ПУБЛИЧНО-ПРАВОВЫЕ (ГОСУДАРСТВЕННО-ПРАВОВЫЕ) НАУКИ / PUBLIC LAW (STATE LAW) SCIENCES

DOI: https://doi.org/10.23670/IRJ.2023.128.7

ПЕРСПЕКТИВЫ, ДОСТОИНСТВА И НЕДОСТАТКИ ЭЛЕКТРОННОЙ ПОДПИСИ

Научная статья

Щука И.О.[1], Нестеренко И.С.[2], Нестеренко Г.А.[3,*]
[2] ORCID : 0000-0003-4749-010X;
[3] ORCID : 0000-0003-1528-4627;
[1] Сибирский институт бизнеса и информационных технологий, Омск, Российская Федерация
[2, 3] Омский государственный технический университет, Омск, Российская Федерация

* Корреспондирующий автор (nga112001[at]list.ru)

Аннотация

На сегодняшний день происходит повсеместное внедрение электронного делопроизводства. В связи с этим применение электронной подписи становится весьма актуальным и имеет огромную эффективность. Однако следует учитывать, что, кроме преимуществ данной цифровой технологии, существуют и некоторые недостатки, нуждающиеся в устранении. Описаны преимущества электронной подписи, которые заключаются в повышении мобильности документооборота. Рассмотрены недостатки электронной подписи, которые заключаются в возможности несанкционированного доступа к ней и ее неправомерного использования. В работе даны рекомендации по практическому использованию и защите электронной подписи при ее использовании в работе с документацией.

Ключевые слова: информационно-коммуникационные технологии, подпись, цифровые технологии, электронный документооборот, электронная подпись, ключ, формирование электронной подписи, проверка электронной подписи, сертификат.

PROSPECTS, ADVANTAGES AND DISADVANTAGES OF ELECTRONIC SIGNATURE

Research article

Shchuka I.O.[1], Nesterenko I.S.[2], Nesterenko G.A.[3,*]
[2] ORCID : 0000-0003-4749-010X;
[3] ORCID : 0000-0003-1528-4627;
[1] Siberian Institute of Business and Information Technologies, Omsk, Russian Federation
[2, 3] Omsk State Technical University, Omsk, Russian Federation

* Corresponding author (nga112001[at]list.ru)

Abstract

Nowadays, electronic record management is being introduced everywhere. In this regard, the use of electronic signature becomes very relevant and is of great efficiency. However, one should keep in mind that apart from the advantages of this digital technology, there are also some drawbacks that need to be addressed. The advantages of electronic signature are described, which consist in increasing document flow mobility. The disadvantages of electronic signature are analysed, which lie in the possibility of unauthorized access to it and its illegal use. The article gives recommendations on the practical use and protection of electronic signature when using it to work with documents.

Keywords: information and communication technologies, signature, digital technologies, electronic document management, electronic signature, key, electronic signature formation, electronic signature verification, certificate.

Введение

Современный, высокотехнологичный и динамично развивающийся мир всецело зависит от информационно-коммуникационных технологий. В свою очередь, благодаря данным технологиям, широкую популярность и востребованность получил электронный документооборот. Возможность оформить любой правовой акт независимо от территориального расположения экономит достаточно большое количество времени и средств. Сейчас совсем не обязательно личное присутствие при совершении любой сделки и заключении договора. С появлением электронной подписи, возникло огромное преимущество использования данной технологии, вместе с тем имеют место и некоторые недостатки.

Актуальность

Повсеместное внедрение технологии электронной подписи не только среди государственных структур, частных предприятий, но и в деятельности рядовых граждан.

Цели, задачи

Заключается в исследовании возможностей, преимуществ и недостатков, слабых и сильных сторон технологии электронной подписи.

Методы исследования

В данной статье применялись метод объективности, а также системного анализа.

Научная новизна

Состоит в исследовании проблемы законодательного и технического обеспечения технологии с научной и правовой точки зрения.

Исследование вопроса

Во все времена любой договор, составленный в письменной форме, удостоверялся личной подписью. Термин «Подпись», согласно словарю С.И. Ожегова это означает собственноручное написание своей фамилии [1].

С точки зрения законодательства «Подпись» является добровольным волеизъявлением человека, необходимым условием заключить гражданско-правовой акт, неким знаком, удостоверяющим его, с помощью которого возможно провести идентификацию и аутентификацию лица, поставившего подпись под документом [2].

