

УДК 343.9

*С.А. Стяжкина***ЭЛЕКТРОННЫЙ ДОКУМЕНТ КАК ПРЕДМЕТ УГОЛОВНО-ПРАВОВОЙ ОХРАНЫ**

Статья посвящена проблеме уголовно-правовой защиты электронных документов. Информационная среда предоставляет широкие просторы для ведения документации, но и создает риски безопасной передачи, хранения документов, защищенности их от неправомерного изменения. Особое значение должно уделяться уголовно-правовой охране официальных электронных документов. Следует отметить, что действующее уголовное законодательство, регулирующее вопросы ответственности за незаконный оборот официальных документов, не совсем соответствует современным реалиям. Уголовный кодекс оперирует понятиями и терминами, которые были ориентированы на бумажный документооборот. Во-первых, необходимо пересмотреть традиционные подходы к установлению уголовной ответственности за незаконный оборот официальных документов, унифицировав основные понятия и признаки для разных документов. Кроме того, следует декриминализировать приобретение, перевозку и хранение поддельных официальных документов, а также использование заведомо поддельных документов. Во-вторых, необходимо решить вопрос квалификации и разграничения преступлений в сфере незаконного оборота официальных документов и преступлений в сфере компьютерной информации.

Ключевые слова: электронный документ, подделка документов, незаконный сбыт документов, официальный документ, использование заведомо поддельного документа, компьютерная информация, незаконный доступ к компьютерной информации, электронный документооборот, электронная подпись.

DOI: 10.35634/2412-9593-2022-32-1-178-184

Электронный документооборот все увереннее входит в нашу жизнь. Все больше и больше документов сегодня создаются и используются в электронной форме. Электронная форма документов удобна и проста в использовании, хранении, удостоверении. Современное цифровое общество активно движется в сторону замены многочисленных бумажных документов на цифровые аналоги. Одним из приоритетных направлений деятельности государства на сегодняшний день выдвигается деятельность по обеспечению информационной безопасности при передаче, обработке и хранении данных, гарантирующей защиту интересов личности, бизнеса и государства. Безусловно, цифровые документы гораздо практичнее как в использовании, так и в порядке оформления и хранения. Но переходя на новый формат документооборота, мы столкнемся с рядом трудностей, которые касаются, прежде всего, его безопасности. Информационная среда предоставляет широкие просторы для ведения документации, но и создает риски безопасной передачи, хранения документов, защищенности их от неправомерного изменения. Представляется, что в ближайшем будущем мы все перейдем на электронный формат документооборота, в связи с чем возникают вопросы обеспечения не только технической, но и правовой защиты цифровых документов. Особое значение должно уделяться уголовно-правовой охране официальных электронных документов. Следует отметить, что действующее уголовное законодательство, регулирующее вопросы ответственности за незаконный оборот официальных документов, не совсем соответствует современным реалиям. Уголовный кодекс оперирует понятиями и терминами, которые были ориентированы на бумажный документооборот. Конструкции составов преступлений сформулированы без учета возможности их применения в ситуациях, когда предметом преступлений выступают электронные документы. В связи с чем, назрела необходимость пересмотреть традиционные подходы к вопросам квалификации действий, посягающих на официальный документооборот.

Прежде всего, хотелось бы остановиться на вопросах определения понятия официального электронного документа. Понятие электронного документа содержится в ст. 2 Федерального закона от 27.02.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», где сказано, что «электронный документ – документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах»¹.

¹ Федеральный закон от 27.02.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СПС «Гарант».

Из этого следует, что электронный официальный документ – это разновидность официального документа, представленного в цифровом виде. Соответственно, признаки, присущие официальному документу, будут характерны и для электронного документа. Об этом говорится и в Постановлении Пленума Верховного Суда РФ от 17.12.20 № 43 «О некоторых вопросах судебной практики по делам о преступлениях, предусмотренных ст. 324 – 327.1 Уголовного кодекса Российской Федерации», в п. 1, что официальные документы – это «такие документы, в том числе электронные документы, которые создаются, выдаются либо заверяются в установленном законом или иным нормативным актом порядке федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, органами местного самоуправления либо уполномоченными организациями или лицами (образовательными, медицинскими и иными организациями, независимо от формы собственности, должностными лицами и лицами, выполняющими управленческие функции в коммерческих и некоммерческих организациях, экзаменационными, врачебными и иными комиссиями, нотариусами и пр.) и удостоверяют юридически значимые факты»².

