МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

имени М.В. Ломоносова

ЮРИДИЧЕСКИЙ ФАКУЛЬТЕТ

Кафедра предпринимательского права

КУРСОВАЯ РАБОТА

«Идентификация субъектов предпринимательских правоотношений в цифровой экономике»

Выполнила: студентка 215 группы

Чернякова Мария

Дмитриевна

Научный руководитель:

д.ю.н., доцент,

Вайпан Виктор

Алексеевич

Дата представления курсовой работы в учебный отдел:

«___»_____ 202__ г.

Дата сдачи научному руководителю: «___»_____ 202__ г.

Дата защиты курсовой работы: «___»_____ 202__ г.

Оценка: _____

МОСКВА - 2020 год

Оглавление

Введение

Актуальность темы исследования.

На данный момент актуальность проблем формирования цифровой экономики объясняется ростом её влияния на общество в целом, а также темпами её развития. Одной из таковых проблем как раз является идентификация лиц в цифровой экономике, без решения которой нельзя было бы никак установить участников правоотношений в цифровой среде.

Цифровая экономика представляет собой систему экономических отношений, в которой данные в цифровой форме являются ключевым фактором производства во всех ее сферах[1]. У новой экономики есть ряд преимуществ перед традиционным рынком товаров и услуг, так как исчезает необходимость в громоздкой транспортной инфраструктуре, уходит бумажный документооборот, сам рынок расширяется, становясь глобальным и доступным. Но несмотря на все положительные стороны такой экономики не до конца очевидны способы её правового регулирования, так как даже сами участники не успевают следить за изменениями, происходящими в ней. При этом оставить без законодательного регулирования цифровую среду нельзя, так как иначе все действия, совершаемые в ней, не будут получать надлежащей правовой защиты по сравнению с аналогичными действиями, совершаемыми в традиционной экономике, что может застопорить её дальнейшее развитие. Так что перед законодателем встаёт задача выявления закономерностей отношений, формирующихся в цифровой экономике, для создания особого юридического подхода для их регулирования[2].

Правовое регулирование требуется как на международном, так и на национальном уровне. В Российской Федерации стратегия цифрового развития является высокоприоритетной и определена в специальном Указе Президента до 2030 года[3]. В соответствии с данным Указом Правительством Российской Федерации была

---

[1] Современные информационные технологии и право: монография / А. С. Ворожевич, Е. В. Заиченко, Е. Е. Кирсанова и др ; отв. ред. Е. Б. Лаутс; Моск. гос. ун-т имени М. В. Ломоносова, Юрид. ф-т. — Москва : Статут, 2019. — 288 с. — (Труды Юридического факультета : кн. 15).

[2] Вайпан В.А. Теория справедливости: право и экономика: Монография. М.: Юстицинформ, 2017. С. 126

[3] Указ Президента РФ от 09.05.2017 N 203 "О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы" // Справочная правовая система «КонсультантПлюс»

определена национальная программа «Цифровая экономика Российской Федерации». Правительство совместно с органами государственной власти субъектов Российской Федерации должно решить задачи по созданию «системы правового регулирования цифровой экономики, основанную на гибком подходе в каждой сфере, а также внедрение гражданского оборота на базе цифровых технологий»[4]. Всё это направлено на исполнение предписаний, заложенных в национальной программе, основной целью которой является формирование единой цифровой среды доверия[5]. Надо отметить, что на 2017 год Правительство Российской Федерации издало Распоряжение «Об утверждении программы "Цифровая экономика Российской Федерации"», которое утратило юридическую силу 12.02.2019, но с точки зрения закреплённых в нём идей осталось актуальным. В целях дальнейшего развития этих идей президиумом Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам был утвержден Паспорт национальной программы «Цифровая экономика Российской Федерации», который содержит специальный федеральный проект «Нормативное регулирование цифровой среды»[6].

Одной из угроз для развития цифровой экономики России являются проблемы обеспечения прав человека в цифровом мире, в том числе при идентификации, сохранности данных пользователей, создания среды доверия – всё это нашло закрепление в старой программе «Цифровая экономика Российской Федерации». В паспорте федерального проекта «Нормативное регулирование цифровой среды» указано, что эти проблемы решаются, и что уже были достигнуты результаты в формировании среды доверия, но пока все планы по созданию информационной инфраструктуры не выполнены[7].

---

[4] Указ Президента РФ от 07.05.2018 N 204 (ред. от 19.07.2018) "О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года" // Справочная правовая система «КонсультантПлюс»

[5] Правовое регулирование экономических отношений в современных условиях развития цифровой экономики : монография / отв. ред. В. А. Вайпан, М. А. Егорова. М. : Юстицинформ, 2019 ;

[6] https://futurerussia.gov.ru/cifrovaya-ekonomika

[7] Паспорт федерального проекта Нормативное регулирование цифровой среды (утв. президиумом Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности, протокол от 28.05.2019 N 9) //sudact.ru/law/pasport-federalnogo-proekta-normativnoe-regulirovanie-tsifrovoi-sredy/

А значит, если в условиях быстроразвивающейся цифровой экономики невозможно универсальное решение этих проблем «на века», то тема моей курсовой будет оставаться актуальной, так как законодателю придётся соответствовать в юридической технике вызовам цифровой среды.

Эта тема ещё широко не освещалась в доктрине, так как само понятие цифровой экономики вошло в систему права сравнительно недавно. В своей работе я попытаюсь раскрыть особенности идентификации субъектов предпринимательских правоотношений и её законодательному урегулированию на данный момент времени.

Цель и задачи исследования.

Целью исследования является изучение способов идентификации лиц в цифровой экономике и использование этого в предпринимательской деятельности. Решение следующих **задач** позволяет достичь поставленной цели:

1. Изучение видов цифровых идентификаторов;
2. Рассмотрение нормативного правового регулирования идентификации субъектов в цифровой экономике, в особенности соотнесение с законодательством «о защите персональных данных»;
3. Изучение правовых основ применения различных способов идентификации в предпринимательской деятельности.

Объект и предмет исследования.

Предметом исследования являются нормативные правовые акты и правоприменительная практика, связанные с использованием способов идентификации лиц в целях развития предпринимательских отношений в цифровой экономике.

Объект исследования – общественные отношения, складывающиеся в сфере идентификации в цифровой экономике.

Методами исследования являются классификация, обобщение, анализ литературы.

Глава 1. Правовое регулирование единой цифровой среды доверия для субъектов предпринимательской деятельности

Участники цифровой экономики нуждаются в своей деятельности в таких средствах дистанционных коммуникаций, которым они могли бы «доверять». Для формирования единой цифровой среды доверия нужна соответствующая правовая база, где были бы определены, помимо прочего, основные понятия, присущие «цифровой экономике», способы удаленного подтверждения личности лица для совершения сделок (идентификация и аутентификация) и равнозначный статус таких способов в правоприменительной практике, закреплено правовое признание обществом электронного взаимодействия равным образом с очно-бумажным, закреплена возможность использования сервисов третьей доверенной стороной на цифровом рынке[8].

Одна из основных задач на пути к формированию такой среды связана с решением проблемы идентификации субъектов предпринимательских правоотношений: необходима унификация требований ко всем участникам правоотношений, расширение способов идентификации и их признание всеми сторонами. На данный момент правовая база только начинает формироваться, например, был внесён на рассмотрение проект федерального закона № 747513-7 «О внесении изменений в отдельные законодательные акты (в части уточнения процедур идентификации и аутентификации)» и были приняты законопроекты № 747528-7 «О внесении изменений в некоторые законодательные акты Российской Федерации в связи с совершенствованием регулирования в сфере электронной подписи» № 728232-7 «О внесении изменений в Федеральный закон „О государственной регистрации недвижимости“»[9]. К настоящему моменту были внесены поправки в федеральные законы "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма", "Об электронной подписи", "О связи", "Об организации

[8] Вайпан В.А. Правовое регулирование цифровой экономики // Предпринимательское право. Приложение "Право и Бизнес". 2018. N 1. С. 12 - 17.
[9] Виктор Наумов «Цифровая среда доверия» // Комментарий для журнала «Закон» URL:https://zakon.ru/blog/2019/10/16/cifrovaya_sreda_doveriya__kommentarij_dlya_zhurnala_zakon#_ftnref1

предоставления государственных и муниципальных услуг". Правительством РФ была принята Концепция введения в РФ удостоверения личности гражданина РФ с помощью пластиковой карты с электронным носителем информации[10]. Но, говоря по справедливости, положения этой концепции не получили ожидаемого дальнейшего развития. Так, в 2017 году был остановлен выпуск в Российской Федерации универсальных электронных карт, с помощью которых хотели организовать предоставление государственных и муниципальных услуг в электронном виде, обеспечить межведомственное электронное взаимодействие, создать базовые информационные ресурсы[11]. Также, на данный момент Постановлением Правительства РФ МВД России было предписано отложить мероприятия по введению на территории РФ удостоверения личности, оформленного в виде пластиковой карты с электронным носителем информации, в качестве основного документа, удостоверяющего личность гражданина РФ, а значит, в скором будущем не стоит ждать замены бумажного паспорта на электронный[12].

