Министерство образования Республики Беларусь
Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

УДК 004.056+004.738.5:005.92

На правах рукописи

ПРИСТАВКА
Елена Сергеевна

МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ В СИСТЕМАХ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА НА БАЗЕ DOCSVISION И DIRECTUM

АВТОРЕФЕРАТ
диссертации на соискание степени

магистра техники и технологий

по специальности 1-39 81 01 – Компьютерные технологии

проектирования электронных систем

Минск 2018

Работа выполнена на кафедре проектирования информационно-компьютерных систем учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»

Научный руководитель: **ЛИХАЧЕВСКИЙ Дмитрий Викторович,** декан ФКП, кандидат технических наук, доцент кафедры проектирования информационно-компьютерных систем учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»

Рецензент: **ТОНКОВИЧ Ирина Николаевна,** заведующая кафедрой информационных технологий МИУ, кандидат химических наук, доцент

Защита диссертации состоится «26» июня 2018 г. года в $13^{\underline{00}}$ часов на заседании Государственной экзаменационной комиссии по защите магистерских диссертаций в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники» по адресу: 220013, Минск, ул. П.Бровки, 6, копр. 1, ауд. 415, тел. 293-20-80, e-mail: kafpiks@bsuir.by

С диссертацией можно ознакомиться в библиотеке учреждения образования «Белорусский государственный университет информатики и радиоэлектроники».

ВВЕДЕНИЕ

В последние годы наметился переход от традиционной формы представления документов к электронным документам (ЭД).

Переход к электронному документообороту несет целый ряд преимуществ. Прежде всего, введение ЭД позволит существенно сократить сроки разработки и прохождения новых документов в структуре предприятия, упростить работу по формированию и пересылке пакетов документов между предприятиями и территориально распределенными офисами одного предприятия. Использование систем электронного документооборота послужит фундаментом для формирования единого информационного пространства предприятия. Введение электронных архивов документов позволит значительно сократить бумажный архив любого предприятия и обеспечить возможность быстрого поиска и предоставления электронных копий документов. Предполагается также ощутимая экономическая выгода.

Основу для создания защищенного документооборота организации сегодня видят по-разному: одни – в повышении эффективности нормативно-правовых мер защиты информации, другие – в повышении эффективности технических мер по защите информации.

Защищенная система электронного документооборота (СЭД) должна обеспечивать сохранность и подлинность документов, безопасный доступ и протоколирование действий пользователей в условиях потенциальных угроз информационной безопасности.

Вопросы, связанные с противодействием разглашению, перехвату и передаче третьей стороне электронных документов в настоящий момент все еще остаются нерешенными. В тоже время, все большее количество коммерческих организаций сталкивается с жесткой конкурентной борьбой. Современные условия требуют обязательного документирования по сути всех стратегических и тактических решений принимаемых руководством в целях обеспечения более эффективной работы на рынке. Получение или перехват подобных документов или их копий конкурентами, может повлечь за собой серьезные финансовые потери и (или) подорвать имидж организации в глазах потенциальных клиентов. Растущая информатизация современного общества и переход к электронным формам хранения и представления информации несут за собой новые потенциальные угрозы информационной безопасности коммерческих организаций.

Существующие механизмы обеспечения защиты информации не в состоянии решить ряд специфических задач характерных для электронного документооборота. В частности использование открытых каналов связи для предоставления, передачи и распространения ЭД чревато возможным перехватом документов третьей стороной. В отличие от бумажного документа, передаваемого в единичном экземпляре, копии ЭД создаваемые при его передаче по каналам связи могут долгое время храниться на почтовых ящиках пользователей и серверах провайдеров. В результате, если

доступ к обычным документам возможен только физически непосредственно в процессе их передачи, то для получения доступа к электронному документу в современных условиях злоумышленнику предоставляется большое разнообразие возможностей. Доступ к множеству копий ЭД может быть осуществлен удаленно без непосредственного физического доступа к материальным носителям и растянут во времени на период хранения электронных копий. При этом ни отправитель, ни получатель электронных документов могут и не догадываться о наличии хранимых копий и факте получения доступа к ним и перехвата исходных электронных документов в процессе передачи третьей стороной.

