

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ  
федеральное государственное бюджетное образовательное учреждение высшего образования  
«Тольяттинский государственный университет»

Институт права

(наименование института полностью)

Кафедра «Конституционное и административное право»

(наименование)

40.04.01 Юриспруденция

(код и наименование направления подготовки)

Правовое обеспечение государственного управления и местного самоуправления

(направленность (профиль))

## **ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА (МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ)**

на тему Законодательное регулирование использования цифровых подписей в РФ

Обучающийся

А.В. Миллер

(Инициалы Фамилия)

(личная подпись)

Научный

доктор юридических наук, профессор С.Н. Ревина

руководитель

(ученая степень (при наличии), ученое звание (при наличии), Инициалы Фамилия)

Тольятти 2022

## Оглавление

Введение.....	3
Глава 1 Атрибутная характеристика «цифровых» подписей .....	12
1.1 Электронный документ, как одно из средств доказывания в юридическом процессе и носитель «цифровой» подписи.....	12
1.2 Основное назначение и применение «цифровых» подписей .....	27
Глава 2 Особенности правового регулирования использования «цифровых» подписей.....	35
2.1 Нормативно-правовое регулирование использования «цифровых» подписей.....	35
2.2 Ключевые особенности использования «цифровых» подписей .....	44
Глава 3 Актуальные проблемы использования «цифровых» подписей в юридической практике .....	50
3.1 Проблемы обеспечения подлинности «цифровых» подписей .....	50
3.2 Проблемы, возникающие при применении электронных документов, подтвержденных «цифровыми» подписями .....	59
Заключение .....	81
Список используемой литературы и используемых источников.....	86
Приложение А Элементы ЭЦП.....	93
Приложение Б Алгоритм ЭЦП.....	94
Приложение В Виды ЭЦП.....	95

## Введение

**Актуальность темы магистерской диссертации.** Актуальность темы исследования не вызывает сомнений по следующим причинам:

Во-первых, развитие науки и техники, вступление Российской Федерации на «рельсы» рыночной экономики детерминировали возникновение новых форм и видов общественных отношений. Поэтапное внесение различных изменений в отдельные аспекты общественной жизни направлены на оптимизацию различных правовых процедур и снижение бюрократической нагрузки. «Цифровые» подписи являются одной из новелл современной жизни, которые возникли в правовом пространстве относительно недавно и приобрели весьма широкую распространенность в различных сферах. Исследование данного института представляется необходимым, поскольку это позволит его совершенствовать в дальнейшем.

Во-вторых, не следует забывать и о неблагоприятных проявлениях в обществе, среди которых преступность. Общеизвестно, что современные технологии не только облегчают жизнь обществу и государству, но и выступают в качестве средства и орудия совершения преступного деяния. Правоприменительной практики уже известных случаи, когда при помощи «цифровых» подписей осуществлялся подлог официальных документов. В рамках настоящего магистерского исследования, рассматривая основные теоретические аспекты мы уделили особое внимание вопросам национальной безопасности в сфере использования «цифровых» подписей.

В-третьих, неоднократно исследователями в области юридических наук обозначались некоторые проблемы внедрения и использования «цифровых» подписей в различные виды правовых процедур в сфере гражданского, административного и уголовного права. Их использование там позволило бы оптимизировать процессуальные издержки и сократить сроки осуществления процессуальных действий и принятия решений.

Отметим, что круг проблем, связанных с законодательным регулированием и практикой использования цифровых подписей в России обширен и разнообразен, а их «действенное практическое решение без предварительного теоретического осмысления просто невозможно» [3].

Таким образом, актуальность темы исследования автором видится в необходимости дальнейшего научного исследования института «цифровой» подписи с последующей целью его совершенствования.

**Объект исследования.** Объектом настоящего магистерского исследования является совокупность однородных и взаимосвязанных общественных отношений, которые возникают в процессе использования «цифровых» подписей в Российской Федерации на современном этапе.

**Предмет исследования.** Предметом выпускной квалификационной работы являются книги и статьи, авторефераты и диссертации, иностранные источники, в которых рассматриваются вопросы правового регулирования использования «цифровых» подписей в Российской Федерации на современном этапе.

**Цель исследования.** Целью настоящего исследования является комплексное и всестороннее изучение правового регулирования использования «цифровых» подписей в Российской Федерации на современном этапе.

**Задачи исследования.** Для реализации вышеназванной цели, автором магистерской работы был разработан следующий перечень научно-исследовательских задач:

- изучить понятие электронного документа;
- изучить сущность и функции «цифровой» подписи;
- проанализировать особенности нормативно-правового регулирования использования «цифровой» подписи;
- проанализировать особенности использования «цифровой» подписи;
- исследовать проблемы определения подлинности «цифровых» подписей;

- исследовать проблемы исследования электронных документов, подписанных «цифровыми» подписями.

- разработать комплекс мер по совершенствованию отечественной нормативно-правовой базы, в части регулирования общественных отношений в сфере использования «цифровых» подписей.

**Теоретическую основу проведенного исследования в магистерской диссертации** составили труды современных исследователей не только в области юридических, но технических наук, что обусловлено темой, поставленной целью и задачами исследования.

**Степень научной разработанности темы исследования.** Необходимо отметить, что на сегодняшний день научно-практический материал, посвященный законодательному регулированию использования электронных цифровых подписей (далее - ЭЦП) в нашей стране, представлен в достаточном объеме, как в отечественных, так и в зарубежных источниках.

Значительное количество опубликованных в последние годы различными авторами научных работ по указанной тематике свидетельствует о повышенном интересе к проблемам использования цифровых подписей.

Цифровая подпись и проблемы ее применения являются предметом научных исследований не только отечественных, но и зарубежных исследователей [55]. Зарубежные исследователи также озабочены проблемами правового статуса электронных подписей и определения их подлинности [53], вопросами применения цифровой подписи в различных сферах деятельности государственных и частных структурах [56] и дальнейшего развития системы электронных подписей [52]. Более того, проблемы использования цифровой подписи имеет междисциплинарный характер и исследуется не только специалистами права, а также программистами [57].

Среди отечественных исследователей в данной отрасли необходимо можно назвать труды разных лет таких исследователей, как Е.И. Д.Г.-К. Билалова [4], Гончаров[6], А.В. Ермолаева [12], В.Е. Ефремова [13], С.С.

Пастухова[22], А.Ю. Родичев [36], Н.И. Соловяненко[38], К.А. Фетисов[46], А.В. Щепеткова[49], И.И. Ященко[51], и других, которые посвятили свои работы актуальным вопросам электронного документа в российском законодательстве и проблемам использования цифровой подписи.

Имеющиеся разработки, безусловно, способствуют развитию теоретической мысли в рассматриваемой сфере, их авторов объединяет стремление к совершенствованию законодательного регулирования и практики применения цифровых подписей в нашей стране.

Анализ указанных и иных источников с одной стороны свидетельствует о глубокой озабоченности экспертного сообщества проблематикой использования электронной цифровой подписи, с другой – говорит нам о серьезной проработанности многих аспектов рассматриваемой проблемы, с третьей – еще раз свидетельствует об актуальности и значимости вопросов, связанных с современными проблемами электронного документооборота.

Таким образом, востребованность исследования проблемных вопросов правового регулирования использования цифровых подписей носит очевидный характер, обусловивший выбор темы настоящего исследования и её актуальность.

**Нормативно-правовая база исследования.** Нормативно-правовую основу магистерской работы составили положения отечественного законодательства в сфере использования «цифровых» подписей, среди которых: Конституция Российской Федерации, Уголовный кодекс Российской Федерации (далее – УК РФ), Уголовно-процессуальный кодекс Российской Федерации (далее УПК РФ), Гражданский кодекс Российской Федерации (далее – ГК РФ) и др.

В ходе подготовки настоящей работы автором использовались актуальные на момент ее написания редакции вышеназванных нормативно-правовых актов.

**Методологическая база исследования.** Методологическую основу магистерской работы составил комплекс характерных для данного вида исследовательских работ методов научного исследования, среди которых общенаучный, частнонаучные и специальные. Нами активно применены методы анализа, синтеза, индукции, дедукции, сравнительно-правовой, системный, историко-правовой, а также современные методы кибернетических исследований.

В первой главе настоящего исследования нами активно применялись методы анализа, синтеза, дедукции и индукции.

Во второй главе автором исследовательской работы использовались системный, историко-правовой и сравнительно-правовой методы исследования.

В ходе написания третьей главы выпускной квалификационной работы автором использовались наряду с вышеприведенными, современные методы кибернетических исследований.

**Теоретическая и практическая значимость результатов исследования.** Теоретическую значимость достигнутых результатов автором магистерской работы видится в возможности их использования в ходе дальнейших научных разработок по вопросам правового регулирования использования «цифровых» подписей в Российской Федерации на современном этапе.

Практическая значимость полученных результатов заключается в возможности их использования в ходе законодательной деятельности при совершенствовании правового регулирования использования «цифровых» подписей, а также при разработке учебно-методического материала по дисциплинам юридического профиля.

**Научная новизна** данного исследования заключается в его комплексном характере, нацеленности на выявление слабых мест в правовой регламентации использования «цифровых» подписей в Российской Федерации. В работе предпринята попытка проанализировать проблемные

вопросы определения подлинности «цифровых» подписей и проблемы исследования электронных документов, подписанных «цифровыми» подписями.

**Апробация результатов исследования.** Ряд проблемных вопросов по теме исследования выступили предметом острых дискуссий в ходе практических занятий.

### **Положения, вынесенные на защиту.**

Теоретические положения:

1. «Цифровые» подписи создаются при помощи современных криптографических систем, позволяющих использовать закрытые ключи, с помощью которых владелец подписи получает к ней доступ. Отметим, что использование «цифровых» подписей возможно только при наличии специальных компьютерных технологий – мы полагаем, что это является ключевой отличительной чертой «цифровых» подписей от аналогов собственноручных подписей. «Цифровая» подпись выступает в качестве «набора специальных компьютерных символов, полученных в результате использования современных криптографических технологий, позволяющая в свою очередь обеспечить неизменность и целостность любой информации в электронном документе» [6].

2. «Цифровая» подпись обладает двумя важнейшими свойствами: подпись непрерывно связана с конкретным электронным документом; подпись может быть поставлена только конкретным лицом, владеющим секретным кодом (ключом).

3. Анализ положений федерального законодательства позволяет выделить следующие критерии (условия) при которых «цифровая» подпись будет приравниваться равнозначной графической подписи, выполненной на бумажном носителе:

- на момент подписания соответствующего электронного (электронного) документа сертификат ключа (кода) от подписи не утратил свою силу (является действующим);



- подлинность электронной (цифровой) подписи в соответствующем документе была подтверждена ее собственником;

- электронная (цифровая) подпись соответствует сведениям, которые указаны в сертификате ключа.

2. Национальное законодательство не разработало общепринятого определения термина «электронный документ» или «цифровой документ». Это обстоятельство, по нашему мнению, создает определенные проблемы в правовом регулировании соответствующих общественных отношений. Предлагается понимать под электронным (цифровым) документом сведения, представленные в электронно-цифровой форме об обстоятельствах, подлежащих установлению по делу.

3. Полагаем, что эффективность результатов и оказания государственных и муниципальных услуг в электронном виде во многом зависит от предоставления реальной возможности физическим и юридическим лицам использовать электронный документооборот и электронную (цифровую) подпись наравне с «традиционными» документами.

4. Легитимности электронного (цифрового) документа в качестве доказательства по делу, по нашему мнению, будет способствовать создание и реализация четко разработанной схемы предоставления электронных доказательств в суд. Действенным механизмом реализации такой процедуры, по нашему мнению, является обращение к нотариусу как до начала судебного разбирательства, так и в ходе него.

Практические положения:

1. Полагаем, что необходимо принять Федеральный Закон Федеральный Закон обеспечивающий легитимность электронного (цифрового) документа и позволяющий снять ограничения к его применению в судах как источник доказательств. Предлагается название такого нормативного правового акта - Закон «Об электронном (цифровом) документе» или Закон «Об общих правилах организации оборота электронных (цифровых) документов в Российской Федерации».

2. Полагаем, что следует предусмотреть в отечественном законодательстве правовые обеспечительные меры (гарантии), которые могли бы гарантировать достоверность предоставляемых информационных данных. Этому, по нашему мнению, могут способствовать достижения научно-технического прогресса и, в частности в сфере современных цифровых научно-технических средств.

3. Кроме того, следует предусмотреть более жесткие меры юридической ответственности к тем лицам, которые фальсифицируют подобные информационные данные.

4. Необходимо разработать процессуальный порядок проверки подлинности цифровой подписи в электронных документах в рамках судебных заседаний.

5. Предлагается внести изменения в КоАП РФ и дополнить его ст. 26.7.1 в следующей редакции:

«Электронный документ в качестве доказательства в судебном процессе - это информация, содержащаяся в электронной (цифровой) форме об обстоятельствах, которые необходимо расследовать, имеющих значение для дела. Такая информация содержится в файле на любом материальном носителе, созданном с целью хранения ее и передачи во времени и пространстве».

**Структура магистерской диссертации.** Настоящее исследование состоит из введения, трех глав, включающих шесть параграфов, заключения и списка использованных источников.

В введении раскрываются актуальность, объект и предмет, цель и задачи, методологическая, нормативно-правовая и теоретическая базы, теоретическая и практическая значимость результатов, апробация и положения, вынесенные на защиту.

В первой главе изучается атрибутивная характеристика «цифровых» подписей: понятие электронного документа, сущность и функции «цифровых» подписей.

Во второй главе изучаются особенности правового регулирования использования «цифровых» подписей: нормативно-правовое регулирование и особенности использования.

В третьей главе изучаются актуальные проблемы использования «цифровых» подписей в юридической практике на современном этапе.

В заключении автором подводятся окончательные итоги по результатам проведенного исследования, представлены меры по совершенствованию нормативно-правового регулирования использования «цифровых» подписей в Российской Федерации на современном этапе.

Приложения, представленные в магистерской работе, иллюстрируют ее основное содержание.

Магистерская диссертация выполнена в объеме, соответствующем требованиям.

## **Глава 1 Атрибутная характеристика «цифровых» подписей**

### **1.1 Электронный документ, как одно из средств доказывания в юридическом процессе и носитель «цифровой» подписи**

Безусловно, каждая отрасль человеческой жизнедеятельности развивается, эволюционирует, создавая более совершенные модели своего дальнейшего функционирования. Новшества стремительно врываются во многие сферы деятельности человека, улучшая их уже не на количественном, а на качественном уровне, который присущ постиндустриальному обществу, а значит и современному человеку.

Совершенно очевидно, что каждая отрасль обладает своей собственной скоростью изменений и усовершенствований, а порой и вовсе принимает статичное положение. Однако стоит отметить, что сфера функционирования права, огромная отечественная нормативно-правовая база, чьи принципы и идеи берут свои истоки еще из Древнего Рима, является одной из таковых сфер осуществления человеческой жизнедеятельности. К слову, новшества постиндустриального общества затронули и эту отрасль, активно внедряя последние достижения науки и техники, которые оказываются весьма действенными, хоть и одновременно формируют дискуссионный характер мнений среди отечественных ученых-юристов относительно своего применения и использования в рамках осуществления гражданского судопроизводства. В частности, стоит рассмотреть недавно введенное в гражданский процесс явление как электронный документ [48, с. 118].

Начиная с ряда широкомасштабных изменений в сфере отечественного права от 2017 года, затронувшие и сферу гражданско-процессуального права, законодателем были введены электронные документы при осуществлении судебной деятельности. В свою очередь это предоставило субъектам гражданского процесса возможность предъявлять, к примеру, иск, ходатайство или жалобу в электронной форме, что в свою очередь

свидетельствует об оптимизации подобного процесса в рамках рассматриваемого нами вопроса и его упрощении.

Стоит заметить, что данное нововведение предоставило и «пищу для размышлений» ученым-процессуалистам относительно определения понятия электронного документа, а именно письменных доказательств, возможных к получению через сеть Интернет, а также понятия электронной подписи как конкретного способа подписи документов.

Стоит отметить, что электронный документ обладает довольно яркой спецификой в силу новизны данного явления, несмотря, опять же, на то, что законодательно они все же отнесены к разряду письменных доказательств. В контексте рассматриваемого вопроса важным является наличие определенной формы существования информации, подразумевающую под собой непосредственно запись на каком-либо носителе электронного характера.

Исходя из позиции законодателя, все документы, которые приобретены непосредственно с помощью электронной связи, а также предъявляемые в процессе судопроизводства как электронные доказательства, соответственно, могут быть разграничены на две группы[47, с. 12]:

- первая группа представляет собой непосредственно документы электронного характера:
- вторая же подразумевает под собой определенные электронные сообщения.

Необходимо отметить, что содержание вышеназванных дефиниций содержится в ст. 2 Федерального закона (далее – ФЗ) от 27 июня 2006 г. №149. Безусловно, данная пара относительно довольно новых понятий в сфере гражданско-процессуального права адаптирована согласно нормам ГПК РФ, являясь при этом своеобразным дополнением к уже существующим подробно регламентированным положениям относительно доказательств в рамках осуществления гражданского судопроизводства [43].

Небезызвестным является тот факт, что на пути к становлению доказательством как таковым, сам электронный документ должен обладать конкретизированной информацией, которая является необходимой для процесса фиксирования наличия либо же, соответственно, отсутствия обстоятельств, дающих обоснование возражений или требований сторон. В данном контексте важно отметить, что к числу таковых относятся и иные обстоятельства, обладающие статусом важности в сфере грамотного урегулирования рассматриваемого дела.

