Вестник Восточно-Сибирского института МВД России. 2024 № 2 (109). С. 254–264.
Vestnik of the East Siberian Institute of the Ministry of Internal Affairs of Russia. 2024 Vol. no. 2 (109). P. 254–264.

5.1.4. Уголовно-правовые науки (юридические науки)

Научная статья
УДК 343.9
DOI: 10.55001/2312-3184.2024.26.72.022

УГОЛОВНО-ПРАВОВАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С РАЗГЛАШЕНИЕМ СВЕДЕНИЙ О ГРАЖДАНАХ

Родивилин Иван Петрович[1], Коломинов Вячеслав Валентинович[2]
[1]Иркутский национальный исследовательский технический университет, Россия, Иркутск
[2] Байкальский государственный университет, Россия, Иркутск
[1] 377a@bk.ru
[2] offroad88@mail.ru

Введение. В настоящее время наблюдается тенденция в развитии информационного общества, заключающая в растущем интересе к индивидуализированной информации, особенно к персональным данным. Этот интерес обусловлен автоматизацией обработки информации и развитием центров обработки данных, которые генерируют огромные объемы информации, известные как «большие данные», которые в свою очередь подвержены кибератакам и в результате чего, произошел очередной всплеск незаконного собирания и распространения сведений о частной жизни лица, в том числе персональных данные и их свободное распространение в сети Интернет, с использованием ботов «пробивщиков». Рост преступлений, связанных с незаконным собиранием и распространением сведений о частной жизни лица, в том числе персональных данных, позволил автору провести анализ сложившейся практики и предложить свой алгоритм квалификации подобного рода деяний.

Материалы и методы. Нормативную основу исследования образуют Уголовный кодекс Российской Федерации, Гражданский кодекс Российской Федерации, постановление Пленума Верховного Суда Российской Федерации «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «интернет» № 37 от 15 декабря 2022 г., Стратегия национальной безопасности Российской Федерации. Сформулированные выводы основываются на представленных статистических сведениях и материалах уголовных дел. Исследование проведено с использованием сравнительно-правового метода, а также межотраслевого исследования, обобщения и описания.

Результаты исследования. В ходе проведенного исследования авторам удалось установить основные детерминанты преступлений в указанной сфере. На основе проведенного исследования раскрыты некоторые вопросы квалификации незаконного получения и разглашения персональных данных.

Выводы и заключения. Вопрос обеспечения охраны и защиты персональных данных остается в Российской Федерации актуальным и требует внимания со стороны законодателей и правоохранительных органов. В ходе проведенного исследования разработаны механизмы применения уголовного законодательства в данной сфере и решены проблемы квалификации указанных деяний.

Ключевые слова: преступления в сфере компьютерной информации, уголовно-правовая охрана персональных данных, неприкосновенность частной жизни, персональные данные, компьютерная информация, боты-пробивщики

Для цитирования: Родивилин И. П., Коломинов В. В. Уголовно-правовая характеристика преступлений, связанных с разглашением сведений о гражданах / И. П. Родивилин, В. В. Коломинов // Вестник Восточно-Сибирского института МВД России : науч.-практ. журн. Иркутск: Восточно-Сибирский институт МВД России. 2024. № 2 (109). С. 254–264.

DOI: 10.55001/2312-3184.2024.26.72.022

5.1.4. Criminal Law Sciences

Original article

CRIMINAL-LEGAL CHARACTERIZATION OF CRIMES RELATED TO DISCLOSURE OF CITIZENS' INFORMATION

Ivan P. Rodivilin[1], Vyacheslav V. Kolominov[2]
[1]Irkutsk National Research Technical University, Irkutsk, Russian Federation
[2] Baikal State University, Irkutsk, Russian Federation
[1] 377a@bk.ru
[2] offroad88@mail.ru

Introduction. The current trend in the development of the information society is the growing interest in personalised information, especially personal data. This interest is due to the automation of information processing and the development of data processing centres, which generate huge amounts of information, known as "big data", which in turn are susceptible to cyber-attacks and as a result, there has been another upsurge in the illegal collection and dissemination of information about the private life of an individual, including personal data and their free dissemination on the Internet, using "piercing" bots. The growth of crimes related to the illegal collection and dissemination of information about the private life of a person, including personal data, allowed the author to analyse the current practice and to propose his algorithm for the qualification of such acts.

