 DOI 10.17150/2411-6122.2025.2.96-108 ISSN 2411-6122

Научная статья
УДК 343.9
EDN NQGBRY
DOI 10.17150/2411-6122.2025.2.96-108

Криминалистическая характеристика незаконного использования, передачи, сбора и хранения компьютерной информации, содержащей персональные данные

З.И. Харисова

Уфимский университет науки и технологий, г. Уфа, Российская Федерация, Zarinaid@mail.ru

Аннотация. В статье описываются элементы криминалистической характеристики преступлений, связанных с незаконными использованием, хранением, передачей и сбором информации, содержащей персональные данные. Показана необходимость повышения эффективности расследования указанного вида преступлений, что обусловлено ежегодным ростом утечек конфиденциальных сведений. Прикладное значение исследования заключается в возможности формирования на основе криминалистической характеристики указанного вида преступлений частных криминалистических методик их расследования, создания новых криминалистических учетов цифровых доказательств, разработки специализированного программного обеспечения в виде систем поддержки принятия решений, применяемых при выдвижении следственных версий, а также формирования информационной модели (цифрового двойника) преступления. В рамках исследования использовалась совокупность общих методов научного познания (описание, обобщение и сравнение), общенаучных (анализ, синтез, моделирование и классификация), а также частнонаучных методов (статистический, кибернетический).

Ключевые слова: компьютерные преступления, персональные данные, незаконный сбор данных, криминалистическая характеристика преступлений, цифровая модель преступления, цифровые двойники, искусственный интеллект.

Для цитирования: Харисова З.И. Криминалистическая характеристика незаконного использования, передачи, сбора и хранения компьютерной информации, содержащей персональные данные / З.И. Харисова. — DOI 10.17150/2411-6122.2025.2.96-108. — EDN NQGBRY // Сибирские уголовно-процессуальные и криминалистические чтения. — 2025. — № 2. — С. 96–108.

Original article

Criminalistic Characteristics of the Illegal Use, Transfer, Collection and Storage of Computer Information Containing Personal Data

Z.I. Kharisova

Ufa University of Science and Technology, Ufa, the Russian Federation, Zarinaid@mail.ru

Abstract. The article describes elements of the digital characteristics of crimes connected with the illegal use, storage, transfer and collection of personal information. The author proves the necessity of improving the effectiveness of investigating this type of crimes as the number of cases of confidential information leakages

is growing year-by-year. The practical value of this research consists in the possibility of using the criminalistic descriptions of such crimes to form specific forensic investigative methodologies, to create new criminalistic records of digital proof, to develop special software that supports making decisions when generating investigative leads, as well as to build an information model (a digital twin) of a crime. The research is based on an aggregate of general methods of scientific cognition (description, generalization and comparison), general scientific (analysis, synthesis, modeling and classification) and specific scientific methods (statistical, cybernetic).

Keywords: computer crimes, personal data, illegal data collection, criminalistic characteristics of crimes, digital model of crime, digital twins, artificial intelligence.

For citation: Kharisova Z.I. Criminalistic Characteristics of the Illegal Use, Transfer, Collection and Storage of Computer Information Containing Personal Data. *Sibirskie Ugolovno-Processual'nye i Kriminalisticheskie Chteniya = Siberian Criminal Procedure and Criminalistic Readings,* 2025, no 2, pp. 96–108. (In Russian). EDN: NQGBRY. DOI: 10.17150/2411-6122.2025.2.96-108.

Введение

Дополнение Уголовного кодекса Российской Федерации (далее — УК РФ) статьей 272.11, устанавливающей ответственность за незаконные использование, хранение, передачу и сбор информации, содержащей персональные данные (далее — ПДн), а также создание и обеспечение функционирования информационных ресурсов, предназначенных для ее незаконных хранения и распространения, обусловлено тем, что совершенствование технологий и современные потребности общества, подвергшегося цифровизации, делают необходимой автоматизированную обработку значительных по объему массивов личных данных граждан. Формируемые государственными органами и коммерческими организациями базы с указанными сведениями становятся специфическим предметом преступных посягательств, что подтверждает сложившаяся международная ситуация, отчасти связанная с деятельностью транснациональных организованных преступных групп, нацеленных на хищение ПДн, их неправомерное использование и распространение.

