ЛИТЕРАТУРА

1. Способ автоматического включения резервного электропитания потребителей и устройство для его осуществления.Авт. Цырук С. А., Гамазин С.И., Козлов В.Н. и Павлов А.О. Патент РФ на изобретение№ 2326481 с приоритетом МЭИ от 0,7.11.2006г.

2. Устройство быстродействующего микропроцессорного АВР нового поколения. Гамазин С.И., Садыкбек Т.А. и др. –М.:Изд. Дом МЭИ «Вестник МЭИ» №3,2012

3. Способ автоматического включения резервного электропитания и устройство для его осуществления. Авт. Садықбек Т.А., Гамазин С.И., Цырук С.А., Мухамбетов Д.Г., Садыкбек А.Т. Инновационный патент РК на изобретение № 28086 от 27.12.2013г.

4. Научно-технические решения по быстродействующему автоматическому вводу резерва электропитания. Садыкбек Т.А., Шонтыбаев Е., Гамазин С.И., Цырук С.А. Алматы: Тран-Экспресс Казахстан. №6 (61) 2014.

5. Устройство быстродействующего включения резервного электропитания. Авт. Садыкбек Т.А., Цырук С.А., Данилов Н.В. Патент РК на полезную модель №2665 от 11.04.2017. года

УДК 625.1(075.8)

Б.А Казангапова[1,a], А.Б Ахметов[1,b]

[1] Алматинский технологический университет, г.Алматы, Республика Казахстан,

[a]kbayana@mail.ru, [b]aidosmagic@gmail.com

ИННОВАЦИОННЫЙ ПОДХОД К БЕЗОПАСНОСТИ ДЛЯ УПРАВЛЕНИЯ ЭЛЕКТРОННЫМИ ДОКУМЕНТАМИ НА ОСНОВЕ ДАКТИЛОСКОПИРОВАНИЯ

Аннотация. Незаконное распространение цифровых документов авторизованными, но недобросовестными пользователями представляет собой растущую угрозу конфиденциальности организаций, с которой не может полностью справиться система управления документами, использующая только методы шифрования. Эта проблема возникает вместе с доступом к цифровому документу неавторизованных пользователей.

В данной статье в качестве контрмеры для защиты цифровых документов от этих двух угроз предлагается новый подход, который тщательно объединяет методы шифрования и снятия отпечатков пальцев на определенных этапах жизненного цикла цифрового документа. В рамках этого сценария был проведен полный анализ, в котором были определены основные составные элементы, их взаимодействие, поток данных и предоставление услуг по обеспечению безопасности. Данная система защиты гарантирует достаточный уровень безопасности, так как в ней используются стандартные криптографические алгоритмы и рекомендуемые размеры ключей.

Цель этого подхода - обеспечить такие услуги информационной безопасности, как конфиденциальность, целостность, аутентификация, неотказуемость и отслеживание пользователя, тем самым защищая цифровые документы на протяжении всего их жизненного цикла.

Ключевые слова: системы электронного документооборота, информационная безопасность, критерии эффективности, защита электронного документооборота, угрозы информационной безопасности, дактилоскопия.

Аннотация. Рұқсат етілген, бірақ жосықсыз пайдаланушылардың сандық құжаттарды заңсыз таратуы ұйымдардың жеке өміріне қауіп төндіреді, оларды тек шифрлау құжат айналымы жүйесі толығымен шеше алмайды. Бұл мәселе рұқсат етілмеген пайдаланушылардың сандық құжатқа қол жеткізуі кезінде пайда болады.

Бұл екі қауіптен цифрлық құжаттарды қорғаудың қарсы шарасы ретінде бұл құжат цифрлық құжаттың өмірлік циклінің белгілі бір кезеңдерінде шифрлау мен саусақ іздерін алу әдістерін мұқият біріктіретін жаңа тәсілді ұсынады. Бұл сценарийде негізгі құрылыс блоктарын, олардың өзара әрекеттесуін, мәліметтер ағыны мен қауіпсіздік қызметін ұсынуды анықтаған толық талдау жүргізілді. Бұл қорғау жүйесі қауіпсіздіктің жеткілікті деңгейіне кепілдік береді, өйткені ол стандартты криптографиялық алгоритмдер мен ұсынылған кілт өлшемдерін қолданады.

