МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Тольяттинский государственный университет»

Институт математики, физики и информационных технологий
(наименование института полностью)

Кафедра Прикладная математика и информатика
(наименование)

09.04.03 Прикладная информатика
(код и наименование направления подготовки)

Управление корпоративными информационными процессами
(направленность (профиль))

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА (МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ)

на тему «Модели и алгоритмы системы управления информационной безопасностью электронного документооборота предприятия»

Обучающийся А.А. Шмойлова
(Инициалы Фамилия) (личная подпись)

Научный руководитель к.т.н., доцент, О.В. Аникина
(ученая степень (при наличии), ученое звание (при наличии), Инициалы Фамилия)

Тольятти 2023

Оглавление

Введение 3
Глава 1 Анализ современного состояния исследований в области управления безопасностью электронного документооборота предприятий 7
1.1 Анализ угроз и факторов информационной безопасности электронного документооборота предприятий 7
1.2 Анализ современных решений обеспечения информационной безопасности электронного документооборота 11
Глава 2 Анализ методов и технологий управления информационной безопасностью электронного документооборота предприятий 23
2.1 Технологии управления правами доступа пользователей 24
2.2 Технологии шифрования документов и электронно-цифровой подписи 27
2.3 Технология идентификации конфиденциальных документов с помощью интеллектуального анализа данных 35
Глава 3 Разработка моделей и алгоритмов системы управления информационной безопасностью электронного документооборота предприятия 39
3.1 Моделирование системы управления информационной безопасностью электронного документооборота предприятия 39
3.2 Алгоритмы системы управления информационной безопасностью электронного документооборота предприятия 42
Глава 4 Апробация и оценка эффективности проектных решений системы управления информационной безопасностью электронного документооборота предприятия 48
4.1 Апробация проектных решений 48
4.2 Оценка эффективности проектных решений 59
Заключение 64
Список используемой литературы 67

Введение

Система управления электронным документооборотом (далее – СЭД) является одним из ключевых компонентов системы управления многообразной деятельностью современного предприятия.

К сожалению, утечки данных — крупные и мелкие — происходят ежедневно, и почти каждая организация находится в опасности, особенно в связи с тем, что количество и использование данных достигли беспрецедентных масштабов. Этот рост обусловлен цифровизацией общества и сопутствующими ей новыми возможностями. Поэтому в организациях, которые используют СЭД, очень важно обеспечить безопасность своей бизнес-документации и клиентских данных.

Для решения данной проблемы необходимо грамотное управление корпоративным контентом. Цель состоит в том, чтобы дать организациям возможность в полной мере использовать новые возможности, связанные с данными, и контролировать их использование.

На современном ИТ-рынке широко представлены промышленные системы управления электронным документооборотом, реализованные как программно-независимые ИТ-решения, функциональность и архитектура которых полностью соответствует требованиям, предъявляемым к ECM/СЭД-системам.

Однако наиболее важным аспектом, на который следует обратить внимание в этой связи, является необходимость внедрения надежной системы управления информационной безопасностью (СУИБ) электронного документооборота.

При отсутствии эффективной СУИБ, интегрированной с СЭД, невозможно обеспечить безопасность электронного документооборота в масштабах всего предприятия.

Совершенно очевидно, что в основу СУИБ должны быть положены модели и алгоритмы, отвечающие самым современным требованиям

обеспечения безопасности электронного документооборота предприятия.

Исследование и разработка таких моделей и алгоритмов актуальны и представляют научно-практический интерес.

Объектом настоящего исследования является электронный документооборот предприятия.

Предметом исследования является СУИБ электронного документооборота предприятия.

Целью работы является исследование и разработка моделей и алгоритмов эффективной СУИБ электронного документооборота предприятия.

Для достижения поставленной цели необходимо решать следующие задачи:

- проанализировать современное состояние исследований в области управления безопасностью электронного документооборота предприятий;
- проанализировать методы и технологии управления информационной безопасностью электронного документооборота предприятий;
- разработать модели и алгоритмы эффективной СУИБ электронного документооборота предприятия;
- выполнить апробацию предлагаемых проектных решений и оценить их эффективность.

Гипотеза исследования: применение разработанных в рамках диссертационного исследования моделей и алгоритмов обеспечит повышение эффективности СУИБ электронного документооборота предприятия.

Методы исследования. В процессе исследования будут использованы следующие положения и методы: системный анализ, методы и технологии управления безопасностью электронного документооборота предприятий, методология объектно-ориентированного анализа и проектирования информационных систем.

Новизна исследования заключается в разработке моделей и алгоритмов, которые обеспечат повышение эффективности СУИБ электронного документооборота предприятия.

Практическая значимость исследования заключается в возможности применения предлагаемых моделей и алгоритмов при проектировании эффективной СУИБ электронного документооборота предприятия.

Теоретической основой диссертационного исследования являются научные труды российских и зарубежных ученых, занимающихся проблемами управления безопасностью электронным документооборота предприятия.

Основные этапы исследования: исследование проводилось с 2020 по 2023 год в несколько этапов.

На первом (констатирующем) этапе формулировалась тема исследования, выполнялся сбор информации по теме исследования из различных источников, проводилась формулировка гипотезы, определялись постановка цели, задач, предмета исследования, объекта исследования и выполнялось определение проблематики данного исследования.

Второй этап – поисковый. В ходе проведения данного этапа осуществлялся анализ методов и технологий управления безопасностью электронного документооборота предприятий, разработаны модели и алгоритмы эффективной СУИБ электронного документооборота предприятия, опубликована научная статья по теме исследования в научном сборнике.

На третьем этапе осуществлялась апробация предлагаемых проектных решений, произведена оценка их эффективности, сформулированы выводы о полученных результатах по проведенному исследованию.

На защиту выносятся:

- модели и алгоритмы эффективной СУИБ электронного документооборота предприятия;
- результаты апробации и оценки эффективности предлагаемых проектных решений.

По теме исследования опубликована 1 статья:

Диссертация состоит из введения, четырех глав, заключения и списка литературы.

Во введении обоснована актуальность темы исследования, представлены объект, предмет, цели, задачи и положения, выносимые на защиту диссертации.

В первой главе дан анализ современного состояния исследований в области управления безопасностью электронного документооборота предприятий.

Во второй главе дан анализ методов и технологий управления безопасностью электронного документооборота предприятий.

Третья глава посвящена разработке моделей и алгоритмов эффективной СУИБ электронного документооборота предприятий.

В четвертой главе выполнены апробация предлагаемых проектных решений и оценка их эффективности.

В заключении приводятся результаты исследования.

Работа изложена на 71 странице и включает 37 рисунков, 6 таблиц, 42 источника.

Глава 1 Анализ современного состояния исследований в области управления безопасностью электронного документооборота предприятий

1.1 Анализ угроз и факторов информационной безопасности электронного документооборота предприятий

«Эксперты сходятся во мнении, что в настоящее время многие коммерческие организации, прежде всего банки, страховые и промышленные компании, рассматривают СЭД в качестве ядра КИС.

И если раньше эти системы предназначались в первую очередь для организационно-распределительного документооборота и автоматизации канцелярии, то сейчас они все больше вовлекаются в живые бизнес-процессы (использование электронных архивов, простейших, и не только, BPM-систем, согласование документов и пр.)» [10].

В зарубежной классификации информационных систем СЭД относят к категории ECM (Enterprise Content Management)-систем, обеспечивающих систематический сбор и организацию информации, предназначенную для использования определенной аудиторией — руководителями предприятий, клиентами и т. д.

Согласно данной концепции ECM – это динамическое сочетание стратегий, методов и инструментов, используемых для сбора, управления, хранения и доставки информации, поддерживающей ключевые организационные процессы на протяжении всего жизненного цикла [42].

Альтернативой ECM являются DMS (Document Management Systems) – системы управления документами.

DMS представляет собой использование компьютерной системы и программного обеспечения для хранения, управления и отслеживания электронных документов и электронных изображений бумажной информации, снятых с помощью сканера документов [41].

Проще говоря, система управления документами — это автоматизированное программное решение для организации, защиты, захвата, оцифровки, маркировки, утверждения и выполнения задач с бизнес-файлами предприятия.

Некоторое различие концепций ECM и DMS обусловило различие в подходах к интеграции соответствующих систем с ERP-системами предприятий и компаний.

Исходя из представленных определений, системы управления электронным документооборотом в зависимости от решаемых конкретных задач можно позиционировать и как ECM, и DMS – системы.

Системы электронного документооборота, как и их бумажные аналоги, подвержены угрозам. Сотрудники могут ошибиться, а недобросовестные конкуренты попробовать выкрасть данные.

Угрозы для СЭД могут быть внешними и внутренними [3].

К внешним угрозам относятся:

- вредоносные программы;
- хакерские атаки (взлом);
- уязвимости в программном обеспечении (ПО) и интегрированных системах;
- стихийные бедствия. Независимо от того, происходит ли стихийное бедствие, такое как ураган, наводнение или торнадо, происходит массовый сбой в электроснабжении или какое-либо другое бедствие, с центром обработки данных, в котором работает ECM предприятия;
- другие угрозы, которые исходят не от работников предприятия.

К внутренним угрозам относятся [38]:

- неправильное использование систем и информации внутри предприятия;
- нарушения нормативных требований и политики безопасности. Многие внутренние и внешние процедуры обеспечения безопасности в настоящее время предписаны законом в форме

нормативных требований и политик. Это особенно критично для таких отраслей как, здравоохранение и финансовые услуги;

- ошибки или намеренный саботаж со стороны сотрудников организации.

Схема классификации угроз информационной безопасности типовой СЭД показана на рисунке 1.

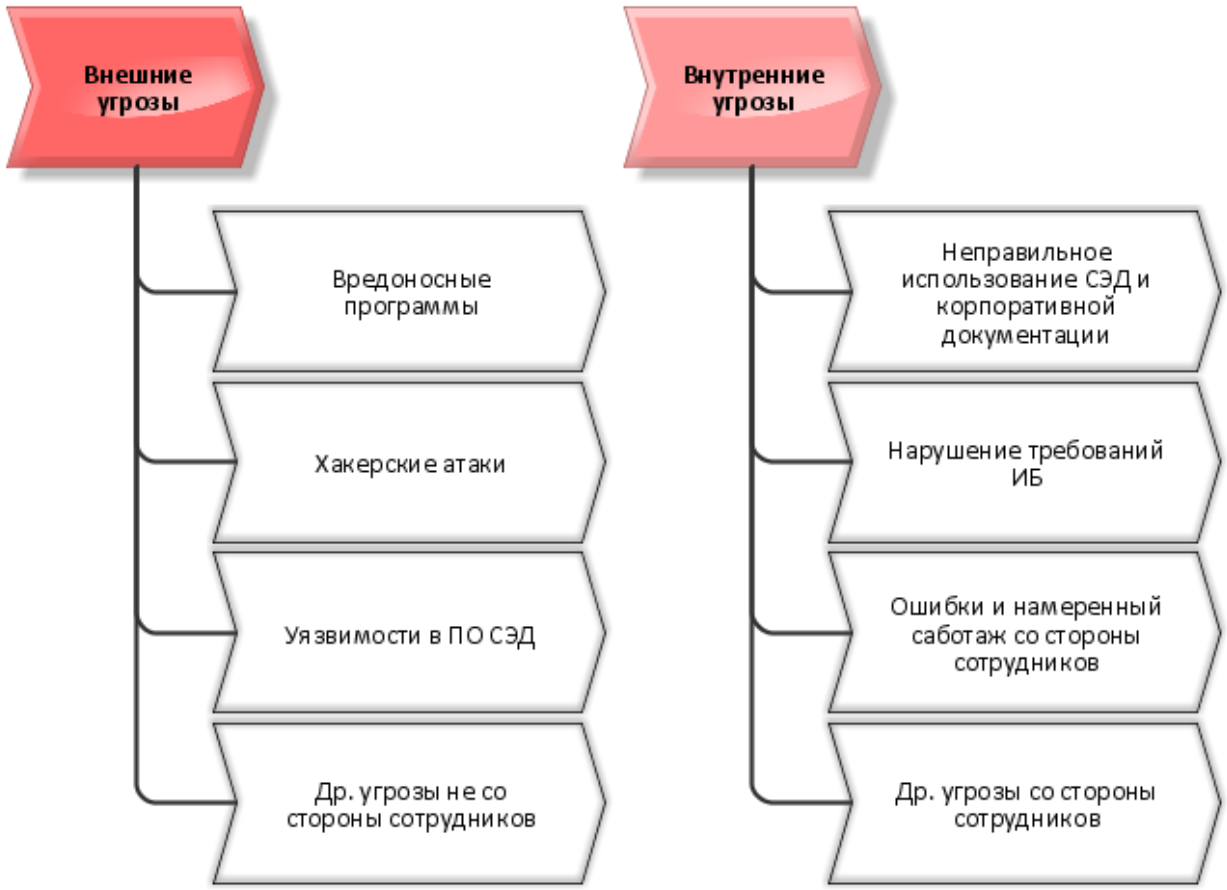

Рисунок 1 – Схема классификации угроз информационной безопасности СЭД

Факторы, влияющие на безопасность электронного документооборота [35]:

- меры безопасности данных на предприятии. Рынок ИТ-продуктов насыщен ПО для обеспечения информационной безопасности. Однако покупка технологического продукта не означает, что СЭД предприятия защищены и соответствуют требованиям;

- защита за пределами предприятия. В какой-то момент к данным предприятия можно будет получить доступ с устройств и сетей за пределами брандмауэров предприятия. Большое количество документов принимается вручную с помощью таких источников, как бумажная почта, электронная почта или факс. Партнерам, подрядчикам или аудиторам может потребоваться получить доступ к внутренним документам предприятия и обновить их. При использовании облачных приложений, данные организации хранятся на сторонних серверах. Все это является потенциальными источниками риска для третьих лиц. Многие утечки данных происходят не внутри предприятия, а в результате воздействия третьих лиц;
- устаревшие системы или устаревшие платформы. В организациях, где преимущества непрерывности бизнеса перевешивают риск сбоев в работе, устаревшие информационные системы все еще существуют и могут представлять угрозу безопасности;
- соответствие требованиям для архивов. Поддержание большого объема устаревших бумажных записей сопряжено с высокими затратами и высоким риском кражи или нанесения ущерба окружающей среде. Доступ и своевременное извлечение также являются проблемами с бумажными документами в хранилище;
- осведомленность и обучение сотрудников. Во многих компаниях менеджеры по качеству сталкиваются с проблемами управления версиями документов без прозрачной системы управления информацией.

Для защиты от угроз безопасности электронного документооборота используются СУИБ электронного документооборота предприятия.

СУИБ – это общая совокупность методов, средств и мероприятий, снижающих уязвимость системы и препятствующих несанкционированному доступу к информации, ее разглашению, повреждению, утрате или утечке [7].

В соответствии с Федеральным законом Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» для защиты информации используются правовые, организационные и технические меры, обеспечивающие [28]:

- защиту информации от несанкционированного доступа, уничтожения, модификации, блокирования, копирования, фальсификации, распространения, а также от других несанкционированных действий в отношении такой информации;
- соблюдение конфиденциальности информации ограниченного доступа;
- реализацию права на доступ к информации.

К основным техническим мерам относятся [9]:

- разграничение прав пользователей;
- применение современных криптографических средств защиты и шифрования документов;
- применение электронной цифровой подписи (ЭЦП);
- резервное копирование с размещением архивной информации на защищенных от порчи и несанкционированного доступа носителях.

По мнению аналитиков, при выборе наилучшей платформы СЭД/ECM для предприятия необходимо учитывать полноту реализации в ней вышеперечисленных технических мер [16].

1.2 Анализ современных решений обеспечения информационной безопасности электронного документооборота

Проблематика обеспечения информационной безопасности электронного документооборота рассматривается в работах российских и зарубежных ученых Булдаковой Т.И., Даниленко А.Ю., Шевцова В.Ю., Vivekanand R. Chudgar, Peneti Subhashini и др., а также специалистов ИТ-компаний IBM, Microsoft, 1С, Directum и др.

Представленные в этих работах решения для управления информационной безопасностью корпоративного контента оказали большое влияние на бизнес и помогают минимизировать риски, улучшить работу пользователей СЭД и снизить операционные расходы.

Рассмотрим некоторые из таких решений.

В исследовании [30] предложена формальная модель СУИБ документооборота.

«В разработанной модели используется матрица бинарных отношений, определяющая связь между множеством средств защиты информации, множеством актуальных угроз и требованиями, предъявляемыми к системам защиты информации в системах электронного документооборота.

Предложенная модель позволяет решить задачу оптимизации средств защиты информации, введённых в эксплуатацию; обеспечить их минимальную стоимость.

Разработаны архитектура и алгоритмы СУИБ документооборота на предприятии, представленные на рисунках 2 и 3» [30].

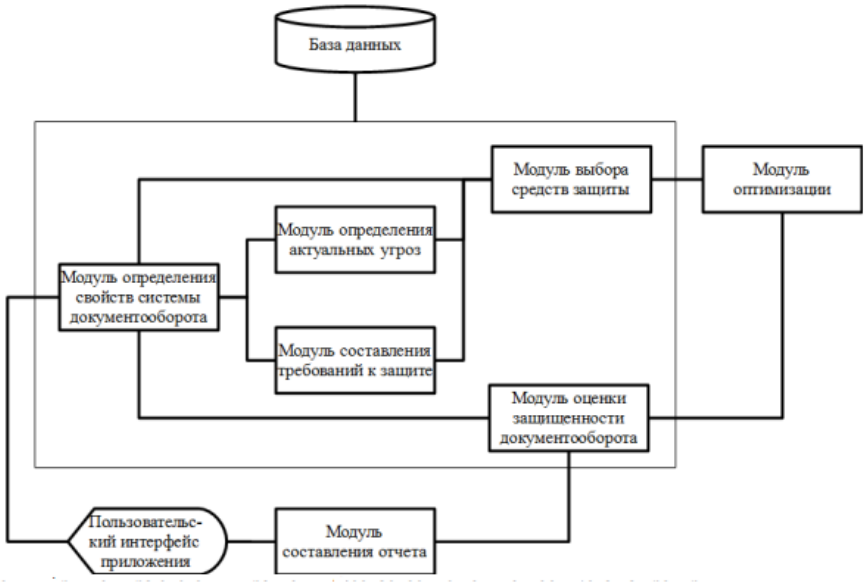

Рисунок 2 – Архитектура СУИБ документооборота

Рисунок 3 – Алгоритм СУИБ документооборота

Рассмотрим особенности решения проблемы информационной безопасности в наиболее популярных зарубежных и отечественных ECM/СЭД.

Как один из наиболее популярных инструментов ECM, Microsoft SharePoint также подвержен нескольким серьезным рискам безопасности контента [34].

Вредоносное ПО представляет собой возможную угрозу, поскольку программное обеспечение используется в веб-среде, а иногда даже на мобильных устройствах.

Однако наиболее распространенные риски безопасности SharePoint включают [37]:

- отсутствие осведомленности о контенте SharePoint;
- неспособность защитить SharePoint от привилегированных внутренних учетных записей;
- недостаточное количество контрольных журналов для использования SharePoint и административного доступа, проблемы с конфигурацией сети, а также плохо настроенные элементы управления доступом и разрешения.

Кроме того, риск сбоя резервного копирования, если его не контролировать должным образом, может привести к серьезным последствиям для предприятия.

Функции безопасности, предоставляемые ECM-системами, можно рассматривать в трех разных областях: люди, процессы и документы.

Инструменты ECM помогают компаниям установить эффективные средства контроля безопасности путем перехода на полностью цифровой формат и предоставления пользователям правил контроля доступа к различным наборам документов, тем самым снижая угрозы безопасности изнутри.