Введение новой статьи в главу 28 УК РФ в первую очередь связано с существенным ростом противоправных действий в отношении ПДн[2], фактами незаконного использования конфиденциальной информации при совершении преступлений в сфере компьютерной информации, а также тем, что наказание, предусмотренное законом за такого рода преступления, было несопоставимо их потенциальным общественно опасным последствиям. Так, только из финансовых организаций за 2024 г. объем утечек ПДн составил 410 млн строк, что более чем в 2,5 раза больше объема утечек, выявленных в 2023 г.[3] Указанные сведения преимущественно содержали информацию об учетных данных клиентов, их адресах, контактных номерах, электронных адресах, кредитной истории и т.п., что использовалось для дальнейшего совершения различного

[1] О внесении изменений в Уголовный кодекс Российской Федерации : Федер. закон от 30 нояб. 2024 г. № 421-ФЗ // СПС «КонсультантПлюс». (дата обращения: 28.03.2025).

[2] Комплексный анализ состояния преступности в Российской Федерации и ожидаемые тенденции ее развития : аналитический обзор. М., 2025. С. 56.

[3] Кибератаки на финансовый сектор в 2024 году : аналит. отчет // Солар секьюрити : офиц. сайт. URL: https://rt-solar.ru/analytics/reports/5206. (дата обращения: 28.03.2025).

 DOI 10.17150/2411-6122.2025.2.96-108 ISSN 2411-6122

рода преступлений и мошенничеств. Поскольку рост противоправных деяний в отношении ПДн является значимым фактором самовоспроизводства киберпреступлений целесообразно рассмотрение возможностей оптимизации процесса расследования преступлений, связанных с незаконным использованием, передачей, сбором и хранением компьютерной информации, содержащей ПДн, в частности, изучение элементов, входящих в их криминалистическую характеристику.

Теоретическое обоснование

Общая криминалистическая характеристика преступлений представляет собой абстрактное описание элементов, связей и закономерностей, присущих всем видам преступлений. Отдельные виды (разновидности или группы) преступлений описываются на базе общей характеристики и в дополнение конкретизируются общими методиками расследования, техническими средствами, тактическими и методическими рекомендациями, облегчая планирование работы и описание конкретной разновидности преступного деяния. Подавляющее большинство определений криминалистической характеристики преступлений представляют ее как функциональную систему, в общем виде – систему данных, способствующих раскрытию и расследованию преступлений [1, с. 133].

Преступления в сфере компьютерной информации, к которым относятся преступные деяния, связанные с незаконными использованием, хранением, передачей и сбором информации, содержащей ПДн, имеют общую родовую криминалистическую характеристику [2, с. 585], которая включает в себя сведения о способах преступлений, лицах, совершивших их, сведения о потерпевшей стороне и обстоятельствах, способствующих и препятствующих данным преступлениям. Между тем лишь перечисление элементов такой системы не может в полной мере определять ее сути, требующей выявления взаимосвязей между ее составляющими. По этой причине необходимо выявить элементы видовой криминалистической характеристики рассматриваемых преступлений с точки зрения системно-структурного, а также кибернетического подходов. Стоит отметить, что эффект внедрения информационных технологий в криминалистическую деятельность не может быть обеспечен только формулированием теоретических положений и научными дискуссиями в отсутствие массовых и значимых результатов прикладных исследований в этой сфере [3, с. 25]. Результаты проводимого анализа, в противовес, смогут послужить основой для формирования информационной модели [4, с. 18] (цифрового двойника) преступления на основе наиболее значимых элементов их криминалистической характеристики.

Под ПДн подразумевается любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту ПДн)[4]. К указанным данным, например, могут относиться: фамилия, имя и отчество субъекта ПДн (физического лица); дата и место его рождения; реквизиты документов; контактный телефон и адрес электронной почты (в связке с определяемым субъектом); семейное и социальное положение; образование; профессия; сведения о доходах и пр. информация. Любое действие (операция) или совокупность действий, со-

[4] О персональных данных : Федер. закон № 152-ФЗ от 27 июля 2006 г. // СПС «КонсультантПлюс». (дата обращения: 28.03.2025).

вершаемых с использованием средств автоматизации или без использования таких средств с ПДн, определяется как обработка ПДн[5]. Под специальными ПДн понимают данные, касающиеся расовой и национальной принадлежности, политических, религиозных либо философских убеждений, состояния здоровья субъекта ПДн, его интимной жизни, а также данные о судимости [5, с. 58]. Биометрическими ПДн являются сведения, характеризующие физиологические и биологические особенности человека, на основании которых можно установить его личность. В соответствии с ч. 2 ст. 272.1 УК РФ за совершение неправомерных действий в отношении специальных и биометрических ПДн предусмотрена повышенная уголовная ответственность. Под трансграничным перемещением носителей информации в указанной статье понимается совершение действий по ввозу на территорию РФ и (или) вывозу с ее территории электронного носителя информации, на который осуществлены запись и хранение такой информации, под трансграничной передачей компьютерной информации понимают передача ПДн на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу [6 с. 35]. Под использованием служебного положения, предусмотренного в диспозиции ч. 3 ст. 272.1 УК РФ, понимается возможность неправомерного доступа к ПДн, возникшего в результате выполняемой работы (по трудовому, гражданско-правовому договору и пр.) или влияния по службе на лиц, имеющих такой доступ (в данном случае субъектом преступления не обязательно является должностное лицо), то есть тех, кто на законных основаниях использует ПДн и средства их обращения.

