Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
АМУРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
(ФГБОУ ВО «АмГУ»)

Факультет математики и информатики
Кафедра информационных и управляющих систем
Направление подготовки 09.03.02 – Информационные системы и технологии
Направленность (профиль) образовательной программы: Безопасность информационных систем

ДОПУСТИТЬ К ЗАЩИТЕ
Зав. кафедрой
_____ А.В. Бушманов
«_____»_____ 2017 г.

БАКАЛАВРСКАЯ РАБОТА

на тему: Разработка подсистемы криптографической защиты персональных данных в системе электронного документооборота

Исполнитель
студент группы 355-об _____ (подпись, дата) П.И. Питулина

Руководитель
доцент, канд. тех. наук _____ (подпись, дата) Л.А. Соловцова

Консультант
по безопасности и
экологичности
доцент, канд. тех. наук _____ (подпись, дата) А.Б. Булгаков

Нормоконтроль
инженер кафедры _____ (подпись, дата) В.В. Романико

Благовещенск 2017

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
АМУРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
(ФГБОУ ВО «АмГУ»)

Факультет математики и информатики
Кафедра информационных и управляющих систем

УТВЕРЖДАЮ
Зав. кафедрой
_____А.В. Бушманов
«_____»_____ 2017 г.

З А Д А Н И Е

К бакалаврской работе студента Питулиной Полины Игоревны.

1. Тема бакалаврской работы: Разработка подсистемы криптографической защиты персональных данных в системе электронного документооборота

(утверждено приказом от 25.04.2017 № 929-уч)

2. Срок сдачи студентом законченной работы 20.06.17 г.

3. Исходные данные к бакалаврской работе: отчет о прохождении преддипломной практики, ГОСТы, внутренние документы компании, дополнительная литература.

4. Содержание бакалаврской работы: анализ деятельности предприятия; проектирование подсистемы криптографической защиты персональных данных в электронном документообороте; разработка программного обеспечения.

5. Перечень материалов приложения: линейно-организационная структура УК «Аист», функциональная структура УК в методологии IDEF0, документооборот отдела кадров УК «Аист», функциональная структура разрабатываемой подсистемы, концептуально-инфологическая модель, логическая модель, блок-схемы алгоритма RC4, структура взаимодействия модулей подсистемы.

6. Консультанты по бакалаврской работе:

по безопасности и экологичности – А.Б. Булгаков, доцент, канд. тех. наук.

7. Дата выдачи задания: 09.05.17 г.

Руководитель бакалаврской работы: Любовь Александровна Соловцова, доцент, кант. тех. наук.

Задание принял к исполнению (20.05.17 г.): _____
(подпись студента)

РЕФЕРАТ

Бакалаврская работа содержит 88 с., 67 рисунков, 33 таблицы, 27 источников, 8 приложений.

УПРАВЛЯЮЩАЯ КОМПАНИЯ АИСТ, ОТДЕЛ КАДРОВ, ЭЛЕКТРОННЫЙ ДОКУМЕНТООБОРОТ, ДОКУМЕНТ, ПЕРСОНАЛЬНЫЕ ДАННЫЕ, ПОДСИСТЕМА, БАЗА ДАННЫХ, ПРОЕКТИРОВАНИЕ, КРИПТОЗАЩИТА, ШИФРОВАНИЕ, РАСШИФРОВАНИЕ, АЛГОРИТМ

В работе исследована деятельность управляющей компании ООО «Аист» и разработана подсистема криптографической защиты персональных данных в системе электронного документооборота для отдела кадров компании. На ряду с разрабатываемыми модулями подсистемы была разработана база данных документационного обеспечения отдела кадров.

Разрабатываемая информационная подсистема должна позволять хранить, обрабатывать, генерировать, передавать документы, и защищать данные в документах с помощью криптографических алгоритмов шифрования, а также решать задачи управления документооборотом отдела кадров компании.

СОДЕРЖАНИЕ

НОРМАТИВНЫЕ ССЫЛКИ

В настоящей бакалаврской работе использованы ссылки на следующие стандарты и нормативные документы:

ГОСТ 2.104-06 ЕСКД Основные надписи

ГОСТ 2.105-95 ЕСКД Общие требования к текстовым документам

ГОСТ 2.106-96 ЕСКД Текстовые документы

ГОСТ 2.111-68 ЕСКД Нормоконтроль

ГОСТ 2.306-68 ЕСКД Обозначение графических материалов и правила нанесения их на чертежах

ГОСТ 7.9-95 Реферат и аннотация. Общие требования

ГОСТ 19.001-77 ЕСПД Общие положения

ГОСТ 19.101-77 ЕСПД Виды программ и программных документов

ГОСТ 19.102-77 ЕСПД Стадии разработки

ГОСТ 19.103-77 ЕСПД Обозначение программ и программных документов

ГОСТ 19.104-78 ЕСПД Основные надписи

ГОСТ 19.105-78 ЕСПД Общие требования к программным документам

ГОСТ 19.106-78 ЕСПД Требования к программным документам, выполненным печатным способом

ГОСТ 19.201-77 ЕСПД Техническое задание, требования к содержанию и оформлению

ГОСТ 19.402-78 ЕСПД Описание программы

ГОСТ 19.502-78 ЕСПД Описание применения. Требования к содержанию и оформлению

ГОСТ 19.504-79 ЕСПД Руководство программиста. Требования к содержанию и оформлению

ГОСТ 19.505-79 ЕСПД Руководство оператора. Требования к содержанию и оформлению

ГОСТ 19.508-79 ЕСПД Руководство по техническому обслуживанию. Требования к содержанию и оформлению

ГОСТ Р 34.10-94 Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма

ГОСТ Р 34.10-2001 Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи

ГОСТ Р 34.10-2012 Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи

ГОСТ Р 34.11-2012 Информационная технология. Криптографическая защита информации. Функция хеширования

ГОСТ 34.201-89 Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначения документов при создании автоматизированных систем

ГОСТ 34.601-90 Информационная технология. Комплекс станддартов на автоматизированные системы. Автоматизированные системы. Стадии создания

ГОСТ 34.602-89 Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы

ГОСТ 34.603-92 Информационная технология. Комплекс стандартов на автоматизированные системы. Виды испытаний автоматизированных систем

ГОСТ 28147-89 Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования

ОПРЕДЕЛЕНИЯ, ОБОЗНАЧЕНИЯ, СОКРАЩЕНИЯ

УК – управляющая компания;

ПТО – производственно-технический отдел;

ЖКХ – жилищно-коммунальное хозяйство;

БД – база данных;

РФ – Российская Федерация;

ГИС ЖКХ – государственная информационная система жилищно-коммунального хозяйства;

СЭД – система электронного документооборота;

СКЗИ – средство криптографической защиты информации;

ЭЦП – электронная цифровая подпись;

ПДн – персональные данные;

КоАП – кодекс об административных правонарушениях;

ПЭВМ – персональная электронная вычислительная машина.

ВВЕДЕНИЕ

В современном мире применение информационных технологий тесно связано с эффективным развитием организаций, которые активно переходят к электронному представлению информации. Для этого в организациях внедряют информационные системы, которые значительно упрощают и ускоряют процессы обработки, хранения и передачи информации, а также решают широкий спектр других организационных задач.

Большую совокупность автоматизированных процессов работы с электронными документами имеют современные системы документооборота, которые все чаще внедряют в организации. Современные реалии диктуют определенные требования в области документационного обеспечения, делопроизводства и документооборота. При существующей смешанной системе делопроизводства, когда все документопотоки в организации рассредоточиваются по структурным подразделениям для их обязательного исполнения, знания в области документационного обеспечения необходимы всем. Молодому специалисту, впервые пришедшему на работу, помимо знаний и навыков составления документов необходимо иметь представление об особенностях взаимодействия и движения документов на предприятии. Руководителям важно знать не только структуру самого документа, но и иметь представление, посредством издания какого документа и как можно разрешить ту или иную административную ситуацию. Таким образом, в наши дни все служащие являются участниками единого делопроизводственного процесса. Сегодня наряду с профессиональными навыками работник должен уметь создавать и защищать документы в соответствии с существующими нормами, государственными стандартами, законами Российской Федерации, методическими рекомендациям министерств и ведомств.

С появлением систем электронного документооборота возникают и новые виды угроз, уязвимостей и рисков, которые прямым образом влияют на деятельность организации в целом, что приводит к необходимости рассматривать вопросы, связанные с информационной безопасностью предприятия. Одним из

многих методов обеспечения защиты документов в электронном документообороте является шифрование информации. Шифрование документа по криптографическим алгоритмам позволяет обратимо преобразовывать информацию в нечитабельный вид, тем самым скрывая суть документа, что позволяет скрыть или защитить ту часть документа, которая и требует защиты. Такая защита требуется документам, содержащие персональные данные, для которых важно обезличивание при обработке.

Таким образом предметом выпускной квалификационной работы является система электронного документооборота и объектом – защита персональных данных в документах. Целью работы является разработка программного модуля криптографической защиты для системы электронного документооборота отдела кадров управляющей компании «Аист».

Для достижения поставленной цели были выделены следующие задачи:

а) провести анализ и исследование предметной области;

б) провести анализ существующих систем электронного документооборота и обосновать необходимость создания подсистемы защиты документов в отделе кадров компании;

в) провести проектирование информационной системы документооборота для отдела кадров управляющей компании «Аист»;

г) провести проектирование программного обеспечения для информационной системы документооборота;

д) разработать функциональные подсистемы, модули и базу данных;

е) разработать методические документы для потенциальных пользователей системы;

ж) провести тестирование разработанной подсистемы;

к) разработать политику информационной безопасности на уровне отдела кадров управляющей компании «Аист».

.

1 АНАЛИЗ ПРЕДМЕТНОЙ ОБЛАСТИ

1.1 Общая характеристика деятельности управляющей компании «Аист»

Управляющая компания (УК) «Аист» занимается обслуживанием домов и предоставлением их жителям коммунальных услуг с 2011 года. В управлении организации находится 3 жилых дома. Главной целью компании является профессиональное предоставление качественных коммунальных услуг жителям. В обязанности управляющей компании входят эксплуатационно-ремонтные работы, которые включают в себя: систематичный осмотр домов, осуществление общестроительных, инженерных, электромонтажных, специализированных строительных, изоляционных, штукатурных, малярных, санитарно-технических работ, обустройство прилегающей к дому территории, уборку подъездов и прилегающей к домам территории. Организационные услуги подразумевают проведения собраний с жильцами.

Политика управляющей компании нацелена на чёткое планирование своей деятельности. Успешная деятельность компании показала жизнеспособность и эффективность частного содержания жилья.

1.2 Организационная структура управляющей компании «Аист»

В линейно-штабной организационной структуре управляющей компании жилищно-коммунального хозяйства «Аист», представленной в приложении А на рисунке А.1, пять отделов: производственно-технический отдел (ПТО), бухгалтерия, отдел кадров, юридический отдел, отдел паспортного стола. ПТО занимается планированием и проведением ремонтных работ, работ по техническому обслуживанию домов, приемом и регистрацией заявок жильцов дома, контролированием за качеством и объемом поставляемых коммунальных услуг. Бухгалтерия занимается ведением бухгалтерского учёта, налогового учёта, планированием и учётом расходов управляющей компании, сохранностью денежных средств и материальных ценностей. Отдел кадров занимается приемом, переводом, увольне-

нием сотрудников, заполнением личных карточек сотрудников, ведением установленной документации по кадрам, оформлением командировок и составлением графиков отпусков. Юридический отдел осуществляет проверку внутренней документации УК ЖКХ на соответствие действующему законодательству, оказание консультационной помощи жильцам, разработку, подготовку и юридическое оформление договоров по различным направлениям деятельности компании. Отдел паспортного стола отвечает за учет граждан, паспортный учёт, сохранность картотеки и ее достоверность, контроль паспортного режима.

На рисунке А.1 использованы обозначения:

а) плотная тонировка – подразделение принимает непосредственное участие в процессе, подлежащем автоматизации, т.е. является пользователем системы;

б) средняя тонировка – отдел поставляет информацию, которая может использоваться в системе;

в) средняя тонировка – подразделение не является пользователем системы, но поставляет информацию и использует её для системы;

г) без тонировки – подразделение не имеет отношения к автоматизированным процессам;

д) точками выделено подразделение, существующее формально, по бумагам.

1.3 Анализ деятельности управляющей компании «Аист»

1.3.1 Функциональная модель управляющей компании

В ходе исследования деятельности управляющей компании была построена функциональная структура в методологии IDEF0, представленная в приложении Б. Рассмотрим контекстную диаграмму, которая изображена на рисунке Б.1. Здесь входными элементами являются: заявки жильцов на проведение ремонтных работ, заявки по юридическим вопросам, заявки о приеме на работу, информация о жильцах, цены на материалы, входящие документы. Управление в компании производится на основании инструкций, устава управляющей компании и законодательства РФ. На выходе деятельности компании формируются:

общий счет, смета затрат, список требуемых вакансий, расчетные листы, судебные иски, заключения, исходящие документы, налоговая отчетность. Механизмами – ресурсами, обеспечивающие деятельность компании – являются: персонал, оборудование и материалы, аппаратно-технический комплекс.

На диаграмме декомпозиции, представленной на рисунке Б.2, отображены деятельности отделов управляющей компании и взаимодействие между ними. Заявки по юридическим вопросам поступают в процесс деятельности юридического отдела. На выходе данного процесса формируются судебные иски, заключения, общий отчет и юридическая политика УК, которая поступает на управление деятельностей всех отделов компании. В процесс деятельности производственно-технического отдела поступают заявки от жильцов на проведение ремонтных работ на основе которых отделом составляются сметы планируемых затрат, передаваемые в бухгалтерию, отделу кадров предоставляется отчет о работе персонала ПТО, а также составляется общий отчет. Процесс деятельности отдела паспортного стола собирает информацию о жильцах, выходными данными этого процесса являются отчет о работе персонала паспортного стола, предоставляемый отделу кадров, и общий отчет. Входящие документы, заявки о приеме на работу, а также указанные выше отчеты о работе персонала поступают в процесс деятельности отдела кадров. На выходе процесса формируются список требуемых вакансий, исходящий документы, общий отчет и данные сотрудников, передаваемые в бухгалтерию. В процесс деятельности бухгалтерии поступают указанные выше данные сотрудниках и смета планируемых затрат, а также цены на материалы. Здесь создаются расчетные листы, смета затрат, налоговая отчетность, общий отчет и отчет о работе персонала бухгалтерии, передаваемый в отдел кадров.

1.3.2 Информационная модель отдела кадров управляющей компании

Рассмотрим более подробно информационные потоки отдела кадров компании, поскольку разрабатываемая подсистема создавалась для данного отдела УК. В приложении В на рисунке В.1 представлен внешний документооборот УК в методологии DFD. Внешними сущностями по отношению к отделу кадров УК

выступают работник, трудовая инспекция, центр занятости, пенсионный фонд, военкомат. Потенциальный работник прибывает в отдел кадров с заявлением о приеме на работу, в случае его трудоустройства отдел кадров отдает ему распоряжения. Трудовая инспекция присылает извещения о проверке на что отдел кадров обязан предоставить книги регистрации документов. В центр занятости отдел кадров посылает сведения о требуемых вакансиях, в ответ цент занятости предоставляет списки нетрудоустроенных для подбора кандидатов. Для пенсионного фонда отдел кадров собирает необходимые сведения о сотрудниках, пенсионный фонд выдает распоряжения. Военкомат отправляет запросы о сотрудниках, в ответ отдел кадров пересылает сведения о военнообязанных гражданах, прибывающих в запасе.

Внутренний документооборот отдела кадров УК «Аист» представлен в приложении В на рисунке В.2. Деятельность отдела кадров УК «Аист» состоит из четырех процессов: регистрация новых работников, обработка кадровых документов, учет кадровой документации, передача кадровых документов. В компании выделяется три хранилища данных: база данных сотрудников, база данных документов, архив. Заявление о приеме на работу поступает в процесс регистрации новых работников, по выполнению которого создаются личные карточки работников, хранящиеся в архиве и собираются персональные в БД сотрудников. В процесс обработки кадровых документов поступают персональные данные сотрудников из БД сотрудников, извещение о проверке, списки о нетрудоустроенных, запрос о сотруднике, распоряжения пенсионного фонда. На выходе данного процесса формируются распоряжения, распределенная документация, поступающая в процесс учета кадровой документации, и созданная документация, сохраняемая в БД документов. Входными информационными потоками процесса учета кадровой документации являются распределенная документация, созданная документация из БД документов и информация об отправленных документах. Выходные информационные потоки данного процесса – книги регистрации документов, кадровая документация, которая хранится в архиве, а также участвует в процессе передачи кадровых документов. В ходе выполнения

процесса передачи кадровых документов на выходе формируются сведения о требуемых вакансиях, сведения о работниках, сведения о военнообязанных граждан, прибывающих в запасе.

Рассмотрим декомпозицию процесса регистрации новых работников, представленной в приложении В на рисунке В.3. Данный процесс состоит из четырех работ. Для оформления трудового договора принимают заявление о приеме на работу, после чего создается согласованный трудовой договор и собираются персональные данные сотрудника. Затем нового работника знакомят с внутренними актами организации, и он подписывает лист ознакомления. Далее оформляется приказ о приеме на работу по форме Т-1, который также подписывается работником. После на основании собранных персональных данных сотрудника и согласованного приказа о приеме на работу оформляется личная карточка работника по форме Т-2, созданная личная карточка передается в архив, а персональные данные заносятся в БД сотрудников.

Декомпозиция процесса обработки кадровых документов, состоящая из четырех работ, представлена в приложении В на рисунке В.4. Входными информационными потоками работы прием и первичная обработка документов являются извещение о проверке, списки о нетрудоустроенных, запрос о сотруднике, распоряжения пенсионного фонда. Выходной поток этой работы – информация о полученных документах поступает в следующую работу – рассмотрение и распределение документов – по выполнению которой на выходе формируется распределенная документация, участвующая в процессе предоставления на исполнение. Персональные данные сотрудника участвуют в работе оформление приказов, выходным информационным потоком которой является созданная документация. Распределенная документация и созданная документация поступают на вход работы предоставление на исполнение, по выполнению которой создаются распоряжения.

Декомпозиция процесса учета кадровой документации состоит из пяти работ и представлена в приложении В на рисунке В.5. Распределенная документа-

ция и созданная документация участвуют в работе сбора документов в ходе которой выделяются реквизиты документов, которые затем участвуют в работе сортировки документов. После текущая кадровая документация участвует в процессах регистрации документов, подготовке документов к передаче и хранении кадровых документов. Также регистрируется информация об отправленных документах и создаются книги регистрации документов. Подготовка документов к передаче формирует необходимую кадровую документацию компании.

Рассмотрим декомпозицию процесса передача кадровых документов представленную в приложении В на рисунке В.6 и состоящую из четырех работ. Выбор документов осуществляется из кадровой документации компании после чего выбранные документы оформляются в письма и выбирается адресат. Пакет документов отправляется, представляющий собой сведения от требуемых вакансиях, сведения о работниках, сведения о военнообязанных граждан, прибывающих в запасе. Сведения об отправке регистрируются, и информация об отправленных документах участвует в учете кадровой документации.

1.4 Характеристика информационной системы объекта исследования

Информационная система управляющей компании «Аист» главным образом ориентирована на обработку данных и составление отчетов и представляет собой документальную информационную систему. Реализована локально на отдельных автоматизированных рабочих местах. По характеру обработки информации является системой обработки данных, которая предназначается для подготовки документов, отчетов, поручений. Собираемая и создающаяся информация в компании хранится в базах данных: документов, сотрудников и жильцов.

У компании есть свой сайт, на котором можно получить всю необходимую информацию. Пользователями сайта являются жильцы домов и сотрудники, выполняющие роль администратора. Сайт компании включает в себя базы данных жильцов, сотрудников, документов и состоит из следующих модулей: «о компании», «отчетность», «новости», «информация», «вопрос-ответ», «кабинет». Модуль «о компании» содержит описание деятельности УК «Аист», ее цели, а также

контактную информацию по которой можно связаться с компанией. Модуль «отчетность» содержит общую информацию о постановлениях правительства РФ в области жилищно-коммунального хозяйства, основные показатели финансово-хозяйственной деятельности УК, сведения о выполняемых работах, порядок и условия оказания услуг, сведения о стоимости работ, тарифы на коммунальные ресурсы. Модуль «Новости» отображает актуальную информацию для пользователей, изменения, принятые как в компании, так и на федеральном уровне в сфере ЖКХ. Модуль «вопрос-ответ» фиксирует вопросы жильцов и ответы администратора сайта. Модуль «кабинет» создан для регистрации жильцов и для предоставления зарегистрированным жильцам личного кабинета на сайте, оборотной ведомости и данных счетчиков.

Управляющая компания «Аист» также взаимодействует с государственной информационной системой жилищно-коммунального хозяйства (ГИС ЖКХ), которая является единой федеральной централизованной системой, содержащей всю информацию о ЖКХ России. Все виды информации, размещаемой в системе перечислены в Федеральном законе от 21 июля 2014 г. N 209-ФЗ «О государственной информационной системе жилищно-коммунального хозяйства». Компания обязана передавать информацию о жильцах, сотрудниках, платежные реквизиты, лицевые счета, договора, регистрировать приборы учета и т.д. Более подробную информацию можно найти в размещенном на сайте ГИС ЖКХ руководстве пользователя.

1.5 Обзор систем электронного документооборота и средств криптографической защиты

В настоящее время на рынке программного обеспечения представлено большое разнообразие систем электронного документооборота (СЭД), которые ориентированы главным образом на переход от бумажных документов к электронным. Основными функциональными возможностями данных систем являются:

а) автоматизация процессов обработки документов;

б) оперативное управление большим количеством документов;

в) обеспечение надежности учета и хранение документации;

г) повышении производительности предприятия.

Остановимся на СЭД, включающие в себя подсистему безопасности, которые были разделены на две группы – это СЭД на основе осуществления разграничения доступа и СЭД, в дополнении использующие криптографическую защиту. Были рассмотрены такие программные продукты, как «ЕВФРАТ-Документооборот», «1С Архив», «Кодекс: Документооборот», относящиеся к первой группе и «LanDocs», «ДЕЛО», «Карма» – представители второй группы. Все перечисленные программные продукты содержат весь необходимый инструментарий, включающий в себя основные функции СЭД, поэтому рассмотрим данные программы с точки зрения обеспечения безопасности.

В СЭД «ЕВФРАТ-Документооборот» безопасность обеспечивается разграничением прав доступа и защитой от несанкционированного доступа, а также с помощью идентификации пользователя для безопасной работы через Интернет. СЭД «1С Архив» управляет правами пользователей и устанавливает различные права доступа к папкам и документам для различных пользователей. «Кодекс: Документооборот» предоставляет постоянный или временный доступ к документам, закрепленными за определенными сотрудниками.

СЭД «LanDocs» защищает информацию посредством электронной цифровой подписи и шифрования. Данная СЭД поддерживает функции центра сертификации и хранения сертификатов пользователей поддерживает инфраструктуру открытых ключей в соответствии со стандартом RFC 2459. СЭД «ДЕЛО» для обеспечения безопасности использует электронную цифровую подпись и шифрование документов при их передаче по открытым каналам связи. Выполнение данных функций защиты обеспечивается с помощью интегрированных в данную СЭД таких средств криптографической защиты, как: «Домен-К», «КриптоПро CSP», «Сигнал-КОМ CSP», «Верба OW». В СЭД «Карма» наряду с ЭЦП и шифрованием информации используются USB-ключи – eToken. Как и «LanDocs» использует инфраструктуру открытых ключей. «Карма» работает с криптопровайдерами «Microsoft», а также с «Домен-К», «КриптоПро CSP», «Smart Crypto»,

«Сигнал-КОМ CSP».

Все представленные выше средства криптографической защиты информации используются для защиты данных, не являющихся государственной тайной и разработаны на основании следующих российских стандартов:

а) ГОСТ 28147–89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования;

б) ГОСТ Р 34.10–94. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма;

в) ГОСТ Р 34.10–2001. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи;

г) ГОСТ Р 34.10–2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи;

д) ГОСТ Р 34.11–94. Информационная технология. Криптографическая защита информации. Функция хеширования;

е) ГОСТ Р 34.11–2012. Информационная технология. Криптографическая защита информации. Функция хеширования.

В средстве криптографической защиты информации (СКЗИ) «Домен-К» реализованы российские стандарты шифрования и хеширования, а также электронно-цифровая подпись. Обеспечивает хранение, обработку, передачу персональных данных и информации не являющейся государственной тайной.

«КриптоПро CSP» может использоваться для шифрования данных, не являющимися государственной тайной, генерации электронной цифровой подписи, работы с сертификатами, формирования ключей шифрования и ключей электронной цифровой подписи (ЭЦП). Данное средство было разработано по техническому заданию Федерального агентства правительственной связи и информации при Президенте Российской Федерации в соответствии с криптографическим интерфейсом фирмы Microsoft.