Безусловно, проблема идентификации и аутентификации субъектов предпринимательских правоотношений сложна еще и тем, что не выработано единого подхода к её решению. С одной стороны, предлагается создать универсальный цифровой идентификатор, например, по образцу квалифицированной усиленной электронной подписи, которая активно применяется во взаимоотношениях с государственными органами. С другой стороны, ограничивать бизнес в использовании разных способов и уровней

10 Распоряжение Правительства РФ от 19.09.2013 N 1699-р (ред. от 22.05.2018) <Об утверждении Концепции введения в Российской Федерации удостоверения личности гражданина Российской Федерации, оформляемого в виде пластиковой карты с электронным носителем информации, и плана мероприятий по реализации Концепции> (вместе с "Концепцией введения в Российской Федерации удостоверения личности гражданина Российской Федерации, оформляемого в виде пластиковой карты с электронным носителем информации, в качестве основного документа, удостоверяющего личность гражданина Российской Федерации на территории Российской Федерации") // Справочная правовая система «КонсультантПлюс»

11 Федеральный закон от 28.12.2016 N 471-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации"// Справочная правовая система «КонсультантПлюс»

12 Постановление Правительства РФ от 16.04.2016 N 315 "О мерах по оказанию содействия избирательным комиссиям в реализации их полномочий при подготовке и проведении выборов депутатов Государственной Думы Федерального Собрания Российской Федерации седьмого созыва"//Справочная правовая система «КонсультантПлюс»

идентификации и аутентификации нельзя, так как это может отразиться на безопасности цифровых сделок между хозяйствующими субъектами. Предприниматели, в свою очередь, нуждаются в упрощённом порядке идентификации для своих клиентов, дистанционном сборе и обновлении данных о них.

§1. Создание правовой системы идентификации и аутентификации субъектов предпринимательской деятельности

В мире не существует единой системы идентификации и аутентификации субъектов в интернете, что объяснимо тем, что цифровая экономика динамично развивается, в том числе благодаря электронной коммерции, а установление жестких правовых и технических рамок только бы помешало её развитию. В документе, учредившем ICANN[13], указано, что «частный сектор» стоит во главе развития Интернета, а главной целью является создание простой, предсказуемой, непротиворечивой правовой среды для электронной коммерции[14].

На данный момент на международном уровне существуют только рамочные акты, регулирующие взаимодействие предпринимателей и других участников в цифровой среде. Так, существует Типовой закон об электронной торговле Комиссии ООН по праву международной торговли (UNICITRAL). В п. 57 ст. 7 Типового закона указывается, что устанавливается «гибкий подход» к способу идентификации и его надежности с помощью договоренности между «составителем и адресатом сообщения данных». Выбранный способ не должен противоречить установленным законом требованиям и соответствующей цели, для которой это было нужно. В п. 58 той же статьи перечислены технические и коммерческие факторы, которые должны быть учтены при выборе метода (способа) идентификации сторон. Среди них стоит отметить такие критерии как: вид и объем сделки, частотность сделок между сторонами, «степень принятия или неприятия» способа идентификации, наличие альтернативных способов идентификации и затраты на их использование - из этого можно сделать заключение, что стороны в рамках этого закона свободны в выборе средств взаимодействия и необходимости в универсальном идентификаторе нет. Подтверждение тому закреплено п. 59 той же статьи, в котором обозначена цель на установление лишь руководящих указаний, которые в свою очередь могут

[13] Расшифровывается как «Корпорация по управлению доменными именами и IP-адресами» - независимая организация, принимает активную роль в создании безопасного интернет-пространства»

[14]«Учредительный договор Интернет-корпорации по присвоению имён и номеров» утверждён Правлением ICANN 9 августа 2016 года и передан Государственному секретарю штата Калифорния 3 октября 2016 года // https://www.icann.org/resources/pages/governance/governance-en

раскрываться в виде императивных норм национального права или оставаться на усмотрение сторон. Стоит также отметить, что несмотря на свободу, предоставленную сторонам этим документом, в нём отмечается, что сама по себе договоренность по поводу средства не будет придавать сообщениям юридическую силу, что последнее слово всё равно остаётся за «применимым правом за рамками Типового закона»[15].

Означает ли это, что нет смысла в создании всеобщей системы требований к способам аутентификации и идентификации, что сама идея создания единого идентификатора невыполнимая? На данный момент, можно однозначно сказать, что универсального решения нет и законодательством предусмотрена возможность обеспечения идентификации любым доступным способом, но при этом попытки по созданию единой системы предпринимаются. В Российской Федерации, например, государство пытается создать такую систему – «Единая система идентификации и аутентификации» (далее ЕСИА).

ЕСИА была разработана Министерством цифрового развития, связи и массовых коммуникаций России (Минкомсвязь) в рамках формирования инфраструктуры электронного правительства в целях упорядочивания и централизации процессов регистрации, идентификации, аутентификации и авторизации пользователей для предоставления государственных услуг[16].

Определение ЕСИА дано в п. 19 ст. 2 Федерального закона «Об информации, информационных технологиях и о защите информации», согласно которому «система идентификации и аутентификации - федеральная государственная информационная система, порядок использования которой устанавливается Правительством Российской Федерации, и которая обеспечивает в случаях, предусмотренных законодательством Российской Федерации, санкционированный доступ к информации, содержащейся в

[15] Резолюция Генеральной Ассамблеи ООН от 16 декабря 1996 г. N A/51/628 "Типовой закон об электронной торговле, принятый Комиссией Организации Объединенных Наций по праву международной торговли" (ЮНСИТРАЛ), и Руководство по принятию// URL: https://www.uncitral.org/pdf/russian/texts/electcom/05-89452_Ebook.pdf

[16] Распоряжение Правительства РФ от 28.07.2017 N 1632-р <Об утверждении программы "Цифровая экономика Российской Федерации"> // Справочная правовая система «КонсультантПлюс»

информационных системах»[17]. Пользователю предлагается создание единой учётной записи с различными методами аутентификаций (электронная цифровая подпись, двухфакторная аутентификация и т.д.), которая будет занесена в один из регистров (физических лиц, юридических лиц и т.д.) – при этом в целях информационной безопасности не происходит накопление данных, а лишь происходит синхронизация учетных данных, которые ведутся различными ведомствами. Благодаря этому обеспечивается доверие к личности пользователя без очной явки лица или его представителя и предъявления необходимого аналогового документа. Получается, что в создаваемой в Российской Федерации цифрой экономике происходит оцифровка данных о человеке, о юридическом лице с последующим связыванием их с учётной записью на портале государственных услуг через ЕСИА – создаётся «цифровой двойник»[18]. Перспективы такой системы для предпринимателей есть: данные пользователей (возможных клиентов), полученные при удалённой идентификации с последующей аутентификацией через ЕСИА, выступающего в качестве сквозной технологии, являются достоверными на достаточно высоком уровне. Еще в 2017 году планировалось открыть доступ коммерческим организациям к персональным данным граждан[19]. Но для иностранных агентов доступ к отечественной системе остаётся закрытым, следовательно, пользоваться своим цифровым профилем на международном уровне не получится. Сама по себе идея такой системы перспективна, но в реальном мире встречается со сложностью в исполнении, так к 2019 году ИТ-системы многих ведомств оказались не готовы к цифровым профилям («ЕСИА 2.0») (Минкомсвязь пыталось обязать их обновлять сведения о гражданах в течении суток)[20].

