечкой конфиденциальной информации из баз ретейлеров, крупных транспортных агрегаторов, масс-маркета и сервисов доставки. Масштабная компрометация личных данных была зафиксирована в приложениях следующих компаний: «Яндекс.Еда» и «Delivery Club» (соответственно 50 млн и 2,2 млн персональных данных пользователей (фамилии, номер телефона, адрес доставки, суммы чеков,

адреса электронной почты, IP-адреса)); Гемотест (две базы данных, состоящие из 554 млн заказов и 31 млн строк с фамилиями, датами рождения, адресами, номерами телефонов, серией и номером паспорта и результатами анализов); Туту.ру (2,6 млн заказов, 2,29 млн телефонных номеров, ФИО и e-mail). В открытые источники попала и клиентская база ГИБДД, СДЭК, Wildberries, «Билайн», ВТБ, «ВКонтакте», РЖД, авиакомпании «Победа», телекоммуникационных компаний «Ростелеком» и «ВымпелКом», сервисов «Мир Тесен», Fotostrana.ru, развлекательного ресурса Pikabu, школы управления «Сколково» и др.

«Лаборатория Касперского» приводит следующие показатели потери персональных данных пользователей: в 2022 г. было скомпрометировано почти 300 млн пользовательских данных, из которых 16%, или около 48 млн строк. В открытом доступе, помимо ФИО и номеров телефонов, оказывались домашние адреса, банковские сведения и сканы паспортов, логины и пароли. Преступники раскрыли 168 значимых баз данных российских компаний1. Эксперты считают, что в 2023 г. число утечек может вырасти еще на 20%2. Эти прогнозы уже подтверждает компания DLBI, специалисты которой раскрывают статистику крупных утечек баз данных за январь-февраль 2023 г. Их количество по сравнению с аналогичным периодом прошлого года выросло в три раза – с 7 до 21. Приведенные цифры отражают общий тренд на активное использование персональных данных преступниками, что обусловливает необходимость проведения научных исследований по этой проблематике.

Методология

Тематика работы предопределила совокупность методов исследования. Его основу составили такие методы, как анализ, синтез, индукция и дедукция, применяемые для выделения и описания новых тенденций преступности, связанной с персональными данными, криминологических рисков персональных данных и формирования прогнозов относительно ее дальнейшего развития. Статистический и документальный методы были использованы для обоснования актуальности исследования, изучения научных публикаций, показателей уголовной статистики, судебной практики, а также данных, характеризующих количество инцидентов по утечке личных данных в публичное пространство. Формально-логический метод позволил описать результаты, комплексно и логически верно систематизировать материал и сформулировать выводы исследования.

Результаты и их обсуждение

В России оценка качественно-количественных параметров преступлений, совершаемых в отношении персональных данных или с их использованием, не представляется объективной ввиду отсутствия персональных данных как самостоятельного предмета уголовно-правовой охраны, за исключением ст. 1732 УК РФ «Незаконное использование документов для образования (создания, реорганизации) юридического лица». На основании анализа материалов уголовных дел, приговоров, вступивших в законную силу, и сообщений средств массовой информации установлены основные ситуации утраты персональных данных:

1. Владелец сам сообщает личную информацию о себе посредством обмана

[1] 300 млн данных пользователей. Названы лидеры по масштабу утечек в России. Ими оказались сервисы доставки и ритейлеры // РБК. URL: https://www.rbc.ru/life/news/63fc38ef9a79474882d03e46 (дата обращения: 09.04.2023).

[2] Эксперт Новикова: Более 1,5 млрд записей с персональными данными попали в сеть в 2022 году // РГ. URL: https://rg.ru/2022/12/08/bolee-15-mlrd-zapisej-s-personalnymi-dannymi-popali-v-set-v-2022-godu.html (дата обращения: 09.04.2023).

злоумышленниками с использованием методов социальной инженерии. Располагая номинативными персональными данными, полученными из социальных сетей и других общедоступных источников, «слитых» баз в теневом сегменте Интернета, преступники устанавливают с предполагаемой жертвой доверительный контакт. В результате психологического манипулирования они чаще всего представляются сотрудниками банков или правоохранительных органов, выманивая у владельца пароли к банковским картам, аккаунтам интернет-магазинов, брокерским счетам и другим приложениям с целью хищения денежных средств.