Создание информационного ресурса представляет собой деятельность, направленную на разработку веб-сервиса, либо информационной системы, заведомо предназначенных для незаконного хранения и передачи компьютерной информации, содержащей ПДн, полученных незаконным путем. Лицо может быть подвергнуто уголовному преследованию за вышеуказанные действия только при условии, что оно достоверно знало об их направленности в плане функционирования ресурса или системы. Действие настоящей статьи не распространяется на случаи обработки ПДн лицами исключительно для личных и семейных нужд.

Выявление незаконного способа завладения ПДн в электронном виде и незаконных действий, связанных с их распространением, является ключевым условием наступления ответственности, предусмотренной ст. 272.1 УК РФ.

Ввиду того, что судебная практика по ст. 272.1 УК РФ на сегодняшний день лишь начинает формироваться, был проведен анализ смежных по составу уголовных дел, затрагиваемых преступные деяния, связанные с незаконным использованием, хранением, передачей и сбором информации, содержащей ПДн, в частности, в соответствии со ст. 137 УК РФ «Нарушение неприкосновенности частной жизни», который позволил выделить соответствующие текущему состоянию схожего вида преступности элементы криминалистической характеристики. На основе проведенного исследования криминалистическую характеристику преступлений, связанных с незаконным использованием, хранением, передачей и сбором информации, содержащей

[5] Научно-практический постатейный комментарий к Федеральному закону «О персональных данных». М. : Статут. 2017. С. 11.

 DOI 10.17150/2411-6122.2025.2.96-108 ISSN 2411-6122

ПДн, предлагается изложить в следующем виде:

– способ совершения преступления (с описанием типичных следов преступления, способов их сокрытия, вероятных мест их нахождения и распространенности (серийности) преступного деяния);

– обстановка (место (среда), время совершения) преступления;

– личность преступника;

– личность потерпевшего и / или предмет посягательства.

Включение в элемент «способ совершения преступления» такого дополнения как «распространенность (серийность) преступного деяния» применительно к преступлениям в сфере компьютерной информации предполагается целесообразным, поскольку подтверждается на практике необходимостью проверки схожести (серийности) эпизода с ранее выявленными преступными деяниями и обязательным включением сведений о способе и иных обстоятельствах совершения преступления в подсистемы программно-технического комплекса интегрированного банка данных федерального уровня ГИАЦ МВД России.

Кроме того, серийность преступного деяния является одним из обязательных реквизитов[6] для указания в статистической карточке преступления, содержание которого может выступить основой для формирования нового криминалистического учета цифровых доказательств, что сонаправлено с одной из основных задач государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий[7].

Способ совершения преступления

Среди основных преднамеренных способов незаконного использования и (или) передачи, сбора и (или) хранения ПДн, создания и (или) обеспечения функционирования ресурсов, предназначенных для их незаконного хранения и (или) распространения можно отметить: преодоление систем защиты в виде хищения учетных данных пользователей с целью получения ПДн; использование несовершенств информационных систем персональных данных (далее — ИСПДн); использования уязвимостей программного обеспечения и операционных систем, эксплуатирующих ИСПДн; несанкционированное подключение к техническим средствам, а также вспомогательному компьютерному оборудованию, эксплуатирующего ИСПДн; сбор и дальнейшее распространение данных, в связи с утечками ПДн; приобретение баз данных, содержащих ПДн; неправомерный доступ к средствам обработки ПДн, их хранения или иного вмешательства в их функционирование (в том числе в отношении ПДн несовершеннолетних лиц и биометрических ПДн); организация и обеспечение функционирования программного обеспечения, веб-ресурсов и систем, предназначенных для незаконной обработки ПДн (распростране-

[6] О едином учете преступлений : Приказ Генпрокуратуры России № 39, МВД России № 1070, МЧС России № 1021, Минюста России № 253, ФСБ России № 780, Минэкономразвития России № 353, ФСКН России № 399 от 29 дек. 2005 г. // СПС «КонсультантПлюс». (дата обращения: 28.03.2025).

[7] О создании государственных информационных систем по противодействию правонарушениям (преступлениям), совершаемым с использованием информационно-телекоммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации : Федер. закон от 25 марта 2025 г. № 41-ФЗ // СПС «КонсультантПлюс». (дата обращения: 28.03.2025).