Таким образом, создание единой системы идентификации и аутентификации участников цифровой экономики возможно, но пока это или требует огромных затрат на техническое оснащение и соответствующее

[17] Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 19.07.2018) "Об информации, информационных технологиях и о защите информации" // Справочная правовая система «КонсультантПлюс»
[18] http://www.tadviser.ru/a/395520
[19] http://www.tadviser.ru/a/119311
[20] https://www.rbc.ru/technology_and_media/11/12/2019/5dee6b1c9a794757c7137684

нормативное регулирование в целях информационной безопасности, или иного подхода, который пока не разработали.

Но необходимо помнить, что на международном и национальных уровнях превалирует принцип свободы выбора средств идентификации и аутентификации самими участниками правоотношений.

§2. Правовые основы использования электронной (мобильной, биометрической) подписи

На данный момент электронная цифровая подпись (далее ЭЦП) является одним из основных идентификаторов лица в условиях цифровой экономики.

В Модельных правилах европейского частного права (Draft of Common Frame of Reference, DCFR) раскрывается понятие электронной подписи, которое означает сведения, закрепленные в электронной форме, которые присоединены к другим сведениям или логически объединены с другими сведениями в электронной форме и которые используются как способ идентификации (I.-1:107(3)). При этом термин «электронный» означает относящийся к электронным, цифровым, магнитным, беспроводным, оптическим, электромагнитным или аналогичным техническим возможностям (I.-1:107(5))[21].

В Российской Федерации все основные положения, связанные с её применением, регулируются отдельным ФЗ «Об электронной подписи». Использование такой подписи неразрывно связано с электронным документооборотом.

Электронный документооборот (ЭДО) не является новым явлением в экономических отношениях и представляет собой замену бумажному. Так, можно определить ЭДО как «последовательность транзакций по обмену документами между его участниками, обеспечивающую некоторый регламентированный процесс по обмену документами»[22]. Основное преимущество такого документооборота связано с возможностью оптимизации с помощью него бизнес-процессов. Обмен документов между контрагентами происходит в специальных системах через операторов, что позволяет значительно уменьшить время и расходы на подготовку, обработку, доставку документов и получение платежей, также ЭДО позволяет контролировать все

[21] Модельные правила европейского частного права = Draft of Common Frame of Reference : пер. с анг. / науч. ред. Н. Ю. Рассказова. М. Статут, 2013 // Справочная правовая система «КонсультантПлюс»
[22] Приказ ФНС России от 09.11.2010 N ММВ-7-6/535@ (ред. от 25.05.2018) "Об утверждении Унифицированного формата транспортного контейнера при информационном взаимодействии с приемными комплексами налоговых органов по телекоммуникационным каналам связи с использованием электронной цифровой подписи" // Справочная правовая система «КонсультантПлюс»

изменения, происходящие с документами. На данный момент основной задачей для обеспечения функционирования ЭДО является обеспечение доверия к электронному документу, сопоставимого с уровнем доверия к бумажному аналогу[23].

Таким образом перед обществом стоит необходимость в правовом и техническом обеспечении информационной безопасности необходимой для развития ЭДО. Законодатель в п. 4 ст. 11 Федерального закона указывает условия, при которых обмен электронными сообщениями (в значении документы) в целях заключения гражданско-правовых договоров будет рассматриваться как обмен документами – при наличии в них ЭЦП или иного аналога собственноручной подписи[24]. Традиционно подпись представляет собой обязательный реквизит любого документа, но в электронном документе «неквалифицированная» и «квалифицированная» усиленная ЭЦП обладает функцией защиты электронного документа от несанкционированных изменений[25].

Наряду с национальным правом ЭЦП также регулируется на международном уровне: Комиссия ООН по праву международной торговли (UNCITRAL) приняла в 2001 г. Типовой закон по электронным цифровым подписям, который придает таким подписям равный статус с обыкновенными при условии соблюдения определенных технических требований[26].

В Федеральном законе «Об информации» в п. 4 ст. 15 указано, что законом может быть предусмотрена обязательная процедура идентификации лица, осуществляющего предпринимательскую деятельность с использованием информационно-телекоммуникационной сети, а получатель электронного сообщения от такого лица может или обязан провести проверку на установление

[23] Указ Президента РФ от 09.05.2017 № 203 «О стратегии развития информационного общества в Российской Федерации на 2017 – 2030 гг.» [Электронный ресурс] // Справочная правовая система «КонсультантПлюс»
[24] Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 19.07.2018) "Об информации, информационных технологиях и о защите информации" // Справочная правовая система «КонсультантПлюс»
[25] Семилетов С.И., Соловьев В.Ю. Законодательная база электронного документооборота в Российской Федерации // Информационное право. 2011. N 3. С. 7 - 13. // "Информационное право", 2011, N 3
[26] Курбалийя Й. Управление Интернетом / Й. Курбалийя; Координационный центр национального домена сети Интернет. – М., 2010. – 208 с. // URL: https://cctld.ru/files/books/IG-Russian-3rd.pdf

личности отправителя[27].

В качестве идентификатора лицом могут быть использованы три вида подписи: простая и усиленные неквалифицированная и квалифицированная ЭЦП (ст. 5 ФЗ «Об электронной подписи»).[28] Законодатель, соответственно, признает за документами, подписанными одной из таких подписей, различную степень достоверности и защищённости. Простая подтверждает, что документ был отправлен определенным лицом посредством паролей, кодов или иным способом; она не может быть использована для подписания документов, содержащие информацию о государственной тайне. Можно сказать, что это ЭЦП для повседневной жизни и её можно создать самому с помощью Microsoft Office, но она ограничена в применении. Неквалифицированная (далее НЭП) электронная подпись имеет ряд преимуществ перед простой, но имеет более сложный процесс получения – через удостоверяющий центр (далее УЦ). Она дополнительно позволяет подтвердить, что с момента подписания документ не менялся, используется в рамках внутреннего документооборота компании или для взаимодействия с контрагентами, если между ними заключено соглашение об использовании НЭП.

Наиболее совершенным видом является квалифицированная подпись (далее КЭП). Так согласно п. 1 ст. 6 ФЗ «Об электронной подписи» «информация в электронной форме, подписанная КЭП, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, и может применяться в любых правоотношениях в соответствии с законодательством Российской Федерации, кроме случая, если федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами установлено требование о необходимости составления документа исключительно на бумажном носителе», то есть его можно использовать широко: для работы с государственными порталами, для

[27] Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 19.07.2018) "Об информации, информационных технологиях и о защите информации"// Справочная правовая система «КонсультантПлюс»
[28] Федеральный закон от 06.04.2011 N 63-ФЗ (ред. от 23.06.2016) "Об электронной подписи"// Справочная правовая система «КонсультантПлюс»

участия в коммерческих и государственных торгах и т.д. КЭП представляет собой ключ, сформированный с помощью криптографических средств, который записан на USB носителе. Такой ключ указывается в сертификате, который выдается УЦ, аккредитованным Минэкономсвязи[29]. Иностранные электронные подписи приравниваются в России к тем видам подписей, которым они соответствуют.

ФЗ «О внесении поправок в ФЗ «Об электронной подписи» и статью 1 ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля», вступивший в силу в 2019 г., внёс следующие изменения в правовое регулирование ЭЦП: уточняется понятие аккредитованного УЦ, изменились требования, предъявляемые к нему, вводится понятие третьей стороны (юридическое лицо, которое осуществляет деятельность по проверке ЭЦП в электронных документах в конкретный момент времени в отношении подписавшего лица – сделано для формирования среды доверия). Также, нововведение касается хранение ключа ЭЦП, теперь он будет храниться в облачном сервисе, а не на USB носителе у владельца. УЦ, которое выдало ЭЦП, теперь будет хранить ЭЦП, а также использовать её по поручению соответствующих владельцев квалифицированных сертификатов[30].

Проблема же заключается в том, что раньше безопасность КЭП обеспечивалась тем, что доступ к ней был только у её правообладателя через физический контроль над материальным носителем, теперь же она находится в облаке на едином сервере УЦ, что потребует усиления его информационной защиты, а также создания безопасного доступа правообладателя к ней. В этой связи не очевидно, как же заинтересованные лица будут идентифицировать себя перед УЦ, чтобы использовать свою КЭП (пароль и логин ненадежны, а

[29] https://www.sberbank.ru/ru/s_m_business/pro_business/chto-takoe-elektronnaya-podpis-kak-poluchit-i-dlya-chego-nuzhna/

[30] Федеральный закон от 27 декабря 2019 г. N 476-ФЗ "О внесении изменений в Федеральный закон "Об электронной подписи" и статью 1 Федерального закона "О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля" // Справочная правовая система «КонсультантПлюс»

использование специального материального носителя (токена) противоречит замыслу реформы).