2. Персональные данные находятся в прямом доступе у злоумышленника в силу его служебного положения. Речь идет о сотрудниках банков, других микрокредитных организаций, специалистах офисов мобильной связи, представителях правоохранительных органов и др. В прошлом году в интернет попало около 100 млн строк личных сведений, основными причинами утечек тогда стали сливы от сотрудников организаций – обычных работников (61%) и руководства компании (9,1%), которые решили подзаработать[1].

3. Хакерские атаки. Глобальные экономические и политические трансформации не могли не повлиять на киберпреступность с персональными данными. В исследовании компании-разработчика решений для обеспечения информационной безопасности InfoWatch говорится, что по всему миру за прошлый год количество утечек выросло на 93%, а в России – на 45%. Геополитическая обстановка в мире и вооруженный конфликт в Украине способствовали смене мотивов и философии хакерских атак на конфиденциальную информацию. По данным аналитиков Group-IB, если раньше преступники стремились извлечь прибыль, то теперь действуют из идейных соображений, стараясь вызвать резонанс[2].

Имеющиеся аналитические материалы и научные труды [1, с. 24; 2, с. 53; 3, с. 158; 4, с. 38; 5, с. 291] позволяют обозначить некоторые тренды в развитии этого нового сегмента преступности. К прогнозируемым криминологическим рискам следует отнести модернизацию качественно-количественных параметров всей преступности как следствие последовательного увеличения посягательств в отношении персональных данных и (или) с их использованием:

1. Количественный прирост показателей преступности, обусловленный высоким уровнем развития технических средств обработки информации, в том числе конфиденциальной. Новейшие биометрические технологии позволяют провести распознавание физического лица, имеющего профиль в Глобальной сети[3]. Например, фотоизображение любого человека, размещаемое в социальной сети или в другом открытом сетевом ресурсе даже без указания номинативных персональных данных, может быть идентифицировано [6, с. 109]. Еще в 2016 г. в средствах массовой информации сообщалось о появлении программы Findface. Опираясь на данные нейросети, ее разработчиками сканировались фото- и видеоизображения из базы данных «ВКонтакте», а далее автоматически систематизировались данные о конкретном лице с подборкой его двойников и клонов. Отсюда следует прогнозировать проблему обеспечения безопасности конфиденциальной

[1] Соломкина Е. В России за полгода в интернет «утекло» более 300 млн. строк персональных данных // Readovka. URL: https://readovka.news/news/109821 (дата обращения: 09.03.2023).

[2] Текучая ситуация: эксперты назвали лидеров по слитым данным в этом году // Известия. URL: https://iz.ru/1477710/ivan-chernousov/tekuchaia-situatciia-eksperty-nazvali-l (дата обращения: 06.04.2023).

[3] Питерский фотограф сравнил пассажиров метро с их профилями «ВКонтакте» // Geektimes. URL: https://geektimes.ru/post/274356/ (дата обращения: 06.04.2023).

информации участников киберпространства [7, с. 769].

В современных реалиях, когда произошла стремительная модификация Интернета в платформу для криминальной деятельности, деанономизация личных данных, размещаемых самими пользователями в открытом доступе, может быть использована, к примеру, для мошенничества, вымогательства, хищения денежных средств и др. Интернет-ресурсы с открытыми персональными данными используются в качестве инструмента распространения клеветы, для оскорблений, буллинга, мести, а виновные в них в большинстве случаев избегают уголовного преследования. Изложенное приводит к выводу о том, что фактические значения динамики и уровня преступлений с персональными данными в разы выше зафиксированных уголовной статистикой.

2. Качественная трансформация общеуголовной преступности и других ее видов. Обладая существенным криминогенным потенциалом, персональные данные как информация уже используются при совершении:

2.1. Тяжких преступлений против личности, в том числе посягательств на жизнь. Примером тому является недавнее резонансное убийство в г. Санкт-Петербурге военного корреспондента Владлена Татарского (Максима Фомина). Его персональные данные были внесены в базу данных «Миротворца» – украинского сайта-деанонимизатора[1]. В ней находятся подробные личные данные и других граждан Российской Федерации, среди которых военнослужащие ФСБ, МВД, Росгвардии, судьи, прокуроры, следователи, работники налоговых органов, журналисты, приговоренные киевским режимом к уничтожению. В СМИ сообщалось и о причастности украинских боевиков к убийству политического обозревателя Международного евразийского движения Дарьи Дугиной, конфиденциальные данные которой также содержит открытый украинский ресурс[2]. После взрыва двух журналистов на странице сайта с их личными данными появилась запись «Ликвидирован», о чем с распечаткой скриншота сообщил на заседании ООН представитель от России Василий Небензя[3].