Углубляясь в изучение данного вопроса, необходимо акцентировать внимание на том, что само приобретение документа электронного характера должно происходить, следуя «букве закона», то есть согласно регламентации положений о процессе собирания доказательств.

Многие отечественные ученые-процессуалисты отмечают неоднозначность положения электронного документа в отечественном законодательстве связи с тем, что таковое не обладает содержанием информации относительно критериев формата и формы получения каких-либо конкретных данных именно в электронном (цифровом) формате.

Представляется важным замечание касательно того, что, в основном, документация электронного характера в практическом плане предъявляется суду именно в печатном виде, то есть непосредственно на бумажном носителе. Это неслучайно, ведь так законодателем и правоприменителями указывается невозможность установления такового электронного доказательства без, соответственно, наличия специального вида технического оборудования.

Существует, конечно же, ряд спорных моментов относительно признания судом каких-либо данных, информации, приобретенных с помощью использования сети Интернет. Факт предоставления суду распечатанных данных, полученных вышеуказанным способом, не является гарантией того, что суд сочтет его в качестве электронного документа и признает как доказательство по делу в сфере гражданско-процессуального

судопроизводства. Это происходит в силу того, что существует ряд факторов, ставящих под вопрос достоверность, истинность такого рода документа и, соответственно, информации, носителем которой он и является.

Нельзя не отметить тот факт, что в рамках современного действующего отечественного законодательства в принципе не установлено каких-либо конкретных требований относительно определения и установления достоверности информации, чье содержание отображается в документах электронного характера. Обычно достоверность как таковая достигается посредством использования определенных способов оформления самих электронных доказательств, ими являются [40, с. 234]:

- непосредственное проведение экспертизы;
- а также осмотр нотариусом.

А также на данный момент времени можно отметить, наверное, один из наиболее результативных способов придания документам электронного характера юридической силы – подписание таковых электронной подписью. Ее относительно недавнее появление в сфере осуществления человеком различного рода деятельности и форсируемой цифровизации общества оставило свой отпечаток и в правовом поле нашего государства. Из-за сравнительной новизны такого уже, казалось бы, совсем привычного явления до сих пор возникает ряд неурегулированных вопросов, требующих их более детальной регламентации со стороны законодателя.

Так, подписание документа электронного характера вышеуказанным способом приравнивается к подписанию лицом собственноручно какого-либо документа в письменной форме, что, по сути, предоставляет право полагать, что оба варианта подписания документа и электронного документа являются альтернативными по своей природе, но не по специфике. Ведь в контексте рассматриваемого вопроса существует положение, регламентирующее деятельность, связанную с оформлением электронного вида документа. В соответствии с данным правилом, если документ электронного характера имеет изображение (либо текст), то возникает необходимость его

дальнейшего размещения на носителе посредством распечатывания его же бумажной копии, соответственно. Последняя должна быть оформлена в надлежащем виде, предусмотренном законодательством, а также заверена лицом, обладающим определенными полномочиями на совершение этой процедуры [17, с. 25]. После вышеуказанного алгоритма действий такой документ может быть приобщен делу в суде, где будет фигурировать в качестве обычного письменного вида документа.

На наш взгляд, было бы продуктивно с научной точки зрения исследовать каждый из способов определения достоверности документа электронного характера.

Так, проанализируем экспертизу как один из нескольких альтернативных вариантов установления достоверности, указанной в документе электронного вида информации. Необходимо заметить, что содействие лица, обладающего профессиональными знаниями в сфере цифровых технологий, может быть весьма целесообразным в процессе исследования, к примеру протоколов связи. Кроме того, это немаловажно при работе с другой различного рода информацией и материалами передачи данных с использованием именно электронного вида каналов связи, рассматриваемых в плоскости тех дел, где все же значимым аспектом выступает проведение экспертизы.

Говоря об органах власти, обладающих полномочиями в сфере осуществления деятельности по непосредственному производству экспертизы, стоит выделить прежде всего государственные, а также негосударственные экспертные организации либо лица, являющиеся носителями специальных знаний в данной отрасли. Причем, необходимо акцентировать внимание на том, что заключение, выдаваемое экспертом, производившим, соответственно, экспертизу, фигурирует в суде с целью удостоверения определенных обстоятельств рассматриваемого им дела.

По нашему мнению, очень важной является возможность проведения такого рода экспертизы в рамках любой стадии до вынесения судом решения



по рассматриваемому им спору. Это в свою очередь предоставляет хорошие возможности для установления достоверности информации, содержащейся в электронном виде документов вне зависимости от стадий дела, что обеспечивает эффективность работы, с подобного рода документами и получения результатов, являющихся значимым для разрешения самого дела.

Раскрывая другой способ удостоверения данных, содержащихся в электронном документе, необходимо отметить, что он подразумевает под собой нотариальное оформление доказательств [39, с. 124]. По статистике, именно данный прием определения уровня достоверности электронного вида документов является наиболее востребованным. Заключается он в следующем: при возникновении запроса лицо, оказывающее данного рода услуги, должно своевременно оказать квалифицированную помощь в установлении доказательственной базы, которая свою очередь станет основой для определения судом полномочий и обязанностей лиц-участников спора, а также для вынесения судом законного и грамотного решения по данному делу.

Существуют, конечно, исключительны случаи, в рамках которых определение уровня достоверности информации электронного документа далеко не всегда представляется вероятным по причине того, что, по сути, удаленная информация, являясь приобретенной с различного рода интернет-ресурсов и выступающей предметом самого спора, сама по себе важна для рассмотрения последнего. А распечатанный формат тех самых интернет-материалов, даже будучи заверенным нотариусом, не в стопроцентной вероятности является исчерпывающим источником установления достоверности той или иной информации электронного вида документов.

Важным является наличие ряда положений в ГПК РФ и Основах законодательства РФ о нотариате (ч. 2 ст. 102) относительно статуса нотариуса в сфере производства им процедуры удостоверения данных, содержащихся в электронном виде документов [35, с. 114]. Согласно вышеуказанным источникам, возможность обеспечения нотариусом

доказательств по тем делам, в рамках которых проходит судопроизводство, недопустима. Но до непосредственной стадии возбуждения дела в сфере гражданского судопроизводства нотариус обладает полномочием на совершение упомянутого раннее действия, то есть обеспечить значимые для разрешения спора доказательства, при наличии возможность полагать, что представление доказательств как таковых далее станет невозможным либо затруднительным.

В дополнение к вышеизложенному, стоит отметить существование еще и электронного сообщения в качестве одного из видов доказательства электронного типа, которое также подразумевает электронную переписку. К слову, подобного рода передача информации довольно популярна, так как задействуется во многих направлениях осуществления, в том числе и профессиональной деятельности, например, часто используется в сфере взаимодействия контрагентов относительно самых разных вопросов: будь то передача разного рода документации, утверждение условий какого-либо соглашения и т.д. В разрезе данной темы полагаем важным заметить существенное отличие электронного вида сообщения от документа электронного характера – электронное сообщение не имеет содержания электронной подписи, о которой было упомянуто ранее.

Углубляясь в корень рассматриваемого вопроса, стоит акцентировать внимание на том, что в самом договоре стороны, вправе указать, что все, например, приложения, различные протоколы согласования цен, иные важные документы для данных сторон являются составной частью такого договора. И, соответственно, вышеупомянутые данные и материалы будут обладать юридической силой, что наделяет в свою очередь договор сторон особой спецификой в связи с наличием в нем, к примеру, электронных материалов и приложений.

Так, одним из наиболее часто используемых и эффективных средств коммуникации путем использования электронных технологий выступает взаимодействие лиц посредством электронной почты. В наше время сложно,

действительно, представить работника какой-либо отрасли или сферы деятельности, не имеющего такую почту. К слову, даже если и так, то во многих организациях предусмотрена корпоративная почта, специально адаптированная для сотрудников этой организации и внутреннего взаимодействия работников. Правда, важно заметить, что таковая не будет считаться доказательством по рассматриваемому судом спору, если в заключенном меж сторонами договоре не содержалось подобного условия либо не указано наличие электронных адресов, а другая сторона договора не подтверждает в принципе существования подобной переписки, взаимодействия путем использования электронной почты.

Полагаем, что вышеуказанные положения относительно фигурирования электронных ресурсов и материалов, а также способов коммуникации лиц и передачи различного рода информации с помощью передачи таковой через сеть Интернет, необходимо проиллюстрировать, ссылаясь на пример судебной практики.

К слову, приведем в пример случай неисполнения обязательств по договору поставки, в котором в роли доказательств выполнения обязательств такого договора ответчик предъявил переписку электронного характера данных сторон по вопросу самого исполнения договора поставки. Истец был против приобщения к делу такого рода переписки, однако суд установил, что заключенный договор стал таковым путем обмена сторон определенными документами с помощью использования электронной почты. И, исходя из того, что ответчиком был переслан ряд документов, таких как устав, свидетельство о государственной регистрации и т.д. а самим истцом – платежные поручения, что свидетельствует о согласии на условия договора и готовность принять товар, стоит отметить следующее: такого рода взаимообмен сторон удостоверяет их восприятие документов по электронной почте как полученные от уполномоченных на то лиц. Последнее означает, что в принципе существует возможность «применения одного и того же правового режима документов электронного характера, форм их

использования и самого оборота с режимом употребления привычных или «традиционных» документов, выполненных непосредственно на бумажном носителе» [34, с. 114].

Учитывая, что отечественный гражданско-процессуальный кодекс не обладает наличием фиксированного перечня критериев допустимости и, соответственно, достоверности рассматриваемых выше видов электронной документации, то это в свою очередь может создавать серьезные препятствия для дальнейшего урегулирования споров, относительно причастности этих документов, их роли и вообще «веса» при рассмотрении гражданско-процессуальных дел. Стоит заметить, что при таком положении дел на практике может быть весьма проблематично признание юридической силы такого рода документации в связи с существованием коллизий и отсутствия детализированности, подробности в рамках регламентирования данного вопроса.

Так, стоит отметить все же некоторые требования применительно к понятию электронного вида документов, а также к их дальнейшему положению в рамках рассмотрения судом, что, по сути, сможет минимизировать риск допущения правоприменителями различного рода ошибок, неграмотного применения закона в контексте анализируемого вопроса:

- во-первых, необходимо отметить важность наличия читаемости данного документа;
- во-вторых, наличие у электронного вида документа определенных реквизитов (с наличием электронной подписи, соответственно).

Естественно, для признания документов электронного характера допустимыми, необходимо их удовлетворение ряду критериев. Так, отечественные ученые-процессуалисты базируются в своих мнениях на том, что стоит выделить следующие требования к электронной документации в качестве основных, способных, если не предотвратить, то снизить

вероятность возникновения сложностей и преград на пути к грамотному оцениванию последних в рамках производства по конкретному делу:

- одним из самых важных критериев определения допустимости электронных документов выступает позиция, относительно которой требованием допуска рассматриваемого вида документов как доказательства в сфере осуществления гражданско-процессуального производства выступает категория доступности в понимании;

- под самим положением допуска важно понимать именно возможность определения ее автора, что, соответственно, устанавливается посредством электронно-цифровой подписи. Однако стоит заметить, что последнее представляется возможным лишь в случае фиксирования подлинности самой рассматриваемой в рамках данного вопроса подписи;

- также основанием такого допуска выступает непосредственно само следование требованиям, которые предусматривают целостность рассматриваемого вида документов. Указанные условия находятся в зависимости от специфики создания, хранения, кроме того, и передачи электронного вида документов по конкретным каналам связи;

- стоит сделать акцент на необходимости наличия у подобного носителя материалов, информации определенной характеристики, подразумевающей под собой категорию контролепригодности, то есть существования возможности производства контрольных мероприятий с целью определения достоверности документа электронного характера.

Ряд существенных изменений, последовавших с 1 января 2017 года, коснулись и сферы рассматриваемого вопроса – положения электронного вида документации, а именно – их возможности применения и роли при рассмотрении спора. Согласно вышеуказанному, иск, ходатайство, а также иные виды документов, возможно заявить в суд в электронном формате, что в свою очередь значительно упрощает процедуру подачи данных документов и, отчасти, упрощает работу суда. Однако, более интересным и, на наш взгляд, далеко не маловажным является положение о расширении перечня

письменных доказательств в сфере гражданского процессуального права. Оно гласит о том, что среди вышеприведенного примера перечня письменных доказательств, теперь также имеют место быть и те документы, которые были получены с помощью сети Интернет, и, соответственно, те документы, которые содержат электронно-цифровую подпись [31, с. 37].

В связи с этим, мнения о подходах к понятию электронного вида документов как доказательств среди отечественных процессуалистов разделились. Большинство стремится к отождествлению понятия документа электронного характера с электронным доказательством, умалчивая о существовании самостоятельной дефиниции последнего с целью упрощения данного вопроса с научной точки зрения несмотря на то, что понятие электронного документа представлено в законодательстве об информационной деятельности.

Следуя положениям из указанных нововведений, «под электронным документом признается определённые задокументированные данные (информация), которые представлены в электронной форме» [34].

По мнению группы отечественных ученых в сфере гражданско-процессуального права, под доказательствами электронного вида понимаются определенные данные об обстоятельствах, которые обладают значимым статусом в рамках рассматриваемого судом дела, а также оформленные в виде цифровой, аудио- и видеозаписи. Стоит также добавить, что к подобного рода доказательствам относят протоколы судебных заседаний, процессуальных действий, установленных с использованием электронно-вычислительной техники.

Важно отметить, что понимание самого электронного вида документа как обладающего определенными данными об обстоятельствах, которые представляют собой значимость в рамках рассмотрения и разрешения спора, а также следование законно установленным требованиям и условиям получения, оформления и их предоставления, соответственно, и подразумевает под собой электронное доказательство.

Говоря подробнее о спорных ситуациях, возникающих в сфере электронного вида документов, стоит сделать акцент на том, что при сомнении сторон относительно подлинности информации, материалов или данных документов электронного характера, также в случае наличия оспаривания его содержания или возражений, возникает необходимость производства экспертизы по данному вопросу. Последняя находит свою дальнейшую регламентацию в ст. 79 ГПК РФ. Так, экспертиза, произведенная относительно данного дела и данных документов позволит предоставить основание достоверности электронной документации в качестве доказательства.

Безусловно, электронно-цифровая подпись (далее ЭЦП) в современных реалиях выступает в качестве одного из самых надежных и эффективных способов надления электронного вида документации юридической силой. Законодательно использование ЭЦП для придания электронным документам юридической силы приравнивается к собственноручному подписанию обычного письменного документа. Это в свою очередь значительно упрощает многие процедуры, делает возможным совершение ряда операций с использованием сети Интернет, при этом предоставляя право легитимного заверения электронной документации, по сути, обычным подписанием письменных документов (как на бумажном носителе) [31, с. 44].

При содержании в электронном виде документа каких-либо изображений или текста, необходима его печать, то есть создание его бумажной копии (письменного формата документа), которая в дальнейшем подлежит надлежащим образом оформлению и заверению уполномоченным на то лицом, соответственно. Пройдя вышеуказанный алгоритм действий, данная копия может уже быть приобщена к рассматриваемому в суде делу, выступая в форме обычного письменного документа (несмотря на то, что первоначально являлась документом электронного характера).

Стоит также отметить, что в рамках даже современных тенденций развития отечественного гражданского процессуального права среди ученых-

юристов до сих пор возникают дискуссии относительно правовой природы анализируемых в данной главе явлений – электронных документов.

Важным является вопрос того, к какому именно виду доказательств следует отнести электронный вид документации, поскольку мнения процессуалистов в данной сфере разнятся, в связи с чем, проблема принадлежности электронного документа к группе письменных либо же вещественных доказательств не урегулирована даже на научном, теоретическом уровне.

Исходя из позиции ряда отечественных ученых, электронный вид документации необходимо рассматривать именно как письменный вид доказательств, так как та информация, те данные, которые в ней содержатся, выражает собой определенные логические и мыслительные процессы в рамках объективно существующей реальности.

Правда, по нашему мнению, нельзя однозначно четко отнести указанный вид документов к группе тех или иных доказательств. Предполагается, что электронный документ нужно рассматривать под призмой смешанного характера особенностей того или иного вида доказательств, так как он содержит в себе признаки обеих указанных групп доказательств. Стоит заметить, что и законодатель не решился сформулировать понятие электронного документа как доказательства, ставя под вопрос саму дефиницию и предоставляя таким образом почву для научных размышлений относительно рассматриваемого вопроса. Более того, нельзя отметить и наличие самих разъяснений и конкретизации о признаках и специфических характеристиках электронного вида документов в роли доказательства, приобщенного к судебному делу.

С точки зрения рассмотрения электронных документов в правовом поле, важно отметить, что последние довольно нечасто употребляются в форме доказательств. Это во многом обусловлено тем, что наличествует довольно большое количество до сих пор неурегулированных пробелов, противоречий, коллизий, по причине чего уполномоченные на то органы и



лица, как и сам суд, могут не признать такие доказательства допустимыми, вследствие чего последние утратят свою юридическую силу и, соответственно, статус самого доказательства.

По вышеизложенному можно судить о проблематичности разрешения данного вопроса в условиях современных правовых реалий, ведь все еще существует слишком много недочетов.

Стоит отметить, что в самом начале изучения данного вопроса можно выделить ряд очевидных плюсов относительно регламентирования сферы доказательств и их приобщения к делу, однако, производя более глубокий и детальный анализ рассматриваемого вопроса, формулируется вывод о далеко не всегда «прозрачной» и ясной системе оценивания электронного вида документов как доказательства в суде. Это во многом связано с необходимостью следования довольно жестким правилам и требования установления достоверности последних, что с практической стороны представляется затруднительным.