Materials and Methods. The normative basis of the study is formed by the Criminal Code of the Russian Federation, the Civil Code of the Russian Federation, the Resolution of the Plenum of the Supreme Court of the Russian Federation "On some issues of judicial

practice in criminal cases of crimes in the sphere of computer information, as well as other crimes committed with the use of electronic or information and telecommunications networks, including the Internet" No. 37 of 15 December 2022, the National Security Strategy of the Russian Federation. The formulated conclusions are based on the provided statistical data and materials of criminal cases. The study was conducted using the comparative legal method, as well as cross-sectoral research, generalisation and description.

The Results of the Study. In the course of the study the authors managed to establish the main determinants of offences in this area. On the basis of the conducted research some issues of qualification of unlawful obtaining and disclosure of personal data are disclosed.

Findings and Conclusions. The issue of ensuring the protection and defence of personal data remains topical in the Russian Federation and requires the attention of legislators and law enforcement agencies. In the course of the conducted research the mechanisms of application of criminal legislation in this area were developed and the problems of qualification of these acts were solved.

Keywords: computer-related offences, criminal law protection of personal data, privacy, personal data, computer information, punching bots

For citation: Rodidilin I.P., Kolominov V.V. Ugolovno-pravovaja harakteristika prestuplenij, svjazannyh s razglasheniem svedenij o grazhdanah [Criminal-legal characterization of crimes related to disclosure of citizens' information]. Vestnik Vostochno-Sibirskogo instituta MVD Rossii - Vestnik of the East Siberian Institute of the Russian Interior Ministry. 2024, no. 2 (109), pp. 254–264.
DOI: 10.55001/2312-3184.2024.26.72.022

Понятие персональных данных или личной информации включает в себя разнообразные сведения, касающиеся конкретного человека и позволяющие его идентифицировать, даже если это не указано явно. С развитием сетевых технологий и автоматизации анализа информации, централизованное хранение данных о человеке становится все более распространенным, а незаконный доступ к таким данным становится реальностью. Эти данные могут быть использованы для различных целей, включая преступные деяния, мошенничество или рекламные кампании. Современные технологии даже позволяют идентифицировать людей по косвенным признакам.

В конце XX века в России ситуация с доступом к личной информации сотрудников и клиентов различных организаций представляла собой крайне неблагоприятную картину. В то время легко было приобрести съемные носители информации, содержащие такие данные, на рынках или в подземных переходах. Законодательство тех лет не устанавливало никакой ответственности за разглашение такой конфиденциальной информации. Понятие «персональные данные» впервые появилось в законе только в 1997 году, но оно было описано весьма ограниченно, не предоставляя четких правил относительно обработки этих данных или ответственности за их неправомерное использование [1].

Следующим значимым этапом в области защиты персональных данных стало принятие в 2001 году Трудового кодекса Российской Федерации, который внес важные изменения, касающиеся защиты персональных данных работников. Введение отдельной главы, посвященной этой теме, позволило закрепить понятие «обработка

персональных данных работника» и установить ответственность работодателя за неправомерное использование такой информации.

Принятый Федеральный закон № 152-ФЗ «О персональных данных» стал еще одним значимым шагом в направлении защиты прав и свобод человека при обработке его персональных данных. В нем были закреплены основные понятия, связанные с защитой персональных данных, а также само понятие «персональные данные», которые определяются как любая информация, прямо или косвенно относящаяся к определенному физическому лицу. Предыдущая редакция закона содержала более детальный, но открытый перечень таких данных.

Среди широкого спектра информации, составляющей персональные данные, можно выделить две основные категории: номинативные и неноминативные [2]. Номинативная информация включает в себя те данные, которые могут быть использованы для идентификации конкретного человека, такие как его фамилия, имя, отчество, пол, серия и номер паспорта, а также дата и место его рождения и прочие подобные данные. Особое важное значение среди номинативных персональных данных имеют биометрические сведения, описывающие физиологические и биологические особенности человека, которые могут быть использованы для его точной идентификации.

К неноминативной категории относится информация, которая не связана непосредственно с идентификацией человека, например, данные о его доходах, месте работы, политических убеждениях, медицинских состояниях, наличии судимости и прочие сведения.