В условиях невозможности обеспечения абсолютного контроля каналов связи и недопущения несанкционированного доступа (НСД) к информации со стороны третьих лиц, защита информации может быть основана на применении средств криптографии и стеганографии. При этом ни одно из указанных направлений на текущем уровне развития не в состоянии самостоятельно решить все задачи связанные с защитой информации в электронном документообороте. Очевидно, что решение некоторых задач возможно только при совместном согласованном применении методов криптографии и стеганографии.

Актуальными задачами являются защита аппаратных средств и прочих устройств подсистем СЭД; защита сетевой среды, в которой функционирует СЭД, а также защита каналов передачи данных и сетевого оборудования.

Эффективным способом защиты является создание системы управления информационной безопасностью, которая является современным процессом обеспечения безопасности информационных ресурсов организации, построенная на лучших мировых практиках.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования

В настоящее время на законодательном уровне установлен переход от бумажного к электронному документообороту для всех предприятий Республики Беларусь, для чего подготовлена и опубликована законодательная база. Переход к электронному документообороту значительно сокращает время на работу с документами и несет в себе экономическую выгоду.

В настоящее время СЭД являются одними из главных программ на предприятии и содержат в себе большое количество конфиденциальной информации. Объединяет и связывает практически все ПО в одну сеть, доступ к которой необходимо постоянно защищать и отслеживать. Поэтому важно обеспечить действенные методы защиты информации от внешних и внутренних атак.

Обеспечение безопасности данных в СЭД является одной из ключевых задач при построении работы всего программного комплекса предприятия.

Особенно остро встает вопрос о защите информации на текущем этапе, по причине того, что почти вся системообразующая информации предприятий хранится и передается в электронном виде.

С развитием технической оснащенности предприятий и появлением новых программных продуктов совершенствуются не только способы защиты информации, а также возможности ее кражи. Зная это, необходимо постоянно отслеживать и анализировать систему и модернизировать способы защиты информации в системах электронного документооборота.

Научная новизна исследования заключается в совершенствовании теоретических положений, разработке оригинальных методов и моделей систем технической защиты электронных документов на базе современных положений криптографии и стеганографии.

Степень разработанности проблемы

Для раскрытия темы диссертации были рассмотрены: Закон Республики Беларусь «Об электронном документе и электронной цифровой подписи», Закон Республики Беларусь «Об информации, информатизации и защите информации», Закон Республики Беларусь «Об электронном документообороте», учебные справочники по делопроизводству, ежемесячный производственно-практический журнал «Секретарское дело», научно- практический иллюстрированный журнал «Архивы и делопроизводство».

Одним из недостатков исследований, представленных в современной литературе, является неполное рассмотрение способов и методов защиты информации в системах электронного документооборота.

Предложенное исследование направлено на дополнение методов и способов защиты электронных документов.

Цель и задачи исследования

Целью диссертации является изучение методов защиты информации в СЭД, а также разработка методов и алгоритмов для совершенствования защиты информации в СЭД.

Поставленная цель работы определяет **следующие основные задачи:**

1. Провести исследование систем электронного документооборота.
2. Провести анализ текущего положения защиты системы электронного документооборота.
3. Определить преимущества и недостатки существующих систем защиты информации в СЭД.
4. Усовершенствовать алгоритмы защиты систем СЭД.
5. Оптимизировать информационную безопасность системы по выявленным недостаткам.

Область исследования

Содержание диссертации соответствует образовательному стандарту высшего образования второй ступени (магистратуры) ОСВО 1-39 81 01-2012

специальности 1-38 81 01 «Компьютерные технологии проектирования электронных систем».

Теоретическая и методологическая основа исследования

В данной диссертационной работе были применены основы информатики и математики, методы информационной безопасности, методы модульной арифметики и программирования, а также анализ нормативных правовых актов по рассматриваемой тематике.

