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 Методы и алгоритмы оптимизации и защиты электронного документооборота

Студент Д.В. Тихонов
(Инициалы Фамилия) (личная подпись)

Научный руководитель канд. тех. наук, доцент, О.В. Аникина
(ученая степень (при наличии), ученое звание (при наличии), Инициалы Фамилия)

Тольятти 2022

Содержание

Введение

Тема данной диссертации посвящена использованию документооборота в учреждении, как комплекса взаимосвязанных процедур, который используется для обеспечения работоспособности организации.

Ввиду того, что внедрение электронного документооборота может таить в себе не только очевидные преимущества, но и недостатки, то следует провести всестороннее исследование методов и алгоритмов оптимизации и защиты электронного документооборота и в итоге получить обобщенные и критически проанализированные результаты.

Рассмотреть алгоритмы, которые в данным момент используются в системах документооборота, их существующие достоинства и недостатки.

Исследовать существующую научную литературу по данной теме, определить существующие предложения по оптимизации и дополнению данных систем.

Обосновать необходимость дополнения существующих систем новыми способами защиты документооборота.

Предложить новые способы защиты документооборота, которые на данный момент не используются в существующих системах.

Определить их степень применимости в существующих системах документооборота.

Целью данной работы является разработка методики защиты информации в сфере электронного документооборота, оптимизирующей существующий процесс выдачи копии документа.

В данной работе рассматриваются современные методы оптимизации документооборота, существующие способы и методы его защиты от несанкционированного доступа, определяется понятие электронного документооборота. Уделяется внимание преимуществам внедрения электронного документооборота, существующим системам и методам их защиты.

Объектом являются системы электронного документооборота в организациях, предметом – методика оптимизации алгоритмов в данных системах.

Проблема исследования состоит в том, что в существующих системах документооборота, отечественных и зарубежных источниках, недостаточное внимание уделено защите хранимых документов, а также представленных в них персональных данных пользователей.

Актуальность данной работы заключается в том, что ввиду усиливающейся протекционистской политики государств, список допустимых к использованию систем документооборота ещё более сокращается.

Так же, в существующих системах не предлагается таких функций, которые позволили бы защитить информацию от различных форм аналогового копирования, что позволяет злоумышленнику беспрепятственно воспользоваться известной фундаментальной уязвимостью под названием «Аналоговая брешь».

Суть данной проблемы состоит в возможности для злоумышленника зафиксировать данные со своего устройства несмотря на существующие ограничения.

Так же, после того как информация будет выведена из системы документооборота, то проследить её след становится практически невозможно.

Классически используется метод, позволяющий аффинными преобразованиями внести изменения в текст так, чтобы человеческий глаз не мог заметить отличий от обычного текста.

Однако, этот метод не защитит от OCR преобразования документов, что не позволит обнаружить злоумышленника.

Для решения данной проблемы мною предлагается несколько алгоритмов, которые также составляют новизну данной работы:

– Использование синонимичных преобразований текста отчётов;

– Преднамеренное внесение в текст уникальных копий опечаток;

– Внедрение символов нулевой ширины.

Теоретическая значимость исследования состоит в определении новых методов защиты документов в системах электронного документооборота и проработки алгоритмов, благодаря которым можно будет определять составителя документа.

Практическая значимость состоит в том, что итоги работы могут быть применены организациями, которым требуется обеспечить защиту собственного документооборота от злоумышленников в том случае, если им недостаточно той степени защищенности, которую предлагают существующие решения.

Был произведён анализ существующих решений, методов и алгоритмов. Выяснены моменты недостаточной защищенности. На основе данных статистических исследований было выяснена необходимость защиты документов в системах документооборота.

В рамках представленной работы была сформулирована следующая гипотеза: внедрение предлагаемой методики защиты информации позволит оптимизировать безопасность существующего электронного документооборота на предприятии.

Далее, исходя из предложенной гипотезы и анализа существующей научной литературы и представленных на рынке коммерческих решений, были определены требования к защите данных в системах электронного документооборота, определены их достоинства и недостатки.

На основании высказанной гипотезы и проведённого анализа, было представлено предложение по оптимизации существующих систем документооборота, разработана типовая модель существующих систем и предложены дополняющие её алгоритмы оптимизации.

Так же, в тексте данной работы были представлены примеры возможной реализации подобных алгоритмов, доказана теоретическая и практическая возможность их внедрения в существующие системы.

Предложенные в рамках данной работы алгоритмы защиты данных позволяют перекрывать недостатки друг друга, а также дают возможность многоуровневой защиты данных, что повышает общую безопасность.

На защиту выносится:

– Предложенная модель защиты данных в системах электронного документооборота, включающая в себя три новых алгоритма защиты данных.

– Результат апробации предложенной модели и анализа эффективности предложенной модели.

Общий объём данной диссертации составляет 73 страницы и включает в себя 8 таблиц, 14 рисунков, 4 формулы и 44 использованных источников.

Данная диссертация состоит из следующих логических пунктов.

В первой главе был проведён:

– анализ проблемы и методов защиты данных в системах электронного документооборота;

– обзор существующих предложений и методик защиты в научной литературе и законодательная оценка регуляторов;

Во второй главе был проведён:

– анализ достоинств и недостатков существующих систем защиты документооборота, применяемых в них алгоритмов;

– определение сферы применения технологии защиты от «аналоговой бреши» в системе электронного документооборота;

В третьей главе было представлено:

– предложение новых алгоритмов решения;

– разработка модели «AS-IS», разработка и анализ модели «TO-BE»;

В четвёртой главе были проведены:

– Анализ и разработка алгоритмов решения поставленной проблемы;

– Апробация и оценка полученных результатов.

1 Анализ проблемы оптимизации и защиты электронного документооборота

1.1 Анализ существующих достоинств и недостатков систем электронного документооборота

Документооборотом называется целостная система управления документами на предприятии, включающая в себя:

– создание документов;

– обработку документов;

– приём документов;

– передачу документов;

– хранение документов;

– архивирование документов.

От того, как качественно организован документооборот зависит скорость доступа, передачи, качество хранения информации, а в следствии – эффективность организации.

Так, если говорить о достоинствах, то следует упомянуть о том, что электронный документооборот позволяет нивелировать проблемы, связанные с использованием защитных красок.

Так, в работе [22] было проведено исследование стойкостных свойств специальных печатных красок, которое говорит о том, что степень их постепенной деградации не позволяет в полной мере отличить подделку от оригинала уже после десяти месяцев для чёрной краски, которая в основном и используется в документах.

Однако, достоинства электронного документооборота неоспоримы, поэтому, однако, не стоит забывать и о недостатках, которые требуется определить [9].

Основными недостатками электронного документооборота являются:

– потребность в электронных устройствах хранения;

– организация безопасной системы передачи конфиденциальных данных для доступа к документам;

– организация защищенного хранилища данных документов;

– защита от внесения изменений в передаваемый и хранимый документ извне посторонним лицом [36].

Существующая стратегия развития РФ до 2030 года, определяет существующие тенденции развития и связывает их с развитием и повсеместным внедрением электронного документооборота, а также определяет необходимую защищенность данного документооборота.

В феврале 2019 года Госдума приняла законопроект об обязательном использовании российских средств шифрования в российском сегменте интернета в первом чтении, и закон вступил в силу в конце 2019 года.

Исходя из существующих тенденций развития документооборота, защиты данных (в том числе – персональных) можно прийти к выводу о том, что требования к безопасности и необходимости использования систем шифрования данных, разработанных в России, будет только усиливаться, что потребует новых реализаций методов и алгоритмов оптимизации, которые будут соответствовать законам.

Так, в подтверждение выявленным тенденциям, в процессе написания данной работы был подписан указ о дополнительных мерах по обеспечению информационной безопасности. Так, в пункте 6 данного указа говорится о том, что: «С 1 января 2025 года организациям запрещается использовать средства защиты информации, странами происхождения которых являются иностранные государства, совершающие в отношении России, российских юридических и физических лиц недружественные действия, либо производителями которых являются организации, находящиеся под юрисдикцией таких иностранных государств, прямо или косвенно подконтрольные им либо аффилированные с ними».[30]

Исходя из всего вышесказанного можно сказать, что актуальность данной проблемы, по внедрению электронного документооборота

заключается в том, что в соответствии с указами и постановлениями правительства требуется осуществлять постепенный переход на полностью электронную систему документооборота и при этом, желательно использовать актуальные в будущем системы защиты данных документов.

В связи с этим возникает проблема выбора методов и алгоритмов защиты данных в системе электронного документооборота и проблема оптимизации этой системы.

Ввиду того, что перед проведением исследования требуется проанализировать данный объект, то требуется произвести систематизацию и проверку на предмет того, соответствует ли данная система документооборота требованиям различных законодательных актов и подзаконных указов.

Ввиду того, что в настоящий момент всё большее количество людей используют мобильные устройства вместо ПК для доступа в Интернет, то имеет смысл говорить о методах и алгоритмах оптимизации и методах, и алгоритмах защиты в мобильных системах документооборота.

Для подтверждения слов о количестве пользователей мобильных устройств можно привести данные, полученные «Всероссийским омнибусом GfK».

Так, на 2018 год 56% россиян (старше 16 лет) пользуются Интернетом на мобильных устройствах и 13,2% пользуются Интернетом только на них. При этом стоит отметить, что в 2016 году количество россиян, которые пользовались Интернетом на мобильных устройствах составляло только 42,1% [15].

Среди выборки молодых пользователей у 41% компьютеры или вообще отсутствуют, или не используются для выхода в Интернет [15].

Исходя из вышеизложенной статистики, можно сделать вывод о том, что предпочтительнее реализовывать будущие системы документооборота для мобильных устройств или же, как минимум, с их поддержкой.

1.2 Анализ научной литературы и законодательства в отношении электронного документооборота

Системы электронного документооборота, разработанные для мобильных устройств, имеют следующие преимущества, в сравнении с системами для ПК:

– мобильность;

– доступность выхода в сеть;

– простота в использовании неподготовленным пользователем;

– большая степень защищенности;

– возможность OCR распознавания текста с фото.

В существующих статьях, рассматривающих проблему организации документооборота, таких как [1, 5, 12, 11] рассматриваются различные вопросы организации, формирования и повышения эффективности документооборота.

К примеру, в статье [12] рассматривается вопрос эффективных направлений в электронном делопроизводстве, рассматриваются существующие системы, их достоинства и недостатки, а также даётся определение и рассматривается идеальный вариант оптимизации документооборота.

В статьях [7, 8, 17, 29, 32] рассматривается вопрос о реализации российских алгоритмов шифрования, их достоинств и недостатков, рассматривается вопрос о защищенности алгоритма, осуществляется алгебраическая атака на данные алгоритмы.

Однако, в данных статьях не рассматривается вопрос о защите документооборота, как об основных направлениях защиты. Не рассматривают также вопрос оптимизации хранения документов.

В статьях [37, 38, 40] рассматриваются и производится обзор алгоритмов оптимизации данных. Рассмотренные в данных статьях методы позволяют

уменьшить занимаемый документом размер и ускорить его передачу через системы передачи данных.

В статье [37] даётся обоснование трудностям в оптимизации моделирования, в сравнении с математическим программированием.

Статья ссылается на современные алгоритмы в этой области, рассматриваются и сопоставляются различные подходы, рассматриваются некоторые существующие решения и задачи, решённые с их помощью, а также приводятся размышления автора о вероятных будущих направлениях в этой области.

В статье [39] рассматривается полностью пересмотренный алгоритм защиты данных, основанный на селективном шифровании.

Данная схема является схемой, которая использует параллельную архитектуру с использованием графического процессора общего назначения, позволяющую производительность, Bitmap, как несжатый мультимедийный формат, рассматривается в качестве первого варианта использования.

Данная работа в значительной степени улучшила другие, опубликованные ранее работы по защите растровых изображений, предоставив новые конструкции и практические эксперименты.

Графический процессор общего назначения (GPGPU) используется в качестве ускорителя для того, чтобы обеспечить более высокую эффективность вычислений, в сравнении традиционными алгоритмами полного шифрования.

Затем, в статье описывается «agnostic selective encryption», которое основано на дискретном Wavelet-преобразовании без потерь.

Данный метод обеспечивает высокий уровень защиты и хорошую производительность, что было выяснено в результате практических экспериментов на различных конфигурациях.

Однако, в данной статье не рассматривается российская специфика документооборота, в частности не учитываются требования следующих законов и подзаконных актов:

– федеральному закону № 152-ФЗ «О персональных данных»;

– приказу ФСТЭК России № 21;

– приказу ФСТЭК России №489;

– постановлению правительства №79;

– постановлению правительства №1119 [25], [26].

В статье [41] производится представление алгоритма по созданию системы электронного документооборота в сфере образования.

Представленный в работе алгоритм представляет собой модульную архитектуру, что даёт возможность повысить функционал, сократить затрачиваемое время на реализацию ИТ-проекта и дает возможность использовать реализацию в различных системах образования.

Данная работа учитывает особенности российской образовательной системы и связанного с ним законодательства, что позволяет использовать данную разработку на территории РФ.

Также в работе приводится реализация структуры информационных потоков в сфере образования.

К недостаткам данной работы относительно темы диссертации можно отнести слабую проработанность относительно других сфер документооборота, не связанных с непосредственно сферой образования. Так же, недостаточное внимание уделено оптимизации существующих алгоритмов, а используются классические способы оптимизации.

Третий недостаток представленной работы заключается в отсутствии использования средств защиты информации, в частности неиспользования алгоритмов шифрования данных.

В статье [42] приведена разработка архитектуры для приложения поддержки принятия решений, которое использует промышленные стандарты связи, что позволяет не тратить дополнительные усилия на интеграцию с существующими системами.

Однако, данная СППР не приспособлена для использования на территории РФ и не удовлетворяет всем положениям законодательства.

В статье [2] производится анализ готовности белорусских предприятий к переходу к электронному документообороту, утверждается необходимость проведение повторного перехода на новые системы электронного документооборота, ввиду того, что существующие систему уже не справляются с возлагаемыми на них требованиями.

Высказываются основные проблемы, общие для наших государств, которые возникают при внедрении электронного оборота в эксплуатацию.

В монографии [3] приводится информация, помогающая организовать систему электронного документооборота в организации, проводится разбор существующих методик внедрения и оптимизации систем, приводится информация о разработке методики по самостоятельной подготовке организации к самостоятельной разработке системы, а так же приводятся примеры успешных реализаций и анализ их эффективности.

Беловым С.П была проведена большая работа по составлению успешных и применяемых в российских и зарубежных организациях методиках внедрения и оптимизации алгоритмов.

Были отправлены и получены письма от 48 различных организаций и произведён анализ с выявлением достоинств и недостатков методов.

Одним из недостатков представленной реализации является то, что недостаточное внимание уделено защите документов в системе. В качестве системы шифрования используется устаревший ГОСТ, описывающий шифр «Магма» несмотря на то, что на данный момент он применяется только в целях совместимости со старыми разработками и для своего использования требует особого разрешения от ФСБ России.

В статье [4], автором были проанализированы различного вида атаки на существующие криптографические средства защиты информации.

Произведено описание методов, используемых для атак на симметричные алгоритмы шифрования, выявлены их преимущества и недостатки.

