принятии и развертывании систем искусственного интеллекта в живых системах, которые имеют задачи высокого риска.

Однако, поскольку авиация является критически важной отраслью безопасности, внедрение технологий, основанных на искусственном интеллекте, должно соответствовать высоким требованиям безопасности и защищенности

Один исследователь ИИ сделал такой вывод: «Использование искусственного интеллекта несет в себе риск резиновой штамповки, где любое окончательное решение человека будет свершившимся фактом, потому что машины обеспечивают всю информацию и интерпретацию. Чтобы избежать этой ситуации, подразумевается, что люди все еще должны будут интенсивно участвовать в надзоре за машинами, чтобы их окончательное решение могло быть основано на соответствующем понимании того, что происходит. Это становится изменением роли человека, а не устранением человеческого элемента».

1. Бобровский С. «Перспективы и тенденции развития искусственного интеллекта» \ PC Week / RE: № 32, 2001. – 32-34 с.
2. Ноткин Л.И. Искусственный интеллект и проблемы обучения // <http://www.erudition.ru/>
3. Уинстон П. Искусственный интеллект. Москва: Мир, 2001. – 520 с.
4. Холодная М.А. Психология интеллекта. Парадоксы исследования / 2-е изд., перераб. и доп. – СПб.: Питер, 2002. – 272 с.
5. ИКАО Док. 9750-AN/963 Глобальный аэронавигационный план 2013-2028. 4 -е изд. Монреаль: ИКАО, 2013.

Павленков М.Н., Байрушин Ф.Т.

Об электронной подписи

*ФГБОУ ВО «Башкирский государственный университет»
(Россия, Уфа)*

doi: 10.18411/lj-11-2020-10

idsp: ljjournal-11-2020-10

Аннотация

В статье рассматривается понятие электронной подписи, которая подтверждает авторство электронного документа и обеспечивает защиту от подделки. Существует три вида электронных подписей, простая, неквалифицированная и квалифицированная. Помимо этого, действует ключ электронной подписи и ключ проверки электронной подписи.

Ключевые слова: электронная подпись, цифровая подпись, ключ электронной подписи, сертификат ключа, усиленная электронная подпись.

Abstract

The article discusses the concept of an electronic signature that confirms the authorship of an electronic document and provides protection against forgery. There are three types of electronic signatures: simple, unqualified, and qualified. In addition, the electronic signature key and the electronic signature verification key are valid.

Key words: electronic signature, digital signature, electronic signature key, the key certificate, an enhanced electronic signature.

Электронная подпись, также имеет название электронная цифровая подпись или цифровая подпись, позволяет подтвердить авторство электронного документа, обеспечивающий защиту от подделки. Первые электронные подписи появились в России 26 лет назад, в 1994 году, однако первый закон был принят только в 2002 году,

который помогает им пользоваться. А уже с 2011 года все государственные структуры используют электронный документооборот. В связи с этим, в современное время электронная цифровая подпись является обязательным требованием для госслужащих. В Российской Федерации существует Федеральный закон «Об электронной подписи» от 06.04.2011 N 63-ФЗ (последняя редакция).

В настоящее время существует три вида электронных подписей. Одна из них простая — используется для аутентификации в информационных системах, например, для получения госуслуг или при банковских операциях. Вторая, неквалифицированная электронная подпись — так же, как и первая используется для электронного документооборота, но при этом обе стороны заранее должны были договориться об этом. Последняя, квалифицированная электронная подпись — соответствует всем признакам неквалифицированной электронной подписи, но имеет дополнительные функции:

- ключ проверки электронной подписи и его сертификат.

Третья электронная подпись используется, чтобы работать, как описывалось ранее, на государственной службе и ими информационными системами, участвовать в качестве поставщика или заказчика того или иного товара в электронных торгах и обменяться документами с федеральной налоговой службой, где присутствует формализация.

Существует два ключа. Оба ключа состоят из ряда символов. Первый из них, ключ электронной подписи — им можно создать электронную подпись. Следующий ключ, ключ проверки электронной подписи — единственный способ проверить электронную подпись на подлинность. Владельцу второго ключа, в обязательном порядке должен быть выдан сертификат ключа проверки электронной подписи. Квалифицированную электронную подпись получают в любом удостоверяющем центре, за которым стоит юридическое лицо. Чтобы убедиться в центре, где получают цифровую подпись, достаточно перейти в раздел «Аккредитация удостоверяющих центров», где будет перечень аккредитованных удостоверяющих центров по состоянию на определенное число и перечень центров, которых либо приостановлена, либо прекращена или досрочно прекращена.