СКЗИ «Сигнал-КОМ CSP» и СКЗИ «Smart Crypto» поддерживают работу с такими известными приложениями, как Microsoft Office, Microsoft Outlook Express.

«Верба OW» осуществляет шифрование файлов, выработку хеш функций файлов и формирование ЭЦП, используя симметричные и асимметричные ключи шифрования для подписи.

Также отметим сертифицированного ФСБ российского криптопровайдера VipNet CSP, который предлагает свои продукты в разном представлении, каждое из которых обеспечивают соответствующие классы защищенности. Это средство позволяет создавать ключи, формировать и проверять ЭЦП, хэшировать и шифровать данные.

Сравнение систем электронного документооборота с точки зрения защиты данных представлено в таблице 1.

Таблица 1 – Сравнение систем электронного документооборота

СЭД с разграничением доступа	СЭД с разграничением доступа и встраиваемым СКЗИ
Достоинства:	
– защита от несанкционированного доступа к данным; – идентификация пользователя; – установление прав доступа.	– защита от несанкционированного доступа к данным; – идентификация пользователя; – установление прав доступа; – защита данных посредством шифрования, ЭЦП или хэширования; – обеспечивают соответствующие классы защищенности.
Недостатки:	
– в случае несанкционированного доступа данные не защищены	– криптографические атаки; – СКЗИ закупается отдельно.

Таким образом разрабатываемая подсистема криптографической защиты персональных данных в системе электронного документооборота будет соответствовать второй группе СЭД, в которую не требуется дополнительно закупать и встраивать СКЗИ.

1.6 Обоснование применения подсистемы криптографической защиты персональных данных

Согласно изученному методическому документу, расположенному на сайте ГИС ЖКХ, «Организация защиты передаваемой в ГИС ЖКХ информации»

передаваемые персональные данные жильцов и сотрудников необходимо шифровать при передаче по каналам связи сети Интернет. Рекомендуемыми криптопровайдорами встраиваемых СКЗИ являются VipNET CSP и КриптоПро CSP.

Обозначив потоки информации внешнего и внутреннего документооборота отдела кадров компании как объект защиты были выделены персональные данные сотрудников. В Федеральном законе от 27 июля 2006 г. № 152-ФЗ «О персональных данных» устанавливает правила обработки персональных данных (ПДн). К ним относятся: фамилия, имя, отчество, место проживания, дата и место рождения, паспортные данные – данные, которые однозначно идентифицируют личность. В статье 3 152-ФЗ вводится понятие обезличивания данных, которое является необходимым в процессе обработки персональных данных. Обезличивание персональных данных представляет собой модификацию информации, посредством которой невозможно определить принадлежность ПДн конкретному лицу. Необходимыми свойствами обезличивания данных являются: обратимость и стойкость к атакам на идентификацию субъекта ПДн. Достичь данных характеристик позволяет достичь использование криптографических алгоритмов шифрования поскольку они преобразуют информацию, являются обратимыми, а также обладают стойкостью к взломам.

Таким образом для защиты персональных данных сотрудников предлагается использовать симметричные алгоритмы блочного шифрования AES и потокового шифрования RC4. Эти алгоритмы обладают высокой скоростью шифрования, простотой реализации, независимостью стойкости не от длины ключа, простотой реализации.

2 ПРОЕКТИРОВАНИЕ ПОДСИСТЕМЫ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ЭЛЕКТРОННОМ ДОКУМЕНТООБОРОТЕ

2.1 Требования к создаваемой подсистеме

Создаваемая подсистема криптографической защиты персональных данных в электронном документообороте для отдела кадров компании должна участвовать во взаимодействии с разработанной базой данных, позволяя создавать документы на основе шаблонов, хранить и передавать их по открытому каналу связи – формируя систему электронного документооборота, а также разрабатываемая подсистема должна обеспечивать защиту персональных данных сотрудников. Для повышения эффективности работы с документами в компании подсистема должна обеспечивать автоматический импорт наиболее часто используемых полей из базы данных в готовые шаблоны документов при создании документов. Передача документов также должна осуществляться по электронной почте организации в шифрованном виде.

К функциям создаваемой системы должен иметь доступ ограниченное число лиц, а именно сотрудники отдела кадров и директор компании. Таким образом доступ предоставляется только зарегистрированным лицам, которые перед входом в подсистему обязаны пройти идентификацию и аутентификацию. Посредством авторизации подсистема определяет права доступа, следовательно, были выделены две роли: пользователи и администратор. Пользователи участвуют в процессах создания, обработки, шифрования, передачи документов, а администратор регистрирует новых пользователей, которые занимают определенные должности и имеет доступ к журналу подсистемы. Журнал должен отображать деятельность лиц в данной подсистеме – пользователя, события, участвующие в этих событиях документы и время происхождения событий.

Разрабатываемая подсистема криптографической защиты должна соответствовать уровню КС1 – средства криптографической защиты, которые могут встраиваться самостоятельно пользователем криптосредства без контроля со

стороны ФСБ. Данный уровень был выбран в соответствии с потенциальными нарушителями, которые представляют собой нарушителей первого уровня (Н1). К данной группе нарушителей относятся:

а) одиночные нарушители;

б) нарушители, располагающие доступными в свободной продаже документацией СКЗИ;

в) нарушители, располагающие только доступными в свободной продаже аппаратными компонентами СКЗИ.

2.2 Характеристика функциональных подсистем

Рассмотрим функциональную структуру подсистемы криптографической защиты персональных данных в электронном документообороте, представленную в приложении в методологии IDEF0 Г на рисунке Г.1.

В создаваемой подсистеме выделяются следующие функциональные подсистемы:

а) авторизации пользователей;

б) обработки документов;

в) передачи документов;

г) шифрования документов;

д) расшифрования документов;

е) регистрации пользователей;

ж) ведения журнала документации.

Авторизация определяет права пользователя или администратора. Посредством предоставления идентификатора – логина, – и аутентификатора – пароля – подсистема определяет какие функциональные возможности доступны тем или иным пользователям. Также данный модуль предоставляет защиту от неправомерного доступа.

Обработка документа включает шаблоны документов, а также позволяет автоматизировать процесс занесения часто используемых полей, представляющие собой персональные данные сотрудников, из БД. Сюда входят документы:

приказ (распоряжение) о приеме работника на работу, личная карточка работника, приказ (распоряжение) о переводе работника на другую работу, приказ (распоряжение) о предоставлении отпуска работнику, приказ (распоряжение) о прекращении (расторжении) трудового договора с работником (увольнении), приказ (распоряжение) о направлении работника в командировку, приказ (распоряжение) о поощрении работника.

Шифрование документов осуществляется по одному из алгоритмов – AES или RC4. Пользователь может выбрать документ для шифрования как из БД, так и сторонний, затем задает ключ шифрования и выбирает алгоритм. Зашифрованный документ, ключ и выбранный алгоритм заносятся в БД.

Расшифрование производится аналогично шифрованию. Пользователь выбирает документ из БД либо сторонний, вводит ключ и выбирает алгоритм шифрования.

Передача документов представляет собой отправку выбранного шифрованного документа по указанному адресу электронной почты. Указывается тема письма, метка шифрования и ключ шифрования.

Регистрация доступная функция администратора, который регистрирует новых пользователей подсистемы, назначает им логины и пароли.

Журнализация регистрирует события, совершаемы пользователями подсистемы и самих пользователей. Администратор имеет доступ к просмотру журнала и поиску в журнале.

2.3 Характеристика обеспечивающих подсистем

2.3.1 Информационное обеспечение

2.3.1.1 Инфологическое проектирование базы данных

2.3.1.1.1 Формирование набора сущностей

Прежде всего в проектировании базы данных необходимо определиться с набором сущностей и с тем, какие данные будут храниться в каждой сущности. Таким образом таблице 2 перечислены все сущности создаваемой базы данных и их краткое описание.

Таблица 2 – Сущности

Название сущности	Описание сущности
Подразделение	Производственные подразделения предприятия, взаимосвязь которых составляет производственную структуру компании
Должность	Служебная обязанность связанная с выполнением определенных обязанностей в компании
Сотрудник	Служащий, работающий в компании и занимающий определенную должность
Журнал	Записи о событиях и связанных с ними пользователях и документов
Событие	Факт, отображающий действия пользователя в программе
Документ	Объект, представленный в электронном виде и содержащий определенную информацию
Категория	Группа документов
Шаблон	Образец документа
Шифрованный документ	Измененный согласно алгоритму шифрования документ
Алгоритм	Тип шифрования

2.3.1.1.2 Спецификация атрибутов сущностей

После определения сущностей необходимо определить параметры данных для каждой сущности, называемые атрибутами. В таблицах 3 – 12 представлены спецификации атрибутов всех сущностей.

Таблица 3 – Спецификация атрибутов сущности «Подразделение»

Название атрибута	Описание атрибута	Диапазон значений	Единицы измерения	Пример
Id_подразделения	Уникальный идентификатор подразделения компании	>0	–	1
Наименование_подразделения	Словесное обозначение подразделения компании	–	–	Отдел кадров

В компании существуют подразделения, отображающие структуру компании, которые отражаются в сущности «Подразделение». Здесь атрибут «Id_подразделения» является ключевым – однозначно идентифицирующим подразделение.

Таблица 4 – Спецификация атрибутов сущности «Должность»

Название атрибута	Описание атрибута	Диапазон значений	Единицы измерения	Пример
Id_должность	Уникальный идентификатор должности	>0	–	1
Наименование_должность	Словесное обозначение должности	–	–	Специалист по кадрам

Информация о должностях в компании заносится в сущность «Долж-

ность», где ключевым атрибутом является «Id_должность» – однозначно идентифицирующий должность.

Таблица 5 – Спецификация атрибутов сущности «Сотрудник»

Название атрибута	Описание атрибута	Диапазон значений	Единицы измерения	Пример
Id_сотрудник	Уникальный идентификатор сотрудника	>0	–	1
ФИО	Фамилия и инициалы имени и отчества сотрудника	–	–	Иванова Дарья Семеновна
Пол	Пол сотрудника	Женский / Мужской	–	Женский
Паспорт	Серия и номер паспорта сотрудника	0000-000000 – 9999-999999	–	9382-983933
ИНН	Идентификационный номер сотрудника	000000000000 – 999999999999	–	728638913980
Пенсионное_страхование	Номер присвоенный пенсионным фондом застрахованному человеку	000-000-00000 – 999-999-99999	–	637-983-29398
Телефон	Номер телефона сотрудника	89000000000 – 89999999999	–	89653728399
Адрес	Местожительство сотрудника – название улицы, номер дома и квартиры	–	–	ул. Калина 149, кв. 203
Индекс	Цифровое обозначение почтового адреса, присваиваемое объекту почтовой связи	000000 – 999999	–	675345
Логин	Набор букв и/или цифр, необходимый для входа в программу	–	–	samoilova
Пароль	Набор букв и/или цифр, подтверждающий пользователя	–	–	111

При приеме на работу в управляющую компанию новых сотрудников собирается вся необходимая информация о них, отображаемая в сущности «Сотрудник». Однозначно идентифицирующим сотрудника атрибутом здесь является «Id_сотрудника».

Таблица 6 – Спецификация атрибутов сущности «Журнал»

Название атрибута	Описание атрибута	Диапазон значений	Единицы измерения	Пример
Id_запись	Уникальный идентификатор записи журнала	>0	–	1
Дата	Дата записи события	–	–	19 февраля 2017 г.
Время	Время записи события	00:00:00 – 23:59:59	–	12:00:33
Почтовый_адрес	Адрес электронного почтового ящика	–	–	dalamur@mail.ru

В сущности «Журнал» отображается информация о пользователях программы и их действиях в программе. Однозначно идентифицирующим сотрудника атрибутом здесь является «Id_запись».

Таблица 7 – Спецификация атрибутов сущности «Событие»

Название атрибута	Описание атрибута	Диапазон значений	Единицы измерения	Пример
Id_событие	Уникальный идентификатор события	>0	–	1
Название_события	Словесное обозначение события	–	–	Создание документа

События, которые являются действиями пользователя программы, заносятся в сущность «Событие». Здесь атрибут «Id_событие» является ключевым.

Таблица 8 – Спецификация атрибутов сущности «Документ»

Название атрибута	Описание атрибута	Диапазон значений	Единицы измерения	Пример
Id_документ	Уникальный идентификатор документа	>0	–	1
Наименование_ документа	Словесное обозначение документа	–	–	Прием Афанасьева Елена Васильевна
Дата_создания	Дата создания документа	–	–	7 марта 2012
Месторасположение	Путь, где находится созданный файл	–	–	D:\Docs\Приём\ Приём Афанасьева Елена Васильевна

Созданные документы отображаются в сущности «Документ» с ключевым атрибутом «Id_документ».

Таблица 9 – Спецификация атрибутов сущности «Категория»

Название атрибута	Описание атрибута	Диапазон значений	Единицы измерения	Пример
Id_категория	Уникальный идентификатор категории документа	>0	–	1
Название_ категория	Словесное обозначение категории документа	–	–	Приём

Документы и шаблоны подразделяются на категории документов. Информация о категориях заносится в сущность «Категория», где однозначно идентифицирующим категорию атрибутом является «Id_категория».

Таблица 10 – Спецификация атрибутов сущности «Шаблон»

Название атрибута	Описание атрибута	Диапазон значений	Единицы измерения	Пример
Id_шаблон	Уникальный идентификатор шаблона документа	>0	–	1
Название_шабло- на	Словесное обозначение категории документа	–	–	Приказ о приеме работника на работу

В сущности «Шаблон» занесена информация о шаблонах документов, располагаемых в директории на жестком диске компьютера. Здесь ключевым атрибутом является «Id_шаблон» – однозначно идентифицирующим шаблон документа.

Таблица 11 – Спецификация атрибутов сущности «Шифрованный документ»

Название атрибута	Описание атрибута	Диапазон значений	Единицы измерения	Пример
Id_шифровдок	Уникальный идентификатор шифрованного документа	>0	–	1
Название_шифровдок	Словесное обозначение шифрованного документа	–	–	Командировка ВРП
Ключ	Последовательность букв, цифр, используемая в шифровании	–	–	36yduw7823287dy2
Месторасположение	Путь, где находится созданный шифрованный файл	–	–	D:\Docs\ Шифрованные_документы\ Командировка ВРП.doc

Информация о шифрованных документах заносится в сущность «Шифрованный документ» с однозначно идентифицирующим шифрованный документ

атрибутом «Id_шифровдок».

Таблица 12 – Спецификация атрибутов сущности «Алгоритм»

Название атрибута	Описание атрибута	Диапазон значений	Единицы измерения	Пример
Id_алгоритм	Уникальный идентификатор алгоритма	>0	–	1
Название_алгоритма	Словесное обозначение типа алгоритма шифрования	–	–	RC4

В сущности «Алгоритм» отображаются названия алгоритмов шифрования. Ключевым атрибутом здесь является «Id_алгоритм».

2.3.1.1.3 Назначение связей

Обозначим связи между сущностями. В таблице 13 представлены родительские, дочерние сущности, название, тип связи и обоснование выбора типа связи. Определение связей между сущностями в дальнейшем позволят моделировать отношения между объектами предметной области.

Таблица 13 – Спецификация связей

Родительская сущность	Дочерняя сущность	Название Связи	Связь	Обоснование выбора типа связи
1	2	3	4	5
Подразделение	Должность	Содержит	Один-ко-многим	Одно подразделение содержит несколько должностей, а одной должности соответствует только одно подразделение
Должность	Сотрудник	Назначается	Один-ко-многим	Одна должность может назначаться нескольким сотрудникам, но одному сотруднику соответствует только одна должность
Сотрудник	Документ	Соотносится	Один-ко-многим	Один сотрудник может соотноситься с несколькими документами, но одному документу соответствует лишь один сотрудник
Категория	Документ	Относится	Один-ко-многим	К одной категории относятся несколько документов, а документ относится только к одной категории документов
Категория	Шаблон	Включает	Один-ко-многим	Одна категория включает в себя несколько шаблонов, но шаблон соответствует только одной категории
Документ	Шифрованный документ	Преобразуется	Один-ко-многим	Один документ может преобразовываться в несколько шифрованных документов. Одному шифрованному документу соответствует только один документ-оригинал

Продолжение таблицы 13

1	2	3	4	5
Алгоритм	Шифрованный документ	Соответствует	Один-ко-многим	Один алгоритм может соответствовать нескольким шифрованным документам, но одному шифрованному документу соответствует только один алгоритм
Документ	Журнал	Заносится	Один-ко-многим	Один документ может заносится в журнал многократно, но одной записи в сущности «Журнал» соответствует один документ
Событие	Журнал	Отображается	Один-ко-многим	Одной записи сущности «Событие» соответствует несколько записей сущности «Журнал», а одной записи сущности «Журнал» соответствует только одна запись сущности «Событие»
Сотрудник	Журнал	Отмечается	Один-ко-многим	Одной записи сущности «Пользователь» соответствует несколько записей сущности «Журнал», но одной записи сущности «Журнал» соответствует только дна запись сущности «Пользователь»

2.3.1.1.4 Концептуально-инфологическая модель

На основе разработанной инфологического проектирования была построена концептуально-инфологическая модель базы данных, которая отражена в приложении Д на рисунке Д.1.

2.3.1.2 Логическое проектирование базы данных

2.3.1.2.1 Отображение концептуально-инфологической модели на реляционную модель данных

Связь «Подразделение – Должность» является связью типа «один – ко – многим». Исходной является сущность «Должность», т.к. от нее исходит простая связь. Порожденной является сущность «Подразделение».

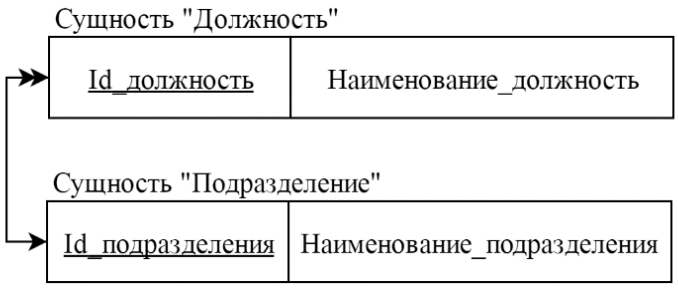


Рисунок 1 – Связь «Подразделение – Должность»

При отображении ключ порожденной сущности добавляется в исходную сущность. Таким образом, ключ «Id_подразделения» из порожденной сущности «Подразделение» добавляется в исходную сущность «Должность» в качестве не ключевого атрибута. Получаем отношения:

Отношение 1 - Должность

Id_должность	Наименование_должность	**Id_подразделения**

Отношение 2 - Подразделение

Id_подразделения	Наименование_подразделения

Рисунок 2 – Отношения «Должность», «Подразделение»

Связь «Должность – Сотрудник» является связью типа «один – ко – многим». Исходной является сущность «Сотрудник», т.к. от нее исходит простая связь. Порожденной является сущность «Должность».

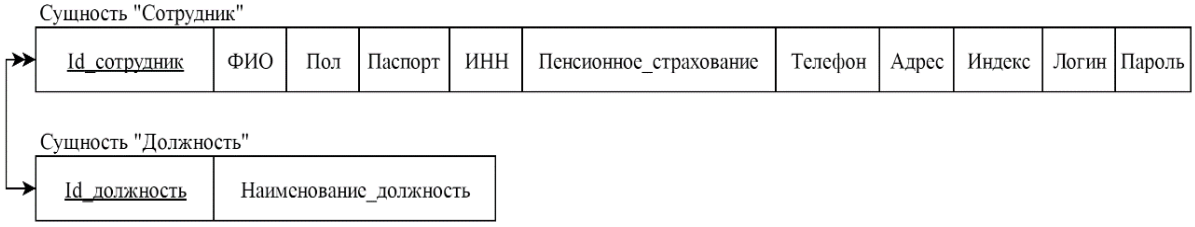


Рисунок 3 – Связь «Должность – Сотрудник»

Ключ «Id_должность» из порождённой сущности «Должность» добавляется в исходную сущность «Сотрудник». Имеем отношения вида:

Отношение 3 - Сотрудник

Id_сотрудник	ФИО	Пол	Паспорт	ИНН	Пенсионное_страхование	Телефон	Адрес	Индекс	Логин	Пароль	**Id_должность**

Отношение 4 - Должность

Id_должность	Наименование_должность

Рисунок 4 – Отношения «Сотрудник», «Должность»

Связь «Сотрудник – Документ» является связью типа «один – ко – многим». Исходной является сущность «Документ», т.к. от нее исходит простая связь. Порожденной является сущность «Сотрудник».

Рисунок 5 – Связь «Сотрудник – Документ»

Ключ «Id_сотрудник» из порождённой сущности «Сотрудник» добавляется в исходную сущность «Документ». Получаем отношения:

Отношение 5 - Документ

Id_документ	Наименование_документа	Дата_создания	Местоположение	**Id_сотрудник**

Отношение 6 - Сотрудник

Id_сотрудник	ФИО	Пол	Паспорт	ИНН	Пенсионное_страхование	Телефон	Адрес	Индекс	Логин	Пароль

Рисунок 6 – Отношения «Документ», «Сотрудник»

Связь «Категория – Документ» является связью типа «один – ко – многим». Исходной является сущность «Документ», т.к. от нее исходит простая связь. Порожденной является сущность «Категория».

Рисунок 7 – Связь «Категория – Документ»

Добавим ключ «Id_категория» из порождённой сущности «Категория» в исходную сущность «Документ». Имеем отношения вида:

Отношение 7 - Документ

Id_документ	Наименование_документа	Дата_создания	Местоположение	**Id_категория**

Отношение 8 - Категория

Id_категория	Название_категория

Рисунок 8 – Отношения «Документ», «Категория»

Связь «Категория - Шаблон» является связью типа «один – ко – многим». Исходной является сущность «Шаблон», т.к. от нее исходит простая связь. Порожденной является сущность «Категория».

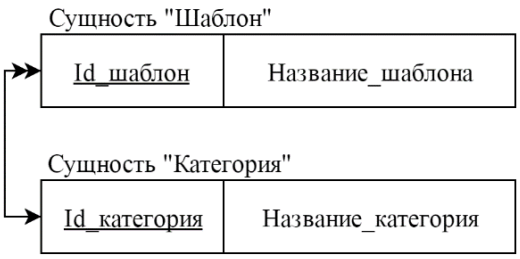


Рисунок 9 – Связь «Категория - Шаблон»

Ключ «Id_категория» из порождённой сущности «Категория» добавляется в исходную сущность «Шаблон». Отношения имеют вид:

Отношение 9 - Шаблон

Id_шаблон	Название_шаблона	**Id_категория**

Отношение 10 - Категория

Id_категория	Название_категория

Рисунок 10 – Отношения «Шаблон», «Категория»

Связь «Документ – Шифрованный документ» является связью типа «один – ко – многим». Исходной является сущность «Шифрованный документ», т.к. от нее исходит простая связь. Порожденной является сущность «Документ».

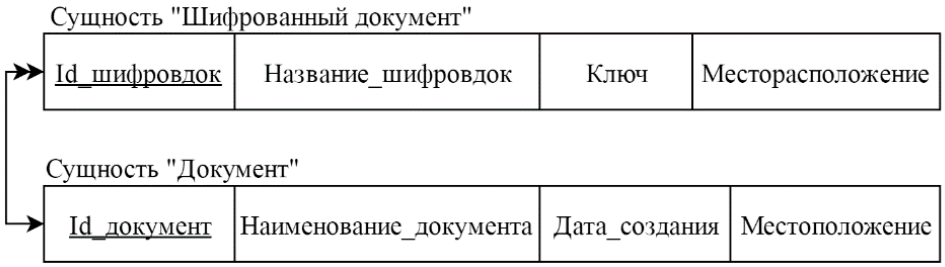


Рисунок 11 – Связь «Документ – Шифрованный документ»

Добавим ключ «Id_документ» из порождённой сущности «Документ» в исходную сущность «Шифрованный документ». Получим отношения вида:

Отношение 11 - Шифрованный документ

Id_шифровдок	Название_шифровдок	Ключ	Месторасположение	**Id_документ**

Отношение 12 - Документ

Id_документ	Наименование_документа	Дата_создания	Местоположение

Рисунок 12 – Отношения «Шифрованный документ», «Документ»

Связь «Алгоритм – Шифрованный документ» является связью типа «один – ко – многим». Исходной является сущность «Шифрованный документ», т.к. от нее исходит простая связь. Порожденной является сущность «Алгоритм».