На основе проведённых исследований был сделан вывод о необходимости использования ключей шифрования с длиной не менее 128 бит, а лучше – 256 бит. Так же данные алгоритмы должны быть устойчивыми к известным атакам.

В статье [10], авторами были выявлены основные принципы документооборота, выявлены достоинства внедрения документооборота в эксплуатацию и его недостатки. В частности, рассматривается вопрос безопасности электронного документооборота, однако не приводится методик проверки защищенности.

В статье [21], автором производится алгебраическая атака на шифр путём анализа на экстремумы полученного S-блока из алгоритма «Кузнечик»

Данный метод отражает то, чему должно быть равно значение $Q = (X \oplus K, \alpha) \oplus (Y, \beta)$, где X, Y и K – вектора входа, выхода и ключа соответственно, а α, β – двоичные вектора, а само значение Q отражает момент завершения работы алгоритма анализа [28].

Приведённый в статье метод позволяет проверить на криптостойкость реализацию алгоритма шифрования, что позволяет сделать вывод о защищенности системы документооборота в целом.

В статье [23] коллективом авторов рассматривается методы нанесения защитных изображений на документы. Производится анализ существующих решений, которые предоставляют возможность защиты изображений путём создания защитных сеток, виньеток, гильошей и тангиров.

К недостаткам существующих решений авторы относят то, что: «… нет возможности осуществить безрастровое воспроизведение цвета без использования специальных красок», а также необходимость создания изображений в векторной графике.

Авторы предлагают использовать различные цветные узоры для защиты документов при том, что данные узоры получаются путём сложения кривых Безье различных цветов.

Пример изображений представлен на рисунке 1.

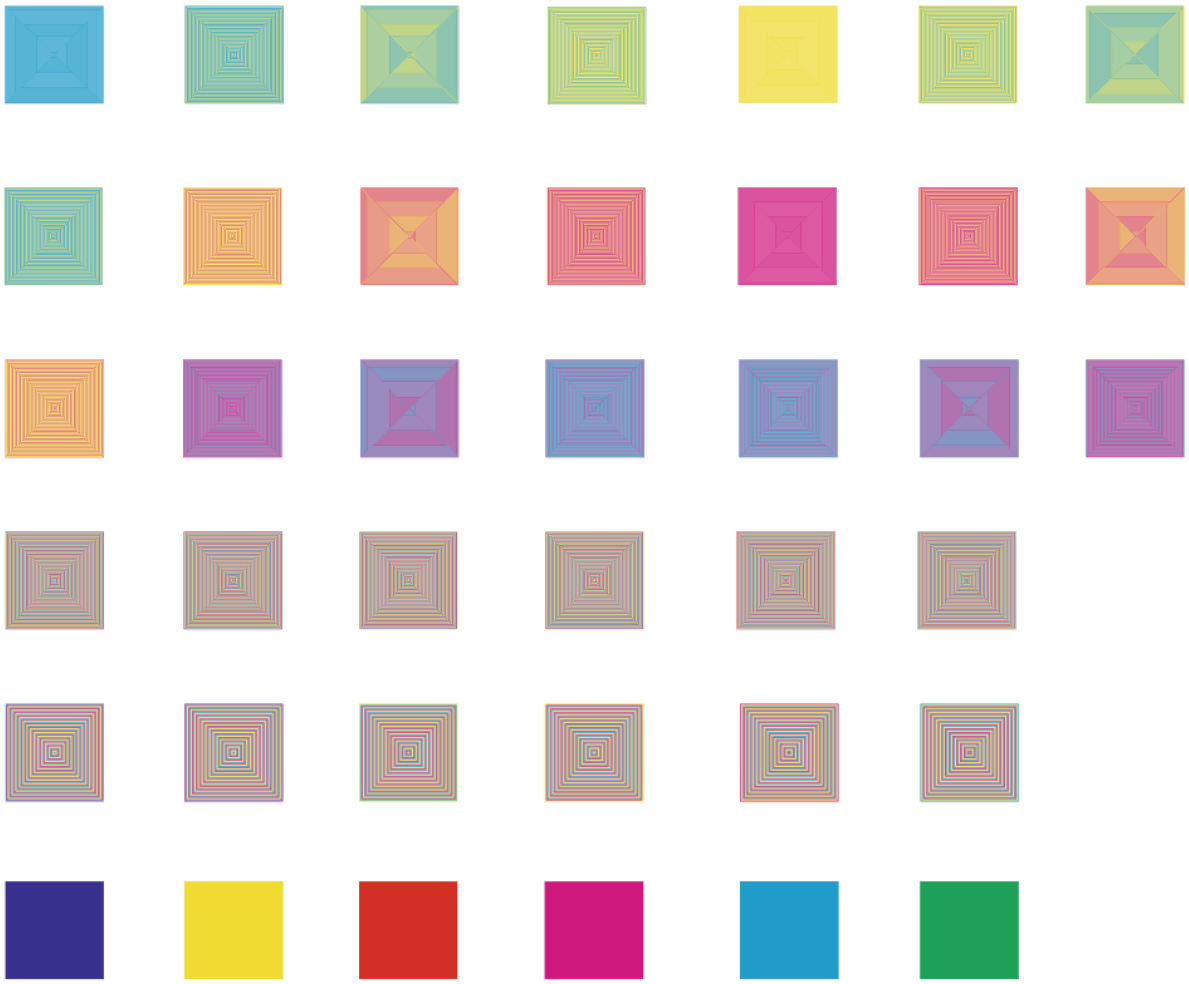

Рисунок 1 – Примеры разработанных защитных узоров

Авторы утверждают, что основным фактором внедрения их решения является возможность воспроизвести такой метод защиты без использования специализированного оборудования или материалов. А также заявляют, что: «…базовым элементом защиты выбраны векторные изображения, которые обладают свойством воспроизводимости на любых устройствах вывода без потери качества».

Однако, необходимо отметить, что недостаток данного метода в разрезе защиты систем электронного документооборота сразу же виден в том случае, если иметь в виду то, что документы в подавляющем большинстве случаев

печатаются на чёрно-белых принтерах, что не позволяет полноценно использовать данный метод без существенных доработок.

Также представление о воспроизводимости векторных изображений можно оспорить тем фактом, что далеко не все устройства позволяют отображать векторные изображения, а также не рассмотрен вопрос печати данных изображений.

Исходя из выявленных недостатков данного метода можно говорить о том, что его использование представляется оправданным исключительно в сфере защиты полиграфии, однако для защиты документов данный метод не применим или применим в крайне ограниченном виде.

Подводя итог всему вышесказанному, можно говорить о том, что в существующих системах документооборота и научных источниках недостаточное внимание уделено защите хранимых документов, а также представленных в них персональных данных пользователей и это позволяет высказать первичную гипотезу о необходимости предложения дополнений в существующие алгоритмы.

1.3 Анализ существующих методов защиты данных в системе электронного документооборота и достаточности существующих решений

Для защиты системы документооборота от воздействия злоумышленников используются различные методики защиты.

Одним основных и наиболее часто применяемых являются криптографические методы. Данные методы необходимо применять в случае, если попадание документа из системы злоумышленнику является недопустимым.

Однако, несмотря на важность защиты данных в системах документооборота, данному направлению уделяется недостаточное внимание. Так, в статьях, посвященных внедрению документооборота, не только не

предлагаются и не анализируются системы защиты данных, но само требование к защите данных зачастую опускается.

Однако в случае, если в организации присутствует единая система документооборота и производится обработка персональных данных пользователей, то использование шифрования данных становится не только необходимостью, но и требованием законодательства.

В результате анализа требований законодательства, можно прийти к выводу о том, что для большинства систем документооборота оптимальным будет использование одного из алгоритмов, описанных в ГОСТ 34.12-2018, а именно – алгоритма «Кузнечик», который является 128 битным шифром с 128 раундовым ключом записываемым в соответствии с формулами (1) и (2):

$$X[i]: V_{128} \to V_{128}, \quad (1)$$

$$X[i](a) = i \oplus a, \quad (2)$$

где $i, a \in V_{128}$.

Данный алгоритм может работать в нескольких возможных режимах, однако для передачи потока данных в системе необходимо использовать режим гаммирования с обратной связью ввиду того, что для шифрования последующего блока открытого текста к данному блоку применяется операция сложения по модулю 2 с перешифрованным (блочным шифром) результатом шифрования предыдущего блока.

Использование алгоритма «Магма», также описанного в ГОСТ 34.12-2018 не является желательным ввиду того, что его использование является допустимым в целях совместимости с уже существующими разработками и требует согласования с ФСБ.

Использование зарубежных реализаций различных алгоритмов шифрования ограничено законодательством РФ и требуются дополнительные исследования для каждого отдельного случая.

Для передачи ключа от симметричного шифра используется асимметричное шифрование, с помощью которого передаётся только сам сеансовый ключ ввиду того, что длина ключа симметричного алгоритма всегда меньше, чем ассиметричный ключ с аналогичной криптостойкостью, а также скорость операций над текстом в среднем меньше на 2-3 порядка.

Для любого ассиметричного шифра требуется его удовлетворение двум условиям:

– легко вычислить $f(x)$, если известен x;

– сложно вычислить x, если известно только значение $y = f(x)$.

Исходя из этого, можно сказать о том, что использование алгоритма RSA для передачи ключа от симметричного алгоритма является приемлемым ввиду того, что данный алгоритм используется в большинстве систем в настоящее время.

Однако, требования к безопасности данных не исчерпываются одним только использованием шифрования.

К системам документооборота, для их оптимизации требуется предъявлять функциональные требования, на основе которых организуется её защита:

– автоматическая регистрация документа в системе;

– OCR сканирование документов;

– экспорт и формирование документа в требуемый формат;

– разграничение прав доступа к различным документам;

– разрешение пользователям доступа только к тем документам, которые требует его должность;

– веерная рассылка распоряжений руководства;

– реализация процесса согласования и принятия документов в работу;

– полнофункциональный поиск требуемых документов, входящих в сферу компетенций сотрудника;

– архивирование невостребованных документов в соответствии с каталогом документов.

Исходя из функциональных требований к системе, можно дополнить требования к безопасности документооборота – требованием об обязательном разграничении прав доступа пользователей системы.

В результате анализа был сформирован список законов и подзаконных актов, которые регулируют данную тему на территории Российской Федерации, который представлен далее, в таблице 1.

Таблица 1 – Подзаконные акты, регулирующие защиту персональных данных

Подзаконные правовые акты	Вопрос, который регулируется в документе
Приказ ФСТЭК России № 21	Регулирует состав и содержание различных мер, применяемых для обеспечения безопасности данных
Приказ ФСТЭК России №489	Утверждает требования о защите информации, которая содержится в ИС общего пользования
Постановление правительства №79	Регулирует лицензирование деятельности по технической защите информации для системы защиты ПДх
Постановление правительства №1119	Регулирует угрозы в системе и составляет на их основе требования к защите ПДх

На практике, в настоящий момент практически отсутствуют предложения систем электронного документооборота, позволяющие защищать информацию от копирования аналоговым способом, а также цена на существующие решения не соответствует их эффективности.

Исходя из результатов проведённого анализа, можно говорить о том, что разработка и внедрение подобных систем представляется оправданным решением.

Суть предлагаемого решения заключается в том, что пользователь, который запрашивает документ, получает немного изменённую копию

документа, которая на внешний вид абсолютно неотличима от исходного документа, однако в базу данных записываются:

- алгоритм, по которому осуществлялось преобразование;
- время генерации уникальной копии;
- ID сотрудника, которому выдана копия документа.

Это означает, что в случае утечки файла будет возможность определения сотрудника, который сгенерировал данный файл и данная система позволит превентивно предотвращать возможные утечки данных путём информирования пользователей о внедрении данной системы в структуру документооборота организации.

Выводы по разделу 1

В ходе выполнения данного раздела были изучены научные работы, исследована литература по теме защиты данных и организации документооборота, законы и подзаконные акты.

Проведено всестороннее исследование существующих в научной литературе методов и алгоритмов оптимизации и защиты электронного документооборота.

В соответствии настоящим законодательством РФ, при хранении и передаче персональных данных, Федеральный закон «О персональных данных» устанавливает следующее требование: «Оператор обязан применить ряд организационных и технических мер, касающихся процессов обработки персональных данных, а также информационных систем, в которых эти персональные данные обрабатываются».

Исходя из данной выдержки, можно сделать вывод о законодательной необходимости осуществлять защиту персональных данных пользователей в разрабатываемых информационных системах.

В результате анализа был сформирован список законов и подзаконных актов, которые регулируют данную тему. Был проведён анализ научной

литературы, определены достоинства и недостатки существующих методов защиты различного вида (текст, изображения и другие) данных в системах электронного документооборота.

Также, можно сказать о том, что существующие методики оптимизации хранения данных в системах документооборота не имеют достаточной степени направленности на решение поставленной задачи, что позволяет произвести оптимизацию существующих.

В результате, на основании анализа данных работ были сделаны выводы о необходимости осуществлять защиту данных в информационных системах, о недостаточном освещении данной темы в существующих на данный момент источниках, были исследованы существующие алгоритмы, подобраны и предложены оптимальные алгоритмы.

Анализ, проведённый в данной главе, позволяет произвести дальнейший анализ в разрезе существующих промышленных решений, их достоинств и недостатков относительно исследуемых систем электронного документооборота.

2 Современное состояние проблемы оптимизации и защиты электронного документооборота

2.1 Обзор существующих методик защиты и оптимизации в коммерческих реализациях систем электронного документооборота

В настоящий момент, человек, который стоит перед выбором предпочтительной системы электронного документооборота должен ставить перед собой несколько задач:

- определение цены;
- определение качества защиты информации;
- определение способа защиты информации;
- определение функционала [24]

По функционалу системы электронного документооборота подразделяются на несколько групп:

- электронный архив;
- системы электронной маршрутизации (workflow);
- системы гибридного типа;
- системы для совместного ведения работ;
- многозадачные системы [34].

Вопросы, связанные с безопасностью актуальны при использовании данных систем вне зависимости от их типа, однако, его решение зависит от того, является ли используемая система электронного документооборота самостоятельным модулем, частью какого-либо иного модуля (например – CRM) или же облачным решением [13].

Также выбор может быть основан на том, где разработано программное обеспечение ввиду того, что в последнее время государства мира усиливают протекционистскую политику.

Если говорить о существующих решениях, то можно сказать о том, что в них слабо освещён вопрос защиты хранимых в них данных. Приведём

показательные примеры того, на что полагаются и что используют одни из самых популярных и часто используемых систем электронного документооборота [34].

«Optima WorkFlow». Одним из преимуществ данной системы является использование диаграммы Ганта для контроля общего хода работ. Передача и хранение документов происходит с использованием Windows Exchange, что дает представление об общей степени защищенности. Для шифрования данных используется система Крипто-Про и системы электронной цифровой подписи (ЭЦП), реализованные как MS CSP.

«E1 Евфрат». Является простым архивом, в котором хранятся ссылки на файлы. Вопрос безопасности хранимых документов ложится на создателей системы.

«1С Документооборот». Степень и качество защиты информации разнятся в зависимости от места хранения информации: локально или на облачном хранилище.

«Дело». Является программой-маршрутизатором, сохранность информации в которой ложится на предприятии ввиду того, что режим безопасности и права доступа определяются самостоятельно.