Информационная база исследования сформированы на основе литературы, открытой информации, технических нормативно-правовых актов, сведений из электронных ресурсов, а также материалов научных конференций и семинаров.

Научная новизна

Научная новизна и значимость полученных результатов работы заключается в том, что в результате исследования разработан усовершенствованный алгоритм для обмена секретных ключей, используя элементы параметрической алгебры.

Теоретическая значимость работы заключается в том, что созданные и исправленные модули защиты могут быть применены при усовершенствовании и улучшении защиты СЭД и обеспечении устойчивости от современных угроз.

Практическая значимость диссертации состоит в том, что представленная в работе программа позволяет создавать защищенные подключения в незащищенных каналах связи, легко встраивается на готовые программные продукты.

Основные положения, выносимые на защиту

1. Модель управления системой защиты информации СЭД, основанная на анализе модели угроз системе информационной безопасности с учетом требований по нормативно-правовому, организационно-техническому и техническому обеспечению для управления безопасностью СЭД.
2. Методический подход по оценке эффективности систем защиты информации СЭД с учетом показателей и критериев оценки эффективности защиты.
3. Метод для безопасного соединения в незащищенных от прослушивания каналах связи, путем применения шифрующих прокси-серверов. Для обеспечения безопасной передачи единого ключа шифрования был усовершенствован алгоритм Диффи-Хеллмана. Программа, реализующая предлагаемый метод и алгоритм.

Апробация диссертации и информация об использовании ее результатов

Результаты исследований, вошедшие в диссертацию, докладывались и обсуждались на 54-ой научно-техническая конференции аспирантов, магистрантов и студентов БГУИР (Минск, Беларусь, 2018 г.).

Публикации

Изложенные в диссертации основные положения и выводы опубликованы в 4 печатных работах. В их числе 4 статьи в сборниках материалов научных конференций.

Общий объем публикаций по теме диссертационной работы составляет 5 авторских листа.

Структура и объем работы

Диссертация состоит из введения, общей характеристики работы, трех глав с краткими выводами по каждой главе, заключения, библиографического списка и приложений.

В первой главе приведен обзор основных методов обеспечения защиты информации в СЭД.

Во второй главе представлены результаты исследовании возможных путей оптимизации защиты информации в СЭД.

В третьей главе представлена разработка программного модуля для оптимизации защиты информации в системах электронного документооборота.

В приложении представлены публикации автора.

Общий объем диссертационной работы составляет 96 страницы. Из них 59 страниц основного текста, 28 иллюстраций на 10 страницах, 2 таблицы на 3 страницах, библиографический список из 55 наименований на 4 страницах, список собственных публикаций соискателя из 4 наименований на 1 странице, 3 приложений на 25 страницах.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** рассмотрено современное состояние проблемы защиты информации в СЭД. Совершен обзор существующих методов и средств защиты информации в СЭД, указаны основные направления исследований, проводимых по данной тематике, а также описано обоснование актуальности темы.

В **общей характеристике работы** показана актуальность проводимых исследований, степень разработанности проблемы, сформулированы цель и задачи диссертации, обозначена область исследований, научная (теоретическая и практическая) значимость исследований, а также апробация работы.

В первой главе приведен обзор современного состояния проблемы защиты информации в СЭД (рисунок 1). Описаны сущность и принципы электронного документооборота.