Федеральный закон от 27.07.2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» устанавливает классификацию персональных данных как конфиденциальной информации. Согласно этому законодательству, обработка персональных данных оказывает значительное влияние на неприкосновенность частной жизни, личную и семейную тайну. В соответствии со статьей 7 федерального закона № 152-ФЗ, «операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом». Это гарантирует конфиденциальность персональных данных, что подразумевает законодательное обеспечение режима их тайны.

В текущей практике обработки персональных данных принято получение согласия от самих субъектов данных на обработку их информации. В соответствии с этим принципом, субъекты данных или их представители должны выразить свое согласие на обработку своих данных любым удобным для них способом, подтверждая этот факт получения согласия, за исключением случаев, когда федеральным законом предусмотрено иное. Однако существуют исключения из этого общего правила, которые должны быть четко определены в федеральных законах. Важно отметить, что данное согласие на обработку персональных данных не является окончательным и необратимым: его можно отозвать в любой момент. Для этого не требуется объяснять причины такого решения или выполнять какие-либо дополнительные условия, достаточно просто уведомить оператора персональных данных о принятом решении.

Важно, однако, отметить, что право на отзыв согласия на обработку персональных данных не распространяется на случаи обработки данных, предусмотренные федеральными законами, которые могут требовать обязательного предоставления персональных данных самим субъектом.

Без такого согласия действуют автоматизированные программы, известные как «боты-пробивщики». Эти программы представляют собой системы, которые активно извлекают информацию о гражданах из различных баз данных, преимущественно похищенных незаконным образом через утечки данных из организаций и государственных учреждений (как правило такие утечки происходят по вине человека) [3, с. 358, 4, с. 43]. Эти действия не соответствуют закону и должны привести к ответственности как лиц, осуществивших кражу таких данных, так и тех, кто незаконно использует эту информацию. Лица, воспользовавшиеся «ботами-пробивщиками», должны быть признаны операторами персональных данных и строго соблюдать все требования законодательства в этой области. Однако, на практике, практически никто не следует этим требованиям.

Современный криминальный рынок услуг претерпел виртуализацию в связи с развитием информационных технологий и ограничениями, вызванными пандемией, что привело к изменениям в объеме и типе предоставляемых услуг [5, с. 70]. Одной из популярных криминальных услуг онлайн-услуг является предоставления сведений о лице (ФИО, телефон, адрес проживания, авиаперелеты, доставка продуктов и т. п.).

В России использование «ботов-пробивщиков» может лишь привести к наложению административных штрафов, несмотря на потенциально серьезные последствия их действий. Однако на практике выявление и привлечение к ответственности владельцев таких программ представляют собой крайне сложные задачи, поскольку определение их личности и местоположения за пределами страны являются весьма трудоемкими процессами, требующими значительных усилий и ресурсов.

В настоящее время с такого рода распространителями информации борется Роскомнадзор, который обращается к представителям мессенджеров о блокировки каналов, содержащих персональные данные граждан. Так, в 2021 г. администрацией мессенджера обмена сообщениями «Telegram» были заблокированы несколько популярных ботов, предоставляющих доступ к информации о любом человеке по запросу[1].

Несмотря на угрозы для конфиденциальности данных, в настоящее время законодательство не предусматривает наказания за использование незаконных сервисов, таких как «Глаза Бога», позволяющих получить личные данные человека. Однако административная и уголовная ответственность возможна для администраторов таких сервисов и лиц, предоставивших им данные без согласия субъектов. Действиям организаторов сбора и предоставления информации о гражданах, в том числе персональных данных, можно квалифицировать по ст. 137 УК

[1] Telegram по требованию Роскомнадзора заблокировал собиравших данные ботов. 2021 // Взгляд: деловая газета : сайт. URL: https://vz.ru/news/2021/3/12/1089106.html (дата обращения: 27.02.2024).

РФ, которая предусматривает уголовную ответственность за незаконный сбор или распространение сведений о частной жизни без согласия субъекта.

В современном информационном обществе необходимо обеспечивать надлежащую защиту персональных данных и соблюдать законодательные требования для предотвращения нарушений и злоупотреблений. Практика привлечения к уголовной ответственности по различным статьям УК РФ за нарушения в области использования персональных данных только усиливает значимость охраны данных в нашем обществе [6].