M-Files, один из лучших инструментов ECM, устраняет вероятность потери данных с помощью решения для электронного управления документами и периодически создает резервные копии в безопасном удаленном или локальном месте [23].

Решение M-Files для управления корпоративной информацией (EIM) позволяет совместно использовать и получать доступ к содержимому, гарантируя, что информация предприятия остается в безопасности и защищена.

Системы управления информационной безопасностью ECM обеспечивают безопасное управление документами, аутентификацию документов, целостность и конфиденциальность.

ECM-решения обеспечивают безопасность и безопасность информации с помощью комплексных журналов аудита и методов упреждающей отчетности, поэтому он внедряется для защиты ИТ-инфраструктуры предприятий и документов от утечек данных.

С помощью управления цифровыми правами, цифровой подписи и шифрования с открытым и открытым ключами инструменты ECM ограничивают внешний доступ к содержимому во время создания, управления и доставки информации.

«В СЭД Directum представлены различные механизмы обеспечения безопасности работы с электронными документами:

- обеспечение сохранности документов. Документы в системе Directum располагаются в Централизованном хранилище, в качестве которого может выступать база данных под управлением SQL сервера или файловые хранилища под управлением службы файловых хранилищ Directum. Это обеспечивает безопасное хранение: документ не может быть утерян или уничтожен, так как среда хранения документов полностью контролируется системой Directum, обеспечивается регулярное централизованное резервное копирование базы данных, доступ к данным ограничен только клиентским приложением Directum в соответствии с установленными правами доступа;
- ограничение доступа к данным системы только посредством клиентского приложения и API (объектной модели) системы является одним из важнейших требований к СЭД;
- обеспечение безопасного доступа к электронным документам. Любой пользователь в системе Directum работает под своим именем и паролем. При этом поддерживается возможность использования имени и пароля, с которым пользователь вошел в Windows (так называемая Windows-аутентификация). Это позволяет решить ряд проблем безопасного доступа в СЭД» [2].

В Directum возможно задание прав доступа на каждый документ.

Существует четыре типа прав: права отсутствуют, есть права на просмотр, права на изменение и полные права на документ (рисунок 4).

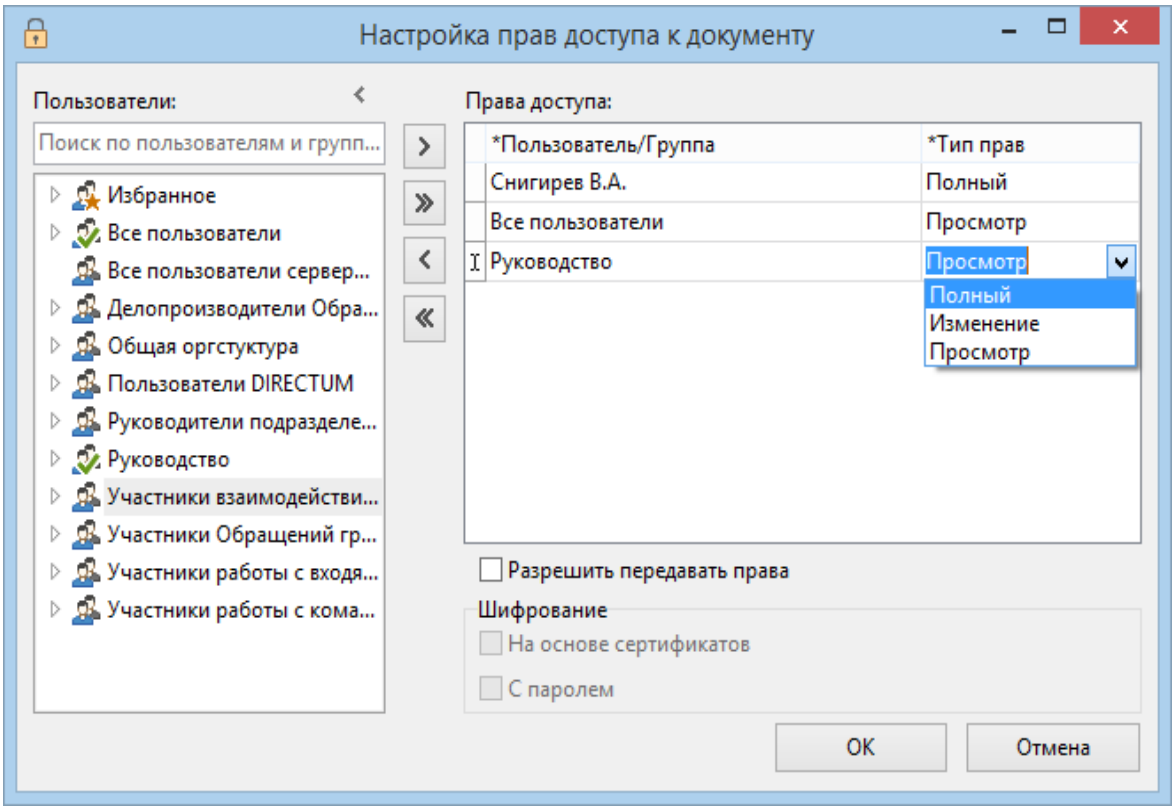

Рисунок 4 – Окно настройки прав доступа пользователей СЭД Directum

Для обеспечения подлинности электронного документа используется ЭЦП.

LanDocs - это российская модульная платформа класса ECM, которая решает весь комплекс задач управления электронными документами территориально-распределенной организации [21].

Структурная схема ECM LanDocs показана на рисунке 5.

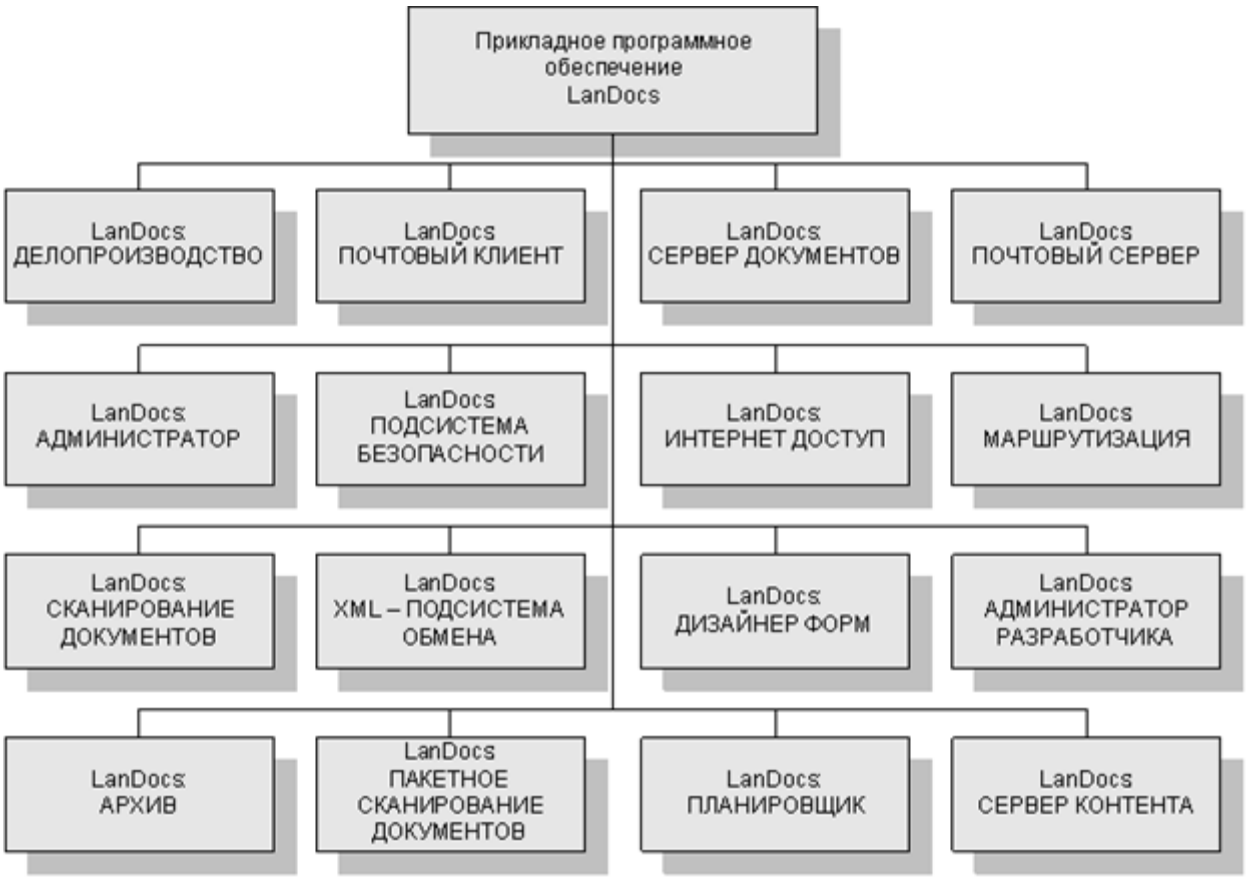

Рисунок 5 – Структурная схема ECM LanDocs

«В целях информационной безопасности LanDocs обеспечивает:

- аутентификацию пользователей при входе в систему (может осуществляться ка к на основе имени и пароля, вводимого пользователем при входе в LanDocs, так и с использованием средств аутентификации операционной системы или с использованием криптографического ключа);
- настраиваемое администратором разграничение прав доступа пользователей к объектам и функциям системы; применение электронной цифровой подписи для подтверждения авторства, целостности документов и придания им юридической значимости;
- шифрование конфиденциальных документов;
- протоколирование и аудит действий пользователей в системе (перечень операций, подлежащих протоколированию, определяется

администратором системы). Система обеспечивает автоматическое протоколирование попыток доступа - к LanDocs в целом, к отдельным функциям, к отдельным документам и к содержанию документов на уровне файлов.

Криптографические средства защиты LanDocs включают в себя интегрированные средства криптозащиты (за это отвечает компонента «Подсистема безопасности»), поддерживающие инфраструктуру открытых ключей (PKI)» [21].

В исследовании [8] на примере программного комплекса «Евфрат-Документооборот» рассмотрены основные принципы и особенности реализации подсистемы управления доступом для защищенных информационных систем (рисунок 6).

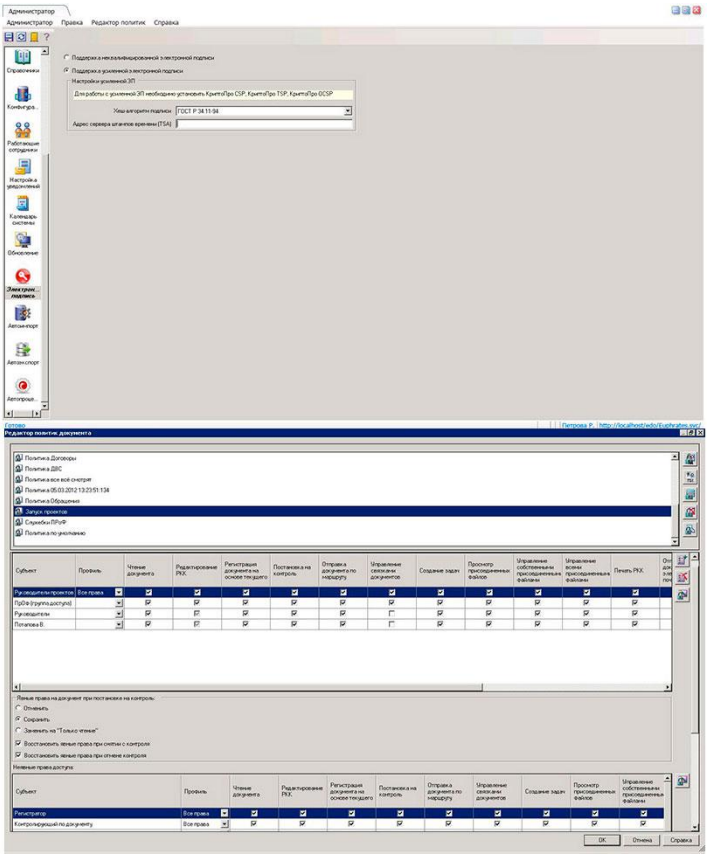

Рисунок 6 – Модуль информационной безопасности СЭД «Е1 Евфрат»

«По мнению разработчиков решения, встроенный в «Евфрат-

Документооборот» модуль информационной безопасности соответствует самым высоким требованиям в области защиты данных.

Модуль обеспечивает комплексную защиту данных и от внешнего, и от внутреннего несанкционированного доступа, а также гарантирует сохранность и целостность документов в случае технических сбоев и аварий.

Система поддерживает использование протокола SSL для шифрования, расширенную квалифицированную электронную подпись КриптоПро и других сертифицированных криптопровайдеров, доменную авторизацию» [26].

В программном продукте (ПП) «1С: Документооборот 8» для обеспечения информационной безопасности используются механизмы разграничения прав пользователей и криптографии [1].

Для разграничения прав пользователей в ПП используется форма «Настройка прав доступа», показанная на рисунке 7.

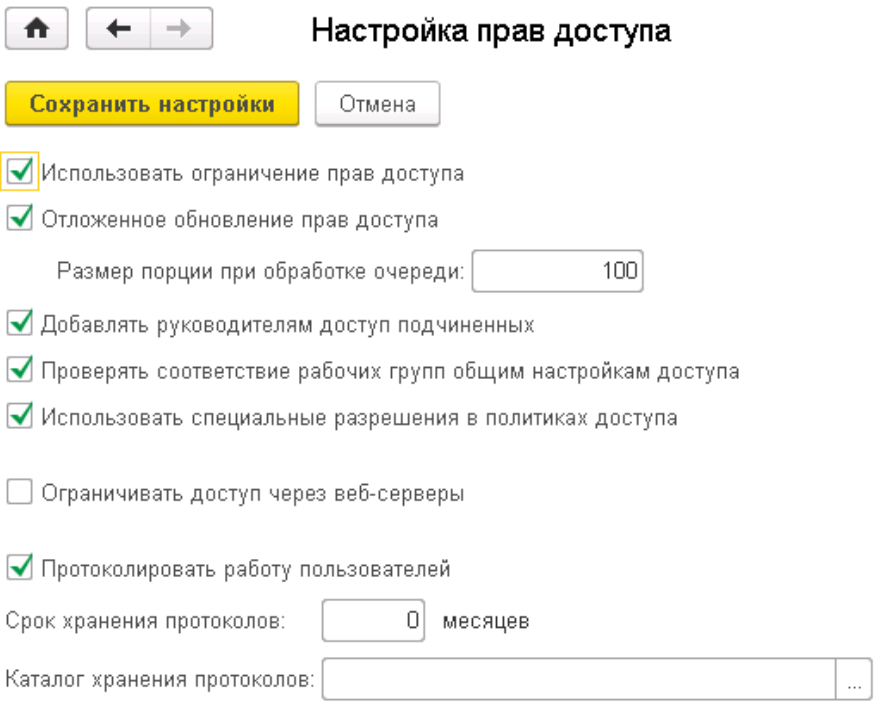

Рисунок 7 – Окно настройки прав доступа пользователей ПП «1С: Документооборот 8»

Одним из основных механизмов является подписание и проверка ЭЦП.

Для обеспечения криптозащиты ЭЦП в системе установлен крипто-провайдер КриптоПро CSP 4.

При подписании документа средствами платформы идет обращение к закрытой части ключа и производится встроенная в платформу проверка целостности (математической валидности) подписи.

Основные криптографические операции выполняются с помощью формы, показанной на рисунке 8.

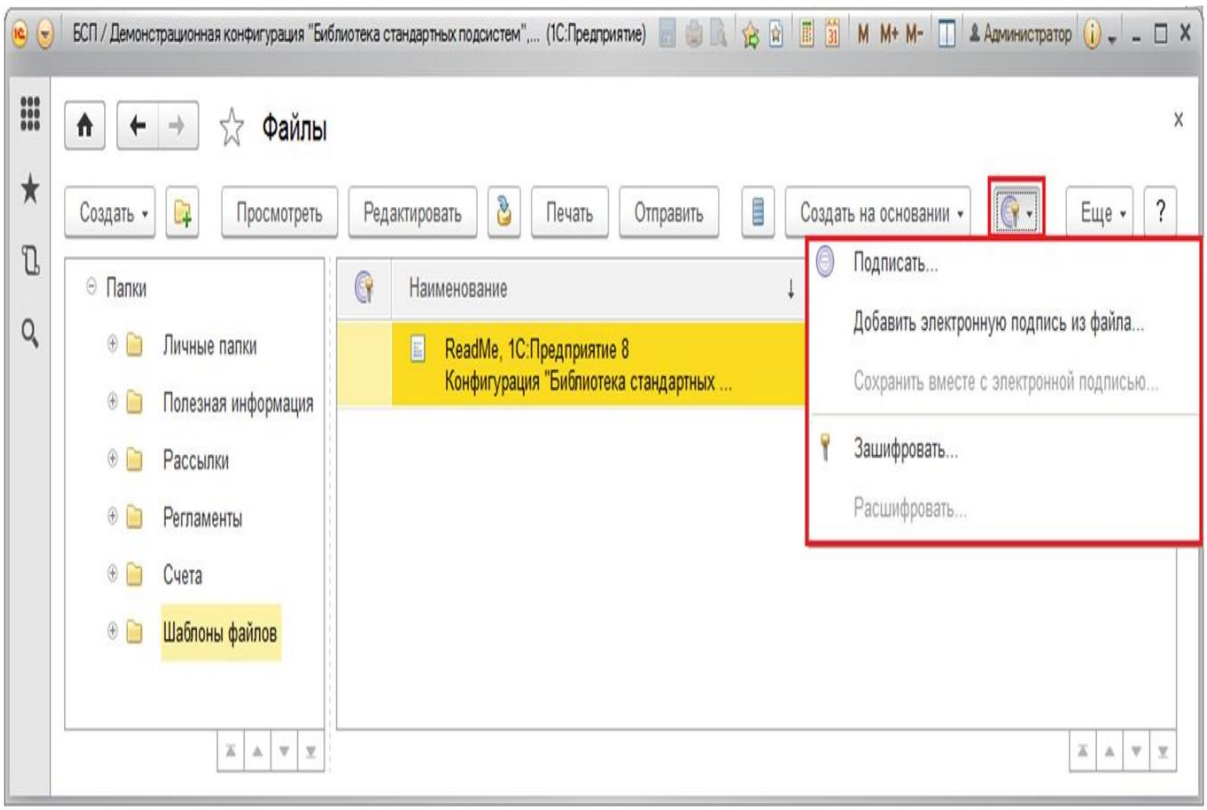

Рисунок 8 – Окно формы основных криптографических операций с документами

В исследовании [27] рассматриваются вопросы защиты информации в системах электронного документооборота.

Рассмотрены основные угрозы СЭД, а также средства защиты от угроз.

В статье приводится сравнение реализации функций защиты информации в отечественных системах электронного документооборота.

Для анализа помимо описанных выше были взяты программные продукты Docsvision, Логика СЭД, «ДЕЛО» и Companymedia.

Результаты анализа возможностей защиты информации в исследуемых СЭД представлены в таблице 1:

«+» – возможность реализована;

«+/−» – возможность доступна в рамках ограниченной функциональности или требуется приобретение дополнительного ПО;

«−» – возможность не реализована.

