МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тольяттинский государственный университет»
Институт права
(наименование института полностью)

Кафедра «Гражданское право и процесс»
(наименование)

40.04.01 Юриспруденция
(код и наименование направления подготовки)

Правовое обеспечение предпринимательской деятельности
(направленность (профиль))

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА (МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ)

на тему «Правовое регулирование электронной подписи в предпринимательской деятельности»

Обучающийся В.А. Алешинцова
(Инициалы Фамилия) (личная подпись)

Научный руководитель канд. пед. наук, доцент, О.А. Воробьёва
(ученая степень (при наличии), ученое звание (при наличии), Инициалы Фамилия)

Тольятти 2024

Оглавление

Введение

В современных реалиях процесс цифровизации проникает во все сферы жизни общества. Сфера предпринимательства не является исключением и постоянно модернизируется под влиянием новых технологий. Актуальность темы диссертационного исследования обусловлена тем, что цифровая подпись является инструментом осуществления предпринимательской деятельности в условиях постоянной цифровизации. С учетом того обстоятельства, что данный инструмент является относительно новым для отечественного законодательства, его правовому регулированию характерен ряд проблемных аспектов.

Вопросы правового регулирования электронной подписи нашли свое отражение в исследованиях И.В. Аристархова, Ф.Г. Бобрицкого, М.В. Климовича, Ю.М. Кукариной, А.А. Суворова, Р.О. Халикова, С.В. Щёголевой, Е.Ю. Шишаевой.

В основе диссертационного исследования лежат труды следующих ученых-юристов: А.Г. Аниной, А.А. Асеева, А.Д. Бабанцева, А.В. Билокапича, Д.Г. Билаловой, Н.С. Волковой, О.А. Гагауза, Д.А. Гуляева, М.М, Дарькиной, М.Н. Дмитриева, А.В. Ефремовой, А.А. Лаврушкиной, В.В, Митрофанова, В.В. Проценко, Н.И. Соловяненко, С.Ю. Стародумовой, Н.А. Титова, Е.Е. Фроловой, В.В. Хоружий, С.С. Шестопала, А.А. Шмагун, А.В. Щепотина, И.О. Щуки.

Объект исследования – общественные отношения, складывающиеся в рамках реализации механизма правового регулирования электронной подписи в предпринимательской деятельности.

Предмет исследования – правовые нормы, регулирующие вопросы использования электронной подписи, а также материалы судебной практики и периодической печати, в которых отражены результаты исследований на тему правового регулирования электронной подписи.

Цель исследования заключается в выявлении актуальных проблем правового регулирования цифровой подписи в предпринимательской деятельности.

Определив цель исследования, мы можем выделить следующие задачи, необходимые для ее достижения:

- рассмотреть понятие, сущность и особенности правового регулирования электронной подписи в отечественном законодательстве;
- охарактеризовать процедуру получения электронной подписи;
- проанализировать особенности применения субъектами предпринимательской деятельности электронной подписи;
- изучить особенности защиты электронной подписи в процессе осуществления предпринимательской деятельности;
- проанализировать проблемные аспекты правового регулирования электронной подписи;
- проанализировать зарубежный опыт правового регулирования электронной подписи.

Методологическую основу данного исследования составляют общенаучные и частнонаучные методы. В группу общенаучных методов познания входят: синтез, анализ, сравнение, дедукция, индукция. В группу используемых частнонаучных методов входят: формально-юридический метод, сравнительно-правовой метод.

Проведенное диссертационное исследование позволило сформулировать и обосновать следующие выводы, выносимые автором на защиту:

- поскольку государство представляет собой единую систему, которую мы в некоторой степени можем рассматривать в качестве единой корпорации, то с технической точки зрения, вполне возможно создать общую экосистему информационных ресурсов, работающих в рамках

одних и тех же алгоритмов. Это в свою очередь позволит создать единую электронную подпись, которая будет использоваться предпринимателем при любых взаимодействиях с органами государственной и муниципальной власти.

- вопросы ответственности нарушение законодательства об электронной подписи, а также неправомерного получения доступа к электронной подписи недостаточно раскрыты законодателем. Мы считаем необходимым ввести уголовную ответственность за нарушение законодательства в сфере электронной подписи, а также ужесточить санкции, предусмотренные в рамках административной ответственности.
- проведенный анализ зарубежного опыта правового регулирования электронной подписи в предпринимательской деятельности позволяет выделить авторскую классификацию подходов влияния государства на правовое регулирование электронной подписи: минималистичный подход; предписывающий подход; двухфакторный подход, смешанный подход.

Теоретическую основу исследования составили монографическая и учебная литература по предпринимательскому праву, научные публикации, а также диссертационные исследования, посвященные правовому регулированию электронной подписи в отечественном законодательстве.

Нормативную базу исследования составили следующие документы: Гражданский кодекс Российской Федерации, Гражданский процессуальный кодекс Российской Федерации, Кодекс Российской Федерации об административных правонарушениях, Уголовный кодекс Российской Федерации, Федеральный закон «Об организации предоставления государственных и муниципальных услуг», Федеральный закон «Об электронной подписи», Федеральный закон «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд», Федеральный закон «О проведении эксперимента по

установлению специального налогового режима «Налог на профессиональный доход».

Эмпирическую основу исследования составляют материалы судебной практики.

Гипотеза диссертационного исследования: «В условиях стремительной цифровизации отечественной экономики правовому регулированию электронной подписи в предпринимательской деятельности характерен ряд существенных недостатков».

Научная новизна исследования заключается в том, что теоретические выводы и положения могут быть использованы для дальнейшего научного исследования проблем правового регулирования электронной подписи в предпринимательской деятельности.

Теоретическая значимость работы заключается в том, что сформулированные в результате проведенного исследования выводы углубляют научные знания о правовом регулировании электронной подписи и могут служить основой для дальнейших исследований по данной теме.

Практическая значимость заключается в том, что идеи и рекомендации, представленные в данной работе, могут быть использованы в учебном процессе при подготовке студентов-бакалавров. В частности, материалы данного исследования, могут учитываться при разработке курса дисциплины «Предпринимательское право».

Отдельные выводы диссертационного исследования были использованы автором при подготовке материалов для публикации в научном журнале «Студенческий».

Структура диссертационного исследования определена введением, тремя главами, заключением, а также списком используемой литературы и используемых источников.

Глава 1 Теоретические основы исследования электронной подписи в предпринимательской деятельности

1.1 Понятие и правовое регулирование электронной подписи в законодательстве Российской Федерации

Рассматривая ту или иную категорию, стремясь определить ее сущность и назначение, в первую очередь необходимо подвергнуть анализу понятие, отражающее его основные признаки. В этой связи необходимо обратиться к нормативно-правовому акту, который предусматривает легальное определение понятия «электронная подпись». Таким нормативно-правовым актом является Федеральный закон «Об электронной подписи». Во второй статье указанного закона раскрываются основные понятия, разъяснение которых необходимо для понимания особенностей регулируемых правоотношений. Законодатель использует следующее определение для раскрытия интересующего нас понятия. «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» [31].

Анализируя законодательное определение, мы можем отметить, что законодатель весьма ограниченно раскрывает понятие электронной подписи. К числу законодательных признаков мы можем отнести следующие характеристики. Во-первых, электронная подпись представляет собой информацию, то есть, определенный набор данных. Во-вторых, информация-подпись имеет активную фазу, когда она присоединяется к другой подписываемой информации. В-третьих, основной целью электронной подписи является подтверждение подлинности личности лица, которое подписывает информацию.

Помимо косвенно предусмотренных законом признаков, мы можем обозначить следующие характеристики электронной подписи. Следующий

признак – электронная подпись основана на криптографических алгоритмах. Особая система шифрования позволяет генерировать специальные ключи при каждом использовании. Сама технология выглядит следующим образом. «Закрытый и открытый ключи генерируются одновременно, при получении подписи в специализированном удостоверяющем центре. После того, как центр подтверждает личность человека и проверяет наличие у него закрытого ключа, он включает в сертификат и открытый ключ. Закрытый ключ известен только владельцу – он хранится на специальном токене и находится под защитой пин-кода» [11, с. 98]. Использование криптографических алгоритмов в процессе создания и использования электронной подписи повышает ее надежность в сравнении с обычной рукописной подписью. В этой связи отдельные авторы указывают на то, что использование электронной подписи подразумевает презумпцию авторства данной подписи [7, с. 299]. Презумпция авторства в данном случае подразумевает, что использование электронной подписи означает, использование ее конкретным лицом – автором подписи. То есть, автор подписи в случае несогласия с тем фактом, что была использована его электронная подпись, должен предоставить существенные доводы, подтверждающие факт неправомерного доступа к его зашифрованным данным.

Следует обратить внимание на то обстоятельство, что законодатель выделяет несколько видов электронной подписи. В статье пятой Федерального закона «Об электронной подписи» упомянуты следующие виды подписей:

- «простая электронная подпись;
- неквалифицированная электронная подпись;
- квалифицированная электронная подпись» [31].

Рассмотрим каждый из обозначенных видов электронных подписей.

«Простой электронной подписью является электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом» [31]. Как правило, простая электронная подпись используется при использовании

банковских приложений, сервиса госуслуги и так далее. Среди всех видов электронных подписей простая подпись имеет наименее защищенный характер, поэтому в большей степени ставит под сомнение авторство лица, использующего подпись. Учитывая низкую защищенность данного вида подписи, при работе с охраняемыми законом сведениями (коммерческая тайна, государственная тайна, тайна усыновления и так далее) простая электронная подпись не используется.

«Электронный документ считается подписанным простой электронной подписью при выполнении в том числе одного из следующих условий:

- простая электронная подпись содержится в самом электронном документе;
- ключ простой электронной подписи применяется в соответствии с правилами, установленными оператором информационной системы, с использованием которой осуществляются создание и (или) отправка электронного документа, и в созданном и (или) отправленном электронном документе содержится информация, указывающая на лицо, от имени которого был создан и (или) отправлен электронный документ» [31].

Простая электронная подпись имеет существенные недостатки. Например, заключая договор при помощи простой электронной подписи путем передачи кода из смс оператору банка, юридический автор подписи может даже не получить для ознакомления полный текст договора при его заключении. Более того, это настолько незащищенный способ, что пользователь в принципе может не знать о том, что от его имени заключается договор и на него возлагаются определенные обязательства. В качестве примера рассмотрим материал из судебной практики. Так, ФИО, зайдя на сайт госуслуг обнаружил, что в отношении него есть судебный приказ о взыскании задолженности на сумму 39125 рублей в пользу ООО МФК «Займер». ФИО обратился в суд с исковым требованием о признании договора незаключенным, а также о запрете на использование персональных данных. В обосновании

ФИО было указано, что никакого договора он не заключал, документы не подписывал, денежные средства не получал. Судом было отмечено, что заемщик заключил договор с использованием кода из смс. Проанализировав материалы дела, суд принял решение об удовлетворении исковых требований, поскольку информация, полученная в ходе заключения договора является недостоверной [24]. Таким образом, мы делаем вывод о высокой уязвимости простой электронной подписи, поскольку технологии развиты до такого уровня, что на сегодняшний день имеется возможность дублировать телефонные номера и получать поступающую на них информацию. Кроме того, нельзя забывать о постоянных утечках персональных данных, которые включают в себя информацию, вплоть до паспортных данных, которые злоумышленник может использовать при заключении кредитного договора. На наш взгляд, законодателю необходимо более подробно регламентировать вопрос заключения договоров при помощи электронной подписи. В частности, можно закрепить необходимость пройти аутентификацию при заключении договора, подписываемого простой электронной подписью, при помощи видеозвонка с сотрудником банка и предоставления документа, удостоверяющего личность. Таким образом, удастся усилить меры безопасности и доподлинно установить авторство простой электронной подписи.

В свою очередь, «неквалифицированной электронной подписью является электронная подпись, которая:

- 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» [31].

Данный вид подписи отличается относительной безопасностью, поскольку позволяет получить данные об авторстве лица, которое подписало

документ. А.Г. Аннин указывает на то, что такой степени идентификации удается достигнуть за счет криптографического алгоритма, который шифрует информацию, составляющую электронную подпись [1, с. 161]. Здесь стоит добавить, что криптографический алгоритм не только позволяет максимально индивидуализировать информацию, но и защитить ее от несанкционированного получения доступа от посторонних лиц. Как правило, данный вид подписи используется в сфере налогообложения при обращении в ФНС с использованием личного кабинета в сети «Интернет».

Говоря об особенностях неквалифицированной электронной подписи, стоит отметить, что порядок ее получения куда более сложен, если сравнивать с простой подписью. Однако, более детально вопросы получения электронной подписи будут рассмотрены нами в следующем параграфе. Другая особенность неквалифицированной подписи обусловлена тем обстоятельством, что при создании такой подписи используются любые криптографические алгоритмы, даже те, которые не были одобрены ФСБ.

«Квалифицированной электронной подписью является электронная подпись, которая соответствует всем признакам неквалифицированной электронной подписи и следующим дополнительным признакам:

- ключ проверки электронной подписи указан в квалифицированном сертификате;
- для создания и проверки электронной подписи используются средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом» [31].

Анализируя отечественное законодательство, можно отметить, что в правоотношениях в сфере документооборота преимущественно предусмотрено использование квалифицированной электронной подписи. Так, в статье четвертой Федерального закона «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» предусмотрено следующее. «Использование

усиленной квалифицированной электронной подписи для подписания электронных документов» [32] является основой обеспечения контрактной системы. В статье 131-ой Гражданского-процессуального кодекса предусмотрен особый порядок подачи документов в суд в электронной форме с обязательным применением усиленной квалифицированной электронной подписи [10]. Обращаясь к статье шестнадцатой Федерального закона «Об организации предоставления государственных и муниципальных услуг», установлено: «создание заверенных усиленной квалифицированной подписью уполномоченного должностного лица многофункционального центра электронных дубликатов документов и информации (преобразование в электронную форму документов и информации на бумажном носителе с сохранением их содержания и (при наличии) реквизитов), необходимых для предоставления государственных и муниципальных услуг» [30]. Таким образом, подтверждается заявленный выше тезис относительно приоритета использования квалифицированной электронной подписи в электронном документообороте.