Стоит отдельно указать на специфику аудио- и видеозаписей, которые обладают наибольшим уровнем убедительности в разрезе восприятия их в качестве доказательств по делу в суде. Исходя из того, что конечную цель процедуры доказывания составляет выяснение истины, то доказательства как таковые, соответственно, содействуют в достижении указанной цели.

Важным моментом является то, что суд при оценивании аудио- и видеозаписей базируется на общих признаках доказательств, к непосредственному рассмотрению предстает лишь та информация и те данные, которые были приобретены сугубо легитимным путем, чья истинность в принципе не подвергается каким-либо сомнениям.

Тем не менее, вопреки вышеизложенному, современное российское законодательство предусматривает наличие электронного вида документов в рамках восприятия последних в качестве доказательств по конкретному делу в суде.

Правда, для их реализации более выраженного и частого применения важно соблюдение определенных правил: например, с целью установления достоверности данных и материалов как содержания документа электронного характера, необходимо обеспечение аутентификации и идентификации такого рода информации для возможности дальнейшего ее использования в суде.

Говоря об аутентификации, стоит отметить, что она представляет собой непосредственную возможность проведения проверки целостности информации, ее содержания в оригинальном виде. Безусловно, это важно с точки зрения элементарного установления смыслового наполнения исследуемого объекта, его связности и роли изложенной информации для рассмотрения судом.

Идентификация же подразумевает под собой возможность установления факта «принадлежности» указанной информации конкретному лицу, иными словами, определение истинного отправителя изучаемого документа электронного характера. В контексте этого положения важно наличие перечня реквизитов, удовлетворяющих требованиям текущего законодательства, в частности, необходимым является содержание ЭЦП.

В дополнение к перечисленному, важно отметить наличие необходимости внедрения определенной категории изменений в действующее законодательство РФ с целью закрепления дефиниции электронного вида документа в качестве доказательства, фиксирования перечня правовых гарантий его употребления, гарантий достоверности. Кроме того, было бы целесообразным регламентировать алгоритм изучения таких источников информации в рамках самого судебного процесса, подготовить перечень правовых критериев к форме электронного вида документов.

Так, применение электронных доказательств в рамках осуществления гражданского судопроизводства – весьма актуальный вопрос в сфере развития института доказательств и доказывания как такового. Очевидно, что

электронные доказательства будут развиваться в ногу с научно-техническим прогрессом, что дает повод предположить их перспективное обособление как самостоятельного вида доказательств.

## **1.2 Основное назначение и применение «цифровых» подписей**

Рассвет электронных подписей начался сорок лет назад. С необходимостью и возможностью доступа к любой личной информации, хранящейся на компьютере, возник вопрос о том, как применять подписи к электронному носителю так же, как это делается с важными документами. Несмотря на то, что сама технология старая, только в последнее время цифровые подписи набрали обороты, поскольку технология используется компаниями, частными лицами - в государственном управлении и связи.

Двумя учеными, принявшими вызов, были американцы Уитфилд Диффе и Мартин Хеллман. В 1976 году они описали решение, которое назвали «односторонней аутентификацией». Однако термин «цифровая подпись» был предложен Ади Шамиром, Ронам Ривестом и Леонардом Адлеманом в статье, опубликованной в 1977 году. Их решение было основано на асимметричном шифровании. Другими словами, как с закрытым, так и с открытым ключом. Один из ключей будет известен обеим сторонам, а другой будет известен только тому, кто подпишет или получит сообщение. В 1977 году указанные ученые разработали «криптографический алгоритм RSA, который без дополнительных модификаций можно было использовать для создания примитивных цифровых подписей» [15].

Складывающиеся в последние десятилетия тенденции к глобализации, проявляющиеся в утверждении вектора на международное сотрудничество в различных правовых вопросах детерминировали необходимость создания единого правового пространства для разрешения различных проблем теоретического и прикладного характеров. Безусловно, развитие науки и техники оказали на вышеназванные процессы существенное влияние,

которое обусловило возникновение института «цифровых» подписей в Российской Федерации.

Для разрешения различных проблем теоретического и прикладного характера необходимо уделить внимание теоретическим основам вышеназванного института.

В рамках настоящего параграфа исследовательской работы мы уделим внимание вопросам сущности и функций электронных «цифровых» подписей в отечественном правовом пространстве.

Исследуя материалы юридической доктрины можно сделать вывод о том, что процессы глобализации и цифровизации повлекли за собой интеграцию явления «виртуального» пространства в документооборот, которые выражаются, в частности, в возникновении и использовании электронных «цифровых» подписей. Вместе с этим возникло ряд проблем, связанных с определением правового статуса электронных документов и его правовым режимом.

В современной юридической доктрине достаточно часто поднимаются проблемы понятия электронного документа, как важнейшего элемента современного документооборота. Такая тенденция характерна не только для отечественного доктринального сообщества, но и для зарубежного. С течением времени, различные компьютерные средства совершенствуются, становятся компактными, мобильными и достаточно простыми в использовании, что делает их популярными в обществе. Иными словами, компьютерные технологии, являясь основным и прочным фундаментом в процедуре использования «цифровых» подписей на сегодняшний день являются многофункциональными и не требуют от пользователей особых навыков.

Известный отечественный исследователь Р.О. Халиков в своих трудах отмечал, что понятие электронного документа, включающее в себя все основные атрибутивные характеристики, на сегодняшний день, уже нашло собственное понимание в доктрине и практической деятельности несмотря на

то, что нормативно-правовое регулирование использование «цифровых» подписей нуждается в совершенствовании [37, с. 22].

Мы полагаем, что позиция вышеназванного исследователя детерминирована наличием ряда факторов, среди которых несовершенство отечественной нормативно-правовой базы, отсутствие легальной дефиниции электронного документа и др.

Процедуры обмена электронными документами «существенным образом отличаются от аналогичной процедуры с документами на бумажном носителе» [52]. Наиболее значимой проблемой в процедуре обмена документами являются вопросы определения подлинности электронных документов, безусловно данная проблематика возникает в различных процессуально-правовых отношениях. На сегодняшний день, вышеописанная проблема разрешается путем применения «цифровых» подписей.

Вместе с этим, существует внушительное количество способов идентификации информации, которая была зафиксирована в электронном документе.

С.А. Агамагомедова в своих работах отмечает, что под ЭЦП необходимо понимать любой процесс, реализованный при помощи ЭВМ, выполненный с намерением связать факт написанного в документе с возникновением юридической обязанности совершить то или иное действие [21, с. 25]. Таким образом, «цифровые» подписи выступают в качестве основного средства удостоверения электронного документа, что придает ему юридическую силу.

Мы полагаем, что под «цифровой» подписью необходимо понимать некий электронный сигнал достаточно сложного биометрического компьютерного устройства, среди которых, например, сканеры отпечатков пальцев рук, сетчатки глаза и др. Наиболее простым устройством в данном случае выступает персональный компьютер, который предполагает только введение специальных символов с помощью устройств ввода, предполагающие создание на их основе «цифровой» подписи. Таким

образом, для создания «цифровой подписи» важное значение имеет вид электронного устройства, поскольку в зависимости от используемых алгоритмов тип и вид подписи может дифференцироваться.

Известный отечественный исследователь Н.И. Соловяненко в своих трудах отмечает, что непосредственно связанные с «цифровой» подписью различные символы, коды, изображения уже могут рассматриваться как элемент «цифровой» подписи. Однако, необходимо сделать оговорку о том, что вышеназванные символы, знаки или иные изображения должны быть обговорены сторонами, как средства возникновения юридических прав и обязанностей [38, с. 123].

Вышеназванный автор отмечает, что доверие к «цифровым» подписям обеспечивается следующим образом:

- во-первых, между сторонами заключается соглашение или договор, в котором определяются условия использования символов, знаков и изображений в качестве «цифровых» подписей [14, с. 77]. Достаточно часто используется в таких соглашениях шаблонная фраза, удостоверяющая факт использования «цифровых» подписей сторонами.

- во-вторых, применение «цифровых» подписей в юридической практике есть реализация международного принципа функционального эквивалента, предполагающего возможность подписания документов и соглашений «цифровыми» подписями, если возникает необходимость в удостоверении данного документа.

Исследователи в своих научно-исследовательских трудах отмечают, что «цифровые» подписи следует понимать, как заданные и преобразованные записи, выполненные при помощи различных хэв-функций и криптосистем. Использование подобных технологий в процессе применения «цифровых» подписей обусловлено необходимостью создания секретных ключей и кодов при помощи которых предоставляется доступ к данной подписи, а вместе с этим и идентифицируется лицо, которое поставило «цифровую» подпись [21, с.26].

Мы полагаем, что смысл, вкладываемый данными авторами в понятие «цифровых» подписей в значительной степени тождественен тому, которые вкладывает в данное понятие отечественный законодатель. Согласно положения федерального законодательства «под «цифровой» подписью необходимо понимать обязательный реквизит документа, которые обеспечивает защиту электронного документа от подделки» [6]. Законодатель также отмечает, что такая защита осуществляется путем использования специальных компьютерных технологий, позволяющих создавать закрытые коды (ключи) доступа владельцу «цифровой» подписи.

В завершении вышеприведенной небольшой дискуссии отметим, что «цифровые» и электронные подписи необходимо рассматривать как равнозначные понятия.

В юридической доктрине существует и иная точка зрения. Так, Е.В. Илыных и М.Н. Козлова в своих научно-исследовательских трудах отмечают, что необходимо дифференцировать не только «цифровые» и электронные подписи, но и электронные аналоги собственноручных подписей [19, с. 7]. К последним следует относить не только изображения подписей, но и различные ПИН-коды, пароли и др. Понятие «цифровых» подписей, по их мнению, следует рассматривать как более широкое явление по отношению к электронным подписям [14, с. 78].

Таким образом, «цифровые» подписи создаются при помощи современных криптографических систем, позволяющих использовать закрытые ключи, с помощью которых владелец подписи получает к ней доступ. Отметим, что использование «цифровых» подписей возможно только при наличии специальных компьютерных технологий – мы полагаем, что это является ключевой отличительной чертой «цифровых» подписей от аналогов собственноручных подписей.

Анализ положений отечественной нормативно-правовой базы показывает, что отечественному законодателю известны и другие трактовки

«цифровой» подписи. В рамках настоящего исследования приведем некоторые из них:

«Цифровая» подпись является «аналогом собственноручной подписи, выступающее основным средством защиты информации и обеспечивающая ее подлинность» [6].

«Цифровая» подпись выступает в качестве набора специальных компьютерных символов, генерируемых с помощью специальных криптографических технологий. Современные технологии позволяют в свою очередь обеспечить безопасность любой информации, т.е. ее неизменность и целостность в электронном (цифровом) документе.

Мы полагаем, что приведенные трактовки «цифровых» подписей обусловлены особенностями правового регулирования тех или иных сфер общественных отношений, в которых они могут применяться.

Анализ мнений исследователей показывает, что предложенные ими определения «цифровых» подписей опираются на необходимость использования специальных криптографических технологий, позволяющих создавать зашифрованные коды.

Безусловно, вышеприведенное является ключевым критерием, отличающим рассматриваемые явления от смежных. Отсюда возникает и особая структура «цифровой» подписи предполагающее использование носителем «двойного» ключа. Иными словами, сама подпись является ключом, удостоверяющим документ, а ее применение требует наличие другого «секретного» ключа, который известен только владельцу. Как правило, сроки действия этих ключей ограничены и периодически они обновляются.

Известный отечественный исследователь А. Гарибян отмечает в своих трудах, что «цифровая» подпись обладает двумя важнейшими свойствами:

- подпись непрерывно связана с конкретным электронным документом;
- подпись может быть поставлена только конкретным лицом, владеющим секретным кодом (ключом) [5, с. 12].



Законодательное определение «цифровой» подписи не определяет круг разрываемых данным явлением целей и задачи. В законе речь идет исключительно об особенностях создания таких подписей и их защите.

Анализ положений федерального законодательства позволяет выделить следующие критерии (условия) при которых «цифровая» подпись будет равнозначной подписи на бумажном носителе:

- действующий на момент подписания электронного (цифрового) документа сертификат ключа;
- подтверждение пользователем подлинности «цифровой» подписи;
- соответствие между информацией в электронном документе и «цифровой» подписью.

Мы полагаем, что презумпция авторства в данном случае, обуславливает гарантию юридической силы подписанного такой подписью документа.

Выводы по главе:

На основании проведенного исследования в первой главе мы сделали следующие научно-исследовательские выводы:

«Цифровая» подпись является обязательным для электронного документа реквизитом.

«Цифровые» подписи создаются при помощи современных криптографических систем, позволяющих использовать закрытые ключи, с помощью которых владелец подписи получает к ней доступ. Отметим, что использование «цифровых» подписей возможно только при наличии специальных компьютерных технологий – мы полагаем, что это является ключевой отличительной чертой «цифровых» подписей от аналогов собственноручных подписей.

«Цифровая» подпись выступает в качестве набора специальных «компьютерных символов, полученных в результате использования современных криптографических технологий, позволяющая в свою очередь

обеспечить неизменность и целостность любой информации в электронном документе» [6].

«Цифровая» подпись обладает двумя «важнейшими свойствами:

- подпись непрерывно связана с конкретным электронным документом;
- подпись может быть поставлена только конкретным лицом, владеющим секретным кодом (ключом)» [5].

Анализ положений федерального законодательства позволяет выделить следующие критерии (условия), при которых «цифровая» подпись будет «равнозначной подписи на бумажном носителе:

- сертификат ключа (кода) от подписи не утратил силу на момент подписания соответствующего электронного документа;

- подлинность «цифровой» подписи в соответствующем документе была подтверждена;

- «цифровая» подпись соответствует сведениям, которые указаны в сертификате кода (ключа)» [5]. Таким образом, можно предположить, что презумпция авторства в данном случае, обуславливает гарантию юридической силы подписанного такой подписью документа.

В следующей главе настоящего исследования мы уделим внимание особенностям нормативно-правовой регулирования использования «цифровых» подписей в России на современном этапе.

В следующей главе настоящего исследования мы уделим внимание особенностям нормативно-правовой регулирования использования «цифровых» подписей в России на современном этапе.

## **Глава 2 Особенности правового регулирования использования «цифровых» подписей**

### **2.1 Нормативно-правовое регулирование использования «цифровых» подписей**

В этом параграфе магистерского исследования мы рассмотрим нормативно-правовое регулирование использования «цифровых» подписей в Российской Федерации.

Для начала уточним категорию «нормативно-правовое регулирование» и «нормативный правовой акт».

Нормативно-правовое регулирование можно представить как процесс упорядочивания какой-либо деятельности посредством совокупности нормативных актов различного уровня. Эти акты представлены во всем их многообразии и динамике, более того, они органически взаимосвязаны между собой тем обстоятельством, что они на разных уровнях регламентируют правовое положение (статус) такой деятельности.

Под нормативным правовым актом следует понимать акт, который содержит нормы права, то есть правила поведения, рассчитанные на неоднократное применение и влекущие юридические последствия.

Регулирование общественных отношений в сфере «цифрового» документооборота на сегодняшний день осуществляется в соответствии с положениями национального гражданского законодательства и иными федеральными законами, среди которых:

- об информации, информатизации и защите информации [45];
- о связи [44];
- об электронной цифровой подписи [43] и др.;

К другим источникам нормативно-правового регулирования общественных отношений в сфере электронного документооборота следует

относить подзаконные акты, акты правительства и президента Российской Федерации и положения законодательств субъектов.

Одним из важнейших законодательных актов в области нормативно-правового обеспечения электронного документооборота является подписанные Президентом Российской Федерации в 2002 году Федеральный закон «Об электронной цифровой подписи», который содержит в себе юридические нормы, определяющие процедуру подписания договоров и соглашения с использованием новейших криптографических технологий, обозначенных в нем как «цифровая» подпись [43]. Мы полагаем, что принятие вышеназванного нормативно-правового акта обозначило новый вектор развития основ национального гражданского права, а также экономической системы Российской Федерации.

Вышеприведенный нормативно-правовой акт содержит в себе следующие положения, регулирующие общественные отношения в сфере использования «цифровых» подписей [15, с. 154]:

- все созданные экземпляры и дубликаты такой подписи имеют одинаковую юридическую силу;
- электронные документы, подписанные такой подписью в установленном порядке имеют доказательственное значение в юридическом процессе;
- «цифровые» подписи равнозначны обычной, собственноручной, в случаях, когда срок действия сертификата владельца подписи на момент подписания соответствующего электронного документа не истек;
- незаконное использование «цифровой» подписи влечет за собой наступление юридической ответственности, в том числе и уголовной.

Необходимо отметить, что к числу нормативных документов, регламентирующих применение ЭЦП в нашей стране, следует отнести постановления правительства Российской Федерации, которые являются актами управления общенормативного содержания. Такие акты регулируют, например, виды электронной подписи, использование которых допускается

при обращении за получением государственных или муниципальных услуг [28] или правил определения видов электронной подписи [29]. Также, такие акты регламентируют правила обмена документами в электронном виде [26], устанавливают систему межведомственного электронного документооборота [25] и использование простой электронной подписи при оказании государственных и муниципальных услуг [27].

Кроме того, применение цифровой подписи в Российской Федерации регулируется региональными стандартами, которые приняты Межгосударственным советом по стандартизации, метрологии и сертификации Содружества Независимых Государств.