ния, предоставления, доступа); фишинг [7, с. 703] (создание поддельных (фишинговых) ресурсов, документов или сообщений для несанкционированного сбора ПДн); веб-скрейпинг (от англ. «web scraping» — автоматизированный сбор данных с веб-ресурсов или социальных сетей); взлом и незаконный сбор ПДн, размещенных в облачных системах хранения данных; доксинг (от англ. «doxing» и сокращения «docs» — сбор и распространение личной информации о человеке без его согласия); трансграничное перемещение носителей информации (ввоз на территорию РФ или вывоз за пределы страны) носителей, на которые осуществлена запись и хранение ПДн); незаконная передача защищаемых ПДн на территорию иностранного государства.

Процессы, возникшие в ходе случайных действий либо стечения обстоятельств, относят к непреднамеренным. К неумышленным способам незаконного использования, передачи, сбора и хранения персональных данных, а также создания и обеспечения функционирования ресурсов для их незаконного распространения можно отнести незащищенную передачу данных (например, через незащищенные каналы связи без шифрования или несертифицированное программное обеспечение); использование общедоступных облачных хранилищ ПДн; ошибки администрировании ИСПДн (неправильная настройка доступа без разграничения ролей и пр.); потеря или кража технических средств (например, ноутбука или электронного носителя информации с ПДн); использование веб-аналитики и трекеров действий пользователей веб-ресурсов без их согласия.

Анализ смежных по составу уголовных дел, например, в соответствии со ст. 137 УК РФ «Нарушение неприкосновенности частной жизни», позволил выявить основные средства совершения подобных преступлений. Так, при непосредственном доступе ими могут выступать носители информации, эксплуатируемые с техническими средствами, а при опосредованном доступе — сетевое оборудование и средства доступа к ИСПДн (средства вычислительной техники, мобильные средства связи и пр.). К основным средствам также относится: программное обеспечение (например, VPN-сервисы, обеспечивающие шифрование трафика и сокрытие реального IP-адреса преступника, системы прокси-серверов и пр.), в том числе криптографическое и вредоносное, способное к распространению в локальных информационных системах и служащих в целях выполнения какого-либо деструктивного действия (удаление, блокирование или изменение файлов) или несанкционированного копирования данных; программное обеспечение для веб-парсинга в виде настраиваемых скриптов для кражи данных из социальных сетей и т.п. ресурсов и скрытого наблюдения, сбора ПДн с персональных компьютеров и мобильных устройств, способного перехватывать совокупность действий пользователей (нажатия клавиш, записей звонков и сбора конфиденциальных данных); сетевые снифферы (анализатор сетевого трафика, содержащего ПДн); поисковые системы, позволяющие находить подключенные к сети устройства и сервисы; теневые маркетплейсы для распространения ПДн и пр.

К средствам хранения компьютерной информации в виде ПДн относятся ее материальные носители (жесткие и оптические диски, USB-накопители, карты памяти и т.п.), средствами обработки ПДн в целом служит вычис-

 DOI 10.17150/2411-6122.2025.2.96-108 ISSN 2411-6122

лительное устройство (процессор) персонального компьютера. Каналы передачи информации могут быть проводными и беспроводными.

Основными способами сокрытия следов незаконного использования и (или) передачи, сбора и (или) хранения ПДн, создания и (или) обеспечения функционирования ресурсов, предназначенных для их незаконного хранения и (или) распространения, являются: использование средств анонимизации и систем прокси-серверов, которые позволяют устанавливать анонимные сетевые соединения с туннелированием; очищение журналов и шифрование событий в системе; удаление сведений о подключениях к персональному компьютеру или ИСПДн; использование чужих, временных или и одноразовых учетных записей для доступа к ПДн и ИСПДн, а также программных средств анонимизации в целях подмены IP-адресов устройств и абонентских номеров, размещение ресурсов ПДн для их последующего распространения в неиндексируемой глубокой сети (от англ. «deep web» — «глубокий «Интернет») и даркнете (от англ. «dark web» — темный «Интернет»); корректировка даты и времени доступа к ПДн для дальнейшего незаконного их распространения и пр.

Типичными следами неправомерного доступа к компьютерной информации в общем случае являются: цифровые (установленное программное обеспечение, используемое для незаконной обработки или хранения ПДн, изменения в конфигурации операционной системы устройства, журналы подключений к персональному компьютеру или ИСПДн, модифицированные или блокированные файлы данных и т.п.), а также материальные следы на компьютерной периферии.

