Научная статья
УДК 343
https://doi.org/10.36511/2078-5356-2023-2-96-100

Электронная подпись как предмет преступления по статье 272 Уголовного кодекса Российской Федерации

Ларичев Василий Дмитриевич[1], Панкратьев Анатолий Николаевич[2]
[1, 2]Всероссийский научно-исследовательский институт МВД России, Москва, Россия, larichev48@mail.ru
[2]Главное управление экономической безопасности и противодействия коррупции МВД России, Москва, Россия, a.pankratev@gmail.com

Аннотация. В статье рассматриваются проблемные вопросы привлечения к уголовной ответственности за использование электронной подписи в криминальных целях. Авторами проведено исследование судебных решений по делам о преступлениях, где в качестве предмета преступного посягательства названа электронная подпись. По итогам сформулирован вывод о том, что действия, направленные на незаконное получение (выдачу) электронной подписи на чужие персональные данные либо на вымышленное лицо, могут быть самостоятельно квалифицированы по статье 272 Уголовного кодекса Российской Федерации при условии, что эти действия повлекли модификацию (изменение) информации.

Ключевые слова: электронная подпись, неправомерный доступ, компьютерная информация, копирование компьютерной информации

Для цитирования: Ларичев В. Д., Панкратьев А. Н. Электронная подпись как предмет преступления по статье 272 Уголовного кодекса Российской Федерации // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2023. № 2 (62). С. 96—100. https://doi.org/10.36511/2078-5356-2023-2-96-100.

Original article

Electronic signature as the subject of a crime under article 272 of the Criminal Code of the Russian Federation

Vasily D. Larichev[1], Anatoly N. Pankratiev [2]
[1, 2]All-Russian Research Institute of the Ministry of Internal Affairs of Russia, Moscow, Russian Federation, larichev48@mail.ru
[2]Main Department of Economic Security and Anti-Corruption of the Ministry of Internal Affairs of Russia, Moscow, Russian Federation, a.pankratev@gmail.com

Abstract. The article discusses the problematic issues of bringing to criminal responsibility for the use of an electronic signature for criminal purposes. The authors conducted a study of court decisions in cases of crimes, where “electronic signature” is named as the subject of criminal encroachment. A number of proposals have been formulated to improve criminal legislation. As a result, the conclusion is formulated that actions aimed at illegally obtaining (issuing) an electronic signature on someone else’s personal data or on a fictitious person can be independently qualified under Article 272 of the Criminal Code of the Russian Federation, provided that these actions entailed modification (modification) of information.

Keywords: electronic signature, illegal access, computer information, copying of computer information

For citation: Larichev V. D., Pankratiev A. N. Electronic signature as the subject of a crime under article 272 of the Criminal Code of the Russian Federation. *Legal Science and Practice: Journal of Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia,* 2023, no. 2 (62), pp. 96—100. (In Russ.). https://doi.org/10.36511/2078-5356-2023-2-96-100.

Относительная простота и доступность электронных подписей (далее — ЭП) сформировали противоправную инфраструктуру, незаконного приобретения и использования

ориентированную на организацию их сбыта, в которой задействованы лицензируемые удостоверяющие центры, при этом имеющиеся факты проведения в отношении них процессуальных проверок, хотя и привели к отзыву аккредитации (*URL: https://iecp.ru/news/item/430096-135-udostoveryayushchih-centrov-lishilis-akkreditacii, https://www.klerk.ru/buh/news/525546/* (дата обращения: 09.09.2022)), но до настоящего времени не завершились привлечением к ответственности виновных лиц.

В практической плоскости правоохранительные органы сталкиваются с массовым неправомерным выпуском ЭП и использованием их в различных противоправных целях (*URL: https://pravdaurfo.ru/articles/199634-v-ekaterinburge-vskryli-centr-mahinaciy-s-ecp, https://77.мвд.рф/news/item/23980031* (дата обращения: 09.09.2022)).