Бұл тәсілдің мақсаты - құпиялылық, тұтастық, аутентификация, бас тартпау және пайдаланушының қадағалануы сияқты ақпараттық қауіпсіздік қызметтерін ұсыну, осылайша сандық құжаттарды бүкіл өмірлік циклында қорғау.

Түйінді сөздер: электрондық құжат айналымы жүйелері, ақпараттық қауіпсіздік, тиімділік критерийлері, электрондық құжат айналымын қорғау, ақпараттық қауіпсіздікке төнетін қатерлер, саусақ іздері.

Annotation. The illegal distribution of digital documents by authorized but unscrupulous users is a growing threat to the privacy of organizations that cannot be fully addressed by an encryption-only document management system. This problem occurs when unauthorized users have access to a digital document.

As a countermeasure to protect digital documents from these two threats, this paper proposes a new approach that carefully integrates encryption and fingerprinting techniques at specific stages in the digital document lifecycle. In this scenario, a full analysis was carried out, which identified the main building blocks, their interactions, data flow and security service delivery. This protection system guarantees a sufficient level of security, since it uses standard cryptographic algorithms and recommended key sizes.

The goal of this approach is to provide information security services such as confidentiality, integrity, authentication, non-repudiation, and user traceability, thereby protecting digital documents throughout their entire life cycle.

Key words: electronic document management systems, information security, performance criteria, protection of electronic document management, information security threats, fingerprinting.

Информационные ресурсы и информационные системы являются частью ряда основных элементов, которые защищены во всех сферах жизни современных компаний. На сегодня средства негативного информационного воздействия активно разрабатываются, и противодействие им требует обширных и разнообразных исследований, разработки связанных концепций, планов, для организации конкретной работы в области создания инструментов, методов и технологий для обеспечения информационной безопасности. Создание и организация функционирования современной структуры и системы в первую очередь требует обеспечения ее информационного взаимодействия с внешней средой. Подобное взаимодействие должно быть как можно более надежным и безопасным, что становится сложной задачей, учитывая экспоненциальный ежегодный рост количества обнаруженных инцидентов, о которых сообщают специалисты (по данным Computer Emergency Response Team (CERT) в 2020 году количество инцидентов с использованием вредоносного ПО увеличилось на 54% по сравнению с 2019 годом. Среди всех вредоносов, используемых в атаках на организации, бессменным лидером на протяжении двух лет остаются программы - вымогатели).

Незаконное (несанкционированное) использование, кража или искажение деловой информации (банковская, коммерческая, статистическая) неизбежно ведет к значительным финансовым потерям. По данным компании McAfee и Центра стратегических и международных исследований, общие финансовые потери от киберпреступности в 2020 году составили 1% мирового ВВП, что составляет более 1 триллиона долларов, что на 50% больше, чем два года назад.

Предлагаемый подход ориентирован на конкретный сценарий, обычно встречающийся в организациях, где цифровыми документами манипулируют пользователи с разными ролями на разных этапах - от создания, оцифровки, хранения до использования.

В данной работе рассматривается сценарий, обычно встречающийся в реальных организациях и предприятиях, где физические или бумажные документы оцифровываются и хранятся в виде цифровых изображений. Обычно это делается для того, чтобы сохранить собственноручно написанные подписи, печати одобрения или любой другой символ, подтверждающий содержание документа. Процесс сканирования физических документов и хранения их как цифровых изображений известен как Document Imaging (DI), который определяет конкретный жизненный цикл документа, часто используемого в контексте локальной сети. Жизненный цикл документа изображен на рисунке 1 и хорошо документирован в [41].

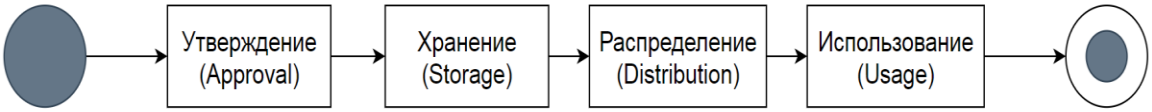

Рисунок 1 - Этапы жизненного цикла документов

Жизненный цикл документа для DI начинается с момента создания и проверки физического документа. После утверждения документа он оцифровывается, и полученное цифровое изображение готово к архивированию в СЭД, что является этапом Утверждения (Approval).