Учитывая сложную геополитическую обстановку, увеличивается в разы угроза физической расправы над лицами, обеспечивающими государственную безопасность страны. Например, в 2022 г. ФСБ России были задержаны участники организованной группы, состоящей из сотрудников налоговых органов и частного сыска. Имея доступ к специальным базам данных, они незаконно собирали и передавали через посредника третьим лицам, в том числе иностранным гражданам, личную информацию о тридцати потерпевших, включая их персональные данные (источники дохода, счета в банках, адреса регистрации, имущество)[4]. Как феномен с высоким индексом деструктивности этот вид криминальной активности может способствовать совер-

[1] Захарова указала на роль одиозного сайта «Миротворец» в убийстве Татарского // 5-TV. URL: https://www.5-tv.ru/news/426677/zaharo-va-ukazala-narol-odioznogo-sajta-mirotvorec-vubijstve-tatarskogo (дата обращения: 06.04.2023).

[2] Досье на Дугина и его дочь было размещено на «Миротворце» // Известия. URL: https://iz.ru/1382662/2022-08-21/dose-na-dugina-i-ego-doch-bylo-razmeshcheno-na-mirotvortce (дата обращения: 06.04.2023).

[3] Небензя показал в ООН распечатку скриншота с украинского сайта «Миротворец», на котором фото Дугиной перечеркнуто надписью «ликвидирована» // Российская газета. URL: https://rg.ru/2022/08/24/postpred-rossii-pri-oon-vasilij-nebenzia-ne-znaiu-pochemu-ssha-pri (дата обращения: 06.04.2023).

[4] ФСБ РФ разоблачила сливавших иностранцам данные о военнослужащих // Известия. URL: https://iz.ru/1352429/2022-06-20/fsb-rf-razoblachila-slivavshikh-inostrantcam-dannye-o-voennosluzhashchikh (дата обращения: 06.04.2023).

шению преступлений против общественного порядка – чужие персональные данные с подменой личности могут обеспечивать анонимность террористам, экстремистам и другим международным преступникам.

2.2. *Должностных и коррупционных преступлений.* Высокий спрос на персональные данные породил криминальный рынок услуг, которые оказывают сотрудники правоохранительных органов на коммерческой основе. Мониторинг судебной практики показывает, что коррумпированными сотрудниками полиции осуществляется продажа персональных данных конкурентам по бизнесу, оппонентам в судебных тяжбах. Например, оперуполномоченный отдела «К» Бюро специальных технических мероприятий МВД по Республике Башкортостан передавал через интернет-мессенджер родственника своей супруги коммерсанту персональные данные его коллег-бизнесменов. Заказчика интересовали их адреса, телефоны, государственные номера автомобилей, сведения о недвижимом имуществе и другие данные[1].

В случае, когда персональные данные получены из специальных баз МВД РФ, они могут быть использованы и в других преступных целях. Так, Кузьминским районным судом г. Москвы был постановлен приговор четырем подсудимым – сотрудникам МВД РФ. Они были признаны виновными по ст. 290 УК РФ за получение незаконного денежного вознаграждения за передачу данных умерших и погибших людей третьим лицам. Как установило следствие, фигуранты уголовного дела, имея доступ к базе данных по происшествиям и фактам смерти людей, в течение двух лет через различные мессенджеры продавали персональные данные представителям фирм, оказывающих ритуальные услуги. Деньги в сумме более 6 млн руб. переводились на карты, принадлежащие родственникам и знакомым полицейских[2].

