ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ

УДК 004.056.53

АЛГОРИТМ ПРОСТОЙ ЭЛЕКТРОННОЙ ПОДПИСИ ДЛЯ ДОВЕРЕННЫХ СИСТЕМ УПРАВЛЕНИЯ ДОКУМЕНТАМИ В ОРГАНИЗАЦИИ

© 2020 П. Е. Алиманов, А. Б. Сизоненко, И. П. Павлов

Краснодарское высшее военное училище (г. Краснодар, Россия)

Рассмотрена система управления электронным документооборотом организации. Проанализированы требования к системам управления документами и простой электронной подписи. Разработан и обоснован алгоритм формирования и проверки простой электронной подписи в организации, учитывающий требования, необходимые для признания такой подписи аналогом собственноручной.

Ключевые слова: система электронного документооборота, управление документными системами, требования к системам безопасности, простая электронная подпись

Документационное обеспечение является одним из основных видов обеспечения управленческой деятельности. Посредством документирования информация записывается на различные носители для дальнейшего использования: хранения информации, доведения управленческих решений, фиксации каких-либо фактов. Документы являются одновременно свидетельством деловой деятельности и информационными активами [1].

Документы, независимо от формы или структуры, должны обладать характеристиками аутентичности, достоверности, целостности и пригодности для использования, которые считаются доказательством подлинности деловых событий или операций и полностью отвечают установленным требованиям по ведению деловых операций [1].

Для эффективного управления документами в организации создаются документные системы. В документную систему входят как исполнители, так и сотрудники, обеспечивающие ее работу. В зависимости от объема, задачи и функции по управлению документной системой организации могут возлагаться на отдельных сотрудников иных подразделений, на специально назначенного сотрудника или, при большом объеме, могут создаваться отдельное подразделение документационного обеспечения управленческой деятельности.

Специалисты в области управления документами или лица иных подразделений, ответственные за управление документами, отвечают за разработку, внедрение и поддержку схем метаданных и других средств управления совместно с другими сотрудниками, такими как специалисты в области информационных технологий, руководители и юристы [1].

Учитывая требования к документным системам, дополнительные обязанности по их управлению возлагаются на сотрудников подразделений защиты информации. Возложение дополнительных обязанностей на сотрудников возможно при наличии у них резерва ресурсов на их выполнение. Подход, позволяющий формализовано оценить загрузку сотрудников подразделений защиты информации, резервы времени и выполнимость тех или иных функций представлен в [2, 3]. Предлагалось ввести матрицу возможности выполнения сотрудником функций защиты информации размерностью n столбцов на m строк (n – количество функций защиты информации, m – количество сотрудников). Модель оптимального распределения функций между сотрудниками подразделений защиты информации описана в [4].

Алиманов Павел Евгеньевич – Краснодарское высшее военное училище, p.e.alimanov@mail.ru.

Сизоненко Александр Борисович – Краснодарское высшее военное училище, д. т. н., доцент, siz_al@mail.ru.

Павлов Илья Павлович – Краснодарское высшее военное училище, pablo26rus@mail.ru.

Все чаще документы создаются и хранятся в цифровой среде, что открывает ряд новых возможностей для использования документов. Цифровая среда также обеспечивает большую гибкость в отношении внедрения средств управления документами внутри и между системами, которые осуществляют управление документами [5].

Одной из таких возможностей, которую предоставляет электронный документооборот, является применение электронной подписи. Внутри организации может использоваться простая электронная подпись, которая, при определенных условиях, приравнивается к собственноручной подписи и обладает юридической силой. Для этого необходимо, чтобы ключ простой электронной подписи применялся в соответствии с правилами, установленными оператором информационной системы, и в электронном документе содержалась информация, указывающая на лицо, от имени которого был создан и (или) отправлен электронный документ [6].

Подписи следует использовать в тех приложениях, где важно иметь возможность подтвердить целостность полученного файла и, возможно, личность отправителя. Следует обеспечить защищенное хранение подписей. Доступ к файлам подписей, ключам и алгоритмам должен разрешаться только авторизованному персоналу [5].

Электронные подписи, используемые для доказательства неизменности электронной информации, должны включать в себя контрольные суммы или значения хэш-кодов, которые могут быть встроены в файлы и (или) сохранятся в защищенной системе с привязкой к исходной информации [5].

Учитывая сказанное выше, разработаем алгоритм простой электронной подписи для использования в организации, учитывающий требования к документным системам, обладающей юридической силой и, в конечном итоге, позволяющей снизить трудозатраты сотрудников подразделений защиты информации при возложении на них функций по управлению документной системой организации.

Алгоритм формирования простой электронной подписи представлен на рисунке 1.

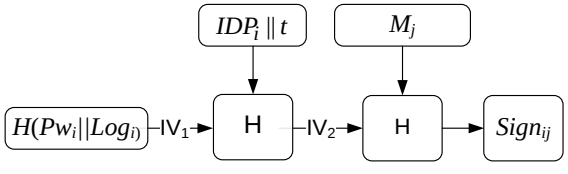

Рисунок 1. Алгоритм формирования простой электронной подписи

На рисунке введены следующие обозначения:

IDP (Identifier of personal) – идентификационный номер сотрудника в информационной системе организации.

Log (Login) – имя пользователя, идентификационные данные пользователя.

t (time) – метка времени.

Pw (password) – пароль, аутентификационные данные пользователя.

H (Hash) – хэш-функция.

IV (Initialization vector) – инициализационный вектор [7] («соль»).