К таким стандартам следует отнести документы, устанавливающие, например, модели криптографической защиты информации [8], обеспечивающие долговременную сохранность электронных документов [9], методы и средства обеспечения безопасности применения цифровых подписей с приложением [16], и другие стандарты, содержащие национальные принципы оформления организационно-распорядительной документации и т.д.

Мы полагаем, что назначение вышеприведенных нормативных актов состоит в том, что они разгружают процедуру осуществления предпринимательской и иной коммерческой деятельности, а также создают прочный фундамент для дальнейшего развития современных компьютерных технологий, что является одним из критериев «нового этапа» коммуникации между субъектами общественных отношений, среди которых физические, юридические лица и органы публичной власти.

Аксиологические и праксиологические основы «цифровой» подписи состоят в том, что она гарантирует подлинность сведений, которые содержатся в электронных документах, и тем самым дает возможность пользователям таких документов отстаивать собственные позиции в органах судебной власти. Обеспечение вышеприведенных гарантий складывается из того, что возможность подписания электронного документа возможна

исключительно владельцем «цифровой» подписи, имеющим соответствующий сертификат.

Целью, принятого в 2002 году вышеупомянутого закона состоит в обеспечении соответствующих правовых условий применения в общественных отношениях «цифровой» подписи, среди которых законодателем выделяется равенство «цифровой» и традиционной подписи и одинаковая юридическая сила [11]. Действия данного нормативно-правового акта распространяется на общественные отношения, которые регулируются национальным гражданским законодательством, но не распространяется на случаи использования «аналогов» такой подписи, значение и содержание которых мы рассмотрели в предыдущих параграфах.

Согласно положения национального гражданского законодательства, использование криптографических технологий в виде «цифровых» подписей при совершении различных гражданско-правовых сделок, допускается не иначе как по соглашению сторон, либо если иное не предусмотрено другими положениями отечественной законодательной базы [15, с. 155].

Следует отметить, что сделки, согласно положения отечественного гражданского законодательства могут совершаться путем составления документов в письменной форме, который, в свою очередь, отражает волю участвующих в ней сторон [11]. Однако, в соответствии с положениями законодательства о «цифровых» подписях для удостоверения подлинности того или иного документа, достаточно поставить «цифровую» подпись, сертификат которой не истек. В данном случае наблюдается дифференциация понятия в разных нормативно-правовых актах относительно смежных явлений. Целесообразно было бы внести конкретизирующие изменения в положения гражданского законодательства, в части прямого указания на допустимость использования «цифровых» подписей для удостоверения сделок и соглашений.

На сегодняшний день, национальное гражданское законодательство заложило лишь некоторые аспекты использования «нетрадиционных» форм

подписания документов, в том числе и электронных. Так, действующее законодательство, например, ГК РФ вполне допускает использование методов факсимильного воспроизведения подписи с использованием средств механического или иного технического копирования при удостоверении сделок или соглашений. Здесь законодатель делает оговорку о том, что использование таких способов удостоверения гражданско-правовых сделок допускается при согласии участвующих в сделке сторон и при отсутствии правовых запретов из других законодательных актов. Вместе с этим, национальное гражданское законодательство допускает возможность электронного («цифрового») обмена подписанными в традиционной форме документами [11].

Использование «цифровых» подписей в общественных отношениях должно отвечать целому ряду условий, которые закреплены в положениях национального законодательства. Причем, спектр нормативно-правовых актов, определяющих данные условия достаточно широк. Несмотря на это, анализ юридической практики зарубежных государств показывает, что использование «цифровых» подписей для удостоверения различных сделок и соглашений, является достаточно прогрессивным и распространённым способом, который упрощает и надежно защищает вышеназванную процедуру.

Перейдем к анализу некоторых вопросов нормативно-правового регулирования ЭЦП, как структурного элемента ЭД в юридическом процессе, на примере гражданского и арбитражного.

Эволюция общественных отношений в нашем государстве привела к тому, что на повестке дня находится целый перечень проблемных вопросов, одним из которых является применение результатов НТП, в частности именно средств технического характера, обсуживающих правовую среду в рамках использования доказательств в процессе осуществления отправления правосудия [30, с. 11].

В контексте рассматриваемой темы важно отметить, что цифровые документы являются альтернативными в сравнительном плане с аналоговыми документами, представляющими собой определенную группу электронного вида документов, обладающих способностью фиксации записей, базируясь на идеях конвертирования информации, данных и материалов документа в определенную кодированную цифровую форму. Углубляясь в специфику анализируемого явления, стоит учесть, что физический способ записи цифровой записи варьируется от механического до электромагнитного.

Кроме того, дополнительными специфичными аспектами в данном вопросе будут выступать существенные признаки документа электронного характера, а именно его непосредственное содержание и форма, выраженные в категориях информации и технического электронного носителя соответственно.

Стоит заметить, что электронная форма подразумевает под собой свое выражение в различного рода технических элементах, а также свойствах, характеристиках носителя информации. Ее формирование обусловлено применением электронно-технических средств, обладающих возможностью фиксации и обработке, а также передачи данных, благодаря чему становится возможным сохранение информации в таких документах, являющих собой состояние не письменной, а электронно-цифровой формы. Также важно отметить, что вместо тех письменных знаков, различных средств, содействующих написанию информации, материальными носителями такого рода данных и материалов являются электромагнитные поля, технические средства.

Далее рассмотрим «файл» в качестве базовой категории электронно-цифрового вида документа, представляющего собой, по сути, некую бумагу электронного характера. Правда, физическое состояние записи такого файла, а также его документированных данных в качестве объективной формы - важное и бесспорное требование самого существования данного файла. В свою очередь ранее изложенное предоставляет возможность файлу,



выражающему саму электронную документацию, во-первых, удовлетворять требованиям и критериям, дефинирующим документ как объект материального мира, а, во-вторых, способность обладания рядом нематериальных характеристик. Последнее означает способ передачи по электронным каналам связи документов электронного характера, а также наличие возможности правового объяснения перемещения и приравнивание таковых к их отправленным аналогам.

Специфика такой формы файла выражения электронного вида документов определяется процессом, при котором в ходе снятия копий каждая последующая абсолютно аналогична первой, а само материальное местоположение файловой записи не является архиважным. Последнее объясняется тем, что сами дефиниции оригинала электронного файла или, соответственно, его электронной копии не обладают должным смысловым наполнением, характерным для обычного письменного вида документа.

Так, электронный документ, будучи рассмотренный в контексте источника электронной формы судебного доказательства, являет собой данные об обстоятельствах, которые должны быть установлены в рамках конкретного дела и записаны на любой доступный носитель, удовлетворяющий требованиям и условиям процессуального порядка их приобретения.

Информационно-смысловое наполнение данных, составляющих сам электронный документ, не обладает существенными различиями с теми информационными материалами, которые, соответственно, могут отображаться на иных носителях, других видов документов. С целью последующего разграничения документов электронного характера и иными видами документов важно отметить в дефиниции данного явления особенности формы выражения этих информационных данных, рассматриваемых как запись на материальном носителе [24, с. 69]. К слову, сама форма электронного вида документов и представляет собой специфику данной группы документов по сравнению с другими.

Так для того, чтобы установить достоверность информационных данных, которые выступают в роли содержания непосредственно самого документа электронного характера, необходим факт существования опции идентификации и аутентификации последней, соответственно.

Аутентификация, рассматриваемая под призмой причастности к электронному документу, подразумевает под собой способ определения целостности, а также неизменности, по сути, «оригинальности», наполнения такого рода документов.

Идентификация же в данном контексте – возможность фиксации факта получения определенного документа от конкретного лица, фигурирующего в качестве его непосредственного отправителя.

Таким образом, важно наличие способности обеспечить действительно уверенную защиту информационных материалов, которые подлежат дальнейшей обработке посредством применения электронно-вычислительных технологий, оберегающих такого рода информацию от различных посягательств, в частности ее искажения, утечки и т.д. Отсутствие подобной защиты информационных данных от различного рода вмешательства и ее искажений ставит под сомнение факт достоверности таковой, что означает утрачивание юридической силы этих документов. Последнее имеет место быть даже в том случае, когда наличествует соблюдение всех необходимых реквизитов, что в свою очередь неизменно приводит к восприятию документов от подобного рода источников в качестве недопустимых в рамках осуществления гражданского судопроизводства.

С целью установления достоверности информационных данных в документе электронно-цифрового характера, как уже было подчеркнуто ранее, необходимо обязательное указание законодательно зафиксированных реквизитов. Соответственно, грамотное и с точки зрения следования правилам и «букве закона» оформление подобного рода документов, его подписание лицами, уполномоченными на совершение данного действия,

формирует базу для придания такому электронному документу юридической силы. Стоит отметить, что наиболее важным реквизитом, помимо указанного перечня в современном отечественном законодательстве, можно выделить именно ЭЦП, чья ценность в разрезе данной темы учитывалась еще издавна.

Так, ссылаясь на п.2 ст. 160 ГК РФ, важно акцентировать внимание на том, что в случае совершения сделок законодатель предусматривает применение электронно-цифровой подписи, если это учитывается соглашением сторон или представляется возможным касательно данной сделки. Являясь своего рода определенным цифровым кодом, ЭЦП идентифицирует, персонализирует лицо-автора данной подписи, отождествляя ее со своим письменным аналогом на бумажном носителе [24, с. 70].

Существует, конечно же, ряд сложностей и затруднений относительно деятельности, связанной с ЭЦП: например, не представляется возможным перенесение таковой с одного документа на другой, как это происходит в случае с обычной подписью бумажного вида документации. Из этого следует, что электронно-цифровая подпись – вид реквизита, предусмотренный только для определенного подписанного ею документа соответственно. Стоит также добавить, что в контексте исследуемого вопроса вышеуказанный вид подписи способствует возникновению опции производства проверочных мероприятий относительно подлинности самого документа электронного характера и установления личности автора, оставившего данную подпись. Кроме того, в случае признания проверочными мероприятиями подлинности и, соответственно, целостности документа, обладающего таким реквизитом, как ЭЦП, то указанная подпись лица, подписавшего документ, не подвергается дальнейшему сомнению. В свою очередь это наделяет электронный документ определенным юридическим статусом в рамках приобщения такого документа к материалам дела в суде.

Подытоживая вышеизложенное в данном параграфе нашего исследования, важно отметить, что было бы целесообразно зафиксировать в отечественном современном гражданско-процессуальном законодательстве перечень правовых гарантий достоверности информационных данных, которые были приобретены посредством применения достижений НТП, в частности современных научно-технических средств. Также важно и закрепление наличия юридической ответственности за осуществление действий, фальсифицирующих подобные информационные данные, а также установление процессуального алгоритма проведения исследования сопутствующих источников в рамках проведения судебного заседания.

Немаловажным представляется и решение рассматриваемого вопроса, исходя из его практической и теоретической сторон, комплексным методом с целью повышения результативности применения электронного вида документации, фигурирующей в качестве доказательств по конкретному делу в рамках осуществления гражданско-процессуального судопроизводства.

## **2.2 Ключевые особенности использования «цифровых» подписей**

Проанализируем ключевые особенности использования «цифровых» подписей.

Анализ положений отечественной нормативно-правовой базы позволяет сделать вывод о том, что на сегодняшний день имеет место быть широкое использование «цифровых» подписей в деятельности органов публичной власти различных уровней, включая:

- федеральный;
- субъектный;
- местное самоуправление
- иные учреждения и организации, которые вступают в отношения с ними.

В таком случае «цифровые» подписи ставятся уполномоченными должностными лицами, наделенными правом подписи юридически значимых документов, и обладающие соответствующим сертификатом [19, с. 66].

Нетрудно сделать вывод о том, что владельцем и пользователем такой подписи является не орган публичной власти, а конкретное физическое лицо, являющееся должностным, то есть представляющее интересы вышеназванных органов.

Анализ юридической практики Самарского региона последних лет показывает, что зачастую имеют место быть случаи злоупотребления полномочиями, при подписании тех или иных электронных документов. Особое место здесь занимают случаи, когда документы подписываются «цифровой» подписью с истекшим сроком действия.

Органом публичной власти, который удостоверяет действительность «цифровой» подписи на сегодняшний день является Министерство цифрового развития (далее – Минцифры). Данный орган публичной власти осуществляет процедуры контроля и выдачи сертификатов на «цифровые» подписи, вместе с этим реализуется их учет, путем ведения соответствующего реестра. Деятельность Минцифры осуществляется на основе положений отечественной законодательной базы в сфере правового регулирования использования современных «цифровых» технологий.

Использование методов и форм реализации электронного документооборота, в том числе и «цифровой» подписи и их аналогов, в виде графических изображений имело место быть и до принятия вышеописанного нормативно-правового акта. В качестве яркого примера реализации современного электронного документооборота можно привести способы взаимодействия по принципу «банк-клиент», которые имеет место быть в общественных отношениях между банковской организацией с одной стороны и физическим или юридическим лицом с другой [15, с. 156].

Особенности процедуры взаимодействия между банковскими организациями устанавливаются нормативно-правовыми предписаниями

Центрального Банка Российской Федерации. Такое положение дел детерминировано наличием особого правового статуса у последнего.

Основной вышеназванной процедуры является наличие у банковских организаций соответствующих корпоративных информационных систем, которые призваны упростить коммуникацию между внутренними структурными подразделениями банковской организации. Одной из характерных черт такой системы является ограниченность численности ее участников. Если говорить точнее, то их количество определяется непосредственно руководством банковской организации.

Отечественное законодательство предписывает вышеприведенным системам полную или частичную автономность работы. Иными словами, если данная система сфокусирована исключительно на внутреннюю коммуникацию между структурными подразделениями учреждения или организации, то нормативно-правовую основу реализации и функционирования коммуникации в рамках данной системы составляют локальные акты. В случаях, когда имеет место быть взаимодействие с органами публичной власти или иными государственными или муниципальными учреждениями, то построение и функционирование электронных информационных систем должно осуществляться в соответствии с положениями федерального законодательства. В тексте закона, такие системы обозначаются как «системы общего пользования». В качестве примера можно привести «Госуслуги», ГАС «Правосудие» и др.

Проанализируем особенности правового регулирования внутренней коммуникации посредством электронных информационных систем в организации или учреждении. К предмету правового регулирования следует относить определение процедуры применения «цифровых» подписей. Следует отметить, что локальная нормативно-правовая база учреждения или организации не должна противоречить положениям федерального законодательства в части регулирования процедуры использования электронных документов и «цифровых» подписей.

Данные нормативные акты определяют содержание информации в сертификатах ключей подписей, порядок ведения реестра сертификатов, порядок хранения аннулированных сертификатов, случаи утраты юридической силы данными сертификатами. Также соглашением участников может быть определен тот участник, на которого возлагаются функции удостоверяющего центра или центра сертификации (далее - ЦС).

«Содержание документа на бумажном носителе, заверенного печатью и преобразованного в электронный документ, может быть подписано электронной цифровой подписью и будет иметь равную юридическую силу, но при условии, что такое преобразование осуществлено согласно имеющемуся соглашению между сторонами либо в соответствии с нормативным правовым актом (ст. 19 Федерального закона)» [43].

Данная возможность использования электронной цифровой подписи в качестве «эквивалента не только собственноручной подписи, но и печати значительно расширяет возможности организаций в гражданско-правовых отношениях» [43].

Следует отметить, что национальное гражданское законодательство не содержит в себе правовых предписаний, которые устанавливали бы в качестве обязательного условия удостоверения договоров печатями [11].

Нетрудно сделать вывод о том, что наличие печатей в договорах, как условие удостоверения сделки может выступать в качестве одного из требований сторон, принимающих участие в подписании такого договора. Однако, несмотря на такое положение дел, анализ отечественной законодательной базы показывает, что ряд документов при удостоверении нуждается в постановке печати, к таким документам следует относить: финансово-экономическую и налоговую документацию. Вместе с этим, и гражданское законодательство допускает в исключительных случаях необходимость постановки печати, например, при выдаче доверенности директором или руководителем юридического лица своему подчиненному, дающему право подписи каких-либо документов.

Национальное законодательство своими предписаниями фактически приравнивает «цифровые» подписи к обычным собственноручным, заверенными печатями. Таким образом, возникает «уникальная возможность использования «цифровых» подписей не только юридическим лицам в ходе осуществления коммерческой или иной деятельности, но и физическим лицам при вступлении в различные правоотношения» [7]. Обеспечения безопасности использования «цифровых» подписей возлагается на органы публичной власти.

Выводы по главе:

На основании праведного в данной глава исследования автором работы были сделаны следующие научно-исследовательские выводы:

Анализирую практику применения ЭЦП, полагаем целесообразным фиксацию в отечественном современном законодательстве перечня правовых гарантий достоверности информационных данных.

Также важно и закрепление наличия юридической ответственности за осуществление действий, фальсифицирующих подобные информационные данные, а также установление процессуального алгоритма проведения исследования сопутствующих источников в рамках проведения судебного заседания.

Отечественное законодательство предписывает информационно-правовым системам полную или частичную автономность работы. Иными словами, если данная система сфокусирована исключительно на внутреннюю коммуникацию между структурными подразделениями учреждения или организации, то нормативно-правовую основу реализации и функционирования коммуникации в рамках данной системы составляют локальные акты. В случаях, когда имеет место быть взаимодействие с органами публичной власти или иными государственными или муниципальными учреждениями, то построение и функционирование электронных информационных систем должно осуществляться в соответствии с положения федерального законодательства. В тексте закона,



такие системы обозначаются как «системы общего пользования». В качестве примера можно привести «Госуслуги», ГАС «Правосудие» и др.