Практика российских судов показывает и неординарные случаи использования правоохранителями чужих персональных данных. Так, в ходе компьютерной игры Radmir RP с участием инспектора ДПС по Буздякскому району Башкирии, старшего лейтенанта М., произошла ссора с другим ее игроком. Пользователи с никами Khabib Ufimskiy, инспектор, и Fernando Carrasco, житель г. Грозного Чеченской Республики, обменялись оскорблениями. Конфликт между ними был продолжен во «ВКонтакте» и мессенджере Discord. Используя служебное положение в целях мести за оскорбление, М. с помощью бота и базы МВД РФ установил имя, адрес, телефон и другие персональные данные обидчика. Затем сотрудник МВД РФ разместил персональные данные оппонента в игровой чат, после чего ему стали поступать угрозы и спам-рассылки. После проведения проверки Следственным комитетом России действия сотрудника МВД РФ были квалифицированы по ст. 137, 272, 285 УК РФ[3].

2.3. *Мошенничества, ставшего наиболее активно применяемой формой незаконного завладения и использования персональных данных.* Персональные данные клиентов онлайн-банкинга используются различного рода мошенниками для хищения денежных средств на

[1] СК РФ проверяет полицейского, который продавал персональные данные граждан // Российская газета. URL: https://rg.ru/2022/10/25/reg-pfo/ (дата обращения: 16.03.2023).

[2] Сотрудники полиции продали данные граждан и попали под суд // Версия. URL: https://versia.ru/sotrudniki-policii-prodali-dannye-grazhdan-i-popali-pod-sud (дата обращения: 23.03.2023).

[3] Ссора в ходе компьютерной игры привела инспектора ГИБДД Башкирии к нескольким уголовным делам // Ufacity News.ru. URL: https://ufacitynews.ru/news/2023/01/19/ ssora-v-hode-kompyuternoj-igry-privela-inspek-tora-gibdd-bashkirii-k-neskolkim-ugolovnym-delam/ (дата обращения: 12.03.2023).

банковских счетах. Один из современных способов интернет-мошенничества в криминалистической литературе получил название «фишинг». Его суть заключается в заманивании жертвы по фишинговой ссылке на фейковую страницу банков или онлайн-магазинов для ввода персональных данных, которыми воспользуются мошенники для вывода чужих денежных средств [8, с. 132; 9, с. 179]. Фактически здесь происходит подмена личности или ее «кража», когда преступник при совершении определенных транзакций действует от имени другого человека, выдает себя за него при помощи похищенных личных данных [10, с. 20; 11, с. 50].

2.4. *Вымогательства.* Сюда относятся случаи распространения материалов с персональными данными, компрометирующими потерпевшего (как правило, сексуального характера). Из фабулы уголовных дел этой категории следует, что, шантажируя размещением в публичном пространстве интимных фото- или видеоизображений жертвы, преступник требует у нее передачи денег. В одной из своих опубликованных работ нами отмечался риск утечки личных данных секс-работников, подыскивающих в сети Интернет клиентов для оказания коммерческих услуг, и вебкам-моделей, занимающихся секс-позированием [12, с. 164]. Многие их профили с фотоизображением были идентифицированы с помощью специальных программ и помещены на спецресурсы о лицах, занимающихся проституцией, что повлекло репутационные потери и групповой буллинг в Интернете [13, с. 106]. К примеру, в одной из социальных сетей был размещен откровенный ролик с изображением новосибирской студентки. Несколько лет назад она занималась веб-камингом, т. е. являлась виртуальной моделью закрытого ресурса в Интернете. Кибервымогатели по изображению идентифицировали ее аккаунт в социальной сети и стали требовать передачи денежных средств. Жертва отказалась платить и написала заявление в полицию. Преступников не нашли, а в сеть попали порносъемки потерпевшей с указанием ее имени, фамилии, места жительства, работы и др.[1] Очевидно, что такой комплекс преступлений, направленных к единой цели – получить денежные средства жертвы – и обеспечивающих ее достижение, требует консолидации организованной групповой деятельности.

В иных случаях мотивом использования изображения жертвы может быть месть, в том числе порноместь [14, с. 62]. Здесь установлены факты опубликования в социальных сетях, приложениях для обмена сообщениями, онлайн-форумах экс-супругами и сожителями фотографий сексуального характера без согласия изображенных на них партнёров. Для мести за расставание один из бывших возлюбленных довольно часто прибегает к помощи хакеров, осуществляющих несанкционированный доступ к чужим персональным данным, их похищение и передачу заказчику за денежное вознаграждение.