Основными следообразующими и следовоспринимающими объектами по рассматриваемому преступлению могут выступать: системное и прикладное программное обеспечение, поименованные области записей на носителях информации; серверное оборудование с размещаемыми на нем ресурсами ИСПДн; электронные файлы; персональные компьютеры, информационные системы, мобильные средства связи; базы данных; электронные ключи (подписи); файлы подкачки и временные файлы; сетевой трафик; идентификаторы в сети передачи данных (например, IP-адреса устройств или MAC-адреса их сетевых карт), DNS-адреса; реестры операционных систем [8, с. 10] и журналы событий ИСПДн; цифровые финансовые активы и электронные кошельки; используемые при приобретении баз данных с ПДн и пр.

Отдельно стоит отметить ресурсы, предназначенные для поиска ПДн по открытым источникам (OSINT-разведка (от англ. «open source intelligence — «разведка по открытым источникам»)) в индексируемой сети «Интернет», неиндексируемой глубокой сети и даркнете, а также по ресурсам Telegram-ботов [9, с. 98] (аккаунтам в кроссплатформенном мессенджере Telegram, которые программируются на автоматическое совершение действий, например, связанных с незаконным сбором и обработкой ПДн). Кроме того, развитие метавселенных порождает такие виды преступных деяний, как подмена личных данных, кража цифровых идентификаторов личности и т.п. По вышеуказанным преступным деяниям следовоспринимающими и следообразующими объектами будут являться, например, сфальсифицированные биометрические данные, метаданные и конфигурации, хранящиеся

на серверах, связанных с эксплуатацией метапространства (журналы функционирования программного обеспечения, обеспечивающего визуализацию трехмерных виртуальных пространств и аутентификацию по биометрическим данным, реестры эксплуатации децентрализованных сетей, конфигурации с настройками протоколов передачи данных, адреса взаимодействия цифровых аватаров и пр.).

Вероятными местами расположения типичных следов незаконной обработки, хранения или распространения ПДн в цифровом виде являются носители информации, серверное оборудование и облачные хранилища, в том числе файлы и каталоги хранения данных, файлы конфигурации программ удаленного доступа и пр.

Распространенность преступного деяния выражается в установлении факта схожести эпизода на основе полученных сведений об использовании в преступной схеме способа совершения преступления. Так, например, идентифицирующими признаками схожести могут выступить идентичные реквизиты в виде: любых идентифицирующих конкретного гражданина ПДн, в том числе биометрических; абонентских номеров; программного обеспечения и технических средств, используемых для совершения атак на ИСПДн или компьютеры, обрабатывающие ПДн; банковских реквизитов и т.п. Так же необходимо отметить массовость утечек данных, при которых число пострадавших лиц могут измеряться миллионами записей.

Обстановка совершения преступления

Незаконные использование и (или) передача, сбор и (или) хранение ПДн, создание и (или) обеспечение функционирования ресурсов, предназначенных для их незаконного хранения и (или) распространения предполагает как непосредственный доступ к ПДн (преимущественно в момент отсутствия обладателя защищаемой информации), так и удаленный с любой точки мира (при наличии подключения к сети «Интернет» или к локальной сети предприятия), которые определяются спецификой работы с ПДн в электронном виде и предполагают использование программно-аппаратных средств для ее обработки, хранения и передачи

Местами совершения указанного преступления являются: компьютеры, сервера или ИСПДн (зачастую значительно удаленные друг от друга), так и локальные территории, учреждения и организации, в которых эксплуатируется ИСПДн; социальные сети и мессенджеры; фишинговые сайты; теневые торговые площадки и форумы, где продаются базы данных, содержащие ПДн; IoT-устройства [10, с. 4380] (от англ. «internet of things (IoT)» — интернет вещей) и сервера-хранилища видеоданных; незащищенные беспроводные сети. В целях сокрытия физического расположения преступника удаленный доступ нередко осуществляется из общественных мест, предоставляющим сеть «Интернет» в порядке пользования услугами на базе организации. В подавляющем большинстве случаев местом (средой) совершения рассматриваемого преступления является киберпространство ввиду его распространенности среди населения, реже – метапространство, блокчейн (распределенные реестры), либо гибридные инфраструктуры (распределенные облачные системы хранения данных и пр.)

Согласно ч. 2 ст. 9 УК РФ временем совершения преступления признается время окончания преступного

 DOI 10.17150/2411-6122.2025.2.96-108 ISSN 2411-6122

деяния вне зависимости от момента наступления последствий. Время доступа к компьютеру, программе или ИСПДн, хранящим ПДн может быть изменено преступником в целях искажения типичных следов.

Обстановка совершения преступления играет довольно важную роль. Так, например, при получении сообщения (заявления) о преступлении в ходе устного опроса заявителя необходимо выяснить все обстоятельства, имеющие значение, а именно, дату, время и способ совершения преступления, установочные данные лица, от которого поступило сообщение (заявление) и пр., после чего возможна организация первоначальных проверочных мероприятий.