Таблица 1 – Информационная безопасность СЭД

«Защита информации	1С: ДО 8	ДЕЛО	Directum	Логика СЭД	Docsvision	Евфрат	Companymedia
Поддержка различных способов аутентификации	+	+/–	+	+	+	+/–	+
Назначение прав пользователям	+	+	+	+	+	+	+
Назначение прав группам пользователей	+	+	+	+	+	+	+
Поддержка пользовательских ролей	+	+	+	+	+	+	+
Шифрование данных системы, шифрование данных при передаче	+	+	+	+	+	+	+
Средства мониторинга событий в системе	+/–	+/–	+/–	+	+	+	+
Использование ЭЦП	+	+	+	+	+	+	+/–
Применение сертифицированных средств защиты	+	+	+	+	+	+	+/–
Протоколирование действий пользователя	+	+	+	+	+	+	+

Продолжение таблицы 1

Защита информации	1С: ДО8	ДЕЛО	Directum	Логика СЭД	Docsvision	Евфрат	Companymedia
Организация резервного копирования базы данных	+	+	+	+	+	+	+» [27]

Следует отметить, что проведенный анализ позволил констатировать недостаточность работ, посвященных проблеме разработки моделей и алгоритмов систем управления информационной безопасностью электронного документооборота предприятия, что подтверждает актуальность темы настоящего исследования.

Выводы по главе 1

Результаты проделанной работы позволили сделать следующие выводы:

- угрозы для ECM/СЭД СЭД могут быть внешними и внутренними;
- нормативно-правовая база обеспечения информационной безопасности СЭД основана на ФЗ РФ от 27 июля 2006 г. № 149-ФЗ;
- СУИБ ECM/СЭД обеспечивают безопасное управление документами, аутентификацию документов, целостность и конфиденциальность информации;
- при выборе наилучшей платформы ECM/СЭД для предприятия необходимо учитывать наличие в ней средств реализации основных технических мер защиты информации.

Вместе с тем проведенный анализ позволил констатировать недостаточность работ, посвященных проблеме разработки моделей и алгоритмов СУИБ электронного документооборота организации, что подтверждает актуальность темы настоящего исследования.

Глава 2 Анализ методов и технологий управления информационной безопасностью электронного документооборота предприятий

Как показал анализ специальной литературы, основными методами управления информационной безопасностью электронного документооборота предприятий являются [33]:

- управление правами доступа пользователей;
- шифрование текста документов;
- использование криптографии и ЭЦП;
- регулярное резервное копирование документов;

На рисунке 9 представлена концептуальная модель СУИБ СЭД.

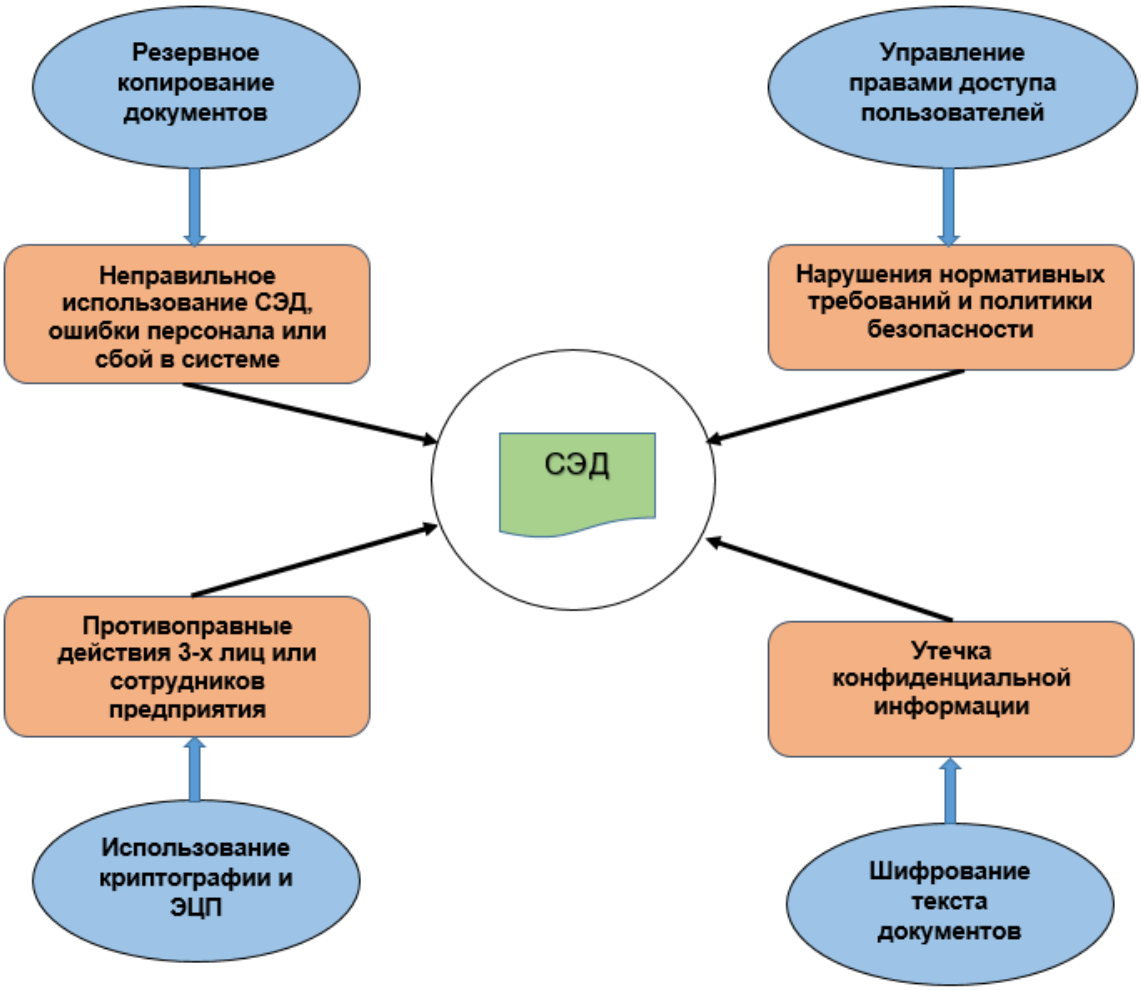

Рисунок 9 – Концептуальная модель СУИБ СЭД

Рассмотрим и проанализируем технологии, используемые для реализации указанных методов.

2.1 Технологии управления правами доступа пользователей

2.1.1 Технология ACL

Технология ACL (Access Control Lists, Списки контроля доступа) используется в ECM IBM Lotus Notus [40].

ACL обеспечивает один из наиболее важных способов контроля и ограничения доступа к данным в любой базе данных Notes.

ACL контролирует доступ к базам данных Notes отовсюду (например, клиенты Notes, веб-браузеры, клиенты POP3 и т. д.). Каждая база данных (БД) Notes имеет свой собственный ACL и, следовательно, позволяет устанавливать индивидуальные ограничения доступа для каждой базы данных сверх ограничений доступа, налагаемых серверным документом.

Каждый ACL содержит:

- имена пользователей, серверов и групп, которым разрешен/запрещен доступ;
- тип разрешения доступа (например, только чтение/автор/дизайнер и т. д.);
- тип пользователя (например, пользователь, сервер или группа);
- журнал всех изменений ACL, сделанных до настоящего времени;
- возможность добавлять/удалять/переименовывать различные роли;
- имя сервера администрирования для ACL/БД (рисунок 10);
- уровень доступа, разрешенный пользователям Интернета.

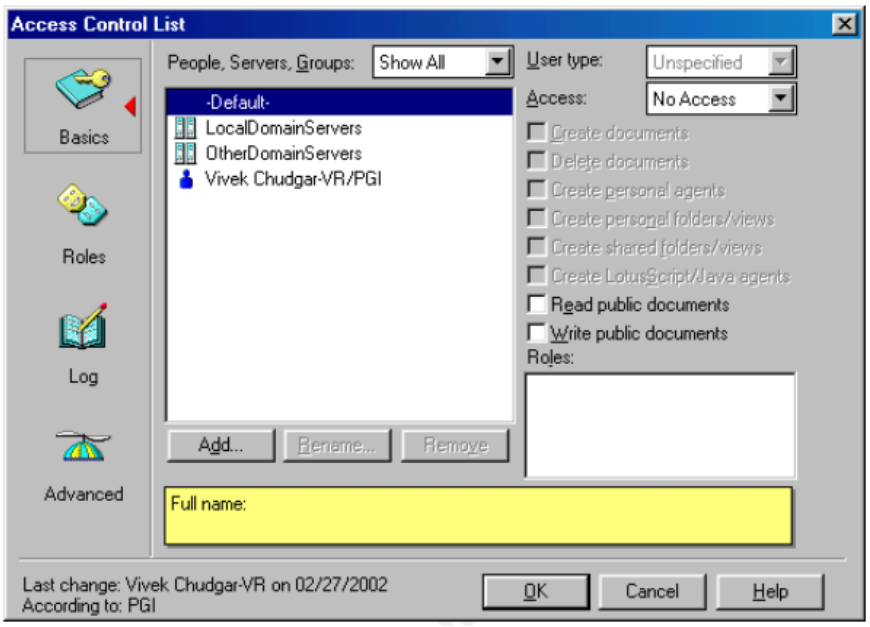

Рисунок 10 – Окно ACL

ACL допускает 7 различных уровней доступа к БД. Самый строгий — «Нет доступа», а наименее строгий — «Менеджер».

Доступ менеджера очень важен, поскольку он позволяет пользователю редактировать данные, вносить изменения в дизайн, а также изменять ACL для базы данных.

Уровень доступа для пользователей Интернета: обслуживание любых данных в Интернете увеличивает их уязвимость, и, следовательно, Notes предоставляет возможность переопределения и, таким образом, ограничения уровня доступа для любого пользователя, когда он получает доступ к информации из Интернета. Например, если для этого поля установлено значение «Доступ редактора», то даже Пользователь с доступом менеджера получит действующие права Редактора, когда он получает доступ к БД из веб-браузера.

Ограничение ACL заключается в том, что для его применения необходим Notes Server.

Это означает, что для любой БД, которая копируется локально, ACL неэффективен. Однако для защиты баз данных в такой ситуации доступны

другие механизмы.

2.1.2 Технология управления доступом платформы «1С: Предприятие 8»

В платформе «1С: Предприятие 8» (далее – 1С8) функция управления доступом реализована в рамках подсистемы «Управление доступом» из состава БСП [18].

Видами доступа могут быть любые объекты системы, по значениям которых можно выполнить отбор. В качестве видов доступа могут выступать:

- отдельные объекты: организации, склады, подразделения, кассы и т.д.;
- группы объектов: группы контрагентов, группы номенклатуры, группы физических лиц;
- составные объекты (группы объектов и объекты) – пользователи, внешние пользователи.

Общая схема назначения прав доступа подсистемы показана на рисунке 11.

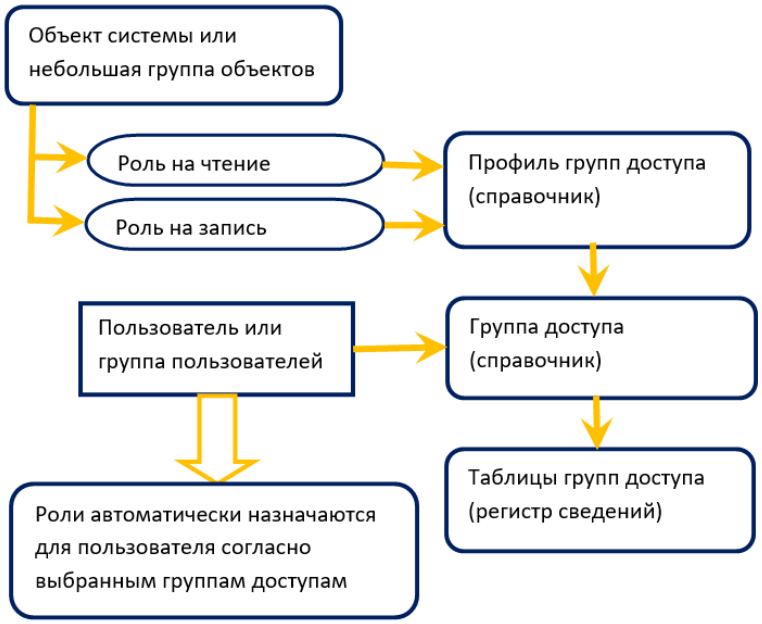

Рисунок 11 – Общая схема назначения прав доступа 1С8

«Элементы справочника «Профили групп пользователей» содержат наборы ролей конфигурации. Точнее, наборы ссылок на элементы справочников: «Идентификаторы объектов метаданных» и «Идентификаторы объектов расширений», описывающие роли, заданные в конфигураторе.

Элементы справочника «Группы доступа» служат для привязки профиля к конкретным пользователям или группам пользователей. Группы доступа, так же, как и профили содержат наборы видов и значений доступа, для ограничения прав на уровне записей.

Существуют обязательные виды доступа: «Пользователи» и «Внешние пользователи». Причем, в состав разрешенных значений, текущий пользователь или текущий внешний пользователь включается автоматически» [18].

Остальные виды доступа, доступные для системы, описываются непосредственно в каждой конфигурации, созданной на базе БСП, в процедуре общего модуля «УправлениеДоступомПереопределяемый >> ПриЗаполненииВидовДоступа».

Для хранения значений видов доступа, в системе применяются специальные регистры сведений. По данным этих регистров происходит обор записей в типовых шаблонах ограничения прав на уровне записей.

Следует отметить, что всю настройку прав доступа необходимо выполнять в пользовательском режиме 1С8.

2.2 Технологии шифрования документов и электронно-цифровой подписи

Средство криптографической защиты информации (СКЗИ) — это программа или устройство, которое шифрует документы и генерирует ЭЦП.

Все операции производятся с помощью ключа электронной подписи, который невозможно подобрать вручную, так как он представляет собой сложный набор символов. Тем самым обеспечивается надежная защита

информации [29].

Процесс функционирования СКЗИ показан на рисунке 12.

Рисунок 12 – Процесс функционирования СКЗИ

В России при работе с ЭЦП в качестве устанавливаемого СКЗИ чаще всего используется криптопровайдер КриптоПро CSP. Программа работает в Windows, Unix и других операционных системах, поддерживает отечественные стандарты безопасности ГОСТ Р 34.11-2012 и ГОСТ Р 34.10-2012.

2.2.1 Технология шифрования ECM Lotus Notus

В ECM Lotus Notus шифрование баз данных обеспечивает дополнительный уровень безопасности, поскольку ACL не применяется к локальным базам данных.

Его также можно использовать для защиты БД, размещенных на сервере, однако в основном он используется для защиты локальных баз данных. Для этого используется шифрование с симметричным ключом, при котором генерируется случайный ключ шифрования и используется для шифрования БД. Затем этот ключ шифруется открытым ключом пользователя и

прикрепляется к БД.

Функция шифрования на уровне документа позволяет шифровать отдельные документы с помощью секретных ключей шифрования (сгенерированных вами или предоставленных кем-то другим).

Только пользователи, у которых есть этот конкретный секретный ключ шифрования в их идентификационном файле, могут получить доступ к этим документам. Следовательно, если пользователь сгенерирует секретный ключ шифрования, никто другой не сможет получить доступ к этому документу, если не предоставить ключ шифрования другим.

Чтобы зашифровать документ, используется форма, показанная на рисунке 13.

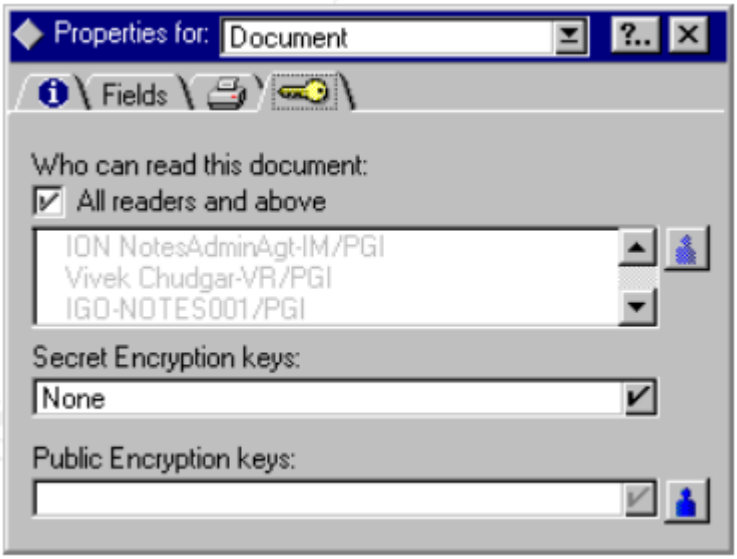

Рисунок 13 – Окно шифрования документа Lotus Notus

Следует учесть, что можно зашифровать документ, используя чей-то открытый ключ, доступный в пользовательской адресной книге (или каталоге Domino). Это ограничило бы доступ к документу только этому пользователю, поскольку теперь документ можно расшифровать только с помощью закрытого ключа этого пользователя.

Шифрование на уровне документа — мощная опция. Однако Notes не

предоставляет инструментов для совместного шифрования нескольких документов. Это означает, что нужно индивидуально шифровать каждый документ один за другим.

Это серьезно ограничивает простоту использования, и, следовательно, очень немногие пользователи действительно решают использовать эту функцию.

Для формирования и проверки ЭЦП в ECM Lotus Notus используется усовершенствованная версия алгоритма RSA, схема работы которого показана на рисунке 14.

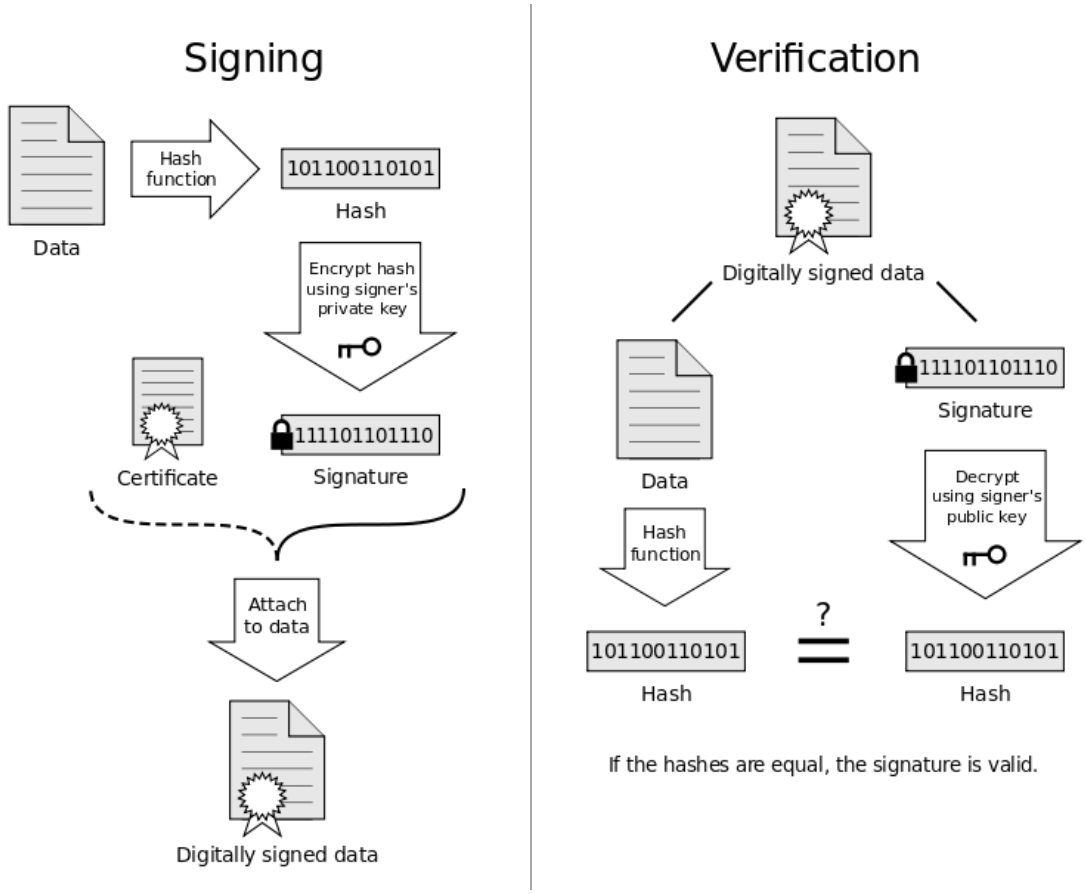

Рисунок 14 – Схема работы алгоритма RSA

Для создания открытых и закрытых ключей Note Domino использует криптосистему RSA с двойным ключом и алгоритмы шифрования RC2, RC4 и AES.