Проблема противодействия использованию ЭП в преступных целях является весьма актуальной и в последнее время неоднократно становилась предметом исследования целого ряда научных работ. Этой проблематике посвящены работы М. В. Демченко [1], Ю. А. Бондаренко [2] и др. [3—5].

Широкое использование ЭП в противоправных целях способствовало созданию новых способов экономических и налоговых преступлений, в том числе по схеме «бумажный» НДС, что являлось предметом отдельной публикации [6].

Ранее авторами были опубликованы результаты исследования современной судебной практики по делам о преступлениях, совершенных с использованием ЭП в первую очередь деяний экономической направленности, в котором сделан вывод о том, что в большинстве случаев незаконный оборот (выпуск и сбыт) ЭП самостоятельно не квалифицируются как преступные действия, а использование ЭП рассматривается преимущественно только как прием в совершении иного преступления без дополнительной квалификации [7].

Одним из вариантов разрешения данной проблемы могла бы являться криминализация незаконного оборота ЭП путем внесения соответствующей статьи Уголовного кодекса Российской Федерации (далее — УК РФ). В данном направлении предпринимались определенные попытки. Так, например, Минцифры России в 2018 году выступило автором законопроекта о введении уголовной ответственности за подделку электронных цифровых подписей (проект Федерального закона «О внесении изменений в некоторые законодательные акты Российской Федерации в связи с совершенствованием регулирования в сфере электронной подписи» (*ID* проекта 02/04/09-18/00083642 подготовлен Минкомсвязью России 4 сентября 2018 года). *URL: https://regulation.gov.ru* (дата обращения: 09.09.2022)). Со схожим предложением в 2021 году выступило МВД России (*URL: https://www.rbc.ru/technology_and_media/18/05/2021/60a3e8759a7947e88055018b?utm_source=yxnews&utm_medium=desktop* (дата обращения: 09.09.2022)). Однако до настоящего времени указанные изменения не приняты.

Сложившаяся ситуация несет существенную угрозу как публичным интересам общества и государства, дискредитируя политику цифровизации, так и частным интересам граждан и организаций, чьи права и законные интересы нарушаются преступными посягательствами.

В этой ситуации существует объективная необходимость проведения углубленного анализа правовой природы правоотношений, связанных с ЭП, с целью поиска возможных механизмов решения названной проблемы в рамках действующего законодательства.

В настоящее время уголовное законодательство не содержит термина «электронная подпись». Однако исходя из иных нормативных актов, ЭП представляет собой информацию в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией (ст. 2 Федерального закона от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи»).

Не рассматривая подробно технологические процессы создания и использования ЭП, необходимо отметить, что они связаны с компьютерными программами, среди которых ассиметричные и симметричные криптографические системы, а также системы, которые не используют в работе криптографические алгоритмы. Однако в любом случае ЭП не может существовать вне носителя электронной информации, и ее невозможно использовать без применения компьютера и компьютерных программ.

Следует отметить, что общественные отношения в сфере использования компьютерной информации являются объектом преступления, предусмотренного статьей 272 УК РФ.

Основные вопросы, возникающие при квалификации преступлений, предусмотренных статьей 272 УК РФ, рассмотрены в соответствующем Пленуме Верховного суда Российской Федерации (постановление Пленума Верховного

Legal Science and Practice: Journal of Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia, 2023, no. 2 (62)

Суда Российской Федерации от 15 декабря 2022 года № 37 «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»). Однако текст Пленума не содержит прямого ответа на вопрос о том, возможно ли рассматривать электронную подпись в качестве предмета преступления, предусмотренного статьей 272 УК РФ.