Личность преступника

Как правило лицо, осуществляющее незаконные использование и (или) передачу, сбор и (или) хранение ПДн, создание и (или) обеспечение функционирования ресурсов, предназначенных для их незаконного хранения и (или) распространения, обладает глубокими знаниями в области информационных технологий, включая сетевую безопасность, методы обхода систем защиты ИСПДн. Указанные лица стабильно отслеживают методы защиты данных, мониторят уязвимости программного обеспечения, адаптируя имеющиеся знания к новым условиям функционирования программного обеспечения, конкретным жертвам, часто пренебрегают правовыми и этическими нормами, не учитывая последствия своих действий для пострадавших и общества в целом. Многие из них обладают навыками социальной инженерии, позволяющими обманом получать доступ к конфиденциальной информации от пользователей или сотрудников организаций.

Отличительной особенностью является то, что они не проявляют сочувствия к жертвам преступлений, рассматривая их лишь как средства достижения собственных целей, как правило, имеют высшее или среднее инженерно-техническое образование, обладает устойчивыми преступными навыками. Совершаемые ими преступления часто носят серийный характер и сопровождаются тщательными действиями по сокрытию следов преступной деятельности. Отдельной категорией являются лица, имеющие доступ к ПДн граждан в связи с исполнением ими служебных обязанностей по месту работы, которые оказывают услуги информирования иных лиц.

Анализ следственной практики также показывает, что преступники часто используют информацию из открытых источников. Основными мотивами совершения указанного преступления могут выступить корыстные побуждения в виде получения материальной выгоды, получаемой посредством продажи полученных ПДн, вымогательство или мошенничество, а также личная неприязнь к собственнику информации, шпионаж (например, получение сведений, связанной с личной жизнью) и пр.

Личность потерпевшего и / или предмет посягательства

Предметом рассматриваемого преступления является компьютерная информация, содержащая ПДн, полученная незаконным путем, включая неправомерный доступ к средствам обработки или хранения данных, вмешательство в функционирование таких средств и прочие незаконные способы. ПДн в данном контексте включают любую информацию, относящуюся к определенному или определяемому физическому лицу. Особо выделяют-

ся при этом ПДн несовершеннолетних лиц, специальные категории ПДн (сведения о расовой или этнической принадлежности, политических взглядах, состоянии здоровья, интимной жизни и пр.) и биометрические ПДн.

Личность потерпевшего можно связать с субъектом ПДн или организацией, в которой функционирует ИСПДн, в отношении которых осуществлены незаконные использование и (или) передача, сбор и (или) хранение ПДн, создание и (или) обеспечение функционирования ресурсов, предназначенных для их незаконного хранения и (или) распространения. Потерпевших по данным преступлениям можно также разделить на категории в принадлежности к физическим или юридическим лицам, а также к государственным структурам.

Исходя из анализа сложившейся за последние несколько лет следственной и судебной практики, связанной со сбором, хранением, использованием и распространением информации о частной жизни лица без его согласия, необходимо отметить отличительные особенности личности потерпевшего по рассматриваемому виду преступления. Потерпевшим, как правило, является физическое лицо, конкретный гражданин, чьи ПДн были собраны или распространены без его согласия, это могут быть, например, клиенты банков, пациенты медицинских учреждений, работники организаций, а также публичные лица, чьи данные представляют интерес для злоумышленников. Довольно часто потерпевший сам предоставляет свои ПДн на фишинговых ресурсах, что объясняется отсутствием знаний в области защиты собственных ПДн.

Таким образом, частым признаком, выявляемым в ходе следствия, является пассивная роль потерпевшего при совершении преступления, так, потерпевший часто не подозревает о незаконном сборе ПДн до момента их использования. Ключевым признаком также является то, что субъект ПДн не давал согласия на обработку его ПДн, однако в результате преступного деяния ему причинен материальный или репутационный ущерб.

Характерной особенностью потерпевшей стороны является их бездействие или неохотное желание сообщать о факте преступного деяния в правоохранительные органы. Кроме того, потерпевшие зачастую не могут предоставить минимально необходимые данные и электронные доказательства для создания картины расследования. Юридические лица часто не желают сообщать в правоохранительные органы об утечках данных из эксплуатируемых ими ИСПДн в связи с действующей репутационной политикой.

Судебная практика по незаконному использованию и (или) передаче, сбору и (или) хранению ПДн, созданию и (или) обеспечению функционирования ресурсов, предназначенных для их незаконного хранения и (или) распространения (ст. 272.1 УК РФ) на текущий момент представлена недостаточно, однако, имеется практика по сбору, хранению, использованию и распространению информации о частной жизни лица без его согласия в соответствии со ст. 137 УК РФ (нарушение неприкосновенности частной жизни), которая показывает, что потерпевшими по такого рода преступлениям могут быть лица любого возраста, профессии и социального статуса. Общей чертой является нарушение их права на неприкосновенность частной жизни и незаконное использование их ПДн без согласия.