С учетом вышеприведенного определения можно выделить несколько признаков, характеризующих документ в качестве официального. Во-первых, официальный электронный документ должен обладать признаками официальности. Это значит, что официальный документ должен удостоверять юридически значимые факты. Как говорится в вышеназванном Постановлении Пленума Верховного Суда РФ: «При этом к предмету преступления, предусмотренного ст. 324 УК РФ, следует относить только официальные документы, способные повлечь юридические последствия в виде предоставления или лишения прав, возложения обязанностей или освобождения от них, изменения объема прав и обязанностей (например, листок нетрудоспособности является основанием для назначения и выплаты работнику пособия по временной нетрудоспособности, медицинское заключение об отсутствии противопоказаний к управлению транспортными средствами предоставляет лицу право сдачи экзамена и получения водительского удостоверения)»³. Речь идет о том, что официальный документ должен определять статус лица как физического, так и юридического, менять объем его прав и обязанностей. Официальный документ всегда связан либо с возложением дополнительных прав и обязанностей, либо с освобождением от них. По сути он является юридическим фактом, с которым закон связывает возникновение, изменение либо прекращение прав и обязанностей лица.

Здесь возникают проблемы отграничения официального документа и просто документа, ответственность за использование которого предусмотрена в ч. 5 ст. 327 Уголовного кодекса РФ. Постановление Пленума Верховного Суда РФ от 17.12.20 № 43 «О некоторых вопросах судебной практики по делам о преступлениях, предусмотренных ст. 324 – 327.1 Уголовного кодекса Российской Федерации» говорит о том, что «Вместе с тем по смыслу ч. 5 ст. 327 УК РФ к заведомо подложным документам относятся любые поддельные документы, удостоверяющие юридически значимые факты, за исключением поддельных – паспорта гражданина, удостоверения или иного официального документа, предоставляющего права или освобождающего от обязанностей (например, подложные гражданско-правовой договор, диагностическая карта транспортного средства)»⁴. Данное положение не вносит ясности в отграничение двух документов. В качестве признака документа указывается, что он должен удостоверять юридически значимые факты. В принципе, то же самое Постановление Пленума Верховного Суда РФ говорит и об официальном документе.

В теории государства и права традиционно под юридическим фактом понимают «конкретные жизненные обстоятельства, с которыми нормы права связывают возникновение, изменение или прекращение правоотношений»⁵. Правоотношения могут быть разные, начиная от отношений гражданства, заканчивая отношениями купли-продажи.

Единственным критерием разграничения этих двух документов, предложенным правоприменителем, является то, что документ не должен быть официальным. Используется негативный признак при раскрытии понятия документа, что создает сложности. Предметом преступления, предусмотрен-

² Постановление Пленума Верховного Суда РФ от 17.12.20 № 43 «О некоторых вопросах судебной практики по делам о преступлениях, предусмотренных ст. 324–327.1 Уголовного кодекса Российской Федерации» // СПС «Гарант».

³ Там же.

⁴ Там же.

⁵ Морозова Л.А. Теория государства и права: учебник. 4-е изд. С. 234. URL: https://www.msmsu.ru/userdata/manual/doc/kaf/sud_med.pdf.

ного ч. 5 ст. 327 УК РФ, будет являться документ, не относящийся к числу официальных. Исходя из вышеизложенного, можно сделать вывод, что уголовная ответственность предусмотрена за использование любого документа, как официального, так и неофициального. Причем к неофициальным документам относятся любые документы, не подпадающие под признаки официального. Это могут быть всевозможные справки, выписки, квитанции, доверенности и т. д. Возникает вопрос об общественной опасности использования поддельного неофициального документа.