Для создания открытого ключа Интернета Domino использует формат сертификата X.509, который представляет собой формат промышленного стандарта, понятный многим приложениям, включая Domino.

Большие ключи обеспечивают более надежную защиту от хакеров. Например, секретный ключ будет сложнее расшифровать на основе открытого.

Кроме того, кому-то будет труднее подделывать криптографические подписи на документах, агентах, формах и электронной почте.

2.2.2 Технология шифрования платформы «1С: Предприятие 8»

Для шифрования данных в 1С8 используется встроенный механизм криптографии.

Механизм криптографии в платформе 1С: Предприятие 8 показан на рисунке 15.

Рисунок 15 – Механизм криптографии в платформе 1С: Предприятие 8

«Механизм криптографии позволяет прикладным решениям использовать криптографические операции для обработки данных, хранящихся в информационной базе.

Механизм криптографии не содержит реализации собственно алгоритмов криптографии. Он обеспечивает набор объектов, позволяющих взаимодействовать с внешними модулями криптографии сторонних производителей – криптопровайдерами.

Для взаимодействия с криптопровайдерами в ОС Windows используется интерфейс CryptoAPI» [12].

Иными словами, криптографию можно применять, только если на компьютере установлено криптосредство. И, с другой стороны, что саму платформу 1С8 не требуется сертифицировать с точки зрения криптографии.

Таким образом прикладные решения могут взаимодействовать с любыми криптопровайдерами, поддерживающими этот криптографический интерфейс.

Для формирования и проверки ЭЦП используются алгоритмы ГОСТ Р 34.10-2012, блок-схемы которых показана на рисунках 16, 17.

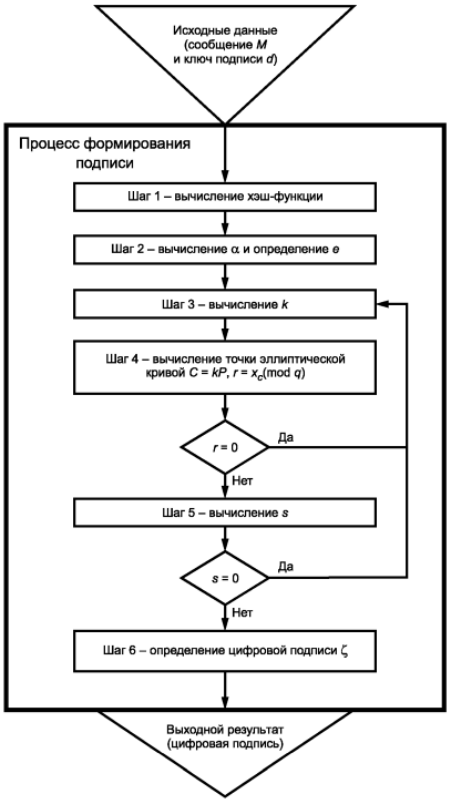

Рисунок 16 – Блок-схема алгоритма формирования ЭЦП

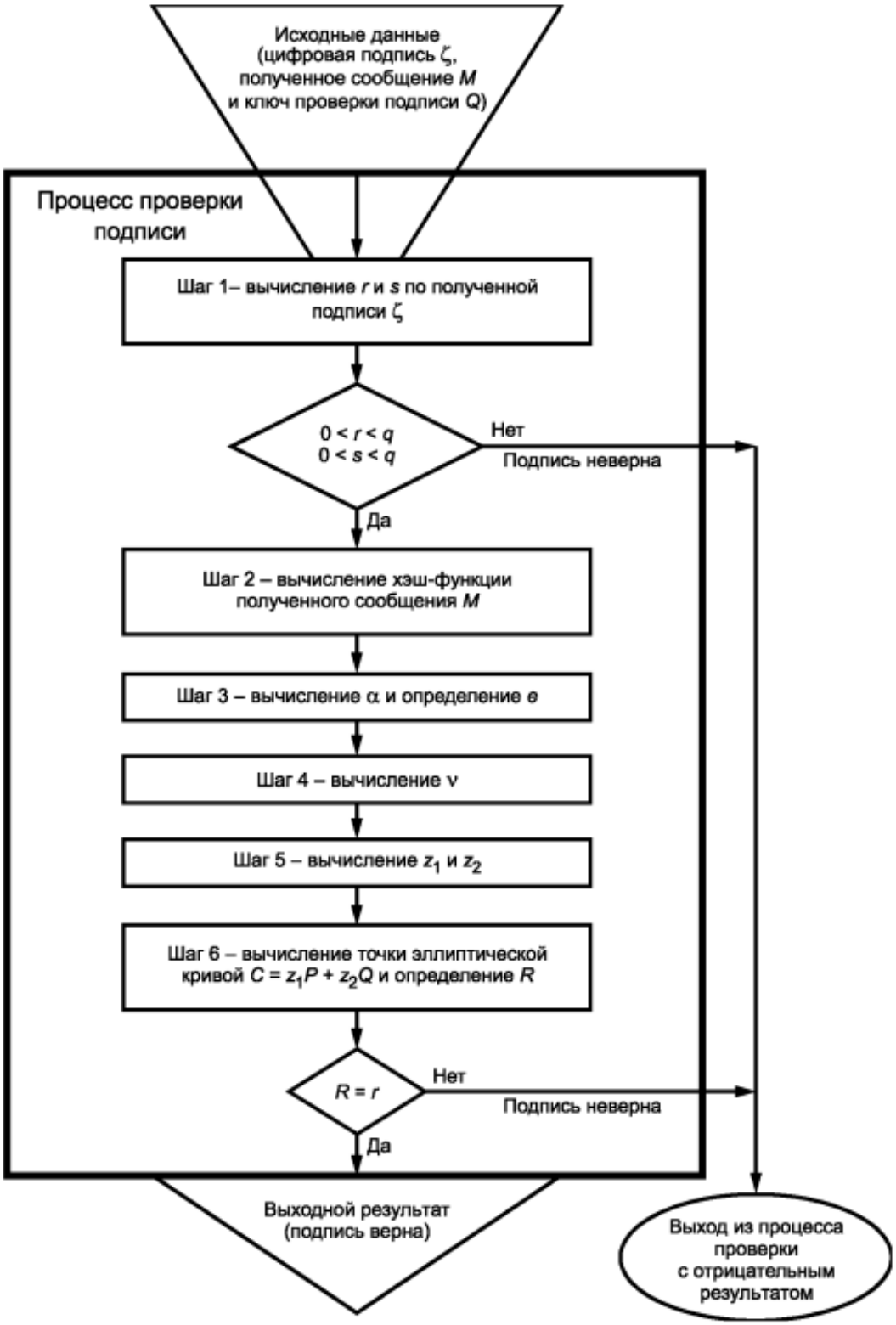

Рисунок 17 – Блок-схема алгоритма проверки ЭЦП

В последнее время для шифрования документов и ЭЦП широкое распространение получил алгоритм шифрования Advanced Encryption Standard (AES) [32].

AES — симметричный алгоритм блочного шифрования (размер блока 128 бит, ключ 128/192/256 бит), принятый в качестве стандарта шифрования правительством США.

Использование данного алгоритма существенно повышает безопасность шифрования.

Схема алгоритма AES показана на рисунке 18.

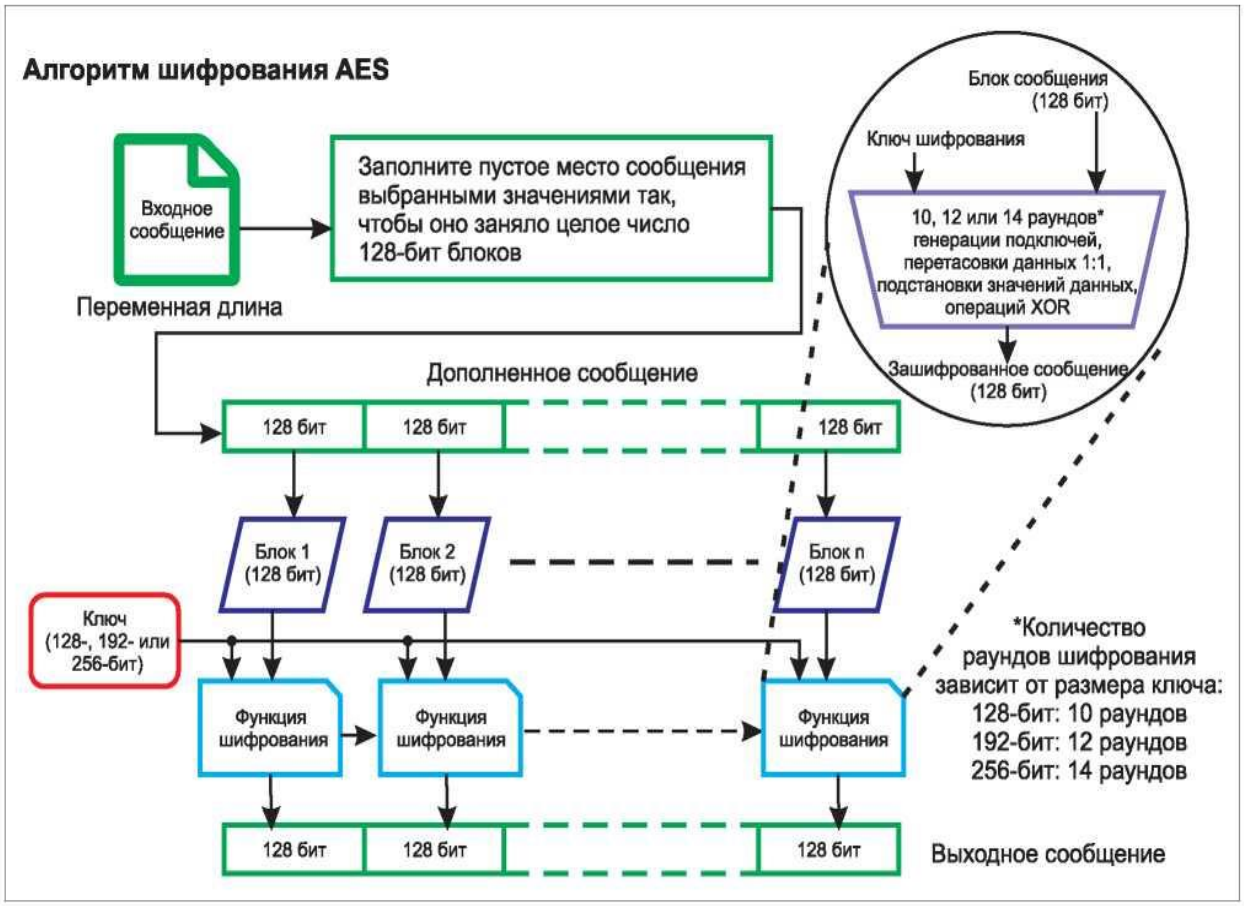

Рисунок 18 – Схема алгоритма AES

Используя мощный алгоритм шифрования AES, можно надежно защитить самые важные файлы.

Как только файл зашифрован, не нужно беспокоиться о том, что кто-то

прочитает конфиденциальную информацию, поскольку зашифрованный файл совершенно бесполезен без пароля. Его просто невозможно прочитать.

2.3 Технология идентификации конфиденциальных документов с помощью интеллектуального анализа данных

Данная технология основа на методе, который состоит из двух этапов: обучения и обнаружения [36].

На этапе обучения документы организации группируются с помощью методов кластеризации и языкового моделирования.

На этапе обнаружения для проверяемого документа рассчитывается конфиденциальная оценка. Если оценка превышает предопределенное пороговое значение, то документ помечается как конфиденциальный.

Рассмотрим указанные этапы подробно.

Целью этапа обучения является представление конфиденциального содержания документа. Это представление должно включать не только конфиденциальные слова и термины, но и контекст, в котором они появляются.

На этапе обучения требуются два набора документов в качестве входных данных.

Первый набор содержит конфиденциальные документы.

Второй - неконфиденциальные документов.

Для каждого документа выполняется токенизация, удаление стоп-слов, затем применение алгоритма поиска корней и, наконец, преобразование их в векторы взвешенных терминов.

Для кластеризации используется неконтролируемый алгоритм K-means с косинусной мерой в качестве функции расстояния.

На рисунке 19 представлена схема этапа обучения.

Рисунок 19 – Схема этапа обучения

Обнаружение ключевых терминов является важным шагом для этого метода.

Ключевые термины используются для следующих целей:

- используются в качестве исходных индикаторов конфиденциального содержания;
- служат основой, вокруг которой генерируются контекстные термины.

Без релевантного и надежного набора ключевых терминов метод, представленный в этой статье, вряд ли будет успешным.

Процесс обнаружения ключевых терминов основан на методе, называемом языковым моделирование. Этот метод представляет значение термина (или последовательности терминов) с точки зрения вероятности.

Контекстные термины используются для следующих целей:

- используются в качестве валидаторов, позволяя определить, действительно ли обнаруженные конфиденциальные термины

указывают на соответствующий контент;

- позволяют количественно оценить степень значимости (много релевантных контекстных терминов = более высокая релевантность для конфиденциального термина);
- они позволяют увидеть, связаны ли обнаруженные ключевые термины, анализируя их общий контекст.

На этапе обнаружения определяется уровень конфиденциальности проверяемого документа.

На рисунке 20 представлена схема этапа обнаружения.

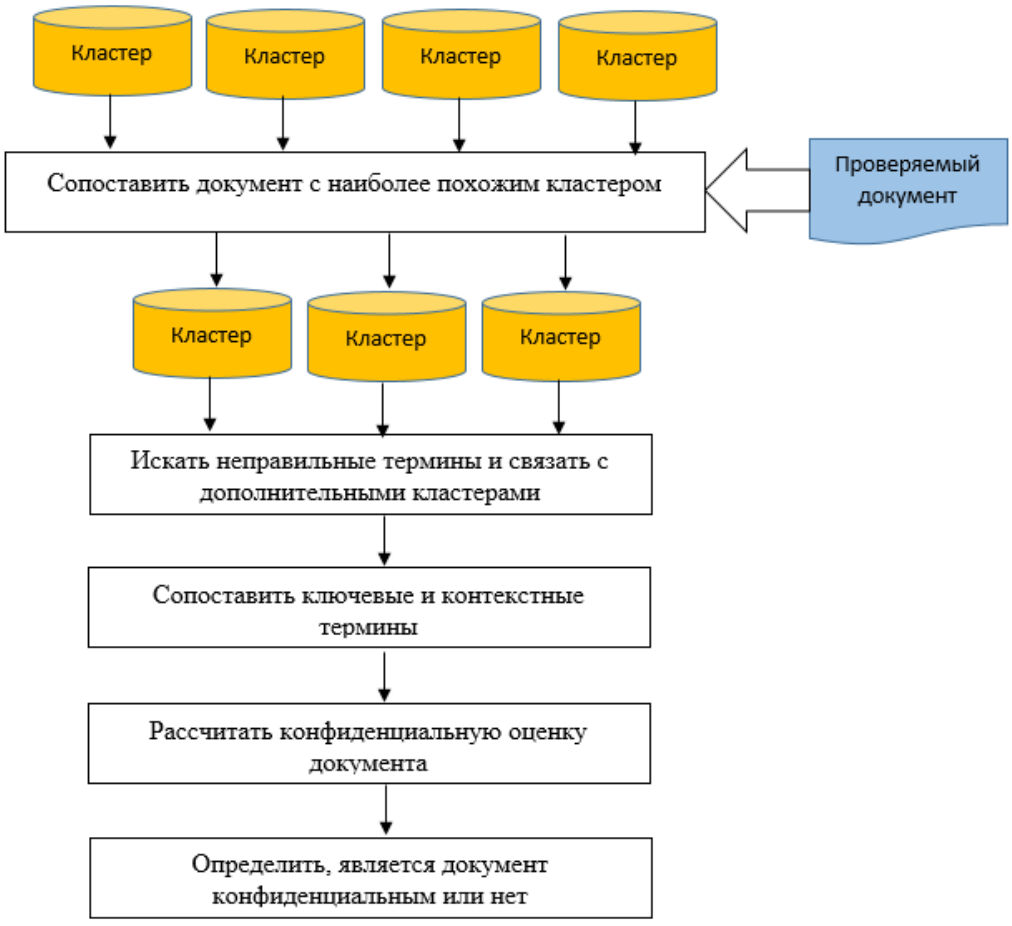

Рисунок 20 – Схема этапа обнаружения

На этапе обнаружения решаются следующие задачи:

- обнаружение полностью конфиденциальных документов

- обнаружение небольших частей конфиденциального текста, встроенных в очень большой неконфиденциальный текст.

Проверяемый документ преобразуется в вектор (после удаления корней и стоп-слов) и находит похожие кластеры. Это делается с помощью меры косинусного расстояния.

Выбираются все кластеры, чье сходство превышает заданный порог.

Как показал анализ, каждая из представленных методов и технологий позволяет решать конкретную задачу по обеспечению информационной безопасности документооборота.

Для разработки надежной СУИБ документооборота рекомендуется использовать комплексный подход, подразумевающий применение всех представленных технологий и решений.

Выводы по главе 2

Основными методами управления информационной безопасностью электронного документооборота предприятий являются:

- управление правами доступа пользователей;
- регулярное резервное копирование документов;
- шифрование текста документов;
- использование ЭЦП.

Как показал анализ, каждые из представленных методов и технологий позволяет решать конкретную задачу по обеспечению информационной безопасности документооборота.

Поэтому для разработки эффективной СУИБ электронного документооборота рекомендуется использовать комплексный подход, подразумевающий применение всех основных методов и технологий их реализации для обеспечения информационной безопасностью.

Глава 3 Разработка моделей и алгоритмов системы управления информационной безопасностью электронного документооборота предприятия

3.1 Моделирование системы управления информационной безопасностью электронного документооборота предприятия

Для разработки эффективной СУИБ СЭД использован комбинированный подход, подразумевающий применение всех основных методов управления информационной безопасностью электронного документооборота.

Для моделирования СУИБ использована методология объектно-ориентированного анализа и моделирования.

В качестве средства моделирования использовано CASE-средство Rational Rose [14].

Для представления функциональной модели СУИБ разработана диаграмма вариантов использования UML.

В результате анализа были выделены следующие акторы СУИБ: Администратор СУИБ, Пользователь СЭД, Криптопровайдер.

Варианты использования СУИБ описаны в таблицах 2-5.