Начиная с этого этапа ЭлД не должен быть изменен. Далее ЭлД отправляется в СЭД для этапа Хранения (Storage), где средства оптического распознавания символов извлекают текст и индексируют его. Наконец, ЭлД готов к этапу Распределения (Distribution), на котором она доступна и может быть использована авторизованными пользователями на этапе Использования (Usage). Обычно доступ к цифровым документам ограничивается пользователями, ранее зарегистрированными в СУД, что предотвращает несанкционированный доступ. Утверждение документов и доступ к ним могут быть сегментированы по областям организации таким образом, чтобы документы были доступны только подмножеству пользователей. Категорируя пользователей по ролям, которые они играют в СЭД, можно выделить различные типы пользователей по областям:

1) Рецензенты, которые утверждают и загружают цифровые документы. Все операции между рецензентами и СЭД гарантированно проходят проверку подлинности и конфиденциальность.

2) Потребители (пользователи), которые получают доступ к цифровым документам и используют их. Все операции между потребителями и DMS гарантированно удостоверяются и являются конфиденциальными.

3) Аудиторы - особый тип Потребителей, которые могут получить доступ к любому цифровому документу без ограничений и подтверждают личность рецензентов, которые утвердили конкретный цифровой документ, требуя отказа от услуг авторства.

4) Администраторы, которые определяют личность пользователя/пользователей, распространивших документ. Администраторы -пользователи имеют специальные полномочия, например, на удаление цифровых документов или на добавление/удаление пользователей системы.

Сценарии использования в предлагаемой СЭД описаны в таблице 1. В случае №1 необходимо учитывать безопасность, т.к. учетные данные, представляемые пользователями для аутентификации, должны быть защищены во время транзита.

Дополнительно варианты использования №2, №3, №4 и №5 могут полагаться на защищенное соединение между системой и агентом, но это не является обязательным, так как передаваемые данные в этих случаях не имеют смысла.

Таблица 1 - Сценарии использования в предлагаемой СЭЭД

Идентификатор случая использования	Описание случая	Ответственное лицо	Этапы жизненного цикла
№1	Вход в систему	Пользователь	Предварительный этап
№2	Выход из системы	Пользователь	Завершающий этап
№3	Регистрация пользователя	Администратор	Предварительный этап
№4	Удаление пользователя	Администратор	Предварительный этап
№5	Удаление электронного документа	Администратор	Хранения
№6	Загрузка электронного документа	Рецензент	Утверждения
№7	Скачивание электронного документа отдельного департамента	Пользователь	Распределения
№8	Скачивание электронного документа всего департамента	Аудитор	Распределения
№9	Подтверждение одобрения рецензента	Аудитор	Хранения
№10	Обнаружение пользователей, которые распространяют незаконные копии	Администратор	Использования

Однако для случаев №6 - №10 безопасность является обязательным требованием. В таблице 2 показаны службы безопасности, которые должны предоставляться в этих случаях использования, а также методы безопасности, рассмотренные при их моделировании и внедрении.

В №6 рецензент должен обеспечить аутентичность, конфиденциальность и целостность при загрузке цифровых документов в систему на этапе утверждения. Для этого рецензент подписывает цифровой документ и загружает документ и его подпись в систему безопасным способом с помощью оптового шифрования. Кроме того, рецензент предоставляет цифровую подпись данных, относящихся к операции утверждения. Эта информация может быть использована в #9 аудитором для подтверждения и обеспечения того, что действия рецензент не будут отвергнуты. #7 и #8 происходят на стадии распространения. В этом случае при загрузке цифровых документов Потребителями или Аудиторами требуются услуги безопасности подлинности, конфиденциальности и целостности. Цифровой документ и его подпись получают из системы в зашифрованном виде. Затем Потребитель или Аудитор локально расшифровывает содержимое и проверяет цифровую подпись документа на подлинность. #9 выполняется на этапе хранения аудитором. В любой момент времени, аудитор может обеспечить службу безопасности без права отказа, проверяя данные, связанные с операцией утверждения цифровых документов рецензентами. Наконец, #10 выполняет отслеживание пользователя на этапе использования для обнаружения пользователя, который загрузил данный цифровой документ из системы и незаконно распространил его. В этом случае используются методы снятия отпечатков пальцев. Только администраторы могут выполнить этот сценарий использования и должны предоставить цифровую копию используемого документа и его оригинальную версию, хранящуюся в системе, чтобы осуществить обнаружение предателя.