«В российском праве прослеживается общая тенденция к интенсификации цифрового взаимодействия на основе безусловного правового признания электронных документов, подписанных квалифицированной электронной подписью» [25, с. 237]. Такое положение вещей можно объяснить тем, что на сегодняшний день отечественная экономика подвержена стремительной цифровизации, обусловленной стремительным развитием технологий. Теперь возникновение правоотношений не зависит от места нахождения сторон, бизнес можно вести, находясь в разных концах страны и даже целого мира. В связи с этим законодатель должен быть ответить на стремительно набирающий актуальность запрос на создание механизмов правового регулирования электронной подписи. Законодатель предусмотрел несколько вариантов такой подписи. Имея альтернативу, участники правоотношений делают свой выбор в пользу наиболее защищенного способа подтверждения своей воли в

электронной форме. Таким образом, они стремятся избежать неблагоприятных последствий, которые могут быть вызваны использованием менее защищенных видов электронной подписи.

Проводя анализ практической ценности электронной подписи в документообороте, Н.Н. Магомедов выделяет следующие преимущества:

- «позволяет удаленно вести документооборот;
- экономит время, не надо выезжать куда - либо, чтобы подписать документы;
- позволяет получить государственные услуги удаленно;
- нельзя вносить изменения в документ, подписанным квалифицированной подписью, т.к это отразится на расшифровке;
- взломать квалифицированную подпись практически невозможно. При ее потере либо же, когда она попадает в руки недобро владельцам, то можно обратиться с заявлением в удостоверяющий центр, который выдал подпись, чтобы отозвать сертификат;
- можно использовать в любых операциях с электронными документами. Квалифицированной подписи доверяют арбитражные суды и ФНС, поэтому с помощью подписью чаще всего подписывают электронные счета – фактуры, договоры, налоговые декларации» [5, с. 7].

В целом мы уже указывали на данные положительные аспекты. Отдельно можно отметить, что электронная подпись делает доступными получение государственных и муниципальных услуг. Особую значимость данный аспект приобретает с точки зрения социальной сферы, поскольку электронная подпись обеспечивает доступность услуг для социальных групп, находящихся в зоне риска (инвалиды, пенсионеры, многодетные семьи). Представители заявленных групп обладают ограниченной возможностью лично посетить учреждения и реализовать свое право на получение тех или

иных услуг, поэтому электронную подпись можно рассматривать как важный инструмент поддержки наименее защищенных социальных групп.

Однако, электронная подпись характеризуется не только положительными чертами, равно как и любой другой правовой конструкции ей характерен ряд недостатков:

- «первый недостаток электронной подписи проявляется в том, что ее ежегодно нужно обновлять и оплачивать, т.к она выдается только на год;
- кроме подписи, необходимо установить программное обеспечение, которое даст возможность подписать документы в электронном виде;
- другая проблема заключается в том, что установить подпись с нуля технически сложно. Сперва нужно скачать и установить КриптоПро CSP, которая позволяет «установить» подпись на компьютер, а потом программу, с помощью которого нужно подписывать документы (например, КриптоПро АРМ, Контур.Крипто);
- если же, пользователю нужно работать в браузере (например, для госзакупок либо для подачи документов через госуслуги, в налоговую), то в свою очередь необходимо установить специальный браузерный плагин КриптоПро ЭЦП Browser plug-in;
- после каждой установки программ, обязательно нужно перезагрузить компьютер;
- помимо этого, подпись не работает на Mac, для этого устанавливают Windows, либо программу которая позволяет работать с электронной подписью» [40, с. 3].

Анализируя заявленные автором недостатки, можно отметить, что использование электронной подписи (за исключением простой электронной подписи) требует определенных технических знаний, что в некоторой степени повышает порог вхождения для использования электронной подписи. Кроме того, отсутствие возможности без дополнительного программного

обеспечения использовать электронную подпись на операционной системе IOS создает некоторые сложности и может расцениваться как дискриминационный фактор данного инструмента. Однако, в актуальных условиях санкционного давления и отказа иностранных компаний вести деятельность на территории Российской Федерации, такие доводы неуместны. Использование техники на базе операционной системе IOS создает определенную угрозу сохранности данных, поскольку они находятся на серверах компании, относящейся к недружественным государствам. В связи с этим на данный момент мы не видим необходимости разработки программного обеспечения, которое позволит беспрепятственно использовать электронную подпись на базе устройств с операционной системой IOS.

В завершении темы данного параграфа мы можем сделать следующие выводы.

Во-первых, легальное определение понятия электронная подпись предусмотрена в статье второй Федерального закона «Об электронной подписи». К числу признаков, характеризующих сущность и назначение электронной подписи, мы можем отнести следующие аспекты. Во-первых, электронная подпись представляет собой информацию, то есть, определенный набор данных. Во-вторых, информация-подпись имеет активную фазу, когда она присоединяется к другой подписываемой информации. В-третьих, основной целью электронной подписи является подтверждение подлинности личности лица, которое подписывает информацию. В-четвертых, электронная подпись основана на криптографических алгоритмах. Особая система шифрования позволяет генерировать специальные ключи при каждом использовании. Кроме того, для электронной подписи характерна презумпция авторства. Использование электронной подписи означает, использование ее конкретным лицом – автором подписи. То есть, автор подписи в случае несогласия с тем фактом, что была использована его электронная подпись, должен предоставить существенные доводы, подтверждающие факт неправомерного доступа к его зашифрованным данным.

Во-вторых, мы делаем вывод о высокой уязвимости простой электронной подписи, поскольку технологии развиты до такого уровня, что на сегодняшний день имеется возможность дублировать телефонные номера и получать поступающую на них информацию. Кроме того, нельзя забывать о постоянных утечках персональных данных, которые включают в себя информацию, вплоть до паспортных данных, которые злоумышленник может использовать при заключении кредитного договора. На наш взгляд, законодателю необходимо более подробно регламентировать вопрос заключения договоров при помощи электронной подписи. В частности, можно закрепить необходимость пройти аутентификацию при заключении договора, подписываемого простой электронной подписью, при помощи видеозвонка с сотрудником банка и предоставления документа, удостоверяющего личность. Таким образом, удастся усилить меры безопасности и доподлинно установить авторство простой электронной подписи.

В-третьих, электронная подпись делает доступными получение государственных и муниципальных услуг. Особую значимость данный аспект приобретает с точки зрения социальной сферы, поскольку электронная подпись обеспечивает доступность услуг для социальных групп, находящихся в зоне риска (инвалиды, пенсионеры, многодетные семьи). Представители заявленных групп обладают ограниченной возможностью лично посетить учреждения и реализовать свое право на получение тех или иных услуг, поэтому электронную подпись можно рассматривать как важный инструмент поддержки наименее защищенных социальных групп.

1.2 Особенности получения электронной подписи

Оформление электронной подписи представляет собой специальную процедуру, осуществляется по инициативе автора подписи или уполномоченного им лица. Для получения подписи необходимо обратиться в удостоверяющий центр или в иные уполномоченные организации. Например,

если подпись требуется для сервиса Госуслуги, то обратиться необходимо в МФЦ. Получить электронную подпись для осуществления банковских операций можно, обратившись в отделение банка [14, с. 189]. Получение неквалифицированной и квалифицированной электронной подписи происходит в удостоверяющем центре. Разница здесь заключается в том, что для получения квалифицированной подписи требуется обращаться в центр, который в соответствии с нормами отечественного законодательства получил аккредитацию.

Правовой статус удостоверяющего центра закреплен в статье 13-ой Федерального закона «Об электронной подписи». В ней закреплены полномочия, обязанности, вопросы ответственности, а также функции удостоверяющего центра. Обращаясь в удостоверяющий центр, заявителю необходимо предоставить документы, подтверждающие его личность. «Идентификация заявителя проводится при его личном присутствии или посредством идентификации заявителя без его личного присутствия с использованием квалифицированной электронной подписи при наличии действующего квалифицированного сертификата либо посредством идентификации заявителя – гражданина Российской Федерации с применением информационных технологий без его личного присутствия путем предоставления информации, указанной в документе, удостоверяющем личность гражданина Российской Федерации за пределами территории Российской Федерации, содержащем электронный носитель информации с записанными на нем персональными данными владельца паспорта, включая биометрические персональные данные, или путем предоставления сведений из единой системы идентификации и аутентификации и информации из единой биометрической системы в порядке, установленном» [31]. По большей части дальнейшие действия имеют преимущественно технический характер, что обусловлено сущностью и двойственной природой электронной подписи.

Перед началом работы сотрудник удостоверяющего центра должен провести следующие технические мероприятия:

- «проверить наличие актуальной версии программного обеспечения КриптоПро УЦ 2.0, которое готово к эксплуатации в штатном режиме функционирования;
- оператор удостоверяющего центра должен иметь ключевой носитель, предоставленный пользователем. Пользователь должен предоставить оператору УЦ ключевой носитель, соответствующий требованиям информационной безопасности и сертифицированный во ФСТЭК России;
- ключевой носитель учитывается в журнале установленной формы;
- на автоматизированном рабочем месте оператора удостоверяющего центра должны быть установлены и настроены средства защиты информации (антивирус, средство контроля доступа, резервное копирование и т.д.), а также настроены параметры подключения к Центру регистрации» [13, с. 129].

После того, как все указанные мероприятия будут выполнены, оператору необходимо осуществить ряд технических действий при помощи упомянутого выше программного обеспечения. В результате действий оператора будет подготовлен и выпущен сертификат, который распечатывается в двух экземплярах. Каждый из сертификатов должен содержать в себе персональные данные заявителя. Кроме того, на сертификате отображается номер ключа и сгенерированный при помощи рандомайзера (программы, которая при помощи алгоритмов выдает случайную последовательность чисел) ПИН код, который будет использоваться заявителем в дальнейшем. Требования к содержанию сертификата предусмотрены частью второй статьи 14-ой и частью второй статьи 17-ой Федерального закона «Об электронной подписи». В сертификате отражаются следующие данные:

- «уникальный номер сертификата ключа проверки электронной подписи, даты начала и окончания срока действия такого сертификата;

- фамилия, имя и отчество (если имеется) – для физических лиц, наименование и место нахождения – для юридических лиц или иная информация, позволяющая идентифицировать владельца сертификата ключа проверки электронной подписи;
- уникальный ключ проверки электронной подписи;
- наименование используемого средства электронной подписи и (или) стандарты, требованиям которых соответствуют ключ электронной подписи и ключ проверки электронной подписи;
- наименование удостоверяющего центра, который выдал сертификат ключа проверки электронной подписи;
- идентификатор, однозначно указывающий на то, что идентификация заявителя при выдаче сертификата ключа проверки электронной подписи проводилась либо при его личном присутствии, либо без его личного присутствия;
- срок действия ключа электронной подписи, соответствующего уникальному ключу проверки электронной подписи, содержащемуся в данном квалифицированном сертификате;
- страховой номер индивидуального лицевого счета и идентификационный номер налогоплательщика владельца квалифицированного сертификата - для физического лица либо идентификационный номер налогоплательщика владельца квалифицированного сертификата - для юридического лица» [31].

После этого один из сертификатов передается пользователю, что подтверждается его физической подписью в специальном журнале учета. Другой сертификат остается в удостоверяющем центре и помещается в архив.

Как правило, причинами отказа в предоставлении доступа к электронной подписи являются следующие обстоятельства:

- отсутствие документов, подтверждающих личность заявителя, либо отказ предоставить необходимые документы уполномоченному лицу;
- информация, содержащаяся в предоставленных заявителем документах, не соответствует сведениям, содержащимся в базах данных;
- отсутствие носителя информации, на который может быть записана информация, составляющая электронную подпись;
- несоответствие носителей установленным требованиям.

Помимо уже указанных обстоятельств, к числу «типичных оснований» для отказа в получении электронной подписи, опираясь на практику, мы можем отнести следующее формальное основание. Отказ может быть мотивирован качеством отсканированных документов, то есть, информация в представленных документах будет достоверной, но в силу качества скана часть информации будет нечитаемой, либо возникнут сомнения в подлинности печатей или подписей на документе по причине ненадлежащего сканирования [21]. Таким образом, мы можем разделить основания отказа в предоставлении электронной подписи на три основных группы: фактические, технические и формальные. Фактические основания определяются тем, что заявитель предоставил необходимые сведения, либо предоставил недостоверные сведения. Технические основания отказа определяются тем обстоятельством, что заявитель не имеет необходимого технического оснащения, либо его техническое оснащение не соответствует заявленным требованиям. Формальные основания определяются тем, что представленные документы не соответствуют форме и правилам документооборота.

Завершая обсуждение по теме данной главы, мы можем сделать следующие выводы по вопросу теоретических основ исследования электронной подписи в предпринимательской деятельности.

Во-первых, легальное определение понятия электронная подпись предусмотрена в статье второй Федерального закона «Об электронной

подписи». К числу признаков, характеризующих сущность и назначение электронной подписи, мы можем отнести следующие аспекты. Во-первых, электронная подпись представляет собой информацию, то есть, определенный набор данных. Во-вторых, информация-подпись имеет активную фазу, когда она присоединяется к другой подписываемой информации. В-третьих, основной целью электронной подписи является подтверждение подлинности личности лица, которое подписывает информацию. В-четвертых, электронная подпись основана на криптографических алгоритмах. Особая система шифрования позволяет генерировать специальные ключи при каждом использовании. Кроме того, для электронной подписи характерна презумпция авторства. Использование электронной подписи означает, использование ее конкретным лицом – автором подписи. То есть, автор подписи в случае несогласия с тем фактом, что была использована его электронная подпись, должен предоставить существенные доводы, подтверждающие факт неправомерного доступа к его зашифрованным данным.

Во-вторых, мы делаем вывод о высокой уязвимости простой электронной подписи, поскольку технологии развиты до такого уровня, что на сегодняшний день имеется возможность дублировать телефонные номера и получать поступающую на них информацию. Кроме того, нельзя забывать о постоянных утечках персональных данных, которые включают в себя информацию, вплоть до паспортных данных, которые злоумышленник может использовать при заключении кредитного договора. На наш взгляд, законодателю необходимо более подробно регламентировать вопрос заключения договоров при помощи электронной подписи. В частности, можно закрепить необходимость пройти аутентификацию при заключении договора, подписываемого простой электронной подписью, при помощи видеозвонка с сотрудником банка и предоставления документа, удостоверяющего личность. Таким образом, удастся усилить меры безопасности и доподлинно установить авторство простой электронной подписи.