Таблица 2 – Управление пользователями СЭД

«Прецедент: Регистрация/Авторизация
ID: 1
Краткое описание: Администратор СУИБ управляет пользователями СЭД
Главный актор: Администратор СУИБ
Второстепенный актор: Пользователь СЭД
Предусловие: Регистрация/Авторизация Пользователя СЭД
Основной поток: Администратор СУИБ назначает права доступа Пользователю СЭД
Постусловие: нет
Альтернативные потоки: нет» [39]

Таблица 3 – Резервное копирование/восстановление базы данных (БД)

«Прецедент: Резервное копирование БД
ID: 2
Краткое описание: Администратор СУИБ создает или восстанавливает БД СЭД
Главный актор: Администратор СУИБ
Второстепенный актор: нет
Предусловие: нет
Основной поток: Администратор СУИБ выполняет процедуру копирования/восстановления БД СЭД
Постусловие: нет
Альтернативные потоки: нет» [39]

Таблица 4 – Шифрование текста документа

«Прецедент: Шифрование документа
ID: 3
Краткое описание: Пользователь СЭД шифрует текст электронный документ
Главный актор: Пользователь СЭД
Второстепенный актор: Криптопровайдер
Предусловие: нет
Основной поток: Пользователь СЭД под управлением Криптопровайдера выполняет процедуру шифрования текста документа
Постусловие: нет
Альтернативные потоки: нет» [39]

Таблица 5 – Использование ЭЦП

«Прецедент: Использование ЭЦП
ID: 4
Краткое описание: Пользователь СЭД использует ЭЦП для защиты документа
Главный актор: Пользователь СЭД
Второстепенные актор: Криптопровайдер
Предусловие: нет
Основной поток: Пользователь СЭД под управлением Криптопровайдера выполняет процедуру вставки/проверки ЭЦП в документ
Постусловие: нет
Альтернативные потоки: нет» [39]

На рисунке 21 показана функциональная модель СУИБ.

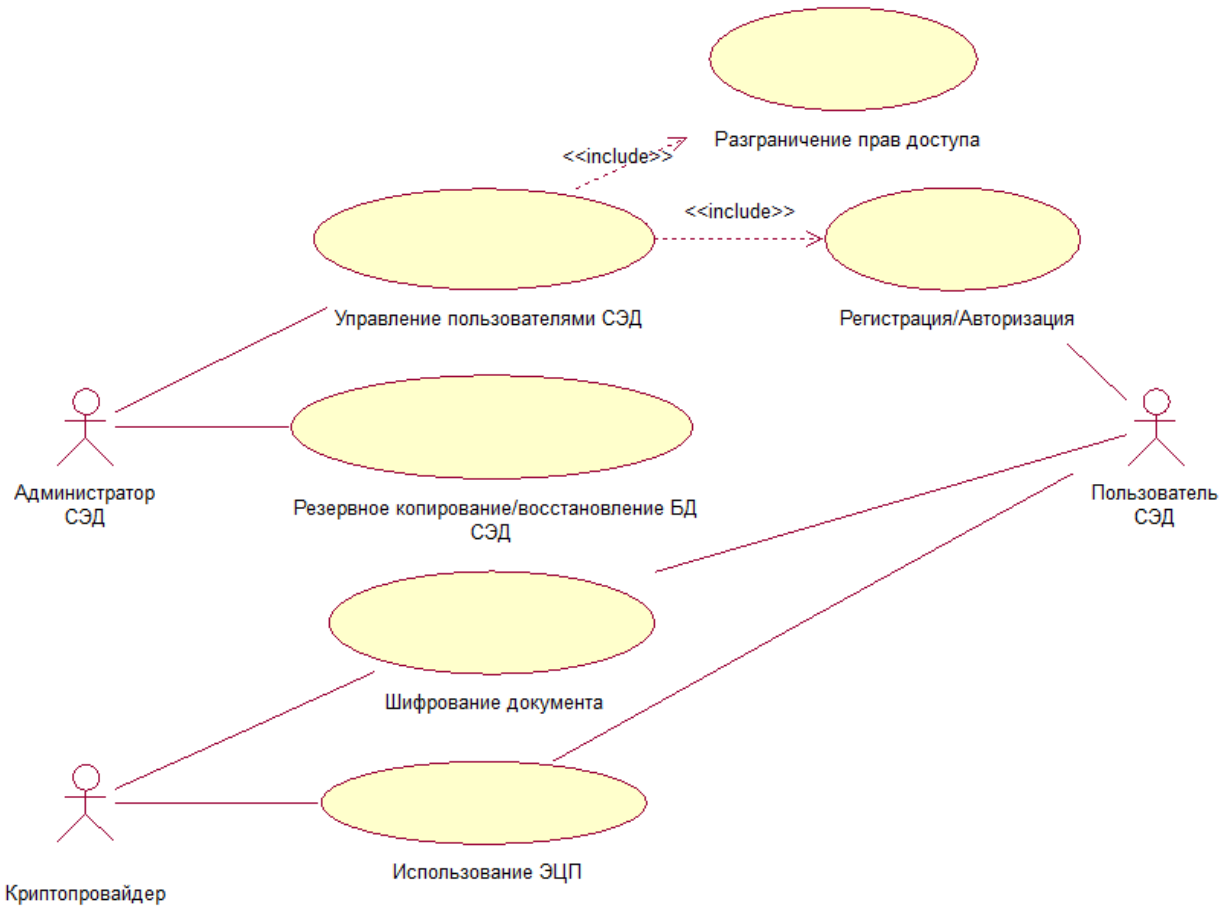

Рисунок 21 – Функциональная модель СУИБ

Для представления архитектуры СУИБ разработана диаграмма компонентов СУИБ.

Диаграммы компонентов используются для визуализации организации компонентов системы и отношений зависимости между ними. Они обеспечивают общее представление о компонентах системы.

Компоненты могут быть программными (база данных, пользовательский интерфейс, модуль) или аппаратными (схема, микросхема или устройство).

Диаграмма компонентов используется, чтобы сосредоточиться на отношениях между компонентами, скрывая детали спецификации.

Это помогает донести и объяснить функции создаваемой системы заинтересованным сторонам.

На рисунке 22 показана компонентная модель СУИБ.

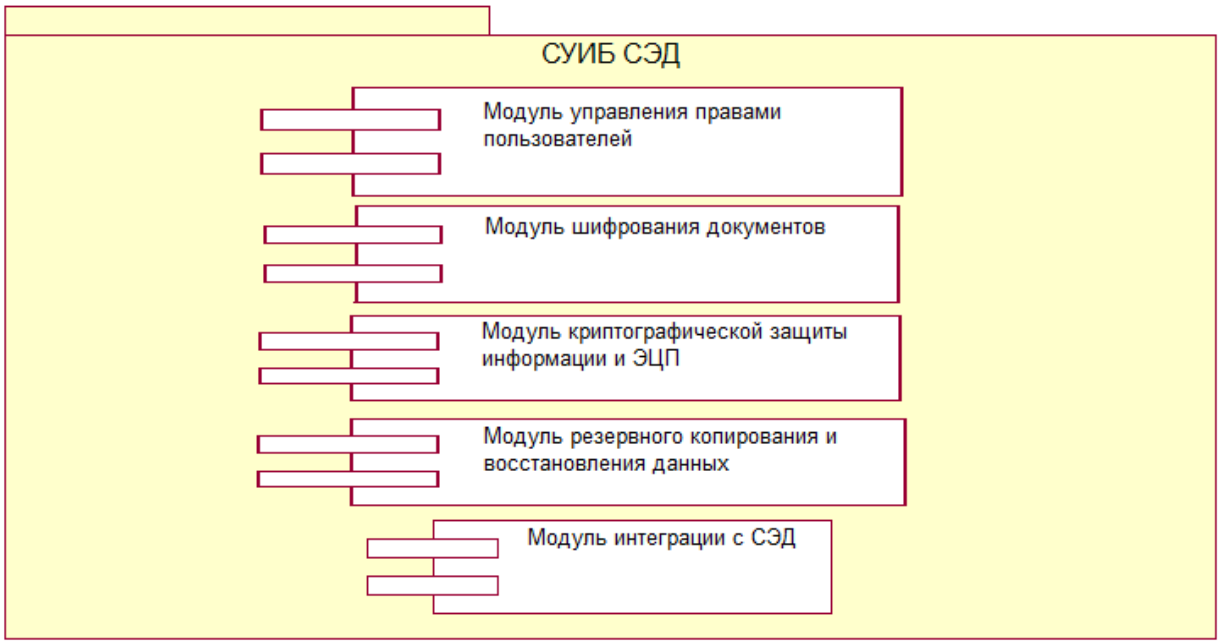

Рисунок 22 – Компонентная модель СУИБ

Представленная компонентная модель является основой для построения эффективной СУИБ электронного документооборота предприятия.

3.2 Алгоритмы системы управления информационной безопасностью электронного документооборота предприятия

3.2.1 Алгоритм процедуры шифрования текста документа

Как показывает практика, основным недостатком метода шифрования текста документов является снижение производительности работы СЭД.

Для решения данной проблемы предлагается использовать алгоритм процедуры шифрования текста документа, блок-схема которого показанна на рисунке 23.

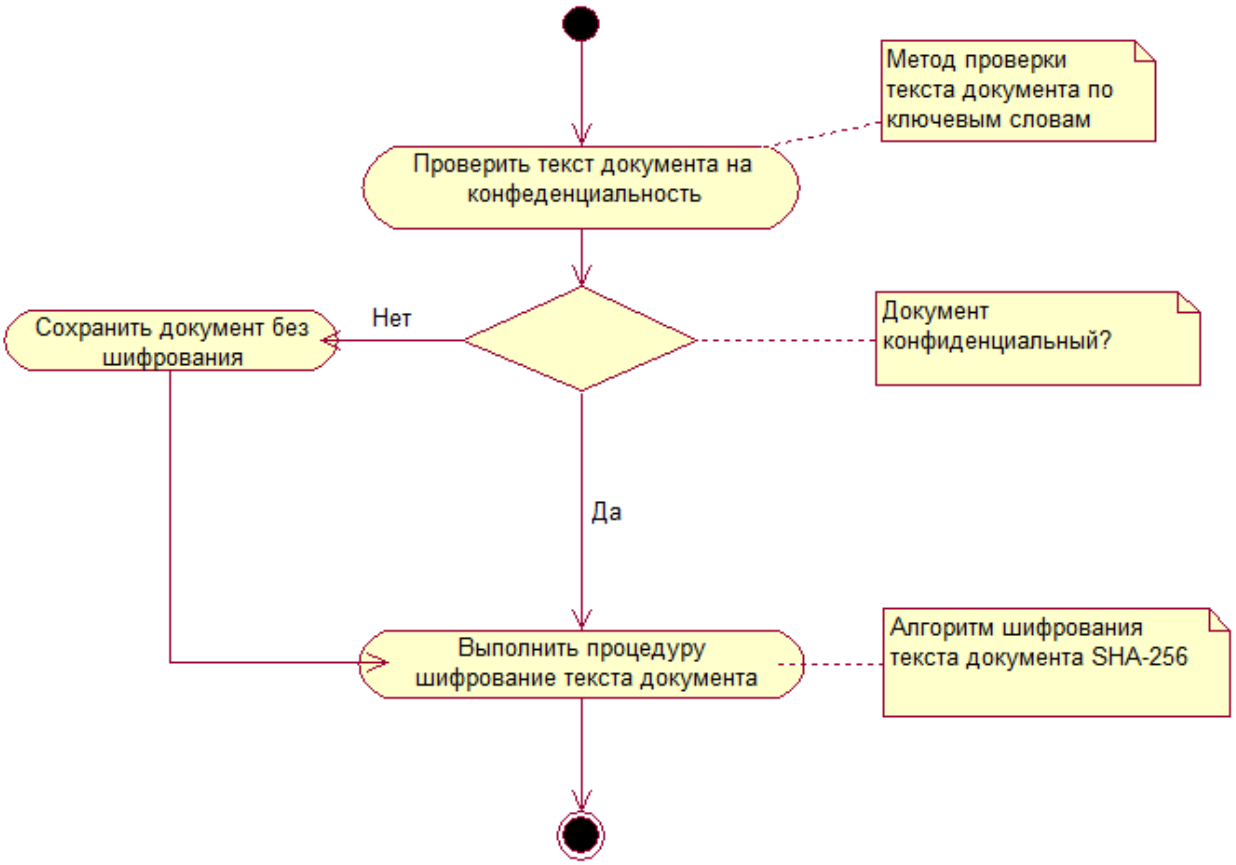

Рисунок 23 – Блок-схема алгоритм процедуры шифрования текста документа

Для проверки текста документа на конфиденциальность предлагается использовать метод, основанный на поиске в тексте соответствующих ключевых слов.

При обнаружении таких ключевых слов выполняется процедура шифрования текста документа.

В противном случае данная процедура не выполняется.

Для шифрования текста документа предлагается использовать хэш-алгоритм SHA-256.

Структурная схема алгоритма SHA-256 представлена на рисунке 24.

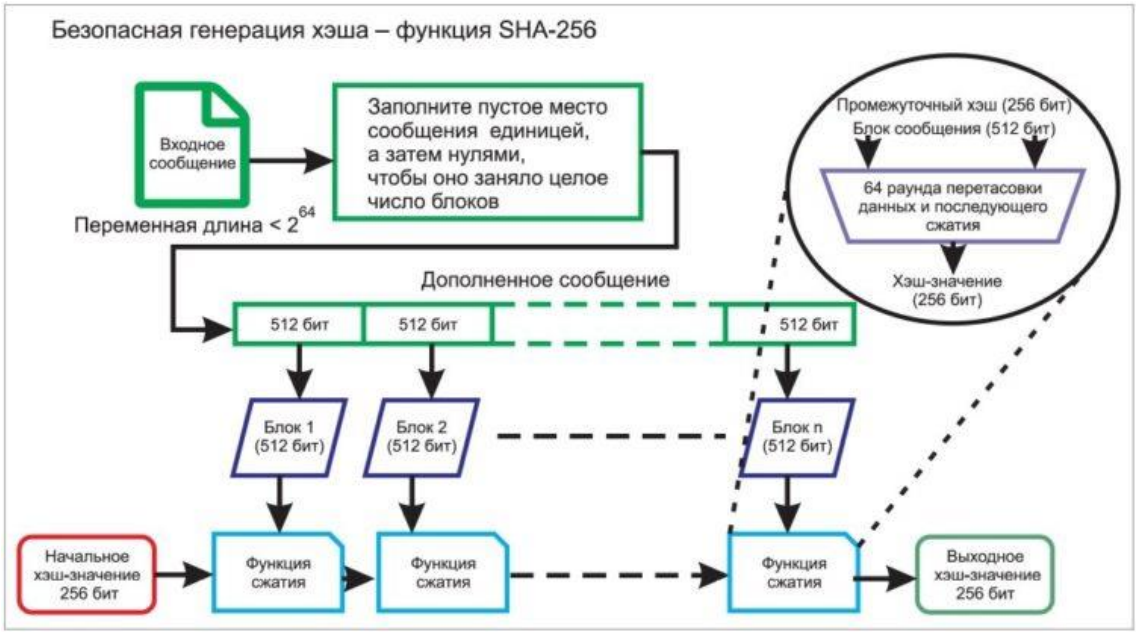

Рисунок 24 – Структурная схема алгоритма SHA-256

SHA-256 — это запатентованная криптографическая хэш-функция, которая выводит значение длиной 256 бит.

«Алгоритм SHA-256 состоит из следующих шагов:

Шаг 1. Добавление заполняющих битов.

Добавляет к сообщению несколько дополнительных битов, так что его длина была ровно на 64 бита меньше числа, кратного 512 (1):

$$M + P + 64 = n \times 512, \quad (1)$$

где M – длина исходного сообщения;

P – добавленные биты.

Биты, которые мы добавляем к сообщению, должны начинаться с «1», а следующие биты должны быть «0».

Шаг 2. Добавление битов длины.

Теперь, когда мы добавили биты заполнения к исходному сообщению, мы можем добавить биты длины, которые эквивалентны 64 битам, ко всему сообщению, чтобы сделать его кратным 512.

Шаг 3. Инициализация буферов.

Необходимо инициализировать значения по умолчанию для восьми буферов, которые будут использоваться в итерациях следующим образом:

a = 0x6a09e667

b = 0xbb67ae85

c = 0x3c6ef372

d = 0xa54ff53a

e = 0x510e527f

f = 0x9b05688c

g = 0x1f83d9ab

h = 0x5be0cd19

Шаг 4. Функция сжатия.

Основная часть алгоритма хеширования заключается в этом шаге.

Весь блок сообщения, который у нас равен «n x 512» бит, делится на «n» фрагментов по 512 бит, и каждый из этих 512 бит затем проходит через 64 итерации, а полученный выход является входом для следующей итерации» [11].

Преимущества:

- это безопасный и надежный отраслевой стандарт, которому доверяют ведущие агентства государственного сектора и который широко используется технологическими лидерами;
- столкновения невероятно маловероятны: существует 2256 возможных хэш-значений при использовании SHA-256, что делает почти невозможным совпадение двух разных документов с одинаковым хеш-значением;
- лавинный эффект: в отличие от некоторых старых алгоритмов хеширования, даже очень незначительное изменение исходной информации полностью меняет значение хеш-функции (так называемый лавинный эффект).

Основная причина, по которой технологические лидеры используют

SHA-256, заключается в том, что он не имеет известных уязвимостей, которые делают его небезопасным, и он не был «сломан», в отличие от некоторых других популярных алгоритмов хеширования.

Следует отметить, что имеется успешный опыт использования данного алгоритма для шифрования текста документов в решениях на платформе 1С8 [31].

3.2.2 Алгоритм реализации ЭЦП

Для реализации надежной ЭЦП предлагается использовать комбинацию алгоритмов SHA-256 и AES [17].

Блок-схема алгоритма представлена на рисунке 25.

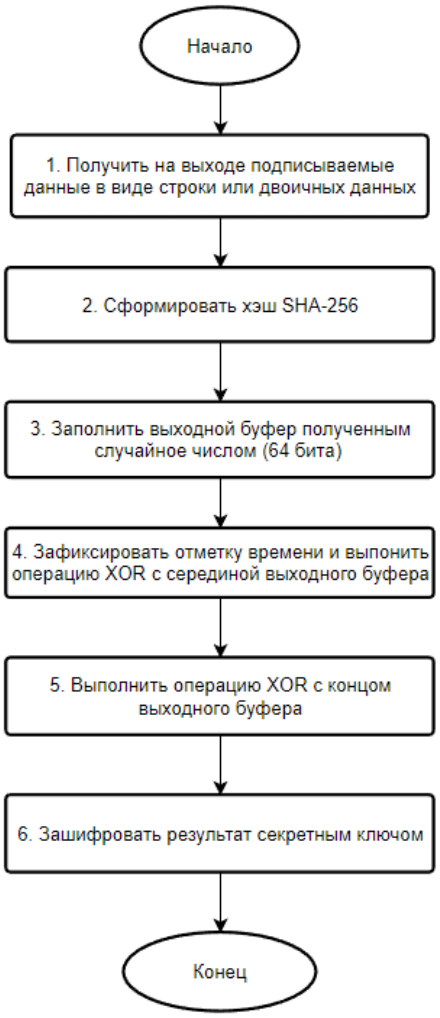

Рисунок 25 – Блок-схема алгоритма реализации ЭЦП методом SHA-256 + AES

Применение предлагаемых моделей и алгоритмов позволит повысить эффективность СУИБ электронного документооборота предприятия.

Выводы по главе 3.

Результаты проделанной работы позволили сделать следующие выводы:

- для разработки эффективной СУИБ СЭД использован комбинированный подход, подразумевающий применение всех основных методов управления информационной безопасностью электронного документооборота;
- как показывает практика, основным недостатком метода шифрования текста документов является снижение производительности работы СЭД. Для решения данной проблемы предлагается использовать алгоритм процедуры шифрования текста документа;
- для проверки текста документа на конфиденциальность предлагается использовать метод, основанный на поиске в тексте соответствующих ключевых слов.