Защитных атрибутов бумажных документов, в их число входит подписи, водяные знаки, печати, штампы и тому подобное у электронных документов нет. Но тем не менее не стоит забывать о не менее тщательной защите документов, чем бумажные. Потому что не стоит забывать, что электронная подпись не даёт сто процентной защиты от злоумышленников, например, при передаче секретного ключа с электронной подписи своему коллеге для подписи важных документов в незапланированное своё отсутствие. Коллега в свою очередь может потерять тот или иной объект и не сообщать об этом своему товарищу по работе о данном происшествии до тех пор, пока он сам не обнаружит это.

Не стоит забывать о Федеральном законе от 27.12.2019 N 476-ФЗ (ред. 23.06.2020), что при создании электронной подписи средства электронной подписи, человек обязан предоставлять самостоятельно или с помощью компьютерных средств, необходимых для отображения информации, подписываемой с использованием назначенной суммы, лицу, выполняющий свою роль в создании электронной подписи, содержание информации, подписание которой производится. Кроме, уже упомянутый ранее, ФЗ от 06.04.2011 N 63-ФЗ (ред. от 08.06.2020) «Об электронной подписи» (с изм. и доп., вступ. в силу от 01.07.2020), статьи 10 пункта 1, при использовании усиленных электронных подписей участники обязуется при электронном документообороте гарантировать конфиденциальность не допускать использование принадлежащих им ключей электронных подписей без их согласия и обеспечивать защиту ключей электронных подписей.

При электронном взаимодействии, у участника есть право на использование электронной подписи одного из любых трёх видов цифровых подписей

самостоятельно, но если не нарушает требования об использовании определенной указанной электронной цифровой подписи и Федеральный закон, либо оба участника своевременно согласовали электронное взаимодействие. Принципом использования так же электронного взаимодействия любой цифровой подписи по собственному решению какой бы то ни было информационной технологии, в свою очередь предоставляющий возможность исполнить требования, описывающего ранее, Федерального закона N 63 «Об электронной подписи» по отношению того или иного вида электронной подписи. И последний принцип использования электронной подписи имеет быть недопустимость признания цифровой подписи или подписанного этой подписью электронный документ, не имеющий юридической силы в случае того, что это подпись действительная и верифицирована, а не создана собственными руками для определенного вида дела.

Квалифицированная электронная подпись является считается действительной, если соблюдается следующие условия:

- квалифицированный сертификат создан и выдан аккредитационным удостоверяющим центром, при этом дата выдачи должна быть действительной с указанной на сертификате;
- квалифицированный сертификат также должен быть действительным на момент подписания того или иного электронного документа или на тот день, когда подписывается электронным документ.

При использовании наиболее улучшенных электронных подписей участники электронного взаимодействия обязаны:

- сохранять конфиденциальность, не допускать использование электронных подписей без собственного согласия;
- в случае нарушения конфиденциальности ключа электронной подписи своевременно сообщить об этом удостоверяющему центру в течение не позднее полных рабочих суток со дня уведомления о том или ином.

Участники электронного взаимодействия не имеют права устанавливать другого вида ограничения признания усиленной квалифицированной электронной подписи, если такое не предусмотрено настоящим Федеральным законом.

Таким образом, мы видим, что электронная подпись хоть и предоставляет повышенную конфиденциальность операций по электронному документообороту, но всё равно есть шанс утечки той или иной информации. Также минимизируются финансовые риски, сокращение расходов на подготовку, доставку и хранение документов. С каждым днём во всём мире повышается активность использования электронной подписи. Об этом свидетельствует изменения в законах, посвященные электронной цифровой подписи.

1. Тимошин П.А. Перспективы развития и использования систем электронной цифровой подписи : научная литература / П.А. Тимошин — Издательство Московский финансово-промышленный университет «Синергия», 2007. — С. 12. — ISBN 1993-8314.
2. Шадура А. А., Гуцин Е. А Электронная подпись. Просто о сложном : научная литература / А.А. Шадура, Е. А. Гуцин — Издательство Издательские решения, 2019. — С. 3. — ISBN 978-5-0050-2557-9.
3. Портал государственных услуг Российской Федерации [Электронный ресурс] // Госуслуги / Режим доступа : / URL: <https://www.gosuslugi.ru/> (дата обращения 14.10.2020 г.).
4. Федеральный закон N 63-ФЗ от 06.04.2011 г. «РОССИЙСКАЯ ФЕДЕРАЦИЯ ФЕДЕРАЛЬНЫЙ ЗАКОН ОБ ЭЛЕКТРОННОЙ ПОДПИСИ» [Электронный ресурс] // КонсультантПлюс : справочно-правовая система / Режим доступа : / URL: <http://base.www.consultant.ru/> (дата обращения 14.10.2020 г.).
5. Электронный фонд правовой и нормативно-технической документации [Электронный ресурс] // Консорциум кодекс / Режим доступа : / URL: <http://docs.cntd.ru/> (дата обращения 14.10.2020 г.).