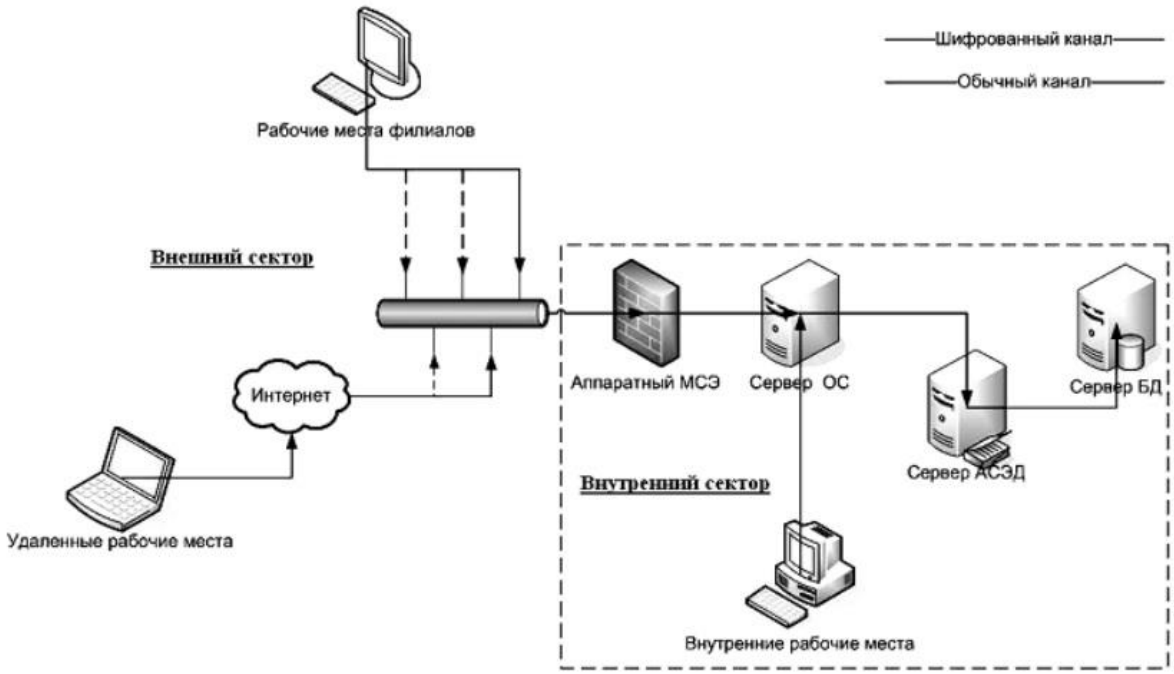

Рисунок 1 – Общая модель СЭД

В целом, СЭД включает в себя три типа компонента, которые показаны на рисунке 1:

1. Серверы.
2. Рабочие места.
3. Каналы связи.

Классифицированы основные угрозы информации в системах электронного документооборота (таблица 1):

Таблица 1 – Основные угрозы информации и вероятность их наступления

Наименование угрозы	**Вероятность наступления**
Остановка функционирования системы в результате некорректных действий администратора СЭД	Высокая
Получение информации о специфике организации документооборота в организации	Высокая
Получение неправомерного доступа к ЭД	Высокая
Выполнение присвоения чужого пользовательского идентификатора	Средняя
Уязвимость системы к различного рода сетевым атакам	Средняя
Перехват трафика	Низкая

Во второй главе рассмотрены общие требования к безопасности СЭД. Представлено исследование возможных путей оптимизации защиты информации в СЭД.

Совершен обзор существующих методов и средств защиты информации в СЭД. Поставлены задачи: исследование путей оптимизации защиты СЭД и изучение международного опыта по усовершенствованию информационной защищенности СЭД.

На рисунке 2 изображена схема степени ценности компонентов СЭД с точки зрения обеспечения целостности хранимой информации.

Рисунок 2 – Степень ценности компонентов СЭД

Документы – данные, хранящиеся на сервере БД, резервные копии документов. Это звено является самым важным и ценным, т. к. именно сами документы содержат конфиденциальную информацию, для безопасности которой организована вся система политики безопасности автоматизированной СЭД.

Степень ценности данного компонента охвачена сектором, отмеченным номером 1.

Сервер БД – среда хранения электронных документов. Целостность сервера БД является второй по значимости после целостности документов - сектор 2.

Сервер ОС и автоматизированной СЭД – операционная система и интерфейсная часть (оболочка) СЭД, установленные на серверах и рабочих станциях, включая клиентов СУБД; протоколы передачи данных; криптографические методы обеспечения безопасности. Безопасность данных компонентов не столь критична, т. к. при их выходе из строя целостность хранимой информации (документов) не будет нарушена. Следует также учесть, что при внештатных ситуациях в рамках этих компонентов частично или полностью могут быть нарушены транзакции информации внутри СЭД. Компоненты отнесены к сектору под номером 3.