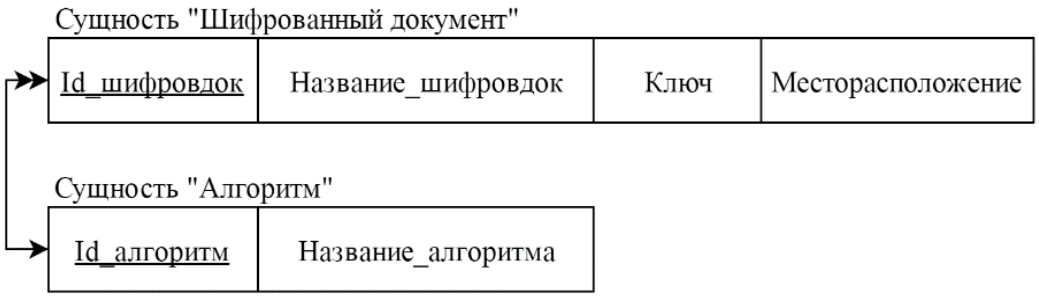


Рисунок 13 – Связь «Алгоритм – Шифрованный документ»

Ключ «Id_алгоритм» из порождённой сущности «Алгоритм» добавляется в исходную сущность «Шифрованный документ». Получаем отношения:

Отношение 13 - Шифрованный документ

Id_шифровдок	Название_шифровдок	Ключ	Месторасположение	**Id_алгоритм**

Отношение 14 - Алгоритм

Id_алгоритм	Название_алгоритма

Рисунок 14 – Отношения «Шифрованный документ», «Алгоритм»

Связь «Документ – Журнал» является связью типа «один – ко – многим». Исходной является сущность «Журнал», т.к. от нее исходит простая связь. Порожденной является сущность «Документ».

Рисунок 15 – Связь «Документ – Журнал»

Добавим ключ «Id_документ» из порождённой сущности «Документ» в исходную сущность «Журнал». Отношения примут вид:

Отношение 15 - Журнал

Id_запись	Дата	Время	Почтовый_адрес	**Id_документ**

Отношение 16 - Документ

Id_документ	Наименование_документа	Дата_создания	Местоположение

Рисунок 16 – Отношения «Журнал», «Документ»

Связь «Событие – Журнал» является связью типа «один – ко – многим». Исходной является сущность «Журнал», т.к. от нее исходит простая связь. Порожденной является сущность «Событие».

Рисунок 17 – Связь «Документ – Журнал»

В данном случае ключ «Id_событие» из порождённой сущности «Событие» добавляется в исходную сущность «Журнал» в качестве не ключевого атрибута. Получим отношения:

Отношение 17 - Журнал

Id_запись	Дата	Время	Почтовый_адрес	**Id_событие**

Отношение 18 - Событие

Id_событие	Название_события

Рисунок 18 – Отношения «Журнал», «Событие»

Связь «Сотрудник – Журнал» является связью типа «один – ко – многим». Исходной является сущность «Журнал», т.к. от нее исходит простая связь. Порожденной является сущность «Сотрудник».

Рисунок 19 – Связь «Сотрудник – Журнал»

Ключ «Id_сотрудник» из порождённой сущности «Сотрудник» добавляется в исходную сущность «Журнал». Отношения имеют вид:

Отношение 19 - Журнал

Id_запись	Дата	Время	Почтовый_адрес	**Id_сотрудник**

Отношение 20 - Сотрудник

Id_сотрудник	ФИО	Пол	Паспорт	ИНН	Пенсионное_страхование	Телефон	Адрес	Индекс

Рисунок 20 – Отношения «Журнал», «Сотрудник»

Проанализировав все отношения, полученные на этапе отображения концептуально-инфологической модели на реляционную, выделяем отношения, относящиеся к одной сущности и составляем итоговый набор отношений, исключая дублирование отношений (исключение повторяющихся отношений). Полученная в результате преобразований реляционная модель представлена в таблицах 14 – 23.

Таблица 14 – Отношение 1 – «Подразделение»

Id_подразделение	Наименование_подразделения

Таблица 15 – Отношение 2 – «Должность»

Id_должность	Наименование_должность	Id_подразделение

Таблица 16 – Отношение 3 – «Сотрудник»

Id_сотрудник	ФИО	Пол	Паспорт	ИНН	Пенсионное_страхование
Телефон	Адрес	Индекс	Логин	Пароль	Id_должность

Таблица 17 – Отношение 4 – «Категория»

Id_категория	Название_категория

Таблица 18 – Отношение 5 – «Шаблон»

Id_шаблон	Название_шаблона	Id_категория

Таблица 19 – Отношение 6 – «Документ»

Id_документ	Наименование_документа	Дата_создания
Месторасположение	Id_категория	Id_сотрудник

Таблица 20 – Отношение 7 – «Алгоритм»

Id_алгоритм	Название_алгоритма

Таблица 21 – Отношение 8 – «Шифрованный документ»

Id_шифровдок	Название_шифровдок	Ключ
Месторасположение	Id_документ	Id_алгоритм

Таблица 22 – Отношение 9 – «Событие»

Id_событие	Название_события

Таблица 23 – Отношение 10 – «Журнал»

Id_запись	Дата	Время	Почтовый_адрес
Id_событие	Id_сотрудник	Id_документ	

2.3.1.2.2 Нормализация отношений

Проведём нормализацию отношений, которая позволит избавиться от избыточности в отношениях и модифицировать их структуру таким образом, чтобы процесс работы с ними не был обременён различными посторонними сложностями.

Все отношения, полученные при отображении концептуальной инфологической модели данных, на реляционную, атомарные, т.е. все значения атрибутов не являются множеством или повторяющейся группой. Следовательно, все отношения находятся в первой нормальной форме.

Диаграммы функциональных зависимостей отношений представлены на рисунках 21 – 30. Отношения находятся во второй нормальной форме, так как

они находятся в первой нормальной форме, нет составных ключей и каждый атрибут, который не является основным, функционально полно зависит от ключа.

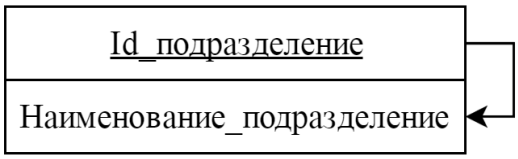


Рисунок 21 – Функциональная зависимость атрибутов отношения «Подразделение»

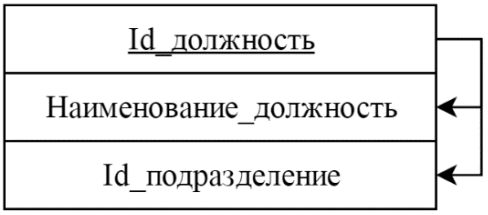


Рисунок 22 – Функциональная зависимость атрибутов отношения «Должность»

Рисунок 23 – Функциональная зависимость атрибутов отношения «Сотрудник»

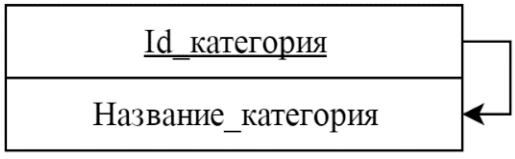


Рисунок 24 – Функциональная зависимость атрибутов отношения «Категория»

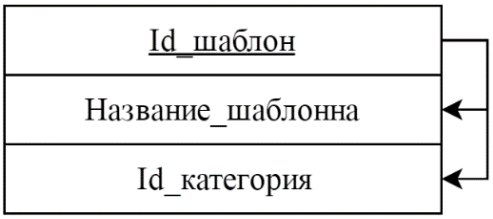


Рисунок 25 – Функциональная зависимость атрибутов отношения «Шаблон»

Рисунок 26 – Функциональная зависимость атрибутов отношения «Документ»

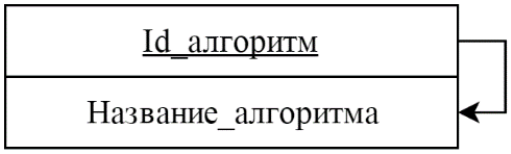


Рисунок 27 – Функциональная зависимость атрибутов отношения «Алгоритм»

Рисунок 28 – Функциональная зависимость атрибутов отношения «Шифрованный документ»

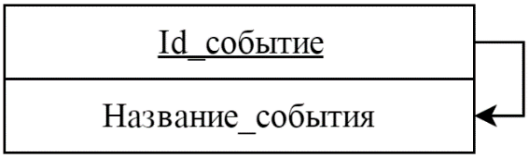


Рисунок 29 – Функциональная зависимость атрибутов отношения «Событие»

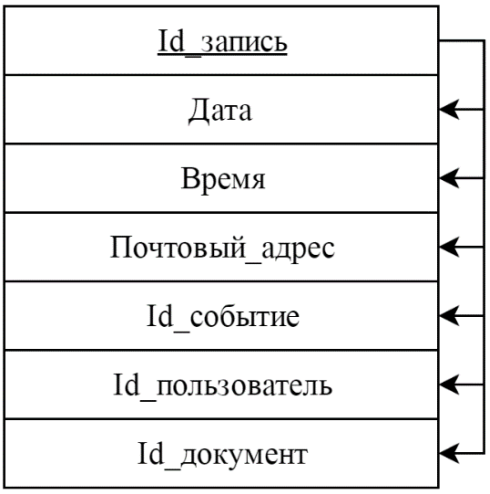


Рисунок 30 – Функциональная зависимость атрибутов отношения «Журнал»

Все полученные нами на предыдущем этапе отношения находятся во второй нормальной форме, и каждый не ключевой атрибут не транзитивно зависит от ключа. Так как между атрибутами оставшихся отношений нет транзитивной зависимости, то, следовательно, эти отношения соответствуют требованиям третьей нормальной форме, и дальнейшей нормализации не требуется.

2.3.1.2.3 Логическая модель

В результате этапа логического проектирования и нормализации были получены отношения, составляющие логическую модель, представленную в приложении Е.

2.3.1.3 Физическое проектирование базы данных

На этапе физического проектирования представлены проекты таблиц, которые будут реализованы в СУБД.

Физическое представление атрибутов сущностей представлено в таблицах 24 − 33.

Таблица 24 – Подразделение

Название поля	Тип данных	Длина	Ограничение	Значение по умолчанию	Допустимость NULL	Индексация
Id_подразделение	int	Длинное целое	>0	−	нет	да
Наименование_подразделения	varchar	25	−	−	нет	нет

Таблица 25 – Должность

Название поля	Тип данных	Длина	Ограничение	Значение по умолчанию	Допустимость NULL	Индексация
Id_должность	int	Длинное целое	>0	–	нет	да
Наименование_должность	varchar	30	–	–	нет	нет
Id_подразделение	int	Длинное целое	>0	–	нет	нет

Таблица 26 – Сотрудник

Название поля	Тип данных	Длина	Ограничение	Значение по умолчанию	Допустимость NULL	Индексация
Id_сотрудник	int	Длинное целое	>0	–	нет	да
ФИО	varchar	60	–	–	нет	нет
Пол	varchar	7	Мужской / Женский	–	нет	нет
Паспорт	varchar	11	0000-000000 – 9999-999999	–	нет	нет
ИНН	bigint	12	000000000000 – 999999999999	–	нет	нет
Пенсионное_страхование	varchar	13	000-000-00000 – 999-999-99999	–	нет	нет
Телефон	int	11	89000000000 – 89999999999	–	нет	нет
Адрес	varchar	50		–	нет	нет
Индекс	bigint	6	000000 – 999999	–	нет	нет
Логин	varchar	20	–	NULL	да	нет
Пароль	varchar	20	–	NULL	да	нет
Id_должность	int	Длинное целое	>0	–	нет	нет

Таблица 27 – Категория

Название поля	Тип данных	Длина	Ограничение	Значение по умолчанию	Допустимость NULL	Индексация
Id_категория	Int	Длинное целое	>0	–	нет	да
Название_категория	varchar	20	–	–	нет	нет

Таблица 28 – Шаблон

Название поля	Тип данных	Длина	Ограничение	Значение по умолчанию	Допустимость NULL	Индексация
Id_шаблон	Int	Длинное целое	>0	–	нет	да
Название_шаблона	varchar	35	–	–	нет	нет
Id_категория	int	Длинное целое	>0	–	нет	нет

Таблица 29 – Документ

Название поля	Тип данных	Длина	Ограничение	Значение по умолчанию	Допустимость NULL	Индексация
Id_документ	int	Длинное целое	>0	–	нет	да
Наименование_документа	varchar	35	–	–	нет	нет
Дата_создания	date	–	≤ Date()	= Date()	нет	нет
Месторасположение	varchar	Max	–	–	нет	нет
Id_категория	int	Длинное целое	>0	–	нет	нет
Id_сотрудник	int	Длинное целое	>0	–	нет	нет

Таблица 30 – Алгоритм

Название поля	Тип данных	Длина	Ограничение	Значение по умолчанию	Допустимость NULL	Индексация
Id_алгоритм	Int	Длинное целое	>0	–	нет	да
Название_алгоритма	varchar	15	–	–	нет	нет

Таблица 31 – Шифрованный документ

Название поля	Тип данных	Длина	Ограничение	Значение по умолчанию	Допустимость NULL	Индексация
Id_шифровдок	int	Длинное целое	>0	–	нет	да
Название_шифровдок	varchar	35	–	–	нет	нет
Ключ	varchar	16	–	–	нет	нет
Месторасположение	varchar	max	–	–	нет	нет
Id_документ	int	Длинное целое	>0	–	нет	нет
Id_алгоритм	int	Длинное целое	>0	–	нет	нет

Таблица 32 – Событие

Название поля	Тип данных	Длина	Ограничение	Значение по умолчанию	Допустимость NULL	Индексация
Id_событие	Int	Длинное целое	>0	–	нет	да
Название_события	varchar	20	–	–	нет	нет

Таблица 33 – Журнал

Название поля	Тип данных	Длина	Ограничение	Значение по умолчанию	Допустимость NULL	Индексация
Id_запись	int	Длинное целое	>0	–	нет	да
Дата	date	–	≤ Date()	= Date()	нет	нет
Время	time	–	≤ Time()	= Time()	нет	нет
Почтовый_адрес	varchar	–	–	–	да	нет
Id_событие	int	Длинное целое	>0	–	нет	нет
Id_сотрудник	int	Длинное целое	>0	–	нет	нет
Id_документ	int	Длинное целое	>0	–	нет	нет

2.3.2 Математическое обеспечение

Для того, чтобы обеспечить надежность, целостность и безопасность информационных технологий активно развиваются и используются кодирование и криптография. Криптография долгое время была засекречена, так как применялась, в основном, для защиты государственных и военных секретов. В настоящее время методы и средства криптографии используются для обеспечения информационной безопасности не только государства, но и организаций, и частных лиц. В современной криптографии все шифросистемы подразделяются на симметричные и асимметричные, а симметричные по конструктивным признакам – на блочные и поточные.

2.3.2.1 Структура алгоритма шифрования AES

Алгоритм шифрования AES представляет собой симметричный алгоритм блочного шифрования блока данных в виде двумерного байтового массива. Алгоритм AES использует ключ шифрования 128 бит и состоит из десяти раундов шифрования.

В каждом раунде алгоритма выполняются преобразования, представленные на рисунке 31.

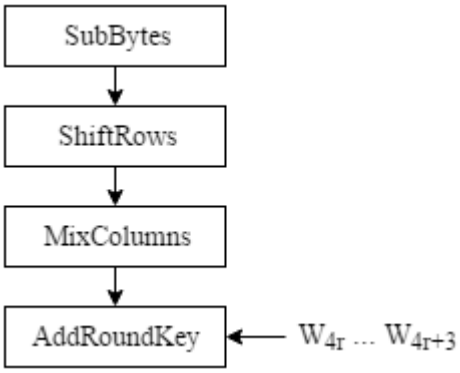


Рисунок 31 – Раунд шифрования алгоритма AES

а) Операция SubBytes эквивалентна комбинации двух операций:

1) вычисление мультипликативной обратной величины от входного значения в конечном поле $GF(2^8)$; обратной величиной от 0 является 0;

2) выходное значение b вычисляется следующим образом:

$$b_i = a_i \oplus a_{i+4 \bmod 8} \oplus a_{i+5 \bmod 8} \oplus a_{i+6 \bmod 8} \oplus a_{i+7 \bmod 8} \oplus c_i, \quad (1)$$

где n_i – i-й бит величины n;

a – результат предыдущей операции;

c – шестнадцатеричная константа 63.

б) Операция ShiftRows, которая выполняет циклический сдвиг влево всех строк массива данных, за исключением нулевой. Сдвиг i-й строки массива (для i = 1,2,3) производится на i байтов.

в) Операция MixColumns выполняет умножение каждого столбца массива данных, который рассматривается как полином в конечном поле $GF(2^8)$, на фиксированный полином a(x):

$$a(x) = 3x^3 + x^2 + x + 2 \quad (2)$$

Умножение выполняется по модулю $x^4 + 1$.

г) Операция AddRoundKey выполняет наложение на массив данных материала ключа. На i-й столбец массива данных (i = 0…3) побитовой логической операцией «исключающее или» накладывается определенное слово расширенного ключа W_{4r+i}, где r – номер текущего раунда алгоритма, начиная с 1.

Перед первым раундом алгоритма выполняется предварительное наложение ключа с помощью операции AddRoundKey, которая производит наложение на открытый текст первых четырех слов расширенного ключа $W_0 \ldots W_3$.

Последний раунд отличается от предыдущих тем, что не выполняется операция MixColumns.

Процедура расширения ключа формирует 4*(R+1) слов Wi для каждого i, вычисляемого по формуле:

$$i = Nk \ldots (4*(R+1) - 1), \quad (3)$$

где Nk – размер исходного ключа шифрования K в словах;

$i = 0 \ldots (Nk - 1)$.

Расширения ключа выполняется в следующей последовательности:

а) Инициализируется временная переменная T:

$$T = W_{i-1} \quad (4)$$

б) Эта переменная модифицируется следующим образом:

1) если i кратно Nk, то:

$$T = SubWord(RotWord(T)) \oplus RC_{i/Nk}, \quad (5)$$

где RCn – слова, в которых все байты, кроме первого, являются нулевыми, а первый байт имеет значение $2^{n-1} \bmod 256$;

2) если Nk = 8 и (i mod Nk) = 4, то:

T = SubWord(T);

3) в остальных случаях модификация переменной T не выполняется.

в) Формируется i-е слово расширенного ключа:

$$W_i = W_{i-Nk} \oplus T \quad (6)$$

Операция SubWord выполняет над каждым байтом входного значения операцию эквивалентную операции SubBytes.

Операция RotWord побайтно вращает входное слово на 1 байт влево.

Расшифрование выполняется применением обратных операций в обратной последовательности. Перед первым раундом расшифрования выполняется обратная самой себе операция AddRoundKey, накладывающая на шифртекст четыре последних слова расширенного ключа, т.е. W_{4R} … W_{4R+3}.

Затем выполняется десять раундов расшифрования, каждый из которых осуществляет преобразования, представленные на рисунке 32.

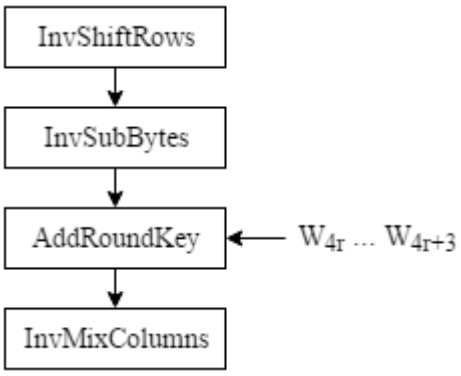


Рисунок 32 – Раунд расшифрования алгоритма AES

а) Операция InvShiftRows производит циклический сдвиг вправо трех последних строк массива данных на то же количество байтов, на которое выполнялся сдвиг операцией ShiftRows при зашифровании.

б) Операция InvSubBytes преобразовывает входной байт обратно второму действию альтернативной операции SubBytes, после чего вычисляется мультипликативная обратная величина от результата предыдущей операции в конечном поле $GF(2^8)$.

в) Операция AddRoundKey, как и при зашифровании, выполняет наложение на обрабатываемые данные четырех слов расширенного ключа W_4 … W_{4r+3}. Нумерация раундов r при расшифровании производится в обратную сторону – от (R – 1) до 0.

г) Операция InvMixColumns выполняет умножение каждого столбца массива данных аналогично прямой операции MixColumns, но умножение производится на полином $a^{-1}(x)$, определенный следующим образом:

$$a^{-1}(x) = Bx^3 + Dx^2 + 9x + E \quad (7)$$

Аналогично зашифрованию, последний раунд расшифрования не содержит операцию InvMixColumns.

2.3.2.2 Структура алгоритма шифрования RC4

Симметричный алгоритм поточного шифрования RC4 представляет собой семейство алгоритмов, задаваемых параметром n = 8. Внутреннее состояние генератора RC4 в момент времени t состоит из таблицы $S_t = (S_t(l))_{l=0}^{2^n-1}$, содержащей 2^n n-битных слов и из двух n-битных слов-указателей i_t и j_t. Таким образом, размер внутренней памяти составляет $M = n2^n + 2n$ бит. Пусть выходное n-битное слово генератора в момент t обозначается как Z_t. Пусть начальные значения $i_0 = j_0 = 0$. Тогда функция следующего состояния и функция выхода RC4 для каждого $t \geq 1$ задается следующими соотношениями:

$$i_t = i_{t-1} + 1 \quad (8)$$

$$j_t = j_{t-1} + S_{t-1}(i_t) \quad (9)$$

$$S_t(i_t) = S_{t-1}(j_t),\ S_t(j_t) = S_{t-1}(i_t) \quad (10)$$

$$Z_t = S_t(S_t(i_t) + S_t(j_t)), \quad (11)$$

где все сложения выполняются по модулю 2^n. Подразумевается, что все слова, кроме подвергаемых свопингу, остаются теми же самыми. Выходная последовательность n-битных слов обозначается как $Z = (Z_t)_{t=1}^{\infty}$. Начальная таблица S_0 задается в терминах ключевой последовательности $K = (K_l)_{l=0}^{2^n-1}$ с использованием той же самой функции следующего состояния, начиная от таблицы единичной подстановки $(l)_{l=0}^{2^n-1}$. Более строго, пусть $j_0 = 0$ и для каждого $1 \leq t \leq 2^n$ вычисляется $j_t = (j_{t-1} + S_{t-1}(t - 1) + K_{t-1}) \bmod 2^n$, а затем переставляются местами $S_{t-1}(t - 1)$ и $S_{t-1}(j_t)$. На последнем шаге порождается таблица, представляющая S_0. Ключевая последовательность K составляется из секретного ключа, возможно повторяющегося, и рандомизирующего ключа, передаваемого в открытом виде в целях ресинхронизации.

Осуществляется алгоритм RC4 в два этапа. На первом, подготовительном этапе производится инициализация таблицы замен – распределителя S – массив. В каждый момент времени таблица S содержит все возможные n-битовые числа

в перемешанном виде. Конкретная перестановка значений в таблице определяется ключом. На втором, основном этапе вычисляются псевдослучайные числа и осуществляется шифрование. Блок-схемы зашифровки и расшифровки сообщений алгоритмом RC4 представлены в приложении Ж на рисунках Ж.1 и Ж.2.

Рассмотрим пример зашифровки сообщения M (таблица 1), где таблица S будет заполнена последовательностью от 0 до 8 (таблица 2), а ключ K – массив, который заполняется последовательностью 4-битовых слов (n=4) такого же размера, как S (таблица 3). В случае, если ключ оказался короче таблицы S, он повторяется необходимое число раз. В данном примере алгоритм вычисления псевдослучайных чисел примет следующий вид:

Первый этап:

а) j = 0, i = 0;

б) j = (j + Si + Ki) mod 8;

в) поменять местами Si и Sj;

г) i = i + 1;

д) если i < 8, то перейти к 2.

Второй этап:

а) i = 0, j = 0, a = 0;

б) i = (i + 1) mod 8;

в) j = (j + Si) mod 8;

г) поменять местами Si и Sj;

д) a = (Si + Sj) mod 8;

е) Zi = Sa.

2.3.2.3 Структура алгоритма хеширования MD5

На вход алгоритма хеширования MD5 поступает входное сообщение длины L – целое неотрицательное число. Затем выполняются следующие шаги алгоритма:

а) Выравнивание потока.

Дописывается единичный бит в конец потока, а затем необходимое количество нулевых бит. Входные данные до нового размера L', сравнимого с 448 по модулю 512.

$$L' = 512 \times N + 448, \quad (12)$$

где N – любое натуральное число, такое, что это выражение будет наиболее близко к длине блока.

б) Добавление длины сообщения.

В сообщение дописывается 64-битное представление длины исходного сообщения, после чего длина потока становится кратной 512.

в) Инициализация буфера.

Буфер четырех переменных размером по 32 бита, представляющий собой двойные слова – A, B, C, D, инициализируется шестнадцатеричными значениями в порядке от младшего байта. Буфере необходим для хранения результатов промежуточных вычислений.

г) Вычисление в цикле

Для вычисления хеша MD5 определены следующие четыре функции:

$$F(X,Y,Z) = (X \wedge Y) \vee (\neg X \wedge Z), \quad (13)$$

$$G(X,Y,Z) = (X \wedge Z) \vee (\neg Z \wedge Y), \quad (14)$$

$$H(X,Y,Z) = X \oplus Y \oplus Z, \quad (15)$$

$$I(X,Y,Z) = Y \oplus (\neg Z \vee X), \quad (16)$$

где X,Y,Z — двойные слова.