На сегодняшний день актуальным является вопрос возможности привлечения к уголовной ответственности лиц, использующих поддельные ПЦР-тесты, сертификаты вакцинации и т. д. Эти документы дают лицу возможность выезда за границу, посещения общественных мест, сохранения работы и т. д. Таким образом, их можно рассматривать в качестве документов, ответственность за использование которых предусмотрена ч. 5 ст. 327 УК РФ. Но, получается, что за использование подобного рода документов ответственность предусмотрена, а за подделку и сбыт не предусмотрена. Кроме того, представляется, что просто документ не должен выступать предметом уголовно-правовой охраны. В данном случае вполне достаточно было бы установление административной ответственности.

Вторым признаком следует назвать то, что официальные документы должны входить в систему регистрации и учета. Таким образом, документы можно проверять на их легальность. Электронные официальные документы обязательно должны входить в систему их учета. Это могут быть автоматизированные базы данных, автоматизированные информационно-поисковые системы, различного рода информационные реестры и т. д.

Немаловажным является и признак, связанный с источником происхождения документа. Официальные документы могут выдаваться как органами государственной власти и местного самоуправления, так и иными организациями, в том числе коммерческими, которым государство делегирует это право. Государство, разрешая выдачу, хранение и обработку официальных документов коммерческим структурам, контролирует порядок их выдачи, хранения и соответствие деятельности данных компаний государственным стандартам. Таким образом, официальные документы могут выдаваться и коммерческими организациями, например, медицинскими организациями, образовательными учреждениями и т. д.

Одним из обязательных признаков официального документа в доктрине уголовного права выделялся признак, касающийся предъявления обязательных требований к оформлению официального документа. Считается, что официальный документ всегда оформляется на соответствующем бланке, на нем должны быть подписи, печати, штампы, обязательные реквизиты. Этот формальный признак выступал гарантом защищенности официальных документов, их легальности.

С переходом на электронный документооборот данный признак утрачивает свое значение и не может рассматриваться в качестве обязательного применительно к цифровым документам. Естественно, что какие-то реквизиты должны быть и у электронного документа. Одним из таких реквизитов является электронная подпись. Существует Федеральный закон, регламентирующий порядок получения и использования электронной подписи. В соответствии со ст. 2 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи», «электронная подпись – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию»⁶. То есть речь идет о реквизите документа, который получен в результате криптографического преобразования и с использованием специального ключа (кода), который позволяет идентифицировать лица, подписавшего документа, а также позволяет проверить наличие или отсутствие искажений в документе с момента его подписания.

Следует отметить, что закон предусматривает два вида подписи: простая и усиленная, которая в свою очередь подразделяется на квалифицированную и неквалифицированную. Для официального документа необходима усиленная квалифицированная электронная подпись. В соответствии со ст. 6 вышеуказанного закона «Информация в электронной форме, подписанная квалифицированной электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, и может применяться в любых правоотношениях в соответствии с законодательством Российской Федерации, кроме случаев, если федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами установлено

⁶ Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи» // СПС «Гарант».

требование о необходимости составления документа исключительно на бумажном носителе»⁷. Для этого вида подписи характерно, что она получена в результате криптографического преобразования информации с использованием ключа электронной подписи; позволяет определить лицо, подписавшее электронный документ; позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания; создается с использованием средств электронной подписи, а также ключ проверки электронной подписи указан в квалифицированном сертификате; для создания и проверки электронной подписи используются средства электронной подписи, получившие подтверждение соответствия требованиям, установленным в соответствии с национальным законодательством⁸. Представляется, что электронная подпись будет единственным реквизитом электронного официального документа.

Сегодня актуальной проблемой является вопрос использования поддельных QR-кодов, дающих людям возможности свободного передвижения. Возникает вопрос о возможности их отнесения к электронным документам. Представляется, что QR-коды к документам мы отнести не можем, так как подобного рода код не отвечает признакам документа, это всего лишь штрих-код, позволяющий быстро считать закодированную информацию.

Отличительной особенностью электронного документа является то, что его восприятие осуществляется только с использованием электронных средств. Данный документ существует только в виде компьютерной информации и ее считывание возможно только при наличии специальных устройств. Форма документа естественным образом определяет и возможности ее хранения, передачи, использования и так называемой подделки.