Результаты исследования

Алгоритмизация в целом позволяет повысить профессиональную компе-

тентность субъектов раскрытия и расследования преступлений, повысить показатели антикриминальной деятельности в российском государстве, а также дополнить и внести вклад во все фундаментальные направления криминалистической науки [11, с. 640]. Поэтому можно сделать вывод, что криминалистическая характеристика преступлений, совершаемых в сфере компьютерной информации в целом, фактически представляет собой информационно-теоретическую базу для создания типовых алгоритмов их расследования и программного обеспечения в виде систем поддержки принятия решений. Изложенное позволяет сделать вывод о возможности формирования на их основе цифрового двойника преступления в виде его цифровой копии, позволяющей оптимизировать эффективность расследования. В качестве исходных дополнительных данных для построения такого рода информационно-компьютерной модели, как объекта познания [12, с. 72], могут быть отобраны условные признаки, которые в наибольшей степени влияют на прогноз раскрываемости (взятые, например, из статистических карт по преступлениям прошлых лет), и, по сути своей, выступают значимыми элементами криминалистической характеристики преступления.

Список использованной литературы

1. Ищенко Е.П. Типовая информационная модель преступления как основа методики расследования / Е.П. Ищенко, В.Я. Колдин. — EDN MUYINR // Известия высших учебных заведений. Правоведение. — 2006. — № 6 (269). — С. 128–144.

2. Россинская Е.Р. Избранное / Е.Р. Россинская. — Москва : Норма, 2021. — 680 с.

3. Головин А.Ю. Технологии искусственного интеллекта в криминалистике: задачи, которые необходимо решить / А.Ю. Головин. — DOI 10.17150/2411-6122.2024.2.25-33. — EDN WBXROE // Сибирские уголовно-процессуальные и криминалистические чтения. — 2024. — № 2. — С. 25–33.

4. Волчецкая Т.С. Криминалистическая ситуалогия / Т.С. Волчецкая. — Москва, 1997. — 248 с.

5. Аверченков В.И. Защита персональных данных в организации / В.И. Аверченков, М.Ю. Рытов. — Москва : ФЛИНТА, 2021. — 124 с.

6. Дупан А.С. Новая парадигма защиты и управления персональными данными в Российской Федерации и зарубежных странах в условиях развития систем обработки данных в сети Интернет / А.С. Дупан. — Москва : Высш. шк. экономики, 2018. — 343 с.

7. Россинская Е.Р. Концепция вредоносных программ как способов совершения компьютерных преступлений: классификации и технологии противоправного использования / Е.Р. Россинская, И.А. Рядовский. — EDN HNMPIX. — DOI 10.17150/2500-4255.2020.14(5).699-709 // Всероссийский криминологический журнал. — 2020. — Т. 14, № 5. — С. 699–709.

8. Белей А.В. Журналы регистрации WEB-серверов и прокси-серверов, сетевого трафика беспроводных сетей (высокопроизводительных сетей, SSL/TLS-трафика) как объекты судебных компьютерно-технических исследований и экспертиз / А.В. Белей, О.П. Калинкова. — EDN AIVWQD // Юрист спешит на помощь. — 2024. — № 3. — С. 10–13.

9. Себякин А.Г. Данные, находящиеся в открытых источниках информации, как объект судебной информационно-аналитической экспертизы / А.Г. Себякин. — DOI 10.17150/2411-6122.2024.2.95-103. — EDN JTTXQP // Сибирские уголовно-процессуальные и криминалистические чтения. — 2024. — № 2. — С. 95–103.

10. Ryu J. A Blockchain-Based Decentralized Efficient Investigation Framework for IoT Digital Forensics / J. Ryu, P. Sharma, J. Jo. — DOI 10.1007/s11227-019-02779-9 // The Journal of Supercomputing. — 2019. — Vol. 75, no. 8. — P. 4372–4387.

11. Варданян А. В. Дискредитация субъектов раскрытия и расследования преступлений и криминалистические методы ее нейтрализации / А.В. Варданян, И.А. Макаренко. — DOI 10.17150/2500-4255.2022.16(5).638-645. — EDN LXWUHY // Всероссийский криминологический журнал. — 2022. — Т. 16, № 5. — С. 638–645.

12. Макаренко И.А. Современное состояние и проблемы развития понятийного аппарата учения о предмете криминалистики / И.А. Макаренко, А.А. Эксархопуло. — DOI 10.17150/2411-6122.2024.4.64-74. — EDN HZLFJQ // Сибирские уголовно-процессуальные и криминалистические чтения. — 2024. — № 4. — С. 64–74.