С точки зрения Уголовного закона применительно к статье 272 УК РФ под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

При этом должен быть установлен специальный правовой режим, ограничивающий свободный доступ к компьютерной информации. На практике это может выражаться в том, что информация содержит сведения, отнесенные к государственной, коммерческой, налоговой, банковской тайне. Однако наряду с этим суды, не увязывая режим охраны с конкретным видом тайны, относят к предмету статьи 272 УК РФ и иные сведения, доступ к которым ограничен законом, в том числе служебную информацию (приговор Петушинского районного суда Владимирской области от 2 июля 2020 г. № 1-85/2020 по ч. 2 ст. 272 УК РФ), а также сведения, составляющие персональные данные (приговор Железнодорожный районный суд г. Хабаровска от 10 июля 2020 г. № -291/2020 по ч. 3 ст. 272 УК РФ), под которыми понимается любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (ст. 3 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»). Одновременно одним из требований к усиленной ЭП является то, что она позволяет определить лицо, подписавшее электронный документ. Таким образом, по крайней мере, квалифицированную ЭП можно отнести к персональным данным.

Однако ЭП обладает и самостоятельными признаками охраняемой информации в силу правового статуса, закрепленного федеральным законодательством, прямо устанавливающего обязанности обеспечения конфиденциальности недопущения использования ключей электронных подписей без согласия участников электронного взаимодействия (ст. 10 Федерального закона от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи»).

Таким образом, по своему содержанию ЭП, являясь охраняемой законом информацией в электронной форме, соответствует указанному определению компьютерной информации и может являться предметом статьи 272 УК РФ.

Проведенное исследование судебных решений по уголовным делам позволило установить, что «электронная подпись» достаточно часто упоминается в тексте судебных решений, при этом использование ЭП расценивается судами как юридически значимая часть способа совершения преступления.

Типовой является ситуация, когда осужденный неправомерно использовал собственную ЭП для совершения незаконных действий, в том числе изменения данных в автоматизированных системах. Так, например, заместитель начальника таможенного поста гр-н Ш. с помощью личной служебной электронной подписи осуществил неправомерный доступ и изменение компьютерной информации в автоматизированной информационной системе таможенного оформления (апелляционное постановление Московского областного суда от 12 марта 2019 года № 22-1179/19 по ч. 3 ст. 272 УК РФ).

Схожим образом квалифицируется использование чужой электронной подписи без ведома владельца. Например, менеджер по продажам ОАО Сбербанк гр-н Р. в нарушение нормативных документов использовал электронную подпись других сотрудников банка без их ведома для неправомерного выпуска банковских карт (апелляционное определение Курского областного суда от 2017 года № 22-1052-2017 по ч. 3 ст. 272 УК РФ).

Показательным в этом смысле является приговор в отношении системного администратора гр-на Ш., который без ведома правообладателя сохранил сведения о ключе для электронной цифровой подписи платежного агента на личной флэш-карте, а затем осуществил неправомерный доступ к охраняемой законом компьютерной информации через сеть «Интернет» для перечисления чужих денежных средств на лицевые счета своих родственников. Обращает на себя внимание тот факт, что суд, мотивируя приговор, указал на то, что неправомерное копирование чужой электронной подписи прямо противоречит действующему законодательству (приговор Узловского городского суда Тульской области от 17 сентября 2013 г. (номер скрыт) ч. 2 ст. 272, ч. 1 ст. 158 УК РФ).

В этой связи под незаконным использованием ЭП следует понимать использование собственной подписи в противоправных целях, а

Legal Science and Practice: Journal of Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia, 2023, no. 2 (62)

равно использование чужой подписи, в том числе ее копирование, без ведома владельца.

Между тем диспозиция статьи 272 УК РФ предусматривает наступление последствия в виде уничтожения, блокирования, модификации либо копирования компьютерной информации.

Такая формулировка, безусловно, является крайне неопределенной и неоднократно подвергалась критике правоведов.

Возвращаясь к типовой ситуации незаконного получения электронной подписи на чужие персональные данные, необходимо разрешить вопрос, на каком этапе такие действия приводят к наступлению последствий, соответствующих статье 272 УК РФ.

