Клименко К. В., Власенко А. В., Егорихин Ю. Е. Проблемы использования облачных технологий в процессе выпуска электронных подписей удостоверяющим центром // Каспий в эпоху цифровой экономики: материалы Международного научно-практического форума, Астрахань, 24–25 мая 2019 г. Астрахань: Астрахан. ун-т, 2019. С. 188–191.

Об электронной подписи: Федеральный закон от 06.04.2011 № 63-ФЗ (последняя редакция) // Российская газета. 2011. 8 апр. (№ 75).

Смирнов П. В., Смышляев С. В. Обеспечение безопасности систем дистанционного формирования электронной подписи в условиях слабодоверенного окружения // International Journal of Open Information Technologies. 2020. Vol. 8, iss. 12. P. 77–84. URL: https://cyberleninka.ru/article/n/obespechenie-bezopasnosti-sistem-distantsionnogo-formirovaniya-elektronnoy-podpisi-v-usloviyah-slabodoverennogo-okruzheniya (дата обращения: 20.01.2022).

Соловяненко Н. И. Юридическое значение электронной подписи в правовых отношениях электронного бизнеса // Colloquium-journal. 2020. № 8 (60), ч. 7. С. 55–58.

Казаков С. Электронная подпись: что изменится с 1 июля 2021 г. и позже // Контур: электронный журнал. 2021. 19 апр. URL: https://kontur.ru/articles/5728 (дата обращения: 20.01.2022).

А. К. Гуторова[1]
Российский государственный
профессионально-педагогический университет

УДК 005.92:004.056.55

ПРИМЕНЕНИЕ ЭЛЕКТРОННОЙ ПОДПИСИ В СОВРЕМЕННОМ ОБЩЕСТВЕ

Аннотация. В статье рассматривается сущность электронной подписи, проблемы применения электронной подписи и защиты информации, а также разбирается возможность использования электронной подписи для придания документу целостности и аутентичности.

Ключевые слова: электронная подпись, электронный документ, конфиденциальность, персональные данные, средства защиты, информационные технологии, идентификация, целостность и аутентичность документа.

Любой документ, издаваемый в организации, должен быть подписан уполномоченным на это лицом, чтобы придать ему юридическую силу и обеспечить правовую значимость. Современные информационные технологии, которые тесно вошли в нашу жизнь, поспособствовали переходу документооборота из бумажного в электронный формат, что в свою очередь привело к упрощению обмена документами, как внутри организации, так и за ее пределами. В итоге появились

[1] Научный руководитель: М. Б. Ларионова, кандидат исторических наук, доцент РГППУ.

новые понятия и термины, одним из которых является «электронная подпись» (далее – ЭП).

Особое место в электронном документообороте занимает задача идентификации волеизъявителей, решить которую призвана электронная подпись – наиболее удобный современный инструмент для обмена юридически важной документацией и совершения сделок в дистанционном режиме. Потребности современного электронного документооборота привели к появлению нетрадиционных задач защиты данных, одной из которых является проверка подлинности электронной информации, когда стороны электронного взаимодействия не доверяют друг другу. Данная проблема связана с созданием систем электронной подписи.

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» [ФЗ № 63 от 06.04.2011]. Исходя из определения, можно сделать вывод, что на сегодняшний день электронная подпись выступает полноценной заменой рукописной подписи, так как имеет полную юридическую силу согласно законодательству РФ. Именно поэтому технология электронной подписи часто применяется в системах электронного документооборота различного назначения: коммерческого, государственного, внутреннего и внешнего обмена документами, а также в работе с организационно-распорядительной, кадровой, законотворческой, торгово-промышленной и другой документацией [Славинская, 2020].

По мере увеличения количества областей, где используется электронная подпись, повышаются и риски, связанные с мошенническими действиями. Злоумышленники пытаются найти различные лазейки, чтобы получить выгоду. Чем больше таких возможностей, тем больше ответственности возлагается на информационные системы и аккредитованные удостоверяющие центры.

Использование информационных технологий в рамках работы с документами способствует усовершенствованию и удешевлению процедуры подготовки, учета и хранения документов. Электронная подпись на практике заменяет традиционные печать и подпись, способствует созданию внутренней корпоративной системы обмена электронными документами, тем самым значительно облегчает и ускоряет процесс визирования одного документа несколькими лицами, сокращая время движения документов [Бобылева, 2019, с. 138]. Электронная подпись дает гарантию того, что подписанная информация существует в ее исходном виде без несанкционированных изменений, а также обеспечивает конфиденциальность информационного обмена документами.

Электронная подпись привнесла свои коррективы в работу с документами, смогла решить и устранить большинство трудностей, которые свойственны подписи на бумажном носителе, но с ее появлением образовался ряд других проблем.