Применение предлагаемых моделей и алгоритмов позволит повысить эффективность СУИБ электронного документооборота предприятия.

Глава 4 Апробация и оценка эффективности проектных решений системы управления информационной безопасностью электронного документооборота предприятия

4.1 Апробация проектных решений

Для апробации предлагаемых проектных решений использовано типовое решение СЭД на платформе 1С8 – «1С: Документооборот 8».

«Программный продукт (ПП) «1С: Документооборот 8» – это система управления документами и современная система с широким набором функциональных возможностей для регулировки деловых процессов и совместной работы сотрудников.

Это типовая конфигурация для автоматизации документооборота на новой платформе 1С8» [1].

На рисунке 26 представлена программная архитектура СЭД.

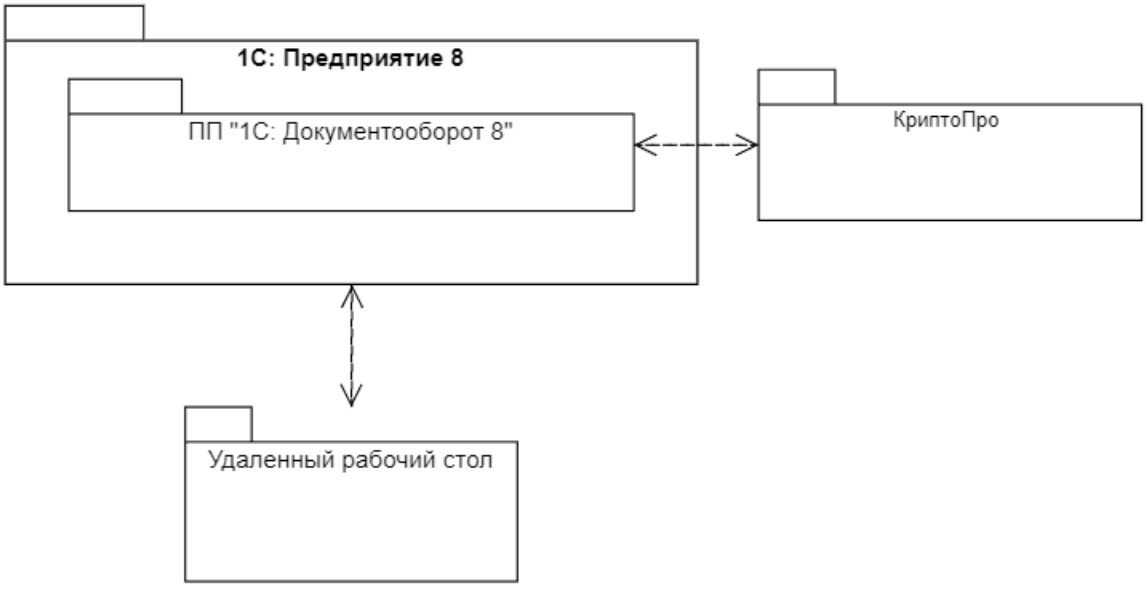

Рисунок 26 – Программная архитектура ПП «1С: Документооборот 8»

Для обеспечения криптозащиты электронных документов использован криптопровайдер КриптоПро [13].

Для представления аппаратно-программной архитектуры СЭД используем диаграмму развертывания UML (рисунок 27).

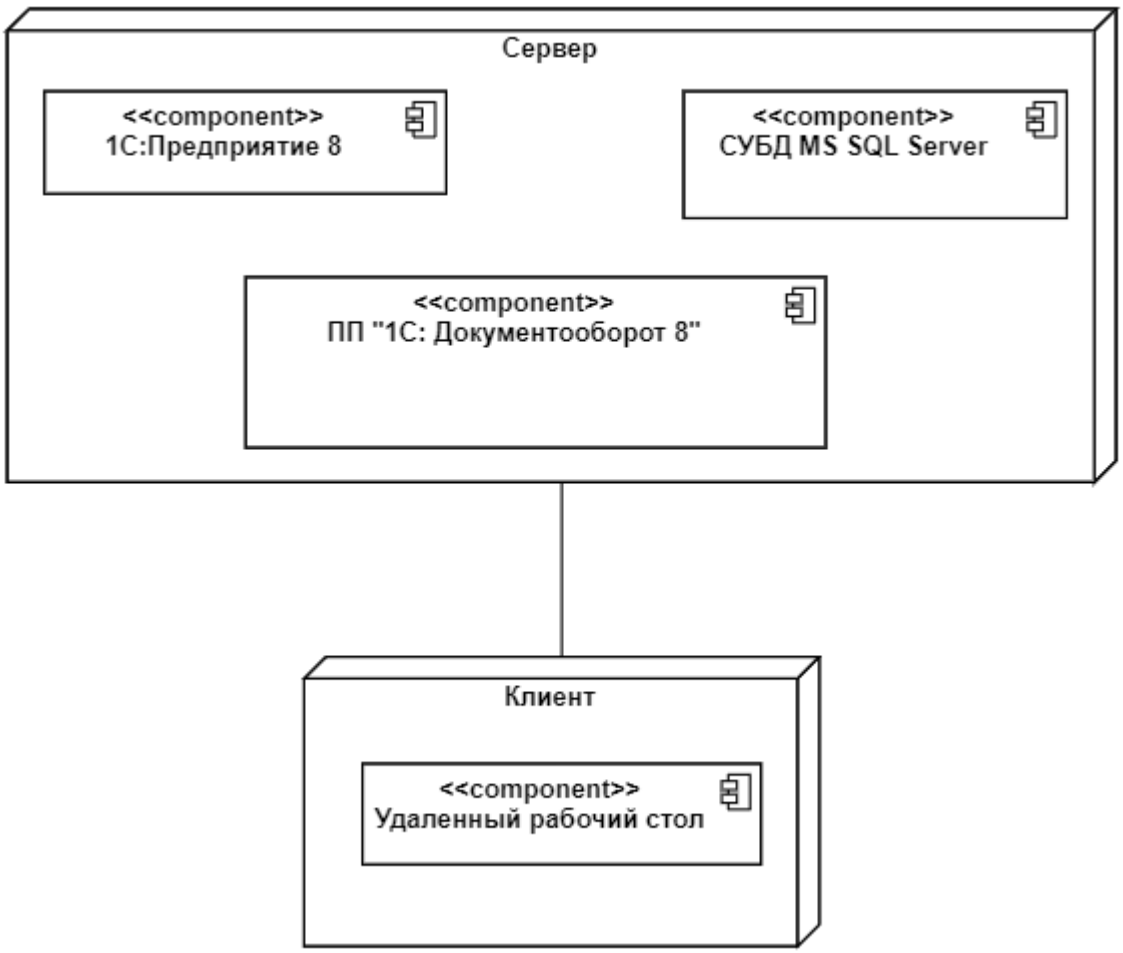

Рисунок 27 – Диаграмма развертывания ПП «1С: Документооборот 8»

Рассмотрим реализацию компонентов СУИБ электронного документооборота в ПП «1С: Документооборот 8».

Для управления правами доступа пользователей используется схема назначения прав доступа ПП, описанная в главе 1.

Полномочия — самое крупное деление прав, базовые настройки. Это готовый набор ролей, определяющий типы данных, которые будут доступны пользователям (рисунок 28).

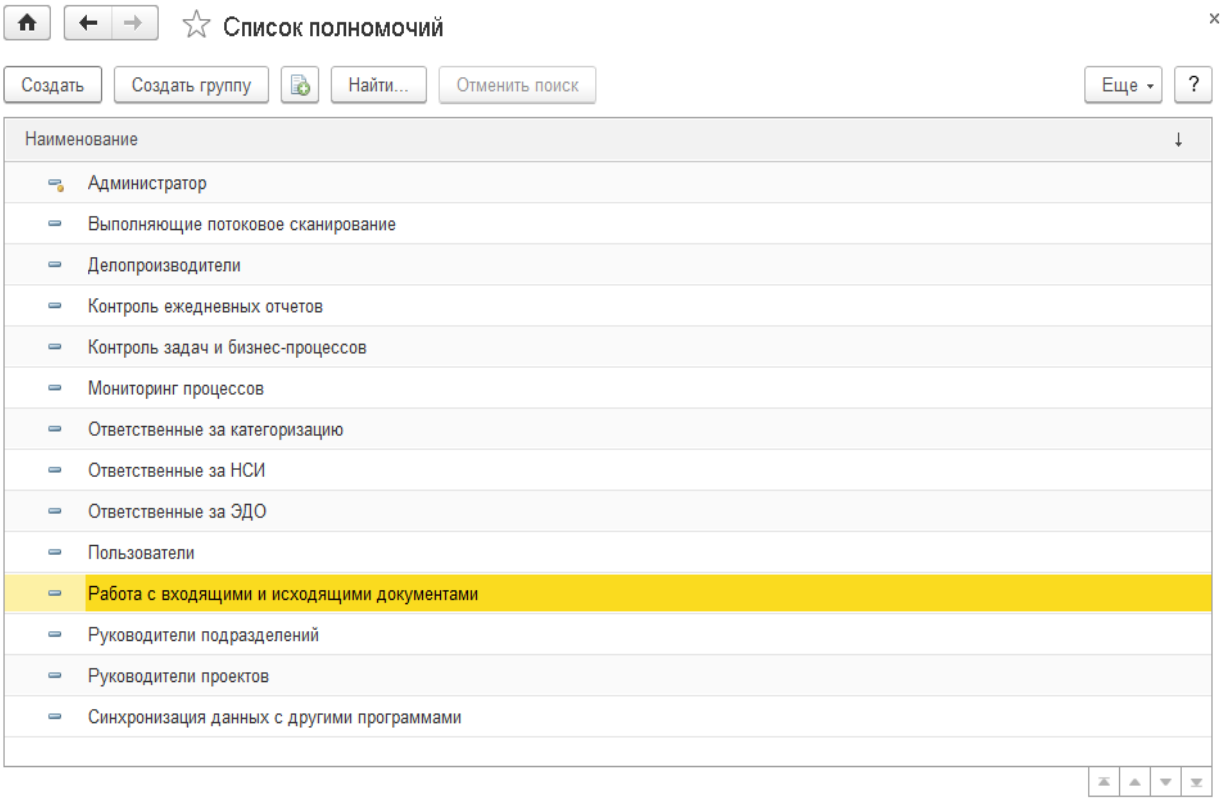

Рисунок 28 – Список полномочий пользователей

«В соответствии с разработанными в организации документами по правам доступа можно задавать политики безопасности.

Действие этих политик распространяются на объекты ПП и могут быть нарушены только рабочими группами объектов (например, если у документа заполнена рабочая группа, то политики перестают действовать).

С помощью политик доступа можно задать как общие настройки прав для рабочих групп и подразделений, так и доступ к определенному виду документа или грифу доступа конкретному пользователю (рисунок 29)» [20].

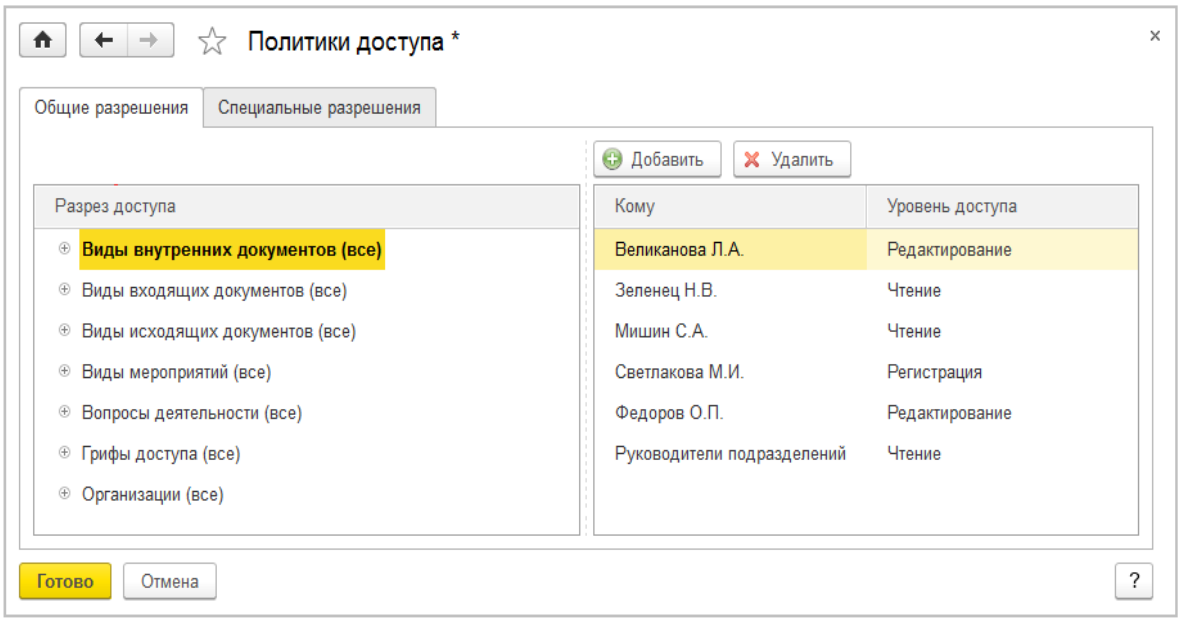

Рисунок 29 – Окно настройки политик доступа

Для управления ЭЦП используется механизм, показанный на рисунке 15. Пример документа с ЭЦП показан на рисунке 30.

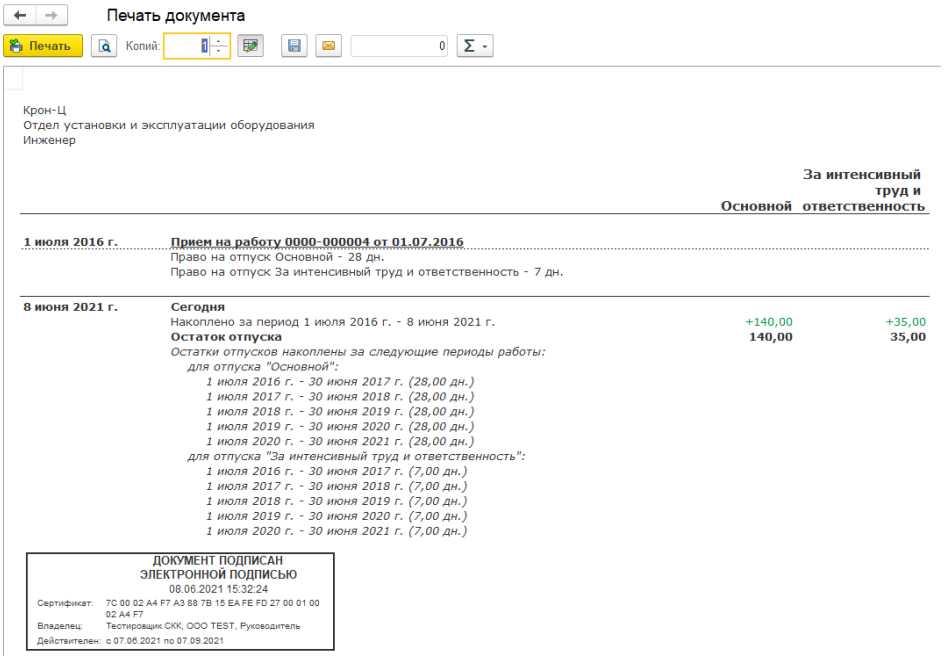

Рисунок 30 – Пример документа с ЭЦП

Файл и электронная подпись присоединяются к объекту, из которого был вызван процесс формирования печатной формы. Для успешного размещения файлов необходима возможность у объекта конфигурации хранить файлы.

Код процедуры визуализации ЭЦП представлен в листинге 1.

Листинг 1 – Код процедуры визуализации ЭЦП

```
«Процедура ВизулизацияЭЦП(Команда)
    // открываем форму настройки положения
    ПараметрыНастроек = Новый Структура;
    ПараметрыНастроек.Вставить("ЗаголовокФормы", НСтр("ru = 'Положение штампа ЭПЦ на странице'"));
    ПараметрыНастроек.Вставить("РежимИспользованияНастроек", 1);
    ПараметрыНастроек.Вставить("ЗапросОриентацииСтраницы", Ложь);
    ОписаниеОповещения = Новый ОписаниеОповещения("ВизуализацияЭЦППродолжение", ЭтотОбъект);
    ШтрихкодированиеКлиент.ПолучитьНастройкиШтрихкода(ПараметрыНастроек, ОписаниеОповещения);
КонецПроцедуры

Процедура ВизуализацияЭЦППродолжение(НастройкиШтрихкода, ДополнительныеПараметры) Экспорт
    ВизуализацияЭЦПКлиент.ПоказатьДокументСЭЦП(ЭтаФорма);
КонецПроцедуры» [6].
```

На рисунке 31 показана форма проверки ЭЦП.

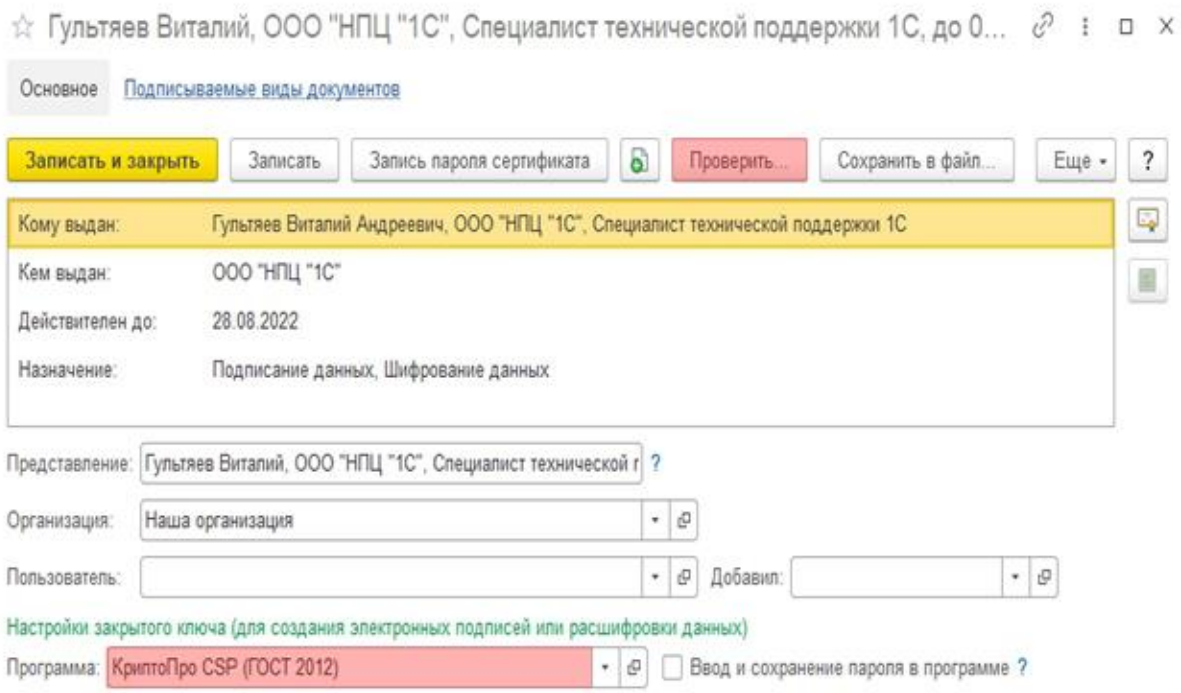

Рисунок 31 – Форма проверки ЭЦП

Для реализации ЭЦП использован алгоритм, описанный в главе 2.

В листинге 2 представлен код 1С8 функции подписи SHA + AES на языке 1С8.