«Directum». Система документооборота с расширенными функциями, оптимизированными под интересы государственных служб и построенное на принципах полного соответствия российскому законодательству. Вопросы безопасности решаются путём разделения прав, при том, что для сторонних посетителей файлы представлены в режиме «Только для чтения». Также применяется системы шифрования и ЭЦП.

«ELMA». Является системой с широким функционалом и поддерживает модель входа только с доверенных устройств, входа по сертификату и токену.

Исходя из представленных выше систем электронного документооборота, можно выделить основные методики, которые используются для защиты документов в системах:

– электронная подпись;

– система «белых списков» устройств, имеющих доступ в систему
– система аутентификации;
– система разделения прав;
– система шифрования данных;
– хранение данных в облачных хранилищах;
– система ведения статистики [32].

Если требуется выбрать или разработать систему документооборота в сфере, где цена утечек наиболее высока, таких как финансовые и промышленные предприятия, то требуется использовать те стандарты, которые уже зарекомендовали себя в данной сфере.

Самым известным и используемым является стандарт ISO 17799 вместе с его модификациями под российскую специфику безопасности, которая отображена в ГОСТ [5, 6, 11, 13].

Если требуется решение, которое имеет более узкую направленность, то следует использовать модель ASA, которая ставит как основополагающую позицию защиту от всевозможных атак, будь то внутренние или внешние утечки.

Данная модель подразделяет архитектуру на несколько уровней:
– предсказание (прогнозирование);
– предупреждение (предотвращение);
– выявление (детектирование) угроз;
– реагирование.

2.2 Анализ достоинств и недостатков существующих систем защиты документооборота, применяемых в них методов, определение требований и используемых методов в системе

Основной гипотезой, высказанной в первой главе была гипотеза о недостаточном внимании, уделённым защите документооборота. Там же были

приведены данные из научной литературы, подтверждающие данную гипотезу [37-44, 8].

Для полного подтверждения гипотезы, следует определить то, какие из существующих систем документооборота имеют средства защиты, хранимой в них и выводимой из них информации и то, как они реализованы и насколько они полезны.

В таблицах 2, 3 и 4, представлен список из существующих систем электронного документооборота и их основные характеристики, связанные с доступностью и встроенным системам безопасности в данные системы.

Таблица 2 – Сравнение политик предоставления систем электронного документооборота

Название системы документооборота	Наличие подписки	Пробный период	Бесплатная версия	Стоимость
1	2	3	4	5
А2Б СЭД	Наличествует	Наличествует	Отсутствует	От 150 рублей в месяц
ELMA365 ECM	Наличествует	Наличествует	Отсутствует	От 500 рублей в год
Контур.Диадок	Наличествует	Наличествует	Отсутствует	От 4200 рублей в год
ЭТЛАС	Отсутствует	Отсутствует	Отсутствует	От 3900 рублей
DocSpace	Наличествует	Отсутствует	Отсутствует	От 450000 рублей
LanDocs	Отсутствует	Наличествует	Отсутствует	От 29900 рублей
OPTIMA-WorkFlow	Отсутствует	Отсутствует	Отсутствует	От 55000 рублей
OpenText Professional Services	Отсутствует	Отсутствует	Отсутствует	Индивидуальная

Продолжение таблицы 2

1	2	3	4	5
Е1 Евфрат	Наличествует	Наличествует	Отсутствует	От 7300 рублей
1С:Документооборот 8	Отсутствует	Отсутствует	Отсутствует	От 77400 рублей
СЭД «ДЕЛО»	Отсутствует	Отсутствует	Отсутствует	От 9900 рублей
TESSA	Отсутствует	Отсутствует	Отсутствует	От 5500 рублей
Alfresco	Наличествует	Отсутствует	Отсутствует	Индивидуальная
IBM Aspera® on Cloud	Наличествует	Наличествует	Отсутствует	Индивидуальная
WSS Docs	Отсутствует	Отсутствует	Отсутствует	Индивидуальная
Verdox	Наличествует	Наличествует	Отсутствует	От 3300 рублей в год
DIRECTUM	Наличествует	Отсутствует	Отсутствует	От 3510 рублей в месяц
ЛОГИКА: СЭД	Отсутствует	Наличествует	Отсутствует	Индивидуальная
ТЕЗИС	Отсутствует	Наличествует	Отсутствует	От 30000 рублей
АЛТИУС – Исполнительная документация	Наличествует	Наличествует	Отсутствует	От 1500 рублей в месяц
Lexema-ECM	Наличествует	Отсутствует	Отсутствует	Индивидуальная

Далее требуется рассмотреть методы, которые используются для защиты данных в рассматриваемых системах, представим их в таблице 3:

Таблица 3 – Методы и сертификации, которые применяются для защиты данных в рассматриваемых системах

Название системы документооборота	Сертификация ФСТЭК	Сертификация ФСБ России	Электронная подпись	Готовая адаптация под потребности
1	2	3	4	5
А2Б СЭД	Отсутствует	Отсутствует	Отсутствует	Наличествует
ELMA365 ECM	Отсутствует	Отсутствует	Наличествует	Наличествует
Контур.Диадок	Отсутствует	По потребности	Наличествует	Наличествует
ЭТЛАС	Отсутствует	Отсутствует	Отсутствует	Отсутствует
DocSpace	Наличествует	Наличествует	Наличествует	Наличествует
LanDocs	Наличествует	Наличествует	Наличествует	Отсутствует
OPTIMA-WorkFlow	Наличествует	Наличествует	Наличествует	Наличествует
OpenText Professional Services	Наличествует	Отсутствует	Отсутствует	Наличествует
Е1 Евфрат	Наличествует	Отсутствует	Наличествует	Наличествует
1С:Документооборот 8	Наличествует	Наличествует	Наличествует	Наличествует

Продолжение таблицы 3

1	2	3	4	5
Alfresco	Отсутствует	Отсутствует	Отсутствует	Наличествует
IBM Aspera® on Cloud	Отсутствует	Отсутствует	Отсутствует	Наличествует
WSS Docs	Отсутствует	Отсутствует	Отсутствует	Наличествует
Verdox	Отсутствует	Отсутствует	Отсутствует	Наличествует
DIRECTUM	Отсутствует	Отсутствует	Отсутствует	Наличествует
ЛОГИКА: СЭД	Наличествует	Отсутствует	Отсутствует	Наличествует
ТЕЗИС	Наличествует	Отсутствует	Отсутствует	Наличествует
АЛТИУС – Исполнительная документация	Наличествует	Отсутствует	Отсутствует	Наличествует
Lexema-ECM	Отсутствует	Отсутствует	Наличествует	Наличествует
СЭД «ДЕЛО»	Наличествует	Наличествует	Наличествует	Наличествует
TESSA	Отсутствует	Отсутствует	Отсутствует	Наличествует

Другими важными функциями, которые непосредственно влияют на защиту данных являются:

- система аутентификации сотрудников и пользователей;
- система разделения прав доступа для категорий сотрудников и пользователей;
- система шифрования данных;

– система ведения статистики работы с документами и действий пользователей;
– система аудита действий сотрудников и пользователей.
– система, позволяющая обнаружить злоумышленника в системе после вывода документа вовне.

Исходя из важности данных функций следует показать, какие из ранее представленных систем предоставляют возможность использования данных функций [33]. Представим их в таблице 4:

Таблица 4 – Функции, которые используются для защиты данных в рассматриваемых системах

Название системы	Система аутентификации и разделения прав	Система шифрования данных	Система ведения статистики	Система защиты от «Аналоговой бреши»
1	2	3	4	5
А2Б СЭД	Наличествует	Отсутствует	Наличествует	Отсутствует
ELMA365 ECM	Наличествует	Наличествует	Наличествует	Отсутствует
Контур.Диадок	Наличествует	Отсутствует	Наличествует	Отсутствует
ЭТЛАС	Наличествует	Наличествует	Наличествует	Отсутствует
DocSpace	Наличествует	Наличествует	Наличествует	Отсутствует
LanDocs	Наличествует	Наличествует	Наличествует	Отсутствует
OPTIMA-WorkFlow	Наличествует	Наличествует	Наличествует	Отсутствует
OpenText Professional Services	Наличествует	Отсутствует	Наличествует	Отсутствует

Продолжение таблицы 4

1	2	3	4	5
Е1 Евфрат	Наличествует	Отсутствует	Наличествует	Отсутствует
1С:Документооборот 8	Наличествует	Наличествует	Наличествует	Отсутствует
СЭД «ДЕЛО»	Наличествует	Наличествует	Наличествует	Отсутствует
TESSA	Наличествует	Наличествует	Наличествует	Отсутствует
Alfresco	Наличествует	Наличествует	Наличествует	Отсутствует
IBM Aspera® on Cloud	Наличествует	Наличествует	Наличествует	Отсутствует
WSS Docs	Наличествует	Наличествует	Наличествует	Отсутствует
Verdox	Наличествует	Наличествует	Наличествует	Отсутствует
DIRECTUM	Наличествует	Наличествует	Наличествует	Отсутствует
ЛОГИКА: СЭД	Наличествует	Наличествует	Наличествует	Отсутствует
ТЕЗИС	Наличествует	Наличествует	Наличествует	Отсутствует
АЛТИУС – Исполнительная документация	Наличествует	Наличествует	Наличествует	Отсутствует
Lexema-ECM	Наличествует	Наличествует	Наличествует	Отсутствует

Как можно понять из данных таблицы 4, в существующих системах не предлагается таких функций, которые позволили бы защитить информацию от различных форм аналогового копирования.

Это позволяет злоумышленнику беспрепятственно воспользоваться известной фундаментальной уязвимостью под названием «Аналоговая брешь».

Суть данной проблемы состоит в возможности для злоумышленника зафиксировать данные со своего устройства несмотря на существующие ограничения.

Так же, после того как информация будет выведена из системы документооборота, то проследить её след становится практически невозможно.

Программы, созданные для защиты конфиденциальных данных от утечек, можно интегрировать с системой документооборота.

Решение заключается в получении каждым сотрудником, при предоставлении ему документа, немного отличную копию от исходного текста, в которых закодированы некоторые параметры, позволяющие определить:

- алгоритм преобразования документа;
- время и дату создания документа и его изменённой версии;
- устройство, получившее индивидуальную копию документа;
- идентификатор того сотрудника, который получил индивидуальную копию.

Данное решение даёт возможность определить по документу, (его фотографии или скриншоту) утечка которого была произведена:

- с какого аккаунта произведена утечка;
- с какого устройства произведена утечка;
- дату и время утечки.

Так же, в случае информирования сотрудников о существовании системы защиты, система получит и превентивную функцию, так как каждый сотрудник будет знать то, что его участие в утечке может быть оперативно определено.

2.3 Определение сферы применения технологии защиты от «Аналоговой бреши» в системе электронного документооборота

Согласно данным аналитического отдела Infowatch, количество скомпрометированных данных в первом полугодии 2019 году по сравнению с первым полугодием 2018 года выросло в 3,6 раза [16].

Данные утечки можно подразделить на две категории: внешние и внутренние утечки, на которые приходится 56% от общего объёма.

Исходя из графика на рисунке 2, можно сделать вывод о том, что количество скомпрометированных данных и количество утечек будет только увеличиваться.

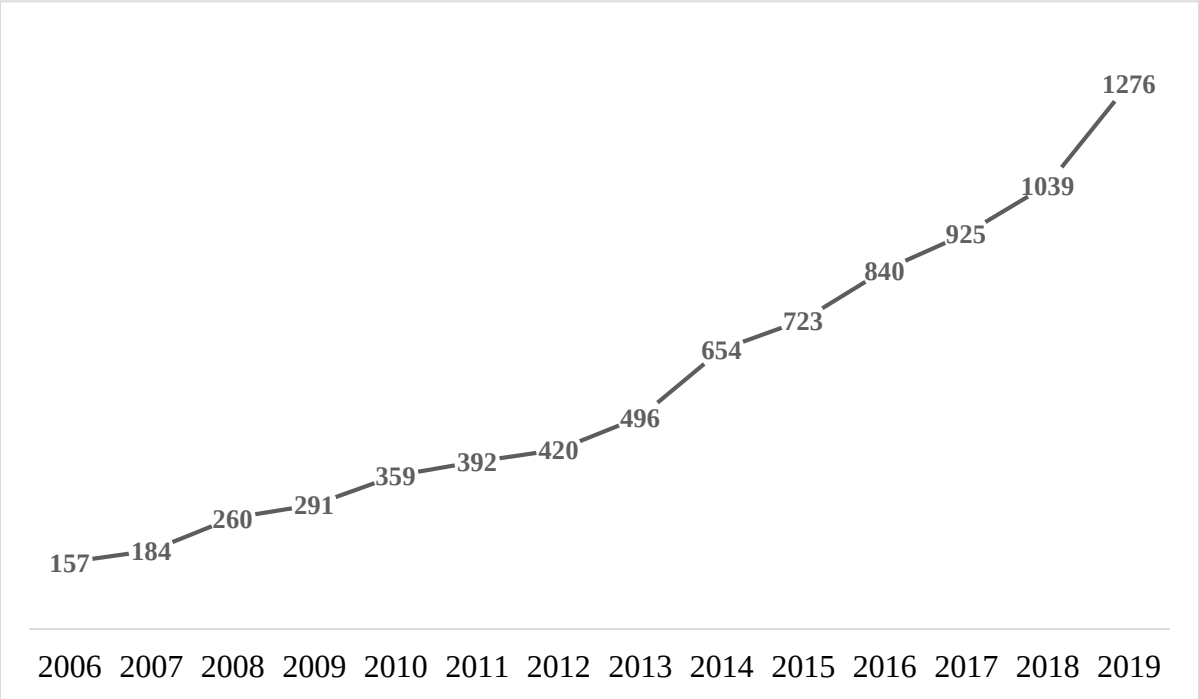

Рисунок 2 – Число зарегистрированных утечек информации в первых полугодиях с 2006 по 2019 года

Так же, на рисунке 3 видно, что основным источником внутренних утечек являются сотрудники, процент которых сравним с процентом внешних злоумышленников.