Органом публичной власти, который удостоверяет действительность «цифровой» подписи на сегодняшний день является Министерство цифрового развития (далее – Минцифры). Данный орган публичной власти осуществляет процедуры контроля и выдачи сертификатов на «цифровые» подписи, вместе с этим реализуется их учет, путем ведения соответствующего реестра. Деятельность Минцифры осуществляется на основе положений отечественной законодательной базы в сфере правового регулирования использования современных «цифровых» технологий.

Использование «цифровых» подписей позволяет разрешать следующие задачи:

- обеспечивать невозможность отказа от факта подписи электронного документа конкретным лицом;
- установление целостности электронных сообщений;
- осуществление аутентификацию источников электронных сообщений.

Безусловно, использование понятия «подпись» в приведенном контексте детерминировано тем, что и «цифровые», и традиционные собственноручные имеют много общего, в частности и та и другая способны удостоверить соглашения и сделки, то есть влекут за собой придание юридические силы подписанным документам.

Заключительная глава магистерской диссертации будет посвящена актуальным проблемам использования «цифровых» подписей в отечественной юридической практике.

## **Глава 3 Актуальные проблемы использования «цифровых» подписей в юридической практике**

### **3.1 Проблемы обеспечения подлинности «цифровых» подписей**

Как мы установили электронный документ обладает присущими ему особенностями и спецификой использования. Такие черты обуславливаются технологией его изготовления. Главное отличие электронного документа от «обычного» состоит в том, что, что в таком документе нет возможности поставить собственноручную подпись (письменно расписаться).

Процедура подтверждения электронного документа электронно-цифровой подписью заключается в использовании специальных (секретных) ключей, которые хранятся только у владельца сертификата ключей подписи. Могут применяться и открытые ключи, владельцами которых выступают любые лица, являющиеся пользователями информационной системы.

Указанные ключи математически взаимозависимы друг от друга. Это объясняется тем обстоятельством, что с помощью открытого ключа можно проверить каким секретным ключом было сообщение зашифровано. Однако сам закрытый ключ вычислить не удастся.

Можно заключить, что секретный (закрытый) ключ является самым важным элементом ЭЦП. Именно с помощью него, а также программы-криптопровайдера создается ЭЦП, происходит подписание электронных документов.

Цифровую подпись не следует путать с классической стильной подписью, которую можно создать и включить в любую программу электронной почты. Несмотря на похожее название, последнее относится к текстовой подписи в нижней части электронного письма, которая появляется в форме, аналогичной нарисованной от руки подписи, и обычно предшествует контактной информации отправителя, такой как имя, адрес,

номер телефона и должность. Вместо этого цифровая подпись представляет собой общую электронную подпись, обычно включающую три алгоритма:

- алгоритм генерации ключей;
- алгоритм подписи;
- алгоритм проверки подписи (Приложение А).

В совокупности эти методы повышают уровень безопасности, связанный с процессом подписания документов.

От обеспечения сохранности закрытого ключа непосредственно зависит степень безопасности информационной системы, которая использует ЭЦП. Как следствие в настоящее время проблема обеспечения защиты от несанкционированного доступа к секретному (закрытому) ключу, как и к электронной цифровой подписи является актуальной и требует принятия соответствующих мер [6, с. 99].

Основным принципом создания цифровой подписи является концепция асимметричного шифрования. Это означает, что отправитель получает два ключа от алгоритма генерации ключей: закрытый ключ и открытый ключ. Почтовая программа отправителя автоматически создает контрольную сумму содержимого почты, шифрует контрольную сумму с помощью закрытого ключа, а затем прикрепляет ее к электронному письму.

Открытый ключ либо отправляется с вложением, либо получается получателем через общедоступный каталог. Затем почтовая программа получателя расшифровывает контрольную сумму, пересчитывает ее и затем проверяет результаты. Если результаты совпадают, можно быть уверенным, что сообщение было подписано закрытым ключом, совпадающим с соответствующим открытым ключом. Аутентификация прошла успешно, и доказано, что электронное письмо поступило из надежного источника и прибыло без манипуляций.

Инфраструктура открытых ключей представляет собой набор требований, которые позволяют (среди прочего) создавать цифровые подписи. Каждая транзакция цифровой подписи включает пару ключей:

закрытый ключ и открытый ключ. Закрытый ключ, как следует из названия, не является общим и используется только подписывающей стороной для электронной подписи документов. Открытый ключ находится в открытом доступе и используется теми, кому необходимо проверить электронную подпись подписавшего. Данный алгоритм предъявляет дополнительные требования, такие как центр сертификации, цифровой сертификат, программное обеспечение для регистрации конечных пользователей и инструменты для управления, обновления и отзыва ключей и сертификатов.

Как уже отмечалось цифровые подписи основаны на открытых и закрытых ключах. Эти ключи должны быть защищены, чтобы обеспечить безопасность и избежать подделки или злонамеренного использования. Когда пользователь отправляет или подписывает документ, необходимо убедиться, что документ и ключи созданы безопасно и что в них используются действительные ключи. Центры сертификации являются сторонними организациями, которые обеспечивают безопасность ключей и могут предоставить необходимые цифровые сертификаты. Лицо, отправляющее документ, и получатель, подписывающий его, должны согласиться на использование данного ЦС.

Для нужд цифровой подписи система может использовать криптографию с открытым ключом, а для проверки личности пользователя, подписывающего документ, удобнее всего использовать цифровые сертификаты.

Одним из требований для использования цифровых подписей является то, что почтовый клиент пользователя должен быть заранее правильно настроен. Если это так, описанный выше процесс будет выполняться автоматически в фоновом режиме.

Сертификаты могут быть самоподписанными или выданными центром сертификации. Если пользователи выдают себе самозаверяющие сертификаты и используют их для подписи документов, нет никакой гарантии, что злоумышленник не выдаст себе сертификат с другим именем и

не подпишет документы, как если бы он был каким-то другим пользователем. Поэтому необходим поиск соответствующих решений, чтобы избежать этого недостатка безопасности.

Еще одной проблемой является следующее обстоятельство. Вполне возможно, что именно лицо, ответственное за обслуживание системы – системный администратор – будет выдавать цифровые сертификаты. Это можно сделать двумя способами – либо системный администратор генерирует открытый и закрытый ключи для пользователей, либо они генерируют их сами.

В первом случае администратор потенциально может злоупотреблять своими правами. Остается возможность, что пользователи лично генерируют свой открытый и закрытый ключ, после чего они каким-то образом отправляют открытый ключ вместе с информацией о своей личности системному администратору, который, в свою очередь, выдает сертификат.

Недостаток этого процесса заключается в том, что он никоим образом не гарантирует, что пользователи не будут подделывать свои идентификационные данные. Единственная оставшаяся возможность заключается в том, что каждый пользователь лично представляет свой открытый ключ, и администратор выдает ему сертификат после тщательного изучения его документов, удостоверяющих личность. Это решение более приемлемо, но на самом деле администратор действует как центр сертификации и все еще может злоупотреблять своими правами на выдачу сертификатов.

Лица, использующие ЭЦП, могут воспользоваться услугами Удостоверяющих центров для получения электронной цифровой подписи, аккредитованных Минкомсвязью России для решения проблем с сертификатами.

Каждый пользователь системы может приобрести сертификат у такого центра сертификации, и этот центр может гарантировать, что сертификат действительно принадлежит лицу, которому он был выдан. Закрытый ключ,

соответствующий любому сертификату, доступен только его владельцу и никому другому. Это гарантирует, что, когда пользователь подписывает документ сертификатом, выданным утвержденным центром сертификации, это действительно его подпись. Подделка возможна только в том случае, если злоумышленники получают закрытый ключ пользователя, за который пользователь несет личную ответственность.

Покупка цифрового сертификата сопряжена с определенными расходами для каждого пользователя, но это единственный надежный способ гарантировать безопасность. Обычно вместе с сертификатом пользователь получает файл PFX, содержащий сертификат и соответствующий ему закрытый ключ, защищенный паролем. Если в результате покупки центр сертификации установит сертификат непосредственно в веб-браузер клиента, пользователь сможет экспортировать его в виде файла и с этого момента использовать файл для подписи документов.

Возможным подходом к решению многих проблем, связанных с использованием ЭЦП, было бы обязательство пользователей устанавливать на свои компьютеры специально разработанное программное обеспечение, но это сопровождается определенными трудностями.

Одной из них является то обстоятельство, что программное обеспечение для подписи должно иметь отдельные версии, поддерживающие разные операционные системы, которые могут быть у пользователей. Более того, поддержка такого программного обеспечения является громоздкой, поскольку любое изменение в нем заставит пользователей загружать и устанавливать новую версию.

Интеграция с веб-интерфейсом системы является еще одной сложной задачей, и если программное обеспечение плохо интегрировано, его использование может вызвать проблемы у пользователей. Существует также вероятность того, что пользователи откажутся устанавливать программное обеспечение на свои компьютеры по соображениям безопасности, также,

если они не используют свои собственные компьютеры, им могут физически помешать это сделать.

Мы полагаем, что с точки зрения юридического подхода разрешение вопросов подтверждения подлинности электронных документов, дало бы возможность ввести в законодательный оборот понятие «электронный юридически значимый документ». Однако сегодня, документы, переданные в электронном виде в рамках документооборота, вряд ли можно считать «юридически значимыми». Такое положение дел связано с тем обстоятельством, что нет стопроцентной гарантии того, кем конкретно этот документ был в действительности подписан. Это в равной степени может быть и владелец закрытого ключа, так и злоумышленник.

Кроме того, как известно, к цифровой подписи доступ можно получить только по выданному паролю, записанному либо на интеллектуальной карте, либо на компьютере. Это, в свою очередь может привести к тому, что карта владельцем может быть утеряна или передана другому лицу. Собственноручную подпись лица в отличие от ЭЦП, можно всегда идентифицировать по особенностям его письма.

Нет ничего более пугающего, чем поддельная или недействительная подпись, подписанная традиционным или электронным способом в юридическом документе, финансовой отчетности, контрактах и других официальных документах. Поддельные подписи являются одним из основных методов мошенничества с удостоверениями личности и иллюстрируют отсутствие безопасности, характерное для физических подписей. Вот почему цифровые подписи становятся отраслевым эталоном для подписания документов и создания доказательств. Цифровые подписи - это наиболее безопасный способ удостоверить личность подписавшего и надежное доказательство того, что этот документ подписал именно он, а никто другой.

В настоящее время компании, предоставляющие услуги по электронному документообороту (СЭД) в России, сами указывают, что такие

электронные документы могут вызывать правовые последствия, только если: помимо обязательных для документа реквизитов, полностью гарантируются целостность и подлинность подписи [50].

Подводя итоги анализа проблем обеспечения подлинности «цифровых» подписей, можно утверждать, что на сегодняшний момент ЭЦП лишь косвенно может подтвердить авторство того или иного электронного документа. Такое положение дел связано с правовыми, организационными и техническими факторами.

Как верно отмечают Е.И. Гончаров и Т.В. Шатковская, вышеперечисленные проблемы становятся особенно актуальными «в условиях цифровой безграмотности значительной части российского общества, а также психологической боязни резкого перехода на новый уклад жизни, где в ней не остается ничего бумажного и овеянного. Поэтому внедрение новых информационных технологий должно проходить последовательно и на основе доверия граждан России» [6, с. 106].

В физическом мире люди интуитивно понимают, что такое подпись в ее рукописной форме, тогда как в электронном мире электронные подписи охватывают гораздо более широкий спектр возможных форм, от блоков подписи электронной почты до записей голоса и защищенной даты онлайн-сеанса (когда вы нажмете «Принимаю») к изображениям рукописных подписей к криптографически защищенным цифровым подписям. Подпись - это постоянный знак, который уникален, используется исключительно и отслеживается до лица и проставляется на статической информации с подразумеваемым или выраженным намерением. Все в электронном мире, выполняющее эту функцию, является подписью. Всякий раз, когда вы применяете подпись к чему-либо, особенно к документам, вы создаете свидетельство транзакции. Степень, в которой это свидетельство будет обладать следующими четырьмя атрибутами надежности, будет влиять на доказательную ценность ЭЦП:



- идентичность (уверенность в личности подписавших);
- целостность (уверенность в отсутствии необнаруженных изменений в подписанной информации);
- подлинность (все, что требуется для подтверждения подлинности, а долговечность заложена в самом документе);
- долговечности (подписанный документ или информация могут быть открыты, прочитаны и аутентифицированы в течение по крайней мере периода их хранения).

Цифровые подписи могут с достаточной степенью уверенности доказать как подлинность, так и целостность. Аутентичность гарантирует, что данный файл действительно был создан лицом, подписавшим его (т. е. что третья сторона не подделала его). Целостность гарантирует, что содержимое файла не было изменено (т. е. что третья сторона не изменила его содержимое незаметно в пути). Целостность означает, что запись является полной и неизменной. Это не означает, что записи не могут претерпевать никаких изменений, однако они должны быть защищены от несанкционированного доступа или повреждения.

Таким образом, целостность не означает, что записи должны быть точно такими же, какими они были при создании или полученный. Целостность записи означает, что ее функция и окончательность не изменились. При этом существенный характеристики или компоненты документа не могут быть изменены.

С учетом того, что текст является преобладающим средством онлайн-коммуникации, становится крайне важным использовать методы для защиты такой информации. Чтобы оценить надежность конкретной электронной подписи, необходимо оценить:

- надежна ли личность подписавших;
- являются ли изменения в документе правильно датированными электронными подписями;
- вся ли необходимая информация для подтверждения подлинности и целостности заложена в документе;
- подписан ли и сохранен ли документ в логическом формате, гарантирующим то, что он останется читаемым и поддающимся проверке столько времени, сколько потребуется.

Таким образом электронная (цифровая) подпись гарантирует целостность как данных, так и отправителя электронного письма. Обычно они используются для аутентификации источника цифровой информации - не только электронных писем, но также документов и макросов. Таким образом, цифровая подпись выполняет ту же роль, что и ее тезка для бумажных документов: она обеспечивает подлинность лица или компании, указанных в качестве отправителя электронной информации. Используя цифровую подпись, возможно защитить целостность любых данных, которые передаются в Интернете. Получатель может быть уверен, что никто не получил доступ к содержимому и не подделал его, поскольку электронная подпись действует как печать. Это означает, что в случае спора эта подпись может быть использована для точного подтверждения того, откуда пришло электронное письмо. И лицо (или компания), подписавшее письмо, и содержание сообщения электронной почты отображаются для просмотра получателем

Тем не менее, стоит отметить, что сегодня отсутствуют правовые нормы, которые регламентировали бы порядок обеспечения привязки ЭЦП к физическому лицу. Тем не менее, по нашему мнению, целесообразным способом решения указанных проблем представляется совместное использование секретного закрытого ключа и технологий цифровой идентификации личности. На современном этапе развития науки выделяют такие биометрические свойства личности, как отпечатки пальцев, геометрия

лица, радужная оболочка глаз, рисунок сетчатки, голос, почерк, узор вен на руках и ногах, и т.д. [33, с. 140].

При выборе биометрических параметров для идентификации личности следует учитывать:

- скорость идентификации, а именно то, сколько времени потребуется для точного сбора идентификационных данных и их распознавания;
- удобство сбора биометрической информации;
- широту охвата данных; способ сбора данных и устойчивость к фальсификации;
- устойчивость к помехам; необходимую инфраструктуру и технические средства;
- общую надежность системы биометрии, которая характеризуется качеством распознавания; стоимость реализации метода и другие факторы.

Решению задачи, которая позволила бы устанавливать неопровержимую связь секретного ключа и его владельца, по нашему мнению, будет способствовать создание электронно-цифровой подписи, основанной на новой методике использования биометрических данных и соответствующего программно-аппаратного комплекса, обеспечивающего защиту от несанкционированного доступа к процессу подписания электронного документа. Это позволило бы уравнивать ЭЦП и собственноручную подпись.

### **3.2 Проблемы, возникающие при применении электронных документов, подтвержденных «цифровыми» подписями**

В данном параграфе магистерской диссертации нами будут рассмотрены на примере различных отраслей права проблемы использование электронных документов, подтвержденных электронными (цифровыми) подписями.

Сегодня использование электронной подписи в гражданско-правовых отношениях, например, при заключении договоров, совершаемых в отношении как движимого, так и недвижимого имущества, представляет серьезную проблему.

В настоящее время для подписания большинства документов требуется наличие электронной подписи [20, с. 55]. Законодатель в статье 2 Федерального закона «Об электронной подписи» дает следующее толкование: «электронная подпись - это 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» [43]. Из данной дефиниции под электронной подписью понимается заверение (утверждение) соответствующих документов, на основании которого приобретает юридическую значимость тот или иной договор.

В соответствии с вышеуказанным законом выделяют следующие виды электронной подписи: простая и усиленная электронная подпись, последняя, в свою очередь, делится на усиленную квалифицированную и усиленную неквалифицированную электронную подпись. Такое разграничение усиленных электронных подписей частично позволило решить проблему. Само деление на данные виды создает определенный уровень защиты этих цифровых подписей, чтобы предотвратить возможную угрозу ее подделки (подмены) другим лицом при заключении соглашений не только относительно движимого, но и недвижимого имущества.

Прежде всего стоит отметить, что законодатель, в области заключения договоров посредством использования электронной подписи не устанавливает определенные виды таких договоров, что следует из 160 статьи ГК РФ [11]. Таким образом, перечень на данный момент остается открытым. Но тем не менее, есть ограничения, которые предусмотрены законом.