В-третьих, электронная подпись делает доступными получение государственных и муниципальных услуг. Особую значимость данный аспект приобретает с точки зрения социальной сферы, поскольку электронная подпись обеспечивает доступность услуг для социальных групп, находящихся в зоне риска (инвалиды, пенсионеры, многодетные семьи). Представители заявленных групп обладают ограниченной возможностью лично посетить учреждения и реализовать свое право на получение тех или иных услуг, поэтому электронную подпись можно рассматривать как важный инструмент поддержки наименее защищенных социальных групп.

Кроме того, получение электронной подписи требует от заявителя обращения в соответствующее учреждения (в зависимости от цели получения электронной подписи) и предоставления ряда документов. Проанализировав практику, мы можем разделить основания отказа в предоставлении электронной подписи на три основных группы: фактические, технические и формальные. Фактические основания определяются тем, что заявитель предоставил необходимые сведения, либо предоставил недостоверные сведения. Технические основания отказа определяются тем обстоятельством, что заявитель не имеет необходимого технического оснащения, либо его техническое оснащение не соответствует заявленным требованиям. Формальные основания определяются тем, что представленные документы не соответствуют форме и правилам документооборота.

Глава 2 Особенности применения и защита электронной подписи в процессе осуществления предпринимательской деятельности

2.1 Особенности применения субъектами предпринимательской деятельности электронной подписи

Легальное определение понятия «предпринимательская деятельность» мы можем найти, обратившись к статье второй Гражданского кодекса, где законодатель раскрывает сущность и характер отношений, регулируемых нормами гражданского права. Предпринимательская деятельность – «самостоятельная, осуществляемая на свой риск деятельность, направленная на систематическое получение прибыли от пользования имуществом, продажи товаров, выполнения работ или оказания услуг» [8]. Анализируя современную практику осуществления предпринимательской деятельности, мы можем утверждать, что на сегодняшний день предпринимательская деятельность может осуществляться в следующих формах:

- путем образования юридического лица;
- путем регистрации статуса индивидуального предпринимателя;
- путем регистрации в качестве самозанятого гражданина.

При анализе содержания Федерального закона «Об электронной подписи» мы видим, что законодатель выделяет отдельные статьи, посвященные «использованию квалифицированной электронной подписи при участии в правоотношениях физического лица, использование квалифицированной электронной подписи при участии в правоотношениях юридических лиц, лиц, замещающих государственные должности Российской Федерации, государственные должности субъектов Российской Федерации, должностных лиц государственных органов, органов местного самоуправления, их подведомственных организаций, а также нотариусов, использование квалифицированной электронной подписи при участии в правоотношениях индивидуальных предпринимателей» [31]. Здесь мы можем

наблюдать, что законодатель не актуализировал положения закона в соответствии с относительно новой формой предпринимательской деятельности (самозанятостью) и не закрепил отдельную статью, посвященную использованию квалифицированной электронной подписи в правоотношениях самозанятых граждан. С одной стороны, такое решение можно аргументировать тем, что самозанятым является обычное физическое лицо, которое не является индивидуальным предпринимателем. Кроме того, осуществление самозанятости в форме предпринимательской деятельности является экспериментом, который продлится в течении 10 лет с момента начала эксперимента [33]. С другой стороны, на сегодняшний день мы не видим предпосылок к тому, чтобы законодатель упразднил данную форму предпринимательской деятельности, поскольку с ее помощью удалось вывести часть экономики из теневого сектора в «легальное поле» [35, с. 154]. Можно также отметить, что физическое лицо, обладающее статусом самозанятого, является участником предпринимательских отношений, а также имеет особый статус для налоговых органов. В связи с этим мы видим необходимость отдельно закрепить в Федеральном законе «Об электронной подписи» статью, закрепляющую особенности использование квалифицированной электронной подписи при участии в правоотношениях самозанятых граждан.

Вопросам использования квалифицированной электронной подписи в правоотношениях с участием индивидуальных предпринимателей посвящена статья 17.3 Федерального закона «Об электронной подписи». «В случае использования квалифицированной электронной подписи при участии в правоотношениях индивидуальных предпринимателей:

- применяется квалифицированная электронная подпись индивидуального предпринимателя, квалифицированный сертификат которой выдается удостоверяющим центром федерального органа исполнительной власти, уполномоченного на осуществление государственной регистрации юридических лиц, в установленном уполномоченным федеральным органом порядке с

указанием также физического лица, являющегося индивидуальным предпринимателем, в качестве владельца данного сертификата. В случае, если квалифицированная электронная подпись применяется только для автоматического создания электронной подписи в электронном документе и (или) автоматической проверки электронной подписи в электронном документе, используется только квалифицированная электронная подпись индивидуального предпринимателя, который осуществляет функции оператора соответствующей информационной системы. При этом квалифицированный сертификат, выдаваемый такому индивидуальному предпринимателю, содержит указание только на индивидуального предпринимателя в качестве владельца данного сертификата (без указания в качестве владельца квалифицированного сертификата также на физическое лицо, являющееся индивидуальным предпринимателем). Такой квалифицированный сертификат создается и выдается удостоверяющим центром федерального органа исполнительной власти, уполномоченного на осуществление государственной регистрации юридических лиц, в установленном уполномоченным федеральным органом порядке. При этом распорядительным актом индивидуального предпринимателя определяется физическое лицо, ответственное за автоматическое создание и (или) автоматическую проверку электронной подписи в информационной системе, и лицо, ответственное за содержание информации, подписываемой данной электронной подписью. В случае отсутствия указанного распорядительного акта лицом, ответственным за автоматическое создание и (или) автоматическую проверку электронной подписи в информационной системе, является индивидуальный предприниматель;

- в случае, если от имени индивидуального предпринимателя действует его представитель (физическое лицо, иной индивидуальный предприниматель или юридическое лицо), уполномоченный действовать от имени индивидуального предпринимателя на основании доверенности, выданной таким индивидуальным предпринимателем в соответствии с гражданским законодательством Российской Федерации, электронный документ подписывается квалифицированной электронной подписью представителя (физического лица, иного индивидуального предпринимателя или юридического лица) и одновременно представляется выданная индивидуальным предпринимателем доверенность. Указанная доверенность в электронной форме должна быть подписана квалифицированной электронной подписью, указанной в пункте 1 настоящей статьи, или квалифицированной электронной подписью лица, которому выдана доверенность с правом передоверия, или квалифицированной электронной подписью нотариуса в случае, если доверенность удостоверена нотариусом. В случае, если указанная доверенность выдана в порядке передоверия, представляется также доверенность, допускающая возможность указанного передоверия, подписанная квалифицированной электронной подписью, указанной в пункте 1 настоящей статьи, или квалифицированной электронной подписью нотариуса, если доверенность удостоверена нотариусом. Представление доверенности осуществляется посредством ее включения в пакет электронных документов, если иной порядок представления такой доверенности не предусмотрен требованиями, установленными Правительством Российской Федерации» [31].

В целом можно отметить, что рассматриваемая статья предлагает два случая использования индивидуальными предпринимателями квалифицированной электронной подписи. В первом случае речь идет о

самостоятельном использовании индивидуальным предпринимателем квалифицированной подписи, во втором случае рассматриваются вопросы использования квалифицированной подписи при условии участия представителя со стороны индивидуального предпринимателя.

Относительно юридического лица также предусмотрены положения о самостоятельном использовании квалифицированной юридической подписи, а также использовании подписи представителем. Помимо этого, законодатель учитывает специфику самой категории «юридическое лицо» и закрепляет дополнительные правила. Так, «квалифицированный сертификат, который содержит указание на филиал, представительство иностранного юридического лица, создается и выдается удостоверяющим центром федерального органа исполнительной власти, уполномоченного на осуществление государственной регистрации юридических лиц, в установленном указанным органом порядке с указанием в качестве владельца квалифицированного сертификата также лица, являющегося руководителем данных филиала, представительства и уполномоченного действовать на основании доверенности, выданной иностранным юридическим лицом» [31]. В этом случае учитывается тот факт, что юридические лица могут иметь свои филиалы, а также в процессе предпринимательской деятельности возможно возникновение правоотношения, осложненного иностранным субъектом.

Особое значение электронная подпись в процессе осуществления предпринимательской деятельности приобретает при заключении договоров между самими предпринимателями, а также между предпринимателями и клиентами, которые не осуществляют предпринимательскую деятельность. «Электронная подпись в электронном документе, выполняет различные юридические функции (все или некоторые из перечисленных в зависимости от особенностей подписываемого документа): идентификацию лица; установление связи данного лица с содержанием документа; подтверждение намерения стороны сделки нести правовые последствия сделки; подтверждение авторства документа; обозначение намерение лица согласиться

с содержанием документа, написанного иным лицом, и ряд других» [26, с. 175]. Таким образом, при помощи электронной подписи удается снизить число личных встреч или вовсе свести их число к нулю, для заключения договора в рамках предпринимательской деятельности. Казалось бы, что с помощью электронной подписи можно значительно оптимизировать бизнес-процессы, однако, на практике ситуация складывается несколько иначе.

Анализируя практику применения электронной подписи в предпринимательской деятельности, исследователи обращают внимание на следующую тенденцию. Представители «крупного бизнеса» активно используют электронную подпись и признают ее преимущества и значимость для своей деятельности. В свою очередь, представители «малого и среднего» предпринимательства в большей степени склонны отказываться от данного инструмента, аргументируя это различными обстоятельствами, например, отсутствие технических специалистов, несовершенство правового регулирования и так далее [12, с. 31]. Такую тенденцию можно объяснить тем, что для крупного бизнеса характерен объемный поток документооборота, а также высокое количество его участников. Электронная подпись упрощает взаимодействие и сам процесс, позволяя отказаться от большого количества бумажных носителей, заменив их на электронные файлы, которые занимают небольшой объем памяти. Кроме того, электронная подпись позволяет предпринимателям расширять список потенциальных клиентов посредством электронных площадок, которых в силу цифровизации экономики становится все больше и больше. С учетом указанных преимуществ, крупному бизнесу удается перекрыть те недостатки, которые характерны электронной подписи, посредством повышения прибыли за счет тех возможностей, которые можно получить с ее помощью. Малый и средний бизнес, как правило, не обладает необходимым ресурсом, чтобы справиться с таким огромным потоком заказов или клиентов, кроме того, документооборот в нем значительно меньше, поэтому в должной степени им не удается оценить все преимущества электронной подписи. В этой связи недостатки, которые характерны для нее,

куда более значительно выражены. Именно таким образом, мы можем объяснить сложившуюся тенденцию использования электронной подписи в предпринимательской деятельности.

Поскольку практика применения субъектами предпринимательской деятельности электронной подписи неоднородна в силу того, что кем-то она используется, а кем-то нет, возникают следующие ситуации. Так, один из контрагентов может использовать электронную подпись, а другой, напротив, не использует ее [18, с. 37]. В этом случае возникнут следующие проблемы. Тот контрагент, который не имеет электронной подписи, не сможет провести проверку статуса документа, поскольку у него отсутствует соответствующее программное обеспечение. В этом случае возникнет необходимость в использовании бумажных носителей, что, соответственно, приведет к дублированию документооборота. Это снижает эффективность электронной подписи в вопросе упрощения ведения архивной документации, поскольку оставляет необходимость вести часть документов в бумажном формате.

Внедрение в предпринимательскую деятельность электронной подписи способствовало активному распространению смарт-контрактов. «Несмотря на часто встречающееся понимание смарт-контрактов как особого вида договоров, все же правильнее называть их особой формой совершения сделки, исполнения обязательства или обеспечения ее исполнения, в которой договоренности сторон достигнуты консенсуально, путем предварительного обоюдного волеизъявления заключить договор на условиях, которые нельзя будет изменить или просрочить» [34, с. 65]. Особую «привлекательность» для предпринимателей смарт-контракты имеют в силу того, что процесс их исполнения максимально прозрачен, поэтому можно отследить любой из этапов его исполнения до самых незначительных аспектов. При этом в силу того, что отечественный законодатель еще неоднозначно относится к блокчейн платформам, смарт-контракты не получили своего широкого распространения.

В завершении темы данного параграфа, мы можем сделать следующие выводы.

Во-первых, хотя законодатель рассматривает самозанятость, как экспериментальную форму предпринимательской деятельности, на сегодняшний день мы не видим предпосылок для ее упразднения, поскольку с ее помощью удалось вывести часть экономики из теневого сектора в «легальное поле». Можно также отметить, что физическое лицо, обладающее статусом самозанятого, является участником предпринимательских отношений, а также имеет особый статус для налоговых органов. В связи с этим мы видим необходимость отдельно закрепить в Федеральном законе «Об электронной подписи» статью, закрепляющую особенности использование квалифицированной электронной подписи при участии в правоотношениях самозанятых граждан.

Во-вторых, на сегодняшний день имеет место быть тенденция, которая заключается в активном использовании электронной подписи «крупным бизнесом», в то время как представители малого и среднего предпринимательства неоднозначно относятся к данному правовому инструменту. Крупному бизнесу удается перекрыть те недостатки, которые характерны электронной подписи, посредством повышения прибыли за счет тех возможностей, которые можно получить с ее помощью (увеличение клиентской базы, упрощение документооборота и так далее). Малый и средний бизнес, как правило, не обладает необходимым ресурсом, чтобы справиться с таким огромным потоком заказов или клиентов, кроме того, документооборот в нем значительно меньше, поэтому в должной степени им не удается оценить все преимущества электронной подписи. В этой связи недостатки, которые характерны для нее, куда более значительно выражены. Именно таким образом, мы можем объяснить сложившуюся тенденцию использования электронной подписи в предпринимательской деятельности.

В-третьих, с учетом развития технологий мы прослеживаем положительную тенденцию внедрения электронной подписи в предпринимательскую деятельность. Однако, нельзя утверждать, что подавляющее большинство предпринимателей в ближайшее время примут

решение о ее использовании в своем бизнесе. Для этого необходимо максимально упростить ее использование, а также решить ряд проблемных аспектов, характерных ее правовому регулированию. До этого на практике будут возникать случаи, когда один из контрагентов может использовать электронную подпись, а другой, напротив, не использует ее. В этом случае возникнут следующие проблемы. Тот контрагент, который не имеет электронной подписи, не сможет провести проверку статуса документа, поскольку у него отсутствует соответствующее программное обеспечение. В этом случае возникнет необходимость в использовании бумажных носителей, что, соответственно, приведет к дублированию документооборота. Это снижает эффективность электронной подписи в вопросе упрощения ведения архивной документации, поскольку оставляет необходимость вести часть документов в бумажном формате.