Листинг 2 – Код функции подписи SHA + AES

```
«Функция Подписать(Данные, Ключ256) Экспорт
// Получаем хэш SHA-256
Хеш = Новый ХешированиеДанных(ХешФункция.SHA256);
Хеш.Добавить(Данные);
SHA256 = Хеш.ХешСумма;
ЧтениеХэш      = Новый ЧтениеДанных(SHA256);
БуферХэш       = ЧтениеХэш.ПрочитатьВБуферДвоичныхДанных();
ЧтениеХэш.Закрыть();
```

```
ВремяСозданияАлгоритма = 63739655820000; // Дата("20201030115700") - Дата("00010101") UTC
Сейчас = ТекущаяУниверсальнаяДатаВМиллисекундах() - ВремяСозданияАлгоритма;
ГенераторСлучайныхЧисел = Новый ГенераторСлучайныхЧисел(Сейчас % 4294967295);
Ч1 = ГенераторСлучайныхЧисел.СлучайноеЧисло();
Ч2 = ГенераторСлучайныхЧисел.СлучайноеЧисло();
Буфер = Новый БуферДвоичныхДанных(48);
Буфер.ЗаписатьЦелое32(0, Ч1);
Буфер.ЗаписатьЦелое32(4, Ч2);
Буфер_R = Буфер.Скопировать();
Буфер.ЗаписатьЦелое64(8, Сейчас);
Буфер.Записать(16, БуферХэш, 32);
Буфер.ЗаписатьПобитовоеИсключительноеИли(8, Буфер_R, 8);
Буфер.ЗаписатьПобитовоеИсключительноеИли(16, Буфер_R, 8);
Буфер.ЗаписатьПобитовоеИсключительноеИли(24, Буфер_R, 8);
Буфер.ЗаписатьПобитовоеИсключительноеИли(32, Буфер_R, 8);
Буфер.ЗаписатьПобитовоеИсключительноеИли(40, Буфер_R, 8);
Поток= Новый ПотокВПамяти(Буфер);
ДанныеПодписи= Поток.ЗакрытьИПолучитьДвоичныеДанные();
Возврат ЗашифроватьAES(ДанныеПодписи, Ключ256);
КонецФункции
// Подписать» [17].
```

Для проверки документа на конфиденциальность по ключевым словам предлагается использовать механизм полнотекстового поиска в БД 1С8 [19].

Механизм полнотекстового поиска в данных системы 1С8 позволяет осуществлять поиск в базе данных с указанием поисковых операторов (И, ИЛИ, НЕ, РЯДОМ и др.).

Механизм полнотекстового поиска основан на использовании двух составляющих:

- полнотекстового индекса, который создается для текущей базы данных и затем периодически, по мере необходимости, обновляется;
- средств выполнения полнотекстового поиска.

Создание и обновление полнотекстового индекса может быть выполнено интерактивно, в режиме 1С8, или программно, средствами встроенного языка.

На рисунке 32 показана форма управления полнотекстовым индексированием в режиме 1С8.

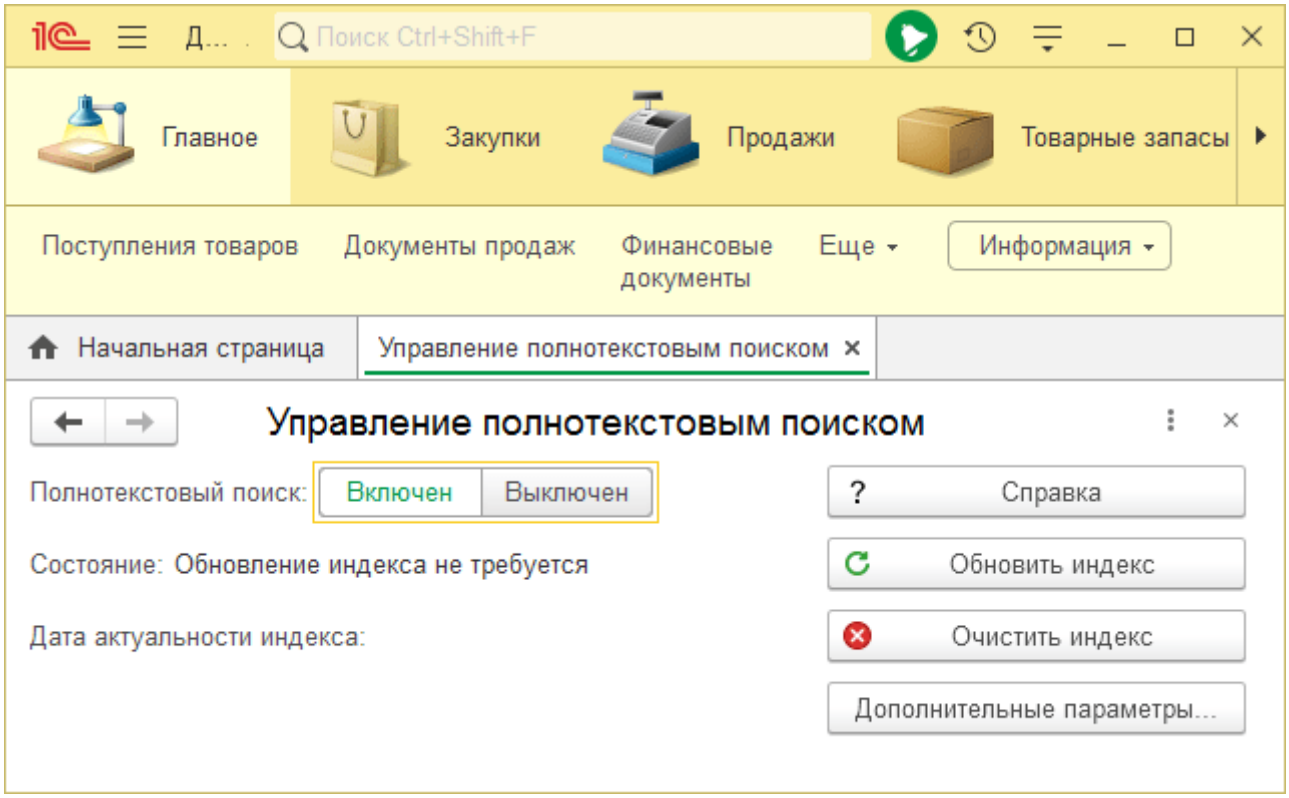

Рисунок 32 – Форма управления полнотекстовым индексированием в режиме 1С8

На рисунке 33 показано окно поиска конфиденциальной информации.

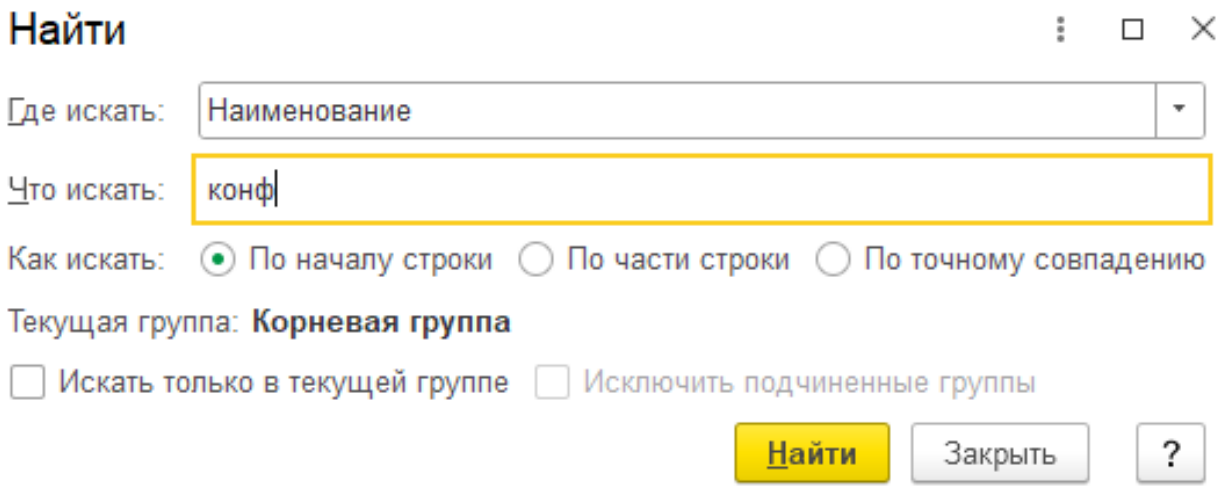

Рисунок 33 – Окно поиска конфиденциальной информации

Также можно использовать собственную обработку проверки текста на конфиденциальность, разработанную средствами встроенного языка 1С8 [25].

Для управления процессом резервного копирования предлагается использовать модуль менеджера резервного копирования [15].

Для автоматического резервного копирования и рассылки статуса необходимо, чтобы база была развернута в клиент-серверном варианте. В случае использования в файловом варианте один сеанс постоянно должен быть запущен [22].

Для развертывания модуля требуется платформа 1С 8.3.10 и выше, архиватор 7zip.

На рисунках 34-36 показаны скриншоты работы менеджера резервного копирования.

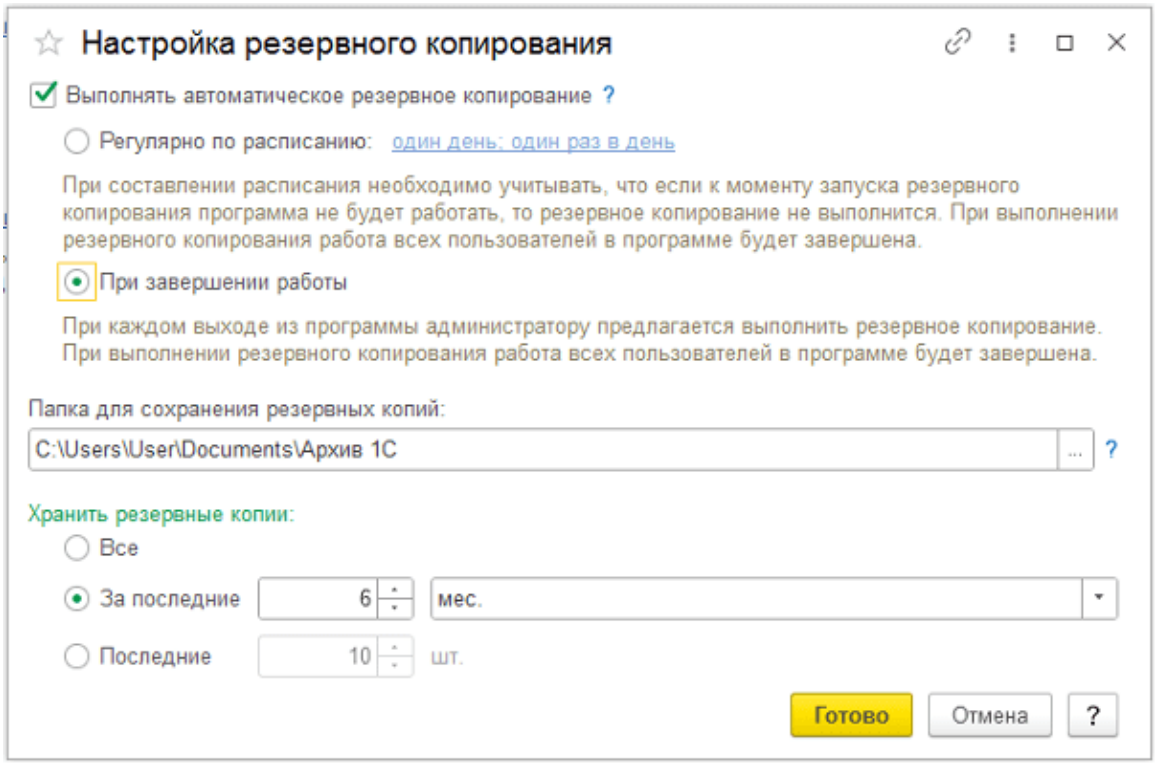

Рисунок 34 – Окно настройки режима резервного копирования

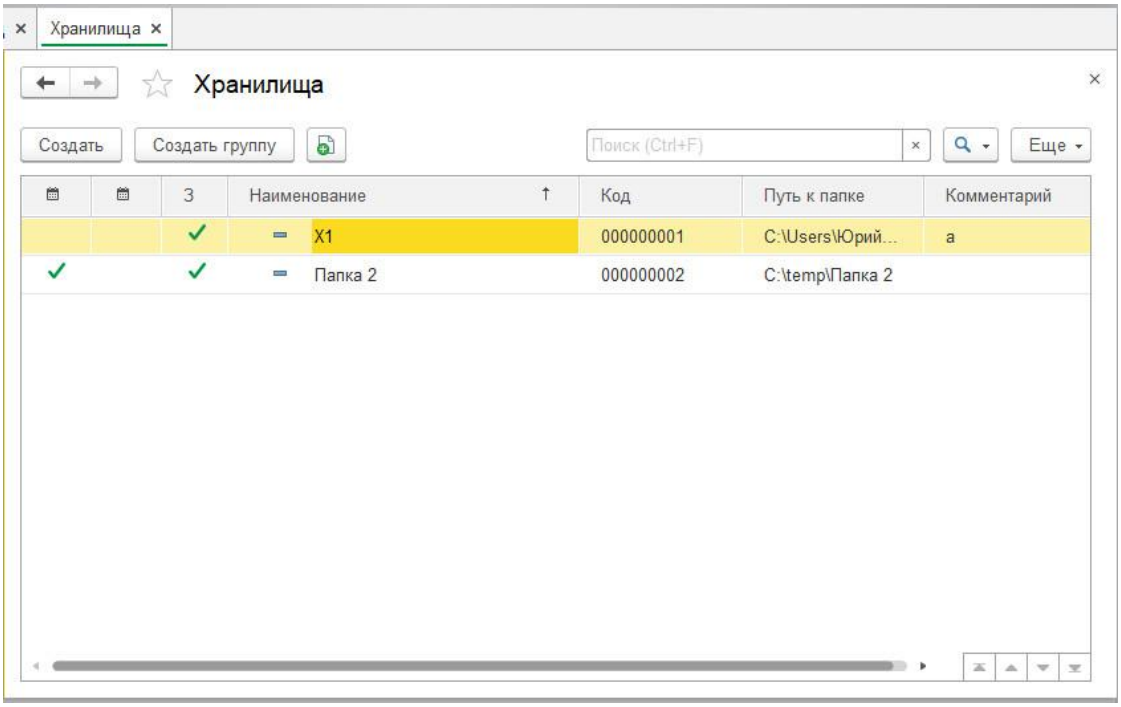

Рисунок 35 – Окно просмотра хранилища данных

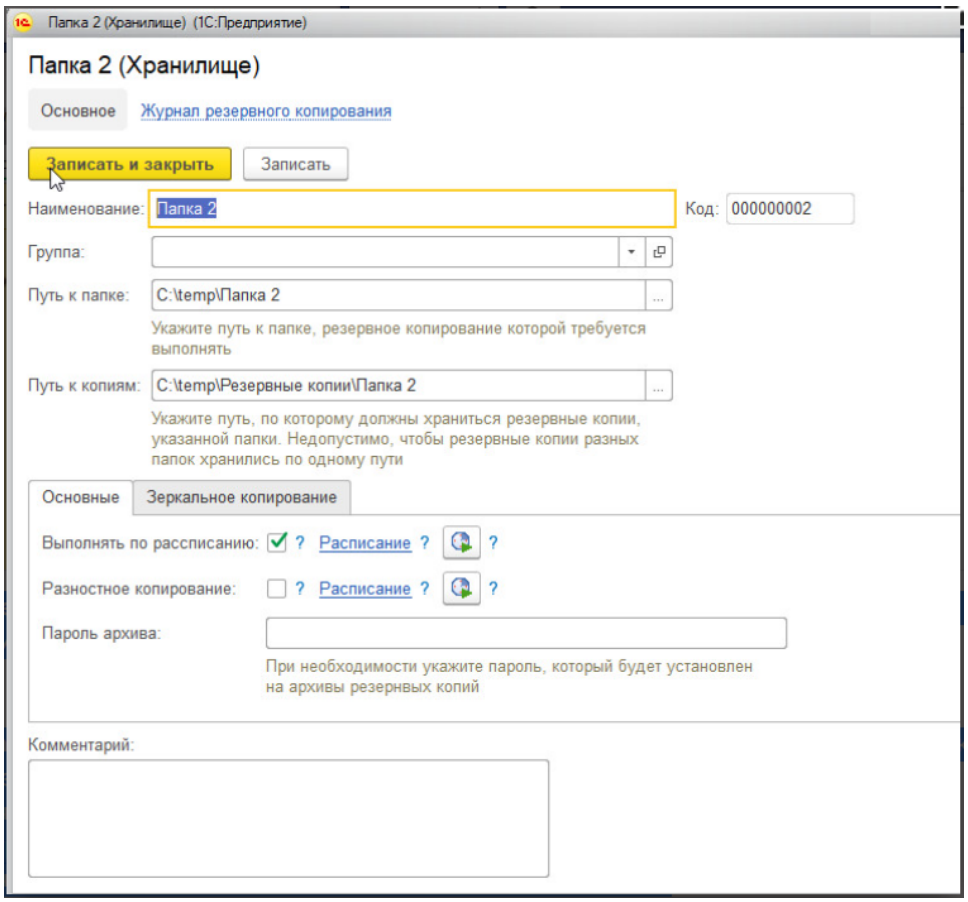

Рисунок 36 – Окно свойств папки хранилища данных

Менеджер выполняет резервное копирование выбранных папок (каталогов) по расписанию.

Также есть возможность сохранять резервные копии на зеркало (протокол FTP) для повышения надежности их хранения.

Функции модуля:

- настройка папок для резервного копирования (не ограниченное количество) и расписания их копирования;
- ручное резервное копирование настроенных папок;
- автоматическое резервное копирование по расписанию;
- анализ журнала резервного копирования;
- автоматическая рассылка статуса резервного копирования на email.

Таким образом, реализация проектных решений СУБП в рамках типового решения СЭД обеспечит повышение эффективности защиты электронного документооборота.

4.2 Оценка эффективности проектных решений

Для оценки эффективности предлагаемых проектных решений используем следующий критерий: средства защиты информации должны удовлетворять максимальному количеству требований по защите информации и при этом обеспечивать минимальную стоимость [4].

Математически задача оценки эффективности может быть формализована как задача оптимизации вида (2):

$$\sum_{j=1}^{n} c_j x_j \rightarrow min, \qquad (2)$$

где c_j – стоимость модуля СУИБ;

x_j – модуль СУИБ;

для следующих ограничений (3):

$$\sum_{j=1}^{n} a_{ij} x_j \geq 1, i = 1 \ldots m; \qquad (3)$$
$$x_j \in \{0,1\}, j = 1..n,$$

где a_{ij} – коэффициент покрытия j-м модулем СУИБ i-й функции информационной защиты электронного документооборота.

Таким образом, наименьшие затраты, а, следовательно, наибольшая эффективность будут достигнуты при использовании СЭД, в которой имеются встроенные средства защиты информационной защиты электронного документооборота (при условии, что данные средства обеспечивают требуемый уровень информационной защиты).

В этом случае не потребуются дополнительные затраты на интеграцию и адаптацию внешней СУИБ.

Для оценки экономической эффективности проекта используем методику сравнения затрат на разработку СУИБ внешним программистом по договору аутсорсинга (базовый вариант) и программистом компании (проектный вариант), соответственно [5].

«В калькуляцию себестоимости заказной разработки СУБЭД включаются следующие статьи затрат:

- зарплата исполнителя проекта по трудовому договору ($ЗБ_1$);
- социальные страховые взносы ($ЗБ_2$);
- прочие прямые расходы ($ЗБ_3$);
- накладные расходы ($ЗБ_4$).