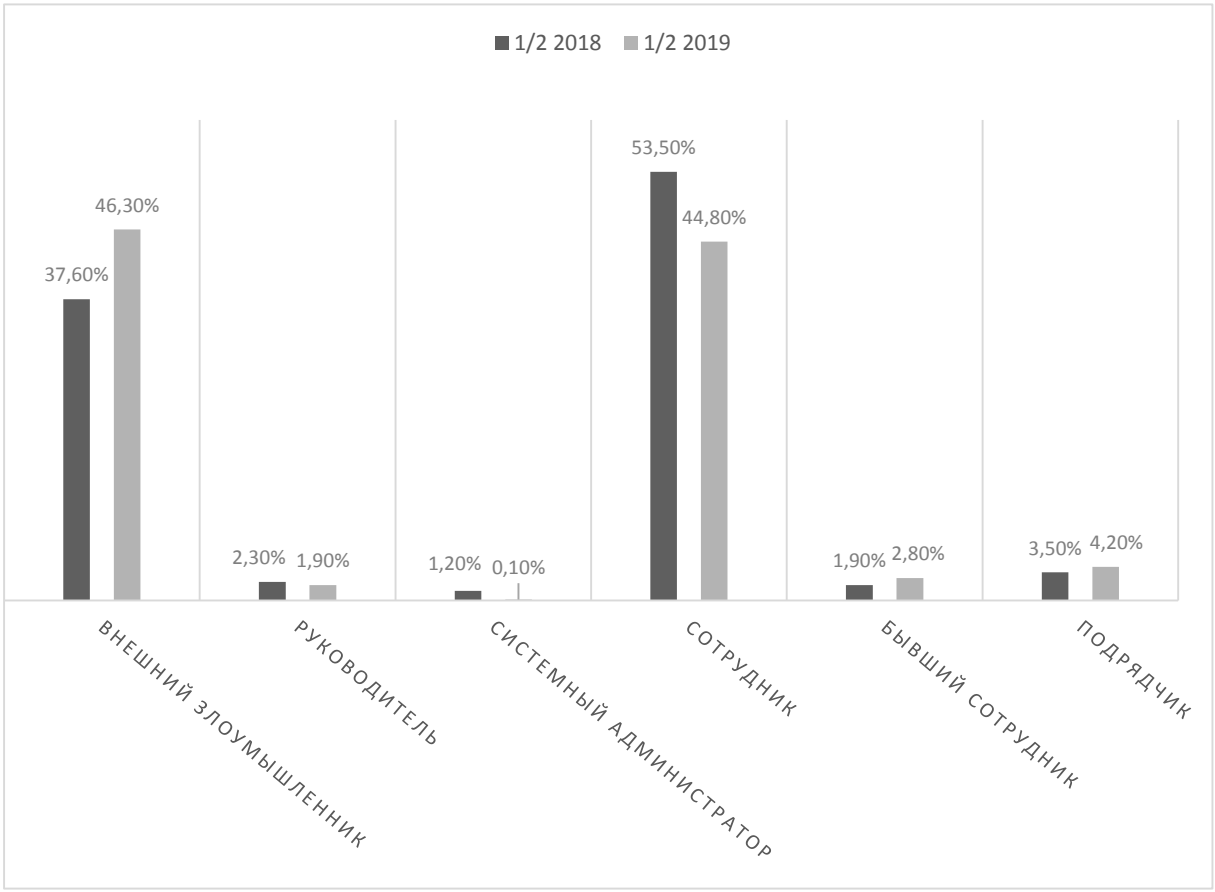

Рисунок 3 – Распределение утечек по их источнику, первые полугодия 2018-2019 годов

Исходя из имеющихся данных, можно сделать вывод о том, что большинство из сотрудников, имеющих доступ к данным, могут стать причиной утечки используя аналоговую брешь.

Исходя из данных анализа, представленных на рисунке 4, видно, что бумажные документы (которые на данный момент, практически невозможно отследить) занимают третье место по частоте. Также необходимо учесть то, что утечка через бумажные документы не является единственно возможной для аналоговой бреши.

Так, аналоговой бреши подвержены:

– мобильные устройства,
– съёмные носители,

– электронная почта,
– бумажные документы,
– IM (текст, голос, видео).

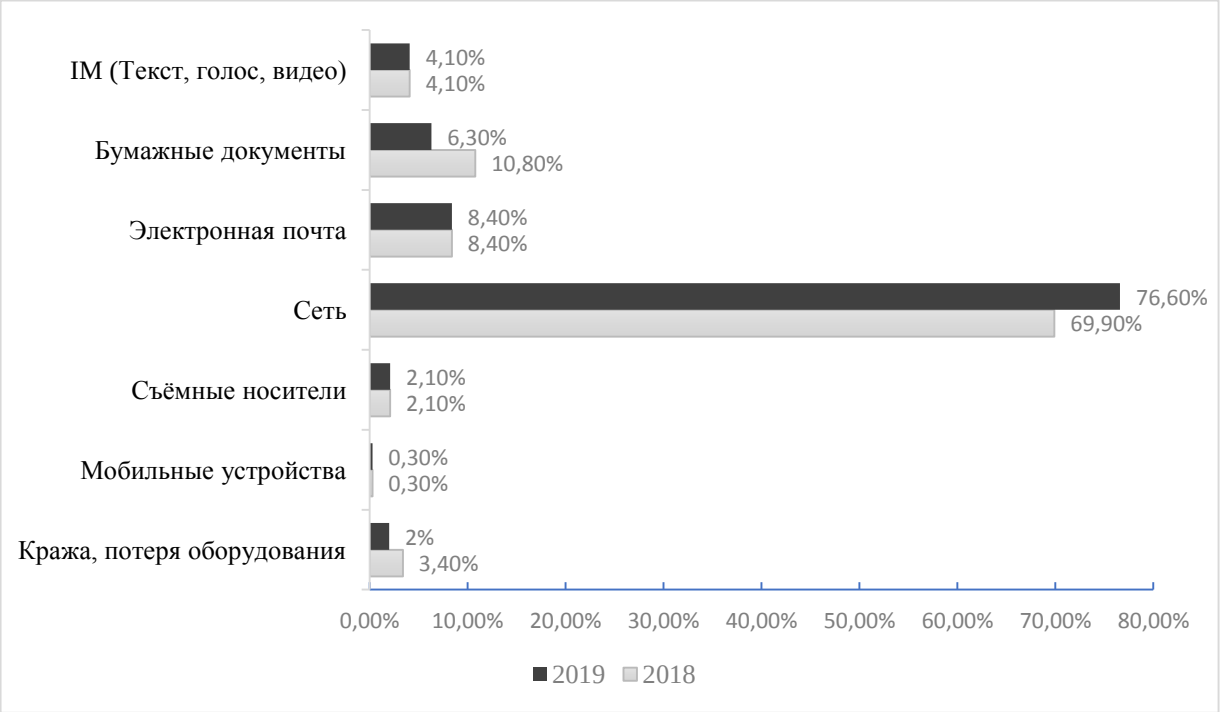

Рисунок 4 – Распределение утечек по каналам, первые полугодия 2018-2019 годов

Общий совокупный объём источников утечек, подверженных аналоговой бреши оценивается в 21,20% от объёма внутренних утечек.

Исходя из проведённого анализа сферы защиты документооборота, можно прийти к выводу о том, что:

– существующие системы документооборота не имеют в своём составе всеобъемлющих средств защиты документов;
– совокупный объём утечек, косвенно и непосредственно связанный с уязвимостью «аналоговая брешь», занимает существенный процент от всех утечек.

Исходя из всего вышесказанного, можно говорить о том, что внедрение данных средств в системы документооборота является не столько оправданным, сколько необходимым.

Выводы по разделу 2

Во втором разделе данной работы были определены и исследованы системы электронного оборота, определены основные параметры, влияющие на выбор оптимальной системы в различных случаях, определены множества, на которые обычно производят подразделение систем электронного документооборота.

Далее, все определённые в ходе работы системы документооборота, были проанализированы в ранее представленных таблицах под номерами 2, 3 и 4 на функции, непосредственно влияющие на безопасность и далее, на основе проведённого в части 2.2 настоящей работы был определён недостаток существующих разработок.

В результате, на основании анализа данных работ, были сделаны выводы о существовании в используемых системах некоторых недостатков, основным из которых является аналоговая брешь, опасность которой была проанализирована в части 2.3 настоящей работы.

По результатам данного анализа можно говорить о том, что аналоговая брешь может использоваться в более чем 20% утечек и точно используется в, как минимум, 6-10% утечек.

Исходя из проведённых исследований, можно сказать о том, что исследуемая тема имеет потенциал к исследованию, а также то, что все задачи, которые были поставлены в данной работе были выполнены.

3 Решение поставленной проблемы оптимизации и защиты электронного документооборота

3.1 Алгоритмы, используемые для защиты в сфере электронного документооборота

Необходимым элементом «цифровой» инфраструктуры современных предприятий и организаций является система документооборота. Такая система может быть эффективной в повышении доходности бизнеса. Она позволяет повысить отдачу от работы, а также будет эффективным решением задач по оптимизации потоков информации или бумаг [34].

Для формирования выходных данных из системы электронного документооборота используется функция экспорта данных, с помощью которой мы можем скачать документ.

Во время формирования отчёта по исходным данным используется набор алгоритмов, которые преобразуют форматирование документа так, чтобы можно было определить несколько параметров, таких как:

- устройство, которое запросило отчёт;
- дату и время создания отчёта;
- информацию о сотруднике, запросившем отчёт.

Однако, одно только аффинное преобразование не защитит от OCR преобразования документов, что не позволит обнаружить злоумышленника [18, 24, 33].

Для решения данной проблемы предлагается несколько методов:

- использование синонимичных преобразований текста отчётов;
- преднамеренное внесение в текст уникальных копий опечаток;
- внедрение символов нулевой ширины.

Таким способом, использование данных методов совместно даёт возможность обнаружить злоумышленника [12, 10, 11, 13].

Классически используется метод, позволяющий аффинными преобразованиями внести изменения в текст так, чтобы человеческий глаз не мог заметить отличий от обычного текста [27]. Пример подобного изменения приведён на рисунке 5

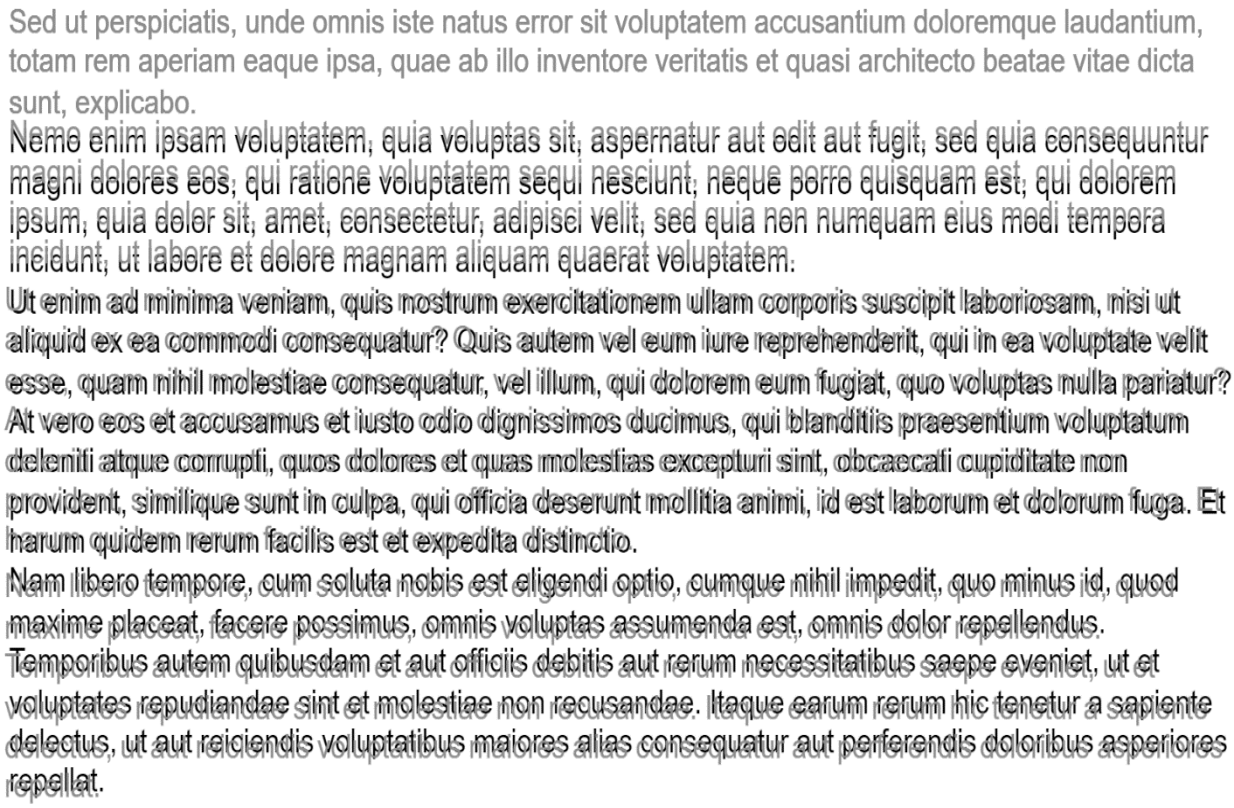

Рисунок 5 – Текст изменённый алгоритмом аффинного преобразования

На рисунке выше представлено сравнение двух текстов: исходного и преобразованного.

Как можно заметить, преобразованный текст несколько отличается от исходного текста, что позволяет определить злоумышленника путём сравнения объявившейся вне организации копии с копией каждого получателя данного документа.

Максимальный уровень совпадения позволяет определить злоумышленника.

Для реализации данного алгоритма используются методики отображения плоскостей (в случае электронного документооборота – абзацев документов) в себя, которые называются аффинными преобразованиями и подразделяются на следующие базовые виды:

– сдвиг-движение;
– растяжение-сжатие;
– преобразование подобия.

В данном случае, сдвигом-движением называется такое преобразование абзаца текста (пространства), которое сохраняет исходное расстояние между двумя любыми точками данного пространства. То есть, если принять A' и B' образами исходных точек A и B, то $A'B' = AB$.

Растяжение-сжатие в случае аффинных преобразований документов означает такое преобразование плоскости, что любая точка исходного документа (пространства) A переходит в точку A' с каким-либо коэффициентом k относительно избранной оси l.

В случае если коэффициент $0 < k < 1$, то данную процедуру называют сжатием, если $|k| > 1$, то растяжением.

Данное преобразование не является сдвигом-движением ввиду того, что не сохраняется исходное расстояние между точками, которые не лежат на прямой относительно избранной оси.

Преобразование подобия означает такое преобразование абзаца документа, что любые точки исходных плоскости A и B, а также точки преобразованных плоскостей A' и B' удовлетворяют соотношению $|A'B'| = k * |AB|$ при $k \neq 0$. Коэффициент k в данном случае означает используемый в преобразовании коэффициент подобия.

На рисунке 6 наглядно изображены описанные ранее аффинные преобразования, так слева-направо представлены: поворот, растяжение и сдвиг оси [19].

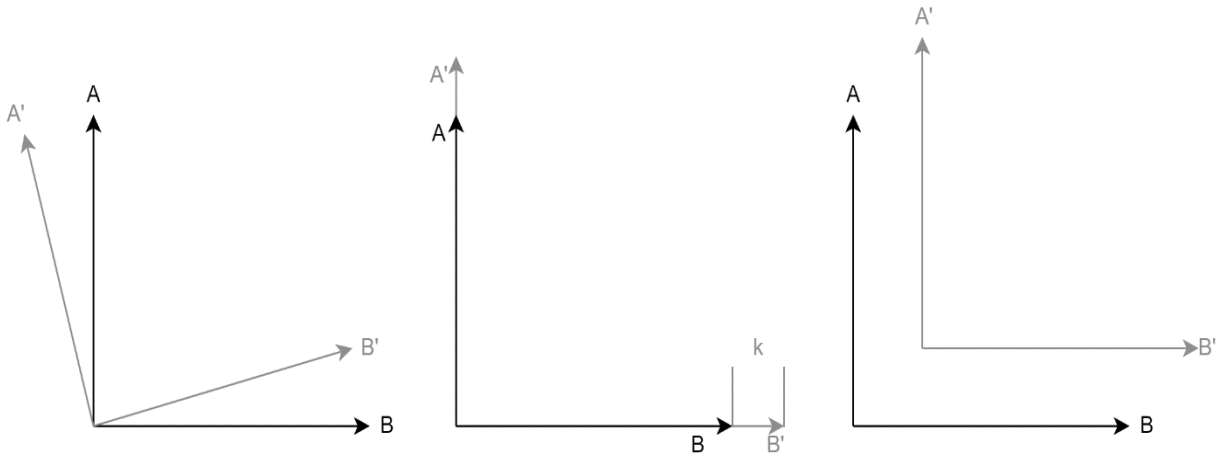

Рисунок 6 – Афинные преобразования осей координат

Изменённые алгоритмом копии не сохраняются, так как алгоритму требуется только набор используемых при генерации признаков, позволяющие определить параметры генерации.