Изучены зарубежные методы защиты электронных документов. Изучена проблема распределения и хранения электронных ключей. Рассмотрены криптографические методы и средства обеспечения защиты при сетевом обмене данными. Осуществлен обзор и анализ возможностей

национальных криптографических алгоритмов для создания защищенных СЭД.

Приведен обзор ЗАО «АВЕСТ», которое является разработчиком и правообладателем программного продукта «Программное средство криптографической защиты информации «Криптопровайдер *Avest CSP*» (криптопровайдер *AvCSP*).

Наиболее полную защиту, как показывает практика, обеспечивает применение сочетания организационных и технических мер (рисунок 3).

Рисунок 3 – Инженерно-техническая защита

Соотношение этих сочетаний зависит от степени конфиденциальности информации и наиболее вероятных угроз.

Рассмотрено нормативно-правовое основание ведения делопроизводства и электронного документооборота в Республике Беларусь.

В ходе исследования определилось, что нормативно-правовое база по данной отрасли развивается поэтапно.

Изучены зарубежные стандарты по организации электронного документооборота. Рассмотрены возможности обеспечения информационной безопасности в сети. Определены существующие проблемы безопасности организации безопасного соединения. Сделан вывод, что оптимальный вариант для создания собственной реализации безопасного соединения является программный метод обеспечения безопасности.

Программные методы обеспечения безопасности - это объективные формы представления совокупности данных и команд, предназначенных для функционирования компьютеров и компьютерных устройств с целью получения определенного результата, а также подготовленные и зафиксированные на физическом носителе материалы, полученные в ходе их разработок, и порождаемые ими аудиовизуальные отображения.

Под программными средствами защиты информации понимают специальные программы (рисунок 5), включаемые в состав программного обеспечения СЭД исключительно для выполнения защитных функций.

Рисунок 5 – Программные средства защиты

Под идентификацией, применительно к обеспечению информационной безопасности СЭД, понимают однозначное распознавание уникального имени субъекта СЭД. Аутентификация означает подтверждение того, что предъявленное имя соответствует данному субъекту (подтверждение подлинности субъекта). Таким образом, механизм идентификации и аутентификации является основой для механизмов разграничения доступа. Необходимый уровень аутентификации определяется требованиями безопасности, которые установлены в организации.

Системы идентификации и аутентификации можно разделить следующим образом (рисунок 5):

Рисунок 6 – Системы идентификации и аутентификации

Совокупность выполнения процедур идентификации и аутентификации принято называть процедурой авторизации.

Преимуществом программных средств является универсальность, гибкость, надежность, простота установки, способность к модификации и развитию.

Одним из аппаратных решений является *Ethernet Encryption HC-8555 10G* от *Crypto AG*. Она обеспечит защиту передаваемых данных/сведений из любого приложения по *Ethernet*-сетям *LAN/MAN/WAN* с наиболее высшей степенью защищенности. Пропускной способность аппарата 10 гигабит/сек на линиях «от точки-к точке», система не забирает дополнительных ресурсов. Время задержки информации системой мало. Периодическая смена ключей для соединений производится автоматически, в заданное время и без прерывания связи. Присутствия персонала при этом не требуется. Шифрование происходит «на заднем плане» - никому из пользователей тех или иных приложений не нужно особо заботиться.

Схема решения по защите в Network Security для Ethernet показана на рисунке 7.