В различных судебных решениях наблюдается противоречивый подход к квалификации деяний в схожих обстоятельствах, что вызывает дискуссии и возражения. Например, в одном случае сотрудника обвиняют в разглашении коммерческой тайны, а в другом подобного обвинения не выдвигается. Также не всегда лицо подвергается обвинениям в неправомерном доступе к компьютерной информации, даже если оно использовало свои учетные данные для доступа к базе данных. Кроме того, не всегда сотрудник признается в использовании своего служебного положения для доступа к информации, несмотря на его обязанность соблюдать конфиденциальность в соответствии с должностной инструкцией.

Анализ судебной практики указывает на то, что данный определяющий фактор не всегда принимается во внимание, даже если лицо, совершившее правонарушение, действовало из корыстных побуждений, получая вознаграждение за копирование и передачу персональных данных в соответствии с частью 2 статьи 272 Уголовного кодекса Российской Федерации [7]. Во-первых, действия нарушителей конфиденциальности информации, которые копируют данные из баз данных и передают их заказчику, оцениваются исключительно с учетом положений статей 137 и (или) 138 УК РФ. Во-вторых, в судебных постановлениях, вынесенных после введения в Уголовный кодекс РФ статьи 274.1, не наблюдается попыток определить, является ли информационная система, к которой был совершен неправомерный доступ, критической информационной инфраструктурой и включена ли она в Реестр значимых объектов критической информационной инфраструктуры. Учитывая перечисленные варианты квалификационных решений правоприменителя, нельзя согласиться с ними в данном контексте.

При оценке степени вины лица в совершении преступления, предусмотренного статьей 183 УК РФ, важно учитывать, что персональные данные считаются конфиденциальной информацией с ограниченным доступом. Это подтверждается особыми условиями доступа для сотрудников к информационной системе и требованиями к безопасности информации. Базы данных клиентов организаций охраняются согласно уголовному законодательству и подпадают под режим коммерческой тайны, если в отношении них были установлены соответствующие правила и меры безопасности [8, с. 100]. Таким образом, нарушение режима конфиденциальности данных, включая использование чужой учетной записи для копирования и передачи персональных данных третьим лицам, является преступлением, предусмотренным статьей 183 УК РФ.

В случаях совместного участия лиц, не являющихся работниками организаций, откуда произошла умышленная утечка персональных данных, квалификация

содеянного определяется в соответствии с положениями статьи 33 и статьи 183 УК РФ. Аналогичный принцип должен применяться и к банковской и налоговой тайне. В соответствии со статьей 857 ГК РФ «О банковской тайне», банк обязуется сохранять конфиденциальность банковских счетов и операций клиентов. Именно поэтому сотрудники банков заключают соглашения о соблюдении конфиденциальности, что суд признает в качестве доказательства их знания и доступа к конфиденциальной информации по работе в банке.

При внесении обвинения в соответствии со статьей 272 УК РФ, необходимо учитывать, что субъектами данного преступления могут быть различные лица, включая тех, кто имеет законный доступ к закрытым базам данных клиентов. Согласно различным теориям уголовного права, существует много точек зрения на оценку законности таких действий. Можно отметить, что доступ к компьютерной информации является неправомерным в случае, если лицо осуществляет какие-либо действия, позволяющие ему распоряжаться информацией без согласия её владельца.

При анализе деятельности персонала банков, операторов мобильной связи и других организаций видно, что они не имеют права доступа к персональным данным клиентов, включая информацию, относящуюся к банковской, коммерческой или налоговой тайне, без строгого соблюдения своих служебных обязанностей. Необходимость пресечения случаев неправомерного доступа к информационным системам требует нового подхода, который учитывает не только функциональные обязанности, но и права сотрудников организаций. Однако, несмотря на ясные нормы и ограничения, в судебной практике встречаются случаи осуждения работников, которые, игнорируя свои должностные обязанности, незаконно копируют и передают личные данные. В таких ситуациях обвинение должно включать признак использования служебного положения для достижения личных корыстных целей.