Как правило, основными видами договоров, которые можно заключать при использовании электронной подписи, являются - договоры с недвижимым имуществом и движимым. Как показывает практика, переход права собственности на недвижимое имущество порождает гораздо больше судебных споров нежели движимое, поскольку сам переход имущества от одного лица к другому предполагает усложненный порядок и с той целью, чтобы защищать права субъектов данных правоотношений и не подвергать их реальным и потенциальным угрозам.

Но означает ли это, что сам факт возможности заключения сделки как с недвижимостью, так и с движимостью при использовании электронной подписи исключает традиционные опасности и порождает новые? Или как раз-таки все происходит с точностью да наоборот? Что же тогда меняется в гражданском обороте? Прежде чем переходить к рассмотрению такого интересного феномена в гражданском праве, нужно исходить из самих предпосылок, определивших появление электронной подписи.

Применение электронной подписи обусловлено рядом причин:

- стремительным развитием информационных технологий и цифровизацией общественных отношений;
- существующей угрозой подделки личных рукописных подписей, например, при заключении сделок;
- ЭЦП предполагает значительное упрощение документооборота (как для физических, так и юридических лиц);
- ЭЦП способствует минимизации субъектами гражданских правоотношений расходов при заключении х договоров (сделок).

Вышеперечисленные факторы демонстрируют очевидное преимущество ЭЦП перед «традиционной».

Конечно же, преимущества такой подписи имеют превышающее значение в сравнении с обычной личной подписью, но с юридической точки зрения, вне зависимости от какой формы - простой письменной или электронной, договор считается заключенным.

Согласно части 1 статьи 160 ГК РФ: «Сделка в письменной форме должна быть совершена путем составления документа, выражающего ее содержание и подписанного лицом или лицами, совершающими сделку, либо должным образом уполномоченными ими лицами. Письменная форма сделки считается соблюденной также в случае совершения лицом сделки с помощью электронных либо иных технических средств, позволяющих воспроизвести на материальном носителе в неизменном виде содержание сделки, при этом требование о наличии подписи считается выполненным, если использован любой способ, позволяющий достоверно определить лицо, выразившее волю. Законом, иными правовыми актами и соглашением сторон может быть предусмотрен специальный способ достоверного определения лица, выразившего волю» [11].

Как видим, законодатель не делает конкретных и существенных разграничений. Разница лишь в объективных причинах, упрощающих порядок заключения сделок с использованием электронных средств, и в предоставлении больших гарантий защиты прав собственности, что, конечно же, имеет важное значение.

Стоит заострить внимание на том, чем отличаются друг от друга данные виды электронной информации, чтобы понимать значимость этих делений и разграничений. В статье 5 Федерального закона «Об электронной подписи» указано следующее: простой электронной подписью является электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом [43].

В статье 5 Федерального закона «Об электронной подписи» указано следующее: «простой электронной подписью является электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом» [43].

Закон устанавливает неквалифицированную и квалифицированную электронные подписи, которые используются различными органами и учреждениями (Приложение Б и В).

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 и создается с использованием средств электронной подписи.

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 и для создания и проверки электронной подписи используются средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии с настоящим Федеральным законом. Это свидетельствует о значительном ряде преимуществ электронной подписи перед личной, поскольку последнюю легко подделать или изменить, и тем самым по статье 169 ГК РФ: «сделка, совершенная с целью, заведомо противной основам правопорядка или нравственности, ничтожна и влечет последствия, установленные статьей 167 настоящего Кодекса» - будет признана недействительной [11].

По этим причинам возникают многочисленные споры в судах, в том числе и в результате злоупотребления правом, которое выражается в некоторых случаях, в умышленном искусственном создании условий и обстоятельств, создающих сомнения в действительности соответствующих документов, подписанных (заверенных) лицом.

Из этого можно сделать следующий вывод: частные лица и организации имеют право по своему собственному усмотрению использовать

электронную подпись любого вида (что, безусловно, должно отражаться в соглашении между ними) - это может быть простая или усиленная подпись, а также усиленная квалифицированная и усиленная неквалифицированная, но за исключением тех случаев, когда условия заключения определенных договоров определены законодателем либо в федеральных законах или в других нормативно-правовых актах.

На основании этого заключаем, что информация в электронной форме, подписанная электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, который подписан собственноручной подписью, а значит обладает неотъемлемой юридической значимостью и вещественным доказательством, свидетельствующим о заключении какого-либо гражданско-правового договора.

Казалось бы, что при использовании электронной подписи при заключении гражданско-правовых договоров (сделок) не могут возникнуть серьезные угрозы, но тем не менее они имеют место быть.

Во-первых, есть вероятность, хоть и небольшая, что электронную подпись можно подделать, в результате чего, как уже отмечалось выше про личную подпись, сделка будет считаться недействительной, то есть оспоримой по статье 168 и 169 ГК РФ [11]. В таком случае, должна быть применена реституция, то есть возвращение сторон в первоначальное положение. Но также, как отмечалось ранее, субъекты правоотношений, ввиду своей недобросовестности, могут злоупотреблять своими правами (ч. 4 ст. 10 ГК РФ), находить пути обхода закона и многие другие мошеннические способы и незаконные действия.

Таким образом, до 2019 года законами не были урегулированы вопросы, касающиеся защиты от мошенничества с использованием электронной подписи. По этой причине, появлялись разного рода мошеннические схемы завладения чужой недвижимостью, которые совершались посредством дистанционной подачи документов на



государственную регистрацию прав с незаконным использованием электронной подписи собственника данного недвижимого имущества.

Итогом стало урегулирование данного вопроса на федеральном уровне, посредством принятия закона «О внесении изменений в Федеральный закон «О государственной регистрации недвижимости»» [41], совершаемых при помощи электронной подписи. Как отмечает автор данного законопроекта, профессор, председатель Комитета Государственной Думы по государственному строительству и законодательству - Павел Владимирович Крашенинников: «данным законопроектом предлагается установить, что переход права на недвижимость физического лица на основании заявления, поданного в электронной форме, будет осуществляться только в том случае, если собственник заранее уведомил Росреестр о возможности такой формы подачи документов. В этом случае регистрирующий орган проставляет в реестре специальную отметку о возможности отчуждения данного объекта на основании электронного заявления с использованием усиленной квалифицированной электронной подписи. Без такой отметки Росреестр не сможет принять к рассмотрению документы о переходе права в электронной форме, и они будут возвращены заявителю. Отметка может быть проставлена в ЕГРН только на основании личного заявления владельца недвижимости, либо посредством почтового отправления в Росреестр, в котором подлинность подписи заявителя свидетельствуется в нотариальном порядке» [10].

Тем самым, данный законопроект закрепил важнейший ряд гарантий, который предусматривает защиту прав собственника данного имущества, что без его подписи электронные документы о переходе права собственности не будут приняты к исполнению. Данная гарантия обусловлена также и тем, что государственная регистрация является единственным доказательством существования зарегистрированного права, что по существу означает презумпцию правильности регистрации не только прав, но и сделок. На основании вышеизложенного возникает некоторая презумпция

подтверждения (использования) электронной подписи собственником имущества.

Также, важно выделить и другие проблематичные аспекты, которые до сих пор в полной мере не урегулированы государством. Возникает некоторая трудность идентификации (определения) субъекта, подписавшего документы электронной подписью.

Помимо этого, при предъявлении иска в суд, связанного с возникшим спором по использованию и применению электронной подписи при заключении гражданских договоров, отсутствуют надлежащие критерии разграничения истинных доказательств, применяемых в суде, по идентификации этой подписи. Так как информационные технологии развиваются стремительно, прослеживается некоторая черта возможной будущей технологической сингулярности, законодатель значительно отстает от стремительно изменяющегося вокруг него не только окружающего, но и информационного мира.

В Российской Федерации деятельность правоохранительных органов в информационной сфере практически не развита и, поэтому возникает ряд трудностей защиты прав человека и гражданина в информационном пространстве.

Необходимо сказать и о проблемах применения электронных документов при разрешении административно-правовых споров.

Кодекс Российской Федерации об административных правонарушениях не содержит ответа вопрос, «что же такое электронный документ». Объясняется это тем обстоятельством, что данная дефиниция в нем отсутствует. Тем не менее, применительно к видам документов в административно-правовых отношениях в ст. 26.7 КоАП РФ говорится о том, что они могут быть представлены как в письменной, так и в иных формах. Иными словами, законодатель предусмотрел существование и такой формы документов, как электронные документы [18].

Кроме того, законодательно установлено, что оформленные в электронной форме материалы и документация, которые были полученные с использованием различных технических устройств (например, позволяющих фиксировать нарушения правил дорожного движения с помощью фото- и видеозаписи), также могут быть использованы в случаях если их правовая природа подтверждается электронной цифровой подписью (п. 6 ст. 29.10 КоАП РФ) [18].

Тем не менее, отсутствие в КоАП РФ законодательного закрепления дефиниции «электронная цифровая подпись», а также не содержит понятия «электронный документ». Это обстоятельство порождает коллизии и проблемы применения на практике электронных документов, скрепленных цифровой подписью, и, в частности отнесения таких документов к доказательствам по делам об административных деликтах.

Тем не менее, среди ученых-юристов и практиков есть точка зрения, что электронные документы могут быть отнесены к письменным доказательствам с учетом положений норм ст. 75 АПК России и 71 ГПК России. Эти нормы указывают нам на то обстоятельство, что письменные доказательства могут существовать как в цифровой форме, так и в письменной, т.е. в виде графической записи.

Так, например, И.Н. Баранов и Н. Д. Бондарев полагают, что электронные (цифровые) документы могут и должны быть использованы в качестве доказательств в сфере гражданского права наравне с бумажными носителями информации [3]

По мнению других специалистов, электронный документ нельзя признавать в качестве самостоятельного письменного доказательства, т.к. он не обладает существенным признаком, а именно - письменной формой.

Полагаем, что наиболее верной и обоснованной является именно эта точка зрения, тем более, что она подкреплена положениями ст. 26.7 КоАП РФ, в которой законодатель прямо указывает на «иную форму документа», отличимую от «традиционной» письменной.

Кроме того, ряд исследователей склоняются к точке зрения, что электронные (цифровые) документы следует относить именно к вещественным доказательствам, находя при этом определенное сходство с ними:

- электронные (цифровые) документы в некотором роде являются недоступными сами по себе человеческим органам чувств;
- электронные (цифровые) документы являются всего лишь средством установления имеющих значение для дела обстоятельств.

Есть еще одна группа ученых и практиков, которые придерживаются точки зрения, что цифровые средства доказывания охватываются всеми возможными известными видами доказательств, однако при этом они нуждаются в особой (дополнительной) правовой регламентации. С этой точкой зрения мы также солидаризируемся.

Таким образом, анализируя различные позиции исследователей, которые изучают проблемные вопросы, связанные с электронными (цифровыми) документами, мы приходим к выводу о том, что последние имеют двойственный характер и как новый вид доказательственной информации содержат в себе признаки как письменных, так и вещественных доказательств.

И действительно, при внимательном рассмотрении электронных (цифровых) доказательств, мы обнаруживаем их новые свойства. Такие как их тиражируемость, т.е. возможность многократного повторения информации без потери ее смысла (содержательной стороны). А это уже свойство, которое присуще только доказательствам в письменной форме [7, с. 27].

При этом, является очевидным тот факт, что с вещественными доказательствами цифровой документ роднит то обстоятельство, что он сам по себе является недоступным человеческому восприятию, при этом выступает в качестве установления значимых для дела обстоятельств. Информация же содержится на материальном носителе, в качестве которого

может выступать любой информационный носитель (внешний диск, USB-флеш-накопитель, карты памяти, память ЭВМ, и т.д.). От письменного доказательства такая информация отличается еще и тем обстоятельством, что далеко не всех электронных (цифровых) документах выражена субъективной авторская мысль, которая основывается на анализе и переработке информации.

По нашему мнению, наиболее верно было бы считать электронный (цифровой) документ сочетанием или своеобразной комбинацией как «традиционного» (письменного), так и вещественного доказательства. При этом, учитывая такой двойственный характер электронного (цифрового) документа, нам представляется наиболее верно говорить о нем как о особой (самостоятельной) форме доказательств -электронной.

Приведем еще ряд аргументов в пользу этой точки зрения:

- письменные и вещественные доказательства являются продуктом деятельности человеческого труда (изготавливаются им);
- несут на себе следы деятельности человека.

При этом электронные (цифровые) документы не всегда обладают этими свойствами, т.к. современные цифровые технологии достигли такого уровня, когда ЭВМ, оснащенные соответствующим программным обеспечением, например, на базе искусственного интеллекта, могут без вмешательства человека, самостоятельно генерировать новые электронные (цифровые) документы.

Приведем пример. Например, нейросети на основе искусственного интеллекта могут по потоку картинок не только считывать информацию о реальном мире, но и создавать собственные новые образы и тексты или превращать бумажные, отсканированные и электронные носители в структурированную информацию, извлеченную из этих документов опять-таки без непосредственного участия человека; компьютер уличного банкомата самостоятельно выдает деньги клиентам без участия человека-

специалиста, при этом обрабатывая огромное количество электронных (цифровых) документов по каждой транзакции.

Более того, сегодня значительное количество документов в течение всего (или почти всего) своего жизненного цикла существуют в иной физической среде и представлены именно в электронном (цифровой) форме. В этом и заключается принципиальная разница электронного (цифрового) и графического (аналогового) документов.

Таким образом, мы полагаем, что электронный (цифровой) документ представляет собой ни что иное, как отображение информационных данных в цифровом формате. Носителем такой информации выступают разнообразные технические устройства и средства ЭВМ. При этом еще раз подчеркнем важную особенность: сам электронный (цифровой) документ возможно непосредственно воспринимать только при помощи специальных технических устройств с соответствующим программным обеспечением. К таким средствам следует относить объекты электронной (цифровой) среды, в которой именно технические (цифровые) устройства, а не человек взаимодействуют и управляют содержимым и действиями по обработке электронного (цифрового) документа: преобразовывает входную информацию в выходную. Человек здесь выступает только как пользователь конечной информации.

При этом необходимо также отметить, что электронный (цифровой) документ существует не только в цифровой среде, но и в виде именованных областей данных на носителе информации - файлах, имеющих фиксированный формат, которые отражают его особенности и характеристику.

Вышесказанное позволяет нам прийти к выводу о том, что электронный (цифровой) документ представляет собой информацию, содержащуюся в файле, созданном для целей хранения и передачи его во времени и пространстве. Эти данные также должны отвечать ряду требований:

- возможность осуществить идентификацию таких данных (проверка достоверности документа);

- возможность аутентификации этих данных (проверка целостности и неизменности содержания документа).

Таким образом, мы приходим к выводу о том, что при использовании электронного (цифрового) документа в качестве доказательства необходимо, исключить сомнения в его подлинности. А это возможно лишь подтверждением такого документа электронной (цифровой) подписью.

Определение и порядок использования электронной подписи установлены в Федеральном законе от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи», направленном на регулирование отношений в области использования электронных подписей при совершении гражданско-правовых сделок, оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций, при совершении иных юридически значимых действий [43]. Целью данного закона является обеспечение правовых условий использования электронной подписи в электронных документах, при соблюдении которых электронная цифровая подпись в электронном документе признается равнозначной собственноручной подписи в документе на бумажном носителе. Закон указывает, что реквизитом электронного документа является электронная подпись, предназначенная для защиты данного электронного документа от подделки.

В результате того, что данный Федеральный закон не раскрывает понятие электронного (цифрового) документа, из смысла его правовых норм можно выделить три важные его составляющие части (компоненты):

- конкретные зафиксированные на материальном носителе данные (информация, сведения);

- сам материальный носитель (изделие или материал), на котором записана документированная информация;

- реквизиты (обязательные сведения), неразрывно связанные с материальным носителем, которые позволяют его идентифицировать.

Причем, каждая из этих компонентов электронного документа является относительно самостоятельным и определяет специфику его правового статуса.

Стоит отметить, что в отечественном законодательстве отсутствуют правовые нормы, направленные на регламентацию отношений, возникающих по поводу использования любых иных аналогов графической (собственноручной) подписи. Между тем, общепринятый в мировом сообществе подход - так называемая «технологическая нейтральность» (комплекс мер законодательного и организационного характера, способствующих развитию информационных технологий), правовое признание любых электронных аналогов графической форме подписи и юридическая сила последних не ограничиваются в зависимости от применяемой технологии. Однако, нашему законодательству до этих новаций еще далеко.

Использование технологии цифровой подписи для электронных подписей значительно различается между странами, которые следуют открытым, технологически нейтральным законам об электронных подписях, включая США, Великобританию, Канаду и Австралию, и странами, которые следуют многоуровневым моделям электронных подписей, которые предпочитают местные стандарты, которые основаны на технологии цифровой подписи, в том числе во многих странах Европейского Союза, Южной Америки и Азии. Кроме того, некоторые отрасли также поддерживают определенные стандарты, основанные на технологии цифровой подписи. В иностранном законодательстве, например, в США, согласно Закону об электронных подписях в мировой и национальной торговле (Electronic Signatures in Global and National Commerce Act), электронной подписью является любой электронный звук, символ или процесс, прикрепленный либо логически связанный с договором либо иным



документом и осуществленный либо примененный лицом с намерением подписать документ [54].

К настоящему времени большинство стран приняли законы и правила, созданные по образцу Соединенных Штатов или Европейского Союза, при этом во многих регионах предпочтение отдается ЕС. модель локально управляемых электронных подписей на основе технологии цифровой подписи. Кроме того, многие компании улучшили соблюдение правил, установленных в их отраслях, что было достигнуто с помощью технологии цифровой подписи. Эти национальные и отраслевые правила постоянно развиваются, ключевым примером является положение об электронной идентификации и доверительных услугах (eIDAS), которое было недавно принято в Европейском союзе.