При квалификации действий с электронными документами проблема заключается не только в отнесении тех или иных электронных документов к числу предметов преступлений, предусмотренных ст. 324 – 327 Уголовного кодекса РФ, но и в признаках их объективной стороны.

Например, сложности представляют вопросы оценки приобретения и сбыта легальных электронных официальных документов, ответственность за которые предусмотрена ст. 325 Уголовного кодекса РФ. Представляется, что электронный официальный документ не может быть предметом по ст. 324 Уголовного кодекса РФ, предусматривающей ответственность за незаконное приобретение или сбыт официальных документов, так как невозможно приобрести легальный электронный официальный документ и, соответственно, нельзя его сбыть. В соответствии с Постановлением Пленума Верховного Суда РФ от 17.12.20 № 43 «О некоторых вопросах судебной практики по делам о преступлениях, предусмотренных ст. 324–327.1 Уголовного кодекса Российской Федерации» «Под незаконным приобретением официальных документов, предоставляющих права или освобождающих от обязанностей, следует понимать действия лица, совершенные им в нарушение установленного порядка выдачи, хранения и иного обращения с такими предметами, в результате которых они поступают во владение этого лица, в том числе их покупку или незаконное получение на безвозмездной основе от других лиц»⁹.

Если электронный официальный документ представлен только в форме электрических сигналов, то в лучшем случае преступник может приобрести или сбыть материальный носитель данной информации, либо электронную версию документа. Также одним из вариантов так называемого приобретения можно рассматривать получение доступа к цифровому документу. Но вряд ли это можно назвать приобретением в том понимании, которое придается ему правоприменительной практикой.

Обращаясь к ст. 325 Уголовного кодекса РФ, предусматривающей ответственность за похищение, повреждение, уничтожение и сокрытие официальных документов, следует отметить, что применительно к настоящим электронным документам возможны только уничтожение и их сокрытие. При этом уничтожение будет выражаться в приведение компьютерной информации в непригодное для использования состояние (когда полностью стирается информация, уничтожаются носители информации). Сокрытие будет выражаться в блокировании информации, то есть ограничении доступа законного пользователя к такой информации, когда владелец электронного документа не может его использовать, предъявлять, передавать, совершать с ним операции в течение длительного периода вре-

⁷ Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи» // СПС «Гарант».

⁸ Там же.

⁹ Постановление Пленума Верховного Суда РФ от 17.12.20 № 43 «О некоторых вопросах судебной практики по делам о преступлениях, предусмотренных ст. 324–327.1 Уголовного кодекса Российской Федерации» // СПС «Гарант».

мени. Но прежде чем его уничтожить или сокрыть, лицо должно получить к нему доступ. Представляется, что такой доступ может быть только незаконным. Исходя из вышеизложенного, получается, что данные действия подпадают и под признаки преступлений в сфере компьютерной информации. Так как электронный документ представлен в виде компьютерной информации, то и все действия с ним будут образовывать незаконные действия с компьютерной информацией. В частности, данные действия подпадают под признаки ст. 272 Уголовного кодекса РФ, предусматривающей ответственность за неправомерный доступ к компьютерной информации.

Также уголовная ответственность предусмотрена за подделку официального документа. Суть подделки заключается во внесении изменений в документы, которые меняют содержательную часть документа, приобретая свойство ложности, не соответствия действительности. Документ на бумажном носителе традиционно подделывают либо путем изготовления нового документа, содержащего ложную информацию, либо путем внесения изменений в настоящий документ, искажающих его действительное содержание. То есть речь идет об изготовлении материального носителя информации либо изменения содержательной части информации путем дописок, подчисток, вытравливания части текста и т. д. Что касается электронного документа, то чтобы внести в него изменения необходимо, во-первых, получить доступ к компьютерной информации, являющейся электронным документом; во-вторых, изменить данную информацию, чтобы при ее считывании электронными устройствами она была в модифицированном виде. Данные действия подпадают под признаки ст. 272 Уголовного кодекса РФ, которая предусматривает ответственность за неправомерный доступ к компьютерной информации.