Однако если сбор информации о личной жизни связан с такими действиями, как проникновение в жилище или подключение к линии связи, то это может быть квалифицировано как преступление по другим статьям УК РФ (138, 139 УК РФ). Распространение информации о частной жизни лица может включать как ограниченное раскрытие информации определенному кругу лиц, так и ее публичное разглашение без согласия субъекта. Подобные действия считаются преступными, если сведения собраны и распространены незаконно, то есть вопреки установленным законом правилам. Однако, если действия совершаются в соответствии с законодательством Российской Федерации, например, в рамках законов о полиции или средствах массовой информации, то они не признаются преступными. Обязательным условием для совершения преступления по статье 137 УК РФ является отсутствие согласия со стороны лица, информация о котором собирается и распространяется.

В судебной практике установление статуса личной и семейной тайны для различных сведений о частной жизни в значительной степени зависит от желания субъекта, что делает эти понятия субъективными. Это приводит к ситуации, когда одно и то же действие, например, сбор и распространение информации о социальном происхождении, может либо привести к уголовной ответственности, либо не иметь юридических последствий, в зависимости от того, считает ли субъект эту информацию личной или семейной тайной.

Для решения этой проблемы предлагается рассматривать личную и семейную тайну не как отдельные категории, а как общие понятия, объединяющие уже существующие виды тайн, установленные в отдельных законах. Например, к личной тайне можно отнести врачебную тайну или тайну завещания, а к семейной тайне - тайну усыновления. Кроме того, внесение соответствующих изменений в законодательство может помочь уточнить, какие конкретно сведения относятся к личной и семейной тайне.

Преступление, описанное в статье 137 УК РФ, требует исключительно умышленного участия. Мотивы и цели не оказывают влияния на квалификацию этого преступления. Помимо вопросов, касающихся толкования понятий потерпевшего и оценочных аспектов в этом преступлении, особый интерес представляет его субъективная сторона. При сравнении с нормами, устанавливающими уголовную ответственность за нарушения, затрагивающие жизнь и здоровье, можно сделать вывод, что законодатель устанавливает относительно мягкие наказания для этого преступления, определяя его как средней тяжести. Максимальное наказание за его совершение не превышает пяти лет лишения свободы, учитывая возможные последствия для лиц, не достигших шестнадцатилетнего возраста, такие как «вред здоровью», «расстройство психики» или «тяжкие последствия».

В связи с этим, для уточнения формы умысла, целесообразно включить в часть 3 статьи 137 УК РФ фразу «повлекшее за собой по неосторожности». Это предложение позволит более точно отразить отношение виновного к указанным последствиям, что соответствует принципу субъективной ответственности за совершенные деяния, установленный в статье 5 УК РФ.

Кроме того, мы считаем, что в случае установления умышленного отношения виновного к указанным последствиям в части 3 статьи 137 УК РФ, ответственность должна быть установлена по совокупности преступлений, например, по части 3 статьи 137 УК РФ и статье 110 УК РФ «Доведение до самоубийства» или по другим нормам, предусмотренным в Главе 16 УК РФ [9].

Это подтверждается и анализом других составов преступлений, например, в пункте "б" части 3 статьи 131 УК РФ «Изнасилование», где тяжкие последствия могут включать самоубийство или попытку самоубийства потерпевшего лица.

Таким образом, анализ объективных и субъективных признаков преступления, предусмотренного частью 3 статьи 137 УК РФ, позволяет выявить ряд проблем квалификации этого деяния и предложить варианты их решения [10].

Судебная практика свидетельствует о многочисленных случаях разглашения в социальных сетях интимных фотографий и видео, сделанных другим человеком, бывшим партнером. Этот вид действий в научном сообществе известен как порноместь. Один из таких случаев был рассмотрен Торжокским городским судом Тверской области[2]. Подсудимый В. обвинялся в том, что он, действуя незаконно и с прямым умыслом, решил опорочить честь и достоинство бывшей партнерши ФИО-1

[2] Приговор Торжокского городского суда (Тверская область) от 21 мая 2019 г. по делу № 1-107/2019 // Судебные и нормативные акты Российской Федерации : сайт. URL: http://sudact.ru (дата обращения: 27.02.2024).