Строится 64-элементная таблица констант T[1 … 64], построенная по формуле:

$$T[n] = \text{int}(2^{32} \times |\sin n|) \quad (17)$$

Каждый 512-битный блок проходит 4 раунда вычислений по 16 преобразований, в общем виде которые имеют вид:

$$A = B + ((A + Fun(B,C,D) + X[k] + T[i]) <<< s), \quad (18)$$

где Fun(B,C,D) — одна из логических функций;

X[k] — k-тый элемент 16-битного блока;

T[i] — i-тый элемент таблицы констант;

<<< s — операция циклического сдвига на s позиций влево.

На рисунке 33 представлено выполнение отдельного шага.

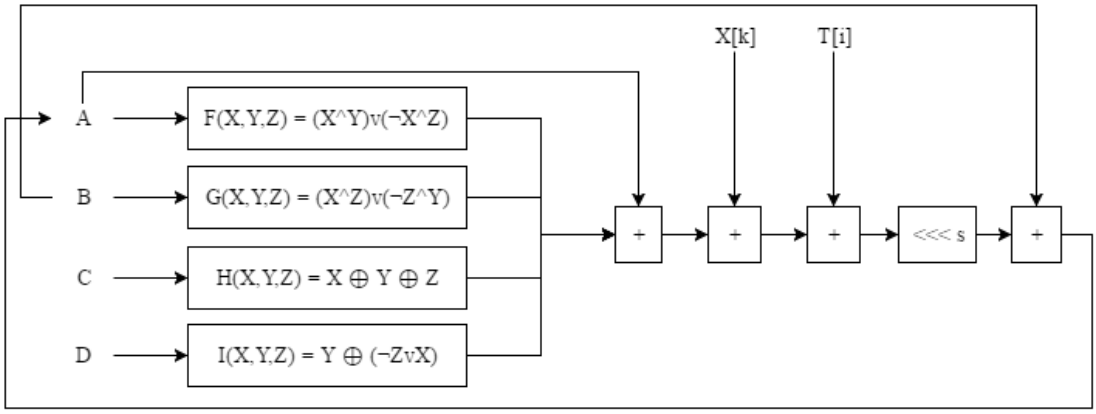


Рисунок 33 – Выполнение цикла алгоритма хеширования MD5

Далее производится суммирование вычислений:

$$A = A + A0; \quad (19)$$

$$B = B + B0; \quad (20)$$

$$C = C + C0; \quad (21)$$

$$D = D + D0, \quad (22)$$

где A0, B0, C0, D0 – значения, полученные на предыдущем шаге.

Результат выводится из буфера побайтово, начиная с переменной A и заканчивая переменной D.

2.3.3 Техническое обеспечение

Для обеспечения централизованного хранения данных, а также для улучшения обмена информации и взаимодействия сотрудников на базе деятельности отдела кадров компании необходимо создать локальную вычислительную сеть на основе сервера БД. Данная ЛВС будет включать в себя 2 компьютера сотрудников отдела и кадров и 1 компьютер директора.

Разрабатываемая ЛВС соответствует архитектуре «клиент-сервер», с моделью сервера БД, представленной на рисунке 34.

Рисунок 34 – Модель сервера БД

В данной модели компонент представления располагается на компьютере клиента, а прикладной компонент SQL, компонент доступа к БД и сама БД располагаются на компьютере-сервере. Компонент представления вызывает прикладной компонент SQL, который в свою очередь посылает запрос компоненту доступа БД. Компонент доступа читает данные из БД и посылает ответ прикладному компоненту SQL, а прикладной компонент предоставляет клиенту результат – блоки данных.

Структурная схема локальной вычислительной сети представлена на рисунке 35. Данная ЛВС имеет топологию типа «звезда», которая включает концентратор, сервер БД, Web сервер, компьютер-клиент директора, компьютер-клиент начальника отдела кадров, компьютер-клиент специалиста по кадрам.

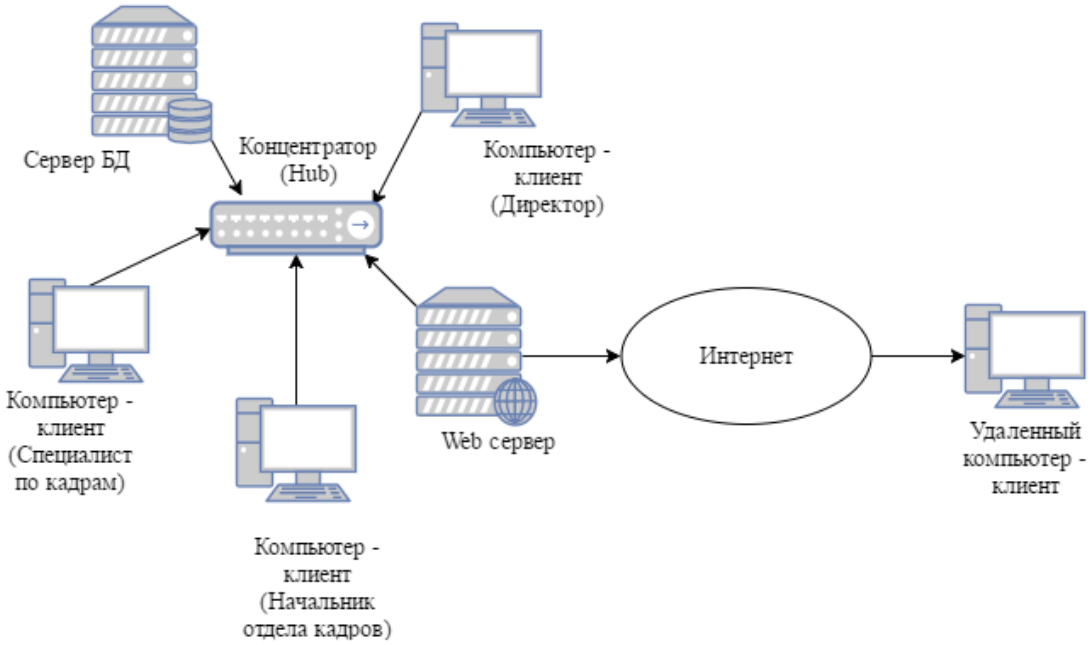


Рисунок 35 – Структурная схема ЛВС

Для реализации, представленной ЛСВ, необходимо закупить сервер БД и концентратор. Сервер БД должен отвечать следующим характеристикам для размещения малой БД:

а) размер файла БД не более 10 Гб;

б) количество одновременных подключений не более 20;

в) оперативная память 16 Гб;

г) операционная система Windows Server 2012 64 бит;

д) файловая система NTFS;

е) количество ядер процессоров до 4-х;

ж) количество жестких дисков для размещения БД до 4 HDD.

Характеристики концентратора:

а) 5-8 портов для подключения сетевых линий;

б) скорость передачи данных 100 Мбит/с;

в) коаксиальное подключение.

2.3.4 Программное обеспечение

Для организации работы подсистемы криптографической защиты ПДн в электронном документообороте необходимо, чтобы на компьютерах-клиентах стояла операционная система семейства Windows. На сервере требуется установить серверную операционную систему Windows Server 2012 64 бит и систему управления реляционными БД Microsoft SQL Server 2012.

В случае необходимости внесения изменений в разрабатываемую подсистему рекомендуется использовать среду разработки программного обеспечения Microsoft Visual Studio 2015 и ее встроенный компилятор.

Для проектирования функциональных структур и документооборота предприятия использовался пакет BPWin, для проектирования и разработки БД использовалось средство разработки структуры базы данных ERWin.

2.3.5 Организационное обеспечение

Изучив линейно-организационную структуру компании были выделены два вида категории пользователей создаваемой подсистемы криптографической защиты ПДн в электронном документообороте – это «Пользователь» и «Администратор».

К категории «Пользователь» относятся сотрудники отдела кадров, а также директор компании, которые непосредственно работают с документами. Данная

категория может создавать документы тем самым пополняя БД, заносить в БД новых сотрудников, открывать и изменять документы, шифровать и расшифровывать документы, передавать документы.

Категория «Администратор» назначается сотруднику, который будет ответственен за регистрацию в подсистеме ее новых пользователей. Также данная категория имеет доступ к журналу событий, по которому может отследить то или иное событие или действия конкретного пользователя.

2.3.6 Правовое обеспечение

Рассмотрим основные законодательные мероприятия применимые к управляющей компании «Аист»:

а) В случае, когда управляющая компания нарушает порядок размещения информации в государственной информационной системе жилищно-коммунального хозяйства кодексом Российской Федерации об административных правонарушениях (КоАП) статьей 13.19.1 и статьей 13.19.2 «Нарушение порядка размещения информации в государственной информационной системе жилищно-коммунального хозяйства» предусматриваются административные наказания в виде административного штрафа либо дисквалификации на срок от одного года до трех лет.

б) Сотрудник, совершивший нарушение правил защиты информации, привлекается к административной ответственности в соответствии с КоАП по статье 13.12 «Нарушение правил защиты информации», которая освещает широкий спектр правонарушений, за которые предусмотрены наказания в виде административного штрафа.

в) Работники кадрового отдела в случае нарушения установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) привлекаются к административной ответственности в соответствии с КоАП по статье 13.11 «Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)». Наказания:

– на должностных лиц – от пятисот до одной тысячи рублей;

– на юридических лиц – от пяти тысяч до десяти тысяч рублей.

г) В случае осуществления сотрудником компании неправомерного доступа к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации, наступает уголовная ответственность по статье 272 «Неправомерный доступ к компьютерной информации». Нарушения по данной статье предусматривают наказания:

– штраф в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев;

– исправительные работы на срок до одного года;

– ограничение свободы на срок до двух лет;

– принудительные работы на срок до двух лет;

– лишение свободы на срок до двух лет.

д) Сотрудники компании, использующие и распространяющие вредоносные программы, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, привлекаются к уголовной ответственности в соответствии со статьей 273 «Создание, использование и распространение вредоносных компьютерных программ». Наказания за эти преступления:

– ограничение свободы на срок до четырех лет;

– принудительные работы на срок до четырех лет;

– лишение свободы на срок до четырех лет со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев.

е) Сотрудники, работающие в компании, в случае нарушения правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуника-

ционным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб привлекаются к уголовной ответственности в соответствии со 274 «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей». Данная статья предусматривает следующие наказания:

– штраф в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев;

– исправительные работы на срок от шести месяцев до одного года;

– ограничение свободы на срок до двух лет;

– принудительные работами на срок до двух лет;

– лишение свободы до двух лет.

3 РАЗРАБОТКА ПОДСИСТЕМЫ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ

3.1 Обоснование выбора среды разработки

Для разработки подсистемы криптографической защиты персональных данных в электронном документообороте была выбрана среда разработки программного обеспечения Microsoft Visual Studio 2015 бесплатной редакции Community Edition, поставляемая вместе с платформой .NET Framework, которая построена на принципах объектно-ориентированного программирования. Данная среда включает в себя широкий спектр библиотек, а также весь необходимый инструментарий, позволяющий быстро и эффективно создать графический интерфейс приложения. Microsoft Visual Studio 2015 совмещает в себе конструкторы, редакторы, отладчики и профилировщики, что повышает производительность программирования. Встроенная платформа .NET Framework, благодаря общеязыковая среда исполнения, поддерживает работу с различными языками программирования высокого уровня. Для разработки подсистемы использовался язык программирования C#.

Язык C# был разработан для платформы .NET на базе таких языков программирования, как C++, Java, Visual Basic, Pascal, Delphy, переняв у них немало полезных свойств. C# является полностью объектно-ориентированным языком, поддерживающий инкапсуляцию, наследование и полиморфизм. Синтаксис C# проще, чем у C++, а значит шансов допустить ошибку при написании меньше.

Для создания и работы с базой данных использовалась СУБД Microsoft SQL Server 2012. Данная СУБД проста в использовании, работа в ней может осуществляться как через интуитивно понятный графический интерфейс, так и через написание SQL запросов.

Управление базой данных осуществляется через структурированный язык запросов SQL, с помощью которого можно заносить, изменять, удалять, выводить данные, а также создавать хранимые процедуры.

3.2 Разработка базы данных

Создаваемая база данных имеет вид реляционной БД, этапы проектирования которой подробно описаны в главе 2. Схемы и диаграммы БД представлены в приложениях Д и Е.

Для создания таблиц использовался оператор CREATE TABLE с описанием создаваемых полей – название, тип и длина. Каждая таблица имеет свой первичный ключ, который в синтаксисе SQL задавался для соответствующего поля ограничителем PRIMARY KEY. Для изменений таблиц использовался оператор ALTER TABLE ADD – добавление новых полей, ограничений, оператор ALTER TABLE DROP – удаление полей и ограничений. Чтобы отобразить результат ведения журнала создаваемой подсистемы в удобном для пользователя виде, было создано представление оператором CREATE VIEW.

Также в создаваемой подсистеме были реализованы операторы манипуляции с данными для работы с базой данных. Оператор SELECT участвует в реализации авторизации пользователей, тем самым допуская их к функционалу пользователя или администратора, либо нет. Также этот оператор участвует в выборке данных, а именно: поиск данных о сотрудниках по ФИО или по занимаемой должности, поиск документов по категории, по ФИО сотрудника или занимаемой должности на которого оформлен документ, поиск записей в журнале по дате, событию и ФИО сотрудника, являющимся пользователем подсистемы.

Оператор INSERT организует добавление новой информации в базу данных. Используется для осуществления добавления информации о новых сотрудниках, создаваемых документах, шифруемых документов, новых пользователях подсистемы, событий, заносимых в журнал.

Для обновления информации используется оператор UPDATE, который задействован в изменении сведений о сотрудниках.

Удаление информации осуществляется посредством оператора DELETE для организации удаления старых учетных записей пользователей.

В создаваемой подсистеме необходимо установить подключение базы данных для взаимодействия программы с ней. Необходимым условием является

подключение библиотеки System.Data.SqlClient, а также создания класса SqlConnection, который подключает базу данных после получения строки соединения.

Затем для выполнения вышеописанных операторов с запросами необходимо открыть подключение методом SqlConnection.Open(). Запросы необходимо оформлять в класс SqlCommand. Для чтения данных, выбранных запросом создается класс SqlDataReader, для построения которого используется метод SqlCommand.ExecuteReader. Добавление новых данных осуществляется с помощью методов SqlParameterCollection.AddWithValue и SqlCommand.ExecuteNonQuery. После работы с БД необходимо закрыть подключение методом SqlConnection.Close().

3.3 Разработка программного модуля криптографической защиты персональных данных

Подсистема включает в себя модули:

а) авторизация пользователей;

б) обработка документов;

в) шифрование документов;

г) расшифрование документов;

д) передача документов;

е) ведение журнала;

ж) регистрация пользователей.

Взаимодействия между модулями и с базой данных, представлены в приложении К на рисунке К.1.

Для работы с содержимым документов необходимо подключение COM библиотеки Microsoft.Office.Interop.Word. С ее помощью можно создавать, заносить данные, открывать документы. Для автоматической интеграции данных используется класс ReplaceWordStub, а для сохранения – wordDocument.SaveAs. Сохранение документов осуществляется в выделенные директории на диске компьютера. Метод System.Diagnostics.Process.Start осуществляет открытие документов.

Шифрование осуществляется по общей схеме симметричного алгоритма, представленной на рисунке 36.

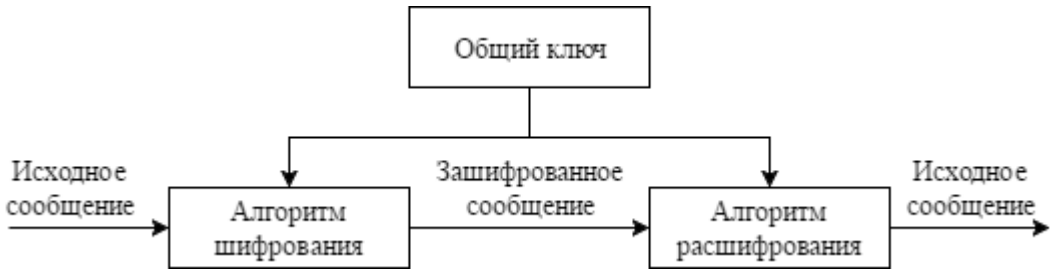


Рисунок 36 – Стандартная схема симметричных алгоритмов шифрования

Для повышения защиты в создаваемой подсистеме шифрования и расшифрования будет использоваться не сам ключ, а заданный фрагмент его хеша, вычисленный по алгоритму MD5. Таким образом стандартная схема преобразуется в схему, представленную на рисунке 37.

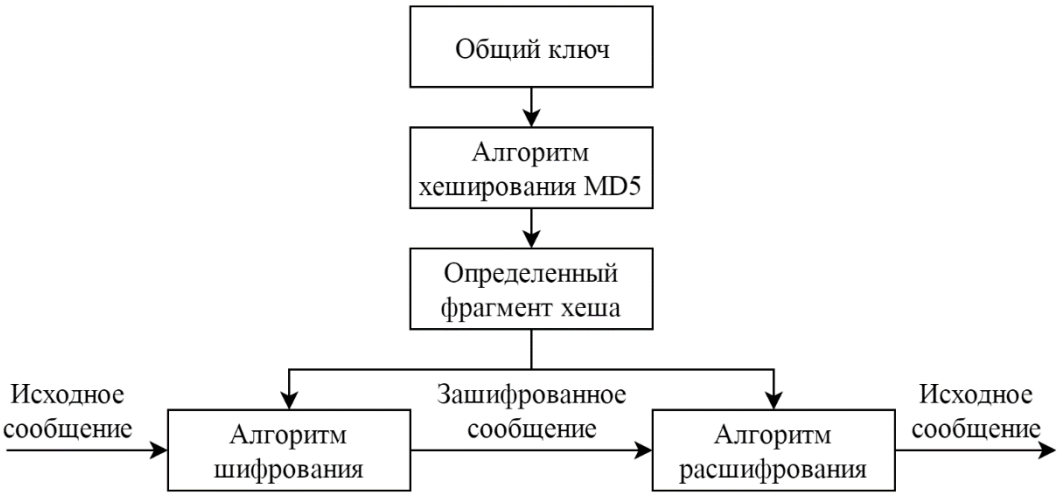


Рисунок 37 – Предлагаемая схема шифрования

Аналогично в обратном порядке производится расшифрование. При написании кода на формах, обеспечивающих процессы шифрования и расшифрования необходимо вызвать библиотеку System.Security.Cryptography. Для алгоритма RC4 нужно создать класс с его алгоритмом.

На формах передачи документов нужно подключить библиотеки System.Net и System.Net.Mail. Класс SmtpClient необходим для задания SMTP-сервера и порта, через которые будет отправляться электронное письмо. Класс ClientCredentials осуществляет проверку адреса отправителя и пароля. Формирование письма с темой, адресатом, прикрепляемыми файлами свойством

MailMessage.Attachments и текстом осуществляет класс MailMessage. Метод SmtpClient.Send непосредственно отправляет электронное письмо. Также используется библиотека System.Text.RegularExpressions, чтобы задать фильтры, которые не позволят задать неправильный электронный адрес.

Остальные модули работают в основном с базой данных, реализация которой описана выше в пункте 3.1.

3.4 Разработка руководства пользователя

Перед началом работы с подсистемой необходимо пройти авторизацию. Окно авторизации представлено на рисунке 38. Здесь нужно ввести логин, пароль пользователя или администратора и нажать кнопку «Вход».

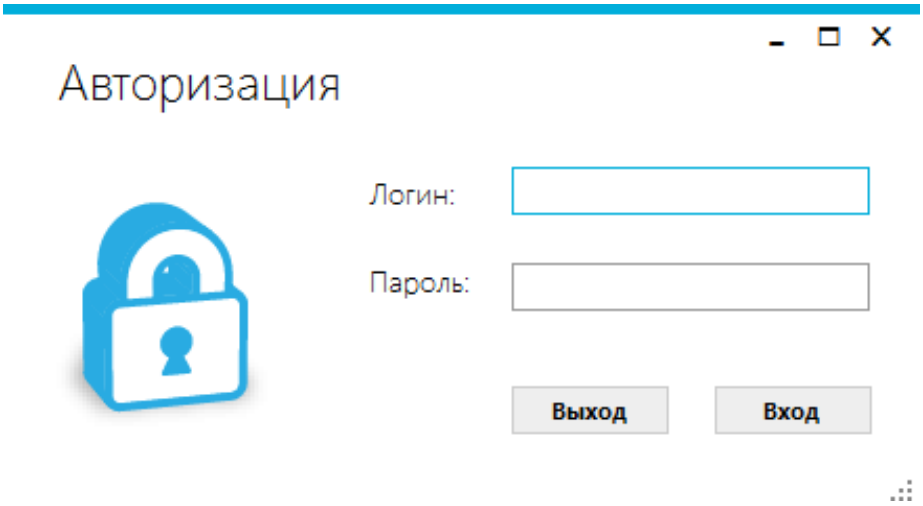


Рисунок 38 – Окно «Авторизация»

После авторизации в соответствии с правами откроется окно для пользователя или администратора. Окно пользователя, представлено на рисунке 39. На этом окне располагаются плитки перехода на другие формы в соответствии с функциями, выполняемыми программой. Плитки разделены по разделам: сотрудники, документы, шифрование.

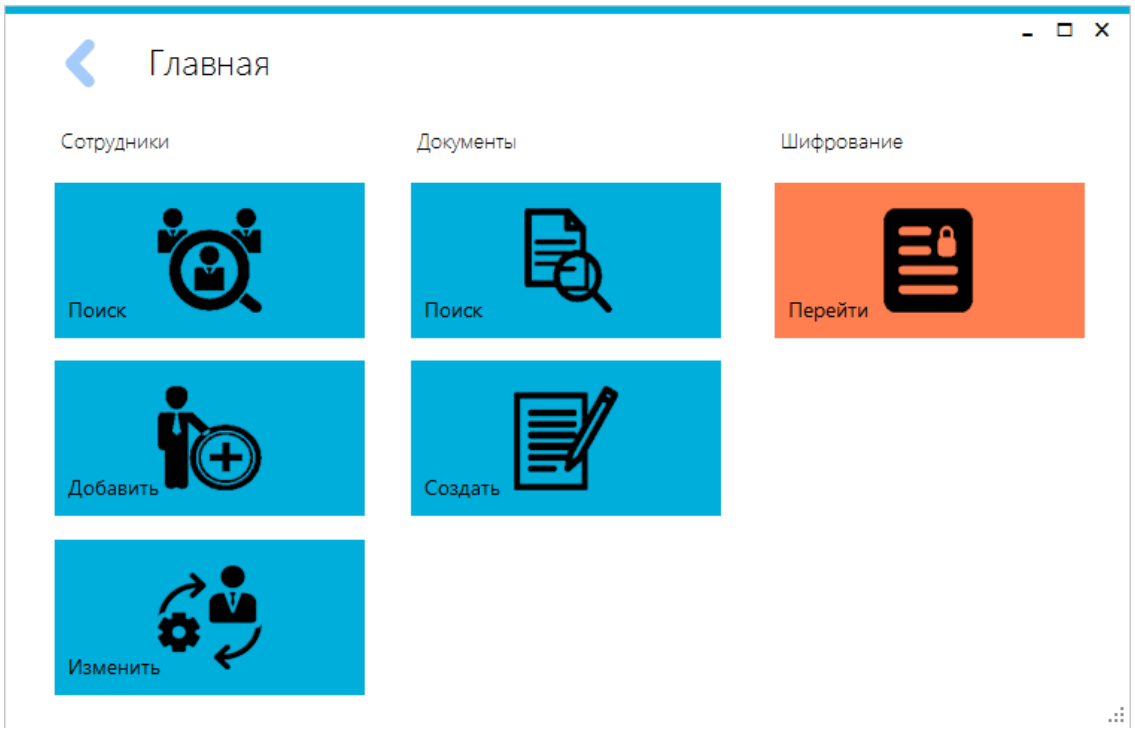


Рисунок 39 – Окно «Главная»

Выбрав плитку «Поиск» из категории сотрудник, откроется окно «Список сотрудников», представленное на рисунке 40. Здесь осуществляется поиск сотрудников по ФИО и по занимаемой должности.