2.2 Особенности защиты электронной подписи в процессе осуществления предпринимательской деятельности

Одним из основных признаков предпринимательской деятельности является ее рисковый характер, который выражается в том, что предприниматель, принимая решение о вложении своих средств и ресурсов, рискует не достигнуть запланированного результата. Говоря о риске, стоит отметить, что предприниматель может обладать средствами и репутацией, которые повышают его виктимность среди мошенников. Факт владения электронной подписью предпринимателя позволит злоумышленнику совершить практически любые действия от имени жертвы, начиная от неправомерного доступа к охраняемой законом информации, завершая списанием денежных средств со счетов предпринимателя или получением кредитных средств от его имени.

Как правило, электронная подпись другого лица может быть получена следующими способами:

- «введение в заблуждение сотрудника удостоверяющего центра, который при выдаче подписи уверен, что подпись выдается ее настоящему владельцу;
- вступление в сговор с сотрудниками удостоверяющего центра, которые изготавливая или выдавая подпись знают, что делают это для ненадлежащего лица;
- незаконное изъятие, например – кража носителя с подписью у ее владельца» [20].

Здесь стоит обратить внимание, что, совершая одно из указанных действий, лицо может не иметь цели завладеть электронной подписью конкретного лица. При этом злоумышленник приобретает возможность совершить ряд потенциально-опасных действий в отношении автора подписи, что уже представляет общественную опасность. При этом ответственность за такие действия законодателем не предусмотрена. Поскольку мы говорим об общественной опасности, то обращаться необходимо к Уголовному кодексу Российской Федерации. Сразу же можно обратить внимание на статью 159.6 Уголовного кодекса, в которой закрепляется ответственность за мошенничество в сфере компьютерной информации. Диспозиция указанной нормы выглядит следующим образом: «Мошенничество в сфере компьютерной информации, то есть хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей» [29]. Хотя мы видим указание на ввод и вмешательство в функционирование компьютерной информации, что по алгоритму соответствует использованию электронной подписи, судебная практика неоднозначно применяет данную норму. А.А. Лаврушкина в своей работе приводит в качестве примера случаи, когда у потерпевших были похищены технические устройства (планшет, мобильный телефон), с их

помощью злоумышленники переводили себе средства при помощи функции мобильный банк. В одном случае содеянное было квалифицировано по статье 159.6 Уголовного кодекса, в другом случае квалификация была по части второй статьи 158 Уголовного кодекса [17, с. 31]. Не совсем понятно, по какой причине отдельные судьи при рассмотрении подобных дел не учитывают специфику применения простой электронной подписи при квалификации содеянного. На наш взгляд, такой подход является не совсем корректным и свидетельствует о том, что еще не все приняли процесс глобальной цифровизации и общественно-опасное значение каждого преступления в сфере цифровой экономики.

Однако, приведенный нами состав является материальным, то есть, предусматривает последствия совершения преступления – хищение имущества, права на него или денежных средств. Нас же в большей степени интересует вопрос, связанный самим фактом хищения информации, составляющей электронную подпись. Анализ уголовного законодательства позволяет нам сделать вывод, что специальной нормы, предусматривающей ответственность за подобное деяние, не предусмотрено. При этом необходимо понимать, что само по себе умышленное хищение информации (носителя информации), которая составляет электронную подпись, является общественно-опасным деянием, независимо от последствий, поскольку ставит под угрозу безопасность персональных данных пользователя и иной охраняемой законом информации, а также создает имущественные и репутационные риски. В этой связи мы видим необходимость закрепить в Уголовном кодексе Российской Федерации отдельную статью, предусматривающую ответственность за хищение информации (носителя информации) составляющую электронную подпись. Поскольку предпринимательская деятельность непосредственно связана с более высокими имущественными и иными рисками (например, возможность заключить кредитный договор на более крупную сумму, доступ к персональным данным сотрудников или клиентов предпринимателя и так

далее), то хищение электронной подписи индивидуального предпринимателя или юридического лица представляет повышенную общественную опасность. В связи с этим указанное деяние в отношении специального потерпевшего необходимо рассматривать в качестве квалифицирующего признака. Кроме того, нельзя не учитывать тот факт, что электронная подпись, похищенная у лица, являющегося должностным лицом на должности государственной или муниципальной службы, нотариуса, а также лиц, замещающих должность государственной или муниципальной службы, в руках злоумышленника может создать дополнительную угрозу для общества, государства, а также интересам государственной и (или) муниципальной службы. В этой связи рассматриваемое деяние в отношении указанных лиц должно рассматриваться в качестве особо квалифицирующего признака и предусматривать повышенную ответственность для преступника.

Рассматривая риски, которые имеют место быть при неправомерном завладении электронной подписью, Федеральная налоговая служба в своем обзоре указывает на следующие потенциальные негативные последствия:

- «регистрация юридических лиц и индивидуальных предпринимателей на номинального (фиктивного) директора;
- сдача налоговых деклараций, подписанных электронной подписью фиктивными лицами;
- систематическая сдача налоговых деклараций с большими суммами начислений от организаций, которые в ходе проведения дальнейших мероприятий налогового контроля отказываются от факта подписания и сдачи подобной отчетности в налоговые органы;
- нарушения при представлении налоговой отчётности, включая представление налоговых деклараций по НДС представителями организаций, в отношении которых территориальными инспекциями в адрес операторов электронного документооборота, направлены - письма об аннулировании электронной подписи;

- подписание налоговых деклараций по НДС физическими лицами (учредителями или руководителями организаций) в период их дисквалификации, компрометация ключевой информации;
- неправомерная смена руководителя юридического лица с использованием электронной подписи;
- регистрация фирм-однодневок с применением электронной подписи;
- выпуск электронной подписи (выдача электронной подписи) подставному лицу по поддельным документам, без уточнения сведений из единого государственного реестра юридических лиц;
- выпуск электронной подписи для юридических и физических лиц по доверенностям без согласия доверителя с целью совершения мошеннических действий» [15].

Оценивая представленные риски, можно отметить, что большая их часть так или иначе может создать негативные последствия для лица, осуществляющего предпринимательскую деятельность. Так, например, неправомерная смена руководителя юридического лица приведет к тому, что к управлению будет допущено лицо без согласования с руководством. После этого предпринимателю потребуется время для того, чтобы подтвердить факт неправомерного доступа к его электронной подписи. Даже в том случае, если это удастся сделать достаточно оперативно и аннулировать все действия руководителя, который неправомерно занимал пост, предприниматель теряет в первую очередь время. За это время, может быть, не получена прибыль, испорчена деловая репутация, не приняты какие-либо срочные управленческие решения, которые в последствие могут негативно сказаться на бизнесе. В свою очередь, незаконные манипуляции с электронной подписью контрагента также могут привести к неблагоприятным последствиям для добросовестного предпринимателя. Так, взятие на себя обязательств, посредством заключения договора фирмой-однодневкой является

потенциальной опасностью для добросовестного контрагента, поскольку он рискует потерять ресурсы, денежные средства и время.

Нередкими являются случаи, когда злоумышленники используют данные юридического лица и от его имени заводят электронную подпись для участия в различных аукционах и заключения сделок. Так, «в Арбитражный суд обратилось ООО Богородские деликатесы с иском к ООО «Сопар» о признании договора ничтожным. ООО Богородские деликатесы стало известно, что на торговой площадке АО Сбербанк-АСТ от имени ООО Богородские деликатесы неизвестное лицо создало личный кабинет, через который осуществлял закупки товара. Поскольку общество не предпринимало никаких действий по участию в торгах, истец обратился с заявлением в АО, в котором указал, что не является участником торгов и выразил свои подозрения о действии мошенников, использующих данные общества. Позже истец обратился в ООО Сопар с заявлением об аннулировании квалифицированной электронной подписи, выпущенной ими для неустановленных лиц, просило предоставить документы, представленные ответчику от имени ООО Богородские деликатесы для изготовления ЭЦП. Ссылаясь на то, что ответчик не предоставил никаких сведений и документов, квалифицированная электронная подпись не аннулирована, между тем, на основании спорной квалифицированной подписи неизвестным лицом от его имени с лицами, участвующими в торгах, подписаны фиктивные договоры на поставку товара и товаросопроводительные документы к договорам, общество обратилось в суд с настоящим исковым заявлением о признании недействительным (ничтожным) договора, заключенного в виде заявления на регистрацию и изготовление квалифицированного сертификата ключа проверки электронной подписи юридического лица, квалифицированный сертификат ключа проверки электронной подписи, серийный номер ***. Материалами дела, в том числе пояснениями истца, подтверждено, что ООО Богородские деликатесы не обращалось к ответчику с заявлением на изготовление квалифицированного сертификата ключа проверки электронной подписи, указанная в спорной

заявке на регистрацию и изготовление квалифицированного сертификата ключа проверки электронной подписи информация и документы о юридическом лице и директоре общества предоставлены неуполномоченным лицом, не имеющим права на заключение указанного договора от имени общества. Данное обстоятельство подтверждено имеющимися в материалах проверки КУСП копиями паспорта директора истца Багина А.В., а также его СНИЛС, представленными ответчиком, которые не соответствуют по своему содержанию нотариально удостоверенным копиям паспорта и СНИЛС Багина А.В. В ходе рассмотрения дела суд пришел к следующему выводу. Договор, заключенный между обществом с ограниченной ответственностью Богородские деликатесы и обществом с ограниченной ответственностью Сопар в форме заявления на регистрацию и изготовление квалифицированного сертификата ключа проверки электронной подписи юридического лица, квалифицированный сертификат ключа проверки электронной подписи, серийный номер *** признается недействительным» [23]. Представленный материал из судебной практики наглядно демонстрирует нам, с какой легкостью неуполномоченное лицо может получить электронную подпись от имени добросовестного предпринимателя и с ее помощью реализовывать мошеннические схемы. При этом весьма негативно, на наш взгляд, на самом процессе сказывается то обстоятельство, что удостоверяющий центр игнорирует заявление юридического автора электронной подписи на отзыв выданного сертификата. Хотя указанное основание предусмотрено пунктом вторым части шестой статьи 14-ой Федерального закона «Об электронной подписи», предпринимателю понадобилось обращаться в суд для восстановления своего нарушенного права в силу бездействия удостоверяющего центра. Такое поведение со стороны удостоверяющего центра не только создает препятствия для защиты прав и интересов предпринимателя, но и позволяет злоумышленнику продолжить его неправомерную деятельность и создать, таким образом, еще больше неблагоприятных последствий для добросовестного предпринимателя.

Кроме того, считаем необходимым рассмотреть другой аналогичный случай. Так, «публичное акционерное общество Промсвязьбанк обратилось в Арбитражный суд города Москвы с иском к обществу с ограниченной ответственностью ЭкоДомСервис о взыскании задолженности по кредитному договору. Как следует из судебных актов и материалов дела, в ПАО электронно по системе PSB On-line поступило заявление-оферта ООО ЭкоДомСервис, подписанное электронной подписью Козлова Игоря Валентиновича, на заключение договора о предоставлении кредита по программе кредитования. Общество заявило о присоединении к действующей редакции правил по программе кредитования и предложило заключить кредитный договор на условиях предоставления кредита в сумме 1 537 000,00 руб. под 19,4% годовых сроком на 12 месяцев. Банк акцептовал предложение ООО путем перечисления заявленной суммы кредита на счет общества. Поскольку ответчик не исполнял возложенные на него обязательства, ПАО обратился в суд. Судом первой инстанции было установлено, что банк не подтвердил совершение спорных банковских операций непосредственно обществом, не представил доказательств тому, что IP-адрес, с которого поступило заявление-оферта на заключение кредитного договора, принадлежит ООО ЭкоДомСервис и использовался им ранее для входа в систему PSB On-line, что заявление и платежные поручения были сформированы с использованием компьютера общества. Кроме того, по мнению банка, суды не учли действующие пункты договора, Правил PSB On-line. Согласно пункту первому указанного документа Клиент несет полную ответственностью за действия лиц, получивших по любым основаниям (в том числе противоправным) доступ к системе PSB On-line, закрытым ключам электронной подписи и иным техническим и информационным средствам, переданным банком клиенту и обеспечивающим возможность формирования и направления в банк электронных документов. Банк не несет ответственность за ущерб, возникший вследствие допущенного клиентом несанкционированного доступа третьих лиц к системам. Суд счел доводы ПАО обоснованными и отправил дело на

дальнейшее рассмотрение» [19]. Анализируя представленный материал судебной практики, нам бы хотелось обратить внимание на следующие обстоятельства. Во-первых, весьма сомнительными видятся нам правила электронной площадки, по смыслу которых вся ответственность за переход доступа электронной подписи к третьим лицам возлагается на автора подписи. При помощи данного пункта площадка стремится снять с себя всю ответственность в случае потенциального возникновения спора. Но такой подход не совсем корректен. Неправомерное выбытие электронной подписи происходит не по воле клиента, кроме того, долгое время клиент может не знать об этом, и, соответственно, не принимать никаких действий. Мы придерживаемся мнения, что юридический автор электронной подписи, несмотря на внутренние правила площадки, не должен нести ответственность, если докажет, что доступ к подписи был получен третьими лицами неправомерным способом. В этой связи мы считаем необходимым закрепить соответствующее правило в нормативно-правовой базе, регулирующие вопросы использования электронной подписи, а также привести в соответствии с данным положением правила и регламенты электронных площадок. Во-вторых, на наш взгляд, при решении подобных споров судам необходимо руководствоваться следующими обстоятельствами. Следует выяснить, насколько добросовестно повел себя предприниматель, который заявляет о неправомерном использовании его электронной подписи, с того момента, как ему стал известен факт неправомерного завладения. Добросовестное поведение может включать в себя различные действия, направленные на изобличение злоумышленника или прекращения действия сертификата подписи. К числу таких действий, на наш взгляд, можно отнести: уведомление контрагента о факте неправомерного доступа к электронной подписи, заявление в полицию о факте совершения мошеннических действий, заявление в удостоверяющий центр о прекращении действия электронной подписи и так далее. Таким образом, суд сможет установить, добросовестный

характер поведения лица или же, напротив, недобросовестный характер его действий, которые направлены на попытку избежать исполнения обязательств.