С другой стороны, если такая система заработает, то облачную ЕЦП можно будет получить дистанционно, после авторизации в Единой системе идентификации и аутентификации, без установки специального софта и подключения токена, то есть в том числе расширятся возможности её использования с разных устройств[31].

Еще одной разновидностью ЭЦП является мобильная подпись (далее МЭП). Особенность её заключается в том, что она выдаётся в салоне сотовой связи и не требует установления специального программного обеспечения и может использоваться с любого устройства. Да, она имеет меньшую юридическую силу, чем неквалифицированная и квалифицированная электронные подписи, но удобна в использовании. Для установки подписи нужна специальная SIM-карта и первоначальное подтверждение личности в салоне сотовой связи. Применять МЭП можно для подписания внутренней и внешней документации, налоговых деклараций, отчетности, транспортных накладных, торговых документов и т.п. Уникальный пин-код обеспечивает безопасность такой подписи. Он выдаётся при активации SIM-карты. Формируется код в соответствии со стандартами ГОСТа РФ Р-34.10-2012[32]. МЭП использует сертификат открытого ключа для идентификации пользователя. В процессе идентификации, аутентификации используется телефонный номер, на который приходят SMS с хэш-значением документа. Активация подписи происходит при помощи повторного введения пин-кода, а после проверки документа сервер передает его поставщику услуг. Для подписи документов вместе с SIM-картой в салоне связи устанавливают специальное приложение[33]. На данный момент ПАО «МегаФон» предлагает своим клиентам такую услугу.

Несмотря на применение ЭЦП, полученной в результате

[31] https://www.rbc.ru/newspaper/2019/10/18/5da876a89a79472c0bcd51a3
[32] Национальный стандарт РФ ГОСТ Р 34.10-2012 "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи" (утв. приказом Федерального агентства по техническому регулированию и метрологии от 7 августа 2012 г. N 215-ст)
[33] https://myedo.ru/elektronnaya-podpis/sfery-primeneniya/mobilnaya-elektronnaya-podpis

криптографического преобразования информации на основе использования открытого и закрытого ключа, остаётся проблема несанкционированного получения ключа электронной подписи и подписания электронных документов неуполномоченными третьими лицами[34].

Эта проблема может быть решена с помощью введения норм по биометрической привязке закрытого ключа подписи к владельцу сертификата ключа или представителя юридического лица, обладающего сертификатом на определенный вид подписи. Так, с 1 июля 2020 года вступит в силу ч. 8 ст. 15 ФЗ «Об электронной подписи», указывающая на то, что аккредитованный УЦ должен будет на основе предоставленных лицом биометрических персональных данных без личного его присутствия представить ему необходимые шифровальные (криптографические) средства для проведения идентификации в УЦ. Таким образом, доступ к КЭП будет осуществляться через предоставление своих биометрических данных, которые в данном случае будут выступать как «биометрическая подпись». ФЗ «Об информации, информационных технологиях и о защите информации» со ссылкой на ФЗ «О персональных данных» (где указаны меры по обеспечению безопасности персональных данных граждан) в п. 19 ст. 14.1 регулирует вопрос по использованию биометрических персональных данных для идентификации лиц удалено государственными органами, банками и иными организациями со ссылкой на сайт, с которого информация была взята[35].

Существуют различные технологии биометрической идентификации: по радужной оболочке глаза (для одноглазых), по лицу, по поту, микровибрации пальцев, голосу и т.д. На данный момент в Российской Федерации существует Единая биометрическая система, которая позволяет распознавать её участников по лицу и голосу. Она была создана в рамках реализации принятой в 2017 году Правительством Российской Федерации программы «Цифровая экономика

[34] Бородин М.В. Технология цифровой подписи в электронном документообороте // Информационное право. 2015. N 3. С. 42 - 45.
[35] Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 19.07.2018) "Об информации, информационных технологиях и о защите информации" // Справочная правовая система «КонсультантПлюс»

Российской Федерации» с целью формирования единой национальной платформы для доступа граждан к государственным и коммерческим услугам. С помощью данной системы можно будет не только идентифицировать лицо, но получить полную информацию о нём, например, подтвердить возраст.

Несмотря на все перспективы, которые открываются с использованием такой системы, встаёт вопрос о её безопасности, так как утечка данных может привести к катастрофическим последствиям. На сайте разработчиков этой программы указано, что «для обеспечения информационной безопасности биометрических данных пользователей системы реализовано распределенное хранение данных: биометрический шаблон хранится в обезличенной форме отдельно от персональных данных - Ф.И.О., паспортные данные, СНИЛС и др., включенных в базы ЕСИА (портал Госуслуг)». Таким образом, обмануть биометрические алгоритмы будет достаточно сложно, но если это всё-таки случилось, то хранитель этой информации несёт ответственность за такую ошибку[36].

[36] https://bio.rt.ru/faq/security/

Глава 2. Влияние цифровых технологий на развитие предпринимательских отношений (правовые аспекты)

Швейцарский экономист Клаус Шварц предполагает, что вместе с промышленными революциями происходит смена технологических укладов. На данный момент происходит четвертая промышленная революция, которая характеризуется сменой экономических, политических и социальных отношений в связи с переходом от цифровизации к инновациям, базирующимся на комбинациях технологий. В основе революции будет лежать развитие новой технологической среды[37]. Эти процессы также влияют на предпринимательскую деятельность. Ключевым фактором для развития бизнеса в сегодняшних условиях становится применение инновационных технологий, которые позволяются существенно повысить эффективность и качество в процессе предпринимательства и потребления товаров, работ и услуг[38].

С этими процессами также связано появление цифровых объектов гражданских и предпринимательских правоотношений (токены, криптовалюты, смарт-контракты). Перед предпринимательским правом в связи с этим встаёт задача по разработке правовой защиты интересов обладателей электронных активов, по выявлению особенностей совершения юридически значимых действий с данными объектами, по определению баланса между правами и обязанностями сторон в смарт-контрактах. Свобода договора рассматривается как свобода присоединения участников к соответствующей информационной системе, а электронная форма документов становится эквивалентом письменной. В этих условиях особым образом должен быть урегулирован процесс идентификации[39].

[37] Шваб К. Четвертая промышленная революция. М.: Эксмо, 2016

[38] Макаренко А.В. Цифровая экономика как драйвер инновационной предпринимательской деятельности / А.В.Макаренко // Экономика и предпринимательство. — 2018. — №3 (92). — С. 603-609. (URL: https://elibrary.ru/download/elibrary_32844053_59059121.pdf)

[39] Статья: Предпринимательское право в условиях инновационной (цифровой) экономики: пути развития (Лаптев В.А., Соловяненко Н.И.) ("Юрист", 2019, N 5)

§1. Правовые основы использования технологий распределенных реестров (блокчейн) для цифровой идентификации субъектов предпринимательской деятельности

Блокчейн (англ. blockchain) или технология распределенного реестра представляет собой непрерывную последовательную цепочку содержащих информацию блоков. Новые блоки, добавляясь в конец цепочки, укрепляют остальные звенья. В этих блоках записывается информация о транзакциях, которая защищена криптографическими средствами от взлома. Основное преимущество использование системы блокчейн в бизнесе заключается в том, что исключается специализированный посредник, так как она позволяет фиксировать достоверные данные о принадлежности существующего в цифровой форме актива определенному лицу и передачи другому лицу. Это достигается за счёт того, что все транзакции связаны между собой за счёт последовательного шифрования (транзакции присваивается криптографический идентификатор (хеш), который добавляется в заголовок записи о следующей транзакции). При попытке изменения данных об одной транзакции, вся цепочка будет «скомпрометирована» и будет отвергнута участниками системы. Так что изменения внести почти нереально, так как на это надо получить согласие всех участников систем[40]. В том числе, такая система позволяет уберечь контрагентов от мошенничества. С помощью технологии можно отслеживать происхождение товара, его движение к месту назначения, лиц, через которых он прошёл. Например, De Beers с мая 2018 года использует технологию распределенного реестра для отслеживания самых дорогих алмазов от места их добычи до торгового представителя, защищаясь таким образом от мошенничества[41].