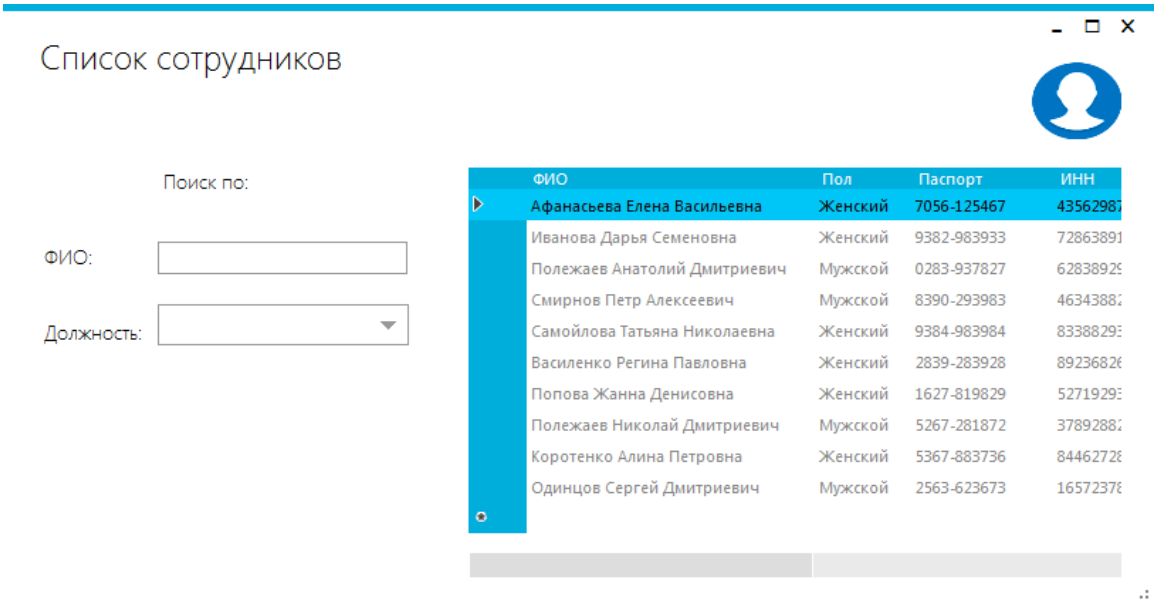


Рисунок 40 – Окно «Список сотрудников»

Выбрав плитку «Добавить» из категории сотрудник, открывается окно «Добавить сотрудников», изображенное на рисунке 41. Здесь необходимо заполнить все поля данными нового сотрудника и нажать кнопку «Добавить».

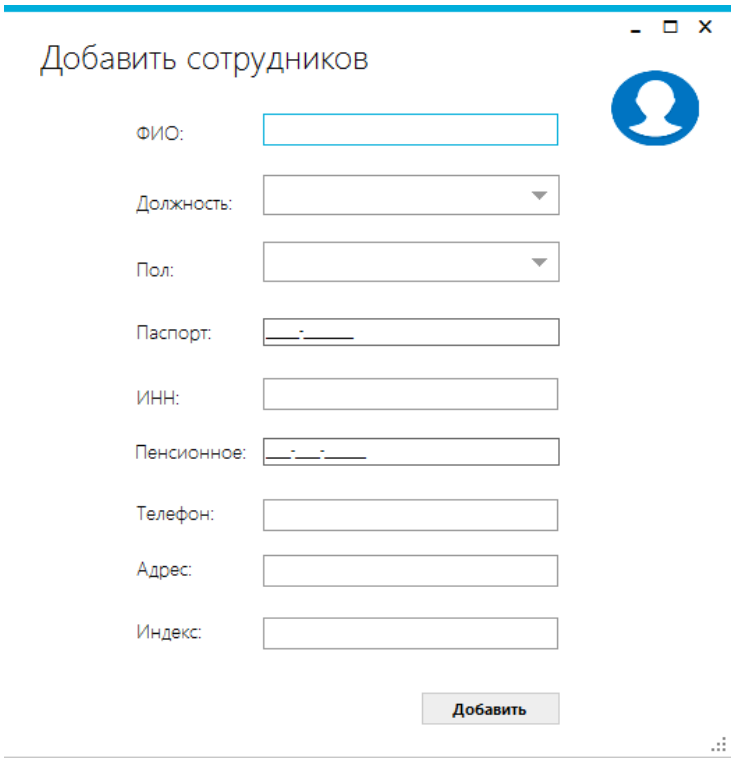


Рисунок 41 – Окно «Добавить сотрудников»

Плитка «Изменить» из категории сотрудник, открывает окно «Изменить данные», представленное на рисунке 42. Для изменения данных сотрудника можно осуществить его поиск по ФИО или по должности, занести его измененные данные в соответствующие поля и нажать кнопку «Изменить».

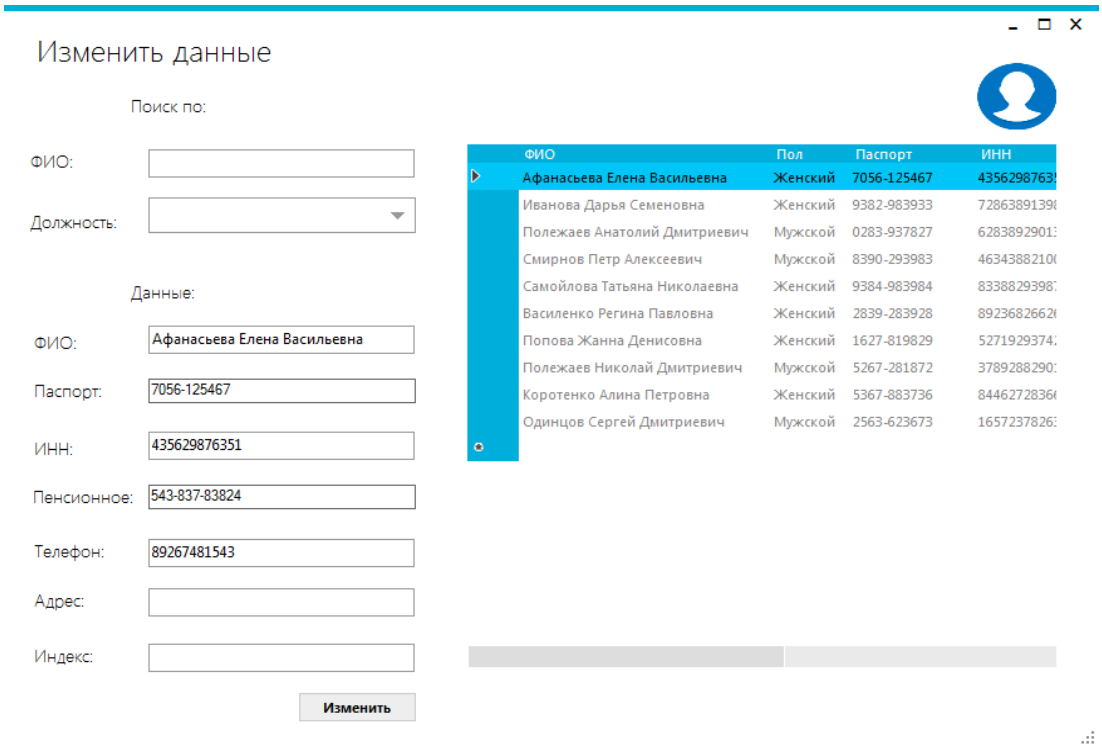


Рисунок 42 – Окно «Изменить данные»

Плитка «Поиск» из категории документы, открывает окно «Список документов», представленное на рисунке 43. Поиск документов осуществляется по категории документа, а также по ФИО или должности сотрудника, на которого оформлен документ. Найденный документ можно сразу же открыть, нажав кнопку «Открыть».

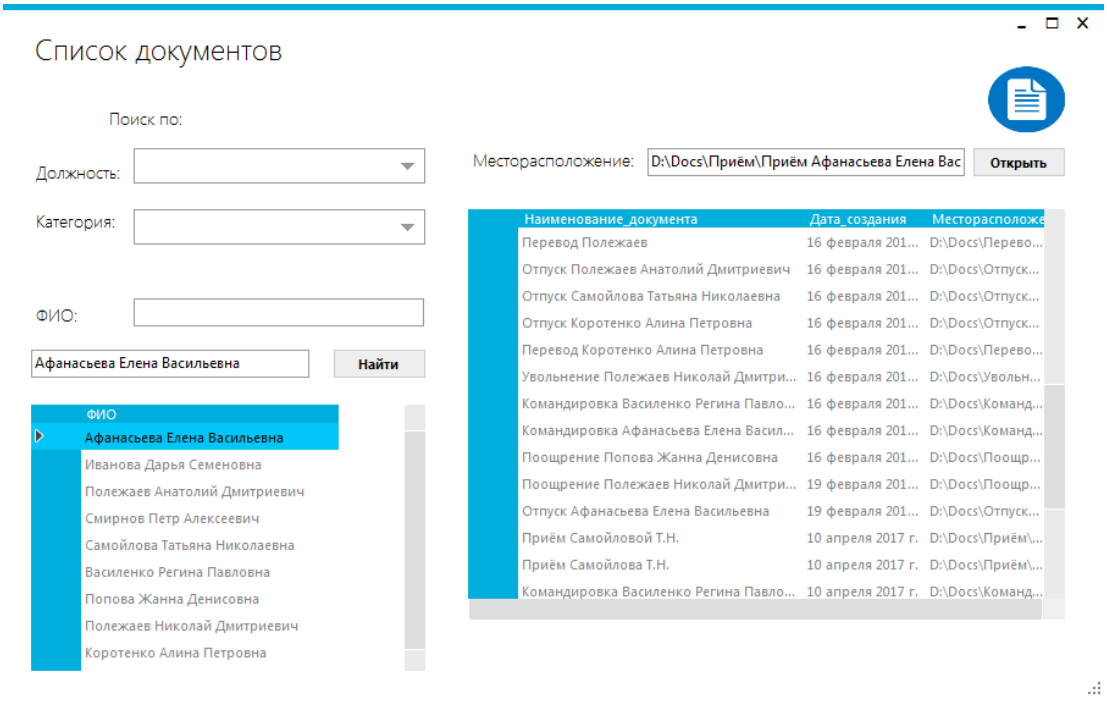


Рисунок 43 – Окно «Список документов»

Выбрав плитку «Создать» из категории документы, открывается окно «Создать документ», изображенное на рисунке 44. Здесь выбирается плитка с категорией документа, который необходимо создать.

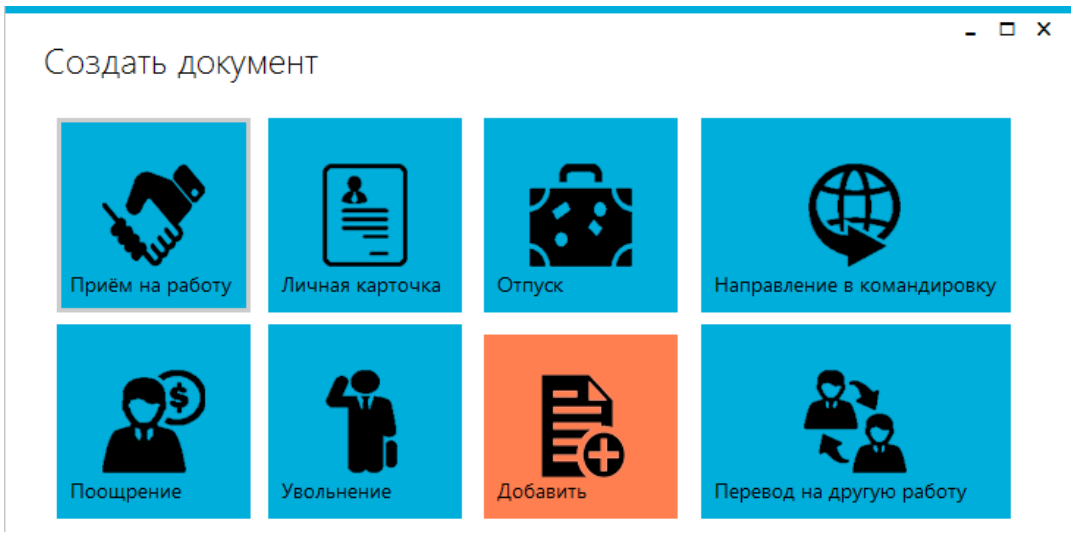


Рисунок 44 – Окно «Создать документ»

Рассмотрим создание документа на примере личной карточки сотрудника. Для этого нужно выбрать плитку «Личная карточка» в окне «Создать документ». Откроется окно «Личная карточка работника», представленная на рисунке 45. Для создания личной карточки работника необходимо выбрать сотрудника из списка для которого создается личная карточка и задать имя документа. Осуществить поиск сотрудника в списке можно по ФИО. Поля, представленные на данном окне, автоматически заносятся в создаваемый документ.

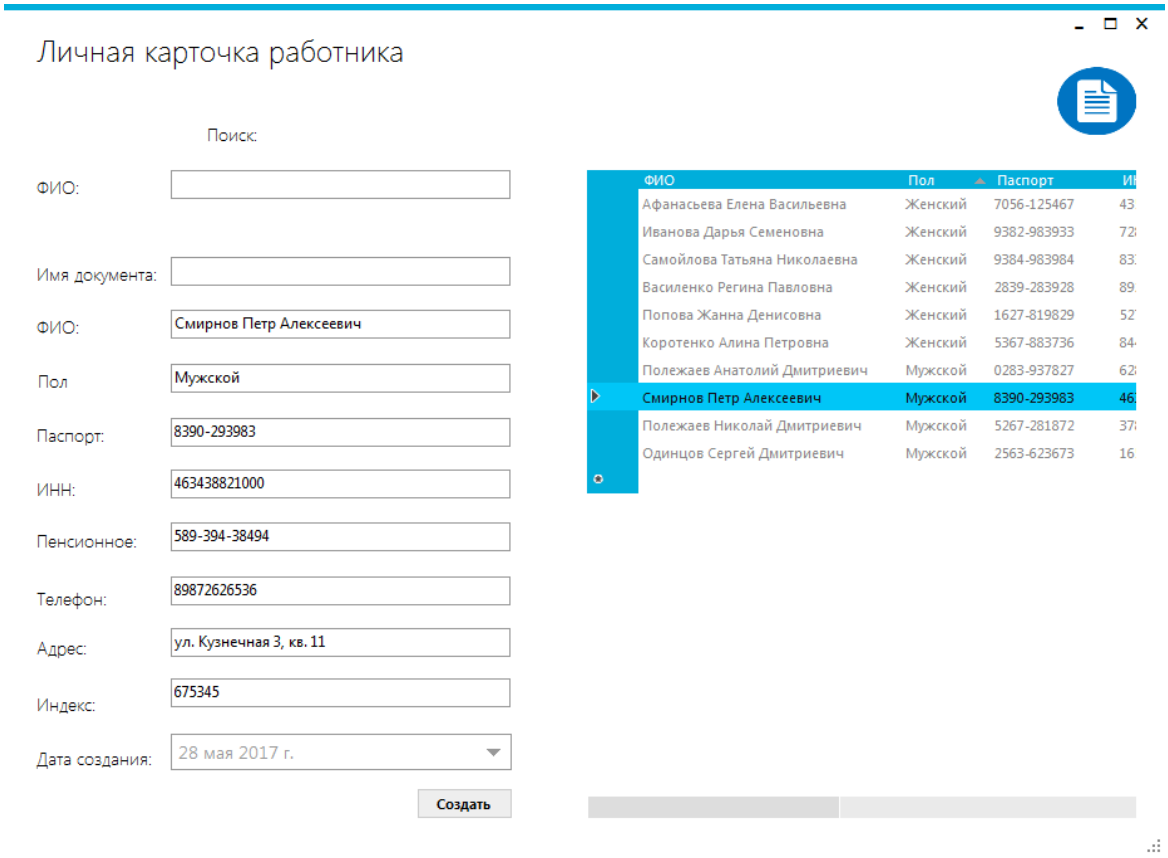


Рисунок 45 – Окно «Личная карточка работника»

Для шифрования документа необходимо выбрать плитку «Перейти» из категории шифрование окна «Главная». Откроется окно «Шифрование», изображенное на рисунке 46. С этого окна можно перейти к шифрованию, расшифрованию, передачи документа.

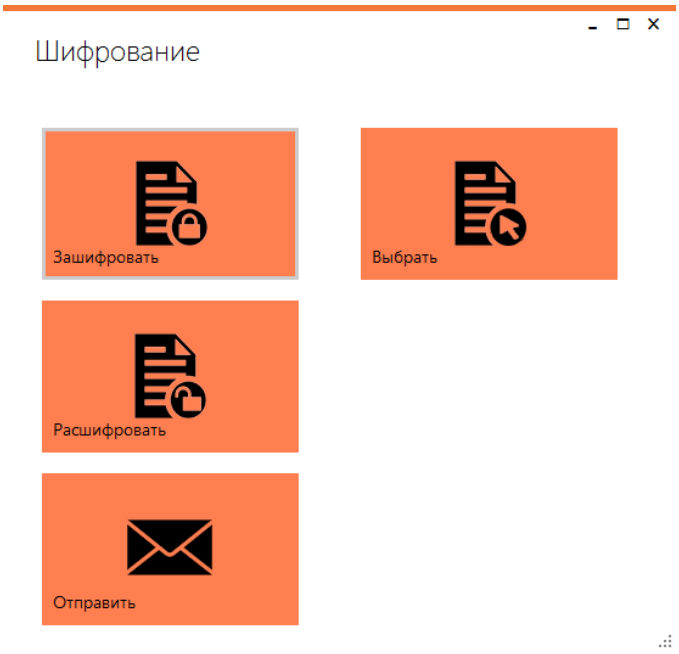


Рисунок 46 – Окно «Шифрование»

Плитка «Зашифровать» открывает окно «Зашифровать документ», представленное на рисунке 47. Для шифрования выбирается документ, который необходимо зашифровать, задается его название и ключ, по которому документ шифруется. Выбирается алгоритм шифрования и нажимается соответствующая кнопка: «Зашифровать AES», «Зашифровать RC4». Также для быстрого нахождения документа реализован поиск по фильтрам.

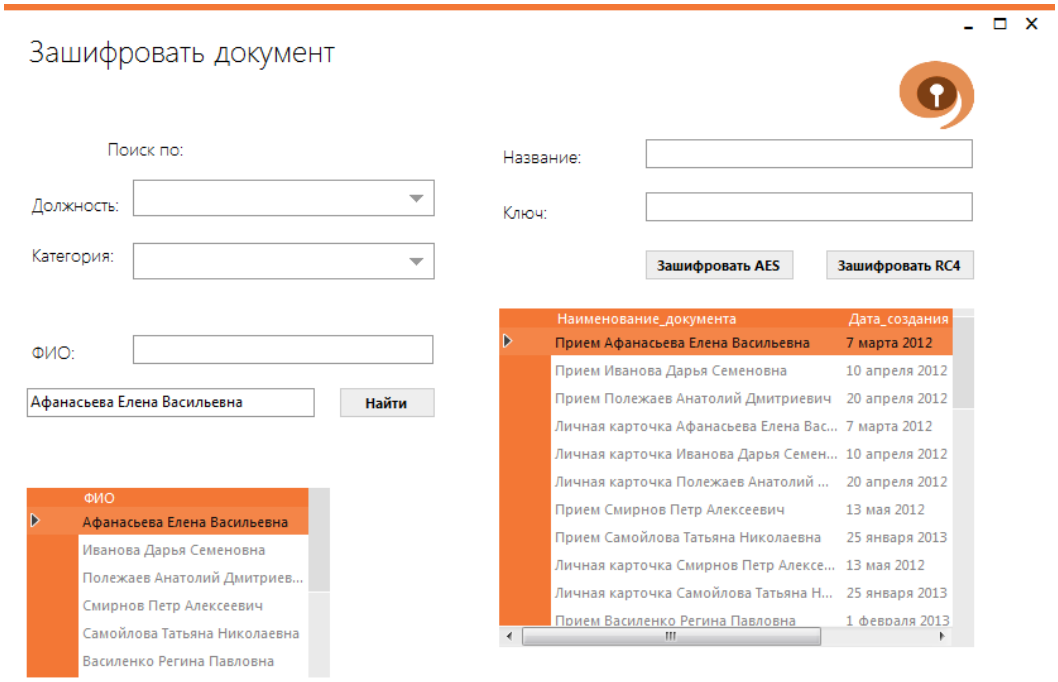


Рисунок 47 – Окно «Зашифровать документ»

Для расшифровки необходимо выбрать плитку «Расшифровать», тогда появится окно «Расшифровать документ», представленное на рисунке 48. Выбирается шифрованный документ и расшифровывается соответствующим алгоритмом. В случае выбора неверного алгоритма будет выдано сообщение об ошибке.

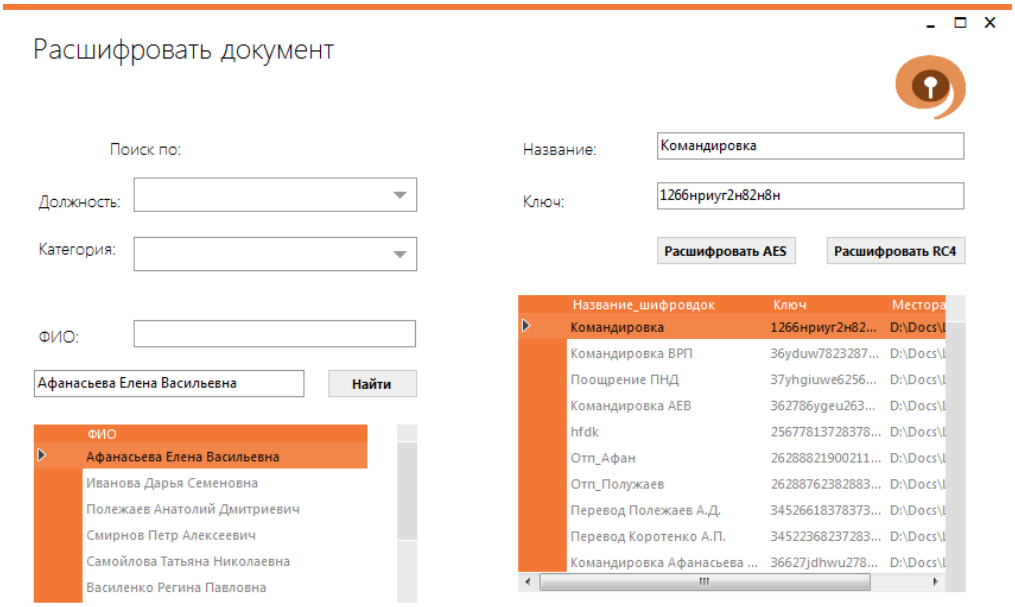


Рисунок 48 – Окно «Расшифровать документ»

При выборе плитки «Отправить» открывается окно «Отправить документ», изображенное на рисунке 49. Здесь выбирается зашифрованный документ из списка и задается адрес по которому отправляется документ.

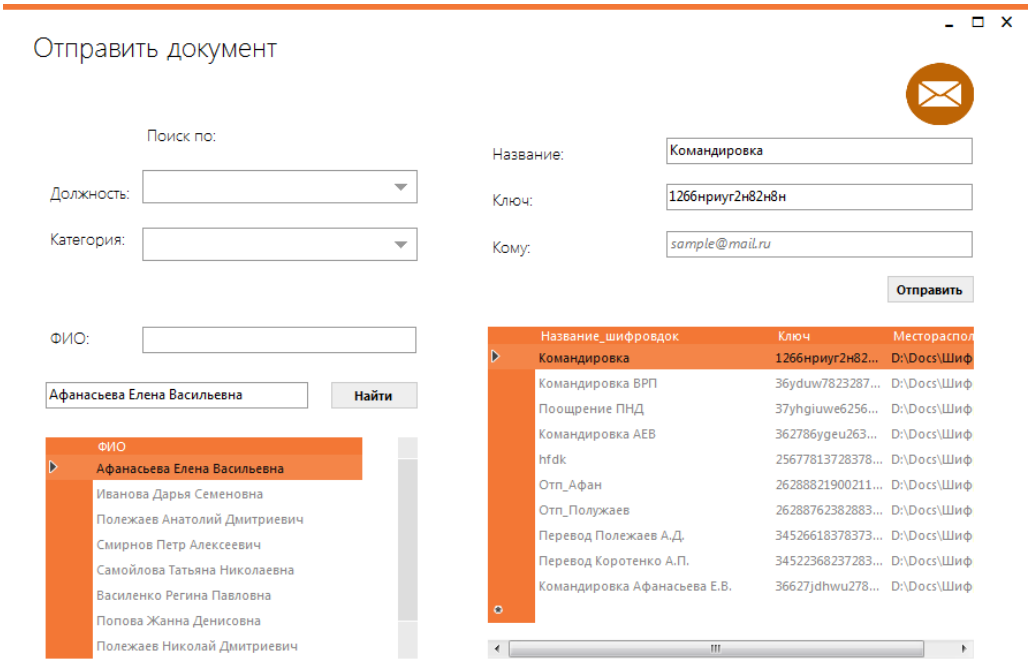


Рисунок 49 – Окно «Отправить документ»

Также можно зашифровать и отправить документ, не хранящийся в БД. Для этого нужно нажать на плитку «Выбрать», после чего откроется окно «Шифрование и отправка документа», представленное на рисунке 50.