Незаконное получение ключа электронной подписи без ведома владельца само по себе связано с копированием компьютерной информации, содержащейся в этом ключе ЭП, злоумышленник в любом случае должен сохранить ее на собственном компьютере или внешнем электронном носителе, однако судебная практика по статье 272 УК РФ в большинстве случаев под копированием понимает сохранение информации на носителе при условии, что первоначальная информация, находящаяся в распоряжении владельца, осталась неизменной.

Однако в рассматриваемой ситуации формальный владелец ЭП не владеет соответствующей информацией и даже не знает о ее существовании. По тем же причинам достаточно сложно говорить о модификации или уничтожении информации. Аналогичным образом в случае незаконного выпуска повторной подписи первичная «законная» ЭП остается неизменной и, как правило, продолжает действовать.

Тем не менее общественно опасные последствия, по нашему мнению, наступают, однако они выражаются не в изменении или копировании первоначальной информации на компьютерной технике формального владельца подписи, а в изменении информации, составляющей содержание реестров учета электронных подписей. Порядок ведения подобных реестров, как правило, определен ведомственными нормативными актами (приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 8 ноября 2021 г. № 1138 «Об утверждении Порядка формирования и ведения реестров, выданных аккредитованными удостоверяющими центрами квалифицированных сертификатов ключей проверки электронной подписи, а также предоставления информации из таких реестров, включая требования к формату предоставления такой информации»; приказ ФАПСИ от 13 июля 2001 г. № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»).

Необходимо отметить, что схожую позицию занимают суды при рассмотрении дел, связанных с подменой данных о владельце сим-карты без его ведома: в этом случае сведения, находящиеся на «законной» сим-карте, не подвергаются изменению или копированию, изменяются сведения в электронной базе данных оператора связи (приговор Кашинского межрайонного суда Тверской области от 21 июля 2020 г. № 1-68/2020 по ч. 3 ст. 272 УК РФ; приговор Железнодорожного районного суда г. Пензы от 29 мая 2020 г. № 1-189/2020).

Так, старший менеджер ПАО «ВымпелКом» гр-н В. произвел незаконную замену сим-карты без ведома лица, на имя которого был оформлен абонентский номер, при этом в качестве объективной стороны совершения преступления суд указал на то, что В. осуществил неправомерный доступ к компьютерной информации в информационных ресурсах ПАО «ВымпелКом» и неправомерно модифицировал через интерфейс программы *1С*: *Retail* сведения об абоненте, относимые к персональным данным (постановление Ленинского районного суда г. Новосибирска от 16 января 2020 г. № 1-104/2020 по ч. 4 ст. 33 и ч. 3 ст. 272, ч. 4 ст. 33 и ч. 3 ст. 272, ч. 4 ст. 33 и ч. 3 ст. 272, ч. 4 ст. 33 и ч. 3 ст. 272, ч. 3 ст. 272 УК РФ).

Подводя итог, допустимо констатировать, что действия, направленные на незаконное получение (выдачу) электронной подписи на чужие персональные данные либо на вымышленное лицо, могут быть самостоятельно квалифицированы по статье 272 УК РФ, как неправомерный доступ к охраняемой законом компьютерной информации при условии, что эти действия повлекли модификацию информации (изменение) в информационных базах данных.

Подобный юридический подход при формировании надлежащей судебной практики смог бы частично восполнить пробел уголовно-правовой защиты, рассматриваемых правоотношений.

Однако его реализация не может, по нашему мнению, рассматриваться как прекращение полемики относительно внесения в УК РФ понятия «электронная подпись» и создания специальной нормы.

Список источников

1. Демченко М. В. К вопросу о совершенствовании регулирования рынка недвижимости в Российской Федерации // Нотариус. 2020. № 8. С. 28—32.