Таблица 2 - Использование необходимых служб безопасностей и методов

Этапы жизненного цикла	Необходимая служба безопасности	Методы
Утверждения и Распределения	Аутентичность	Асимметричная криптография, Цифровые сертификаты, Электронная цифровая подпись
Утверждения, хранения и Распределения	Конфиденциальность	Симметричное и асимметричное шифрование
Утверждения, хранения и Распределения	Целостность	Хэш-функции и цифровые подписи
Хранения	Не отречение (не отклонение) *Non-repudiation	Электронная цифровая подпись
Хранения	Контроль доступа	Контроль доступа на основе ролей, обязательный контроль доступа (ОКД)
Использования	Отслеживания пользователей	Дактилоскопирование (отпечаток пальца)

Как уже было показано в [1], основные угрозы безопасности существуют в двух аспектах: первый - это несанкционированный доступ и использование пользователя к электронному документу, второй - незаконное копирование и распространение электронных документов легальными пользователями. Управление правами в цифровом формате или Rights Management Digital (DRM) является одной из актуальных тем в области информационной безопасности и осуществляет контроль доступа к цифровому информационному контенту в его жизненном цикле через сочетание аппаратного и программного обеспечения механизма доступа. Его суть в том, что с помощью ряда технологий безопасности он контролирует цифровой контент и каналы его распространения, чтобы предотвратить копирование и использование цифрового продукта без разрешения. В настоящее время исследования и применение DRM в основном практикуются в электронных книгах, потоковых Интернет-носителях и электронных документах. Технология DRM, применяемая для защиты электронных документов, может эффективно предотвращать несанкционированный доступ неавторизованных пользователей к электронным документам и их использование.

Что касается проблемы незаконного распространения электронных документов легальными пользователями, то существующая система защиты документов, основанная на DRM, призвана решить эту проблему путем ограничения пользовательских копий оригинальных документов. Основная идея модели заключается в том, что технология цифровой дактилоскопии сочетается с DRM в системе. Вводя в электронный документ информацию о характеристиках пользователей, рассматриваемых в качестве цифрового отпечатка пальца, система может позволить пользователям использовать копии документов, как правило, при одновременном выявлении ответственности пользователей в случае незаконной утечки электронного документа. В результате, система имеет определенные ограничения на незаконное распространение пользователями засекреченных электронных документов.

Модель системы

Учитывая два аспекта использования законных пользователей и защиты документов безопасности, мы объединяем технологию цифровых отпечатков пальцев с DRM, и разработана модель защиты электронных документов, которая может определить ответственность пользователей после того, как электронный документ был передан незаконно. Система состоит из пяти частей: «Распределительная часть документа»,

«Сервер распределения», «Сервер цифровых отпечатков пальцев», «DRM-сервер» и «Использование документов», как показано на рисунке 2. Сервер цифровых отпечатков пальцев состоит из Системы отслеживания отпечатков пальцев, Системы кодирования отпечатков пальцев и Третьей стороны. В отличие от традиционной системы защиты электронных документов, основанной на DRM, сервер распределения и сервер цифровых отпечатков пальцев увеличены.

Основной рабочий процесс системы выглядит следующим образом:

(1) Дистрибьюторская сторона документа генерирует лицензию на документ. Лицензия обеспечивает политику управления и защиты документов, и после аутентификации личности лицензия будет передана на сервер DRM.

(2) Распределяющая сторона документа получает доступ к Серверу Цифровых Отпечатков пальцев для предоставления идентификационной информации пользователя Серверу Цифровых Отпечатков пальцев. Система кодирования отпечатков пальцев на Сервере цифровых отпечатков пальцев кодирует идентификационную информацию пользователя, а затем отправляет последовательность кодирования обратно на Конец распределения документов, последовательность кодирования встраивается в исходный документ в качестве подписи пользователя на Конец распределения документов.