Одной из них является проблема подтверждения личности того, кто отправил документ. Стоит отметить, что при использовании электронной подписи на практике, каждый раз на подписываемом документе проставляется уникальный код, который создается индивидуально для каждого электронного документа [Славинская, 2020]. Однако проблема заключается в том, что нельзя, основываясь только на факте наличия в документе электронной подписи, установить, был ли документ подписан владельцем электронной подписи или же другим лицом, который воспользовался доступом к ЭП.

Вторая проблема использования электронной подписи на практике – подтверждение подлинности самого документа, который не возможен без наличия «секретного ключа», который хранится только у отправителя, и тесно связанного с ним «открытого ключа», которым должен владеть пользователь на другом конце. На основе «секретного ключа» передаваемый текст снабжается специальным атрибутом, а математические методы позволяют однозначно определить с использованием на другом конце «открытого ключа», откуда было отправлено сообщение. От сохранности «секретного ключа» напрямую зависит степень надежности любой системы, использующей электронную подпись [Ермоленко, 2013].

Третья проблема заключается в том, что нет гарантии того, что документ не был искажен в процессе его передачи. Задача целостности передаваемой информации довольно тесно связана с задачей обеспечения конфиденциальности [Шеметова, Чугунова, 2017]. Это обусловлено тем, что в телекоммуникационных сетях идет передача не самого сообщения, а его электронной копии. Однако для целого ряда современных информационных технологий наиболее важным становятся не сохранение конфиденциальности самого сообщения, а создание такого документа, который никто не сможет опровергнуть.

Сложна проблема среднесрочного и длительного хранения документов, подписанных ЭП. Срок действия сертификата ЭП составляет 3–5 лет. В случае с недействительным сертификатом электронной подписи, документ автоматически не теряет юридической силы, однако потребуются доказательства того, что на момент подписания сертификат ЭП был действителен, и ЭП была верна [Бобылева, 2019, с. 211]. Как известно, если срок действия сертификата электронной подписи истёк, то здесь складывается опасная ситуация: он может быть скомпрометирован, а сам документ изменён и доверять ему в чистом виде нельзя.

Исходя из вышеизложенного, появление электронного документооборота повлекло за собой проблему решения трех взаимосвязанных задач: подтверждение авторства (идентификация); подтверждение подлинности документа (аутентификация); обеспечение целостности передаваемой информации.

Электронные подписи являются безопасными, если вероятность того, что злоумышленник может сгенерировать или найти секретный ключ подписанного документа, очень мала, но, к сожалению, она никогда не равна нулю. Недостаточная безопасность смарт-карт, операционных систем и компьютеров

должна быть принята во внимание теми, кто пользуется ЭП постоянно, поскольку существующие пробелы в нормативно-правовой документации и в алгоритмах получения и проверки электронной подписи могут существенно снизить надежность этой технологии.

Таким образом, можно сделать вывод, что электронная подпись – это эффективное средство защиты информации от модификации, искажений, позволяющее при этом идентифицировать отправителя сообщения и перенести свойства реальной подписи под документом в область электронного документа. Электронная подпись является наиболее перспективным и широко используемым в мире способом защиты электронных документов от подделки и обеспечивает высокую достоверность сообщения.

Список источников и литературы:

Бобылева М. П. Управленческий документооборот от бумажного к электронному. Вопросы теории и практики. М.: Термика.ру, 2019. 379 с.

Ермоленко А. В. Практика применения электронной цифровой подписи в деятельности организаций: реальность и перспективы // Правовая информатика. 2013. № 3. С. 29–35. URL: https://cyberleninka.ru/article/n/praktika-primeneniya-elektronnoy-tsifrovoy-podpisi-v-deyatelnosti-organizatsiy-realnost-i-perspektivy (дата обращения: 22.11.2021).

Об электронной подписи: Федеральный закон от 06.04.2011 № 63-ФЗ // Российская газета. 2011. 8 апр. (№ 75).

Облачная электронная подпись. Проблемы безопасности и перспективы использования // SecurityLab.ru. URL: https://www.securitylab.ru/blog/personal/Informacionnaya_bezopasnost_v_detalyah/342098.php (дата обращения: 28.10.2021).

Славинская А. Н. Электронная подпись: виды и использование // Секретарь-референт. 2020. № 1. URL: https://www.profiz.ru/sr/1_2020/elektronnaya_podpis/ (дата обращения: 06.11.2021).

Шеметова О. В., Чугунова С. В. Некоторые проблемы применения электронной подписи в управленческой деятельности предприятий и пути их решения // Актуальные проблемы авиации и космонавтики. 2017. Т. 3, № 13. С. 425–427. URL: https://cyberleninka.ru/article/n/nekotorye-problemy-primeneniya-elektronnoy-podpisi-v-upravlencheskoy-deyatelnosti-predpriyatiy-i-puti-ih-resheniya (дата обращения: 08.11.2021).