2. Бондаренко Ю. А. Особенности расследования мошенничества, совершенного с использованием электронной подписи // Гуманитарные, социально-экономические и общественные науки. 2020. № 3. С. 60—63.

3. Маринкин Д. Н. Риски экономических преступлений: информационная безопасность электронной подписи в России // Проблемы правоохранительной деятельности. 2020. № 1. С. 61—65.

4. Арутюнов А. С., Фаниев П. А. Электронная подпись как орудие совершения преступления // Актуальные проблемы теории и практики оперативно-розыскной деятельности: материалы X Всероссийской научно-практической конференции, Краснодар, 14 октября 2021 года. Краснодар: Федеральное государственное казенное образовательное учреждение высшего профессионального образования «Краснодарский университет Министерства внутренних дел Российской Федерации», 2022. С. 7—11.

5. Маринкин Д. Н., Шмыков Д. В. Риски информационной безопасности при использовании электронной подписи в России, как важный элемент деятельности по предупреждению экономических преступлений // Право и государство: теория и практика. 2020. № 5 (185). С. 198—200.

6. Ларичев В. Д., Панкратьев А. Н. Перспективы нормативного противодействия налоговой схеме «бумажный» НДС // Научный портал МВД России. 2021. № 4 (56). С. 56—62.

7. Ларичев В. Д., Панкратьев А. Н. Проблемы развития уголовного законодательства в сфере использования ключей усиленной квалифицированной электронной цифровой подписи // Вестник Казанского юридического института МВД России. 2021. Т. 12. № 3 (45). С. 344—350.

References

1. Demchenko M. V. On the issue of improving the regulation of the real estate market in the Russian Federation. *Notary*, 2020, no. 8, pp. 28—32. (In Russ.)

2. Bondarenko Yu. A. Features of the investigation of fraud committed using an electronic signature. *Humanities, socio-economic and social sciences*, 2020, no. 3, pp. 60—63. (In Russ.)

3. Marinkin D. N. Risks of economic crimes: information security of electronic signatures in Russia. *Problems of law enforcement*, 2020, no. 1, pp. 61—65. (In Russ.)

4. Arutyunov A. S., Faniev P. A. Electronic signature as an instrument of committing a crime. Actual problems of theory and practice of operational investigative activity: materials of the X All-Russian Scientific and Practical Conference, Krasnodar, October 14, 2021. Krasnodar: Federal State Educational Institution of Higher Professional Education “Krasnodar University of the Ministry of Internal Affairs Of the Russian Federation” Publ., 2022. Pp. 7—11. (In Russ.)

5. Marinkin D. N., Shmykov D. V. Risks of information security when using an electronic signature in Russia as an important element of activities for the prevention of economic crimes. *Law and State: theory and practice*, 2020, no. 5 (185), pp. 198—200. (In Russ.)

6. Larichev V. D., Pankratiev A. N. Prospects of regulatory counteraction to the tax scheme “paper” VAT. *Scientific portal of the Ministry of Internal Affairs of Russia*, 2021, no. 4 (56), pp. 56—62. (In Russ.)

7. Larichev V. D., Pankratiev A. N. Problems of development of criminal legislation in the field of using keys of enhanced qualified electronic digital signature. *Bulletin of the Kazan Law Institute of the Ministry of Internal Affairs of Russia*, 2021, vol. 12, no. 3 (45), pp. 344—350. (In Russ.)

Информация об авторах

В. Д. Ларичев — доктор юридических наук, профессор;
А. Н. Панкратьев — кандидат юридических наук.

Information about the authors

V. D. Larichev — Doctor of Sciences (Law), Professor;
A. N. Pankratyev — Candidate of Sciences (Law).

Статья поступила в редакцию 12.05.2023; одобрена после рецензирования 31.05.2023; принята к публикации 05.06.2023.

The article was submitted 12.05.2023; approved after reviewing 31.05.2023; accepted for publication 05.06.2023.