(3) Копия документа трансформируется и шифруется на Конец распределения документов, а копия трансформируется в DRM-документ и передается на Сервер распределения. Создание Дистрибьюторского Сервера заключается в унификации выпуска DRM документа, исключая возможность получения DRM документов пользователями из других способов. Это необходимо для достижения идентификации ответственности за незаконное распространение.

(4) Пользователь, использующий документ, предоставляет действительную учетную запись пользователя и имя файла, при прохождении аутентификации личности - "Документ, использующий конечный доступ" к требуемому DRM-документу.

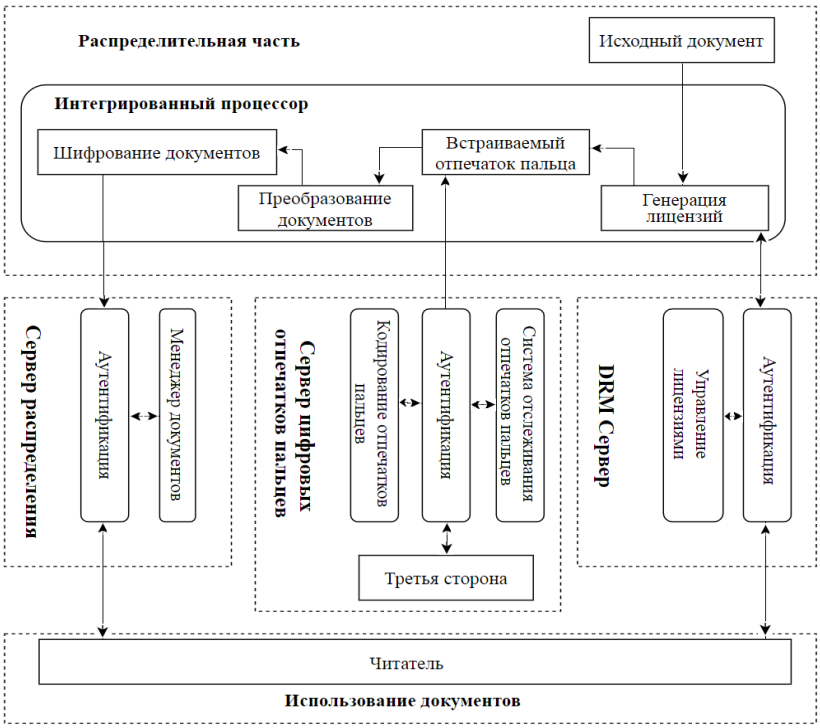

Рисунок 2 - Модель системы

Генерация лицензий, преобразование документов, шифрование документов, аналогичны традиционной системе защиты электронных документов, основанной на

DRM. Основные функции и методы реализации Сервера распределения, встраивания отпечатков пальцев, а также Сервера цифровых отпечатков пальцев подробно рассматриваются ниже:

A. Сервер цифровых отпечатков пальцев

Сервер цифровых отпечатков пальцев состоит из системы кодирования отпечатков пальцев и системы отслеживания отпечатков пальцев. Тем временем, сервер цифровых отпечатков пальцев завершает аутентификацию личности вместе с третьей стороной.

1. Система кодирования отпечатков пальцев

Функцией системы кодирования отпечатков пальцев является кодирование отпечатков пальцев, это означает, что система кодирования отпечатков пальцев кодирует идентификатор пользователя для получения соответствующей последовательности отпечатков пальцев.

2. Система отслеживания отпечатков пальцев

Система отслеживания отпечатков пальцев в основном завершает извлечение и сопоставление отпечатков пальцев. Сначала система извлекает отпечатки пальцев из документа, а затем сравнивает извлеченный отпечаток с отпечатанной записью в базе данных. Процесс извлечения и сопоставления отпечатков пальцев: сначала с помощью алгоритма извлечения отпечатков пальцев извлекается последовательность отпечатков пальцев из электронного документа, декодируется последовательность отпечатков пальцев для исправления ошибок, чтобы получить исправленную последовательность отпечатков пальцев, сопоставление исправленной последовательности отпечатков пальцев с отпечатками пальцев в базе данных отпечатков пальцев, чтобы удостовериться, какой пользователь скопировал и распространил документы, и кто должен нести ответственность за это. Процесс отслеживания показан на рисунке 3.