M (Message) – сообщение, подписываемое простой электронной подписью;

Sign (Signature) – электронная подпись.

i, j – индексы для обозначения номера пользователя и документа соответственно.

|| – знак конкатенации двоичных векторов.

Процесс формирования электронной подписи заключается в следующем. Вырабатывается хэш-код пароля и логина пользователя, который используется как инициализационный вектор IV_1:

$$IV_1 = H(Log_i \| Pw_i). \qquad (1)$$

Применение в качестве инициализационного вектора хэш-кода логина и пароля необходимо для того, чтобы избежать их распространения при проверке электронной подписи.

Далее вычисляется второй инициализационный вектор путем определения хэш-кода от конкатенации идентификатора пользователя, метки времени. При этом используется вычисленный первый ранее идентификационный вектор:

$$IV_2 = H(IV_1, IDP_i \| t). \qquad (2)$$

Простая электронная подпись формируется из подписываемого электронного документа с использованием второго инициализационного вектора:

$$Sign_{ij} = H(IV_2, M_j). \qquad (3)$$

Для выполнения требований, необходимых для признания простой электронной подписи аналогом собственноручной, сведения о подписавшем лице и метке времени включаются в подписываемый файл. Конкатенация логина и пароля пользователя используется в качестве ключа простой электронной подписи.

Предлагаемая инфраструктура простой электронной подписи представлена на рисунке 2. Доверие к простой электронной подписи строится на доверии к серверу. На сервере ведется база данных электронных

подписей (DBSign), база данных электронных документов (DBDoc) и база данных хэш-кодов идентификационных данных пользователей (DBPw).

После формирования электронная подпись добавляется в DBSign. Кроме самой электронной подписи запись базы данных содержит идентификатор пользователя (IDP_i) и идентификатор подписанного документа (IDD_j).

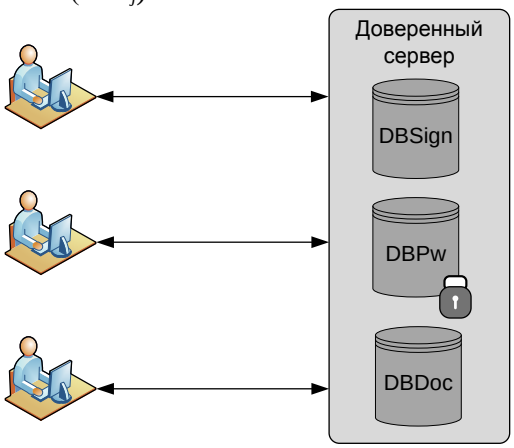

Рисунок 2. Инфраструктура простой электронной подписи

Для проверки электронной подписи пользователь направляет на сервер запрос, содержащий IDP_i, IDD_j, метку времени t. Сервер в соответствии с (1) и (2) вычисляет IV_2 и направляет его вместе с электронной подписью документа $Sign_{ij}$ пользователю. Пользователь в соответствии с (3) вычисляет значение электронной подписи и сравнивает его с подписью из DBSign, полученной от сервера. При условии их равенства простая электронная подпись считается аутентичной.

ЛИТЕРАТУРА

1. Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Информация и документация. Управление документами. Часть 1. Понятия и принципы: ГОСТ Р ИСО 15489-1-2019 – введ. 01.01.2020. // СПС «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

2. Алиманов П. Е. Формализация процесса определения оптимальной организационно-штатной структуры подразделений защиты информации / П. Е. Алиманов, А. Б. Сизоненко // Научные труды КубГТУ – 2019 –№ 7 – С. 73-79.

3. Алиманов П.Е. Модель организационно-штатного обеспечения подразделений защиты информации / П. Е. Алиманов, А. Б. Сизоненко // Вестник Воронежского института МВД России. – 2020. – № 1. – С. 33-38.

4. Алиманов П. Е. Математическая модель распределения функций между сотрудниками подразделений защиты информации для решения задачи линейного программирования / П. Е. Алиманов, А. Б. Сизоненко // Вестник Воронежского института высоких технологий. – 2020. – № 1 (32). – С. 21-23.

5. Системы электронного документооборота. Управление документацией. Информация, сохраняемая в электронном виде. Рекомендации по обеспечению достоверности и надежности: ГОСТ Р 54471-2011/ISO/TR 15801:2009 – введ. 01.08.2012. // СПС «КонсультантПлюс». – Режим доступа http://www.consultant.ru.

6. Об электронной подписи: федер. закон РФ от 06.04.2011 № 63-ФЗ // СПС «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

7. Информационная технология. Криптографическая защита информации. Функция хэширования: ГОСТ Р 34.11-2012. – Взамен ГОСТ Р 34.11-94; введ. 01.01.2013. – М.: Стандартинформ, 2013. – 24 с.

SIMPLE ELECTRONIC SIGNATURE ALGORITHM FOR OF TRUSTED DOCUMENT MANAGEMENT SYSTEMS IN THE ORGANIZATION

© 2020 P. E. Alimanov, A. B. Sizonenko, I. P. Pavlov

Krasnodar Higher Military School (Krasnodar, Russia)

The system of electronic document management of the organization is considered. The requirements for document management systems and a simple electronic signature are analyzed. An algorithm has been developed and justified for the formation and verification of a simple electronic signature in an organization, taking into account the requirements necessary for recognizing such a signature as an analogue of a handwritten one.

Keywords: electronic document management system, document management, security system requirements, simple electronic signature