Если подпись рассматривать с технической точки исполнения, то это некое графическое изображение, состоящее из букв, посредством которых слагается имя, отчество и фамилия, всевозможных штрихов, иногда различных графических изображений, в конце может стоять росчерк и дополнительные элементы её конструкции [3, С. 44].

Постоянное и стремительное преобразование деятельности человека привело к интенсивному внедрению в его жизнь информационно-коммуникационных технологий и упрощению его быта. Теперь нет необходимости в личном присутствии при подписании различных правовых документов. Достаточно иметь электронную подпись.

Сущность понятия электронной подписи определяется в п. 1 ст. 2 Федерального закона № 63-ФЗ от 06.04.2011 «Об электронной подписи» и заключается в следующем: информация, которая содержится в электронном формате и присоединенная к иной информации в электронном формате (информация, которая подписывается) или другим способом связанная с информацией такого вида используемая для идентификации лица, ставящего подпись под данной информацией [4].

В данном законодательном акте разрешается получение электронной подписи не только физическому лицу, но и юридическому, закрепляется система аккредитации удостоверяющих центров и т.д.

В 2020 году вступил в силу очередной закон, связанный с электронной подписью в котором говорится о возможности использования данной подписи как средства, при помощи которого удостоверяется намерение стороны, оформить сделку при помощи обмена информации в электронном виде [5].

На сегодняшний день электронная подпись имеет широкое применение в различных сферах деятельности человека. К ним следует отнести электронный документооборот внешнего и внутреннего плана, документооборот непосредственно с физическими лицами, деятельность ФСС, ПФР, ФНС, арбитражного суда, Госуслуги, платежную систему, ведение бухгалтерской документации, электронную торговлю и цифровые торги, бизнес [6].

Основными задачами электронной подписи является следующее:

- Контролирование целостности и неизменности электронного документа.
- Обеспечение защиты данных и невозможность подделки документа и внесения незаконных изменений.
- Поддержка авторских прав владельца электронной подписи.

Создание электронной (криптографической) подписи подразделяется на два этапа. Первый – формирование подписи, в этом процессе используется закрытый ключ. И второй – проверка самой подписи, в этом процессе используется открытый ключ.

Законом предусмотрено три возможных вида электронной подписи:

- простая электронная подпись;
- усиленная неквалифицированная электронная подпись;
- усиленная квалифицированная электронная подпись.

Рассмотрим все три вида более подробно [7]. Простой электронной подписью следует считать электронную подпись, при помощи применения кодов, паролей и других средств возможно подтверждение факта формирования электронной подписи конкретным лицом. Эта подпись является наиболее популярной: востребована для создания личного кабинета в Интернет-магазинах, на всевозможных веб-сайтах, в различных социальных сетях. Формирование простой электронной подписи происходит с помощью логина и обязательного пароля в личном кабинете. Идентификация пользователя происходит при получении пароля по SMS на номер телефона или на электронный почтовый ящик.

В законе «Об электронной подписи», сказано, что документ будет считаться подписанным при соблюдении определенных условий. Одно из их это содержание простой электронной подписи в самом электронном документе. Применение ключа простой электронной подписи должно регламентироваться правилами, которые установил оператор информационной системы. В самом электронном документе обязательно должна содержаться информация, которая указывает на лицо, от чьего имени создается и (или) отправляется электронный документ.

Следующий вид подписи – неквалифицированная электронная подпись, она позволяет определять лицо, которое подписывает электронный документ. При помощи этой подписи и обнаруживается факт всех изменений, внесенных в документ после окончания процесса подписания. Эта подпись получается посредством криптографических преобразований информации с применением ключа самой электронной подписи. Самым важным различием неквалифицированной подписи по сравнению с простой электронной состоит в не только идентификации определенного лица, но и в выполнении защитной функции. Благодаря неквалифицированной подписи предоставляются гарантии того, что содержание документа останется неизмененным. Часто использование такой подписи применяется во время оформления налоговых деклараций и отправлении их в налоговые службы, при обращении налогоплательщиков в личный кабинет в ФНС РФ.

И третья подпись – усиленная квалифицированная электронная подпись, она содержит все признаки усиленной неквалифицированной подписи, вместе с тем у нее имеется ключ проверки электронной подписи, который указывается в квалифицированном сертификате. Чтобы создать и проверить квалифицированную электронную подпись используют существующие средства электронной подписи, которые подтверждают соответствие требованиям, согласно Федеральному закону «Об электронной подписи».