2.5. *Неправомерного доступа к компьютерной информации*. Большую популярность среди злоумышленников приобретают хищения персональных данных для целей последующей продажи. Эксперты говорят о высоком спросе на базы персональных данных, которые продаются в теневом секторе сети Интернет – Даркнете и Tor. При этом в Даркнете 30% слитой информации – это базы данных компаний США, на втором месте количество данных из России – 13%. Данные для продажи могут дробиться по количеству деанонимизированных записей и даже строк. По оценкам специалистов, в 2022 г. хакеры украли 970,5 млн строк записей о персональных данных. Только в февральской утечке 2022 г. базы дан-

[1] «С тебя 15 тысяч»: вебкам-девушку шантажировали «голым» видео из приват-чата, а потом выложили его в сеть // Комсомольская правда. URL: https://www.nsk.kp.ru/daily/27088/4161402/ (дата обращения: 12.03.2023).

ных службы доставки СДЭК было предано огласке 823 млн строк с персональными данными[1]. Эти показатели косвенно подтверждают ожидание возрастания интенсивности атак хакеров в 2023 г. Злоумышленники будут разрабатывать новые схемы и решения, которые сложно будет обнаружить, что приведет к многократному росту преступлений, связанных с персональными данными. Не случайно правоведы предлагают в отдельной норме криминализировать хищение баз персональных данных [15, с. 36].

В криминологическом плане обращает на себя внимание тенденция расширения спектра новых криминальных форм использования персональных данных. Исследователи отмечают увеличение запросов на неправомерный доступ к компьютерной информации, взлом аккаунтов в социальных сетях для получения персональных данных и личной переписки человека [16, с. 26]. Правоприменительная практика подтверждает, что эти сведения используются в целях слежки за конкурентами и для сталкинга. Нарушая личную свободу преследуемого лица, сталкер осуществляет навязчивое преследование жертвы, в том числе посредством нежелательных коммуникаций (звонки, сообщения в соцсетях и мессенджерах), угроз применения насилия, оскорблений, распространения клеветы и сведений конфиденциального характера, рождающих у жертвы страх [17, с. 279], дистресс (истощение от напряжения). Зафиксированы случаи, когда сталкер незаконно проникал в жилище, размещал в сети Интернет материалы сексуального характера без согласия потерпевшего и т.п. Учеными в этой связи поднимается проблема кибersталкинга как девиантной формы поведения [18, с. 29] и уголовной ответственности за него как нарушающего неприкосновенность частной жизни человека [19, с. 58].

Новой криминологической реальностью становится совершение преступлений для завладения именно персональными данными для их последующего использования в преступных целях – получения микрозаймов и кредитов по поддельным паспортам с настоящими персональными данными. Статистика преступлений с персональными данными не ведется, однако имеющиеся экспертные оценки позволяют говорить о том, что в 80% случаев преступники используют их для совершения новых общественно опасных деяний. Так, получила широкое распространение криминальная практика хищений мобильных телефонов для получения хранящихся в них персональных данных. М. А. Бугера, отмечая их рост, пишет, что «сегодня хищения сотовых телефонов совершаются не для их последующей продажи, а в целях получения персональных данных граждан (фамилия, имя, отчество; номер и серия паспорта; адрес электронной почты; номер банковской карты и т. д.), которые нужны для доступа к их картам и банковским счетам» [20, с. 120].

Этот вывод ученого подтверждает и следственно-судебная практика. Например, при помощи персональных данных, полученных из похищенного у И. телефона, злоумышленники не только перевели денежные средства из его мобильного банка, но и, получив доступ к учетной записи на «Госуслугах», изменили контактную информацию и оформили электронную цифровую подпись. С ее помощью и с использованием ИНН, СНИЛС и паспортных данных с портала «Госуслуги» преступниками в нескольких банках были получены микрозаймы и кредиты на общую сумму более 1 млн руб.[2]

[1] Черноусов И. Урожай сливов: утечки персональных данных россиян выросли в 40 раз // Известия. URL: https://iz.ru/1457616/ivan-chernousov/urozhai-slivov-utechki-personalnykh-dan (дата обращения: 12.03.2023).