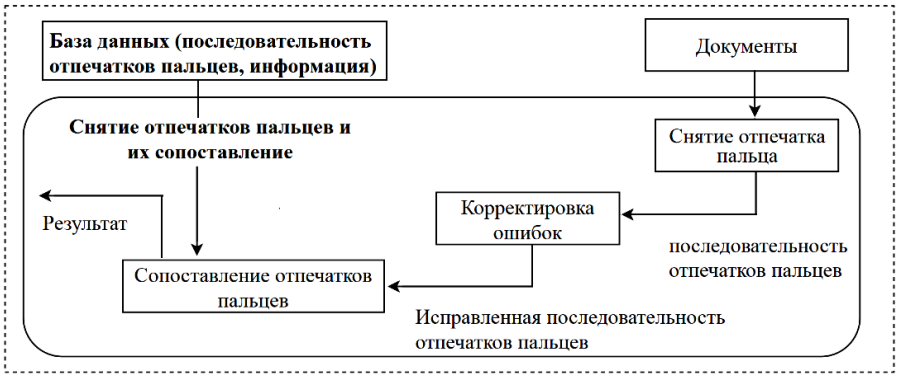

Рисунок 3 - Процесс отслеживания отпечатка пальца

B. Встраивание отпечатка пальца

Встраиваемый отпечаток пальца - это встраивание последовательности отпечатков кода пользователя в копию оригинального документа. В качестве основы для отслеживания авторских прав, последовательность отпечатков кода пользователя встраивается в каждую копию оригинального документа. Процесс встраивания заключается в следующем: во-первых, информация, подлежащая встраиванию, предварительно обрабатывается, чтобы получить последовательность отпечатков пальцев с идентификационной информацией пользователя, которая является фактическими данными, полученными от имени пользователя, рабочего блока, публичного ключа и так далее. Затем последовательность отпечатков пальцев пользовательской идентификационной информации берется в основу формирования закодированной последовательности отпечатков пальцев. И, наконец, применяя алгоритм встраивания отпечатков пальцев, такой как алгоритм NEC, кодированная последовательность отпечатков пальцев встраивается в копию документа Дистрибьютором документов.

Причина, по которой встраивание отпечатков пальцев помещается в дистрибьюторе документов, заключается в том, что если встраивание отпечатков пальцев осуществляется сервером цифровых отпечатков, то сервер цифровых отпечатков может быть слишком тяжелым, чтобы образовывать узкие места в системе в целом. Кроме того, передача копии оригинального документа между центром распределения документов и сервером цифровых отпечатков пальцев также может вызвать некоторые проблемы с безопасностью.

С. Сервер распределения

Сервер-распределитель является ядром разработки и внедрения системы, которая в основном состоит из подсистем управления пользователями и подсистем DRM документооборота.

1. Управление пользователями

Подсистема управления пользователями в основном обеспечивает управление пользователями и выполняет аутентификацию личности при входе пользователя в систему. Администраторы создают на сервере распределения базу данных пользователей, в которой в основном хранится информация об учетных записях и паролях пользователей. Идентификационная информация пользователя на сервере распределения может принимать технические средства для обеспечения согласованности идентификационной информации пользователя на сервере DRM и на сервере цифровых отпечатков пальцев.

2. Управление документооборотом DRM

DRM документ передается Интегрированным процессором на сервер дистрибуции по защищенному каналу, а подсистема управления документами DRM сохраняет и управляет документом и информацией о документе, такой как кодировка документа, имя документа, пользователь документа, производитель документа и дата, и т.д.. Каждый документ соотносится со своими законными пользователями, так что документы будут распространяться соответствующему пользователю в системе.

3. Обращение за документами

Когда пользователю необходимо подать заявку на получение документа, необходимо выполнить следующие действия:

(1) Пользователь входит в Сервер распределения и после успешной аутентификации личности сообщает имя документа или код документа;

(2) Сервер распределения запрашивает в информационной базе данных документов информацию о документе в соответствии с информацией о документе, введенной пользователем. В случае отсутствия идентификационной информации пользователя, который может получить доступ к документам, запросы пользователя отклоняются; в противном случае пользователю разрешается использовать документы, Сервер распределения забирает документ и отправляет пользователю, который отмечен информацией пользователя;

(3) записывает информацию о распространении документов, например, дату выдачи, идентификационную информацию пользователя и т.д.