Усиленная квалифицированная электронная подпись, создаваемая и применяемая строго под контролем государства, придает высокий правовой статус самому электронному документу, который подписан ею. Данный

электронный документ равнозначен документу в бумажном виде, на котором стоит собственноручная подпись, заверенная печатью [8].

Обсуждение

В законодательстве России имеет место понятие презумпции действительности квалифицированной электронной подписи. Данную подпись возможно оспорить только в суде.

Как любая цифровая технология, электронная подпись нуждается в защите от незаконного проникновения и использования данных.

Инструментом сохранения конфиденциальности, средством противодействия несанкционированного копирования и распространения интеллектуальной собственности, является криптография, ее основополагающими требованиями стал «Принцип ранопрочности». Он заключается в том, что при разделении защиты на звенья, все они должны быть одинаково стойки к взлому.

Основные принципы применения алгоритмов криптографии:

1. Обеспечение защиты данных, которые могут передаваться даже в ненадежной среде.

2. Применение шифрования, с целью защитить файлы, в которых содержатся ценные сведения, для максимального снижения вероятности проникновения посторонних лиц.

3. Использование криптографии как для того, чтобы обеспечить секретность, так и для того, чтобы сохранить целостность данных [9].

Для обеспечения электронной цифровой подписи на электронных документах, для обеспечения их шифрования, в дальнейшем расшифрования, применяются следующие криптопрограммы:

«Карма» – основным назначением данной системы является бесперебойное обеспечение возможности применять электронную подпись и шифрование, не только при оформлении частных, но и в юридических электронных документах.

«ViPNet CSP ViPNet CSP» – обеспечивает генерацию как закрытых, так и открытых ключей электронной подписи и возможности совершать шифрование согласно алгоритму ГОСТ Р 34.10 – 2001, вычислять хеш-функции согласно алгоритму ГОСТ Р 34.11-94, вычислять и проверять электронные подписи согласно алгоритму ГОСТ Р 34.10-2001.

«КриптоАРМ» – обеспечивает шифровку и дешифровку данных, создание и проверку электронной подписи [10].

Схема электронной подписи, может быть двух типов, с восстановлением и без возможности восстановить сообщение. Схемой предусматривается три процесса [11].

Первый – генерация ключей ЭП. Сущность этого процесса заключается в формирования самой уникальной комбинации.

Набираемые символы создаются спонтанным образом посредством осуществления манипуляций мышки на стационарном компьютере либо тачпадом на ноутбуке, эти действия контролируются специально предназначенной программой, которая определяет координаты, далее создается некий шифр. Процесс выстраивается таким путем, чтобы ключ генерировался индивидуально, без возможности повторения шифра.

Второй – заключается в формировании самой подписи. Для определенного электронного документа при помощи хеш-функции в сочетании с закрытым ключом происходит вычисление подписи и в завершении происходит проверка подписи. Для данных, которые заключены в документе в совокупности с открытым ключом определяют достоверность подписи.

Механизм функционирования электронной подписи заключается во взаимодействии двух немаловажных процессов, которые в обязательном порядке входят в работу схемы электронной подписи, это ее формирование и проверка [12].

Одним из недостатков электронной подписи являются мошеннические действия, связанные с ее использованием в результате несанкционированного доступа к алгоритму шифрования. Для того чтобы обезопасить свои данные, в частности электронную подпись, недостаточно защиты криптографического алгоритм RSA и использования математических мер безопасности, проще говоря применение ключа определенной длины, очевидно, что завершаются успехом именно атаки, которые происходят на незащищенных этапах действия ключей системы RSA [13].

Заключение

Подводя итоги проведенных исследований электронной подписи, ее создания, видов, проверки и методов защиты, следует отметить, что современные методы шифрования, а также проверки, несмотря на то, что имеют высокую степень надежности кодировки информации, не дают гарантии защиты пользователя от действий недобросовестного характера. Однако данный недостаток не снижает значительного преимущества использования электронной подписи при внедрении электронного документооборота в различные сферы деятельности человека. Электронная подпись является эффективным и актуальным способом подписи документов.

Конфликт интересов

Не указан.

Рецензия

Все статьи проходят рецензирование. Но рецензент или автор статьи предпочли не публиковать рецензию к этой статье в открытом доступе. Рецензия может быть предоставлена компетентным органам по запросу.

Conflict of Interest

None declared.

Review

All articles are peer-reviewed. But the reviewer or the author of the article chose not to publish a review of this article in the public domain. The review can be provided to the competent authorities upon request.