Так же, для повышения устойчивости следует использовать описываемый далее метод.

В случае если злоумышленник не сохраняет документ, а копирует содержимое веб страницы, то в текст подготовляемого отчёта добавляются символы нулевой ширины, в которых скрывается требуемая для деанонимизации информация.

Для преобразования данных в данном случае используется их перевод в двоичную систему и запись преобразованных данных таким образом, что 1 записывается символом непечатаемого пробела, а 0 – символами запрета и разрешения лигатур.

Полученный в результате двоичный текст равномерно распределяется по всему документу, по отдельным страницам или абзацам в зависимости от используемых настроек, что позволяет безошибочно определить злоумышленника в случае, если утерянный документ был распространён в электронном виде [1, 2, 3, 5].

Достоинством подобного преобразования является то, что даже удаление форматирования из готового документа не удаляет непечатаемые символы.

Однако, использование данного метода представляется недостаточным, поскольку существует вероятность обнаружения подобных вложений в документ и их удаления.

Ещё одним дополнительным методом является использования того факта, что кодировка Юникод содержит в себе множество различных видов пробелов, практически идентичных для пользователя, но с разными кодами.

Далее, в таблице 5 представлены подходящие для использования в процессе сокрытия требуемой информации символы пробела.

Таблица 5 – Подходящие для сокрытия информации символы пробела

Наименование в Юникоде	Шестнадцатеричный код в Юникоде	Представление	Уточнение
THREE-PER-EM SPACE	2004	« »	Практически идентичен обычному пробелу
SIX-PER-EM SPACE	2006	« »	В два раза меньше обычного пробела
FIGURE SPACE	2007	« »	Равен ширине цифр в используемом шрифте
PUNCTUATION SPACE	2008	« »	Ширина равна знаку «.»
THIN SPACE	2009	« »	Обычно 0,2 ширины обычного пробела
MEDIUM MATHEMATICAL SPACE	205F	« »	Узкий пробел для применения в математических формулах

Однако, все вышеприведённые способы не позволяют защитить документ от перепечатывания вручную или от распознавания с помощью систем оптического распознавания символов, что не позволяет говорить о полной защищенности документации в системе электронного документооборота.

Для того, чтобы предотвратить подобный способ утечки информации, предлагается использовать замену в тексте слов на так называемые лингвистические дублеты или абсолютные синонимы.

Требуется использовать именно абсолютные синонимы, чтобы предотвратить ситуации неуместного употребления квазисинонимов и контекстуальных синонимов с различной эмоциональной окраской (например: чужой и зарубежный).

Был проведён анализ, определены наиболее часто употребляемые в документации слова, имеющие абсолютные синонимы. Примеры подобных пар слов представлен в таблице 6.

Таблица 6 – Пример абсолютных синонимов, используемых в документации

вербальный	словесный
воспаление легких	пневмония
дистрибуция	распределение
использованы	применены
китаистика	китаеведение
лингвистика	языкознание
подстановка	замена
распылитель	форсунка
сульфид марганца	сернистый марганец,
…	…
утвержденного	одобренного

Использование подобного словаря позволяет производить замену некоторых слов в подготовляемом тексте по заранее определённому алгоритму, скрывающему идентификатор пользователя, которые генерирует документ.

3.2 Общая структура системы электронного документооборота «AS-IS», разработка и анализ модели «TO-BE»

Ранее нами были рассмотрены алгоритмы, которые в данным момент используются в системах документооборота, их существующие достоинства и недостатки. Так же были предложены новые способы защиты документооборота, которые на данный момент не используются в существующих системах [38, 42, 44].

Для внесения дополнений в существующие процессы защиты документооборота требуется предоставить существующую методику генерации защищенных документов [39, 40, 41].

Используем для этого диаграмму последовательности и предоставим её на рисунке 7.

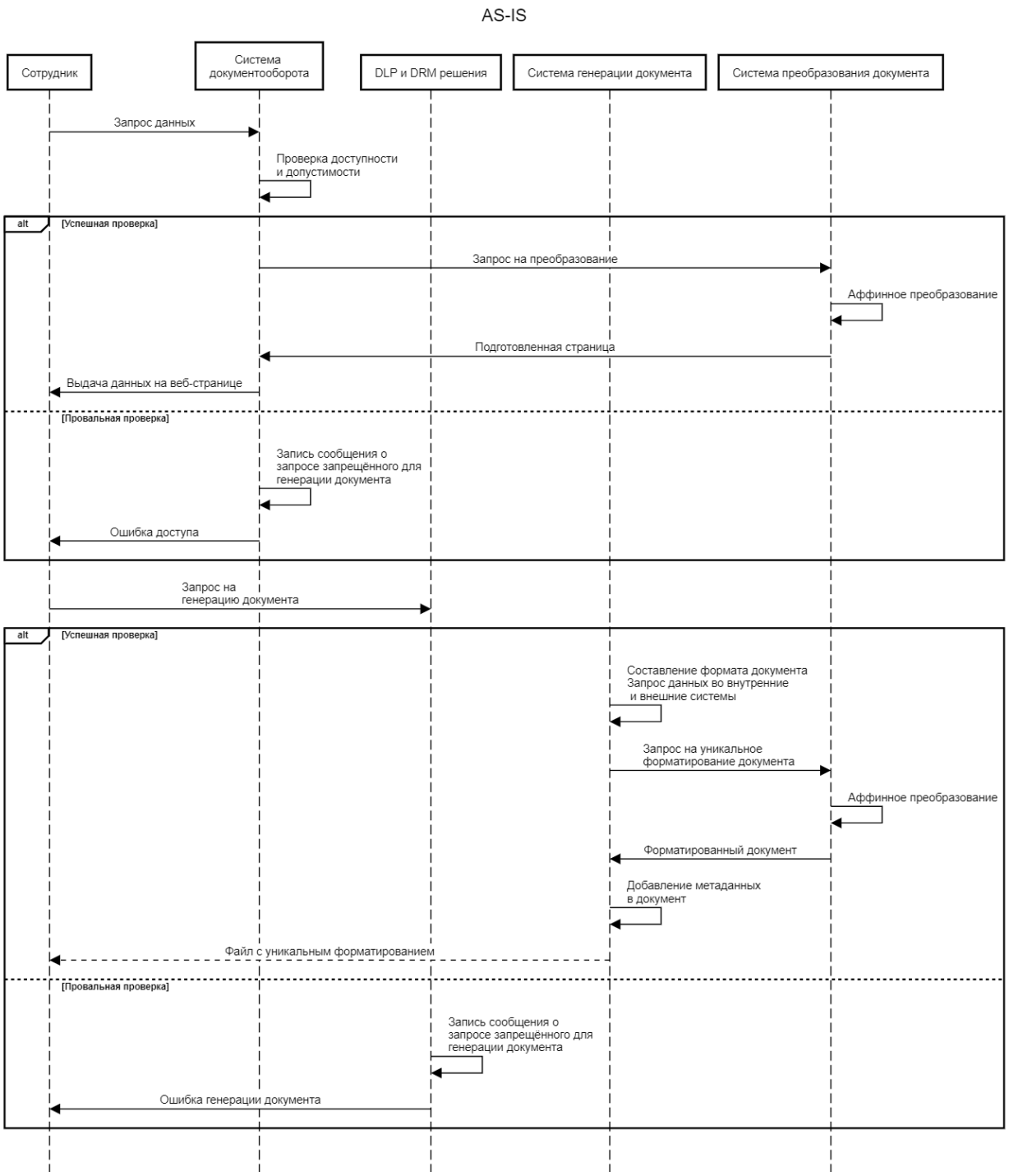

Рисунок 7 – Диаграмма последовательности процесса генерации защищенного документа AS-IS

Произведём изменение существующей модели форматирования документов, внедрив в неё описываемые ранее изменения и представим их на рисунке 8.

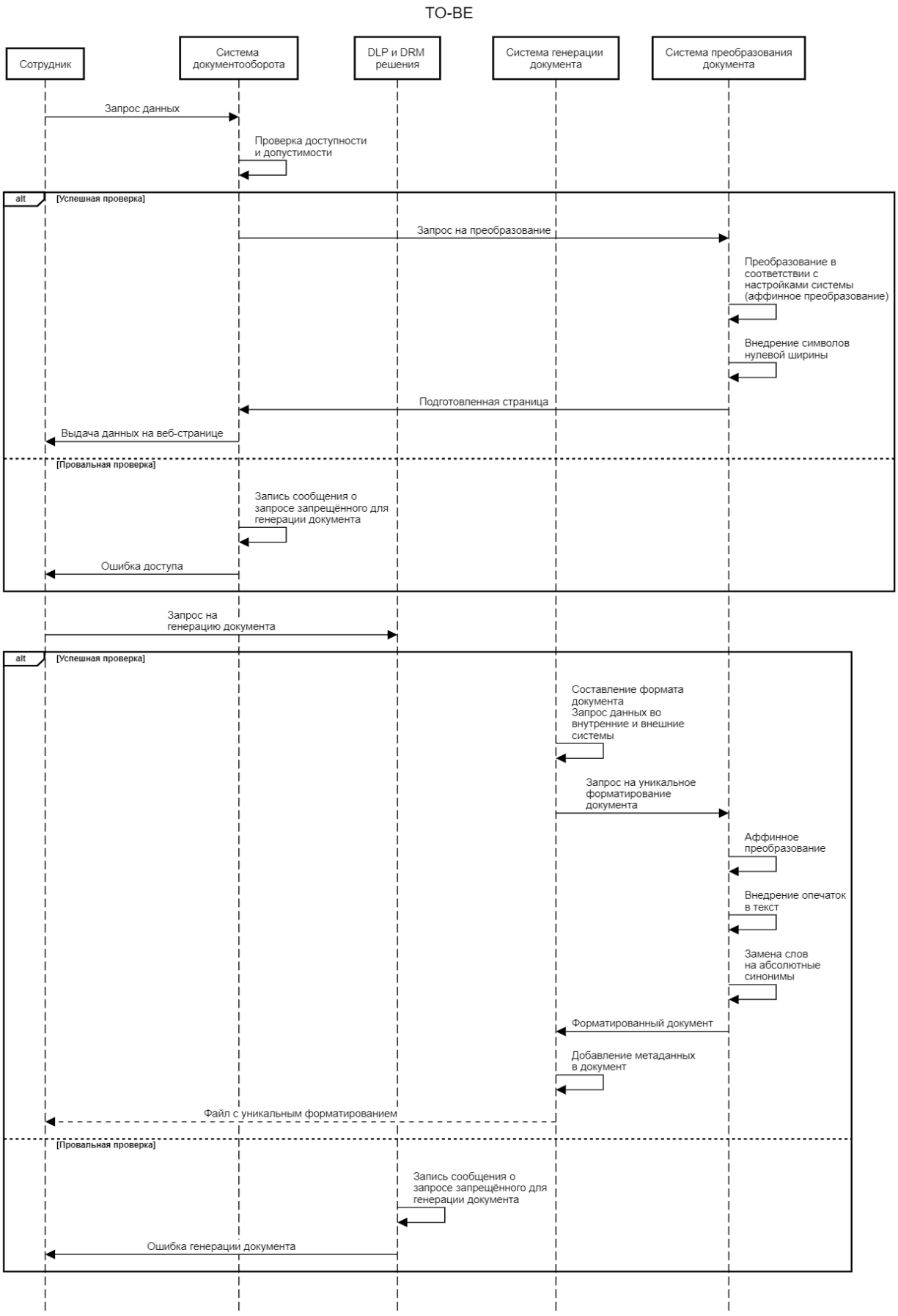

Рисунок 8 – Диаграмма последовательности процесса генерации защищенного документа TO-BE

Далее, в случае возникновения различного рода компрометирующих ситуаций, следуют различные действия. Например, когда фотография распечатанного сотрудником документа попала в Интернет, то тогда сотруднику СБ необходимо загрузить обнаруженный в сети документ в модуль распознавания, определить края документа и запустить процесс распознавания нарушителя.

В основе данного алгоритма лежит алгоритм аффинных преобразований, который модифицирует межбуквенное и межстрочное расстояние таким образом, чтобы имелась возможность однозначно определить принадлежность экземпляра и его автора.

В случае, если документ был скомпрометирован путём его копирования с веб-страницы с удалением форматирования, то тогда следующий процесс возможен только в процессе соответствующему диаграмме TO-BE.

Сотруднику СБ необходимо загрузить текст обнаруженного в сети документа в модуль распознавания символов нулевой ширины и на основе дешифровки данных определить сотрудника, который сгенерировал документ и время генерации страницы.

В том случае, если документ был скомпрометирован путём его копирования и его дальнейшего распознавания с помощью OCR инструментов или перепечатывания вручную, то тогда сотруднику СБ требуется загрузить обнаруженный документ в модуль распознавания, который сравнит имеющиеся в данном документе внедрённые опечатки и заменённые на синонимами слова, а далее сравнит данный документ с базой изменений внесённых в сгенерированные ранее документы и определит сотрудника, который сгенерировал документ и время генерации данного документа.

Следует обратить внимание на то, что две последних ситуации не затрагиваются существующими на данный момент системами документооборота и теоретически могут быть обнаружены исключительно путём внедрения изменений в нынешние процессы.

Также, в качестве одного из нововведений можно рассмотреть возможность дополнения существующей модели предложением, описанным в статье [23].

Однако, ввиду малой применимости в разрезе тематики документооборота следует оговориться, что использования защитных виньеток следует применять исключительно в случае присутствия в защищаемом документе полиграфической информации.

Так, в случае внедрения данного алгоритма, информационная ёмкость полиграфического изображения будет составлять значение, рассчитанное по формуле (3):

$$O_f = O_b + O_a * N_{el}^2 + \frac{N_c(128 + 512 + O_c)}{N_v}, \quad (3)$$

где O_f – информационная ёмкость;

O_b – базовый объем файла;

O_a – объем аффинных преобразований в изображении;

N_{el} – количество входящих элементов;

N_c – количество используемых цветов;

128 байт занимает определяющая прямую вершина;

512 байт занимает определяющая кривую вершина;

O_c – объем, который занят цветом;

N_v – количество вершин.

Так, исходя из данной формулы (3) можно выяснить, что для изображения на рисунке 1, количество элементов составляет около 500.

Выводы по разделу 3

В ходе выполнения данной части работы, на основе ранее определенных и исследованных систем электронного оборота, были определены

используемые в данный момент алгоритмы защиты и сферы их использования в системах электронного документооборота.