Ключевым моментом, является то, что в цифровом дактилоскопировании используется другой код распознавания символов - дактилоскопирование встраивается в цифровые носители, которые затем распространяются среди пользователей. Таким образом, он является эффективным средством и одной из ключевых технологий защиты конфиденциальных электронных документов [2].

Цифровой отпечаток пальца, встроенный в документ трудно подделать, т.к. происходит сжатие данных до нескольких десятков байт и дальнейшие их шифрование (стегоключ). Схема кодирования информации по отпечатку пальца - это процесс, при котором информация, относящаяся к пользователю, кодируется по определенным правилам для генерации кодовых слов с определенной способностью сопротивляться атаке. Хорошее кодирование отпечатков пальцев является ключевым фактором для отслеживания нелегального распространения, каждая схема кодирования отпечатков

пальцев имеет соответствующую систему отслеживания. В настоящее время метод кодирования, основанный на тексте, включает в себя следующее: метод кодирования сдвига, метод замены синонимов, метод кодирования признаков, метод кодирования преобразования [3].

Вывод. Внедрена технология цифровой дактилоскопии в защиту документов на основе технологии защиты электронных документов DRM, в модели предложен новый способ идентификации ответственности за незаконное копирование и распространение конфиденциальных электронных документов, а также изучены ключевые технологии модели.

ЛИТЕРАТУРА

1. Казангапова Б.А. Информационная безопасность компьютерных систем и сетей: Алматы: ТОО «Power Print», 2019. - 119с.

2. Чунг К., Чой С., Чой У., и др. Эффективное анонимное снятие отпечатков пальцев с электронной информации с улучшенной автоматической идентификацией распространителей. В: Труды Третьей Международной конференции по информационной безопасности и криптологии, том 2015 LNCS.

3. Муноз-Хернандез М.Д., Гарсиа-Хернандез J.J. and Моралез-Сандовал, М. (2014) Исследование устойчивости цифровых документов с отпечатками пальцев к атакам с повторным вводом в частотной области. 9-й межд. Конф. Int. Технологии и обеспеченные транзакции (ICITST-2014), Лондон, Великобритания, 8–10 декабря, стр. 25–30. IEEE, Нью-Джерси, США.

УДК 656.228

С.Е. Бекжанова[1,a], Б.М.Исина[2,b], С.Ж. Косбармаков[2,c]
[1]Академии логистики и транспорта
[2]Карагандинский технический университет
[a]s.bekzhanova@bk.ru, [b]bota_kazatk@mail.ru, [c]samat.130579@mail.ru

ЕДИНЫЕ ИНТЕЛЛЕКТУАЛЬНЫЕ СИСТЕМЫ УПРАВЛЕНИЯ И АВТОМАТИЗАЦИИ ПРОИЗВОДСТВЕННЫХ ПРОЦЕССОВ НА ЖЕЛЕЗНОДОРОЖНОМ ТРАНСПОРТЕ

Аннотация. В статье рассматривается информационная система управления железнодорожным транспортом и информация о текущем состоянии и местоположении подвижного состава, потребностях всех участников перевозочного процесса. Речь идет о системах планирования работы товарного кассира и электронного продвижения поступления перевозочных документов на таможенный орган пограничной станции. То есть сотрудник получает задание на работу на автоматизированное рабочее место, определяет с помощью спутниковой навигации местоположение и фиксирует факт выполнения задания. Такое решение повысит оперативность и качество выполнения работ. Статья посвящена усовершенствованию условий перевозок для грузоотправителей за счет предоставления услуги железных дорог отслеживание грузов в пути следовании. Чтобы не была отсутствия заявки необходимо организовать перевозочный процесс со всеми подразделениями, согласовать с предприятиями, таможенными органами, станциями о предстоящих планах. Перевозочный документ в электронном виде единовременно поступал на таможенный орган и на промежуточную станцию который проходить груз. Обосновывается идея о том, что информационная система управления железнодорожным транспортом позволит собирать и анализировать информацию о