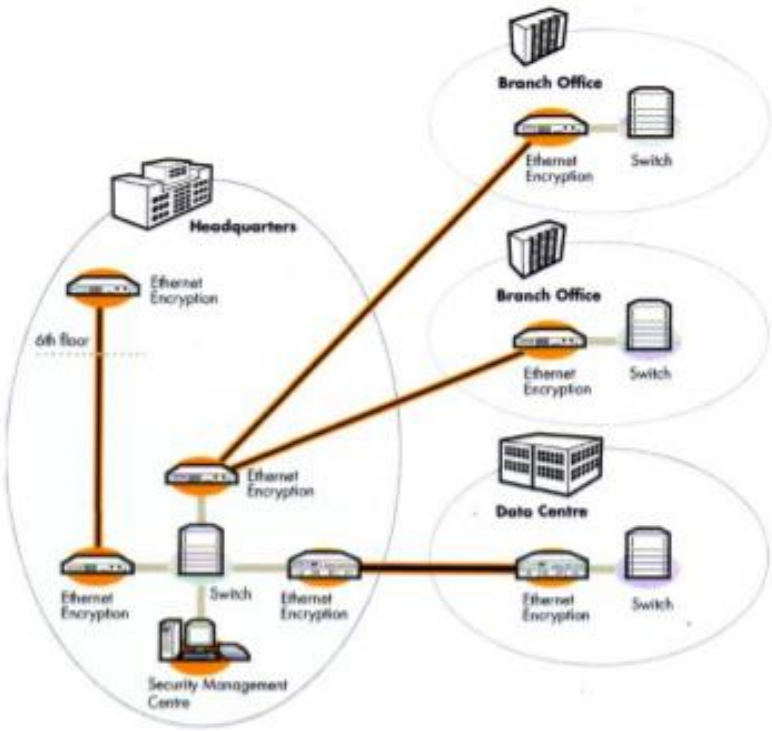

Рисунок 7 – Решения обеспечения защиты *Network Security* для *Ethernet*

В целом мероприятия по реализации защищенного документооборота можно свести в три группы, по мере уменьшения их важности: Работа с человеческим фактором. Техническое, программное и организационное обеспечение по ограничению доступа к защищаемой информации. Программные средства непосредственной защиты информации.

В третьей главе предложен метод для безопасного соединения в незащищенных от прослушивания каналах связи, путем применения шифрующих прокси-серверов.