после разрыва личных отношений. С целью распространения сведений о ее частной жизни, которые составляют ее личную тайну, В. разместил на своих персональных страницах в социальных сетях «ВКонтакте», «Одноклассники» и Instagram ее фамилию, имя, дату рождения, а также 16 фотоснимков, на которых ФИО-1 изображена в нижнем белье, которые ранее были в его личном владении. Суд принял во внимание, что размещенная В. информация является открытой и доступной для всех пользователей этих социальных сетей, включая знакомых ФИО-1. Таким образом, В. предполагал, что эти материалы будут просмотрены неограниченным числом пользователей, в том числе и знакомых ФИО-1, что могло нанести ущерб ее авторитету и репутации.

Вопрос обеспечения защиты персональных данных в рамках статей 137 и 138 УК РФ, которые регулируют различные категории тайн, продолжает оставаться в центре внимания в сфере правоприменительной практики. Передача персональных данных третьим лицам нарушает не только право на неприкосновенность личной информации, но и сам принцип согласия, поскольку клиенты не дали разрешения на использование и передачу их данных вне заранее определенных целей. Отказ от применения обеих статей 137 и 138 УК РФ в делах, связанных с нарушением различных видов тайн, обусловлен тем, что судебные органы признают использование двойного признака виновности противоречащим принципам законности и может привести к неоднозначным судебным решениям.

СПИСОК ИСТОЧНИКОВ

1. Алямкин, С. Н. Персональные данные как объект правового регулирования: понятие и способы защиты // Мир науки и образования. 2016. №4 (8). С. 4.

2. Бачило, И. Л., Лопатин, В. Н., Федотов, М. А. Информационное право : учебник / Под ред. акад. РАН Б. Н. Топорнина. СПб. : Издательство «Юридический центр Пресс», 2001. 789 с.

3. Репецкая, А. Л., Родивилин, И. П. Предупреждение преступлений в сфере обращения охраняемой законом информации // Академический юридический журнал. 2021. № 4. С. 352–360.

4. Степаненко, Д. А., Рудых, А. А. Технико-криминалистическое обеспечение противодействия преступлениям против информационной безопасности объектов здравоохранения // Академический юридический журнал. 2021. № 1. С. 41–48.

5. Репецкая, А. Л. Криминальный рынок услуг, теневые услуги, пандемия, детерминация, криптовалюта // Сибирский юридический вестник. 2023. № 1. С. 65-71.

6. Братановский, С. Н. Специальные правовые режимы информации. Саратов: «Научная книга», 2010. 172 с.

7. Родивилина, В. А., Коломинов, В. В. Криминалистическая характеристика отдельных видов преступлений, совершенных с использованием информационно-телекоммуникационных технологий // Криминалистика: вчера, сегодня, завтра. 2022. № 1. С. 110–120

8. Климанов, А. М. Некоторые вопросы квалификации преступления, предусмотренного ст. 137 УК РФ // Теория и практика общественного развития. 2015. № 9. С. 98–102.

9. Хохлова, Е. В. К вопросу о защите изображения человека как персональных данных (на основе судебной практики по ст. 137 УК РФ) // Вестник Воронежского института МВД России. 2023. № 1. С. 1–5.

10. Усманова, Е. Ф. Проблемы и особенности формирования правовой культуры в современном правовом государстве // Инновационные тенденции, социально-экономические и правовые проблемы взаимодействия в международном пространстве. Саранск, 2016. С. 235–237.

REFERENCES

1. Alyamkin S.N. Personalnye dannye kak ob"yekt pravovogo regulirovaniya: ponyatie i sposoby zashchity [Personal Data as an Object of Legal Regulation: Concept and Protection Methods]. 2016, no. 4 (8), pp. 4.

2. Bachilo I.L., Lopatin V.N., Fedotov M.A. Informatsionnoe pravo [Information law]. St. Petersburg: Publishing House "Juridical Center Press", 2001, 789 p.

3. Repetskaya A.L., Rodivilin I.P. Preduprezhdeniye prestupleniy v sfere obrashcheniya okhranyaemoy zakonom informatsii [Prevention of Crimes in the Sphere of Handling Information Protected by Law]. Akademicheskij juridicheskij zhurnal - Academic Legal Journal. 2021, no. 4, pp. 352-360.