[2] Потерял телефон – отдавай миллион // Финансовая культура: [сайт]. URL: https://fincult.info/rake/poteryal-telefon-otdavay-million (дата обращения: 12.03.2023).

Выводы

В криминологическом плане для предупреждения преступлений с персональными данными имеет значение научное знание о совершении других, в том числе тяжких преступлений, с использованием незаконно полученных персональных данных. В ходе исследования установлено, что их совокупность может включать: убийства, причинение различного вреда здоровью, посягательства против свободы, чести и достоинства, собственности, политических, экономических прав граждан, интересов службы, нарушение неприкосновенности частной жизни, переписки и иных сообщений и др.

Негативная трансформация преступности, связанной с незаконным оборотом персональных данных, с высоким уровнем ее латентной части во многом объясняется тем, что в России не в полной мере осознаны возможные масштабы угрозы, которую представляет их незаконный оборот. Об этом свидетельствует и отсутствие специальной уголовной ответственности за посягательства в отношении персональных данных или с их использованием на фоне сообщений средств массовой информации и пресс-служб правоохранительных ведомств о беспрецедентном количестве утечек личных данных в публичное пространство. А потому и наука не приступила к серьезному изучению основных криминологических рисков деанонимизации персональных данных и ведущих трендов преступности, связанной с использованием конфиденциальной информации о человеке.

Список литературы

1. Ефимова Е. А., Семенов С. А. Персональные данные как объект преступного посягательства // StudNet. 2021. Т. 4, № 12. С. 23–25.

2. Пикуров Н. Проблемы квалификации преступных посягательств на частную жизнь: теория и судебная практика // Уголовное право. 2019. № 2. С. 51–58.

3. Стяжкина С. А. Информация как объект уголовно-правовой охраны: понятие, признаки, виды // Вестник Удмуртского университета. Экономика и право. 2015. № 2. С. 157–161.

4. Филатова М. А. Персональные данные как предмет преступного посягательства // Уголовное право. 2021. № 11. С. 35–43.

5. Халиулина Э. Т. Преступления, совершаемые с использованием персональных данных: характеристика состояния // Военное право. 2021. № 2 (66). С. 289–294.

6. Чукреев В. А. Персональные данные, в том числе биометрические данные, как предметы уголовно-правовой охраны // Вестник Университета имени О. Е. Кутафина (МГЮА). 2022. № 3 (91). С. 107–116.

7. Бегишев И. Р., Хисамова З. И. Криминологические риски применения искусственного интеллекта // Всероссийский криминологический журнал. 2018. № 6. С. 767–775.

8. Чупрова А. Ю. Проблемы квалификации мошенничества с использованием информационных технологий // Уголовное право. 2015. № 5. С. 131–134.

9. Сафонов В. Н., Андреев Д. В. «Мошенничество от пандемии»: новые способы хищений // Вестник Волжского университета им. В. Н. Татищева. 2022. Т. l, № 2 (101). С. 177–184.

10. Атагимова Э. И., Потемкина А. Т., Цопанова И. Г. «Кража личности» как самостоятельное преступление или разновидность мошенничества // Правовая информатика. 2017. № 3. С. 14–22.

11. Кузьмин Ю. А. Кража персональных данных (криминологический аспект) // Oeconomia et Jus. 2020. № 3. С. 48–57.

12. Алихаджиева И. С. О новых тенденциях современной секс-индустрии и ее криминологических рисках // Актуальные проблемы российского права. 2021. Т. 16, № 4. С. 160–173.

13. Ильницкий А. С. Криминологические риски интимной коммуникации в сети Интернет // Гуманитарные, социально-экономические и общественные науки. 2021. № 9. С. 106–109.

14. Соловьев В. С. Порноместь: сущность явления и проблемы его уголовно-правовой оценки // Уголовное право. 2017. № 6. С. 60–64.

15. Баринов С. В. О криминализации преступного нарушения неприкосновенности частной жизни, совершаемого в форме распространения баз персональных данных // Российский следователь. 2017. № 4. С. 35–38.