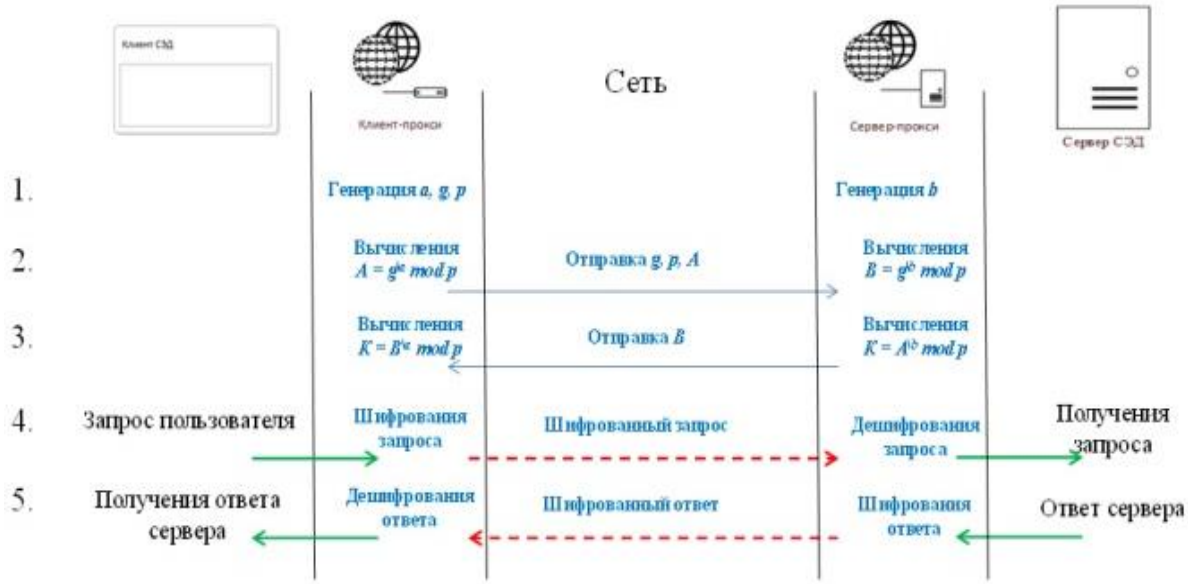

Рисунок 7 – Алгоритм работы шифрованного соединения с помощью прокси- серверов

Для обеспечения безопасной передачи единого ключа шифрования был усовершенствован алгоритм Диффи-Хеллмана. Разработана программа, реализующая предлагаемый метод и алгоритм. Анализ работы программы показал неплохой результат – увеличилась устойчивость безопасности данных, причем потеря времени при обмене данными не значительна. Предложены рекомендации по применению программы в СЭД в качестве отдельного модуля.

ЗАКЛЮЧЕНИЕ

Основные научные результаты диссертации

1. Изучено нормативно-правовое основание ведения делопроизводства и электронного документооборота в Республике Беларусь. В ходе исследования определилось, что нормативно-правовая база по данной отрасли развивается поэтапно.
2. Проанализированы достоинства и недостатки систем электронного документооборота, где главным недостатком в таких системах является информационная безопасность.
3. Определены основные группы методов и средств защиты информации в системах электронного документооборота. Был сделан вывод, что при использовании современных систем электронного документооборота следует применять в комплексе вышеописанные группы методов и средств защиты информации.
4. Рассмотрены основные требования для систем электронного документооборота в целом, и определены дополнительные требования для защищенных систем электронного документооборота.
5. Проанализированы возможности национальных криптографических алгоритмов. Выявлены достоинства и недостатки национальных крипто-модулей.
6. Разработан метод обмена информацией для защиты от прослушивания в каналах связи и усовершенствован алгоритм Диффи-Хеллмана для обмена секретным ключом.
7. Создана программа, реализующая вышеуказанный алгоритм и метод.
8. Подготовлены рекомендации по внедрению программы в систему электронного документооборота в качестве отдельного модуля.

Рекомендации по практическому использованию результатов

Полученные результаты могут быть использованы в качестве дополнительного модуля защиты в СЭД с открытым ключом.

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

1. ServiceDesk система / В.В. Сапун, Н.Н. Дубешко, Е.С. Приставка, Б.А. Железко// материалы 54−ой науч. конф. аспирантов, магистрантов и студентов «Проектирование информационно−компьютерных систем», Минск, Респ. Беларусь, 23–27 апреля 2018 г. / УО «БГУИР». – Минск, 2018. – принято в печать.

2. Оптимизация системы базы данных «Студенты 2.0» / Н.В. Измашкина, Н.Н. Дубешко, Е.С. Приставка, Б.А. Железко// материалы 54−ой науч. конф. аспирантов, магистрантов и студентов «Проектирование информационно−компьютерных систем», Минск, Респ. Беларусь, 23–27 апреля 2018 г. / УО «БГУИР». – Минск, 2018. – принято в печать.

3. Приставка Е.С. Конфиденциальный документооборот на платформе Docvision система / Е.С. Приставка, В.В. Сапун, Н.Н. Дубешко// материалы 54−ой науч. конф. аспирантов, магистрантов и студентов «Проектирование информационно−компьютерных систем», Минск, Респ. Беларусь, 23–27 апреля 2018 г. / УО «БГУИР». – Минск, 2018. – принято в печать.

4. Приставка Е.С. Система электронного документооборота Docsvision для учреждений образования / Е.С. Приставка, В.В. Сапун, Н.Н. Дубешко// «Репозиторий БГУИР» [Электронный ресурс]. – 2018. - Режим доступа: https://libeldoc.bsuir.by/handle/123456789/31978. – Дата доступа: 15.06.2018.

РЭЗЮМЭ

Прыстаўка Алена Сяргееуна

Метады абароны інфармацыіў сістэмы электроннага дакументазвароту на базе DocsVision і DIRECTUM

Ключавыясловы: дакументаабарот, электронны дакументаабарот, сістэма электроннага дакументазвароту, папяровы дакументаабарот, электронны дакумент, электронны лічбавы подпіс.