Список литературы / References

1. Орфографический словарь русского языка: более 100 000 слов / Под ред. С.И. Ожегова. — М.: Локид-Пресс, 2007. — 910 с.

2. Российская Федерация. Законы. Гражданский кодекс Российской Федерации: федер. закон // КонсультантПлюс. — 2022. — URL: https://www.consultant.ru/document/cons_doc_LAW_5142/08b8673b58e230c76f61b3a81736d4b2fd9ea3d2/. (дата обращения: 03.12.22)

3. Кошманов М.П. Удостоверительная и защитная функции подписи. / М.П. Кошманов, П.М. Кошманов, А.А. Шнайдер // Нотариус. — 2020. — 3. — с. 40-46.

4. Российская Федерация. Законы. Об электронной подписи: федер. закон: [от 06.04.2011 N 63-ФЗ] // КонсультантПлюс. — 2011. — URL: https://www.consultant.ru/document/cons_doc_LAW_112701/. (дата обращения: 03.12.22)

5. Российская Федерация. Законы. О внесении изменений в Федеральный закон "Об электронной подписи» и статью 1 Федерального закона "О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля": федер. закон: [от 27.12.2019 N 476-ФЗ (последняя редакция)] // КонсультантПлюс. — 2019. — URL: https://www.consultant.ru/document/cons_doc_LAW_341757/. (дата обращения: 03.12.22)

6. Аннин А.Г. Электронная подпись: понятие и практика применения / А.Г. Аннин, С.С. Новиков // Аграрное и земельное право. — 2020. — 8. — URL: https://cyberleninka.ru/article/n/elektronnaya-podpis-ponyatie-i-praktika-primeneniya. (дата обращения: 03.12.22)

7. Черемушкин А.В. О содержании понятия «Электронная подпись» / А.В. Черемушкин // ПДМ. — 2012. — 3. — URL: https://cyberleninka.ru/article/n/o-soderzhanii-ponyatiya-elektronnaya-podpis. (дата обращения: 03.12.22)

8. Савельев А.И. Электронная коммерция в России и за рубежом: правовое регулирование [Электронный ресурс] / А.И. Савельев // КонсультантПлюс. — 2016. — URL: https://www.consultant.ru/law/podborki/savelev_a.i._jelektronnaya_kommerciya_v_rossii_i_za_rubezhom%253A_pravovoe_regulirovanie/. (дата обращения: 03.12.22)

9. Попов С.С. Система электронной подписи в современном документообороте. / С.С. Попов // Молодой ученый. — 2019. — 6. — с. 86-88.

10. Баричев С.Г. Основы современной криптографии / С.Г. Баричев, В.В. Гончаров, Р.Е. Серов — М.: Питер, 2020. — 176 с.

11. Комарова А.В. Анализ основных существующих пост-квантовых подходов и схем электронной подписи. / А.В. Комарова, А.Г. Коробейников // Вопросы кибербезопасности. — 2019. — 2.

12. Бондаренко Ю.А. Особенности расследования мошенничества, совершенного с использованием электронной подписи / Ю.А. Бондаренко // Гуманитарные, социально-экономические и общественные науки. — 2020. — 3. — URL: https://cyberleninka.ru/article/n/osobennosti-rassledovaniya-moshennichestva-sovershennogo-s-ispolzovaniem-elektronnoy-podpisi. (дата обращения: 03.12.22)

13. Гончаров Е.И. Проблемы применения цифровой подписи в электронном документообороте России. / Е.И. Гончаров, Т.В. Шатковская // Северо-Кавказский юридический вестник. — 2020. — 2. — с. 97-103.

Список литературы на английском языке / References in English

1. Orfograficheskij slovar' russkogo yazyka: bolee 100 000 slov [Spelling dictionary of the Russian language: more than 100,000 words] / Ed. by S.I. Ozhegov. — M.: Lokid-Press, 2007. — 910 p. [in Russian]

2. Russian Federation. Laws. Grazhdanskii kodeks Rossiiskoi Federatsii [The Civil Code of the Russian Federation]: Federal Law // Consultant Plus. — 2022. — URL: https://www.consultant.ru/document/cons_doc_LAW_5142/08b8673b58e230c76f61b3a81736d4b2fd9ea3d2/. (accessed: 03.12.22) [in Russian]

3. Koshmanov M.P. Udostoveritel'naya i zashhitnaya funkcii podpisi [Authentication and security functions of the signature]. / M.P. Koshmanov, P.M. Koshmanov, A.A. Shnajder // Notarius [Notary]. — 2020. — 3. — p. 40-46. [in Russian]