Далее, на основе проведённого анализа были определены сферы оптимизации существующего процесса, предложены дополнения в существующие алгоритмы защиты ввиду того, что не была предусмотрена защита от всех существующих методов несанкционированного копирования, в частности, не была проведена работа по защите от «аналоговой бреши», что является недостатком существующих разработок.

В результате, на основании проведённого анализа научных работ и существующих коммерческих разработок были созданы модели того, как выглядит существующий процесс защиты документов в системах электронного документооборота AS-IS, предложены дополнения в существующий процесс, произведён анализ реализуемости существующих предложений и вывод о возможности полноценной интеграции предложений в существующие системы электронного документооборота.

Необходимость же интеграции обусловлена тем фактом, что аналоговая брешь может использоваться в более чем 20% утечек и точно используется в, как минимум, 6-10% утечек согласно данным, полученным в результате анализа научных источников во второй НИР [15, 16, 32].

Исходя из проведённых исследований, можно сказать о том, что необходимость внедрения предложенных дополнений к существующим системам документооборота имеет место, а также то, что все поставленные задачи были выполнены.

4 Практическая реализация разработанных алгоритмов и анализ их эффективности

4.1 Анализ и разработка алгоритмов

В случае, если ограничить систему маркировки документов с остальными корпоративными системами, то сфера ее применения, скорее всего, будет ограничена только бумажным документооборотом, который, несомненно, уходит в прошлое [14].

А также, в данном случае использование маркировки вряд ли будет удобным ввиду того, что потребуется изготавливать копии для каждого загружаемого документа [12].

Однако, если интегрировать её с другими системами, тогда будет заметна существенная польза подобного решения.

Так, исходя из данных предпосылок, требуется интегрировать систему маркировки документов в систему электронного документооборота.

В СЭД выделяют несколько видов документов, которые требуют маркировки. В тех случаях, когда пользователь запрашивает подобный документ из СЭД, то требуется отправить ему маркированную копию, с данными данного пользователя [31].

Так же требуется организовать интеграцию со службами управления печатью и с корпоративными почтовыми сервисами.

Так, в случае отправки документа через почтовый сервис или отправки его на печать, сервис добавляет в документ все требуемые маркировки.

В случае если почтовый сервер, получает письмо с данной меткой, то почтовый сервер организует запрос в систему преобразования документов, который создаёт для всех адресатов изменённую специально для них копию документа.

Для организации подобной задачи на почтовый сервер инсталлируется специальный компонент, который исполняет роль транспортного агента. В

данном случае, пользователи никак не участвуют в автоматической процедуре перемаркировки документа.

Исходя из диаграммы, представленной на рисунке 8, можно сформулировать список того, что требуется реализовать для улучшения существующих систем защиты электронного документооборота, это:

- внедрение в текст символов нулевой ширины;
- замена слов в тексте на их абсолютные синонимы.
- запланированное внедрение в текст опечаток;

Реализация данных алгоритмов и их внедрение в существующие системы защиты документооборота повысит вероятность обнаружения утечек ввиду решения проблемы аналоговой бреши.

Для внедрения символов нулевой ширины требуется преобразовать требуемые для идентификации данные о пользователе в двоичный формат так, как представлено далее:

```
const spacePad = number => number + ‘00000000’.slice(String(number).length);
const translateTextToBinFormat = userData => (
  userData.split('').map(char =>
    spacePad(char.charCodeAt(0).toString(2))).join(' ')
);
```

Далее требуется преобразовать каждый исходный бит транслируемых данных в непечатаемые символы в соответствии со следующим далее алгоритмом.

Следует отметить, что ввиду технических ограничений, значениям 'α', 'β' и 'γ' соответствуют различные символы нулевой ширины, которые невозможно отобразить корректно в тексте данной работы.

```
const binToSpaceTranslate = bin => (
  bin.split('').map((binNumber) => {
    const number = parseInt(binNumber, 10);
    if (number === 1) {
      return 'α'; // zero-width space
    } else if (num === 0) {
      return 'α';
    }
    return 'γ';
  }).join('')
);
```

Далее преобразованную строку из непечатаемых символов требуется вставить в текст, который требуется защитить и в случае, если потребуется восстановить исходную строку текста, то потребуется провести обратную процедуру.

Очень небольшое количество существующих решений позволяет отображать непечатаемые символы, однако они существуют.

Также необходимо отметить, что существуют специальные браузерные и программные расширения, которые позволяют помечать непечатаемые символы специальным знаком, что позволяет принять меры по их удалению вероятному злоумышленнику.

Пример работы подобных расширений представлен на рисунке 9.

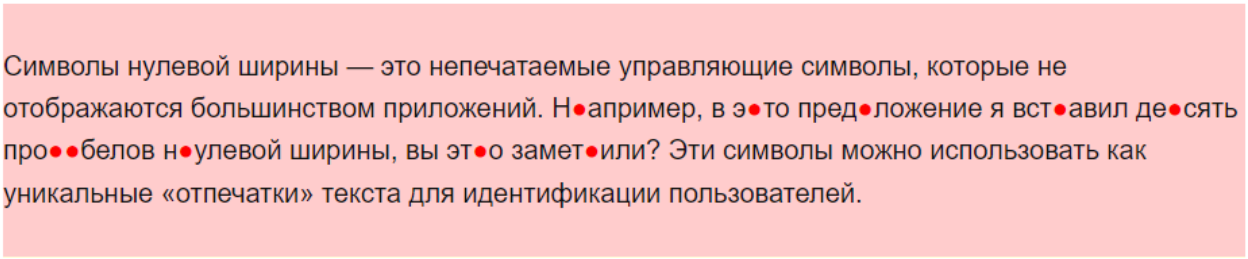

Рисунок 9 – Пример работы расширения Detect Zero-Width Characters

Следующие методики защиты позволяют деаномизировать злоумышленника даже в том случае, если непечатаемые символы были удалены.

Для реализации алгоритма замены слов наиболее оптимальным решением будет использовать решения на основе алгоритма Ахо-Корасик, который позволяет реализовать поиск во множестве подстрок из составленного ранее словаря в поданной на вход алгоритма строки [37, 43].

Данный подход позволяет сканировать текст только один раз для всего словаря составленных синонимов, а не проводить сканирование для каждого абсолютного синонима [20].

```
acho_korasik_algorythm.add_keywords_from_dict(dictionary_of_keywords)
with open('input_source_file', 'r+') as input:
    protected_replace = input.read()
    output_file = keyword_processor.replace_keywords(protected_replace)
    input.seek(0)
    input.truncate()
    input.write(output_file)
```

Представленный алгоритм позволяет заменить слова из списка абсолютных синонимов, пример которых представлен в таблице 6 на их аналоги, что позволяет определить злоумышленника если заменять их по

аналогии с кодировкой, которая используется для замены данных на символы нулевой ширины.

Точно такой же алгоритм можно использовать для внедрения в текст опечаток, кодирующих данные о пользователе, потребуется лишь заменить используемый в процессе преобразования словарь.

4.2 Проведение вычислительных экспериментов для оценки эффективности разработанных алгоритмов и оценки эффективности защиты информации в системах электронного документооборота

Для того, чтобы использовать разработанные алгоритмы необходимо убедиться, что их использование допустимо с точки зрения производительности.

Данное нефункциональное требование предъявляется к любой системе электронного документооборота и позволяет ранжировать данные системы [35].

Дополнение новых элементов в алгоритм, добавляющие новые элементы защиты в системы электронного документооборота ожидаемо повысит время обработки документов до выдачи пользователю, однако необходимо определить предельные значения.

Для расчета времени, которое требуется для обработки документа в системе электронного документооборота изначально строится функциональная модель, а затем сеть Петри-Маркова, которая моделирует то, какие процессы происходят над документом в системах электронного документооборота.

Приведём в таблице 7 основные обозначения, применяемые далее в цепи Петри-Маркова на рисунке 10.

Таблица 7 – Основные применяемые обозначения в рисунке 10

Номер процедуры	Название
Процедура 1.1	Приём входящего документа
Процедура 1.2	Регистрация входящего документа
Процедура 1.3	Сканирование документа
Процедура 1.4	Уведомление о сканировании
Процедура 1.5	Определение исполнителей
Процедура 1.6	Определение предельных дат реализации
Процедура 1.7	Контроль за датами для осуществления требуемых действий с документом
Процедура 1.8	Регистрация описания документа во внутренней системе
Процедура 1.9	Регистрация описания документа во внешней системе
Процедура 1.10	Процедура передачи документа в архив или его уничтожение

Исходя из тематики данной работы, описание внутренней структуры электронного документооборота представляется излишней ввиду того, что похищение документа путём эксплуатации аналоговой бреши возможно на любом из вложенных этапов, если оно возможно на более высоком уровне.

Так, можно представить процесс циркуляции документа в системе электронного документооборота в виде сети Петри-Маркова так, как представлено далее на рисунке 10.

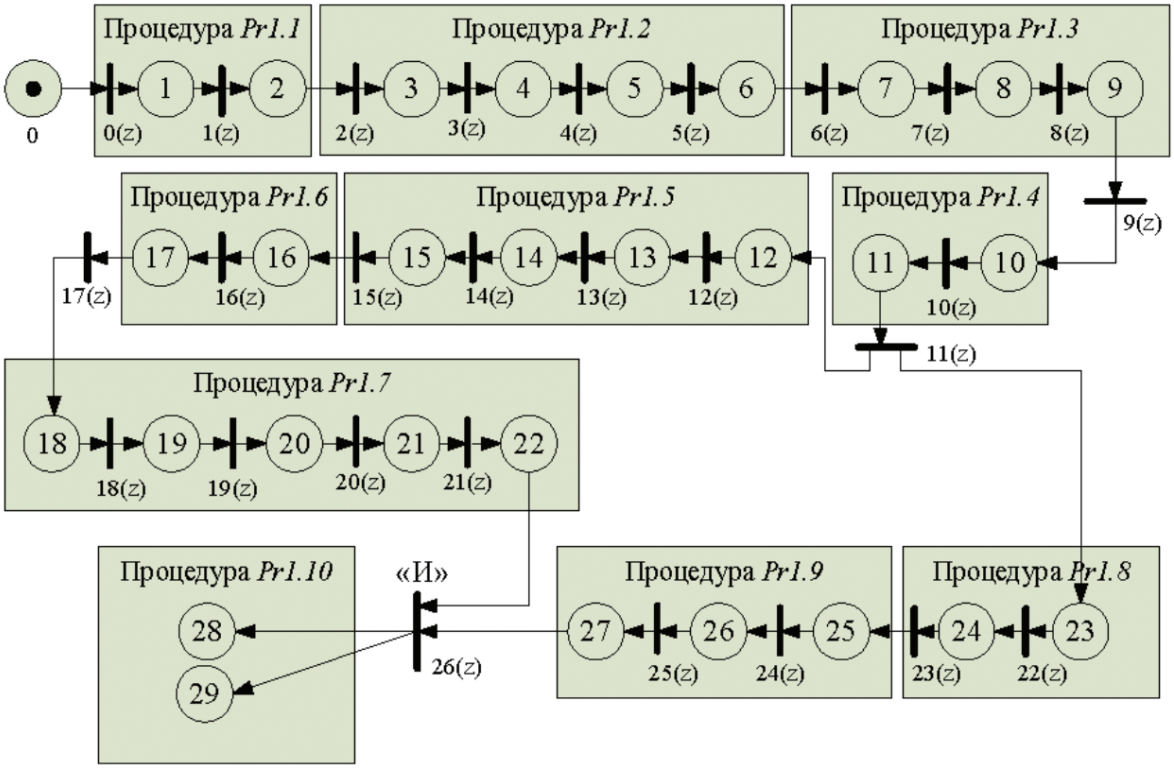

Рисунок 10 – Циркуляция документа в системе электронного документооборота в виде графа сети Петри-Маркова

Так, исходя из представленного изображения, можно утверждать, что похищение документа в виде OCR копии возможно, как минимум в следующих процедурах:

- процедура 1.1 Приём входящего документа;
- процедура 1.2 Регистрация входящего документа;
- процедура 1.3 Сканирование документа;
- процедура 1.8 Регистрация описания документа во внутренней системе;
- процедура 1.9 Регистрация описания документа во внешней системе;
- процедура 1.10 Процедура передачи документа в архив или его уничтожение.

Исходя из проведённого анализа можно утверждать, что как минимум в 60% всех процессов, которые проводятся над документом он подвергается риску похищения со стороны злоумышленника.

Далее необходимо определить то, насколько замедляют выдачу электронного документа существующие алгоритмы защиты информации и насколько сильно их будут замедлять предлагаемые алгоритмы. Для проверки были проведены численные эксперименты на документе общим весом 15 и 30 мегабайт и представляющим из себя усреднённую модель существующих в системе электронного документооборота документов, усреднённые результаты которых представлены в таблице 8.

Таблица 8 – Результаты численных экспериментов

Название системы	Система шифрования данных	Время выдачи документа для документа размером 15 мегабайт, секунды	Время выдачи документа для документа размером 15 мегабайт, секунды
1	2	3	4
А2Б СЭД	Отсутствует	69	138
ELMA365 ECM	Наличествует	290	580
Контур.Диадок	Отсутствует	65	122
ЭТЛАС	Наличествует	138	276
DocSpace	Наличествует	291	582
LanDocs	Наличествует	255	510
OPTIMA-WorkFlow	Наличествует	171	342
OpenText Professional Services	Отсутствует	26	42

Продолжение таблицы 8

1	2	3	4
Е1 Евфрат	Отсутствует	226	452
1С:Документооборот 8	Наличествует	168	336
СЭД «ДЕЛО»	Наличествует	97	194
TESSA	Наличествует	203	406
Alfresco	Наличествует	45	90
IBM Aspera® on Cloud	Наличествует	155	310
WSS Docs	Наличествует	266	532
Verdox	Наличествует	210	420
DIRECTUM	Наличествует	211	422
ЛОГИКА: СЭД	Наличествует	229	458
ТЕЗИС	Наличествует	228	456
АЛТИУС – Исполнительная документация	Наличествует	84	168
Lexema-ECM	Наличествует	419	918

Исходя из анализа данных в таблице можно сделать вывод о том, что существует прямая корреляция относительно скорости подготовки документа и использованию в системе шифрования.

Далее, проведём анализ того, насколько сильно предлагаемые изменения повлияют на скорость генерации документа.

Ввиду того, что предложенные изменения состоят из нескольких алгоритмов, опишем их влияние по порядку.

Использование синонимичных преобразований текста отчётов.

Время выполнения данного алгоритма линейно зависит от размера входного документа, что позволяет утверждать, что трудоёмкость данного алгоритма составляет $O(n)$.

График трудоёмкости применения данного алгоритма на входных файлах разного объёма, представленный на рисунке 11 подтверждает данное утверждение.