Мэтапрацы: распрацоўка метаду і алгарытму для ўдасканалення абароны сістэмы электроннага дакументазвароту.

Атрыманыявынікі і іхнавізна: вывучана нарматыўна-прававое падстава вядзення справаводства і электроннага дакументазвароту ў Рэспубліцы Беларусь; ппроанализированы вартасці і недахопы сістэм электронны дакументаабарот, дзе галоўны недахоп у такіх сістэмах з'яўляецца інфармацыйнай бяспекай; вызначаны асноўныя групы метадаў і сродкаў абароны інфармацыі ў сістэмах электроннага дакументазвароту; разгледжаны асноўныя патрабаванні для сістэм электроннага дакументазвароту ў цэлым, і вызначаны дадатковыя патрабаванні для абароненых сістэм электроннага дакументазвароту; прааналізаваны магчымасці нацыянальных крыптаграфічных алгарытмаў; распрацаваны метад абмен інфармацыі для абароны ад праслухоўвання ў каналах сувязі і ўдасканалены алгарытм для абмену сакрэтнага ключа; створана праграма, якая рэалізуе вышэйзгаданы алгарытм і метад. Падрыхтаваны рэкамендацыі па ўкараненні праграмы ў сістэме электроннага дакументазвароту ў якасці асобнага модуля..

Ступень выкарыстання: вынікі могуць быць выкарыстаны ў працы СЭД з адкрытым зыходным кодам для абароны перадаванай інфармацыі.

Вобласцьужывання: абарона электронных дакументаў у СЭД з адкрытым зыходным кодам.

РЕЗЮМЕ

Приставка Елена Сергеевна

Методы защиты информации в системы электронного документооборота на базе DocsVision и DIRECTUM

***Ключевые слова*:** документооборот, электронный документооборот, система электронного документооборота, бумажный документооборот, электронный документ, электронная цифровая подпись.

***Цель работы*:** разработка метода и алгоритма для совершенствования защиты системы электронного документооборота.

***Полученные результаты и их новизна*:** изучено нормативно-правовое основание ведения делопроизводства и электронного документооборота в Республике Беларусь; ппроанализированы достоинства и недостатки систем электронного документооборота, где главным недостатком в таких системах является информационная безопасность; определены основные группы методов и средств защиты информации в системах электронного документооборота; рассмотрены основные требования для систем электронного документооборота в целом, и определены дополнительные требования для защищенных систем электронного документооборота; проанализированы возможности национальных криптографических алгоритмов; разработан метод обмена информацией для защиты от прослушивания в каналах связи и усовершенствован алгоритм для обмена секретным ключом; создана программа, реализующая вышеуказанный алгоритм и метод. Подготовлены рекомендации по внедрению программы в систему электронного документооборота в качестве отдельного модуля.

***Степень использования*:** результаты могут быть использованы в работе СЭД с открытым исходным кодом для защиты передаваемой информации.

***Область применения*:** защита электронных документов в СЭД с открытым исходным кодом.

SUMMARY

Pristavka Elena Sergeevna

Methods of protection of the information in the electronic document management system based on DocsVision and DIRECTUM

***Keywords*:** workflow, electronic document management, electronic document management system, paper document, electronic document, digital signature.

***The object of study*:** development of a method and algorithms for improving the protection of electronic document management systems.

***The results and novelty*:** studied the normative-legal base of records management and electronic document management in the Republic of Belarus; to analyzed advantages and disadvantages of electronic document management systems, where the main drawback of such systems is an information security; main group identified methods and means of information protection systems in the electronic document; examined basic requirements for the electronic document management systems in general, and identify additional requirements for secure electronic document management system; we analyzed the possibility of national cryptographic algorithms; information exchange method developed for protection against listening to communication channels and the improved algorithm for sharing the secret key; we created a program that implements the above method, and algorithm. Recommendations on the implementation of the program in the electronic document management system as a separate module.

***Degree of use*:** results can be used in the electronic document management system open source to protect the transmitted information.

Sphere of application: protection of electronic documents in the electronic document management system open source.