Блокчейн представляет собой производную технологию, но никак не самостоятельную – это лишь способ обмена цифровыми активами, в регулировании которых заинтересованы юристы. Для предпринимателей особый интерес могут представлять смарт-контракты. Смарт-контракты оформляются в

40 Савельев А.И. Договорное право 2.0: "умные" контракты как начало конца классического договорного права // Вестник гражданского права. 2016. N 3. С. 32 - 59

41 http://www.tadviser.ru/a/298820

виде особого программного кода, который исполняется автоматически при наступлении определенных условий. Для того, чтобы смарт-контракты могли исполняться автоматически, используется крипотовалюта, так как оплата ей происходит вместе с выполнением установленных задач по контракту без каких-либо препятствий (лицо, например, не может взять и отказаться от оплаты после согласия на совершения сделки)[42]. Также, в идеале для полной автоматизации выполнения контракта (по признанию некоторых специалистов такие контракты будут исполняться лучше, чем аналогичные, основанные на праве) нужна особая среда существования, в которой ничего не зависит от субъективных факторов.

Объектами умных контрактов являются подписанты, предмет договора и условия, при этом последние должны иметь полное математическое описание, которое можно запрограммировать. Подписанты для заключения смарт-контракта должны воспользоваться цифровой подписью или её аналогом для подтверждения условий и своего согласия на совершения сделки. После одобрения смарт-контракта его действие уже нельзя остановить[43]. Но все эти понятия не являются закрепленными законом, а процессы, происходящие на основании смарт-контрактов, не признаются правом. Встаёт вопрос, а есть ли в этом необходимость?

В Российском законодательстве на данный момент не урегулированы вопросы, связанные с распределенным реестром данных, с цифровыми финансовыми активами. Так, законопроект ФЗ "О цифровых финансовых активах" находится на стадии рассмотрения с 2018 года и по официальным данным с сайта www.sozd.duma.gov.ru - дата рассмотрения законопроекта во втором чтении так и не определена[44]. Еще один связанный законопроект ФЗ «О внесении поправок в части первую, вторую и четвертую Гражданского кодекса Российской Федерации» (о цифровых правах) был рекомендован к отклонению в 2019 году, но всё же был принят и поправки, внесённые им, уже вступили в силу. На мой взгляд, оба законопроекта были направлены на формирование

[42] Булгаков И.Т. Правовые вопросы использования технологии блокчейн // Закон. 2016. N 12. С. 80 - 88.
[43] http://www.tadviser.ru/a/396004
[44] https://sozd.duma.gov.ru/bill/419059-7

правовой основы для отношений, складывающихся в «децентрализованной информационной системе»[45]. Так, в ФЗ «О цифровых активах» даётся понятие таким активам, где указывается, что они не являются законным средством платежа на территории Российской Федерации, но при этом Закон даёт возможность «участникам реестра транзакций» на использование цифровых активов в своей деятельности. Фактически предполагается установить централизованную систему регулирования работы децентрализованных систем (или распределенных реестров цифровых транзакций), о чём можно судить из ст. 4 Закона. Предполагается, что бразды правления будут переданы Центральному банку Российской Федерации и Правительству Российской Федерации. «Владельцы цифровых финансовых активов вправе совершать сделки по обмену токенов на рубли, иностранную валюту только через оператора обмена цифровых финансовых активов», которым при этом и могут совершать действия с цифровыми кошельками участников. Также, для того, чтобы работать в системах распределённых реестров легально на территории РФ участники должны идентифицировать себя в соответствии с правилами ФЗ "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма"[46]. В итоге законодатель хочет создать жёсткую систему управления цифровыми активами, что разрушает основную концепцию цифровых активов и технологии распределенных реестров – открытость, работу без посредников и свободу. Может именно из-за этого законопроект "О цифровых финансовых активах" и не был принят[47].

В мире вопрос о регулировании сделок, совершенных с применением технологии блокчейн, решается не только в публичной плоскости. Так, консорциум европейских банков во главе со швейцарским UBS запустил блокчейн-платформу, которая функционирует в соответствии с новыми

[45] Проект Федерального закона N 424632-7 "О внесении изменений в части первую, вторую и четвертую Гражданского кодекса Российской Федерации" // Справочная правовая система «КонсультантПлюс»
[46] Федеральный закон от 07.08.2001 N 115-ФЗ (ред. от 23.04.2018) "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма" // Справочная правовая система «КонсультантПлюс»
[47] Проект Федерального закона N 419059-7 "О цифровых финансовых активах" // Справочная правовая система «КонсультантПлюс»

банковскими законами ЕС. Банки теперь вынуждены раскрывать больше данных и проводить более тщательные проверки клиентов и контрагентов. Каждому клиенту-юрлицу присваивается 20-значный идентификатор, содержащий всю информацию о компании (название, местоположение, отрасль и проч.). Данные компании фиксируются в распределенном реестре, каждая запись неоспорима, но ее можно обновить с помощью следующей записи. Таким образом, происходит идентификация клиентов и происходит слежение за сделками, совершенными такими лицами – вся система максимально прозрачна и надёжна[48].

Основным преимуществом использования системы блокчейн считалось анонимность пользователей. А. И. Савельев пишет, что для использования системы не нужно проходить регистрацию или идентификацию, так как достаточно установить «кошелёк» (специальное приложение). Сам кошелёк состоит из содержащихся в нём цифровых активов, публичного и частного ключа (адресы) (по аналогии с цифровой подписью)[49]. Для совершения транзакции сторона-отправитель «подписывает» договор с помощью частного ключа, отправляя биткоин или иной цифровой актив на публичный адрес стороны-получателя со своего открытого для остальных участников адреса[50]. Таким образом реальная личность лица будет скрыта, а всем остальным будет виден лишь Bitcoin-адрес участника транзакций. Тут я не соглашусь до конца с мнением профессора Савельева по поводу полной анонимности субъекта, так как первичную идентификацию он всё-таки проходит. Идентификация – это «действия по присвоению субъектам и объектам доступа идентификаторов и (или) по сравнению предъявляемого идентификатора с перечнем присвоенных идентификаторов», а первичная представляет собой действие по формированию и регистрации информации о субъекте доступа или объекте доступа с присвоением им идентификатора и включения его в перечень присвоенных

[48] https://www.vedomosti.ru/management/blogs/2018/04/18/767028-blokcheina-biznese
[49] Савельев А.И. Договорное право 2.0: "умные" контракты как начало конца классического договорного права // Вестник гражданского права. 2016. N 3. С. 32 - 60. // Справочная правовая система «КонсультантПлюс»
[50] Blockchain Technology: Beyond Bitcoin (2016), Crosby, Nachiappan, Pattanayak, Verma & Kalyanaraman // URL: https://j2-capital.com/wp-content/uploads/2017/11/AIR-2016-Blockchain.pdf

идентификаторов доступа[51]. Из этого следует, что субъект просто бы не смог завести «кошелёк» без первичной идентификации и получить публичный и частный ключ – он бы не квалифицировался как участник системы. Другой вопрос в том, что существует презумпция совпадения лица, использующего ключи при совершении транзакций, и лица, реально обладающего двумя ключами. Следовательно, встаёт вопрос об аутентификации лиц[52].

В мире уже давно поднимается идея всеобщей цифровой идентичности. FATF (Группа разработки финансовых мер борьбы с отмыванием денег) в своём консультационном документе указывает на то, что в ближайшем времени все физические и юридические лица должны быть охвачены единой системой цифровой идентичности. Таким образом планируется, что на основе наших биометрических и иных персональных данных мы сможем идентифицировать себя в интернете или, например, на кассе в магазине. Эти правила также будут применимы в бизнесе. Но как обеспечить сохранность этих данных?

