УДК 004.77

ФУНКЦИИ ХЭШИРОВАНИЯ И ЭЛЕКТРОННО-ЦИФРОВАЯ ПОДПИСЬ

А.А. ТОЛСТОПЯТОВА[1], А.К. СУБАЕВА[2]
[1] магистрант кафедры «Приборостроение»
[2] д.э.н., доцент кафедры «Приборостроение»
«Казанский национальный исследовательский технический университет им. А.Н. Туполева -КАИ»
Чистопольский филиал «Восток»,
г. Чистополь, Российская Федерация

Аннотация. В данной статье рассматриваются основные функции современного подхода к использованию хэширования и электронно-цифровой подписи. Основная задача исследования- изучить существующие различные функции хэширования и электронно-цифровая подпись, а также изучить современные функции и рассмотреть предполагаемые функции в последствие применения хэширования и электронно-цифровая подпись. Изучена существующая литература по выбранной тематике. Выявлены различные подходы и пути их применения.

Ключевые слова: Хэширование, электронно-цифровая подпись, функции хэширования, преимущества и недостатки использования хэширования и электронно-цифровой подписи.

HASHING FUNCTIONS AND DIGITAL SIGNATURE

A.A. TOLSTOPYATOVA[1], A.K SUBAEVA[2]
[1] master students of the Department of the Department of Instrument Engineering
[2] Doctor of Economics, Associate Professor of the Department of Instrument Engineering
Kazan National Research Technical University named after A.N. Tupolev -KAI, Chistopol branch «Vostok»,
Chistopol, Russian Federation

Annotation. This article discusses the main functions of the modern approach to the use of hashing and digital signature. The main objective of

the study is to study the existing various hashing functions and electronic digital signature, as well as to study modern functions and consider the proposed functions as a consequence of the use of hashing and electronic digital signature. The existing literature on the chosen topic has been studied. Various approaches and ways of their application have been identified.

Keywords: Hashing, digital signature, hashing functions, advantages and disadvantages of using hashing and digital signature.

В современном мире обеспечение безопасности данных становиться все более актуальной задачей. Одним из главных задач защиты данных являются функции хэширования и электронно-цифровая подпись – это обеспечение и безопасность данных человека. Актуальность функции хэширования и электронно-цифровой подписи связана с увеличение количества использования и модернизации процесса электронной коммуникации. Неправильное использование функции хэширования может привести к утечке данных информации, а в последствии и к повреждению репутации организации, откуда произошла данная утечка.

Хеширование – это преобразование с помощью математических формул. Основная задача состоит в том, что происходит проверка информации. Хэширование содержит в себе несколько функций.

Функции хэширования – это математические алгоритмы, которые преобразуют произвольные данные в фиксированную строку фиксированной длинной, называемую хэш значением. Все функции хэширования рассмотрим на рисунке 1.

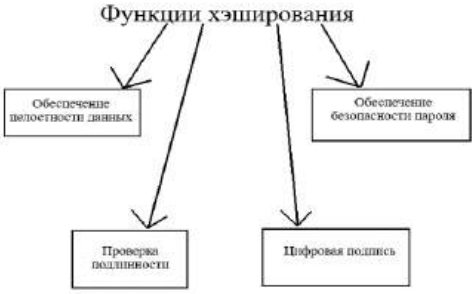

Рисунок 1 – Основных функций хэширования

Основные функции хэширования:

1. обеспечение целостности данных - хэширование данных используется для их проверки, были ли они изменены или повреждены (путем создания хеш-значения из исходных данных можно получить своего рода «отпечаток» данных);

2. проверка подлинности - хэширование используется для проверки целостности данных (если два набора данных имеют одинаковое хэш-значение, это означает, что данные не были изменены);

3. обеспечение безопасности паролей - хеширование широко применяется для защиты паролей (при использовании хэш-функции пароль преобразуется в хэш-значение, которое сохраняется в базе данных; при попытке входа в систему, введенный пароль хэшируется и сравнивается с соответствующим хэш-значением в базе данных);

4. цифровая подпись - при создании цифровой подписи, хэш-значение исходных данных шифруется с использованием закрытого ключа отправителя, чтобы создать уникальную подпись (получатель может использовать открытый ключ отправителя для расшифровки подписи и сравнения с хэш-значением исходных данных) [1].