16. Алихаджиева И. С. Некоторые проблемы уголовно-правовой охраны неприкосновенности частной жизни // Конституционные чтения: межвузовский сборник научных трудов. Вып. 9, ч. 2. Саратов: Поволжская акад. гос. службы им. П. А. Столыпина, 2009. С. 25–29.

17. Сторублёнкова Е. Г., Самуткин В. Л. Сталкинг: синдром навязчивого преследования // Пробелы в российском законодательстве. 2017. № 6. С. 278–281.

18. Кобец П. Н. Противодействие угрозам кибersталкинга – важнейшей проблеме, исследуемой в рамках совершенствования аспектов информационной безопасности регионов в условиях глобализации информационного пространства // Вестник Прикамского социального института. 2017. № 1 (76). С. 27–35.

19. Юрченко И. А. Сталкер как субъект уголовной ответственности // Вестник Университета имени О. Е. Кутафина. 2018. № 12 (52). С. 53–61.

20. Бугера М. А. Борьба с хищениями сотовых телефонов и персональных данных, содержащихся в них: проблемы и пути решения // Вестник Санкт-Петербургского университета МВД России. 2022. № 2 (94). С. 109–111.

References

1. Efimova E. A., Semenov S. A. Personal'nye dannye kak ob"ekt prestupnogo posyagatel'stva [Personal data as an object of criminal encroachment]. *StudNet = StudNet*, 2021, vol. 4, no. 12, pp. 23–25.

2. Pikurov N. Problemy kvalifikacii prestupnyh posyagatel'stv na chastnuyu zhizn': teoriya i sudebnaya praktika [Problems of qualification of criminal encroachments on privacy: theory and judicial practice]. *Ugolovnoe pravo = Criminal law*, 2019, no. 2, pp. 51–58.

3. Styazhkina S. A. Informaciya kak ob"ekt ugolovno-pravovoj ohrany: ponyatie, priznaki, vidy [Information as an object of criminal law protection: concept, signs, types]. *Vestnik Udmurtskogo universiteta. Ekonomika i pravo = Bulletin of Udmurt University. Economics and law*, 2015, no. 2, pp. 157–161.

4. Filatova M. A. Personal'nye dannye kak predmet prestupnogo posyagatel'stva [Personal data as a subject of criminal encroachment]. *Ugolovnoe pravo = Criminal law*, 2021, no. 1, pp. 35–43.

5. Haliulina E. T. Prestupleniya, sovershaemye s ispol'zovaniem personal'nyh dannyh: harakteristika sostoyaniya [Crimes committed using personal data: characteristics of the state]. *Voennoe pravo = Military law*, 2021, no. 2 (66), pp. 289–294.

6. Chukreev V. A. Personal'nye dannye, v tom chisle biometricheskie dannye, kak predmety ugolovno-pravovoj ohrany [Personal data, including biometric data, as subjects of criminal law

protection]. *Vestnik Universiteta imeni O. E. Kutafina (MGYUA) = Bulletin of O. E. Kutafin University (MGUA)*, 2022, no. 3 (91), pp. 107–116.

7. Begishev I. R., Hisamova Z. I. Kriminologicheskie riski primeneniya iskusstvennogo intellekta [Criminological risks of the use of artificial intelligence]. *Vserossijskij kriminologicheskij zhurnal = All-Russian Criminological Journal*, 2018, no. 6, pp. 767–775.

8. Chuprova A. Yu. Problemy kvalifikacii moshennichestva s ispol'zovaniem informacionnyh tekhnologij [Problems of qualification of fraud using information technologies]. *Ugolovnoe pravo = Criminal law*, 2015, no. 5, pp. 131–134.

9. Safonov V. N., Andreev D. V. "Moshennichestvo ot pandemii": novye sposoby hishchenij ["Fraud from a pandemic": new methods of theft]. *Vestnik Volzhskogo universiteta im. V. N. Tatishcheva = Bulletin of the Volga University named after V.N. Tatishchev*, 2022, vol. 1, no. 2 (101), pp. 177–184.

10. Atagimova E. I., Potemkina A. T., Copanova I. G. "Krazha lichnosti" kak samostoyatel'noe prestuplenie ili raznovidnost' moshennichestva ["Identity theft" as an independent crime or a type of fraud]. *Pravovaya informatika = Legal informatics*, 2017, no. 3, pp. 14–22.