Одним из способов защиты как раз является внедрение системы распределенных реестров, так как это позволяет отслеживать и сохранять информацию о тех, кто пытался получить доступ к данным клиентов[53]. На данный момент, нет единого формата применения блокчейн для защиты данных, но уже есть организации, предлагающие такие услуги на основе этой системы. Фактически, в основе сохранения личных данных о лице лежит криптографическая защита всей информации, содержащейся в блокчейне, что позволяет «рассекречивать» лишь часть персональной информации для использования, не раскрывая остальной массив. Например, это достигается с помощью гомофорного шифрования: вычисления могут происходить с зашифрованными данными без их предварительной расшифровки; только пользователи с соответствующими ключами могут получить доступ к частным сведениям о данных и транзакциях[54]. Например, компания Cambridge Blockchain

[51] https://fstec.ru/component/attachments/download/2488
[52] Рожкова М.А. Право в сфере Интернета: сборник статей / М.З. Али, Д.В. Афанасьев, В.А. Белов и др.; рук. авт. кол. и отв. ред. М.А. Рожкова. М.: Статут, 2018. 528 с. // Справочная правовая система «КонсультантПлюс»
[53] https://decenter.org/ru/fatf-cifrovaya-identichnost
[54] https://bitnovosti.com/2018/09/24/kak-blockchain-obespechit-zashhitu-personalnih-dannyh/

представляет бизнесу услуги по цифровой идентификации их клиентов на базе системы распределенных реестров и их защиты в соответствии с Общим регламентом по защите данных[55].

В соответствии с этим регламентом клиенты имеют «право на забвение» их данных (удаление из системы, что бывает технически сложно) и на передачу копий их данных другим компаниям при согласии лица. Стандартная система блокчейн не может быть использована в соответствии с этими правилами, так как не предполагает выборочное удаление информации. Сейчас можно удалить цепочку вплоть до определенного блока при согласии 51% ноды (нода — любой компьютер, подключенный к блокчейн-сети). Это сильно затрудняет выполнение положений ст. 17 Регламента, которая дает «право на забвение»). Но при этом благодаря надежности системы и прозрачности всех совершаемых действий в ней она становится базой для дальнейшей защиты данных клиентов, например, с помощью системы IDKEEP, которая работает совместно с продуктами компании Cambridge Blockchain и предлагает пользователю полный контроль над своими персональными данными.

На мой взгляд, применение технологии блокчейн в предпринимательстве – это настоящее и будущее. Так, например, технологии распределенного реестра обеспечивают среду для выполнения смарт-контрактов[56]. Но в связи с этим возникает вопрос о правовой природе таких контрактов, заключаемых на основе использования технологии блокчейн. Хотя благодаря цифровой среде и обеспечивается автоматизация выполнения обязательств по договорам, всё-таки процессы заключения договора, идентификации пользователей системы блокчейн (с возможностью аутентификации в определённых случаях) требуют правовой основы. Вопрос встаёт – регулировать сразу на международном уровне или на национальном?

---

[55] Регламент Европейского Парламента и Совета Европейского Союза 2016/679 от 27 апреля 2016 г. о защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС (Общий Регламент о защите персональных данных / General Data Protection Regulation /GDPR// Справочная правовая система «КонсультантПлюс»

[56] Кратко: самоисполнимые цифровые контракты. Программа сама исполняет контракт, встроенный в код, не нуждаясь в дополнительных действиях со стороны участников контракта.

Так как одним из преимуществ системы, что и вызывает сложность в её регулировании, заключается в трансграничности такого способа передачи активов, то не понятно под какую юрисдикцию может попадать спор между участниками транзакции. Следовательно, определённые моменты требуют международного регулирования. Также, должны быть созданы единые требования по идентификации участника в системе, которые бы соответствовали международному и национальным законодательствам. На данный момент, нет кодифицированного акта, регулирующего этот вопрос, но при этом правовое регулирование всё же наличествует пусть и в разрозненных источниках, регулирование которых направлено на защиту персональных данных, противодействию преступности и облегчение коммерческого оборота.

§2. Адаптивные системы IAM в предпринимательской деятельности

Для развития предпринимательской деятельности идентификация необходима не только самим предпринимателям для совершения сделок с контрагентами, но также и для их работников внутри предприятия.

IAM (Identity and Access Management) представляет собой набор технологий и программных продуктов, отвечающих задачам управления жизненным циклом учетных записей и управления доступом к различным системам в компании. Но более распространённым является обозначение IDM (Identity Management), что означает управление учетными записями или электронными представлениями пользователей, для предоставления им доступа к системам компании.

В небольших фирмах обслуживанием ИТ блока занимается один отдел ИТ сотрудников. Но, крупные компании вынуждены создавать несколько отделов для управления ИТ структурой компании. Несмотря на количество работников ИТ отделов управление доступом к информационным ресурсам (ИР) вручную является долгим, трудоёмким и порой неэффективным процессом. ИР могут быть расположены в разных информационных системах, которые в свою очередь могут принадлежать разным владельцам. Основной угрозой для информационной безопасности становятся риски кражи или искажения информации из-за наличия «бесхозных» учётных записей или записей с избыточными привилегиями в цифровых системах.

Так, существует целый пласт судебной практики: работник скопировал базы данных клиентов для последующей перепродажи, уволенный сотрудник удалил всю базу данных и т.д. Несмотря на то, что в таких ситуациях работодатель может обратиться в суд, чтобы возместить убытки, чаще всего он не получает возмещение. Согласно материалам дела ООО «Постер Уан» *vs.* Разумейко О.П. о взыскании денежных средств уволенный работник уничтожил клиентскую базу данных, являющейся интеллектуальной собственностью ООО «Постер Уан», и не передал свои рабочие документы новому сотруднику. При всей очевидности неправомерности действий сотрудника, тем не менее суд

встал на сторону работника, отказав истцу в удовлетворении иска[57]. Помимо неутешительной для бизнеса практики о взыскании убытков встаёт вопрос о причинённом вреде такими действиями, который порой невозможно восстановить в денежном эквиваленте.

С внедрением IDM системы эти проблемы решаются, так как управление учётными записями автоматизируется в соответствии с правилами компании. Да, установка такой системы достаточно дорогостоящая процедура, так как её использование предполагает наличие полномасштабной корпоративной ролевой модели пользователей – учитываются все информационные активы предприятия, а также описываются бизнес-роли персонала и порядок доступа для каждой из них к каждому активу[58]. Но установка такой системы оправдана для крупных компаний. Например, IDM может автоматически выбирать сервер электронной почты на основании региона пользователя при создании почтового ящика, генерировать имена учетных записей по заданным правилам транслитерации, заполнять атрибуты организационной принадлежности для системы учета затрат и т.д. IDM система следит за тем, чтобы не оставались «бесхозные» учётные записи, а доступ к частям цифровой инфраструктуры соответствовал положению работника, задачам его специальности. Система реагирует на изменение кадровых событий: приём на работу, повышение, уход в отпуск, увольнение и т.д.

Таким образом, она может оперативно реагировать на любой процесс, благодаря чему можно избежать простоя новых работников, которые не могут получить доступ к информационной среде компании. Также, дополнительным механизмом автоматизации в IDM системе является интерфейс самообслуживания – сотрудники могут запрашивать права доступа к системам, менять пароли своих учётных записях, не дожидаясь ответа из ИТ отдела. При этом всё действия, которые совершаются в цифровой инфраструктуре, записываются в журналах системы, в связи с чем снижаются затраты на

[57] Решение № 2-674/12 от 25 апреля 2012 г. Тимирязевский районный суд (Город Москва)//sudact.ru/regular/doc/NZGVZ4FJ5nNK/ (дата обращения: 13.04.2020).
[58] http://www.tadviser.ru/index.php/ИБ_-_Аутентификация

расследование правонарушений[59].

По данным, представленным на 2019 год в систему IDM были внедрены такие механизмы: контроль SOD-конфликтов (Segregation of Duties) – конфликтные полномочия, которыми не могут наделяться два лица одновременно, оценка рисков (система научилась осуществлять подсчёт рисков для каждой роли, права и ресурса)[60]. Но как достигается полный контроль за действиями работников в системе?

Решение этой задачи лежит в плоскости применения процессов идентификации, аутентификации и авторизации в сети, чем обеспечивается необходимая информационная безопасность ИР. Так, для начала работы сотруднику необходимо пройти процедуру идентификации. Затем при каждом входе в систему он проходит аутентификацию. Например, компания RSA предлагает применять мультифакторную аутентификацию для входа[61]. В РФ в основном используется в адаптивных системах модель аутентификации на основе утверждений (claim-based authentication, CBA). Такая модель состоит из трёх компонентов: доверяющей стороны, центра идентификации и пользователя. Доверяющая сторона – веб-сервис, которая запрашивает от пользователя «утверждение» (единица идентификационной информации). Центр идентификации в свою очередь выпускает электронный идентификаторы с набором «утверждений», в которых зашифрована информация о пользователе – всё это заверяется цифровой подписью центра. Центр идентификации заменяет аутентификацию пользователя на доверие к предоставляемым им «утверждениям». Вся дальнейшая ответственность за авторизацию пользователя ложится на Центр идентификации, для этого могут использоваться такие методы аутентификации как: логины/пароли, информационные карты, фактически, представляющие собой электронные паспорта[62].