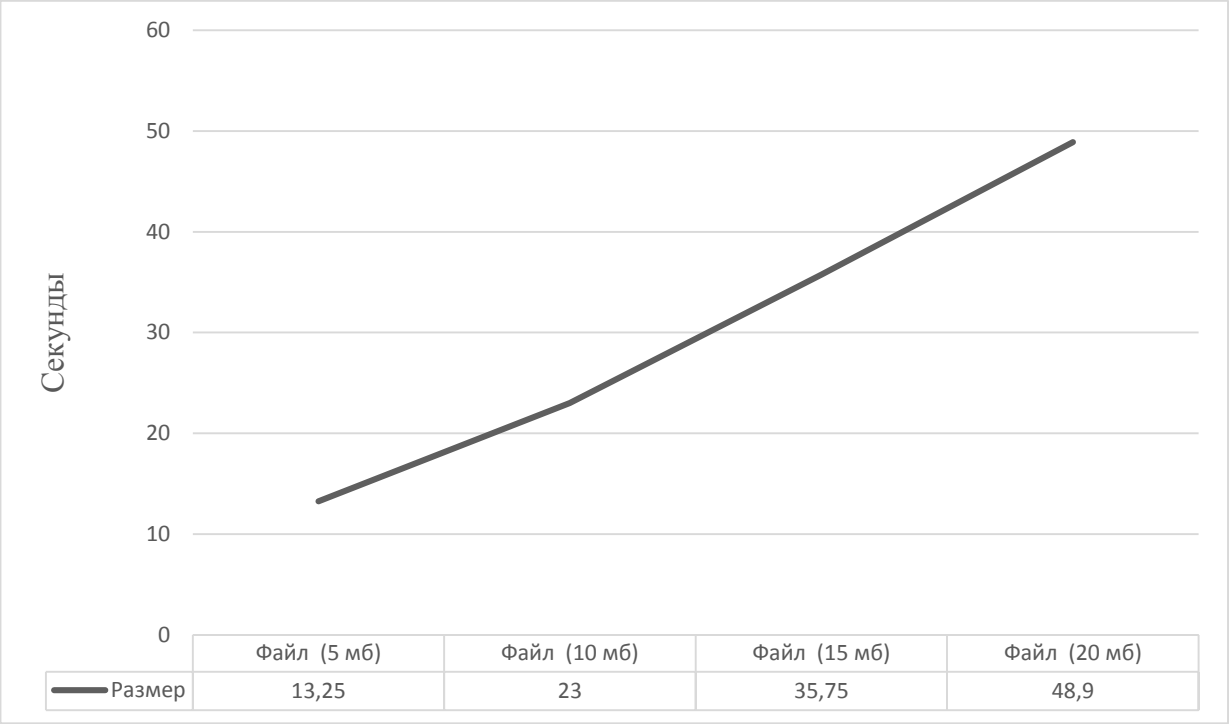

Рисунок 11 – График зависимости времени от размера входного файла для алгоритма синонимичного преобразования текста

Преднамеренное внесение в текст уникальных копий опечаток.

Время выполнения данного алгоритма так же линейно зависит от размера входного документа, что позволяет утверждать, что трудоёмкость данного алгоритма составляет значение, вычисляемое по формуле (4)

$$O(n + t), \quad (4)$$

где t – количество всех возможных вхождений всех строк-образцов в текст.

График трудоёмкости применения данного алгоритма на входных файлах разного объёма, представленный на рисунке 12 подтверждает данное утверждение.

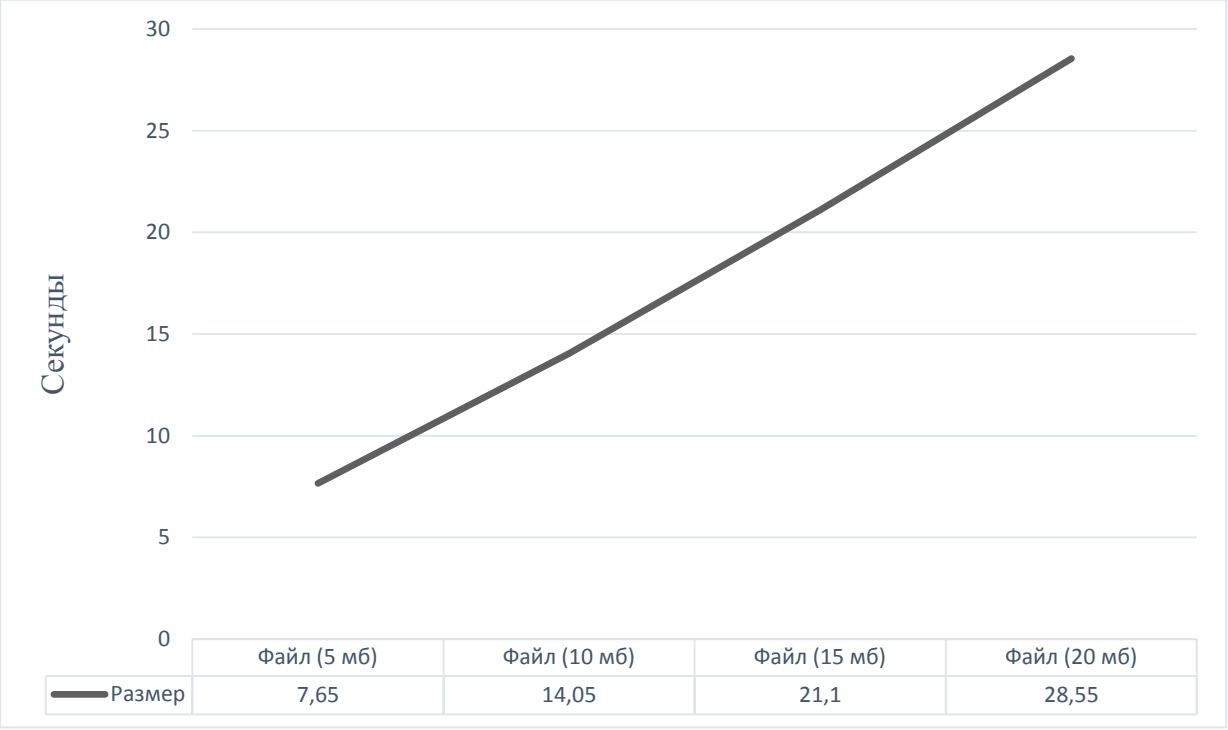

Рисунок 12 – График зависимости времени от размера входного файла для алгоритма для внесения опечаток в текст уникальных копий

Внедрение символов нулевой ширины.

Время выполнения данного алгоритма зависит не зависит от размера входного документа ввиду того, что внесение изменений не требует знаний о содержимом файла.

Так, если минимально требуемой единицей для идентификации пользователя является сам файл, то можно утверждать, что трудоёмкость данного алгоритма составляет $O(1)$.

Также, в случае если в качестве минимально требуемой единицы используется страница или абзац текста, то время выполнения алгоритма (относительно страницы или абзаца) ожидаемо не изменится и составит $O(1)$, что видно исходя из графика, представленного на рисунке 13.

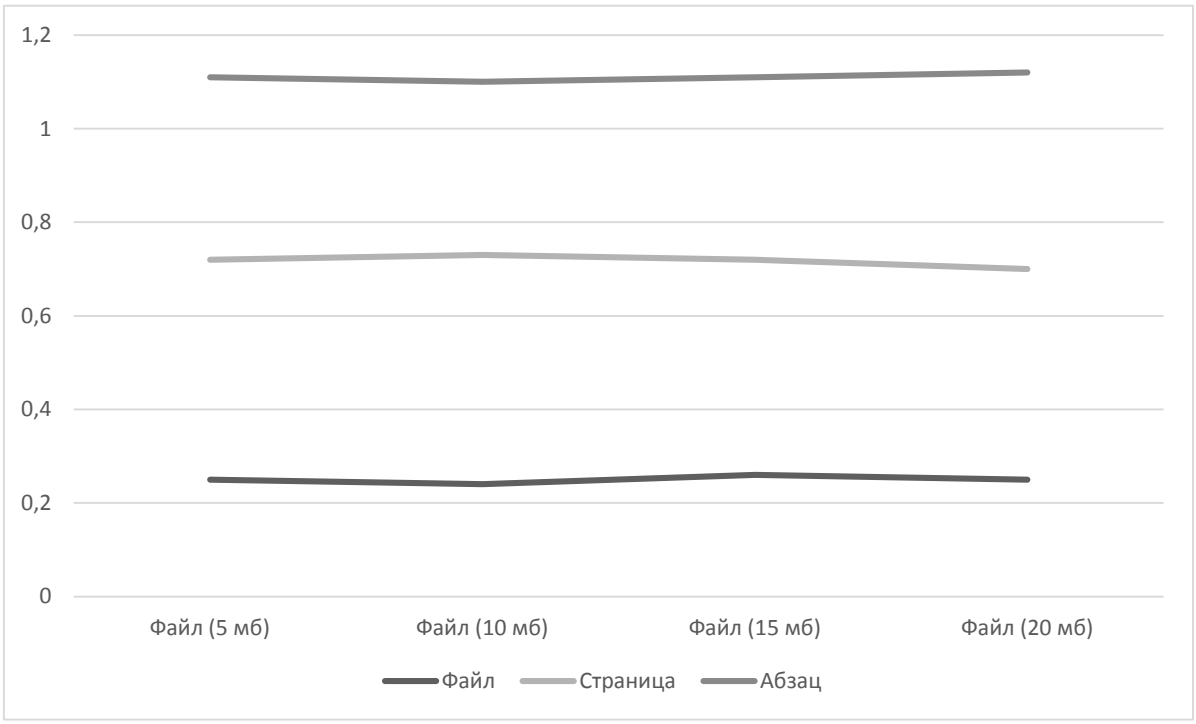

Рисунок 13 – График зависимости времени от размера входного файла для алгоритма внедрения символов нулевой ширины для файла, страницы или абзаца

В случае если в качестве минимально требуемой единицы используется страница или абзац текста, то время внедрения символов нулевой ширины

относительно файла будет подчиняться линейному закону $O(n)$ так как представлено на рисунке 14.

Данные полученные и отображенные на данном рисунке свидетельствуют о том, что применять данный алгоритм для внедрения в каждый абзац текста представляется избыточным ввиду крайне высокой длительности данной операции.

Исходя их этого предлагается использовать вариант с внедрением нечитаемых символов как минимум один раз на файл или, если размер файла позволяет, то один раз на страницу.

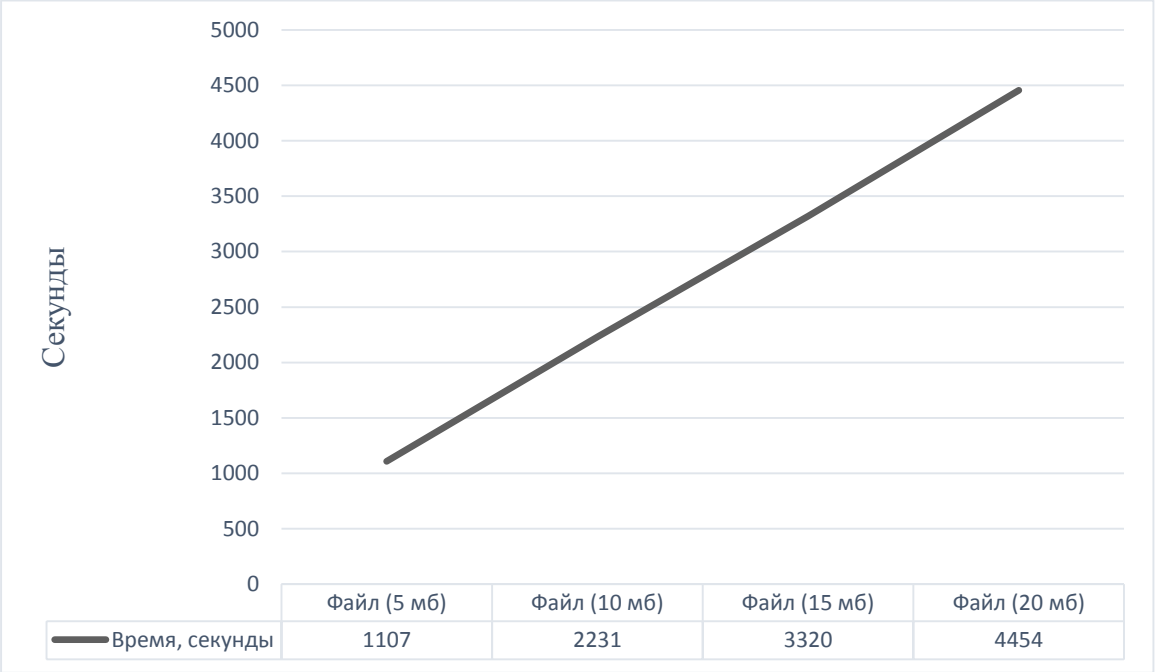

Рисунок 14 – График зависимости времени для абзаца от размера входного файла для алгоритма внедрения символов нулевой ширины

Исходя из представленных ранее графиков можно сделать вывод о том, что влияние на общее время генерации файла будет несущественным и будет составлять порядка 20% от среднего времени генерации в случае, если использовать генерацию символов нулевой ширины постранично для документов небольшого размера.

В случае если использовать пофайловое внедрение символов нулевой ширины и все остальные предлагаемые алгоритмы, то общее время генерации файла повысится на 38 секунд, что составляет 20,74% от среднего времени генерации в исследуемых системах электронного документооборота при минимальном значении в 9,07% для Lexema-ECM и максимальном 146,15% для OpenText Professional Services.

Подобное высокое значение для OpenText Professional Services связывается с тем, что данная система электронного документооборота не включает в себя функционал защиты документов и генерирует их без предварительных вычислений.

В случае если исключить из списка рассматриваемых систем те, которые не включают в себя функции защиты документооборота, то доля предлагаемых к внедрению дополнительных алгоритмов в общей доле времени на генерации снизится до 18,67%.

Выводы по разделу 4

В ходе выполнения данной части работы, на основе ранее определенных сфер оптимизации существующего процесса и предложенных дополнений в существующие алгоритмы защиты были реализованы следующие алгоритмы:

- внедрение в текст символов нулевой ширины;
- замена слов в тексте на их абсолютные синонимы.
- запланированное внедрение в текст опечаток;

Необходимость интеграции подтверждается тем фактом, что аналоговая брешь может использоваться в более чем 20% утечек и точно используется в, как минимум, 6-10% утечек согласно данным [15, 16, 32].

На основе ранее разработанной модели того, как выглядит существующий процесс защиты документов в системах электронного документооборота AS-IS и на основе предложенных дополнений в

существующий процесс, были произведены вычислительные проверки того, насколько затратным представляется использование данных алгоритмов.

Исходя из проведённых проверок разработанных алгоритмов, можно сделать вывод о том, что существует возможность и необходимость полноценной интеграции предложений в существующие системы электронного документооборота, а также то, что все поставленные задачи данного раздела были выполнены.

Заключение

В ходе выполнения данной работы были изучены научные работы, исследована литература по теме шифрования данных и организации документооборота, законы и подзаконные акты проведено всестороннее исследование методов и алгоритмов оптимизации и защиты электронного документооборота.

В существующих системах документооборота недостаточное внимание уделено защите хранимых документов, а также представленных в них персональных данных пользователей.

А ввиду усиливающейся протекционистской политики государств, список допустимых к использованию в системах документооборота систем ещё более сокращается.

Исходя из проведённого анализа, в существующих системах не предлагается таких функций, которые позволили бы защитить информацию от различных форм аналогового копирования.

Это позволяет злоумышленнику беспрепятственно воспользоваться известной фундаментальной уязвимостью под названием «Аналоговая брешь».