Таким образом, можно сделать вывод, что хеширование играет важную роль в обеспечении безопасности данных и широко применяется в различных областях. Оно используется для проверки целостности данных, защиты паролей, проверки подлинности информации и создания цифровых подписей.

Также, хэширование является неотъемлемой частью электронно-цифровой подписи.

Электронно-цифровая подпись – это механизм, который подтверждает подлинность и целостность электронных документов или сообщений. Он основан на использовании асимметричного шифрования и функций хеширования. При создании электронно-цифровой подписи, хэш-значение исходных данных шифруется с помощью закрытого ключа отправителя. Получатель может использовать открытый ключ отправителя для расшифровки подписи и сравнения с хэш-значением исходных данных. Если значения совпадают, это гарантирует, что данные остались не изменёнными, и подпись была создана отправителем.

Электронно-цифровую подпись можно создать следующим образом:

1. с помощью специальных программ или онлайн-сервисов, которые помогают в создание данной подписи. Такие программы предлагают функциональность по различной генерации ключевой пары, хэшированию данных, а также подписанию с помощью использования своего приватного ключа;

2. с помощью использованию криптографических устройств. Такие устройства предоставляют возможность генерации ключевой пары и подписанию данных;

3. с помощью самостоятельной разработки программного решения для генерации ключевой пары, хеширования данных и создания электронно-цифровой подписи. При использовании данного метода потребуется хорошее знание криптографии и безопасности.

После создания данной электронно-цифровой подписи потребуется подтверждение в специальных государственных учреждениях. Такую подпись можно подтвердит в своем личном кабинете на портале государственных услуг Российской Федерации(госуслуги), в инспекции федеральной налоговой службы, а также в многофункциональном центр (МФЦ).

На рисунке 2 ниже представлено изображение электронно-цифровой подписи онлайн.

Рисунок 2 – Электронно-цифровой подпись

Электронно-цифровая подпись содержит преимущества и недостатки. Плюсы и минусы электронно-цифровой подписи рассмотрим в таблице 1.

Таблица 1 – Преимущества и недостатки электронно-цифровой подписи

Преимущества	Недостатки
Подписанный текст был отправлен именно от лица, которое поставило подпись	Юридической формальность. По истечению срока у электронно-цифровой подписи истечет ее юридическая значимость. После определенного срока времени ее придется продлевать
Невозможность отказа от обязательств, связанных с подписанным текстом	Усложнение процесса. Для использование электронно-цифровой подписи требуется определенные знания для ее создания и проверки. Не всегда это доставляет удобство пользователю, так как не все владеют современными технологиями
Гарантирует целостность подписанного текста, то есть отсутствие изменений в сообщении после его подписи	Зависимость от закрытого ключа. Создание электронно-цифровой подписи основан на использование закрытого ключа пользователя. Закрытый ключ может быть передан третьим лицам, которые могут использовать в будущем

Применение функций хеширования и электронно-цифровых подписей приносит множество преимуществ в обеспечении безопасности данных. Они помогают определить, были ли данные изменены, подтверждают подлинность отправителя и исключают возможность отрицания отправки сообщения. В нашем современном мире, где передача и хранение данных являются неотъемлемой частью нашей жизни, использование функций хеширования и электронно-цифровых подписей становится все более важным и необходимым.

Рассмотрев статистику применения электронной подписи в российских компаниях на сайте [2], можно сделать вывод применения электронной подписи в виде диаграмм. Статистику применения электронной подписи рассмотрим на рисунке 3.

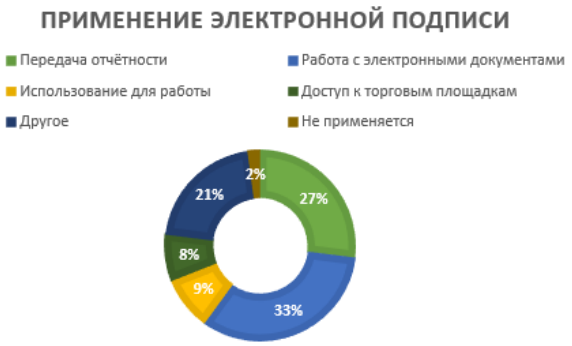

Рисунок 3 – Применение электронной подписи в России в 2023 году

Электронная подпись является неотъемлемым инструментом в удостоверение документов в государственных органах. Она используется для быстроты и удобства подтверждения индивидуальности и целостности данных бумаг. Но определенная часть людей не пользуется электронно-цифровой подписью. Согласно опрошенной часть людей, которая работает в определенной компании, можно увидеть статистику почему же люди не пользуется электронной подписью [2]. Причины, по которым люди не пользуются электронно-цифровой подписью, рассмотрим на рисунке 4.