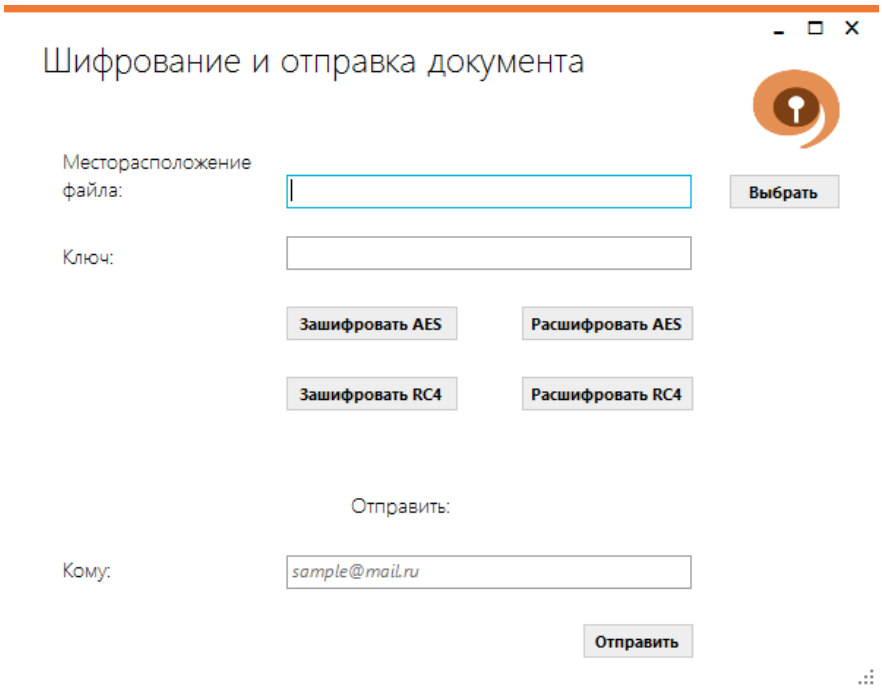


Рисунок 50 – Окно «Шифрование и отправка документа»

Если вход в программу осуществляется под логином и паролем администратора, после окна «Авторизация» открывается окно «Администратор», представленное на рисунке 51. Здесь представлены плитки двух категорий – пользователь и журнал.

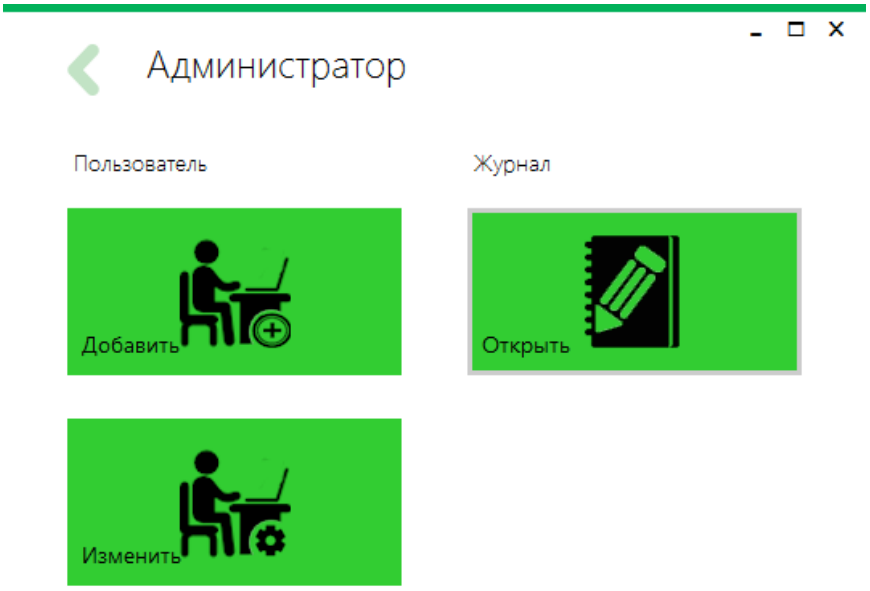


Рисунок 51 – Окно «Администратор»

Выбрав плитку «Добавить» категории пользователь, откроется окно «Регистрация пользователя», изображенное на рисунке 52. Здесь выбирается регистрируемый сотрудник и задается для него логин и пароль.

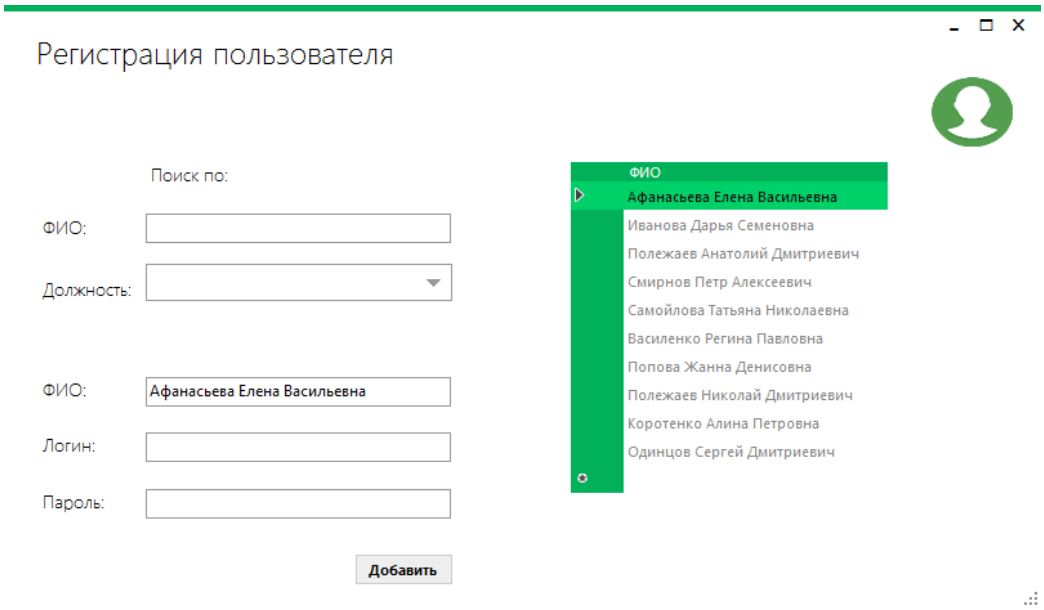


Рисунок 52 – Окно «Регистрация пользователя»

Плитка «Изменить» категории пользователь открывает окно «Изменить данные», представленное на рисунке 53. Здесь можно изменить логин и пароль уже зарегистрированных пользователей.

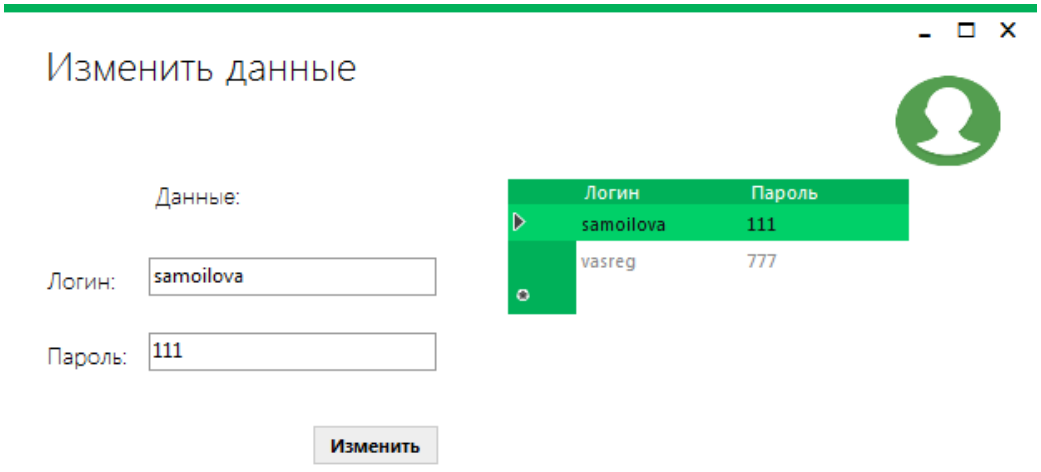


Рисунок 53 – Окно «Изменить данные»

Администратор может просматривать журнал событий, для этого ему необходимо нажать по плитке «Открыть» из категории журнал. Откроется окно «Журнал», представленное на рисунке 54. Администратор может осуществить

поиск событий в журнале по дате, событию, или по ФИО зарегистрированных пользователей.

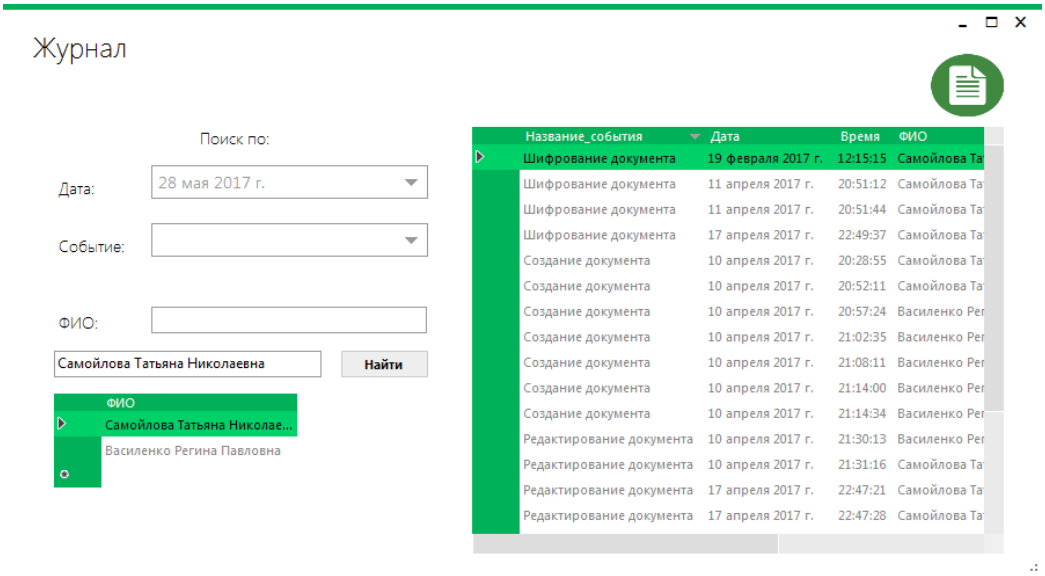


Рисунок 54 – Окно «Журнал»

3.5 Тестирование разработанной подсистемы

Проведем тестирование регистрации нового пользователя, представленное на рисунке 55. При успешном выполнении этой функции появляется сообщение «Пользователь зарегистрирован».

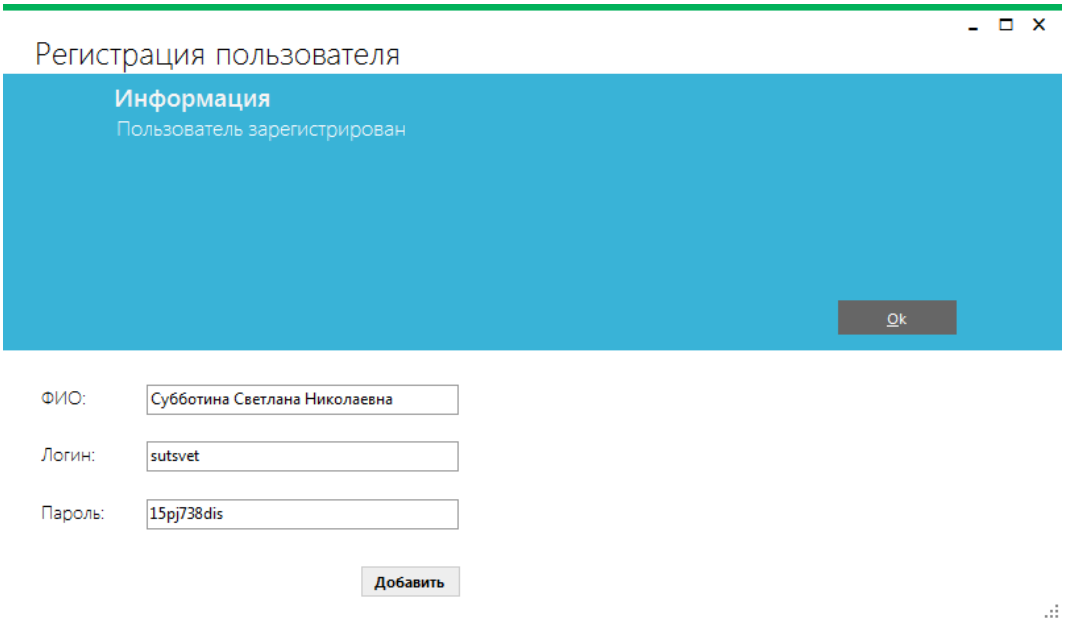


Рисунок 55 – Результат тестирования модуля регистрации пользователя

Тестирование следующих модулей и функций будем производить под этой учетной записью.

Протестируем добавление в БД данных о новом сотруднике. Результат тестирования изображен на рисунке 56. Далее будут создаваться документы для этого пользователя.

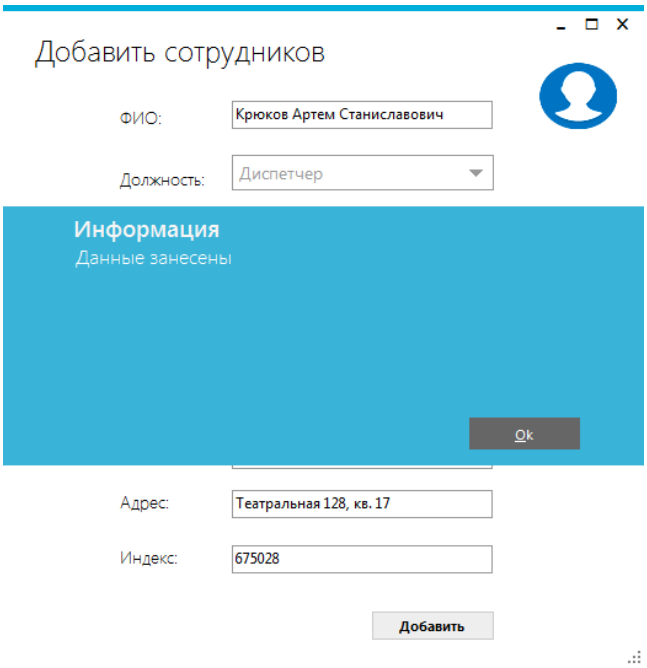
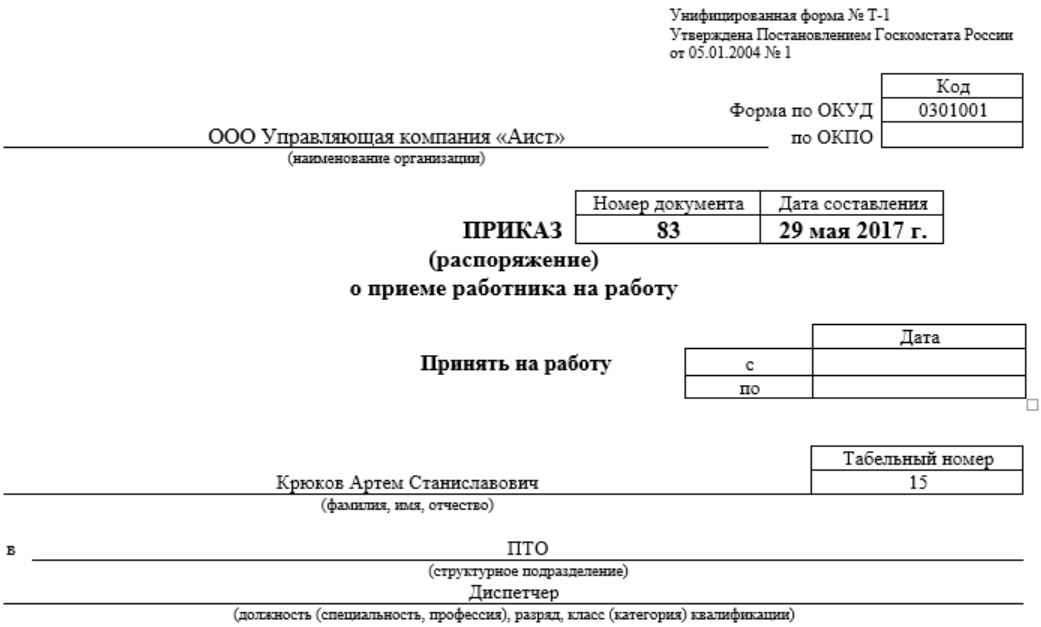


Рисунок 56 – Результат тестирования добавления в БД нового сотрудника

Далее протестируем модуль обработки документов, а именно процесс создание документа. Результат представляет собой документ, изображенный на рисунке 57, с автоматически заполненными полями, которые импортируются из БД. Также подсистема выдает сообщение об успешном занесении данных.



Унифицированная форма № Т-1
Утверждена Постановлением Госкомстата России
от 05.01.2004 № 1

	Код
Форма по ОКУД	0301001
по ОКПО	

ООО Управляющая компания «Аист»
(наименование организации)

Номер документа	Дата составления
83	29 мая 2017 г.

ПРИКАЗ
(распоряжение)
о приеме работника на работу

	Дата
с	
по	

Принять на работу

Табельный номер
15

Крюков Артем Станиславович
(фамилия, имя, отчество)

в ПТО
(структурное подразделение)
Диспетчер
(должность (специальность, профессия), разряд, класс (категория) квалификации)

Рисунок 57 – Результат тестирования модуля обработки документов

При тестировании модуля шифрования документа был получен результат, изображенный на рисунке 58. Подсистема также выдает сообщение об успешном шифровании документов.

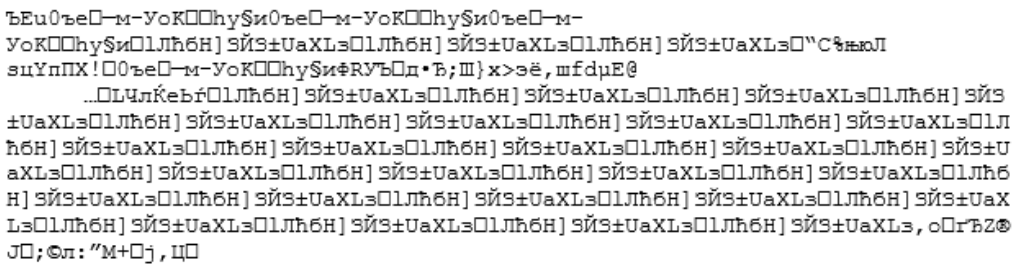


Рисунок 58 – Результат тестирования модуля шифрования документов

Протестируем модуль передачи документов. Подсистема выдает сообщение об успешные передачи данных, а самый главный результат – пришедшее сообщение с шифрованным документом, изображен на рисунке 59.

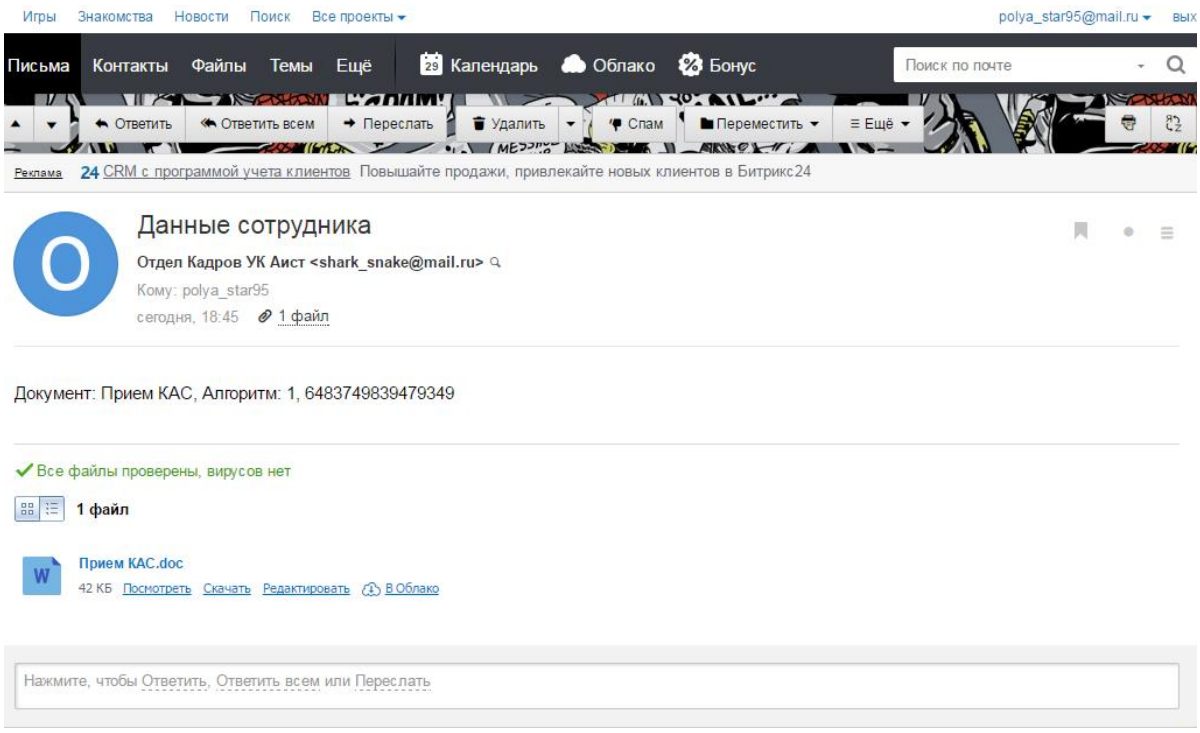


Рисунок 59 – Результат тестирования модуля передачи документов

Результатом тестирования модуля расшифрование является получение исходного документа из зашифрованного. На рисунке 60 представлен результат тестирования в виде сообщения от подсистемы об успешном расшифровании.

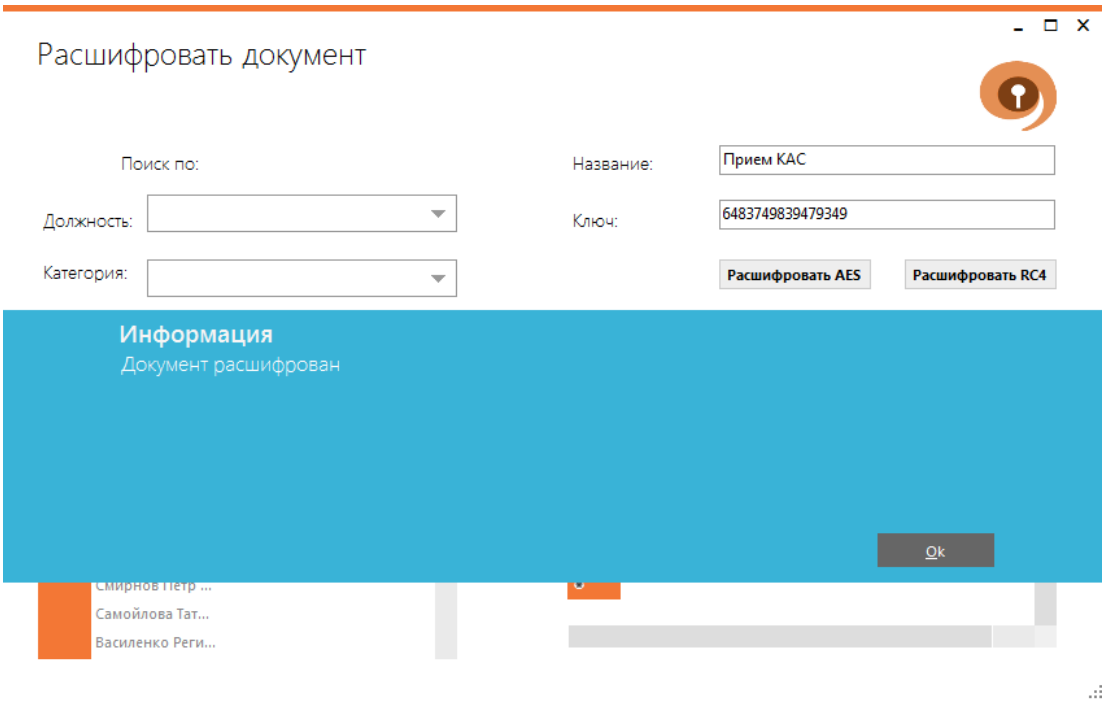


Рисунок 60 – Результат тестирования модуля расшифрования документов

В завершении протестируем модуль ведения журнала события подсистемы, доступный администратору. На рисунке 61 представлен результат тестирования, который отображает все действия, которые были выполнены зарегистрированным в начале пользователем.