Возникает вопрос о квалификации действий лица, внесшего изменения в электронный официальный документ. Здесь может быть несколько вариантов квалификации. Во-первых, можно квалифицировать по ст. 272 УК РФ как неправомерный доступ к компьютерной информации, повлекший ее модификацию. Эта квалификация обусловлена тем, что предметом преступления является компьютерная информация, то есть информация, представленная в виде электрических сигналов. Таким образом, и объектом преступления выступают общественные отношения, обеспечивающие безопасность именно компьютерной информации.

Еще одним вариантом квалификации может быть ст. 327 Уголовного кодекса РФ, предусматривающая ответственность за подделку официального документа. В данном случае объектом преступления выступают общественные отношения, обеспечивающие порядок официального документооборота, а предметом, соответственно, официальный документ, представленный в электронном виде.

Возможной уголовно-правовой оценкой будет по совокупности преступлений ст. 272 Уголовного кодекса РФ и ст. 327 Уголовного кодекса РФ. Представляется, что данная квалификация на сегодняшний день будет наиболее приемлемой. Преступник, внося изменения в компьютерную информацию, являющуюся официальным документом, посягает на два объекта преступления и, соответственно, на два предмета. В данном случае информация имеет две составляющие – это форма ее представления и содержание. По форме она будет являться компьютерной, так как представлена в виде электрических сигналов, а по содержанию – она будет являться официальным документом.

Еще одно действие, предусмотренное в ст. 327 Уголовного кодекса РФ, заключается в сбыте поддельного официального документа. Вот здесь возникают проблемы, связанные с понятием сбыта и относимости данного понятия к электронному документу. Под сбытом традиционно понимаются «нарушающие установленный порядок действия по передаче этих документов другим лицам возмездно или безвозмездно»¹⁰, то есть речь идет о любом способе отчуждения (продажа, дарение, обмен). Сбыть поддельный электронный документ в том понимании, которое содержится в Постановлении Пленума Верховного Суда РФ от 17.12.20 № 43 «О некоторых вопросах судебной практики по делам о преступлениях, предусмотренных ст. 324 – 327.1 Уголовного кодекса Российской Федерации», невозможно. Применительно к электронным документам речь может идти о предоставлении доступа к таким документам с целью дальнейшего использования. Для того, чтобы создать поддельный электронный документ необходимо, во-первых, получить доступ к месту его хранения, затем внести изменения в содержание документа либо создать новый, не соответствующий действительности, и после этого можно говорить о предоставлении доступа к нему лица, собирающегося его ис-

¹⁰ Постановление Пленума Верховного Суда РФ от 17.12.20 № 43 «О некоторых вопросах судебной практики по делам о преступлениях, предусмотренных ст. 324–327.1 Уголовного кодекса Российской Федерации» // СПС «Гарант».

пользовать. Поэтому, скорее всего, в таком случае речь будет идти о преступлениях в сфере компьютерной информации, а не о преступлениях против порядка управления.

Отдельного внимания заслуживает проблема квалификации использования заведомо поддельного электронного документа. В п. 10 вышеназванного Постановления Пленума Верховного Суда РФ говорится, что «под использованием заведомо поддельного (подложного) документа понимается его представление (а в случае электронного документа – в том числе посредством применения информационно-телекоммуникационных сетей, включая сеть «Интернет») по собственной инициативе или по требованию уполномоченных лиц и органов в соответствующее учреждение либо должностному лицу, иным уполномоченным лицам в качестве подлинного в целях получения (подтверждения) права, а равно освобождения от обязанности»¹¹. Таким образом, использование электронного документа предполагает применение информационно-телекоммуникационных сетей. Естественно, если документ представлен в виде электрических сигналов, то его представление возможно только с использованием специальных технических средств уполномоченным лицом. Причем сам документ может быть на любом носителе, в том числе на смартфонах, компьютерах, чипах, магнитных лентах и т.д.

Новеллой уголовного законодательства стало установление уголовной ответственности за приобретение, хранение и перевозку поддельных официальных документов в целях их сбыта или использования. Не вдаваясь в подробности целесообразности криминализации данных действий в отношении официальных документов, следует отметить, что квалификация этих действий в отношении электронных документов будет весьма проблематичной.