4. Stepanenko D.A., Rudikh A.A. Tekhniko-kriminalisticheskoye obespecheniye protivodeystviya prestupleniyam protiv informatsionnoy bezopasnosti ob"yektov zdravookhraneniya [Technical and Criminalistic Support for Counteracting Crimes Against Information Security of Healthcare Facilities]. Akademicheskij juridicheskij zhurnal - Academic Legal Journal. 2021, no. 1, pp. 41-48.

5. Repetskaya A.L. Kriminal'nyy rynok uslug, tenevyye uslugi, pandemiya, determinatsiya, kriptovalyuta [Criminal Market of Services, Shadow Services, Pandemic, Determination, Cryptocurrency]. Sibirskij juridicheskij Vestnik - Siberian Legal Herald. 2023, no. 1, pp. 65-71.

6. Bratanovskiy S.N. Spetsial'nye pravovye rezhimy informatsii [Special Legal Regimes of Information]. Saratov: "Scientific Book", 2010, 172 p.

7. Rodivilina V.A., Kolominov V.V. Kriminalisticheskaya kharakteristika otdel'nykh vidov prestupleniy, sovershennykh s ispol'zovaniem informatsionno-telekommunikatsionnykh tekhnologiy [Criminalistic Characteristics of Certain Types of Crimes Committed Using Information and Telecommunication Technologies]. Kriminalistika: vchera, segodnja, zavtra.- Criminalistics: Yesterday, Today, Tomorrow. 2022, no. 1, pp. 110-120.

8. Klimanov A.M. Nekotorye voprosy kvalifikatsii prestupleniya, predusmotrennogo stat'ei 137 UK RF [Some Issues of Qualification of a Crime under Art. 137 of the Criminal Code of the Russian Federation]. Teorija i praktika obshhestvennogo razvitija - Theory and Practice of Social Development. 2015, no. 9, pp. 98-102.

9. Khokhlova E.V. K voprosu o zashchite izobrazheniya cheloveka kak personal'nykh dannykh (na osnove sudebnoy praktiki po stat'e 137 UK RF) [On the Issue of Protecting a Person's Image as Personal Data (Based on Judicial Practice under Art. 137 of the Criminal Code of the Russian Federation)]. Vestnik Voronezhskogo instituta MVD Rossii - Vestnik of the Voronezh Institute of the Ministry of Internal Affairs of Russia. 2023, no. 1, pp. 1-5.

10. Usmanova E.F. Problemy i osobennosti formirovaniya pravovoy kul'tury v sovremennom pravovom gosudarstve [Problems and Features of Forming Legal Culture in a Modern Legal State]. Innovacionnye tendencii, social'no-jekonomicheskie i pravovye problemy vzaimodejstvija v mezhdunarodnom prostranstve - Innovative Trends, Socio-Economic and Legal Problems of Interaction in the International Space. Saransk, 2016, pp. 235-237.

ИНФОРМАЦИЯ ОБ АВТОРАХ

Родивилин Иван Петрович, кандидат юридических наук, доцент центра компетенций по кибербезопасности. Иркутский национальный исследовательский технический университета. 664074, г. Иркутск, ул. Лермонтова, 83.
ORCID ID: 0000-0002-9411-1048
Коломинов Вячеслав Валентинович, кандидат юридических наук, доцент, доцент кафедры криминалистики, судебных экспертиз, и юридической психологии Института юстиции. Байкальский государственный университет. 664003, г. Иркутск, ул. Ленина, 11.
ORCID ID: 0000-0003-0824-4395

INFORMATION ABOUT AUTHOR

Rodivilin Ivan Petrovich, Candidate of Law Sciences, Associate Professor at the Center for Cybersecurity Competencies. Irkutsk National Research Technical University. 664074, Irkutsk, 83 Lermontov str.
Kolominov Vyacheslav Valentinovich, Candidate of Law Sciences, Associate Professor, Associate Professor of the Department of Criminology, Forensic Examinations, and Legal Psychology at the Institute of Justice. Baikal State University. 664003, Irkutsk, 11 Lenin Street.

Статья поступила в редакцию 22.02.2024; одобрена после рецензирования 22.03.2024; принята к публикации 25.05.2024.

The article was submitted 22.02.2024; approved after reviewing 22.03.2024; accepted for publication 25.05.2024.