11. Kuzmin Yu. A. Krazha personal'nyh dannyh (kriminologicheskij aspekt) [Identity theft (criminological aspect)]. *Oeconomia et Jus = Economia et Jus*, 2020, no. 3, pp. 48–57.

12. Alikhadzhieva I. S. O novyh tendenciyah sovremennoj seks-industrii i ee kriminologicheskih riskah [On new trends in the modern sex industry and its criminological risks]. *Aktual'nye problemy rossijskogo prava = Actual problems of Russian law*, 2021, vol. 16, no. 4, pp. 160–173.

13. Il'nickij A. S. Kriminologicheskie riski intimnoj kommunikacii v seti Internet [Criminological risks of intimate communication on the Internet]. *Gumanitarnye, social'no-ekonomicheskie i obshchestvennye nauki = Humanitarian, socio-economic and social sciences*, 2021, no. 9, pp. 106–109.

14. Solov'ev V. S. Pornomest': sushchnost' yavleniya i problemy ego ugolovno-pravovoj ocenki [Porn revenge: the essence of the phenomenon and the problems of its criminal law assessment]. *Ugolovnoe pravo = Criminal law*, 2017, no. 6, pp. 60–64.

15. Barinov S. V. O kriminalizacii prestupnogo narusheniya neprikosnovennosti chastnoj zhizni, sovershaemogo v forme rasprostraneniya baz personal'nyh dannyh [On the criminalization of a criminal violation of privacy committed in the form of distribution of personal data databases]. *Rossijskij sledovatel' = Russian investigator*, 2017, no. 4, pp. 35–38.

16. Alikhadzhieva I. S. [Some problems of criminal and legal protection of privacy]. *Konstitucionnye chteniya. Mezhvuzovskij sbornik nauchnyh trudov* [Constitutional readings. Intercollegiate collection of scientific works]. Saratov, Povolzhskaya akademiya gosudarstvennoj sluzhby im. P. A. Stolypina Publ., 2009, vol. 9, pt. 2, pp. 25–29. (In Russ.)

17. Storublyonkova E. G., Samutkin V. L. Stalking: sindrom navyazchivogo presledovaniya [Stalking: obsessive persecution syndrome]. *Probely v rossijskom zakonodatel'stve = Gaps in Russian legislation*, 2017, no. 6, pp. 278–281.

18. Kobec P. N. Protivodejstvie ugrozam kiberstalkinga – vazhnejshej probleme, issleduemoj v ramkah sovershenstvovaniya aspektov informacionnoj bezopasnosti regionov v usloviyah globalizacii informacionnogo prostranstva [Countering cyber stalking threats is the most important problem investigated as part of improving information security aspects of regions in the context of globalization of the information space]. *Vestnik Prikamskogo social'nogo instituta = Bulletin of the Prikamsk Social Institute*, 2017, no. 1 (76), pp. 27–35.

19. Yurchenko I. A. Stalker kak sub"ekt ugolovnoj otvetstvennosti [Stalker as a subject of criminal liability]. *Vestnik Universiteta imeni O. E. Kutafina = Bulletin of the University named after O. E. Kutafin*, 2018, no. 12 (52), pp. 53–61.

20. Bugera M. A. Bor'ba s hishcheniyami sotovyh telefonov i personal'nyh dannyh, soderzhashchihsya v nih: problemy i puti resheniya [The fight against theft of cell phones and personal data contained in them: problems and solutions]. *Vestnik Sankt-Peterburgskogo universiteta MVD Rossii = Bulletin of St. Petersburg University of the Ministry of Internal Affairs of Russia*, 2022, no. 2 (94), pp. 109–111.

Информация об авторе / Information about the Author

Алихаджиева Инна Саламовна, доктор юридических наук, доцент, Российская криминологическая ассоциация имени Азалии Ивановны Долговой, г. Москва, Российская Федерация,
e-mail: Alins1@yandex.ru,
ORCID: 0000-0002-6998-930X

Inna S. Alikhadzhiyeva, Dr. of Sci. (Juridical), Associate Professor, Russian Criminological Association named after Azalea Ivanovna Dolgova, Moscow, Russian Federation,
e-mail: Alins1@yandex.ru,
ORCID: 0000-0002-6998-930X