Обобщая все вышеизложенное в рамках данной главы, мы можем сделать следующие выводы в рамках диссертационного исследования.

Во-первых, хотя законодатель рассматривает самозанятость, как экспериментальную форму предпринимательской деятельности, на сегодняшний день мы не видим предпосылок для ее упразднения, поскольку с ее помощью удалось вывести часть экономики из теневого сектора в «легальное поле». Можно также отметить, что физическое лицо, обладающее статусом самозанятого, является участником предпринимательских отношений, а также имеет особый статус для налоговых органов. В связи с этим мы видим необходимость отдельно закрепить в Федеральном законе «Об электронной подписи» статью, закрепляющую особенности использование квалифицированной электронной подписи при участии в правоотношениях самозанятых граждан.

Во-вторых, на сегодняшний день имеет место быть тенденция, которая заключается в активном использовании электронной подписи «крупным бизнесом», в то время как представители малого и среднего предпринимательства неоднозначно относятся к данному правовому инструменту. Крупному бизнесу удается перекрыть те недостатки, которые характерны электронной подписи, посредством повышения прибыли за счет тех возможностей, которые можно получить с ее помощью (увеличение клиентской базы, упрощение документооборота и так далее). Малый и средний бизнес, как правило, не обладает необходимым ресурсом, чтобы справиться с таким огромным потоком заказов или клиентов, кроме того, документооборот в нем значительно меньше, поэтому в должной степени им не удается оценить все преимущества электронной подписи. В этой связи недостатки, которые характерны для нее, куда более значительно выражены. Именно таким образом, мы можем объяснить сложившуюся тенденцию использования электронной подписи в предпринимательской деятельности.

В-третьих, с учетом развития технологий мы прослеживаем положительную тенденцию внедрения электронной подписи в предпринимательскую деятельность. Однако, нельзя утверждать, что подавляющее большинство предпринимателей в ближайшее время примут решение о ее использовании в своем бизнесе. Для этого необходимо максимально упростить ее использование, а также решить ряд проблемных аспектов, характерных ее правовому регулированию. До этого на практике будут возникать случаи, когда один из контрагентов может использовать электронную подпись, а другой, напротив, не использует ее. В этом случае возникнут следующие проблемы. Тот контрагент, который не имеет электронной подписи, не сможет провести проверку статуса документа, поскольку у него отсутствует соответствующее программное обеспечение. В этом случае возникнет необходимость в использовании бумажных носителей, что, соответственно, приведет к дублированию документооборота. Это снижает эффективность электронной подписи в вопросе упрощения ведения архивной документации, поскольку оставляет необходимость вести часть документов в бумажном формате.

Кроме того, мы видим необходимость закрепить в Уголовном кодексе Российской Федерации отдельную статью, предусматривающую ответственность за хищение информации (носителя информации) составляющую электронную подпись. Поскольку предпринимательская деятельность непосредственно связана с более высокими имущественными и иными рисками (например, возможность заключить кредитный договор на более крупную сумму, доступ к персональным данным сотрудников или клиентов предпринимателя и так далее), то хищение электронной подписи индивидуального предпринимателя или юридического лица представляет повышенную общественную опасность. В связи с этим указанное деяние в отношении специального потерпевшего необходимо рассматривать в качестве квалифицирующего признака. Кроме того, нельзя не учитывать тот факт, что электронная подпись, похищенная у лица, являющегося должностным лицом

на должности государственной или муниципальной службы, нотариуса, а также лиц, замещающих должность государственной или муниципальной службы, в руках злоумышленника может создать дополнительную угрозу для общества, государства, а также интересам государственной и (или) муниципальной службы. В этой связи рассматриваемое деяние в отношении указанных лиц должно рассматриваться в качестве особо квалифицирующего признака и предусматривать повышенную ответственность для преступника.

Также нами было отмечено, что весьма сомнительными видятся нам правила электронной площадки, по смыслу которых вся ответственность за переход доступа электронной подписи к третьим лицам возлагается на автора подписи. При помощи данного пункта площадка стремится снять с себя всю ответственность в случае потенциального возникновения спора. Но такой подход не совсем корректен. Неправомерное выбытие электронной подписи происходит не по воле клиента, кроме того, долгое время клиент может не знать об этом, и, соответственно, не принимать никаких действий. Мы придерживаемся мнения, что юридический автор электронной подписи, несмотря на внутренние правила площадки, не должен нести ответственность, если докажет, что доступ к подписи был получен третьими лицами неправомерным способом. В этой связи мы считаем необходимым закрепить соответствующее правило в нормативно-правовой базе, регулирующие вопросы использования электронной подписи, а также привести в соответствии с данным положением правила и регламенты электронных площадок.

Глава 3 Актуальные направления совершенствования правового регулирования электронной подписи в предпринимательской деятельности

3.1 Актуальные проблемы правового регулирования электронной подписи в предпринимательской деятельности

Электронная подпись является инновационным инструментом, который позволяет предпринимателю расширить свои возможности и соответствовать актуальным тенденциям экономики. Несмотря на это обстоятельство, электронная подпись является сравнительно новой правовой конструкцией, которая постепенно внедряется в жизнь общества и еще имеет ряд существенных недостатков, которые требуют устранения. В рамках данного параграфа мы рассмотрим позиции различных авторов, исследовавших проблемные аспекты правового регулирования электронной подписи в предпринимательской деятельности.

А.Д. Бабанцев в своей работе в качестве одного из проблемных аспектов применения электронной подписи выделяет отсутствие универсального характера цифровой подписи. Автором обращено внимание на то, что разные области применения могут потребовать разные электронные подписи, например, электронная подпись для налоговых деклараций не подойдет на портале Росалкогольрегулирования [3, с. 220]. Здесь необходимо учитывать то обстоятельство, о какой именно универсальности электронной подписи говорит автор статьи. Обеспечить универсальность на всех цифровых площадках на данный момент не представляется возможным, как минимум по той причине, что они используют разные виды электронной подписи. Кроме того, необходимо понимать, что частные площадки администрируются разными субъектами, поэтому способы шифрования и иные аспекты программного обеспечения могут значительно отличаться, что будет препятствовать универсальности цифровой подписи. Если же мы будем брать

в расчет исключительно государственные сервисы, то здесь вполне можно говорить о возможности применения единой подписи. Поскольку государство представляет собой единую систему, которую мы в некоторой степени можем рассматривать в качестве единой корпорации, то с технической точки зрения, вполне возможно создать общую экосистему ресурсов, работающих в рамках одних и тех же алгоритмов. Это в свою очередь позволит создать единую электронную подпись, которая будет использоваться предпринимателем при любых взаимодействиях с органами государственной и муниципальной власти. При этом необходимо учитывать, что создание единой экосистемы приведет к повышению рисков, связанных с утерей или неправомерным завладением электронной подписи третьими лицами. Поэтому при разработке законопроекта о создании единой экосистемы государственных и муниципальных цифровых ресурсов, параллельно необходимо обеспечить максимальную защиту электронной подписи, в целях избежания неправомерного доступа и иных противоправных действий со стороны злоумышленников.

Отдельно авторы обращают внимание на то обстоятельство, что уязвимым местом правового регулирования электронной подписи являются вопросы ответственности в рамках ее применения, а также непосредственно связанных с ним правоотношений [22, с. 572]. В предыдущей главе мы уже от части затронули данный вопрос и в качестве одной из новаций предложили норму, закрепляющую уголовную ответственность за хищение информации (носителя информации), составляющей электронную подпись. Кроме того, нами был рассмотрен случай из судебной практики, когда удостоверяющий центр проигнорировал заявление об отзыве электронной подписи, поступившее от предпринимателя, на чье имя она была сделана. В этой связи необходимо рассмотреть вопрос ответственности удостоверяющего центра. Так, частью третьей статьи 13-ой Федерального закона «Об электронной подписи» установлено следующее: «Удостоверяющий центр в соответствии с

законодательством Российской Федерации несет ответственность за вред, причиненный третьим лицам в результате:

- неисполнения или ненадлежащего исполнения обязательств, вытекающих из договора оказания услуг удостоверяющим центром;
- неисполнения или ненадлежащего исполнения обязанностей, предусмотренных Федеральным законом» [31].

При конструировании указанной нормы законодатель даже не указывает, о каких именно видах ответственности удостоверяющего центра идет речь. Очевидно, что к уголовной ответственности юридическое лицо не может быть привлечено, поскольку не является субъектом преступления. Основываясь на статье 1064 Гражданского кодекса [9], мы можем сделать вывод, что удостоверяющий центр можно привлечь к материальной ответственности в рамках арбитражного процесса. Отметим, что в ходе проведения исследования нам не удалось найти соответствующую судебную практику, но положения закона позволяют заявить соответствующий иск. Помимо этого, юридическое лицо может быть привлечено к административной ответственности. В частности, нас интересует статья 13.33 Кодекса Российской Федерации об административных правонарушениях, где закрепляется ответственность за нарушение обязанностей, предусмотренных законодательством Российской Федерации в области электронной подписи. Часть пятая закрепляет ответственность за «нарушение аккредитованным удостоверяющим центром порядка формирования и ведения реестров квалифицированных сертификатов, включая нарушение сроков внесения в реестр квалифицированных сертификатов информации о прекращении действия квалифицированного сертификата или о его аннулировании, либо порядка предоставления информации из такого реестра» [16]. Санкция за данное правонарушение предусматривает штраф в размере от пяти до десяти тысяч рублей. На наш взгляд, такой размер штрафа является чрезмерно мягким наказанием, поскольку указанные действия могут привести к серьезным последствиям для предпринимателя. Ранее мы указывали, что внесение информации об отзыве

электронной подписи и ее аннулировании, позволяет злоумышленнику и дальше реализовывать свои мошеннические схемы. Однако, в силу того, что наказание за рассматриваемое деяние чрезмерно мягкое, удостоверяющий центр может не разбираться в вопросе и игнорировать вполне законные требования лица, от имени которого неправомерно была выпущена электронная подпись. Даже в том случае если правонарушение совершается повторно, санкция удваивается относительно размера штрафа, применяемого к удостоверяющему центру в первый раз. Таким образом, мы видим необходимость увеличить размер штрафов, предусмотренных в качестве наказания за нарушение законодательства в области электронной подписи. Поскольку актуальные размеры штрафов, на наш взгляд, являются чрезмерно низкими, в результате чего нарушается принцип соразмерности наказания содеянному административному правонарушению.

В литературе отдельно можно встретить мнение о необходимости закрепления уголовной ответственности в отношении должностных лиц, за нарушение порядка выдачи сертификата электронной подписи [28, с. 155]. Рассматривая данное предложение, следует обратить внимание на тот факт, что необходимо разграничить весьма схожий состав административного правонарушения и преступления. В этой связи в качестве обязательных последствий нарушения законодательства об электронной подписи необходимо предусмотреть крупный ущерб, причиненный пострадавшему. В качестве квалифицирующих признаков можно предусмотреть: причинение особо крупного ущерба, совершение деяния группой лиц, совершение преступления должностным лицом Федеральной налоговой службы (в этом случае ущерб причиняется в том числе и интересам государственной службы). Кроме того, обязательным признаком преступления должна быть субъективная сторона, которая определяется умышленной формой вины. Нарушение законодательства в сфере электронной подписи совершенное с неосторожной формой вины, на наш взгляд, не должно квалифицироваться в рамках предлагаемой статьи.

«Введение единых универсальных электронных карт, однозначно идентифицирующих личность человека и хранящих сведения о физическом лице, позволит также упростить процедуры работы с ЭП и ее получения либо замены на новую. Снижение затрат на приобретение ЭП возможно за счет создания терминалов отправки электронных документов в контролирующих органах, с помощью которых индивидуальные предприниматели и физические лица получат возможность отправлять отчетность, не имея личных программно-аппаратных средств» [39, с. 563]. Мы не разделяем позицию автора относительно предложенных нововведений, направленных на решение актуальных проблем правового регулирования электронной подписи. Относительно предлагаемых электронных карт мы можем отметить, что они станут бесполезным промежуточным звеном в системе получения электронной подписи. Их получение будет дублировать процедуру получения электронной подписи, что, по сути, затянет процесс, но никак не упростит его. Также стоит отметить, что не совсем понятно, каким образом, в современных реалиях предприниматель может не иметь хотя бы простейшего технического устройства для сетевого взаимодействия. Обычные телефоны, как правило, имеют функционал, который позволит сканировать и отправлять документы. Если же требуется использование квалифицированной электронной подписи, а у предпринимателя отсутствует компьютер, куда более простым вариантом будет отправиться в библиотеку и бесплатно воспользоваться их устройствами. Поэтому мы не видим необходимости в дополнительных тратах бюджетных средств на создание и установку специальных терминалов.