В соответствии настоящим законодательством РФ, при хранении и передаче персональных данных, Федеральный закон «О персональных данных» устанавливает требование: «Оператор обязан применить ряд организационных и технических мер, касающихся процессов обработки персональных данных, а также информационных систем, в которых эти персональные данные обрабатываются».

Исходя из данной выдержки, можно сделать вывод о необходимости осуществлять защиту данных в информационных системах.

В результате анализа был сформирован список законов и подзаконных актов, которые регулируют данную тему, которые представлены ранее в таблице 1.

Также, можно сказать о том, что существующие методики оптимизации хранения данных в системах документооборота не имеют достаточной степени направленности на решение поставленной задачи, что позволяет произвести оптимизацию существующих.

В результате, на основании анализа данных работ были сделаны выводы о необходимости осуществлять защиту данных в информационных системах, о недостаточном освещении данной темы в источниках, были исследованы существующие алгоритмы и подобраны оптимальные.

Программы, созданные для защиты конфиденциальных данных от утечек, можно интегрировать с системой документооборота.

Решение заключается в получении каждым сотрудником, при предоставлении ему документа, немного отличную копию от исходного текста, в которых закодированы некоторые параметры, позволяющие определить:

– алгоритм преобразования документа;

– время и дату создания документа и его изменённой версии;

– устройство, получившее индивидуальную копию документа;

– идентификатор того сотрудника, который получил индивидуальную копию.

Данное решение даёт возможность определить по документу, (его фотографии или скриншоту) утечка которого была произведена:

– с какого аккаунта произведена утечка;

– с какого устройства произведена утечка;

– дату и время утечки.

Так же, в случае информирования сотрудников о существовании системы защиты, система получит и превентивную функцию, так как каждый сотрудник будет знать то, что его участие в утечке может быть оперативно определено.

В результате работы была разработана модель системы документооборота, направленная на повышение защищенности, определено

место предлагаемых алгоритмов в общей структуре в системах электронного документооборота, апробирована их эффективность, соответствие поставленным в данной работе целям и определены перспективы дальнейшего использования предложенных решений.

Также было проведено исследование применимости использования данных алгоритмов относительно временных затрат на их внедрение в используемые системы. Результат показал, что среднее время, затрачиваемое на процесс генерации документа, увеличилось в среднем не более чем на 20% относительно средних по существующим системам электронного документооборота проводящих защиту своих данных, что позволяет говорить, что нефункциональное требование о скорости генерации документа не будет нарушено.

Таким образом, можно сказать, что все задачи, поставленные в данной работе, были выполнены, а следовательно, цель данной работы была в полной мере достигнута.

Список используемой литературы

1. Алифирова, А.М. К вопросу о ведении электронного документооборота в организации / А.М. Алифирова, В.П. Васильев // Символ науки. – 2016. – №6-1. – С.133-135.

2. Бакунова, О.М., Применение электронного документооборота в программе 1С / О.М. Бакунова, Е.В. Анохин, А.Ф. Палуйко, Е.Н. Александрович, Е.Д. Антонов, М.Ю. Ситник, И.С. Гречко, Д.М. Кабаков // International Journal of Innovative Technologies in Economy. – 2018. – №4 (16). – С. 64-66.

3. Белов С.П. Подготовка предприятий к внедрению систем электронного документооборота. Монография. – М.: Мир науки, 2016. – 210 с. 7. Б

4. Берников, В.О. Сравнительный анализ криптостойкости симметричных алгоритмов шифрования // Труды БГТУ. Серия 3: Физико-математические науки и информатика. 2020. №1 (230). URL: https://www.cyberleninka.ru/article/n/sravnitelnyy-analiz-kriptostoykosti-simmetrichnyh-algoritmov-shifrovaniya (дата обращения: 01.06.2020).

5. Владычанский, Т.В. Электронный документооборот предприятий малого бизнеса / Т.В. Владычанский // Символ науки. – 2016. – №5-2. – С. 246-249.

6. Воронина, Е.И. Система электронного документооборота в бухгалтерском учете / Е.И. Воронина // Economics. – 2018. – №4 (36). – С. 77-79.

7. Дмитриев, М.А. Возможные варианты повышения криптостойкости алгоритмов шифрования на основе конструкции Ниберг // Сибирский журнал науки и технологий. 2017. №3. URL: https://www.cyberleninka.ru/article/n/vozmozhnye-varianty-povysheniya-kriptostoykosti-algoritmov-shifrovaniya-na-osnove-konstruktsii-niberg (дата обращения: 01.06.2020).

8. Дорохин, С.В., Качков, С.С., Сидоренко, А.А. Реализация блочного шифра «Кузнечик» с использованием векторных инструкций // Труды МФТИ. 2018. №4 (40). URL: https://www.cyberleninka.ru/article/n/realizatsiya-blochnogo-shifra-kuznechik-s-icpolzovaniem-vektornyh-instruktsiy (дата обращения: 02.04.2020).

9. Дюсембаев, У.М., Смагулова, А.С., Искаков, М.Б. ВОПРОСЫ ЗАЩИТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА // E-Scio. 2020. №5 (44). URL: https://www.cyberleninka.ru/article/n/voprosy-zaschity-informatsionnoy-bezopasnosti-elektronnogo-dokumentooborota (дата обращения: 03.04.2022).

10. Жильников, А.Ю. Электронный документооборот / А.Ю. Жильников, О.С. Михайлова // Территория науки. – 2017. – №2. – С. 116-120.

11. Запольских О.М. Электронный документооборот - повышение эффективности управления организацией // Ученые записки Тамбовского отделения РоСМУ. 2018. №11. URL: https://www.cyberleninka.ru/article/n/elektronnyy-dokumentooborot-povyshenie-effektivnosti-upravleniya-organizatsiey (дата обращения: 24.10.2020).

12. Иванова Елена Владимировна Электронный документооборот как форма современного делопроизводства // Гуманитарий Юга России. 2017. №1. URL: https://www.cyberleninka.ru/article/n/elektronnyy-dokumentooborot-kak-forma-sovremennogo-deloproizvodstva (дата обращения: 24.10.2020).

13. Иващенко А.С. Анализ и оптимизация систем электронного документооборота для образовательных учреждений // Обучение и воспитание: методики и практика. 2014. №14. URL: https://www.cyberleninka.ru/article/n/analiz-i-optimizatsiya-sistem-elektronnogo-dokumentooborota-dlya-obrazovatelnyh-uchrezhdeniy (дата обращения: 16.12.2020).

14. Исачкова, Л.Н. ОБЕСПЕЧЕНИЕ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ В СИСТЕМЕ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ БИЗНЕСА / Л.Н. Исачкова,

Н.А. Асанова, С.Ю. Хут, Ф.Р. Ешугова // Вестник Академии знаний. 2021. №4 (45). URL: https://www.cyberleninka.ru/article/n/obespechenie-ekonomicheskoy-bezopasnosti-v-sisteme-elektronnogo-dokumentooborota-v-usloviyah-tsifrovoy-transformatsii-biznesa (дата обращения: 03.04.2022).

15. Исследование GfK: Проникновение Интернета в России [Электронный ресурс]. URL: https://www.gfk.com/ru/press/issledovanie-gfk-proniknovenie-interneta-v-rossii-1 (дата обращения: 12.12.20).

16. Исследование аналитического центра InfoWatch: Глобальное исследование утечек конфиденциальной информации в первом полугодии 2019 года [Электронный ресурс]. URL: https://www.infowatch.ru/sites/default/files/report/analytics/russ/Global_Data_Leaks_Report_2019_half_year.pdf (дата обращения: 22.06.21)

17. Ищукова, Е.А. Разработка и реализация высокоскоростного шифрования данных с использованием алгоритма Кузнечик / Е. А. Ищукова, Р. А. Кошуцкий, Л. К. Бабенко // Auditorium. 2015. №4. URL: https://www.cyberleninka.ru/article/n/razrabotka-i-realizatsiya-vysokoskorostnogo-shifrovaniya-dannyh-s-ispolzovaniem-algoritma-kuznechik (дата обращения: 01.06.2020).

18. Королев И.Д., Мезенцев А.С., Махнев А.П. [и др.] Анализ систем электронного документооборота по распределению электронных документов в дела // Вопросы технических и физико-математических наук в свете современных исследований: сб. ст. по матер. III-IV междунар. науч.- практ. конф. No 3-4(3). – Новосибирск: СибАК, 2018. – С. 6-11.

19. Кудрина М. А., Мурзин А. В. Аффинные преобразования объектов в компьютерной графике // НиКа. 2014. №. URL: https://www.cyberleninka.ru/article/n/affinnye-preobrazovaniya-obektov-v-kompyuternoy-grafike (дата обращения: 03.04.2022).

20. Мазуренко А. В., Болдырихин Н. В. Ускоренный препроцессинг в задаче поиска подстрок в строке // Advanced Engineering Research. 2019. №3.

URL: https://www.cyberleninka.ru/article/n/uskorennyy-preprotsessing-v-zadache-poiska-podstrok-v-stroke (дата обращения: 23.01.2022).

21. Маро, Е.А. Реализация алгебраической атаки на шифры ГОСТ Р 34. 12-2015 // ИВД. 2015. №4-2. URL: https://www.cyberleninka.ru/article/n/realizatsiya-algebraicheskoy-ataki-na-shifry-gost-r-34-12-2015 (дата обращения: 01.06.2020).

22. Медяк, Д.М., Трусевич Н.Э. Исследование стойкостных свойств специальных печатных красок // Труды БГТУ. Серия 4: Принт- и медиатехнологии. 2020. №1. URL: https://www.cyberleninka.ru/article/n/issledovanie-stoykostnyh-svoystv-spetsialnyh-pechatnyh-krasok (дата обращения: 03.04.2022).

23. Новосельская, О.А., Савчук, Н.А., Щербакова А.Н. [и др.] Алгоритмы и программное средство для генерации защитных изображений печатных документов // Труды БГТУ. Серия 3: Физико-математические науки и информатика. 2022. №1 (254). URL: https://www.cyberleninka.ru/article/n/algoritmy-i-programmnoe-sredstvo-dlya-generatsii-zaschitnyh-izobrazheniy-pechatnyh-dokumentov (дата обращения: 24.03.2022).

24. Парамонова, М.Г. Системы электронного документооборота / М.Г. Парамонова // Ученые записки Тамбовского отделения РоСМУ. – 2018. – №12. – С. 194-198.

25. Приказ ФСТЭК России от 18 февраля 2013 г. №21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

26. Приказ ФСТЭК России от 31 августа 2010 г. №489 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

27. Сагиндыков, Б.Ж., Эллиптические числа и их аффинные преобразования / А. Канатова, Н. Абуханова, // Естественные и математические науки в современном мире. 2016. №3 (38). URL: https://www.cyberleninka.ru/article/n/ellipticheskie-chisla-i-ih-affinnye-preobrazovaniya (дата обращения: 03.04.2022).

28. Соколов А.В., Жданов О.Н. Нелинейные преобразования конструкции Ниберг над изоморфными представлениями полей Галуа // Системный анализ и прикладная информатика. 2017. №3. URL: https://www.cyberleninka.ru/article/n/nelineynye-preobrazovaniya-konstruktsii-niberg-nad-izomorfnymi-predstavleniyami-poley-galua (дата обращения: 01.06.2020).

29. Толоманенко, Е.А. Дифференциальный анализ трех раундов шифра «Кузнечик» // Доклады ТУСУР. 2018. №2. URL: https://www.cyberleninka.ru/article/n/differentsialnyy-analiz-treh-raundov-shifra-kuznechik (дата обращения: 01.06.2020).

30. Указ Президента Российской Федерации от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»

31. Ушаков, Н.О., Сибикина, И.В., Космачева, И.М. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СИСТЕМАХ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА // Техническая эксплуатация водного транспорта: проблемы и пути развития. 2021. №1. URL: https://www.cyberleninka.ru/article/n/informatsionnaya-bezopasnost-v-sistemah-elektronnogo-dokumentooborota (дата обращения: 03.04.2022).

32. Харченко, А.Ю., Харченко, Ю.А. Анализ и определение рисков информационной безопасности // Вестник науки и образования. 2020. №6-1 (84). URL: https://www.cyberleninka.ru/article/n/analiz-i-opredelenie-riskov-informatsionnoy-bezopasnosti-1 (дата обращения: 01.06.2020).

33. Шевцова, Г.А. Особенности внедрения системы защищенного электронного документооборота // История и архивы. 2016. №2 (4). URL:

https://www.cyberleninka.ru/article/n/osobennosti-vnedreniya-sistemy-zaschischennogo-elektronnogo-dokumentooborota (дата обращения: 16.12.2020).

34. Шишин, И.О. Информационные технологии управления документами. - СПб.: Санкт-Петербургский государственный экономический университет, 2017. – 78 с.ф

35. Язов Ю.К. К вопросу об оценке эффективности защиты информации в системах электронного документооборота / Ю.К. Язов, Авсентьев О.С., И.О. Рубцова // Вопросы кибербезопасности. – 2019. – № 1 (29). URL: https://www.cyberleninka.ru/article/n/k-voprosu-ob-otsenke-effektivnosti-zaschity-informatsii-v-sistemah-elektronnogo-dokumentooborota (дата обращения: 03.04.2022).

36. Яппаров Р.М. Некоторые проблемы защиты конфиденциальной информации в системах электронного документооборота // Вестник УЮИ. 2019. №1 (83). URL: https://www.cyberleninka.ru/article/n/nekotorye-problemy-zaschity-konfidentsialnoy-informatsii-v-sistemah-elektronnogo-dokumentooborota (дата обращения: 03.04.2022).

37. Amaran S. et al. Simulation optimization: a review of algorithms and applications //Annals of Operations Research. – 2016. – Т. 240. – №. 1. – С. 351-380.

38. Baratov D. X. The issues of creating a formalized model of the technical documentation // International Scientific Journal «Internauka». – 2017. – №. 4 (1). – С. 22-23.

39. Han Qiu. An Efficient Data Protection Architecture Based on Fragmentation and Encryption // Télécom ParisTech Spécialité “Informatique et Réseaux” 2018 [Электронный ресурс]. URL: https://www.researchgate.net/publication/323746675_An_Efficient_Data_Protection_Architecture_Based_on_Fragmentation_and_Encryption (дата обращения: 24.10.2020).

40. Hunter S. R. et al. An Introduction to Multiobjective Simulation Optimization //ACM Transactions on Modeling and Computer Simulation (TOMACS). – 2019. – Т. 29. – №. 1. – С. 7.

41. Krasnyanskiy M. N. et al. Algorithm for Structural and Parametric Synthesis of Electronic Document Management System of Research and Education Institution //Journal of Applied Sciences. – 2016. – Т. 16. – №. 7. – С. 332-337.

42. Martínez G. S. et al. An integrated implementation methodology of a lifecycle-wide tracking simulation architecture // IEEE Access. – 2018. – Т. 6. – С. 15391-15407.

43. Okun V. "Aho-Corasick", in Dictionary of Algorithms and Data Structures // National Institute of Standards and Technology. – 2020. [Электронный ресурс]. URL: https://www.nist.gov/dads/HTML/ahoCorasick.html (дата обращения: 12.12.2021).

44. Schwabach A. Internet and the Law: Technology, Society, and Compromises, 2nd Edition // Athens Journal of Law - Volume 3, Issue 3. – 2014. P. 201-214.