4. Russian Federation. Laws. Ob jelektronnoj podpisi [About the electronic signature]: Federal Law: [dated 06.04.2011 N 63-FZ] // ConsultantPlus. — 2011. — URL: https://www.consultant.ru/document/cons_doc_LAW_112701/. (accessed: 03.12.22) [in Russian]

5. Russian Federation. Laws. O vnesenii izmenenii v Federalnii zakon "Ob elektronnoi podpisi» i statiu 1 Federalnogo zakona "O zashchite prav yuridicheskikh lits i individualnikh predprinimatelei pri osushchestvlenii gosudarstvennogo kontrolya (nadzora) i munitsipalnogo kontrolya" ot 27.12.2019 N 476-FZ (poslednyaya redaktsiya) [On Amendments to the Federal Law "On Electronic Signature" and article 1 of the Federal Law "On the Protection of the Rights of Legal Entities and Individual Entrepreneurs in the Exercise of State Control (Supervision) and Municipal Control"]: Federal Law: [dated 27.12.2019 N 476-FZ (latest edition)] // ConsultantPlus. — 2019. — URL: https://www.consultant.ru/document/cons_doc_LAW_341757/. (accessed: 03.12.22) [in Russian]

6. Annin A.G. Elektronnaya podpis: ponyatie i praktika primeneniya [Electronic signature: concept and practice of application] / A.G. Annin, S.S. Novikov // Agrarnoe i zemel'noe pravo [Agrarian and land law]. — 2020. — 8. — URL: https://cyberleninka.ru/article/n/elektronnaya-podpis-ponyatie-i-praktika-primeneniya. (accessed: 03.12.22) [in Russian]

7. Cheremushkin A.V. O soderzhanii ponyatiya «Elektronnaya podpis» [About the content of the concept of "Electronic signature"] / A.V. Cheremushkin // PDM. — 2012. — 3. — URL: https://cyberleninka.ru/article/n/o-soderzhanii-ponyatiya-elektronnaya-podpis. (accessed: 03.12.22) [in Russian]

8. Savel'ev A.I. E'lektronnaya kommerciya v Rossii i za rubezhom: pravovoe regulirovanie [E-commerce in Russia and abroad: legal regulation] [Electronic source] / A.I. Savel'ev // Consultant Plus. — 2016. — URL: https://www.consultant.ru/law/podborki/savelev_a.i._jelektronnaya_kommerciya_v_rossii_i_za_rubezhom%253A_pravovoe_regulirovanie/. (accessed: 03.12.22) [in Russian]

9. Popov S.S. Sistema e'lektronnoj podpisi v sovremennom dokumentooborote [Electronic signature system in modern document management]. / S.S. Popov // Molodoj ucheny'j [Young scientist]. — 2019. — 6. — p. 86-88. [in Russian]

10. Barichev S.G. Osnovy' sovremennoj kriptografii [Fundamentals of Modern Cryptography] / S.G. Barichev, V.V. Goncharov, R.E. Serov — M.: Piter, 2020. — 176 p. [in Russian]

11. Komarova A.V. Analiz osnovny'x sushhestvuyushhix post-kvantovy'x podxodov i sxem e'lektronnoj podpisi [Analysis of the main existing post-quantum approaches and electronic signature schemes]. / A.V. Komarova, A.G. Korobejnikov // Voprosy' kiberbezopasnosti [Cybersecurity issues]. — 2019. — 2. [in Russian]

12. Bondarenko Yu.A. Osobennosti rassledovaniya moshennichestva, sovershennogo s ispolzovaniem elektronnoi podpisi [Features of the investigation of fraud committed using an electronic signature] / Yu.A. Bondarenko // Gumanitarnye, social'no-jekonomicheskie i obshhestvennye nauki [Humanities, socio-economic and social sciences]. — 2020. — 3. — URL: https://cyberleninka.ru/article/n/osobennosti-rassledovaniya-moshennichestva-sovershennogo-s-ispolzovaniem-elektronnoy-podpisi. (accessed: 03.12.22) [in Russian]

13. Goncharov E.I. Problemy' primeneniya cifrovoj podpisi v e'lektronnom dokumentooborote Rossii [Problems of using digital signatures in electronic document management in Russia]. / E.I. Goncharov, T.V. Shatkovskaya // Severo-Kavkazskij yuridicheskij vestnik [North Caucasian Legal Bulletin]. — 2020. — 2. — p. 97-103. [in Russian]