Рассматривая проблемные аспекты, которые оказывают существенное влияние, в том числе и на правовое регулирование электронной подписи, в своей работе О.В. Шеметова и С.В. Чугунова указывают на следующие обстоятельства. «Главной и существенной проблемой, не позволяющей внедрить электронную подпись во все сферы повседневной жизни, является недоверие граждан инновационным, высокотехнологичным решениям задач, стоящих перед современным человеком. Причина этой проблемы лежит в

низком уровне информационной культуры населения. Определенный психологический барьер испытывают и многие руководители предприятий. Поэтому для обеспечения электронного документооборота с использованием электронной подписи на предприятии необходимо иметь не только соответствующие технические средства, но и знания, соответствующую квалификацию и определенный психологический настрой, как рядовых менеджеров, так и руководителей. Следующая проблема ограниченного применения электронной подписи – это защита электронной подписи от несанкционированного использования или изменения. Так, например, если автоматизированная система документационного обеспечения управления предприятия территориально распределена, то желательно, чтобы при обмене документами по открытым каналам связи имелись встроенные сертифицированные средства цифровой подписи и шифрования. Однако, эта проблема является комплексной и затрагивает в целом защиту информации и коммерческой тайны предприятия, что является предметом отдельного обсуждения. Третьей и не менее важно проблемой можно считать отсутствие в документах прямого действия указаний на повсеместное применение электронной отчетности. Решение этой проблемы даст значительный толчок для внедрения электронной подписи во все сферы нашей деятельности. Кроме того, распространению электронной подписи препятствуют ее высокая цена и необходимость оформления разных подписей для взаимодействия с разными госорганами и доступа к различным базам данных» [36, с. 425]. Если затрагивать психологический аспект вопроса, который относится к первой из заявленных автором проблем, то можно упомянуть тенденцию применения электронной подписи преимущественно крупными предпринимателями. Темп законодательного регулирования напрямую зависит от общественной потребности в нем. Пока большинство предпринимателей не будет активно использовать возможности электронной подписи, вопросы ее правового регулирования не будут иметь первостепенный характер для законодателя. Оценивая же перспективы обязательного использования электронной подписи,

можно отметить, что подавляющая часть предпринимательского сектора готова к данному решительному шагу, в том случае, если квалифицированная подпись будет доступной и простой в использовании. Однако, обязывание использования электронной подписи во всех сферах видится нам преждевременным, поскольку на данный момент отсутствует фактор технической оснащенности для этого.

Другой проблемный аспект, по мнению А.А. Асеева, заключается в том, что «в основном руководители крупных компаний, предприятий оформляют электронную подпись на менеджеров по продажам или же на системных администраторов. Такую практику нельзя считать правильной, поскольку электронная подпись удостоверяет все полномочия генерального директора, а другое лицо (представитель) может использовать ключ без его согласия при совершении других операций. Законодательство не требует нотариального удостоверения доверенности на получение электронной подписи и наличия на ней штампа, печати организации» [2, с. 21]. Именно то обстоятельство, что для получения электронной подписи достаточно доверенности в простой письменной форме, позволяет злоумышленникам получать электронную подпись на имя другого лица и использовать ее в противоправных целях. По этой причине мы видим необходимость изменения законодательства в части предоставления доверенности, необходимой для получения электронной подписи от имени другого лица.

В завершении параграфа, мы можем сделать следующие выводы относительно актуальных проблем правового регулирования электронной подписи.

Во-первых, в качестве одной из проблем регулирования электронной подписи называют отсутствие у нее универсального характера. Поскольку государство представляет собой единую систему, которую мы в некоторой степени можем рассматривать в качестве единой корпорации, то с технической точки зрения, вполне возможно создать общую экосистему ресурсов, работающих в рамках одних и тех же алгоритмов. Это в свою очередь позволит

создать единую электронную подпись, которая будет использоваться предпринимателем при любых взаимодействиях с органами государственной и муниципальной власти. При этом необходимо учитывать, что создание единой экосистемы приведет к повышению рисков, связанных с утерей или неправомерным завладением электронной подписи третьими лицами. Поэтому при разработке законопроекта о создании единой экосистемы государственных и муниципальных цифровых ресурсов, параллельно необходимо обеспечить максимальную защиту электронной подписи, в целях избежания неправомерного доступа и иных противоправных действий со стороны злоумышленников.

Во-вторых, другая проблема правового регулирования электронной подписи связана с ответственностью за нарушение соответствующих правовых норм. В частности, нами было отмечено, что в статье 13.33 Кодекса об административных правонарушениях предусмотрены весьма небольшие штрафы. На наш взгляд, такой размер штрафа является чрезмерно мягким наказанием, поскольку указанные действия могут привести к серьезным последствиям для предпринимателя. Ранее мы указывали, что внесение информации об отзыве электронной подписи и ее аннулировании, позволяет злоумышленнику и дальше реализовывать свои мошеннические схемы. Однако, в силу того, что наказание за рассматриваемое деяние чрезмерно мягкое, удостоверяющий центр может не разбираться в вопросе и игнорировать вполне законные требования лица, от имени которого неправомерно была выпущена электронная подпись. Даже в том случае если правонарушение совершается повторно, санкция удваивается относительно размера штрафа, применяемого к удостоверяющему центру в первый раз. Таким образом, мы видим необходимость увеличить размер штрафов, предусмотренных в качестве наказания за нарушение законодательства в области электронной подписи. Поскольку актуальные размеры штрафов, на наш взгляд, являются чрезмерно низкими, в результате чего нарушается

принцип соразмерности наказания содеянному административному правонарушению.

Кроме того, предлагается ввести уголовную ответственность для физических лиц за нарушение законодательства об электронной подписи. В качестве обязательных последствий нарушения законодательства об электронной подписи необходимо предусмотреть крупный ущерб, причиненный пострадавшему. В качестве квалифицирующих признаков можно предусмотреть: причинение особо крупного ущерба, совершение деяния группой лиц, совершение преступления должностным лицом Федеральной налоговой службы (в этом случае ущерб причиняется в том числе и интересам государственной службы). Кроме того, обязательным признаком преступления должна быть субъективная сторона, которая определяется умышленной формой вины.

В-третьих, нами было отмечено, что темп законодательного регулирования напрямую зависит от общественной потребности в нем. Пока большинство предпринимателей не будет активно использовать возможности электронной подписи, вопросы ее правового регулирования не будут иметь первостепенный характер для законодателя.

3.2 Зарубежный опыт правового регулирования электронной подписи в предпринимательской деятельности

Для разработки предложений, направленных на совершенствование правового регулирования электронной подписи, на наш взгляд, в первую очередь следует обратиться к зарубежной практике регулирования исследуемого вопроса. Анализ зарубежного опыта позволит нам выявить потенциально-полезные механизмы правового регулирования и рассмотреть возможность их апробации в отечественное законодательство.

«Интересным является и опыт Эстонии, которая в 2014 году ввела институт цифрового (электронного или виртуального) резидентства (E-

Residency). Эта программа дает возможность вести финансовую и хозяйственную деятельность на территории Эстонии, физически не находясь в этой стране, что очень актуально для юридических лиц. Так, после прохождения процедуры идентификации и предоставления биометрических данных лицо получает аналог эстонской ГО-карты с электронным чипом и имеет право ставить на документах электронную подпись, признаваемую органами власти Эстонии, банками и т.д. Е-резидент может в течение одного дня зарегистрировать юридическое лицо по Интернету, управлять им онлайн из любой точки мира, пользоваться услугами электронного банкинга, декларировать налоги, заключать контракты по Интернету с использованием цифровой подписи и тому подобного» [27, с. 245]. Именно об этом мы говорили в прошлой главе, когда рассматривали возможность сделать электронную подпись универсальной. Единая цифровая экосистема, которая позволяет осуществлять предпринимательскую деятельность на рынке, находясь в самой стране или за ее пределами. На наш взгляд, весьма удачное решение, которое открывает доступ финансовым потокам из-за пределов государства и позволяет в большей степени развивать экономику государства. Для предпринимательской деятельности единое цифровое пространство и возможность участия в нем иностранными субъектами позволяет расширить границы возможностей и вести бизнес даже с иностранными контрагентами, не создавая при этом филиалов в других государствах. На наш взгляд, Российская Федерация находится на пути формирования единой цифровой экосистемы. Однако, возможность полноценного участия иностранных субъектов во всех цифровых правоотношениях пока находится под вопросом из-за санкционного давления и ухода крупных компаний с отечественного выбора. С одной стороны, пока отсутствует спрос на осуществление электронной предпринимательской деятельности из-за пределов страны, с другой стороны, государство пока не стремится создавать открытые каналы информационного взаимодействия в рамках обеспечения информационной

безопасности, как части национальной системы безопасности личности, общества и государства.

«В Великобритании эффективно работает Государственная цифровая служба, которая является частью кабинета министров и помогает взаимодействовать с правительством, а также правительству действовать более эффективно и результативно, в частности, в вопросах стандартизации цифровых услуг и поддержания различных межправительственных платформ и инструментов» [42, с. 95]. Аналогичное учреждение есть и в Российской Федерации, речь идет о Министерстве цифрового развития, связи и массовых коммуникаций. Однако, опять же вынуждены отметить тот факт, что полноценно осуществлять свою деятельность в сфере цифрового развития указанное учреждение не может. Это обусловлено несколькими обстоятельствами. Основными является санкционное давление, предвзятое и необоснованное притеснение отечественных пользователей иностранными компаниями, владеющими важными продуктами в сфере цифровой деятельности, а также сложности в создании отечественных аналогов, вызванные оттоком специалистов в IT сфере.

Отдельные авторы обращают внимание на то обстоятельство, что законодательства других стран по-разному могут определять электронную подпись. «Сингапурский законодатель раскрывает понятие подписи через метод (электронный или иной), который используется для идентификации человека и указания намерения этого лица в отношении информации, содержащейся в соответствующей записи. В свою очередь безопасная электронная подпись означает такую электронную подпись, которая является уникальной в своем роде для конкретного лица, позволяет идентифицировать это лицо, была создана способом или с использованием средств, находящихся под исключительным контролем человека, использующего его, и связана с электронной записью. Таким образом, в основе электронной подписи положено понятие электронной записи, которые соотносятся друг с другом как общее и частное. В соответствии со статьей 2 этого закона электронная запись

представляет собой запись, созданную, переданную, полученную или сохраненную электронными средствами в информационной системе или для передачи из одной информационной системы в другую» [37, с. 169]. В свою очередь законодательство Японии рассматривает электронную подпись в качестве «меры, принятой относительно информации, которая может быть записана в электромагнитную запись (то есть любая запись, которая создается с помощью электронных, магнитных или любых других средств, не распознаваемых естественной функцией восприятия, и используется для обработки данных компьютера), при условии, что такая мера позволяет идентифицировать лицо ее создавшее, а также констатировать изменения информации. Презумпция подлинности электромагнитной записи означает, что информация считается аутентичной, если электронная подпись выполняется принципалом в отношении информации, представленной в электромагнитной записи» [44, с. 305].

Если отечественный законодатель раскрывает понятие электронной подписи посредством определения ее в качестве информации, то законодатели указанных стран исходят из того, что электронная подпись – это метод. Мы не разделяем данную позицию и не видим перспективным апробировать такой подход при понимании электронной подписи в отечественное законодательство. Электронная подпись – это именно информация, которая выполняет определенные функции. Безусловно, эта информация предоставляется при помощи определенного метода, но для понимания сущность данный категории, ключевое значение имеет именно тот факт, что это информация. Вокруг такого понимания в дальнейшем выстраивается все правовое регулирование. Изменение концепции понимания в данном случае приведет к необходимости изменения всей системы правового регулирования электронной подписи, однако, не позволит в какой-то степени усовершенствовать законодательство в рамках данного вопроса.

Весьма интересным видится опыт Кореи, где электронная подпись получила активное распространение, но при этом предусматривает ряд

существенных ограничений. «не допускается подписание электронной подписью документов о передаче недвижимости (кроме договора аренды и некоторых других договоров, которые законом допускаются), договоров, предусматривающих передачу нематериальных благ (в частности, уступка патентных или авторских прав) и документов о залоге, регистрации брака, завещании и учредительного договоров» [45, с. 3]. Стоит отметить, что, с одной стороны, такой подход обусловлен обеспечением безопасности участников правоотношений. Отсутствие возможности отчуждать имущество посредством использования электронной подписи, позволяет избежать применения мошеннических схем в данной сфере. Подобный подход достаточно приемлем, но ограничивает многие инновационные достоинства для сферы предпринимательской деятельности. Поэтому даже если вводить подобные ограничения в отечественное законодательство, необходимо учитывать интересы предпринимателей. Например, можно предусмотреть ряд ограничений на использование электронной подписи физическими лицами, которые не осуществляют предпринимательскую деятельность, с целью обезопасить их от мошеннических действий. При этом наличие статуса индивидуального предпринимателя или самозанятого позволит физическому лицу расширить возможности применения электронной подписи с целью реализации ее потенциальной эффективности в данной сфере. Как мы уже отмечали ранее, предпринимательская деятельность характеризуется своим рисковым характером, поэтому предприниматель, который готов полноценно использовать электронную подпись в своей деятельности, также должен быть готов к потенциальным рискам, характерным ее использованию.

Законодательство Германии изначально предъявляло достаточно жесткие требования к удостоверяющим центрам. В последствии, с принятием Директивы ЕС, законодательство об электронной подписи было приведено в соответствие с положениями Директивы, в результате чего положения подверглись коррективам в сторону смягчения предъявляемых требований. «Стремясь обеспечить надежность удостоверяющих центров, законодатель

устанавливает дополнительные требования к сотрудникам. Их можно сравнить с требованиями, предъявляемыми к банковским служащим. Сотрудники должны быть надежными, там не могут работать лица, осужденные за преступления против собственности, за совершение ряда других преступлений на срок более трех месяцев. Работники должны иметь экспертные навыки, пройти, по меньшей мере, годовые курсы либо иметь профессиональный стаж не менее трех лет» [41, с. 585]. На наш взгляд, мы можем использовать опыт Германии для повышения уровня безопасности предпринимателей и иных пользователей электронной подписи, апробировав соответствующие требования в положения об удостоверяющих центрах. Как уже было отмечено ранее, часть мошеннических схем с электронной подписью реализуется посредством участия сотрудника удостоверяющего центра, либо его халатного отношения к исполнению своих служебных обязанностей. Кроме того, к служащим налоговых органов, которые отвечают за выдачу электронной подписи, предъявляются особые квалификационные и иные критерии. Сотрудники удостоверяющего центра также выполняют работу, которая характеризуется доступом к персональным данным и информации, составляющей электронную подпись. Поэтому мы видим возможность закрепить в их отношении особые критерии отбора, которые, на наш взгляд, позволят увеличить качество их работы, а также снизить вероятность их участия в мошеннических схемах, связанных с получением неправомерного доступа к электронной подписи. К числу таких требований мы можем отнести: отсутствие судимостей у сотрудника или его близких родственников, наличие высшего образования в сфере IT, полученного в образовательном учреждении, имеющем государственную аккредитацию. Кроме того, можно обязать лицо пройти специальные курсы, целью которых будет формирование представления о правовом регулировании электронной подписи и защите персональных данных, а также представлен информациях об актуальных мошеннических схемах с применением электронных подписей.