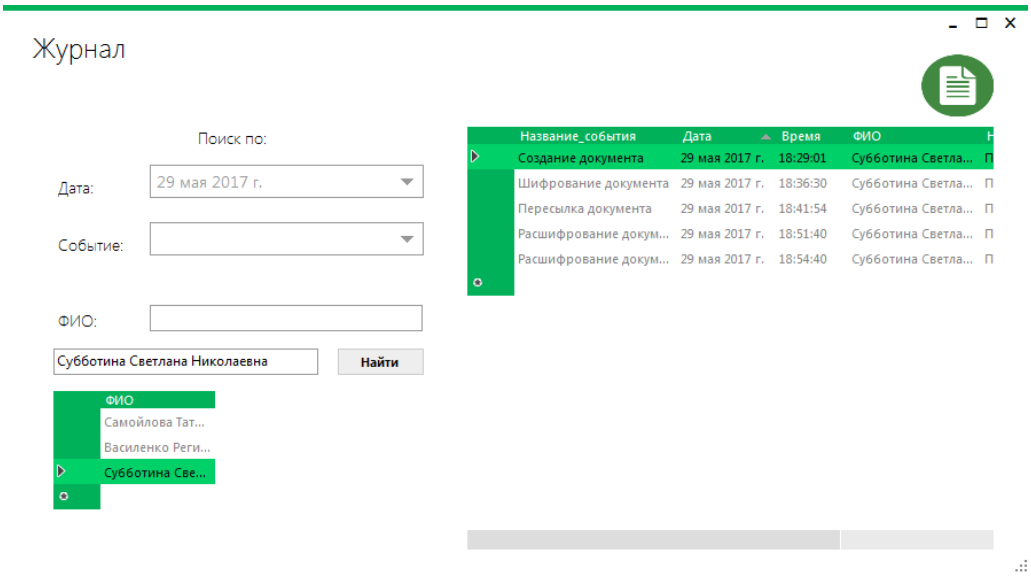


Рисунок 61 – Результат тестирования модуля ведения журнала

4 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

4.1 Исследование информационной безопасности

4.1.1 Описание объекта защиты

Защищаемым объектом в УК «Аист» выбран отдел кадров компании. Этот отдел занимается проведением организационных работ с сотрудниками компании, поиском, наймом и регистрацией новых сотрудников. Отдел кадров заведует личными карточками сотрудников и обрабатывает их персональные данные, а также составляет необходимую документацию, включающую эти данные.

4.1.2 Анализ угроз информационной безопасности отдела кадров

В отделе кадров УК «Аист» согласно теории информационной безопасности, выделяются три типа источников угроз: антропогенные, техногенные и угрозы, обусловленные стихийными источниками, которые являются причиной хищения, модификации, утраты, блокирования, уничтожения информации.

К антропогенным угрозам относятся как нанимаемые сотрудники, так и те, которые уже состоят в штате компании. Нанимаемые сотрудники могут оказаться агентами других управляющих компаний или организаций, которые могут наносить вред компании: внедрять шпионские программы, вирусы, осуществлять сбор конфиденциальной информации, склонить ценных сотрудников к трудоустройству в компанию конкурента или иную организацию. Штатные сотрудники могут осуществлять те же действия по неосторожности или неосведомленности в области информационной безопасности либо злонамеренно из корыстных целей.

К техногенным источникам угроз информации относятся: некачественные технические и программные средства; вспомогательные средства – охраны, сигнализации, телефонии. Так же УК располагается близко к проводам электросети и сети инженерных коммуникаций – водоснабжение, канализации, которые также являются техногенными источниками угроз.

Организациями, которые могут быть источниками антропогенных и техногенных угроз по отношению к УК «Аист», могут оказаться располагаемые

вблизи компании магазин мебели «Rialto» и кафе «Якорь». Эти организации, завладев персональными данными сотрудников, могут начать спам атаки или фишинговые атаки в целях рекламы своей продукции и услуг.

Вероятным стихийным источником, по отношению к защищаемому объекту, является пожар. Отдел кадров оснащен персональными компьютерами и периферийной техникой и оснащен электросетью 220 вольт, что может послужить причиной возникновения возгорания. Следующим по вероятности возникновения является наводнение из-за близкого расположения УК к реке Амур, а также из-за нахождения на 1 этаже. Не исключены и землетрясения, ураганы, наводнения и другие непредвиденные обстоятельства.

4.2 Разработка политики безопасности для отдела кадров управляющей компании «Аист»

4.2.1 Организационный уровень защиты информационной безопасности

Организационные мероприятия для отдела кадров управляющей компании «Аист» должны включать в себя следующие требования безопасности:

а) проверка принимаемых в компанию работников и ознакомление их под роспись с мерами ответственности за нарушение правил защиты информации;

б) ограничение доступа к модулям, которые исполняются и несут важную информацию;

в) осуществление доступности обрабатываемой информации пользователям системы, которые работают с необходимой им информацией в соответствии с разграничением доступа, за приемлемое время;

г) проведение сертификации и тестирования программных средств и помещения отдела кадров УК;

д) ведение журналов выдачи и использования документов, которые содержат информацию, подлежащую защите, с датой выдачи, с фамилией, именем, отчеством выдавшим, кому выдали и их подписями;

е) ведение журналов отправки документов с автоматизированного рабочего места, которые содержат информацию, подлежащую защите, с датой отправки, с фамилией, именем, отчеством отправившим и адресатом кому отправили;

ж) осуществлять проверки автоматизированных рабочих мест сотрудников на наличие не лицензированного и стороннего ПО;

к) устанавливать на каждом автоматизированном рабочем месте только закупленные лицензированные программы;

л) обеспечить на каждом автоматизированном рабочем месте идентификацию и аутентификацию сотрудника;

м) создание резервных копий важной информации;

н) архивирование информации;

п) хранение отдельных файлов в шифрованном виде;

р) тщательное уничтожение мусора организации.

А также включать следующие запреты:

а) устанавливать не лицензированное ПО;

б) устанавливать стороннее ПО;

в) предоставлять персональные данные сторонним лицам.

Немаловажным является соблюдение морально-этических мероприятий, включающие в себя следующие требования безопасности, которым должны следовать сотрудники:

а) быть ответственным при работе с документами компании;

б) соблюдать профессиональную этику;

в) не совершать действий, направленных на нарушение нормальной работы компьютерных систем;

г) не совершать действий, вызывающих дополнительные неоправданные затраты ресурсов – памяти, машинного времени;

д) управляющим необходимо быть внимательными к сотрудникам и предотвращать конфликтные ситуаций во избежание появления недовольных, обиженных сотрудников.

4.2.2 Законодательный уровень защиты информации

Основанием для выбранного объекта защиты – персональных данных – послужил Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных», согласно которому персональные данные необходимо обезличивать, что было достигнуто в разработанной подсистеме криптографической защиты персональных данных в системе электронного документооборота отдела кадров компании путем шифрования документов с персональными данных сотрудников. Более подробно законодательные мероприятия рассмотрены в главе 2 пункт 2.3.6.

4.2.3 Программные уровень защиты информации

Разработанная подсистема криптографической защиты персональных данных в системе электронного документооборота обеспечивает защиту доку-ментов с персональными данными от нарушителей первого уровня, которые описаны в главе 2 пункт 2.1. Также на ряду с этой подсистемой для предотвращения заражения компьютеров отдела кадров вирусными программами необходимо установить на каждом автоматизированном рабочем месте закупленные лицензированные антивирусные программы и настроить автоматическое ежедневное обновление антивирусных баз данных.

Требуется закупить, установить и настроить лицензированный межсетевой экран, чтобы предотвратить несанкционированный доступ к информации, контролируя, фильтруя трафик сети.

Необходимо установить программу, ограничивающую доступ к файловой системе и документам. Также рекомендуется использовать созданную подсистему криптографической защиты персональных данных в электронном документообороте на базе отдела кадров компании при передаче документов по сети.

4.2.4 Технический уровень защиты информации

Все оборудование и провода должны быть экранированы во избежание снятия с них информации посторонними лицами техническими средствами. Также допускается установка генераторов шума на цепи электропитания и на сети инженерной коммуникации.

4.3 Выбор модели управления доступом

Для отдела кадров УК «Аист» была выбрана ролевая модель управления доступом. Данная модель максимально приближена к реальному разделению функций персонала и логике работы компании. Она включает в себя: администрирование, иерархию ролей, принцип наименьшей привилегии, разделение обязанностей. Администрирование в ролевой модели управления доступа представляет собой назначение и удаление ролей пользователей, что наделяет их привилегиями либо ограничивает в них. Иерархия ролей – множество на котором задано отношение наследования привилегий. Иными словами, каждая роль может наследовать привилегии других ролей, что значительно упрощает администрирование. Согласно принципу наименьшей привилегии, требуется организовать доступ пользователя к информации и ресурсам, которые минимально необходимы для успешного выполнения его рабочей цели. Важной составляющей ролевой модели управления доступом является разделение обязанностей, которое может быть статическое и динамическое. Статическое разделение обязанностей назначает ограничения на добавление пользователям ролей, а динамическое разделение обязанностей возлагает ограничения на одновременно активные роли, тем самым уменьшая количество привилегий. Определение роли и привилегий пользователя, которые необходимы ему для выполнения задачи, происходит в момент активизации сессии.

Схема ролевой модели управления доступа представлена на рисунке 62, согласно которой был реализован доступ в разработанной подсистеме. В качестве администратора выступает начальник отдела кадров, у которого есть права на регистрацию новых пользователей подсистемы, просмотр журнала событий и управление доступом. Специалистам по кадрам предоставляются права на обработку документов и манипуляции с ними.

Рисунок 62 – Схема ролевой модели управления доступа

5 БЕЗОПАСНОСТЬ И ЭКОЛОГИЧНОСТЬ

5.1 Безопасность

Помещение отдела кадров управляющей компании «Аист» соответствует действующему САНПИН 2.2.2/2.4.1340-03, для предотвращения воздействия неблагоприятных факторов на здоровье человека в процессе работы с ПЭВМ. Данное помещение содержит окно, оборудованное регулируемыми жалюзи и два рабочих места с ПЭВМ. Ширина рабочего стола пользователя ПЭВМ составляет 1,3 м, глубина – 0,55 м, высота рабочего – 0,72 м. Расстояние от глаз пользователя и монитора составляет 0,65 м. Рабочие стулья регулируются по высоте, с полумягкой спинкой, с шириной и глубиной сиденья 0,5 м. Расстояние между рабочими столами с ПЭВМ составляет 2 м. Рабочие места с ПЭВМ расположены так, что естественный свет падает слева, а также вдали от силовых кабелей, трансформаторов и другого, создающего помехи в работе ПЭВМ, оборудования. В помещении ежедневно проводится влажная уборка и систематическое проветривание. Таким образом планировка помещения отдела кадров управляющей компании «Аист» имеет вид, представленный на рисунке 63.

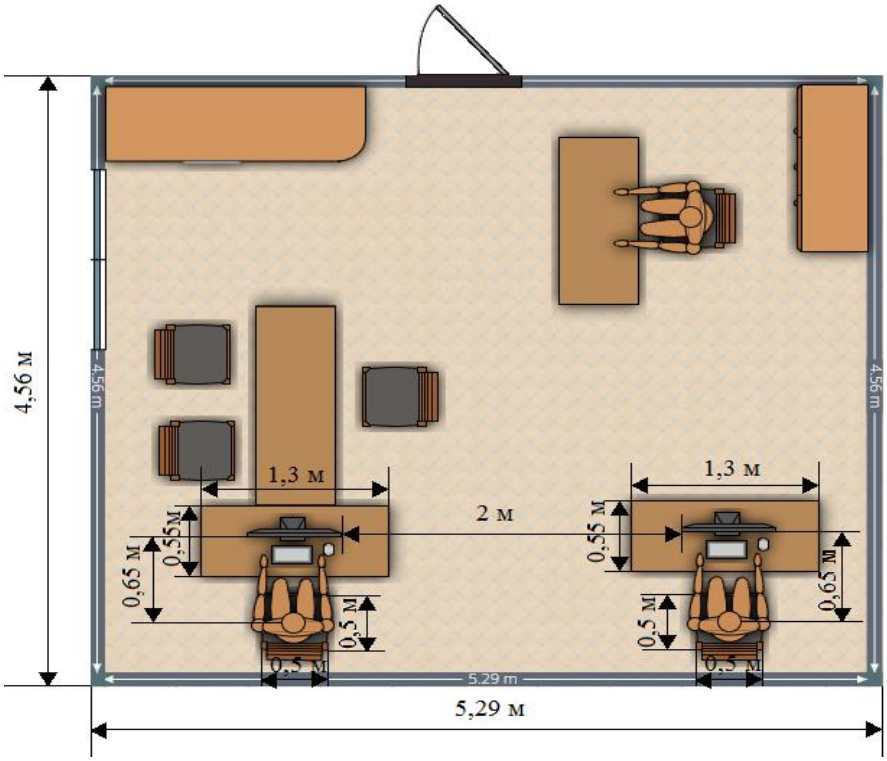


Рисунок 63 – Планировка помещения отдела кадров УК «Аист»

Нужно следить за чистотой окон и светильников и проводить их чистку не реже двух раз в год. Освещение поверхности экрана ПЭВМ не должно превышать 300 лк, а освещение поверхности стола при работе с документами находиться в диапазоне 300 – 500 лк и не создает блики на экране ПЭВМ.

Необходимо рабочие места с ПЭВМ оборудовать дополнительным заземлением для снижения напряжения прикосновения, обеспечивающее электробезопасность. Также должны соблюдаться следующие требования к параметрам электромагнитных полей на рабочих местах с ПЭВМ:

а) напряженность электрического поля в частотном диапазоне 5 Гц – 2 кГц не должен превышать 25 В/м, в диапазоне 2 кГц – 400 кГц – не более 2,5 В/м;

б) индукция магнитного поля в частотном диапазоне 5 Гц – 2 кГц должен быть не более 250 нТл, в диапазоне 2 кГц – 400 кГц – не превышать 25 нТл;

в) напряженность электростатического поля не более 15 кВ/м;

г) фоновый уровень напряженности электрического поля промышленной частоты при 50 Гц не более 500 В/м;

д) фоновый уровень индукции магнитного поля промышленной частоты при 50 Гц не более 5 мкТл.

Интерфейс разработанной программы выполнен в тонах, приятных для глаз и представляет собой набор окон, отвечающие за выполнение конкретных функций. Дизайн разрабатывался в стиле оформления Windows Metro, представляющий собой плитки, нажатие на которые открывает соответствующее окно. После прохождения авторизации с правами пользователя откроется окно «Главная», представленное на рисунке 64. На белом фоне по категориям располагаются голубые и оранжевая, выделяющая модуль шифрования. Каждая плитка также содержит графическое изображение выполняемой функции.

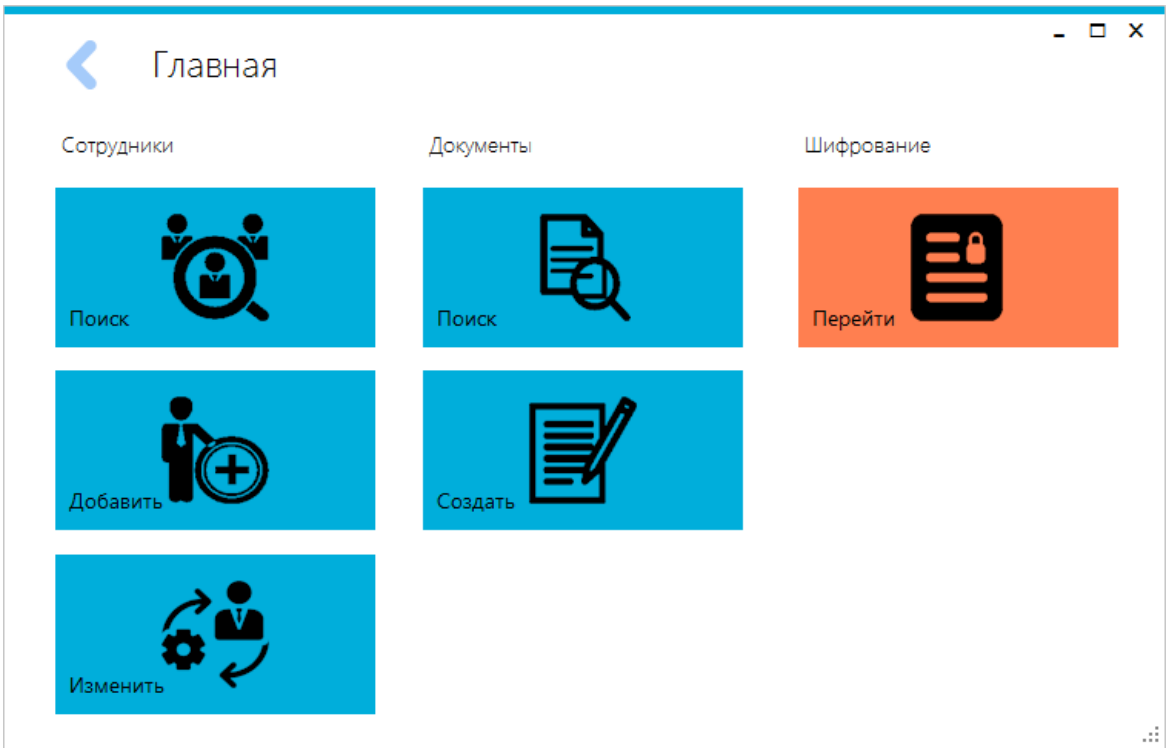


Рисунок 64 – Окно «Главная»

В программе предусмотрены диалоговые окна, сообщающие пользователем ошибки при выполнении задач или успешность выполнения задач. Сообщение об удачном выполнении задачи с заголовком «Информация» предоставляется на голубом фоне и изображено на рисунке 65.

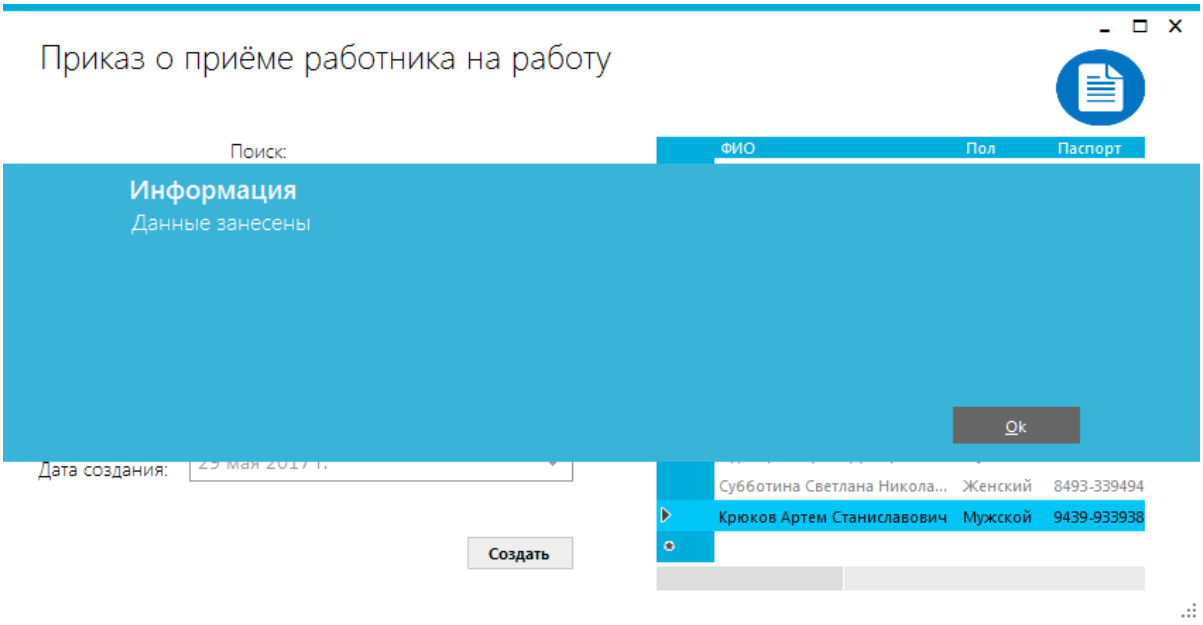


Рисунок 65 – Сообщение об удачном выполнении задачи

Сообщение об ошибке с заголовком «Ошибка» предоставляется на красном фоне и изображено на рисунке 66.

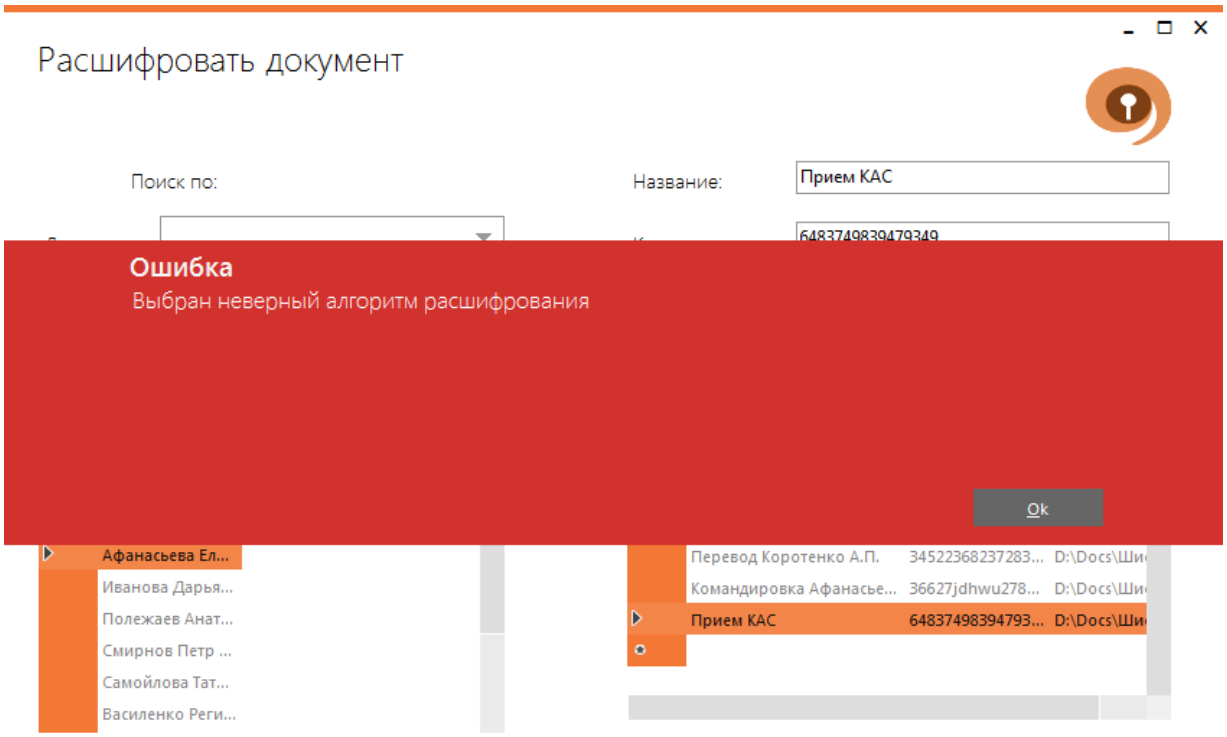


Рисунок 66 – Сообщение об ошибке

Окно администратора представляет собой набор плиток по категориям с графическим изображением функции только зеленого цвета, расположенные также на белом фоне. Окно администратора изображено на рисунке 67.

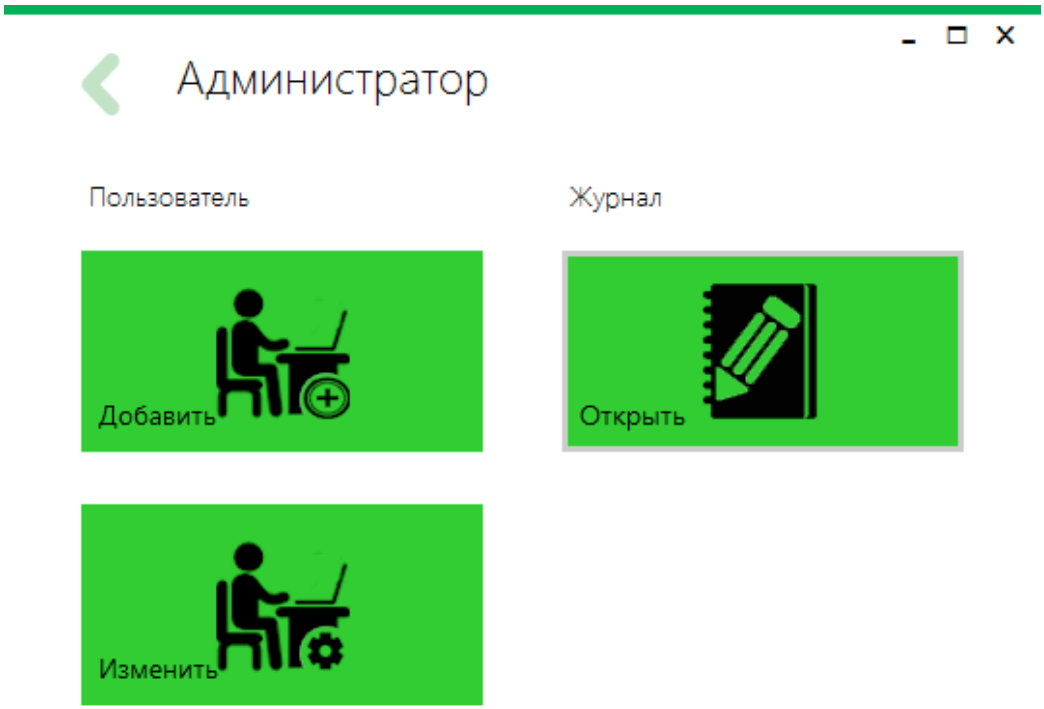


Рисунок 67 – Окно «Администратор»

Для пользователей со слабым зрением предусмотрены пиктограммы, которые отображают функции, выполняемые с документами и базой данных. Выбранные строки в таблицах подсвечиваются синим, оранжевым или зеленым цветом в зависимости от окна работы и изменяют цвет шрифта на яркий. Также семейство операционных систем Windows на которой работает разработанный программный продукт содержит утилиту «Экранная лупа», которая позволяет в соответствии с заданными настройками масштаба увеличивать весь экран либо выбранную область экрана. С помощью утилиты «Экранный диктор» пользователь может прослушать документ, который создал с помощью программы.