[59] Мажорова Анастасия Олеговна Преимущества и варианты внедрения identity management system // Вопросы науки и образования. 2018. №8 (20). URL: https://cyberleninka.ru/article/n/preimuschestva-i-varianty-vnedreniya-identity-management-system
[60] https://acribia.ru/articles/idm-systems_or_corporate_security_issues
[61] https://www.rsa.com/en-us/products/rsa-securid-suite/rsa-securid-access
[62] https://www.cryptopro.ru/products/idm

Основным преимуществом данной системы перед ручным управлением информационной средой компании заключается ещё в том, что пользователи имеют расширенный профиль. Такой профиль может быть использован для сравнения действий и поведения пользователей в реальном времени с историческим базовым показателем, в результате чего выявляются существенные отклонения от «нормального» поведения, свидетельствующие о наличии проблем с безопасностью[63].

С точки зрения правового регулирования такая система не противоречит положениям российского законодательства. В Трудовом кодексе (ТК) урегулированы вопросы, связанные с защитой персональных данных работников. В системе указываются данные, связанные с должностью работника, а также ФИО, рабочий почтовый адрес, телефонные данные, так что положения ст. 10 ФЗ «О персональных данных» не нарушаются[64]. По смыслу ст. 87 ТК работодатель имеет право устанавливать «порядок хранения и использования персональных данных работников», а также он обязан обеспечивать защиту таких данных. Система IDM как раз направлена на обеспечение общей информационной безопасности, в том числе защитить компанию от утечки информации о персональных данных её работников[65].

Таким образом, IDM-система позволяет компании снизить издержки на ИТ-отдел, организовать безопасный сбор персональных данных работников и в целом создать работающую цифровую среду, которую могут использовать все, имеющие доступ, в соответствии с их полномочиями. Повышенные требования к идентификации, аутентификации позволяют уберечь компанию от мошенничества со стороны как работников, так и третьих лиц.

[63] http://www.tadviser.ru/a/179400
[64] Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 31.12.2017) "О персональных данных" // Справочная правовая система «КонсультантПлюс»
[65] "Трудовой кодекс Российской Федерации" от 30.12.2001 N 197-ФЗ (ред. от 03.08.2018) // Справочная правовая система «КонсультантПлюс»

Заключение

В данной работе были продемонстрированы различные подходы к идентификации субъектов предпринимательских правоотношений в цифровой экономике, такие как создание единой для всех системы идентификации или признание альтернативных способов идентификации с установлением для них руководящих указаний при использовании.

Также были раскрыты и описаны различные виды цифровой подписи, которая на данный момент является наиболее распространенным средством цифровой идентификации. По своей юридической силе ЭЦП может быть простой, усиленной неквалифицированной или квалифицированной. Наибольшее доверие у субъектов вызывает КЭП, но при этом её использование не всегда является оправданным в связи с трудностью её использования в повседневной жизни.

Появляются новые формы воплощения цифровой подписи: мобильная, биометрическая. Использование последней в цифровой среде сталкивается с проблемой защиты персональных данных. Данный вопрос регулируется как на национальном, так и на международном уровне. Чтобы идентификатор можно было с правовой точки зрения использовать в предпринимательских (и в любых других) правоотношениях он должен быть надёжен не только в целях определения участника, но также и в целях сохранения персональной информации о нём в целях защиты от злоупотребления со стороны третьих лиц. Исходя из этого, можно сказать, что отношения в цифровой среде несмотря на свою неопределенную до конца правовую природу всё равно требуют законодательного урегулирования, например, в части защиты персональных данных.

В работе было исследовано влияние цифровых технологий на развитие предпринимательских отношений. Так, использование системы блокчейн позволяет предпринимателям совершать надежные транзакции, заключать смарт-контракты, которые подвержены минимальному воздействию субъективного фактора. Несмотря на то, что все процессы в таких системах

регулируются математическими процессами, они безусловно нуждаются в правовом регулировании, например, для признания правовой защиты за сделками, заключенными в таких системах. В том числе, необходимо более детальное регулирование идентификации в системах блокчейн и возможности контроля за распространением данных о субъектах в них. Также, с использованием IAM/IDM систем предприниматели могут обеспечить безопасность внутренней цифровой среды компании, что особо актуально в условиях, когда основной обмен документацией между подразделениями крупных организаций происходит в электронном формате.

В своей работе я опиралась на опыт Российской Федерации по построению правовой и технологической среды для цифровой экономики. Исходя из анализа законодательства, предлагаемых законопроектов, действий, предпринятых органами государственной власти для создания цифровой инфраструктуры (например, создание Единой системы идентификации и аутентификации), можно сделать вывод, что у нас превалирует подход централизации управления цифровой экономикой. Перспективы такого решения пока не очевидны, так как это может повлечь как положительные результаты (например, обеспечить лучшую защиту персональных данных), так и отрицательные, ведь это ограничивает свободу выбора способа идентификации субъектов предпринимательской деятельности в цифровой среде и в некоторой степени отрывает национальный сектор цифровой экономики от остального мира. Также, нельзя не учитывать, что такой подход уже показал, что он трудно осуществим, так как объемы данных, которыми нужно будет управлять, огромны, а это может повлечь за собой технические сложности.

Подводя общий итог, цифровая экономика постепенно может заменить традиционную рыночную, но при этом основное назначение её останется неизменным. Её правовое регулирование необходимо, но, возможно, нужен иной подход, чем полная централизация регулирования всех процессов, происходящих в цифровой экономике; бизнесу должна быть предоставлена возможность саморегулирования в определённых пределах. Основная задача,

которая сейчас стоит перед странами как на национальным, так и на международном уровне – это обеспечение формирования цифровой среды доверия, способствующей развитию правоотношений внутри неё, в том числе и предпринимательских.

Библиография

I. Нормативно-правовые акты и судебные решения

1. Регламент Европейского Парламента и Совета Европейского Союза 2016/679 от 27 апреля 2016 г. о защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС (Общий Регламент о защите персональных данных / General Data Protection Regulation /GDPR// Справочная правовая система «КонсультантПлюс»
2. Резолюция Генеральной Ассамблеи ООН от 16 декабря 1996 г. N A/51/628 "Типовой закон об электронной торговле, принятый Комиссией Организации Объединенных Наций по праву международной торговли" (ЮНСИТРАЛ), и Руководство по принятию// URL: https://www.uncitral.org/pdf/russian/texts/electcom/05-89452_Ebook.pdf
3. "Трудовой кодекс Российской Федерации" от 30.12.2001 N 197-ФЗ (ред. от 03.08.2018) // Справочная правовая система «КонсультантПлюс»
4. Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 31.12.2017) "О персональных данных" // Справочная правовая система «КонсультантПлюс»
5. Федеральный закон от 07.08.2001 N 115-ФЗ (ред. от 23.04.2018) "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма" // Справочная правовая система «КонсультантПлюс»
6. Федеральный закон от 27 декабря 2019 г. N 476-ФЗ "О внесении изменений в Федеральный закон "Об электронной подписи" и статью 1 Федерального закона "О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля" // Справочная правовая система «КонсультантПлюс»
7. Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 19.07.2018) "Об информации, информационных технологиях и о защите информации" //

"Российская газета", N 165, 29.07.2006// Справочная правовая система «КонсультантПлюс»