Также положительно в своем исследовании опыт немецкого законодательства об электронной подписи оценивает А.В. Билокапич. Автор указывает следующее. «Представляется, что для нашей страны наиболее подходящим является использование опыта Германии, включающего разумное вмешательство государства в деятельность участников электронного документооборота. Объясняется это тем, что правоотношения по использованию электронных средств телекоммуникаций в коммерческой деятельности возникли относительно недавно, еще ни одна страна не имеет эффективно действующего законодательства в данной области. Поэтому пускать процесс формирования соответствующих норм на самотек представляется крайне неразумным» [4, с. 495]. В целом мы разделяем позицию автора и придерживаемся следующего мнения по данному вопросу. Законодатель не должен устанавливать каких-то жестких рамок относительно использования электронной подписи. В особенности это касается предпринимателей, для которых электронная подпись является инструментом расширения бизнеса. Основная задача правового регулирования в данной сфере заключается в том, чтобы обеспечить максимальную безопасность участников правоотношений. При этом же сами способы и иные особенности применения электронной подписи должны оставаться на усмотрение предпринимателя, поскольку отсутствие ограничений по данному вопросу будет способствовать обеспечению развития рыночных отношений.

Иного подхода при регулировании электронной подписи придерживается Индия. «Законы об электронной подписи жестоко регулируют рынок услуг в данной сфере путём лицензирования деятельности по предоставлению таких услуг. Данный подход лишен достаточной гибкости и практически не способен своевременно реагировать на меняющиеся условия и механизмы развития информационной сферы общественно-производственной деятельности» [43, с. 75]. Жесткий подход в регулировании инструментов предпринимательской деятельности ограничивает возможность их развития. Как отмечает автор, при таком подходе система может меняться

только при условии внесения соответствующих изменений в нормативно-правовое регулирование. Этот процесс может затянуться на длительное время, что негативно скажется на деятельности предпринимателя, который имеет способ оптимизировать свою деятельность, но в силу формальных обстоятельств сделать этого не может и вынужден ожидать пока соответствующая инициатива доберется до уполномоченного органа, будет рассмотрена и одобрена, после чего необходимые изменения будут внесены. Здесь необходимо руководствоваться принципом экономии императивных средств и целесообразностью их использования для достижения безопасности участников правоотношений.

«Для США характерен технологически нейтральный (минималистский) подход в области правового регулирования электронной подписи, который законодательно не навязывает использование определенной технологии создания электронной подписи, предоставляя участникам электронного взаимодействия право выбора. При этом само понятие электронной подписи трактуются максимально широко (акцент только на электронном способе представления информации). Данный подход позволяет использовать новые технологии, появляющиеся на рынке, без существенных изменений законодательства, однако требует применение норм договорного права при отсутствии таковых в законодательстве» [38, с. 121]. Подход США отражает инновационный характер электронной подписи, то есть, при помощи гибких и нестрогих формулировок, законодательство позволяет данному правовому инструменту соответствовать актуальным реалиям технологического развития и рыночным условиям. Однако, в отечественных реалиях подобный подход недопустим, поскольку США и Российская Федерация относятся к разным правовым семьям. Если в США допустимо установить только основу законодательного регулирования, которая будет дополняться судебной практикой и обычаями делового оборота, то в России, где прецедент официально не является источником права, дополнить законодательные «бреши» не удастся. Отечественное законодательство, как правило,

дополняется и расширяется при помощи подзаконного нормотворчества, которое также характеризуется административным характером закрепления правовых норм. В этих условиях подобный подход недопустим, поскольку создаст хаос в правоотношениях, который будет дополнен отсутствием единообразия судебной практики при решении споров относительно законодательства об электронной подписи.

«Для правового режима электронной подписи в Швеции характерен более строгий законодательный подход, который характеризуется своим двойственным характером. Де-юре существует технологическая нейтральность: законодатель вводит относительно широкое понятие электронная подпись, ее различные виды (электронная подпись в широком смысле, усиленная электронная подпись, квалифицированная электронная подпись), предоставляя свободу в выборе технологии. Де-факто законодатель стимулирует применение только квалифицированной электронной подписи, основанной на технологии криптографии открытым ключом, путем определения ее правового статуса и установления к ней жестких законодательных требований определения надежности, соответствие которым проверяется государственными органами. В частности, такие требования устанавливаются к сертификатам квалифицированной подписи; удостоверяющим центрам, выдающим такие сертификаты (например, необходимость уведомления и получения разрешения Государственного управления связи и телекоммуникаций Швеции для открытия такого удостоверяющего центра в качестве юридического лица, расширенная ответственность к возмещению ущерба и т.д.); а также к защищенным средствам создания квалифицированной электронной подписи, которые должны быть обязательно сертифицированы на соответствие общеевропейским техническим стандартам» [6, с. 473]. Шведская модель правового регулирования электронной подписи весьма приемлема и отражает стремление законодателя максимально обезопасить участников правоотношений от противоправного воздействия со стороны

злоумышленников. При этом стремление законодателя обеспечить преимущество квалифицированной электронной подписи не подразумевает его существенного вмешательства в развитие соответствующих правоотношений, что благоприятно отражается на ее использовании предпринимателями.

Обобщая все вышеизложенное в рамках данной главы, мы можем сделать следующие выводы.

Во-первых, в качестве одной из проблем регулирования электронной подписи называют отсутствие у нее универсального характера. Поскольку государство представляет собой единую систему, которую мы в некоторой степени можем рассматривать в качестве единой корпорации, то с технической точки зрения, вполне возможно создать общую экосистему ресурсов, работающих в рамках одних и тех же алгоритмов. Это в свою очередь позволит создать единую электронную подпись, которая будет использоваться предпринимателем при любых взаимодействиях с органами государственной и муниципальной власти. При этом необходимо учитывать, что создание единой экосистемы приведет к повышению рисков, связанных с утерей или неправомерным завладением электронной подписи третьими лицами. Поэтому при разработке законопроекта о создании единой экосистемы государственных и муниципальных цифровых ресурсов, параллельно необходимо обеспечить максимальную защиту электронной подписи, в целях избежания неправомерного доступа и иных противоправных действий со стороны злоумышленников.

Во-вторых, другая проблема правового регулирования электронной подписи связана с ответственностью за нарушение соответствующих правовых норм. В частности, нами было отмечено, что в статье 13.33 Кодекса об административных правонарушениях предусмотрены весьма небольшие штрафы. На наш взгляд, такой размер штрафа является чрезмерно мягким наказанием, поскольку указанные действия могут привести к серьезным последствиям для предпринимателя. Ранее мы указывали, что внесение

информации об отзыве электронной подписи и ее аннулировании, позволяет злоумышленнику и дальше реализовывать свои мошеннические схемы. Однако, в силу того, что наказание за рассматриваемое деяние чрезмерно мягкое, удостоверяющий центр может не разбираться в вопросе и игнорировать вполне законные требования лица, от имени которого неправомерно была выпущена электронная подпись. Даже в том случае если правонарушение совершается повторно, санкция удваивается относительно размера штрафа, применяемого к удостоверяющему центру в первый раз. Таким образом, мы видим необходимость увеличить размер штрафов, предусмотренных в качестве наказания за нарушение законодательства в области электронной подписи. Поскольку актуальные размеры штрафов, на наш взгляд, являются чрезмерно низкими, в результате чего нарушается принцип соразмерности наказания содеянному административному правонарушению.

Кроме того, предлагается ввести уголовную ответственность для физических лиц за нарушение законодательства об электронной подписи. В качестве обязательных последствий нарушения законодательства об электронной подписи необходимо предусмотреть крупный ущерб, причиненный пострадавшему. В качестве квалифицирующих признаков можно предусмотреть: причинение особо крупного ущерба, совершение деяния группой лиц, совершение преступления должностным лицом Федеральной налоговой службы (в этом случае ущерб причиняется в том числе и интересам государственной службы). Кроме того, обязательным признаком преступления должна быть субъективная сторона, которая определяется умышленной формой вины.

В-третьих, рассматривая правовое регулирование электронной подписи зарубежными странами, мы можем предложить следующую классификацию. В зависимости от влияния государства на правовое регулирование электронной подписи можно выделить следующие подходы:

- минималистичный подход;

- предписывающий подход;
- двухфакторный подход.

При минималистичном подходе законодатель закладывает только основы правового регулирования, оставляя остальные вопросы нераскрытыми. Оставшиеся без внимания вопросы регулируются судебной и договорной практикой. В этом случае законодатель стремится не «привязывать» электронную подпись к положениям закона, а позволяет ей развиваться в соответствии с техническими нововведениями и актуальными реалиями рынка. Данный подход наиболее лоялен к предпринимательской деятельности, но создает высокий риск безопасности использования электронной подписи. Применяется в США, но не подходит для Российской Федерации, поскольку в условиях романо-германской правовой системы весьма сложен для реализации. Предписывающий подход подразумевает жесткий контроль правового регулирования со стороны государства, который обусловлен достичь максимального уровня безопасности и иными целями. При таком подходе система может меняться только при условии внесения соответствующих изменений в нормативно-правовое регулирование. Этот процесс может затянуться на длительное время, что негативно скажется на деятельности предпринимателя, который имеет способ оптимизировать свою деятельность, но в силу формальных обстоятельств сделать этого не может и вынужден ожидать пока соответствующая инициатива доберется до уполномоченного органа, будет рассмотрена и одобрена, после чего необходимые изменения будут внесены. Такой подход характерен для Индии. Двухфакторный подход подразумевает, что законодатель не ставит жестких рамок перед участниками правоотношений, но фактически стимулирует к использованию только одного варианта (как правило, это квалифицированная электронная подпись). Указанный подход характерен для правового регулирования электронной подписи в Швеции. В целом мы допускаем выделение смешанного подхода, который будет включать в себя характеристики обозначенных нами вариантов, поскольку в условиях высокой

динамики развития современных технологий и правоотношений, весьма сложно провести четкую градацию, которой будут соответствовать все возможные варианты.

В-четвертых, мы видим возможность закрепить в отношении сотрудников удостоверяющих центров особые критерии отбора, которые, на наш взгляд, позволят увеличить качество их работы, а также снизить вероятность их участия в мошеннических схемах, связанных с получением неправомерного доступа к электронной подписи. К числу таких требований мы можем отнести: отсутствие судимостей у сотрудника или его близких родственников, наличие высшего образования в сфере IT, полученного в образовательном учреждении, имеющем государственную аккредитацию. Кроме того, можно обязать лицо пройти специальные курсы, целью которых будет формирование представления о правовом регулировании электронной подписи и защите персональных данных, а также представлен информациях об актуальных мошеннических схемах с применением электронных подписей.

Кроме того, проанализировав различные варианты правового регулирования электронной подписи, мы пришли к выводу, что законодатель не должен устанавливать каких-то жестких рамок относительно использования электронной подписи. В особенности это касается предпринимателей, для которых электронная подпись является инструментом расширения бизнеса. Основная задача правового регулирования в данной сфере заключается в том, чтобы обеспечить максимальную безопасность участников правоотношений. При этом же сами способы и иные особенности применения электронной подписи должны оставаться на усмотрение предпринимателя, поскольку отсутствие ограничений по данному вопросу будет способствовать обеспечению развития рыночных отношений.

Заключение

Легальное определение понятия электронная подпись предусмотрена в статье второй Федерального закона «Об электронной подписи». К числу признаков, характеризующих сущность и назначение электронной подписи, мы можем отнести следующие аспекты. Во-первых, электронная подпись представляет собой информацию, то есть, определенный набор данных. Во-вторых, информация-подпись имеет активную фазу, когда она присоединяется к другой подписываемой информации. В-третьих, основной целью электронной подписи является подтверждение подлинности личности лица, которое подписывает информацию. В-четвертых, электронная подпись основана на криптографических алгоритмах. Особая система шифрования позволяет генерировать специальные ключи при каждом использовании. Кроме того, для электронной подписи характерна презумпция авторства. Использование электронной подписи означает, использование ее конкретным лицом – автором подписи. То есть, автор подписи в случае несогласия с тем фактом, что была использована его электронная подпись, должен предоставить существенные доводы, подтверждающие факт неправомерного доступа к его зашифрованным данным.

В ходе исследования мы сделали вывод о высокой уязвимости простой электронной подписи, поскольку технологии развиты до такого уровня, что на сегодняшний день имеется возможность дублировать телефонные номера и получать поступающую на них информацию. Кроме того, нельзя забывать о постоянных утечках персональных данных, которые включают в себя информацию, вплоть до паспортных данных, которые злоумышленник может использовать при заключении кредитного договора. На наш взгляд, законодателю необходимо более подробно регламентировать вопрос заключения договоров при помощи электронной подписи. В частности, можно закрепить необходимость пройти аутентификацию при заключении договора, подписываемого простой электронной подписью, при помощи видеозвонка с

сотрудником банка и предоставления документа, удостоверяющего личность. Таким образом, удастся усилить меры безопасности и доподлинно установить авторство простой электронной подписи.

На сегодняшний день имеет место быть тенденция, которая заключается в активном использовании электронной подписи «крупным бизнесом», в то время как представители малого и среднего предпринимательства неоднозначно относятся к данному правовому инструменту. Крупному бизнесу удается перекрыть те недостатки, которые характерны электронной подписи, посредством повышения прибыли за счет тех возможностей, которые можно получить с ее помощью (увеличение клиентской базы, упрощение документооборота и так далее). Малый и средний бизнес, как правило, не обладает необходимым ресурсом, чтобы справиться с таким огромным потоком заказов или клиентов, кроме того, документооборот в нем значительно меньше, поэтому в должной степени им не удается оценить все преимущества электронной подписи. В этой связи недостатки, которые характерны для нее, куда более значительно выражены. Именно таким образом, мы можем объяснить сложившуюся тенденцию использования электронной подписи в предпринимательской деятельности.

С учетом развития технологий мы прослеживаем положительную тенденцию внедрения электронной подписи в предпринимательскую деятельность. Однако, нельзя утверждать, что подавляющее большинство предпринимателей в ближайшее время примут решение о ее использовании в своем бизнесе. Для этого необходимо максимально упростить ее использование, а также решить ряд проблемных аспектов, характерных ее правовому регулированию. До этого на практике будут возникать случаи, когда один из контрагентов может использовать электронную подпись, а другой, напротив, не использует ее. В этом случае возникнут следующие проблемы. Тот контрагент, который не имеет электронной подписи, не сможет провести проверку статуса документа, поскольку у него отсутствует соответствующее программное обеспечение. В этом случае возникнет необходимость в

использовании бумажных носителей, что, соответственно, приведет к дублированию документооборота. Это снижает эффективность электронной подписи в вопросе упрощения ведения архивной документации, поскольку оставляет необходимость вести часть документов в бумажном формате.