В заказной доработке задействован внешний программист» [5].

Средняя стоимость часа работы программиста 1С по договору составляет 1125 руб [24].

Ориентировочное время разработки составляет 100 час.

Итого затраты базового варианта $С_{баз}$ составят (4):

$$С_{баз} = ЗБ_1 + ЗБ_2 + ЗБ_3 + ЗБ_4 = 1125*100 +0,271*1125*100+0+0 =143000 \text{ руб} \quad (4)$$

В самостоятельной разработке СУИБ задействованы программист, аналитик и системный администратор компании.

«В калькуляцию себестоимости собственной разработки СУИБ включаются следующие статьи затрат:

- зарплата исполнителей проекта с учетом затраченного времени 100 час ($ЗП_1$);
- социальные страховые взносы ($ЗП_2$);
- прочие прямые расходы ($ЗП_3$);
- накладные расходы ($ЗП_4$)» [5].

Итого затраты проектного варианта $С_{пр}$ составят (5):

$С_{пр} = ЗП_1 + ЗП_2 + ЗП_3 + ЗП_4 = (35000+20000+10000)$ руб+0,3*(35000+30000)+0+0 = 84500 руб (5)

Сформируем таблицу и график показателей экономической эффективности (таблица 6, рисунок 37).

Таблица 6 – Показатели эффективности проекта разработки СУИБ

«Затраты		Абсолютное изменение затрат	Коэффициент относительного снижения затрат	Индекс снижения затрат
Базовый вариант	Проектный вариант			
$С_{баз}$ (руб.)	$С_{пр}$ (руб.)	$\Delta С = С_{баз} - С_{пр}$ (руб.)	$К_С = \Delta С / С_{баз} \times 100\%$	$У_С = С_{баз} / С_{пр}$
143000	84500	58500	41	1,7» [5]

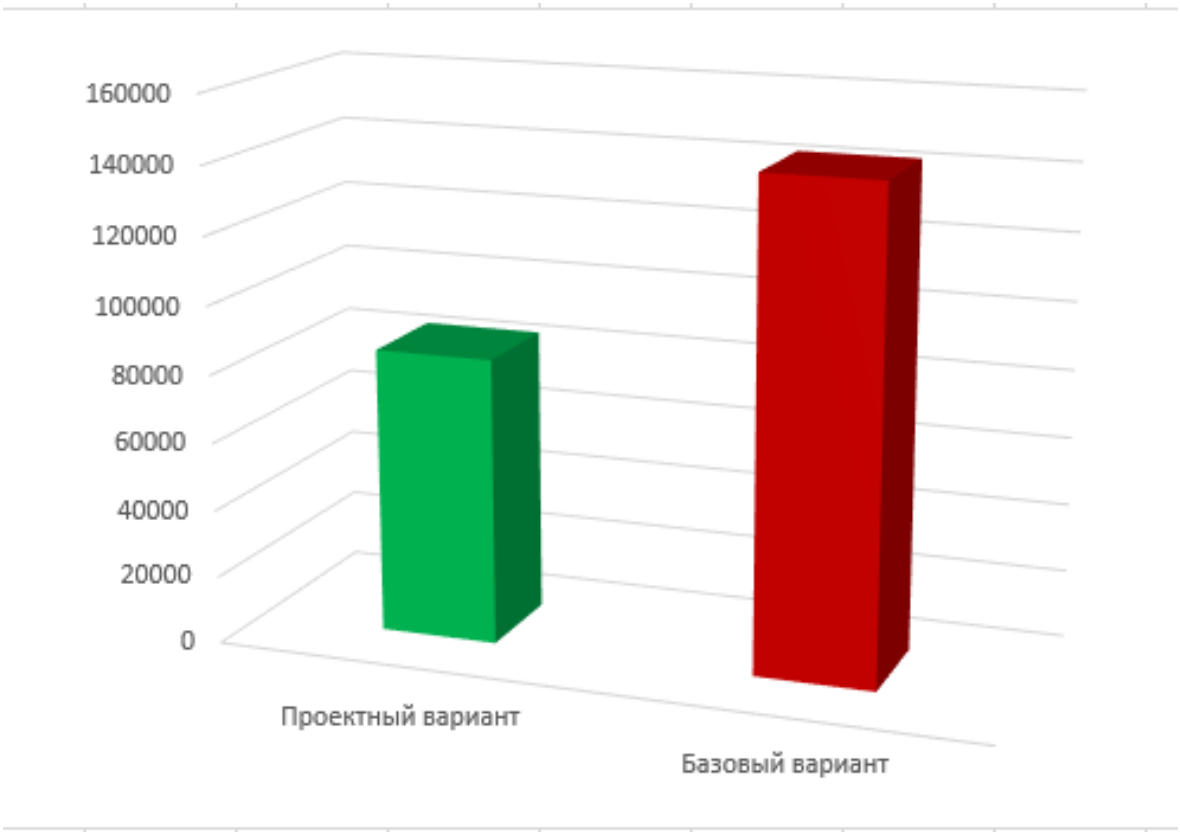

Рисунок 37 – Гистограмма сравнения затрат на разработку СУИБ

Таким образом, затраты при проектном варианте разработки СУИБ сократились в 1,7 раза.

«Срок окупаемости затрат на внедрение проектного решения ($Т_{ок}$) определяется по формуле (5):

$$Т_{ок} = К_{П} / \Delta С \text{ (мес.)}, \quad (5)$$

где $К_{П}$ – затраты на реализацию проектных решений (проектирование и внедрение СУИБ).

Следовательно, срок окупаемости СУИБ равен (6):

$$Т_{ок} = 84500/58500 \approx 1{,}5 \text{ мес.} \quad (6)$$

Представленные расчеты подтвердили существенное снижение затрат на проектирование и эффективность проектного решения» [5].

Для оценки эффективности управления СУИБ электронного документооборота предприятия используем формулу [5]:

$$К_{эу} = \frac{\sum_{i=1}^{n} Р_{уi}}{n}$$

где:

n - количество функций управления, реализуемых СУИБ;

$Р_{уi}$ - вероятность выработки СУИБ эффективного управляющего воздействия при реализации *i*-й функции управления.

Для управления информационной безопасностью электронного документооборота используются следующие функции:

− управление пользователями;

- управление шифрованием текста документа;
- управление ЭЦП;
- резервное копирование БД.

Как показывает практика, на выполнение функций «Управление шифрованием текста документа» и «Управление ЭЦП» может негативно повлиять человеческий фактор.

Пусть вероятность выработки эффективного управляющего воздействия для каждой функции равна 0.5.

В этом случае значение показателя функциональной эффективности управления СУИБ будет равно:

$$К_{эу} = 3/4 = 0,75$$

Таким образом, коэффициент эффективности управления предлагаемой СУИБ Кэу> 0,5, что свидетельствует о высокой функциональной эффективности управления информационной безопасностью электронного документооборота предприятия.

Выводы по главе 4

Результаты проделанной работы позволили сделать следующие выводы:

- СЭД обеспечит повышение эффективности защиты электронного документооборота;
- наименьшие затраты, а, следовательно, наибольшая эффективность будут достигнуты при использовании СЭД, в которой имеются встроенные средства защиты информационной защиты электронного документооборота.

Коэффициент эффективности управления СУИБ Кэу> 0,5, что свидетельствует о высокой функциональной эффективности управления информационной безопасностью электронного документооборота предприятия.

Заключение

На современном ИТ-рынке широко представлены промышленные системы управления электронным документооборотом, реализованные как программно-независимые ИТ-решения, функциональность и архитектура которых полностью соответствует требованиям, предъявляемым к ECM-системам.

Системы электронного документооборота, как и их бумажные аналоги, подвержены угрозам. Сотрудники могут ошибиться, а недобросовестные конкуренты попробовать выкрасть данные.

Однако наиболее важным аспектом, на который следует обратить внимание в этой связи, является необходимость внедрения надежной системы управления информационной безопасностью (СУИБ) электронного документооборота.

При отсутствии эффективной СУИБ, интегрированной с СЭД, невозможно обеспечить безопасность электронного документооборота в масштабах всего предприятия.

Совершенно очевидно, что в основу СУИБ должны быть положены модели и алгоритмы, отвечающие самым современным требованиям обеспечения безопасности электронного документооборота предприятия.

Магистерская диссертация посвящена актуальной проблеме исследования и разработки моделей и алгоритмов эффективной СУИБ электронного документооборота предприятия.

Выполненные в работе научные исследования представлены следующими основными результатами:

- проанализировано современное состояние исследований в области управления безопасностью электронного документооборота предприятия. Как показал анализ, угрозы для ECM/СЭД СЭД могут быть внешними и внутренними. Нормативно-правовая база обеспечения информационной безопасности СЭД основана на ФЗ РФ

от 27 июля 2006 г. № 149-ФЗ. СУИБ ECM/СЭД обеспечивают безопасное управление документами, аутентификацию документов, целостность и конфиденциальность информации. При выборе наилучшей платформы ECM/СЭД для предприятия необходимо учитывать наличие в ней средств реализации основных технических мер защиты информации. Вместе с тем проведенный анализ позволил констатировать недостаточность работ, посвященных проблеме разработки моделей и алгоритмов СУИБ электронного документооборота организации, что подтверждает актуальность темы настоящего исследования;

− проведен анализ методов и технологий управления информационной безопасностью электронного документооборота предприятий. Как показал анализ. Основными методами управления информационной безопасностью электронного документооборота предприятий являются: управление правами доступа пользователей; регулярное резервное копирование документов; шифрование текста документов и использование ЭЦП. Как показал анализ, каждые из представленных методов и технологий позволяет решать конкретную задачу по обеспечению информационной безопасности документооборота. Поэтому для разработки эффективной СУИБ электронного документооборота рекомендуется использовать комбинированный подход, подразумевающий применение всех основных методов и технологий их реализации для обеспечения информационной безопасностью;

− разработаны модели и алгоритмы эффективной СУИБ. Как показывает практика, основным недостатком метода шифрования текста документов является снижение производительности работы СЭД. Для решения данной проблемы предлагается использовать алгоритм процедуры шифрования текста документа. Для проверки текста документа на конфиденциальность предлагается использовать

метод, основанный на поиске в тексте соответствующих ключевых слов. Применение предлагаемых моделей и алгоритмов позволит повысить эффективность СУИБ электронного документооборота предприятия;

- выполнена апробация и оценка эффективности проектных решений. Для апробации предлагаемых проектных решений использовано типовое решение СЭД на платформе 1С8 – «1С: Документооборот 8». Наименьшие затраты, а, следовательно, наибольшая эффективность будут достигнуты при использовании СЭД, в которой имеются встроенные средства защиты информационной защиты электронного документооборота. Коэффициент эффективности управления СУИБ Кэу> 0,5, что свидетельствует о высокой функциональной эффективности управления информационной безопасностью электронного документооборота предприятия.

Таким образом, в работе решена актуальная научно-практическая проблема исследования и разработки моделей и алгоритмов эффективной СУИБ.

Работа может представлять интерес для системных аналитиков и ИТ-специалистов, занимающихся проблемами управления информационной безопасностью электронного документооборота предприятия.

Гипотеза исследования подтверждена.

Список используемой литературы

1. 1С: Документооборот 8 КОРП [Электронный ресурс]. URL: https://rarus.ru/1c8/1c-doc-8-korp/ (дата обращения: 22.01.2023).

2. Безопасность системы Directum [Электронный ресурс]. URL: http://www.mtgroup-it.ru/directum/arkhitektura/informatsionnaya-bezopasnost-sistemy-directum#:~:text=%D0%9B%D1%8E%D0%B1%D0%BE%D0%B9%20%D0%BF%D0%BE%D0%BB%D1%8C%D0%B7%D0%BE%D0%B2%D0%B0%D1%82%D0%B5%D0%BB%D1%8C%20%D0%B2%20%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B5%20Directum,%D0%B4%D0%BE%D1%81%D1%82%D1%83%D0%BF%D0%B0%20%D0%B2%20%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B5%20%D1%8D%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%BE%D0%B3%D0%BE%20%D0%B4%D0%BE%D0%BA%D1%83%D0%BC%D0%B5%D0%BD%D1%82%D0%BE%D0%BE%D0%B1%D0%BE%D1%80%D0%BE%D1%82%D0%B0. (дата обращения: 22.01.2023).

3. Безопасность электронного документооборота [Электронный ресурс]. URL: https://astral.ru/info/elektronnyy-dokumentooborot/bezopasnost-elektronnogo-dokumentooborota/ (дата обращения: 22.01.2023).

4. Булдакова Т.И., Глазунов Б.В., Ляпина Н.С. Оценка эффективности защиты систем электронного документооборота // Доклады ТУСУРа. 2012. № 1 (25). Часть 2. С. 52-56.

5. Вдовин В.М., Суркова Л.Е., Шурупов А.А. М. : Дашков и К, 2016. 388 с.

6. Визуализация электронной подписи на исходящих документах в соответствии [Электронный ресурс]. URL: https://infostart.ru/public/931674/ (дата обращения: 22.01.2023).

7. Викулина А. Защита систем электронного документооборота [Электронный ресурс]. URL: https://wiseadvice-it.ru/o-

kompanii/blog/articles/zashhita-sistem-edo/ (дата обращения: 22.01.2023).

8. Даниленко А.Ю. Управление доступом в системах электронного документооборота // Труды ИСА РАН 2009. Т. 45. С. 39-45.

9. Информационная безопасность документооборота [Электронный ресурс]. URL: https://searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/informatsionnaya-bezopasnost-v-otraslyakh/informatsionnaya-bezopasnost-dokumentooborota/ (дата обращения: 22.01.2023).

10. Колесов А. СЭД как интегрированная часть корпоративной системы // PC Week Review: Документооборот, сентябрь 2011. URL: https://www.itweek.ru/ecm/article/detail.php?ID=133753 (дата обращения: 12.02.2022).

11. Криптографические алгоритмы [Электронный ресурс]. URL: http://elcomdesign.ru/market/kriptograficheskie-algoritmy/ (дата обращения: 22.01.2023).

12. Криптография и электронная подпись в решениях на 1С [Электронный ресурс]. URL: https://infostart.ru/1c/articles/809967/ (дата обращения: 22.01.2023).

13. КриптоПро CSP [Электронный ресурс]. URL: https://www.cryptopro.ru/products/csp (дата обращения: 12.02.2023).

14. Леоненков А. В. Объектно-ориентированный анализ и проектирование с использованием UML и IBM Rational Rose [Электронный ресурс] : учебное пособие. М. : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. 317 с. [Электронный ресурс]. URL: https://www.iprbookshop.ru/97554.html (дата обращения: 12.02.2022).

15. Менеджер резервного копирования [Электронный ресурс]. URL: https://infostart.ru/public/805571/ (дата обращения: 22.01.2023).

16. Обеспечение безопасности электронного документооборота [Электронный ресурс]. URL: https://www.doc-online.ru/tags/bezopasnost_sed/ (дата обращения: 12.02.2022).

17. Подпись данных алгоритмами SHA + AES собственным модулем

[Электронный ресурс]. URL: https://infostart.ru/public/1319502/ (дата обращения: 22.01.2023).

18. Подсистема БСП «Управление доступом», основные объекты и регистры [Электронный ресурс]. URL: https://infostart.ru/1c/articles/1065487/ (дата обращения: 22.01.2023).

19. Полнотекстовый поиск [Электронный ресурс]. https://v8.1c.ru/platforma/polnotekstovyy-poisk/ (дата обращения: 22.01.2023).

20. Права доступа в 1С: Документооборот 2.1 [Электронный ресурс]. URL: https://www.doc-lvv.ru/ (дата обращения: 12.02.2023).

21. Программно-технологическая платформа документооборота LanDocs [Электронный ресурс]. URL: http://www.ecmonline.ru/software/landocs/ (дата обращения: 22.01.2023).

22. Резервное копирование файлов 1С: Документооборот [Электронный ресурс]. URL: https://infostart.ru/public/912511/ (дата обращения: 22.01.2023).

23. Система управления документами и информацией M-Files [Электронный ресурс]. URL: http://fts-eu.com/m-files/ru/s/chto-takoe-m-files/ (дата обращения: 22.01.2023).

24. Сколько стоят услуги программистов? [Электронный ресурс]. URL: https://www.kadrof.ru/articles/46641 (дата обращения: 20.02.2023).

25. Строковые отборы в 1С [Электронный ресурс]. URL:https://infostart.ru/1c/articles/1343680/ (дата обращения: 22.01.2023).

26. СЭД «Е1 Евфрат» [Электронный ресурс]. URL: https://evfrat.ru/sed-e1-evfrat/obzor-sistemy/ (дата обращения: 12.02.2023).

27. Ушаков Н.О., Сибикина И.В., Космачева И.М. Информационная безопасность в системах электронного документооборота // В сборнике трудов 3-й международной научно-технической конференции «Техническая эксплуатация водного транспорта: проблемы и пути развития», 2021. С.70-74.

28. Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Консультант плюс: справочно-правовая система.

29. Что такое СКЗИ, и какие они бывают [Электронный ресурс]. URL: https://tensor.ru/uc/ep/skzi (дата обращения: 22.01.2023).

30. Шевцов В.Ю., Бабенко А.А., Козунова С.С., Кравец А.Г. Система управления информационной безопасностью документооборота на предприятии // Прикаспийский журнал: управление и высокие технологии. 2018. №1 (41). С. 161-172.

31. Шифрование текста и файлов с помощью 1С [Электронный ресурс]. URL: https://infostart.ru/1c/articles/1083158/ (дата обращения: 22.01.2023).

32. AES Crypt [Электронный ресурс]. URL: https://www.aescrypt.com/ (дата обращения: 22.01.2023).

33. Best Practices for Document Management Security [Электронный ресурс]. URL: https://www.passportalmsp.com/blog/11-best-practices-for-document-management-security (дата обращения: 22.01.2023).

34. Enterprise Content Management in SharePoint [Электронный ресурс]. URL: https://support.microsoft.com/en-us/office/enterprise-content-management-in-sharepoint-930dd985-5bb9-447b-affd-86fcf690e994 (дата обращения: 22.01.2023).

35. Five Data Security Measures to Protect Your Enterprise Content Management System [Электронный ресурс]. URL: https://www.revolutiondatasystems.com/blog/data-security-ecm (дата обращения: 22.01.2023).

36. Peneti Subhashini and B Padmaja Rani “Confidential data identification using data mining techniques in data leakage prevention system”, International Journal of Data Mining & Knowledge Management Process (IJDKP) Vol.5, No.5, September 2015, P. 65-73.

37. Raju R. Security and Enterprise Content Management, Conference Paper ITx New Zealand, 2015.

38. Security Issues in Enterprise Content Management [Электронный ресурс]. URL: https://zcomsolutions.com/security-issues-in-ecm/ (дата обращения: 22.01.2023).

39. UML 2.ru – Сообщество Аналитиков [Электронный ресурс]. URL: https://www.uml2.ru/ (дата обращения: 22.01.2023).

40. Vivekanand R. Chudgar “Security Features of Lotus Notes/Domino Groupware”, CLP, PCLP, Solaris SA1, MCSE, MCP+I GSEC Practical Requirements (v 1.3), 2021.

41. What is a document management system? [Электронный ресурс]. URL: https://www.efilecabinet.com/what-is-a-document-management-system/ (дата обращения: 22.01.2023).

42. What is Enterprise Content Management [Электронный ресурс]. URL: https://www.aiim.org/resources/glossary/enterprise-content-management (дата обращения: 22.01.2023).