References

1. Ishchenko E.P., Koldin V.Ya. Typical Information Model of Crime as the Basis of Investigation Methods. *Izvestiya vysshikh uchebnykh zavedenii. Pravovedenie = Proceedings of Higher Education Institutions. Pravovedenie,* 2006, no. 6, pp. 128–144. (In Russian). EDN: MUYINR.

2. Rossinskaya E. R. *Favorites*. Moscow, Norma Publ., 2021. 680 p.

3. Golovin A.Yu. Artificial Intelligence Technologies in Criminalistics: Tasks to be Solved. *Sibirskie ugolovno-protsessual'nye i kriminalisticheskie chteniya = Siberian Criminal Procedure and Criminalistic Readings*, 2024, no. 2, pp. 25–33. (In Russian). EDN: WBXROE. DOI: 10.17150/2411-6122.2024.2.25-33.

4. Volchetskaya T.S. *Criminalistic Situational Analysis.* Moscow, 1997. 248 p.

5. Averchenkov V.I., Rytov M.Yu. *Protection of Personal Data in an Organization.* Moscow, FLINTA Publ., 2021, 124 p.

6. Dupan A.S. *New Paradigm of Protecting and Managing Personal Data in the Russian Federation and Foreign Countries in the Conditions of Developing Data Processing Systems on the Internet.* Moscow, HSE Publishing House Publ., 2018. 343 p.

7. Rossinskaya E.R., Ryadovskiy I.A. The Concept of Malware as a Means of Committing Computer Crimes: Classification and Methods of Illegal Use. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2020, vol. 14, no. 5, pp. 699–709. (In Russian). EDN: HNMPIX. DOI: 10.17150/2500-4255.2020.14(5).699-709.

8. Belei A.V., Kalinkova O.P. Journals of Registering WEB-servers and Proxy-servers, Network Traffic of Wireless Networks (High-capacity Networks, SSL/TLS-traffic) as Objects of Forensic Computer-technical Research and Examination. *Yurist speshit na pomoshch = A Lawyer is Rushing to Help*, 2024, no. 3, pp. 10–13. (In Russian). EDN: AIVWQD.

9. Sebyakin A.G. Data from Open Sources as Objects of Information-Analytical Forensic Examination. *Sibirskie ugolovno-protsessual'nye i kriminalisticheskie chteniya = Siberian Criminal Procedure and Criminalistic Readings*, 2024, no. 2, pp. 95–103. (In Russian). EDN: JTTXQP. DOI: 10.17150/2411-6122.2024.2.95-103.

10. Ryu J., Sharma P., Jo J. A Blockchain-Based Decentralized Efficient Investigation Framework for IoT Digital Forensics. *The Journal of Supercomputing,* 2019, vol. 75, no. 8, pp. 4372–4387. DOI: 10.1007/s11227-019-02779-9.

11. Vardanyan A.V., Makarenko I.A. Discrediting the Subjects of Crime Disclosure and Investigation and the Criminalistic Methods of Neutralizing It. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2022, vol. 16, no. 5, pp. 638–645. (In Russian). EDN: LXWUHY. DOI: 10.17150/2500-4255.2022.16(5).638-645.

12. Makarenko I.A., Exarkhopulo A.A. The Current State and Problems of Developing the Conceptual Apparatus in the Theory of the Subject of Criminalistics. *Sibirskie ugolovno-protsessual'nye i kriminalisticheskie chteniya = Siberian Criminal Procedure and Criminalistic Readings*, 2024, no. 4, pp. 64–74. (In Russian). EDN: HZLFJQ. DOI: 10.17150/2411-6122.2024.4.64-74.

Информация об авторе

Харисова Зарина Ирековна — кандидат технических наук, доцент, старший преподаватель кафедры криминалистики, Институт права, Уфимский университет науки и технологий, г. Уфа, Российская Федерация, https://orcid.org/0000-0002-3902-3459, SPIN-код: 8293-1823, AuthorID РИНЦ: 819031.

 DOI 10.17150/2411-6122.2025.2.96-108 ISSN 2411-6122

Author Information

Kharisova, Zarina I. — Ph.D. in Technical Sciences, Ass. Professor, Senior Lecturer, Department of Criminalistics, Institute of Law, Ufa University of Science and Technology, Ufa, the Russian Federation, https://orcid.org/0000-0002-3902-3459, SPIN-Code: 8293-1823, AuthorID RSCI: 819031.

Поступила в редакцию / Received 01.05.2025
Одобрена после рецензирования / Approved after reviewing 13.05.2025
Принята к публикации / Accepted 21.05.2025
Дата онлайн-размещения / Available online 26.06.2025