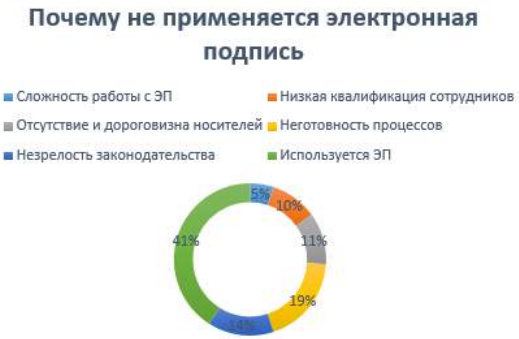

Рисунок 4 – Причины боязни использование электронной подписи в России в 2023 году

Для увеличения использования электронной подписи существует несколько способов:

- информирование людей о преимуществах и удобствах применения электронной подписи;
- создание удобство для использование такой подписи, а также способах ее подтверждения;
- поддержка от государства о использовании такой подписи в разных сферах услуг и так далее;
- обеспечение надежной защиты использования данной подписи, включая безопасное хранение информации, а также защиту от несанкционированного доступа и возможность проверки и подтверждения подлинности подписи;
- участие на международном уровне с участием применения и улучшения электронно-цифровой подписи

Таким образом, можно сделать вывод, что использование функции хэширования и применение электронно-цифровой подписи требует ряд правил. При соблюдении этих правил, можно быстро и легко подписывать какой-либо документ и тем самым применить к нему его индивидуальность. Со временем большинство людей сможет применять данную процедуру, так как не все оснащены специальной компьютерной техникой и знаниями о электронно-цифровой подписи. Изучив плюсы и минусы можно понять, что применение данной подписи очень удобно в современном мире.

Для того чтобы проанализировать уже существующие функции хэширования и электронно-цифровой подписи при написании статьи были рассмотрены открытые источники литературы по выбранной теме

Таким образом, в статье были изучены и описаны различные функции использования по выбранной теме, а также рассмотрены методы их применения.

ЛИТЕРАТУРА

1. Громов, Ю.Ю. Информационная безопасность и защита информации: Учебное пособие/ Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. – Ст. Оскол: ТНТ, 2017. – 384 с.

2. Все об электронной подписи в 2023 году [Электронный ресурс]. – Режим доступа: https://www.anti-

malware.ru/analytics/Technology_Analysis/All-about-electronic-signature-in-Russia-2023 (дата обращения: 16.02.2024).

3. Функции хэширования и электронно-цифровая подпись [Электронный ресурс]. – Режим доступа: https://studfile.net/preview/2014326/page:36/ (дата обращения: 18.02.2024).

4. Учебный программный комплекс по изучению отечественных стандартов функции хэширования и цифровой подписи [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/uchebnyy-programmnyy-kompleks-po-izucheniyu-otechestvennyh-standartov-funktsii-heshirovaniya-i-tsifrovoy-podpisi/viewer (дата обращения: 20.02.2024).

REFERENCES

1. Gromov, Yu.Yu. Information security and information protection: A textbook/ Yu.Yu. Gromov, V.O. Drachev, O.G. Ivanova. – St. Oskol: TNT, 2017. – 384 p.

2. All about the electronic signature in 2023 [Electronic resource]. – Access mode:https://www.anti-malware.ru/analytics/Technology_Analysis/All-about-electronic-signature-in-Russia-2023 (date of access: 02/16/2024).

3. Hashing functions and digital signature[Electronic resource]. – Access mode: https ://studfile.net/preview/2014326/page:36/ (date of access: 02/18/2024).

4. Educational software package for the study of domestic standards of hashing function and digital signature [Electronic resource]. – Access mode:https: //cyberleninka.ru/article/n/uchebnyy-programmnyy-kompleks-po-izucheniyu-otechestvennyh-standartov-funktsii-heshirovaniya-i-tsifrovoy-podpisi/viewer (date of application: 02/20/2024).