Таким образом, использование иных аналогов собственноручной подписи, чем тех, применение которых регламентировано законами и иными нормативно-правовыми актами, возможно только по соглашению сторон электронного документооборота. Причем такое соглашение может носить как частноправовой характер, так и публично-правовой характер. Потому что только в таком соглашении возможно закрепить конкретный способ аутентификации электронного сообщения: определить понятие аналога собственноручной подписи и способ проверки его подлинности.

Между тем, многие авторы не без оснований называют электронный документ «актуальным» видом иных доказательств и справедливо полагают, что проблема использования электронного (цифрового) документа имеет как национальный аспект, так и носит межгосударственный характер. Это обстоятельство объясняется тем, Россия принимает участие во многих международных проектах, в частности осуществляет внешнюю торговлю, оборот средств в иностранной валюте и др. Все это приводит к необходимости принимать во внимание новые условия создания и функционирования пока еще нетрадиционного электронного (цифрового) документа.

Кроме того, внутригосударственный характер проблем правового регулирования электронных (цифровых) документов обусловлен стремительным переходом на оказание многих видов государственных и муниципальных услуг в электронной форме на всей территории Российской Федерации. На это направлен Федеральный закон от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» [42]. Сегодня в России внедрение системы информационно-государственного управления - «Электронного правительства», направлено на эффективное обеспечение доступа граждан к предоставляемым сведениям об услугах (функциях), которые осуществляются в электронном виде с использованием сети Интернет и с помощью электронных (цифровых) документов. Целью данной услуги является предоставление заявителям возможности осуществлять взаимодействие с органами власти дистанционно в электронном виде, в том числе обращаться в органы власти и получать результаты такого обращения.

Данные шаги вперед к мировому технологическому прогрессу, безусловно, определяют приоритетное развитие электронных (цифровых) документов. Не смотря на бурное развитие технологий и стремительный переход во многих сферах общественных отношений с бумажной формы документов на электронную (цифровую), в настоящее время в нашей стране не принят соответствующий нормативно правовой акт - Федеральный закон об электронном документе. Как следствие пока еще не внесены соответствующие изменения в федеральные законы, систематизирующие нормы в какой-то отрасли права, в том числе и в КоАП РФ. Хотя очевидно, что современное законодательство должно соответствовать времени и все сферы государственного управления следует переводить на электронный (цифровой) уровень.

Таким образом, в связи развитием и все большим распространением электронного документооборота в современных правоотношениях и отсутствием новых законодательных нормативных актов, которые могли бы

регулировать рассмотрение подобной информации в качестве доказательств по тому или иному делу, многие судьи не принимают подобные документы в качестве доказательств по административному делу, поскольку в настоящее время не существует единого порядка рассмотрения этих документов в качестве доказательств [2, с. 74].

Однако, ситуация в российском законодательстве начинает меняться вместе с законодательными изменениями Арбитражного процессуального кодекса Российской Федерации, в частности ст. 75 предусмотрено, что в качестве письменных доказательств по делу признаются документы, полученные посредством факсимильной, электронной или иной связи, в том числе с использованием информационно-телекоммуникационной сети Интернет, а также документы, подписанные электронной подписью или иным аналогом собственноручной подписи [1].

Существующая судебная практика подтверждает принятие электронных документов к производству, так же, как и письменные варианты.

Так, в судебной практике нередки случаи, когда вышестоящие суды отменяют решения судов первой инстанции в связи с обращением заявителя через официальные сайты госорганов. Так, по административному делу № А26-10762/2010 о привлечении заявителя к административной ответственности Федеральный арбитражный суд Северо-Западного округа Постановлением от 21 октября 2018 г. по делу № А31-12312/2018 отменил определение арбитражного апелляционного суда на том основании, что суд апелляционной инстанции возвратил апелляционную жалобу, поданную в электронном виде посредством заполнения форм, размещенных на официальном сайте арбитражного суда в сети Интернет (<http://my.arbitr.ru>), о чем заявителем было получено электронное уведомление, согласно которому апелляционная жалоба направлена в апелляционный суд. Порядок подачи документов в электронном виде в арбитражные суды предусматривает, что после подачи документов в электронном виде в «личный кабинет»

пользователя приходит уведомление о том, что документы поступили в систему, при этом указывается конкретное время и дата поступления обращения. При рассмотрении вопроса о соблюдении заявителем срока для совершения процессуальных действий именно эта дата должна учитываться (ч. 6 ст. 114 АПК РФ) [1].

Как показывает практика, первые серьезные проблемы появляются уже на стадии присоединения электронных (цифровых) документов к материалам дел. В законе отсутствуют требования относительно формы и формата предоставления любых фактических данных в электронной форме по порядку исследования форм предоставления электронных документов и по порядку приобщения их к судебному делу. Зачастую электронные документы должны представляться в суд не на техническом, а на бумажном носителе, т.е. преобразованными в печатный вид, позволяющий визуальное исследование и обсудить доказательство.

В этой связи возникает ситуация, когда электронные доказательства не рассматриваются судом как прямые доказательства, поскольку суд технически не подготовлен или в судах есть давно существующий бумажный документооборот.

Суды как прямое доказательство оценивают электронный (цифровой) документ в следующих случаях:

- если электронный (цифровой) документ несет в себе текстовую или графическую информацию и предоставляется на бумажном носителе его копия;
- если оспаривается электронная подпись на электронном документе и предоставляется заключение эксперта.

Например, сегодня большое количество граждан не оплачивает в установленные сроки штрафы за нарушения ПДД, дожидаясь постановления об исполнительном производстве. Согласно ст. 24 Федерального закона от 2 октября 2007 г. № 229-ФЗ «Об исполнительном производстве» должник может быть уведомлен телеграммой, факсом, электронными видами связи. В

случае последнего варианта, это может sms, ICQ, web-камера, сообщения в социальных сетях и т.д. Однако, в случае оспаривания должником данного вида уведомления, особенно если оно является единственным прямым доказательством надлежащего уведомления должника, очевиден ряд проблем, так, например, персонифицировать получателя уведомления и доказать получение данного уведомления крайне сложно.

Безусловно, простого перечисления в законе средств уведомления недостаточно, нужна четкая процедура, регламентирующая достоверность доказательства, полученного с помощью электронной связи.

Что касается использования электронных документов в качестве доказательств по делам об административных правонарушениях, то как источники доказательств они могут быть использованы при соответствии следующим существенным признакам:

- если электронный документ имеет доказательственное значение по административному делу, т.е. содержит сведения, подлежащие установлению. При этом для суда доказательственное значение имеет сама информация, содержащаяся на материальном носителе, а не сам носитель.

- если электронный документ обладает определенными реквизитами, позволяющими его идентифицировать, тем самым обеспечивается его юридическая сила. К реквизитам, например, относятся: дата и время создания данных; сведения о лицах, которые используют технические средства; адрес электронной почты; данные получателя электронных данных и т.д.

Однако, по нашему мнению, включение в содержание понятия электронного документа только информации, которую можно аутентифицировать и/или идентифицировать, приводит к выделению в качестве существенного признака фактических данных, получаемых с помощью электронного документа, как судебных доказательств признака достоверности. В этом случае участники процесса могут попасть в ситуацию, при которой вплоть до вынесения судебного решения им не будет известно,

доказательство перед ними или нет, поскольку достоверность фактических данных заранее определить невозможно;

- если электронный документ доступен восприятию органами чувств человека. Иными словами, данные содержащиеся в данном электронном (цифровом) документе можно считать или преобразовать в форму, которая пригодна для обычного восприятия и дальнейшего хранения в материалах дела. Для преобразования информации используют технические средства (ЭВМ, принтер и т.д.);

- если электронный (цифровой) документ получен с соблюдением требований собирания информации.

Соблюдение вышеуказанных признаков при использовании электронного документа в качестве доказательств, несомненно, окажет помощь при рассмотрении данных доказательств в производстве по делам об административных правонарушениях.

Институт использования информации в электронной форме (содержащейся на электронных носителях), по нашему мнению, может быть обеспечен и в том случае если такая информация заверяется нотариусами.

Представляется, что процедура обеспечения электронного доказательства будет выглядеть так:

- лицо, нуждающееся в обеспечении доказательств, должно направить нотариусу запрос, где указывает сведения, которые необходимо обеспечить (интернет-страницу, файл и т.д.);

- нотариус, предварительно распечатав текст электронного документа, осматривает и описывает содержащуюся в нем информацию;

- распечатка электронного документа, протокол его осмотра и электронный носитель информации представляется в суд.

Мы полагаем, что данная схема лучшим образом защищает информацию от возможных злоупотреблений со стороны участников процесса.

Таким образом, поводя итоги вышесказанному, отметим, что современные проблемы восприятия электронного (цифрового) документа в качестве доказательства по гражданским и административным делам представляется основной, и разрешать ее, следует не только фактически, но в правовом аспекте.

Это позволит исключить возможность неоднозначного подхода (трактовки) к электронным документам с цифровой подписью как к доказательствам, а суды не будут иметь возможности произвольно признавать или не признавать такие документы в качестве доказательств. Очевидно, что в таких условиях необходимо в кратчайшие сроки решить вопрос правовой природы электронных доказательств.

Выводы по главе:

На основании проведенного исследования в данной главе мы сделали следующие выводы:

Национальное законодательство не разработало общепринятого определения термина «электронный документ» или «цифровой документ». Это обстоятельство, по нашему мнению, создает определенные проблемы в правовом регулировании соответствующих общественных отношений.

Как показывает практика, первые серьезные проблемы появляются уже на стадии присоединения электронных (цифровых) документов к материалам дел. В законе отсутствуют требования относительно формы и формата предоставления любых фактических данных в электронной форме по порядку исследования форм предоставления электронных документов и по порядку приобщения их к судебному делу. Зачастую электронные документы должны представляться в суд не на техническом, а на бумажном носителе, т.е. преобразованными в печатный вид, позволяющий визуальнo исследовать и обсудить доказательство.

Полагаем, что эффективность результатов и оказания государственных и муниципальных услуг в электронном виде во многом зависит от предоставления реальной возможности физическим и юридическим лицам

использовать электронный документооборот и электронную (цифровую) подпись наравне с «традиционными» документами. Необходимо свести до минимума процедуру подтверждения бумажных копий электронных (цифровых) документов, а в перспективе лучше и вовсе от нее отказаться.

Требуется принять Федеральный Закон обеспечивающий легитимность электронного (цифрового) документа и позволяющий снять ограничения к его применению в судах как источник доказательств.

Предлагается название такого нормативного правового акта - Закон «Об электронном (цифровом) документе» или Закон «Об общих правилах организации оборота электронных (цифровых) документов в Российской Федерации».

Предлагается понимать под электронным (цифровым) документом сведения, представленные в электронно-цифровой форме об обстоятельствах, подлежащих установлению по делу.

Предлагается внести изменения в КоАП РФ и дополнить его ст. 26.7.1, в которой раскрыть дефиницию понятия «электронный документ в качестве доказательства».

Достоверность электронного документа, скрепленного цифровой подписью, как источника доказательств может быть подтверждена электронной подписью.

Легитимности электронного (цифрового) документа в качестве доказательства по делу, по нашему мнению, будет способствовать создание и реализация четко разработанной схемы предоставления электронных доказательств в суд. Действенным механизмом реализации такой процедуры, по нашему мнению, является обращение к нотариусу как до начала судебного разбирательства, так и в ходе него.

Итак, исследование отдельных проблем правового регулирования использования цифровых подписей в нашей стране нами завершено.



## Заключение

Подводя итог магистерского исследования, можно с уверенностью сказать, что изучение вопросов законодательное регулирование использования цифровых подписей в РФ имеет большое значение как для правовое науки, так и для практики.

Опираясь на поставленные задачи, удалось рассмотреть сущность основных компонентов данной темы. В процессе написания работы были достигнуты такие задачи, как:

- проанализировано понятие электронного документа;
- изучены сущность и функции «цифровой» подписи;
- выявлены особенности нормативно-правового регулирования использования «цифровой» подписи;
- проанализированы особенности использования «цифровой» подписи;
- исследованы проблемы определения подлинности «цифровых» подписей;
- показаны проблемы исследования электронных документов, подписанных «цифровыми» подписями.

На основании проведенного исследования автором были сделаны следующие научно-исследовательские выводы:

Существует острая необходимость во внедрении определенной категории изменений в действующий ГПК РФ с целью закрепления дефиниции электронного документа в качестве доказательства, фиксирования перечня правовых гарантий его употребления, гарантий достоверности. Кроме того, было бы целесообразным регламентировать алгоритм изучения таковых источников информации в рамках самого судебного процесса, подготовить перечень правовых критериев к форме электронного вида документов.

Так, применение электронных доказательств в рамках осуществления гражданского судопроизводства – весьма актуальный вопрос в сфере развития института доказательств и доказывания как такового. Очевидно, что электронные доказательства будут развиваться в ногу с научно-техническим прогрессом, что дает повод предположить их перспективное обособление как самостоятельного вида доказательств.

«Цифровая» подпись является обязательным для электронного документа реквизитом.

«Цифровые» подписи создаются при помощи современных криптографических систем, позволяющих использовать закрытые ключи, с помощью которых владелец подписи получает к ней доступ. Отметим, что использование «цифровых» подписей возможно только при наличии специальных компьютерных технологий – мы полагаем, что это является ключевой отличительной чертой «цифровых» подписей от аналогов собственноручных подписей.

«Цифровая» подпись выступает в качестве набора специальных компьютерных символов, полученных в результате использования современных криптографических технологий, позволяющая в свою очередь обеспечить неизменность и целостность любой информации в электронном документе.

«Цифровая» подпись обладает двумя важнейшими свойствами:

- подпись непрерывно связана с конкретным электронным документом;
- подпись может быть поставлена только конкретным лицом, владеющим секретным кодом (ключом).

Анализ положений федерального законодательства позволяет выделить следующие критерии (условия) при которых «цифровая» подпись будет равнозначной подписи на бумажном носителе:

- сертификат ключа (кода) от подписи не утратил силу на момент подписания соответствующего электронного документа;

- подлинность «цифровой» подписи в соответствующем документе была подтверждена;

- «цифровая» подпись соответствует сведениям, которые указаны в сертификате кода (ключа). Мы полагаем, что презумпция авторства в данном случае, обуславливает гарантию юридической силы подписанного такой подписью документа.

Полагаем, что следует предусмотреть в отечественном законодательстве правовые обеспечительные меры (гарантии), которые могли бы гарантировать достоверность предоставляемых информационных данных. Этому, по нашему мнению, могут способствовать достижения научно-технического прогресса и, в частности в сфере современных цифровых научно-технических средств.

Кроме того, полагаем, что необходимо предусмотреть более жесткие меры юридической ответственности к тем лицам, которые фальсифицируют подобные информационные данные. Возможно это потребует внесение соответствующих изменений в уголовное и административно-деликтное законодательство России.

Также, по нашему мнению, следует разработать процессуальный порядок проверки подлинности цифровой подписи в электронных документах в рамках судебных заседаний.

Принимаемые меры будут способствовать повышению результативности и эффективности применения электронного документооборота в различных отраслях отечественного права, существенно снизит уровень подлогов и махинаций. Только в этом случае электронный документ с цифровой подписью будет эффективно выступать по конкретному делу в качестве доказательств наравне с «традиционным».

Национальное законодательство не разработало общепринятого определения термина «электронный документ» или «цифровой документ». Это обстоятельство, по нашему мнению, создает определенные проблемы в правовом регулировании соответствующих общественных отношений.

Предлагается понимать под электронным (цифровым) документом сведения, представленные в электронно-цифровой форме об обстоятельствах, подлежащих установлению по делу. Полагаем, что эффективность результатов и оказания государственных и муниципальных услуг в электронном виде во многом зависит от предоставления реальной возможности физическим и юридическим лицам использовать электронный документооборот и электронную (цифровую) подпись наравне с «традиционными» документами.

Легитимности электронного (цифрового) документа в качестве доказательства по делу, по нашему мнению, будет способствовать создание и реализация четко разработанной схемы предоставления электронных доказательств в суд. Действенным механизмом реализации такой процедуры, по нашему мнению, является обращение к нотариусу как до начала судебного разбирательства, так и в ходе него.

Анализ актуальной юридической практики свидетельствует о необходимости принятия Федерального Закона, обеспечивающего легитимность электронного (цифрового) документа и позволяющий снять ограничения к его применению в судах как источник доказательств. Нами предлагается название такого нормативного правового акта - Закон «Об электронном (цифровом) документе» или Закон «Об общих правилах организации оборота электронных (цифровых) документов в Российской Федерации».

Полагаем, что следует предусмотреть в отечественном законодательстве правовые обеспечительные меры (гарантии), которые могли бы гарантировать достоверность предоставляемых информационных данных. Этому, по нашему мнению, могут способствовать достижения научно-технического прогресса и, в частности в сфере современных цифровых научно-технических средств. Кроме того, следует предусмотреть более жесткие меры юридической ответственности к тем лицам, которые фальсифицируют подобные информационные данные.

Необходимо разработать процессуальный порядок проверки подлинности цифровой подписи в электронных документах в рамках судебных заседаний. Предлагается внести изменения в КоАП РФ и дополнить его ст. 26.7.1 в следующей редакции:

«Электронный документ в качестве доказательства в судебном процессе - это информация, содержащаяся в электронной (цифровой) форме об обстоятельствах, которые необходимо расследовать, имеющих значение для дела. Такая информация содержится в файле на любом материальном носителе, созданном с целью хранения ее и передачи во времени и пространстве».