В рамках проведенного исследования нами были предложены следующие рекомендации, направленные на совершенствование законодательства об электронной подписи.

Во-первых, весьма сомнительными видятся нам правила электронной площадки, по смыслу которых вся ответственность за переход доступа электронной подписи к третьим лицам возлагается на автора подписи. При помощи данного пункта площадка стремится снять с себя всю ответственность в случае потенциального возникновения спора. Но такой подход не совсем корректен. Неправомерное выбытие электронной подписи происходит не по воле клиента, кроме того, долгое время клиент может не знать об этом, и, соответственно, не принимать никаких действий. Мы придерживаемся мнения, что юридический автор электронной подписи, несмотря на внутренние правила площадки, не должен нести ответственность, если докажет, что доступ к подписи был получен третьими лицами неправомерным способом. В этой связи мы считаем необходимым закрепить соответствующее правило в нормативно-правовой базе, регулирующие вопросы использования электронной подписи, а также привести в соответствии с данным положением правила и регламенты электронных площадок.

Во-вторых, вопросы ответственности нарушение законодательства об электронной подписи, а также неправомерного получения доступа к электронной подписи недостаточно раскрыты законодателем.

Мы видим необходимость закрепить в Уголовном кодексе Российской Федерации отдельную статью, предусматривающую ответственность за хищение информации (носителя информации) составляющую электронную подпись. Поскольку предпринимательская деятельность непосредственно связана с более высокими имущественными и иными рисками (например,

возможность заключить кредитный договор на более крупную сумму, доступ к персональным данным сотрудников или клиентов предпринимателя и так далее), то хищение электронной подписи индивидуального предпринимателя или юридического лица представляет повышенную общественную опасность. В связи с этим указанное деяние в отношении специального потерпевшего необходимо рассматривать в качестве квалифицирующего признака. Кроме того, нельзя не учитывать тот факт, что электронная подпись, похищенная у лица, являющегося должностным лицом на должности государственной или муниципальной службы, нотариуса, а также лиц, замещающих должность государственной или муниципальной службы, в руках злоумышленника может создать дополнительную угрозу для общества, государства, а также интересам государственной и (или) муниципальной службы. В этой связи рассматриваемое деяние в отношении указанных лиц должно рассматриваться в качестве особо квалифицирующего признака и предусматривать повышенную ответственность для преступника.

Кроме того, предлагается ввести уголовную ответственность для физических лиц за нарушение законодательства об электронной подписи. В качестве обязательных последствий нарушения законодательства об электронной подписи необходимо предусмотреть крупный ущерб, причиненный пострадавшему. В качестве квалифицирующих признаков можно предусмотреть: причинение особо крупного ущерба, совершение деяния группой лиц, совершение преступления должностным лицом Федеральной налоговой службы (в этом случае ущерб причиняется в том числе и интересам государственной службы). Кроме того, обязательным признаком преступления должна быть субъективная сторона, которая определяется умышленной формой вины.

В частности, нами было отмечено, что в статье 13.33 Кодекса об административных правонарушениях предусмотрены весьма небольшие штрафы. На наш взгляд, такой размер штрафа является чрезмерно мягким наказанием, поскольку указанные действия могут привести к серьезным

последствиям для предпринимателя. Ранее мы указывали, что внесение информации об отзыве электронной подписи и ее аннулировании, позволяет злоумышленнику и дальше реализовывать свои мошеннические схемы. Однако, в силу того, что наказание за рассматриваемое деяние чрезмерно мягкое, удостоверяющий центр может не разбираться в вопросе и игнорировать вполне законные требования лица, от имени которого неправомерно была выпущена электронная подпись. Даже в том случае если правонарушение совершается повторно, санкция удваивается относительно размера штрафа, применяемого к удостоверяющему центру в первый раз. Таким образом, мы видим необходимость увеличить размер штрафов, предусмотренных в качестве наказания за нарушение законодательства в области электронной подписи. Поскольку актуальные размеры штрафов, на наш взгляд, являются чрезмерно низкими, в результате чего нарушается принцип соразмерности наказания содеянному административному правонарушению.

В-третьих, мы видим возможность закрепить в отношении сотрудников удостоверяющих центров особые критерии отбора, которые, на наш взгляд, позволят увеличить качество их работы, а также снизить вероятность их участия в мошеннических схемах, связанных с получением неправомерного доступа к электронной подписи. К числу таких требований мы можем отнести: отсутствие судимостей у сотрудника или его близких родственников, наличие высшего образования в сфере IT, полученного в образовательном учреждении, имеющем государственную аккредитацию. Кроме того, можно обязать лицо пройти специальные курсы, целью которых будет формирование представления о правовом регулировании электронной подписи и защите персональных данных, а также представлен информациях об актуальных мошеннических схемах с применением электронных подписей.

Кроме того, в качестве одной из проблем регулирования электронной подписи называют отсутствие у нее универсального характера. Поскольку государство представляет собой единую систему, которую мы в некоторой

степени можем рассматривать в качестве единой корпорации, то с технической точки зрения, вполне возможно создать общую экосистему ресурсов, работающих в рамках одних и тех же алгоритмов. Это в свою очередь позволит создать единую электронную подпись, которая будет использоваться предпринимателем при любых взаимодействиях с органами государственной и муниципальной власти. При этом необходимо учитывать, что создание единой экосистемы приведет к повышению рисков, связанных с утерей или неправомерным завладением электронной подписи третьими лицами. Поэтому при разработке законопроекта о создании единой экосистемы государственных и муниципальных цифровых ресурсов, параллельно необходимо обеспечить максимальную защиту электронной подписи, в целях избежания неправомерного доступа и иных противоправных действий со стороны злоумышленников.

Список используемой литературы и используемых источников

1. Аннин А.Г., Новиков С.С. Электронная подпись: понятие и практика применения // Аграрное и земельное право. 2020. №8 (188). С. 159-163.

2. Асеев А.А. Макаров В.В., В.Е. Наружный Проблемы и практика использования электронной цифровой подписи // Экономика и бизнес: теория и практика. 2021. №1-1. С. 20-23.

3. Бабанцев А.Д. Некоторые проблемы правового регулирования использования цифровой (электронной) подписи // Фестиваль права. 2021. С. 220-222.

4. Билокапич А.В. Международный опыт и зарубежное законодательство в сфере регулирования электронного документооборота // Молодой ученый. 2022. № 20 (124). С. 490-497.

5. Билалова Д. Г.-К., Магомедов Н.Н. Понятие электронной цифровой подписи // Инновационная наука. 2022. №2-1. С. 6-8.

6. Волкова Н.С. Сравнительно-правовой анализ российского и шведского законодательства, регулирующего отношения в информационной сфере // Экономика и социум. 2021. №7 (26). С. 471-474.

7. Гагауз О.А., Гребень А.А., Морозова Е.Е. Электронная подпись: понятие и практика применения // Наука и образование: отечественный и зарубежный опыт. 2023. С. 288-294.

8. Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51-ФЗ (ред. от 08.08.2024 // СЗ РФ. 1994. №32. Ст. 3301.

9. Гражданский кодекс Российской Федерации (часть вторая) от 26.01.1996 № 14-ФЗ (ред. от 24.07.2023) // СЗ РФ. 1996. №5. Ст. 410.

10. Гражданский процессуальный кодекс Российской Федерации от 14.11.2002 № 138-ФЗ (ред. от 08.08.2024) // СЗ РФ. 2002. №46. Ст. 4532.

11. Гуляев Д.А. Принцип работы электронной цифровой подписи и ее применение на практике // Современные информационные технологии и информационная безопасность. 2022. С. 97-100.

12. Дарькина М.М. Практика использования электронной подписи в предпринимательской деятельности // Право и цифровая экономика. 2020. №3(09). С. 28-35.

13. Дмитриев М.Н. Порядок оформления и выдачи электронной подписи пользователям в удостоверяющем центре // Безопасность информационного пространства. 2024. С. 127-134.

14. Ефремова А.В. Правовое регулирование порядка использования электронного документа и электронной подписи // Вестник студенческого научного общества ГОУ ВПО «Донецкий национальный университет» 2021. № 13. С. 187-192.

15. Как происходит мошенничество с электронной подписью и как его избежать // [Электронный ресурс]. https://www.nalog.gov.ru/rn89/news/activities_fts/11197417/ (дата обращения: 10.10.2024).

16. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (ред. от 14.10.2024) // СЗ РФ. 2002. №1. Ст. 1.

17. Лаврушкина А.А. Проблемы применения статьи 159. 6 УК РФ с позиции теории и практики // Контентус. 2020. №3 (68). С. 28-35.

18. Митрофанов В.В. Вопросы правового регулирования использования электронной подписи в современной России // Юридический вестник Кубанского государственного университета. 2020. №4(21). С. 37-38.

19. Определение Верховного Суда РФ от 11.04.2022 № 305-ЭС21-27249 по делу № А40-212650/2020 // Консультант плюс: справочно-правовая система.

20. О развитии законодательства в целях предупреждения преступлений, связанных с использованием электронной подписи //

[Электронный ресурс]. https://www.garant.ru/ia/opinion/author/stavickii/1295999/ (дата обращения: 10.10.2024).

21. Получен отказ в выдаче сертификата – Электронная подпись // [Электронный ресурс]. URL: https://support.kontur.ru/ca/38770-poluchen_otkaz_v_vydache_sertifikata (дата обращения: 10.10.2024).

22. Проценко В.В. Проблемы применения и правового регулирования электронно-цифровой подписи в Российской Федерации // Традиции и новации в системе современного российского права. 2020. С. 571-573.

23. Решение Арбитражного суда Свердловской области от 22 июня 2021 г. по делу № А60-2524/2021 // Консультант плюс: справочно-правовая система.

24. Решение Шпаковского районного суда № 2-248/2021 2-248/2021(2-3011/2020;)~М-2894/2020 2-3011/2020 М-2894/2020 от 25 марта 2021 г. по делу № 2-248/2021 // Консультант плюс: справочно-правовая система.

25. Соловяненко Н.И. Правовой режим квалифицированной подписи и ее функции в механизме защиты прав участников электронного взаимодействия // Гуманитарные, социально-экономические и общественные науки. 2022. №12. С. 236-240.

26. Соловяненко Н.И. Юридическое значение электронной подписи в правовых отношениях электронного бизнеса // Colloquium-journal. 2020. №8 (60). С. 173-176.

27. Стародумова С.Ю. Цифровые инструменты и процедуры электронной коммерции в зарубежных правопорядках // Право: история и современность. 2023. №2. С. 241-247.

28. Титов Н.А. Электронная подпись: проблемы правового регулирования // Кооперация науки и общества: проблемы и перспективы. 2021. С. 153-163.

29. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 25.10.2024) // СЗ РФ. 1996. №25. Ст. 2954.

30. Федеральный закон от 27.07.2010 № 210-ФЗ (ред. от 08.07.2024) «Об организации предоставления государственных и муниципальных услуг» // СЗ РФ. 2010. №31. Ст. 4179.

31. Федеральный закон от 06.04.2011 № 63-ФЗ (ред. от 04.08.2023) «Об электронной подписи» // СЗ РФ. 2011. №15. Ст. 2036.

32. Федеральный закон от 05.04.2013 № 44-ФЗ (ред. от 08.08.2024) «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» // СЗ РФ. 2013. №14. Ст. 1652.

33. Федеральный закон от 27.11.2018 № 422-ФЗ (ред. от 08.08.2024) «О проведении эксперимента по установлению специального налогового режима «Налог на профессиональный доход» // СЗ РФ. 2018. №49. Ст. 7494.

34. Фролова Е.Е., Берман А.М. Способы волеизъявления сторон в условиях цифровой трансформации: актуальные тренды правоприменения // Право. Журнал высшей школы экономики. 2024. №3. С. 57-83.

35. Хоружий В.В. Электронная цифровая подпись: вопросы правового регулирования // Юридическая наука в XXI веке: актуальные проблемы и перспективы их решений. 2020. С. 153-155.

36. Шеметова О.В., Чугунова С.В. Некоторые проблемы применения электронной подписи в управленческой деятельности предприятий и пути их решения // Актуальные проблемы авиации и космонавтики. 2021. №13. С. 425-427.

37. Шестопал С.С., Рубичев Д.В. Законодательный опыт регламентации применения цифровой подписи в странах азиатского-тихоокеанского региона на примере Сингапура, Японии и Южной Кореи // Вопросы устойчивого развития общества. 2021. №1. С. 168-173.

38. Шмагун А.А. Правовое регулирование электронных документов и электронных подписей в Соединенных штатах Америки и Королевстве Швеция // Сборник 70-ой конференции юрфака БДУ. 2022. С. 119-123.

39. Щепотин А.В. Цифровые аспекты современного права: перспективы цифровизации и электронного документооборота //

Модернизация российского общества и образования: новые экономические ориентиры, стратегии управления, вопросы правоприменения и подготовки кадров. 2023. С. 560-564.

40. Щука И. О., Нестеренко И. С., Нестеренко Г. А. Перспективы, достоинства и недостатки электронной подписи // МНИЖ. 2023. №2 (128). С. 1-5.

41. Berkovits L. Germany: Digital Signatures Ordinance // International Legal Materials. 2018. № 37(3). P. 579-586.

42. Christopher Reed. Legally Binding Electronic Documents: Digital Signatures and Authentication // The International Lawyer. 2021. № 35. P. 89-106.

43. Darrel Menthe. Jurisdiction in Cyberspace: A Theory of International Spaces. // Mich. Telelecomm. Tech. L. 2018. P. 69–103.

44. Emad A-R. Dahiyat The Legal Recognition of Electronic Signatures in Jordan: Some Remarks on the Electronic Transactions Law // Arab Law Quarterly. 2021, №. 3. P. 297-309.

45. Randolph Kahn. Law’s Great Leap Forward: How Law Found a Way to Keep Pace with Disruptive Technological Change // Business Law Today. 2020. P. 1-4.