8. Федеральный закон от 06.04.2011 N 63-ФЗ (ред. от 23.06.2016) "Об электронной подписи"// Справочная правовая система «КонсультантПлюс»
9. Федеральный закон от 28.12.2016 N 471-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации"
10. Указ Президента РФ от 09.05.2017 № 203 «О стратегии развития информационного общества в Российской Федерации на 2017 – 2030 гг.» [Электронный ресурс] // Справочная правовая система «КонсультантПлюс»
11. Указ Президента РФ от 07.05.2018 N 204 (ред. от 19.07.2018) "О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года" // Справочная правовая система «КонсультантПлюс»
12. Постановление Правительства РФ от 16.04.2016 N 315 "О мерах по оказанию содействия избирательным комиссиям в реализации их полномочий при подготовке и проведении выборов депутатов Государственной Думы Федерального Собрания Российской Федерации седьмого созыва" // Справочная правовая система «КонсультантПлюс»
13. Распоряжение Правительства РФ от 19.09.2013 N 1699-р (ред. от 22.05.2018) <Об утверждении Концепции введения в Российской Федерации удостоверения личности гражданина Российской Федерации, оформляемого в виде пластиковой карты с электронным носителем информации, и плана мероприятий по реализации Концепции> (вместе с "Концепцией введения в Российской Федерации удостоверения личности гражданина Российской Федерации, оформляемого в виде пластиковой карты с электронным носителем информации, в качестве основного

документа, удостоверяющего личность гражданина Российской Федерации на территории Российской Федерации") // Справочная правовая система «КонсультантПлюс»

14. Приказ ФНС России от 09.11.2010 N ММВ-7-6/535@ (ред. от 25.05.2018) "Об утверждении Унифицированного формата транспортного контейнера при информационном взаимодействии с приемными комплексами налоговых органов по телекоммуникационным каналам связи с использованием электронной цифровой подписи" // Справочная правовая система «КонсультантПлюс»
15. Национальный стандарт РФ ГОСТ Р 34.10-2012 "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи" (утв. приказом Федерального агентства по техническому регулированию и метрологии от 7 августа 2012 г. N 215-ст)
16. Решение № 2-674/12 от 25 апреля 2012 г. Тимирязевский районный суд (Город Москва)//sudact.ru/regular/doc/NZGVZ4FJ5nNK/ (дата обращения: 13.04.2020).
17. Проект Федерального закона N 424632-7 "О внесении изменений в части первую, вторую и четвертую Гражданского кодекса Российской Федерации" // Справочная правовая система «КонсультантПлюс»
18. Проект Федерального закона N 419059-7 "О цифровых финансовых активах" // Справочная правовая система «КонсультантПлюс»
19. Паспорт федерального проекта Нормативное регулирование цифровой среды (утв. президиумом Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности, протокол от 28.05.2019 N 9) //sudact.ru/law/pasport-federalnogo-proekta-normativnoe-regulirovanie-tsifrovoi-sredy/

II. Договоры корпораций

1. «Учредительный договор Интернет-корпорации по присвоению имён и номеров» утверждён Правлением ICANN 9 августа 2016 года и передан Государственному секретарю штата Калифорния 3 октября 2016 года // https://www.icann.org/resources/pages/governance/governance-en

III. Учебники и монографии

1. Современные информационные технологии и право: монография / А. С. Ворожевич, Е. В. Заиченко, Е. Е. Кирсанова и др ; отв. ред. Е. Б. Лаутс; Моск. гос. ун-т имени М. В. Ломоносова, Юрид. ф-т. — Москва : Статут, 2019. — 288 с. — (Труды Юридического факультета : кн. 15).

2. Blockchain Technology: Beyond Bitcoin (2016), Crosby, Nachiappan, Pattanayak, Verma & Kalyanaraman // URL: https://j2-capital.com/wp-content/uploads/2017/11/AIR-2016-Blockchain.pdf

3. Правовое регулирование экономических отношений в современных условиях развития цифровой экономики : монография / отв. ред. В. А. Вайпан, М. А. Егорова. М. : Юстицинформ, 2019 ; Вайпан В. А.

4. Вайпан В.А. Теория справедливости: право и экономика: Монография. М.: Юстицинформ, 2017. С. 12/

IV. Публикации в периодике и диссертации

1. Мажорова Анастасия Олеговна Преимущества и варианты внедрения identity management system // Вопросы науки и образования. 2018. №8 (20). URL: https://cyberleninka.ru/article/n/preimuschestva-i-varianty-vnedreniya-identity-management-system

2. Рожкова М.А. Право в сфере Интернета: сборник статей / М.З. Али, Д.В. Афанасьев, В.А. Белов и др.; рук. авт. кол. и отв. ред. М.А. Рожкова. М.: Статут, 2018. 528 с. // Справочная правовая система «КонсультантПлюс»

3. Вайпан В.А. Правовое регулирование цифровой экономики // Предпринимательское право. Приложение "Право и Бизнес". 2018. N 1. С. 12 - 17.

4. Модельные правила европейского частного права = Draft of Common Frame of Reference : пер. с анг. /науч. ред. Н. Ю. Рассказова. М. Статут, 2013 // Справочная правовая система «КонсультантПлюс»
5. Савельев А.И. Договорное право 2.0: "умные" контракты как начало конца классического договорного права // Вестник гражданского права. 2016. N 3. С. 32 - 60. // Справочная правовая система «КонсультантПлюс»
6. Булгаков И.Т. Правовые вопросы использования технологии блокчейн // Закон. 2016. N 12. С. 80 - 88.
7. Макаренко А.В. Цифровая экономика как драйвер инновационной предпринимательской деятельности / А.В.Макаренко // Экономика и предпринимательство. — 2018. — №3 (92). — С. 603-609. (URL: https://elibrary.ru/download/elibrary_32844053_59059121.pdf)
8. Статья: Предпринимательское право в условиях инновационной (цифровой) экономики: пути развития (Лаптев В.А., Соловяненко Н.И.) ("Юрист", 2019, N 5)
9. Шваб К. Четвертая промышленная революция. М.: Эксмо, 2016
10. Бородин М.В. Технология цифровой подписи в электронном документообороте // Информационное право. 2015. N 3. С. 42 - 45.
11. Семилетов С.И., Соловьев В.Ю. Законодательная база электронного документооборота в Российской Федерации // Информационное право. 2011. N 3. С. 7 - 13. // "Информационное право", 2011, N 3
12. Курбалийя Й. Управление Интернетом / Й. Курбалийя; Координационный центр национального домена сети Интернет. – М., 2010. – 208 с. // URL: https://cctld.ru/files/books/IG-Russian-3rd.pdf
13. Виктор Наумов «Цифровая среда доверия» // Комментарий для журнала «Закон» URL:https://zakon.ru/blog/2019/10/16/cifrovaya_sreda_doveriya__kommentarij_dlya_zhurnala_zakon#_ftnref1

V. Электронные ресурсы

1. http://www.tadviser.ru/a/179400

2. https://acribia.ru/articles/idm-systems_or_corporate_security_issues
3. https://www.rsa.com/en-us/products/rsa-securid-suite/rsa-securid-access
4. https://www.cryptopro.ru/products/idm
5. http://www.tadviser.ru/index.php/ИБ_-_Аутентификация
6. https://bitnovosti.com/2018/09/24/kak-blockchain-obespechit-zashhitu-personalnih-dannyh/
7. https://fstec.ru/component/attachments/download/2488
8. http://www.tadviser.ru/a/396004
9. http://www.tadviser.ru/a/395520
10. http://www.tadviser.ru/a/119311
11. https://www.rbc.ru/technology_and_media/11/12/2019/5dee6b1c9a794757c7137684
12. https://sozd.duma.gov.ru/bill/419059-7
13. https://bio.rt.ru/faq/security/
14. https://sozd.duma.gov.ru/search?q=Проект+Федерального+закона+N+424632-7
15. https://decenter.org/ru/fatf-cifrovaya-identichnost
16. https://www.sberbank.ru/ru/s_m_business/pro_business/chto-takoe-elektronnaya-podpis-kak-poluchit-i-dlya-chego-nuzhna/
17. https://www.rbc.ru/newspaper/2019/10/18/5da876a89a79472c0bcd51a3
18. https://myedo.ru/elektronnaya-podpis/sfery-primeneniya/mobilnaya-elektronnaya-podpis
19. http://www.tadviser.ru/a/298820
20. https://www.vedomosti.ru/management/blogs/2018/04/18/767028-blokcheina-biznese
21. https://futurerussia.gov.ru/cifrovaya-ekonomika
22. Семинар Всемирного банка в московском офисе 20.12.2016 г. «О перспективах цифровой экономики в России» // URL: https://bi.hse.ru/data/2017/03/30/1168539176/КС28.03%20-%20Владимир%20Ефимушкин.pdf