По нашему мнению, применение именно инновационных методик, цифровых технологий, позволяющих обеспечить надежную защиту механизма применения электронной подписи, а также укрепление законодательства в сфере электронной цифровой подписи, будет и дальше способствовать развитию цифровой экономики.

Нормативная составляющая, а также организационные механизмы применения электронной цифровой подписи в электронном документообороте, на наш взгляд, требуют развития на постоянной основе.

Хотелось бы также отметить, что совершенствование отечественной нормативно-правовой базы и практики применения электронной цифровой подписи невозможно без консолидации усилий как представителей юридической науки, так и технических специалистов.

## Список используемой литературы и используемых источников

1. Арбитражный процессуальный кодекс Российской Федерации от 24.07.2002 № 95-ФЗ (ред. от 30.12.2021) (с изм. и доп., вступ. в силу с 10.01.2022) // СПС К+ (дата обращения 12.05.2022 г.).
2. Балашова А. // Статья: E-mail как доказательство. Миф или реальность? // «Административное право», 2011. № 2. С.73-89.
3. Баранов И.Н., Бондарев Н.Д. Электронный документ как доказательство в гражданском процессе // Право и практика. 2021. №2. URL: <https://cyberleninka.ru/article/n/elektronnyu-dokument-kak-dokazatelstvo-v-grazhdanskom-protsesse> (дата обращения: 09.06.2022).
4. Билалова Д. Г.-К., Магомедов Н.Н. Понятие электронной цифровой подписи // Инновационная наука. 2022. №2-1. С. 6-9.
5. Гарибян А. Электронная цифровая подпись: правовые аспекты // Российская юстиция. 1996. № 11. С. 12-13.
6. Гончаров Е.И., Шатковская Т.В. Проблемы применения цифровой подписи в электронном документообороте России // Северо-Кавказский юридический вестник. 2020. №2. С. 97-103.
7. Горелов М.В. Современные источники информации как доказательства в гражданском процессе // Информационное право. 2005. № 3. С.27-29.
8. ГОСТ 34.10-2018. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.
9. ГОСТ Р 54989-2012 (ISO/TR 18492:2005). Обеспечение долговременной сохранности электронных документов.
10. Государственная Дума Федерального Собрания Российской Федерации. Комитет по государственному строительству и законодательству: официальный сайт. [Электронный ресурс] // URL: <http://komitet2-10>.

km.duma.gov.ru/novosti\_Komiteta/item/19122542/10.km.duma.gov.ru/novosti\_Komiteta/item/19122542 (дата обращения: 18.05.2022 г.).

11. Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51-ФЗ (03.07.2016) (с изм. и доп., вступ. в силу с 01.09.2016) // Российская газета. № 238-239. 08.12.1994.

12. Ермолаева А.В. Электронный документ и электронная подпись: проблемы регламентации и практики применения // Региональная власть, местное самоуправление и гражданское общество: механизмы взаимодействия: сб. научных трудов. Изд-во Поволжского института управления им. П.А. Столыпина, 2017. С 77-80.

13. Ефремова В.Е. Особенности использования электронной подписи при заключении гражданско-правовых договоров (сделок): проблемы и перспективы // Вопросы российской юстиции. 2022. №19. С. 192-197.

14. Защита нематериальных благ и неимущественных прав граждан и юридических лиц в гражданском праве России [Текст] : монография / Е. Г. Дюбко. – М.: Дашков и К°, 2014. - 165 с.

15. Интеллектуальная собственность (исключительные права): учеб. пособие / [Коршунов Н. М. и др.] ; под ред. Н. М. Коршунова. – М.: Eksmo Education : Эксмо, 2006 (Ульяновск : Ульяновский Дом печати). - 572 с.

16. ИСО/МЭК 14888-3:2018. Информационная технология. Методы и средства обеспечения безопасности. Цифровые подписи с приложением. Часть 3. Механизмы на основе дискретного логарифма.

17. Квалификация преступлений, совершенных с документами : монография / Р. А. Сабитов, Е. Ю. Сабитова ; Челябинский юридический ин-т М-ва внутренних дел Российской Федерации. - Челябинск : Челябинский юридический ин-т МВД России, 2007. - 252 с.

18. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (ред. от 16.04.2022, с изм. от 17.05.2022) (с изм. и доп., вступ. в силу с 27.04.2022) // СПС К+ (дата обращения 12.05.2022 г.).

19. Комментарий к Федеральному закону от 10 января 2002 года № 1-ФЗ «Об электронной цифровой подписи» (постатейный) / Е. В. Ильиных, М. Н. Козлова. - М. : Юстицинформ, 2005. - 80 с.

20. Кузнецов П. У. Информационные технологии в юридической деятельности: учебник для вузов / П. У. Кузнецов; под общей редакцией П. У. Кузнецова. - 3-е изд., перераб. И доп. - Москва: Издательство Юрайт, 2022. - 325 с.

21. Основы административного механизма защиты прав на объекты интеллектуальной собственности: трансграничный аспект [Текст]: монография / С. А. Агамагомедова ; М-во образования и науки РФ, Федеральное гос. бюджетное образовательное учреждение высш. проф. образования "Пензенский гос. ун-т" (ПГУ). - Пенза : Изд-во ПГУ, 2013. - 401.

22. Пастухова С.С. Электронная подпись в гражданском процессе // Вестник СГЮА. 2022. №1 (144). С. 148-154.

23. Погуляев В.В. Правонарушения в сети Интернет // ЭЖ-Юрист. 2010. № 12. С.199-203.

24. Погуляев В.В. Средства доказывания по делам, связанным с Интернетом // Хозяйство и право. - М., 2004, № 7. С. 69-71

25. Постановление Правительства РФ от 22.09.2009 № 754 «Об утверждении Положения о системе межведомственного электронного документооборота» // СПС К+ (дата обращения 12.05.2022).

26. Постановление Правительства РФ от 25 декабря 2014 г. № 1494 «Об утверждении Правил обмена документами в электронном виде при организации информационного взаимодействия».



27. Постановление Правительства РФ от 25.01.2013 № 33 «Об использовании простой электронной подписи при оказании государственных и муниципальных услуг» // СПС К+ (дата обращения 12.05.2022).

28. Постановление Правительства РФ от 25.06.2012 № 634 «О видах электронной подписи, использование которых допускается при обращении за получением государственных или муниципальных услуг» // СПС К+ (дата обращения 12.05.2022) // СПС К+ (дата обращения 12.05.2022).

29. Постановлением Правительства РФ от 25.06.2012 № 634 «Об утверждении Правил определения видов электронной подписи, использование которых допускается при обращении за получением государственных и муниципальных услуг» // СПС К+ (дата обращения 12.05.2022).

30. Прохоров А.Г. Принцип допустимости средств доказывания в советском гражданском процессуальном праве: автореф. дис. ... канд. юрид. наук. - Свердловск. 1979. – 20 с.

31. Пучинский В. Оценка доказательств в российском гражданском и арбитражном процессуальном праве // Хозяйство и право. 2019. № 6. С. 32-44.

32. Пучинский В.К. Понятие, значение и классификация судебных доказательств в российском процессуальном праве // Законодательство. №12. 2020. С. 28-34.

33. Ральникова Н.С. Статические методы биометрической идентификации личности // Перспективы развития информационных технологий. 2015. №27. С. 140-144.

34. Решетникова, И. В. Доказывание в гражданском процессе : учебно-практическое пособие для вузов / И. В. Решетникова. - 7-е изд., перераб. и доп. – М.: Издательство Юрайт, 2022. - 388 с.

35. Рогожин С.П. Процессуальные особенности доказывания по делам, возникающим из таможенных правоотношений: монография. - М.: Волтерс Клувер, 2019. 214 с.

36. Родичев А. Ю. Электронная цифровая подпись и законодательство РФ // Вестн. Сам. гос. техн. ун-та. Сер.: Физ.-мат. науки. 2003. №19. С.190-193.
37. Серго А. Электронный документооборот // Российская юстиция. - 2013. № 5. С. 22-26.
38. Соловяненко Н.И. Актуальные тенденции правового регулирования и защиты прав в сфере цифрового взаимодействия субъектов предпринимательской деятельности // Право и практика. 2022. №1. С. 114-119.
39. Судебная экспертиза в гражданском, арбитражном, административном и уголовном процессе [Текст]: [монография] / Е. Р. Россинская; Российский федеральный центр судебной экспертизы при М-ве юстиции Российской Федерации. - 3-е изд., доп. - М.: Норма : ИНФРА-М, 2014. - 735 с.
40. Судебные доказательства : [Монография] / М.К. Треушников. - 3. изд., испр. и доп. - М. : Издат. дом "Городец", 2004 (1-я Обр. тип.). - 268 с.
41. Федеральный закон «О государственной регистрации недвижимости» от 13.07.2015 № 218-ФЗ // СПС К+ (дата обращения 12.05.2022 г.): справочно-правовая система.
42. Федеральный закон «Об организации предоставления государственных и муниципальных услуг» от 27.07.2010 № 210-ФЗ (последняя редакция) // СПС К+ (дата обращения 12.05.2022 г.).
43. Федеральный закон от 06.04.2011 № 63-ФЗ (ред. от 23.06.2016) «Об электронной подписи» // «Российская газета». № 75. 08.04.2011.
44. Федеральный закон от 07.07.2003 № 126-ФЗ (ред. от 30.12.2021) «О связи» (с изм. и доп., вступ. в силу с 01.05.2022) // СПС К+ (дата обращения 12.05.2022).
45. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 30.12.2021) «Об информации, информационных технологиях и о защите информации» (с изм. и доп., вступ. в силу с 01.01.2022) // СПС К+ (дата обращения 12.05.2022).

46. Фетисов К.А. Электронная цифровая подпись и законодательство // Вестник РГГУ. Серия «Экономика. Управление. Право». 2008. №5. С. 289-296.

47. Хеликов Р.О. Правовой режим электронного документа: вопросы использования электронной цифровой подписи: автореф. дис. ... канд. юрид. наук. - Казань. 2016. - 28 с.

48. Шварц М. З. Обеспечение доказательств и некоторые общие вопросы доказывания в арбитражном процессе // Доказательства в арбитражном процессе: сб. - м., 2004. С. 118-130.

49. Щепеткова А.В. О правовой регламентации применения электронной подписи / Щепеткова А.В., Шокорова Н.Н. // Информационные технологии в науке и образовании. Проблемы и перспективы. : сб. ст. по материалам VI Всерос. межвуз. науч-практ. конф. (г.Пенза, 13 марта 2019 г.) /под ред. Л.Р. Фионовой. – Пенза: Изд-во ПГУ, 2019, с. 393-395.

50. Юридически значимый ЭДО // Сайт «СКБ Контур» [https://kontur.ru/diadoc/spravka/272-yuridicheskaya\\_sila\\_elektronnoho\\_dokumenta](https://kontur.ru/diadoc/spravka/272-yuridicheskaya_sila_elektronnoho_dokumenta) (дата обращения: 01.06.2022).

51. Ященко И.И. Понятие, признаки и функции электронного документа в российском законодательстве, науке и уголовно-процессуальной деятельности // Вестник Восточно-Сибирского института МВД России. 2022. №1 (100). С.174-186.

52. Bartok, Sandor P. and Peter Mate Erdesi. 2018. "Can an extended biometric electronic signature be used in public administration?". Central and Eastern Europe EDem and eGov Days 325 (February):455-62.

53. Dumortier, Jos. "Legal Status of Qualified Electronic Signatures in Europe." *ISSE* (2004). // URL: <http://www.icri.be/publications> (дата обращения: 11.05.2022 г.).

54. Electronic Signatures in Global and national Commerce Act, Sec. 7006, article (5) // URL: <http://uscode.house.gov/download/pls/15C96.txt>. (дата обращения: 11.05.2022 г.).

55. Fang, W., Chen, W., Zhang, W. et al. (2020) Digital signature scheme for information non-repudiation in blockchain: a state of the art review. J Wireless Com network 2020, 56.

56. Maté, Peter I. and Erdősi. “Comparative analysis and measurement of Electronic 23ignatures created by notaries in Europe.” (2019).

57. Mihir Bellare & Phillip Rogaway. Introduction to Modern Cryptography, Chapter 12 Digital Signatures, p. 237 (Dec. 27, 2016), [http://digidownload.libero.it/persiahp/crittografia/2005\\_Introduction\\_to\\_Modern\\_Cryptography.pdf](http://digidownload.libero.it/persiahp/crittografia/2005_Introduction_to_Modern_Cryptography.pdf). (дата обращения: 11.05.2022 г.).

## Приложение А Элементы ЭЦП

		
<b>Закрытый ключ</b>	<b>Программа-криптопровайдер</b>	<b>Сертификат</b>
<p>Это уникальный код, необходимый для создания уникальной подписи. Его знает только владелец. Закрытый ключ гарантирует защиту ЭЦП от фальсификации и взломов</p>	<p>Специализированная программа, которая необходима для работы с электронной подписью в ОС Windows</p>	<p>Документ, который подтверждает принадлежность подписи конкретному человеку. В ней содержится открытый ключ, который позволяет получателю проверить заверенный файл</p>

Рисунок А.1 – Элементы ЭЦП

Приложение Б  
Алгоритм ЭЦП

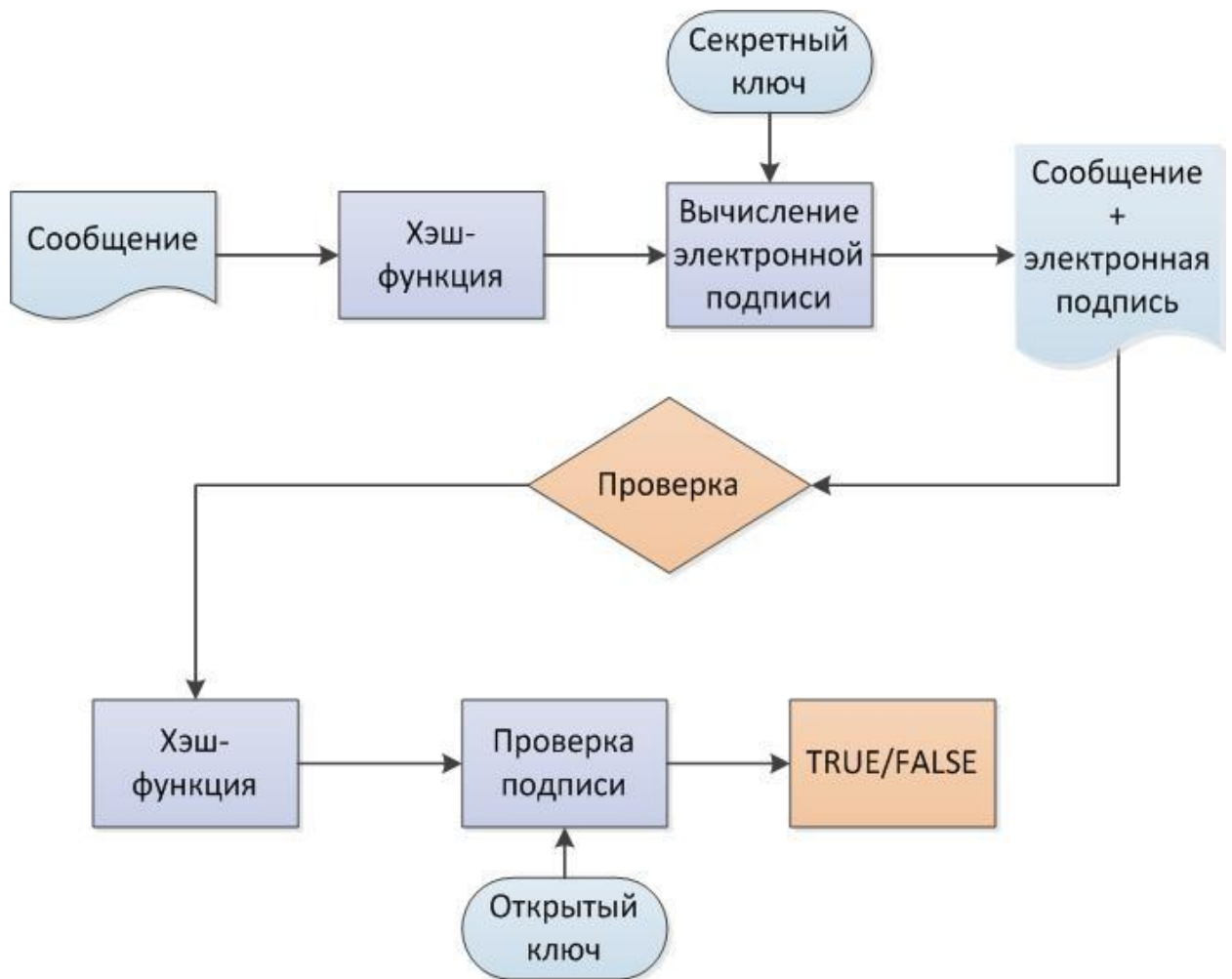


Рисунок Б.1 – Алгоритм ЭЦП

**Приложение В**  
**Виды ЭЦП**

	Простая	Неквалифицированная	Квалифицированная
<b>Внутренний и внешний документооборот</b>			
<b>Арбитражный суд</b>			
<b>Госуслуги</b>			
<b>Контролирующие органы (ФНС, ПФР, ФСС)</b>			
<b>Электронные торги</b>		 (Может приниматься на ряде ЭТП)	

Рисунок В.1 – Виды ЭЦП