Приобретение поддельных электронных документов будет заключаться в получении к ним доступа и возможности их дальнейшего использования. В данном случае речь идет не о материальных носителях, а о цифровом формате информации, которая должна содержать заведомо ложные сведения.

Хранение поддельных электронных документов может осуществляться вообще исключительно в цифровом формате (облачные хранилища, флеш-карты и т. д.). Перевозка для таких документов вообще не нужна.

Таким образом, следует признать, что устанавливать уголовную ответственность за приобретение, перевозку и хранение поддельных официальных документов не целесообразно. Во-первых, отсутствует необходимая степень общественной опасности подобного рода деяний. Во-вторых, с практической точки зрения невозможно выявить факты хранения и перевозки электронных официальных документов.

В заключении следует отметить, что действующее уголовное законодательство, предусматривающее ответственность за незаконный оборот официальных документов, требует нового осмысления с учетом меняющихся форм и видов официальных документов. Массовый переход на электронный документооборот приведет и к серьезным проблемам квалификации незаконных действий с электронными документами.

Во-первых, необходимо пересмотреть традиционные подходы к установлению уголовной ответственности за незаконный оборот официальных документов, унифицировав основные понятия и признаки для разных документов. Кроме того, на наш взгляд, следует декриминализировать приобретение, перевозку и хранение поддельных официальных документов, а также использование заведомо поддельных документов. Это обусловлено невысокой степенью общественной опасности рассматриваемых деяний и сложностью их выявления.

Во-вторых, необходимо решить вопрос квалификации и разграничения преступлений в сфере незаконного оборота официальных документов и преступлений в сфере компьютерной информации. Электронный документ подпадает и под признаки предмета преступлений против порядка управления, и под признаки компьютерных преступлений. Одним из возможных вариантов разрешения этой проблемы можно предложить квалифицировать незаконные действия с электронными документами как преступления в сфере компьютерной информации, и отнести электронные официальные документы к критической информационной инфраструктуре, ответственность за неправомерное воздействие на которую предусмотрена ст. 274.1 Уголовного кодекса РФ.

Поступила в редакцию 21.11.2021

¹¹ Постановление Пленума Верховного Суда РФ от 17.12.20 № 43 «О некоторых вопросах судебной практики по делам о преступлениях, предусмотренных ст. 324–327.1 Уголовного кодекса Российской Федерации» // СПС «Гарант».

Стяжкина Светлана Александровна, кандидат юридических наук,
доцент кафедры уголовного права и криминологии
ФГБОУ ВО «Удмуртский государственный университет»
426034, Россия, г. Ижевск, ул. Университетская, 1 (корп. 4)
E-mail: styazhkina.sv@yandex.ru

S.A. Styazhkina

ELECTRONIC DOCUMENT AS A SUBJECT OF CRIMINAL LAW PROTECTION

DOI: 10.35634/2412-9593-2022-32-1-178-184

The article is devoted to the problem of criminal legal protection of electronic documents. The information environment provides ample space for documentation, but also creates risks of safe transfer, storage of documents, their protection from unlawful modification, special attention should be paid to the criminal legal protection of official electronic documents. It should be noted that the current criminal legislation regulating the issues of liability for illegal trafficking of official documents does not quite correspond to modern realities. The Criminal Code operates with concepts and terms that were focused on paper document flow. Firstly, it is necessary to revise the traditional approaches to establishing criminal liability for illegal trafficking in official documents, unifying the basic concepts and features for different documents. In addition, the acquisition, transportation and storage of counterfeit ofs should be decriminalized.

Keywords: electronic document, forgery of documents, illegal sale of documents, official document, use of a deliberately forged document, computer information, illegal access to computer information, electronic document management, electronic signature.

Received 21.11.2021

Styazhkina S.A., Candidate of Law, Associate Professor
Udmurt State University
Universitetskaya st., 1/4, Izhevsk, Russia, 426034
E-mail: styazhkina.sv@yandex.ru