5.2. Экологичность

Основными отходами отдела кадров УК «Аист» являются макулатура, компьютеры, магнитные носители и периферийные устройства. В соответствии с ФЗ № 89 «Об отходах производства и потребления» от 24.06.1998 запрещается заниматься самостоятельной утилизацией отходов. Ненужную бумагу необходимо собирать в служебном помещении, предварительно измельчив шредером секретные документы. Затем собранную макулатуру нужно передать в пункт приема макулатуры в Благовещенске – ОАО «Вторресурсы». Ни в коем случае нельзя самостоятельно сжигать и закапывать бумагу.

Для утилизации вышедших из строя и не подлежащих ремонту компьютеров, магнитных носителей и периферийных устройств – принтеры, сканеры, мониторы, клавиатуры, оптические мыши – также необходимо обратиться в соответствующую организацию. Одна из компаний в Благовещенске, занимающейся утилизацией компьютеров, магнитных носителей и периферийной техники – ООО «Радиолом».

5.3 Чрезвычайные ситуации

Велика вероятность возникновение пожара в помещении отдела кадров УК «Аист». Данное помещение оборудовано датчиком пожарной сигнализации – детектором дыма, размещенным на потолке посередине комнаты. Также в этом помещении есть порошковый огнетушитель, подходящий для тушения возгорания

на участке цепи с напряжением до 1000 В. Проверка датчика пожарной сигнализации и порошкового огнетушителя должна проводиться не менее двух раз в год ответственными представителями проверяющей организации.

В случае возникновения возгорания необходимо не поддаваться панике и немедленно покинуть помещение и соответствовать общему плану пожарной безопасности УК «Аист». Плотно закрыть дверь отдела и сообщить работникам других отделов о возгорании и немедленной эвакуации здания. Вызвать пожарную охрану по номеру «01» или по сотовому телефону «112». Не рекомендуется тушить пожар самостоятельно, можно использовать огнетушитель только в случае небольшого возгорания на начальной стадии. Ни в коем случае нельзя использовать огнетушитель для тушения одежды на человеке. В этом случае необходимо не позволять горящему человеку бежать, повалить его на землю, закутать в одеяло и обильно полить его водой.

ЗАКЛЮЧЕНИЕ

В ходе выполнения выпускной квалификационной работы был проведен анализ и исследование деятельности управляющей компании «Аист» и были сформулированы цели и поставлены задачи в области управления документами в отделе кадров компании, а также рассмотрены существующие системы электронного документооборота и применение криптографических средств защиты информации.

В работе обоснована необходимость создания подсистемы криптографической защиты документов в отделе кадров УК «Аист». Спроектирована система документооборота и программное обеспечение для информационной системы документооборота для отдела кадров управляющей компании «Аист» с криптографической подсистемой защиты, обеспечивающей шифрование и расшифрование документов. Разработаны функциональные подсистемы, модули и база данных документационного обеспечения отдела кадров, составляющие программный продукт. Создана подсистема криптографической защиты персональных данных в электронном документообороте, которая была успешно протестирована. Разработано руководство пользователей для работы с созданной подсистемы, а также политика информационной безопасности на уровне отдела кадров управляющей компании «Аист». Результаты работы были апробированы на научной конференции «Молодежь XXI века: Шаг в будущее», где были представлены тезисы разрабатываемой подсистемы криптографической защиты персональных данных в электронном документообороте. Была опубликована статья в электронном научном издании «Ученые заметки ТОГУ», в которой рассмотрено применение параллельных вычислений в современных методах криптоанализа. Отдельные результаты, представленные в акте о внедрении, применяются в УК «Аист».

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1 Барихин, А. Б. Делопроизводство и документооборот / А. Б. Барихин. – М.: Книжный мир, 2014. – 416 с.

2 Бирюков, А. А. Информационная безопасность: защита и нападение / А. А. Бирюков. – М.: ДМК Пресс, 2013. – 474 с.

3 Быкова, Т.А. Документационное обеспечение управления (делопроизводство): Учебное пособие / Т. А. Быкова, Т. В. Кузнецова, Л. В. Санкина. – 2-е изд. – М.: Инфра-М, 2012. – 304 с.

4 Варфоломеева, А. О. Информационные системы предприятия: Учебное пособие / А. О. Варфоломеева, А. В. Коряковский, В. П. Романов. – М.: НИЦ ИНФРА-М, 2013. – 283 с.

5 Васильков, А. В. Информационные системы и их безопасность: Учебное пособие / А. В. Васильков, А. А. Васильков, И. А. Васильков. – М.: Форум, 2013. – 528 с.

6 Государственная информационная система жилищно-коммунального хозяйства [Электронный ресурс]: офиц. сайт. – 1.07.2016 – Режим доступа: https://dom.gosuslugi.ru/#!/regulations?rubricCode=18.

7 Графкина, М.В. Охрана труда и производственная безопасность: учебное пособие / М.В. Графкина — М.: ТК Велби, Изд-во Проспект, 2007. — 424 с.

8 Гринберг, А. С. Информационные технологии управления: учебное пособие / А. С. Гринберг, Н. Н. Горбачев, А. С. Бондаренко. – М.: Юнити-Дана, 2015. – 479 с.

9 Даниленко, А. Ю. Безопасность систем электронного документооборота. Технология защиты электронных документов / А. Ю. Даниленко. – М.: Ленанд, 2015. – 232 с.

10 Емельянова, Н. З. Проектирование информационных систем: Учебное пособие / Н. З. Емельянова, Т. Л. Партыка, И. И. Попов. – М.: Форум, 2013. – 432 с.

11 Зазулинский, В.Д. Безопасность жизнедеятельности: учебное пособие / В.Д. Зазулинский. — М.: Экзамен, 2014. – 256 с.

12 Киреенко, А. Е. Современные проблемы в области информационной безопасности: классические угрозы, методы и средства их предотвращения: учебное пособие / А. Е. Киреенко. – М.: Молодой ученый, 2012. – №3. – 337–501 с.

13 Кириллов, В. В. Введение в реляционные базы данных. Введение в реляционные базы данных / В. В. Кириллов, Г. Ю. Громов. - СПб.: БХВ-Петербург, 2012. - 464 с.

14 Маклаков, С. В. Моделирование бизнес-процессов с BPwin 4.0. / С. В. Маклаков. – М.: ДИАЛОГ-МИФИ, 2013. – 224 с.

15 О введении в действие санитарно-эпидемиологических правил и нормативов САНПИН 2.2.2/2.4.1340-03 [Электронный ресурс]: Постановление Министерства здравоохранения РФ от 3 июня 2003 г. N 118. Доступ из справ.-правовой системы «Гарант».

16 Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности [Электронный ресурс]: Приказ Федеральной службы безопасности Российской Федерации от 10 июля 2014 г. № 378. Доступ из справ.-правовой системы «Гарант».

17 Об утверждении Порядка проведения классификации информационных систем персональных данных [Электронный ресурс]: Приказ Федеральной службы по техническому и экспортному контролю Федеральной службы безопасности Российской Федерации Министерства информационных технологий и связи Российской Федерации от 13 февраля 2008 г. № 55/86/20. Доступ из справ.-правовой системы «Гарант».

18 Питулина, П. И. Разработка подсистемы криптографической защиты персональных данных в электронном документообороте / П. И. Питулина // Молодёжь XXI века: шаг в будущее : материалы XVIII региональной научно-практической конф. (18 мая 2017 года) – Благовещенск: Изд-во БГПУ, 2017. – 1335 с.

19 Семенихин, В. В. Кадровый документооборот / В. В. Семенихин. – М.: Эксмо, 2014. – 384 с.

20 Семичевская, Н. П. Применение параллельных вычислений в современных методах криптоанализа [Электронный ресурс] / Н.П. Семичевская, Л. А. Соловцова, П. И. Питулина // Электронное научное издание «Ученые заметки ТОГУ» – Хабаровск, 2016. – Режим доступа: http://pnu.edu.ru/media/ejournal/articles-2016/TGU_7_194.pdf

21 Советов, Б. Я. Базы данных: теория и практика: Учебник для бакалавров / Б. Я. Советов, В. В. Цехановский, В. Д. Чертовской. – М.: Юрайт, 2013. – 463 с.

22 Уголовный кодекс Российской Федерации: принят Гос. думой 24 мая 1996 г.: одобр. Советом Федерации 5 июня 1996 г. (Официальный интернет-портал правовой информации www.pravo.gov.ru)

23 Федеральный закон РФ от 24.06.1998 № 89-ФЗ «Об отходах производства и потребления» (Официальный интернет-портал правовой информации www.pravo.gov.ru)

24 Федеральный закон Российской Федерации от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации» (Официальный интернет-портал правовой информации www.pravo.gov.ru)

25 Федеральный закон РФ от 27 июля 2006 года № 152-ФЗ «О персональных данных» (Официальный интернет-портал правовой информации www.pravo.gov.ru)

26 Шихаб, Д. Т. Реализация алгоритма RC4 на CBuilder / Д. Т. Шихаб, Л.Т. Рашид // Молодой ученый. – 2014. – №8. – С. 60-67.

27 Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. – М.: ДМК, 2014. – 702 с.

ПРИЛОЖЕНИЕ А

Линейно-штабная организационная структура УК «Аист»

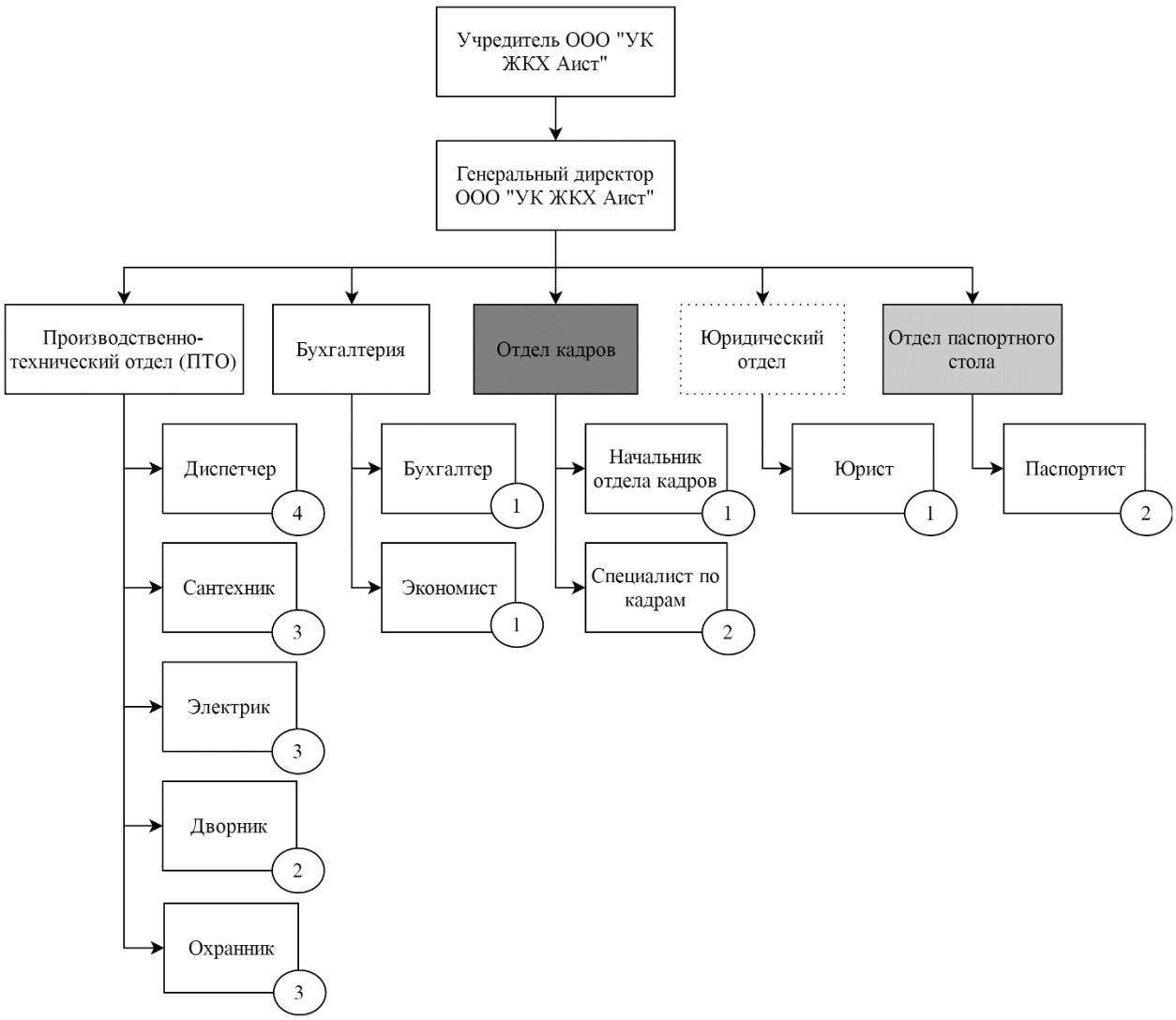


Рисунок А.1 – Линейно-штабная организационная структура компании

ПРИЛОЖЕНИЕ Б

Функциональная диаграмма УК «Аист»

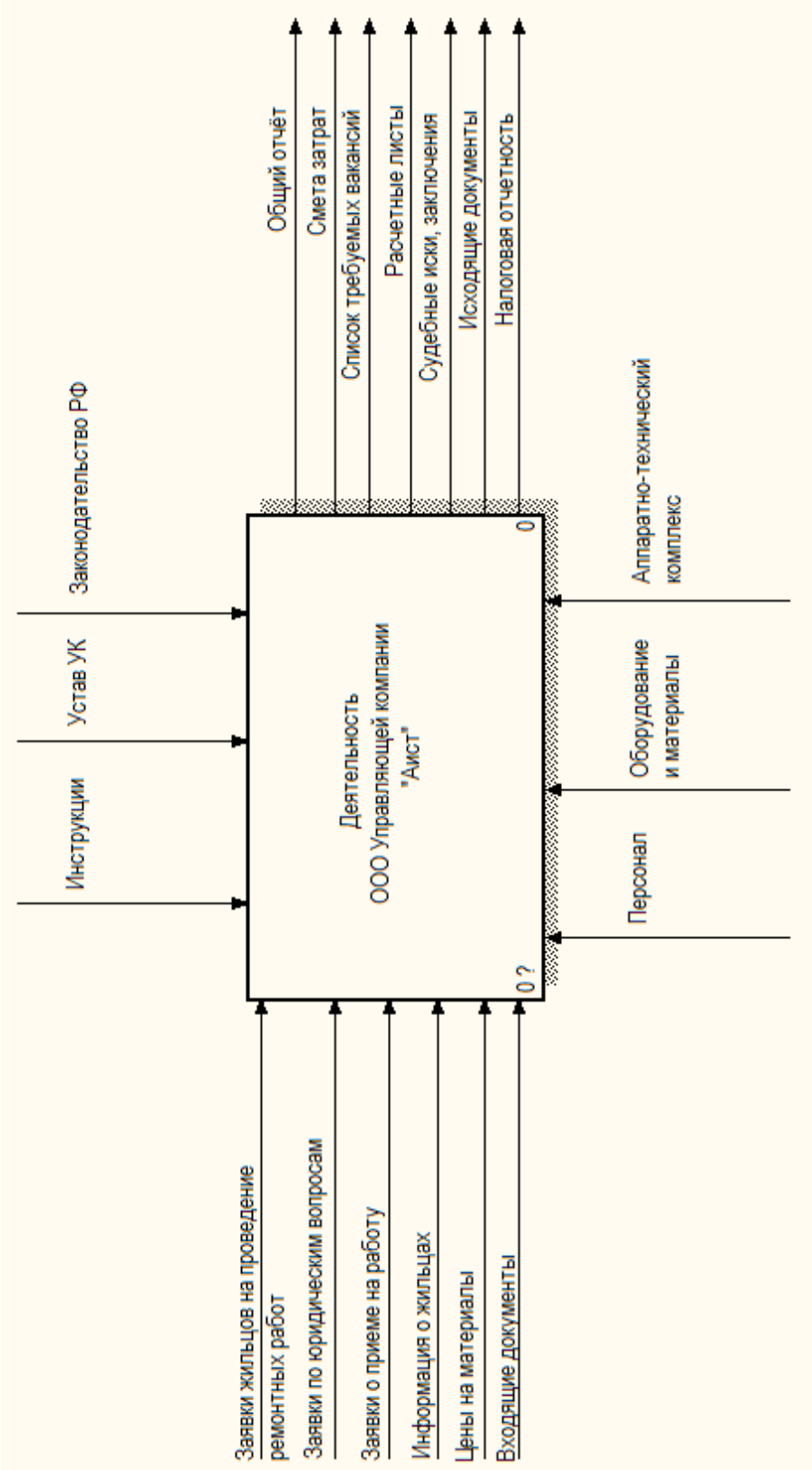


Рисунок Б.1 – Контекстная диаграмма

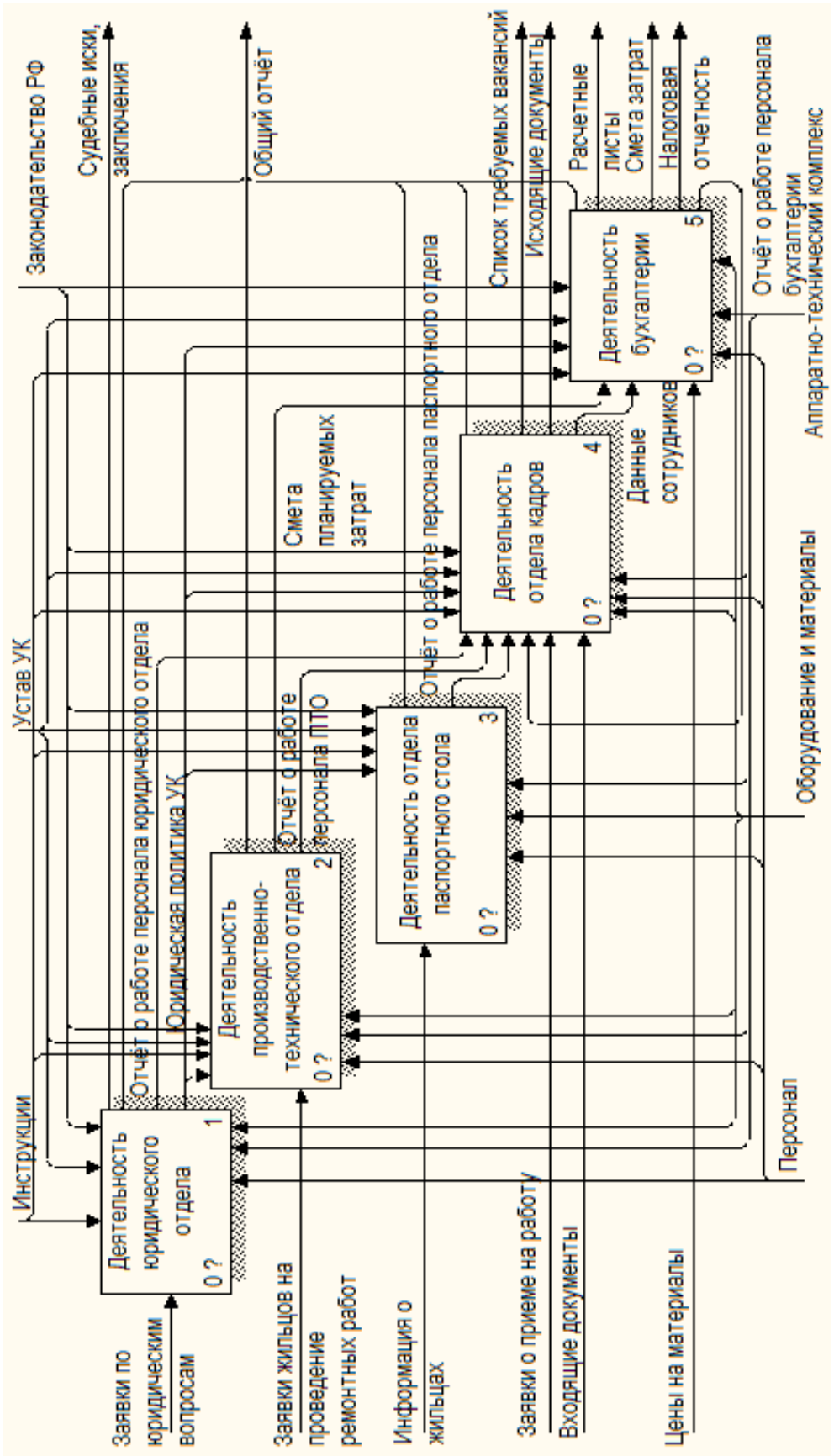


Рисунок Б.2 – Декомпозиция контекстной диаграммы

ПРИЛОЖЕНИЕ В

Документооборот отдела кадров УК «Аист»

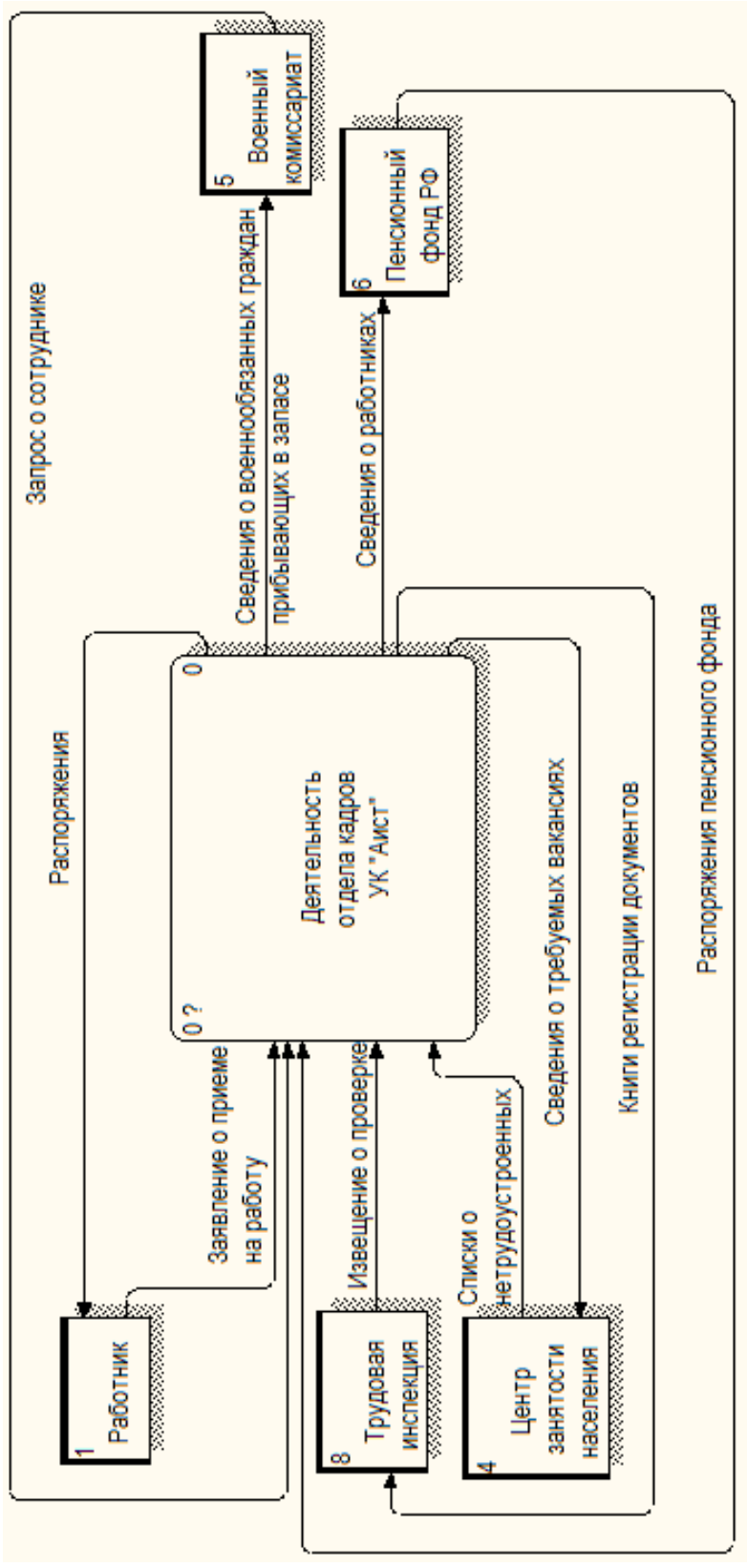


Рисунок В.1 – Внешний документооборот

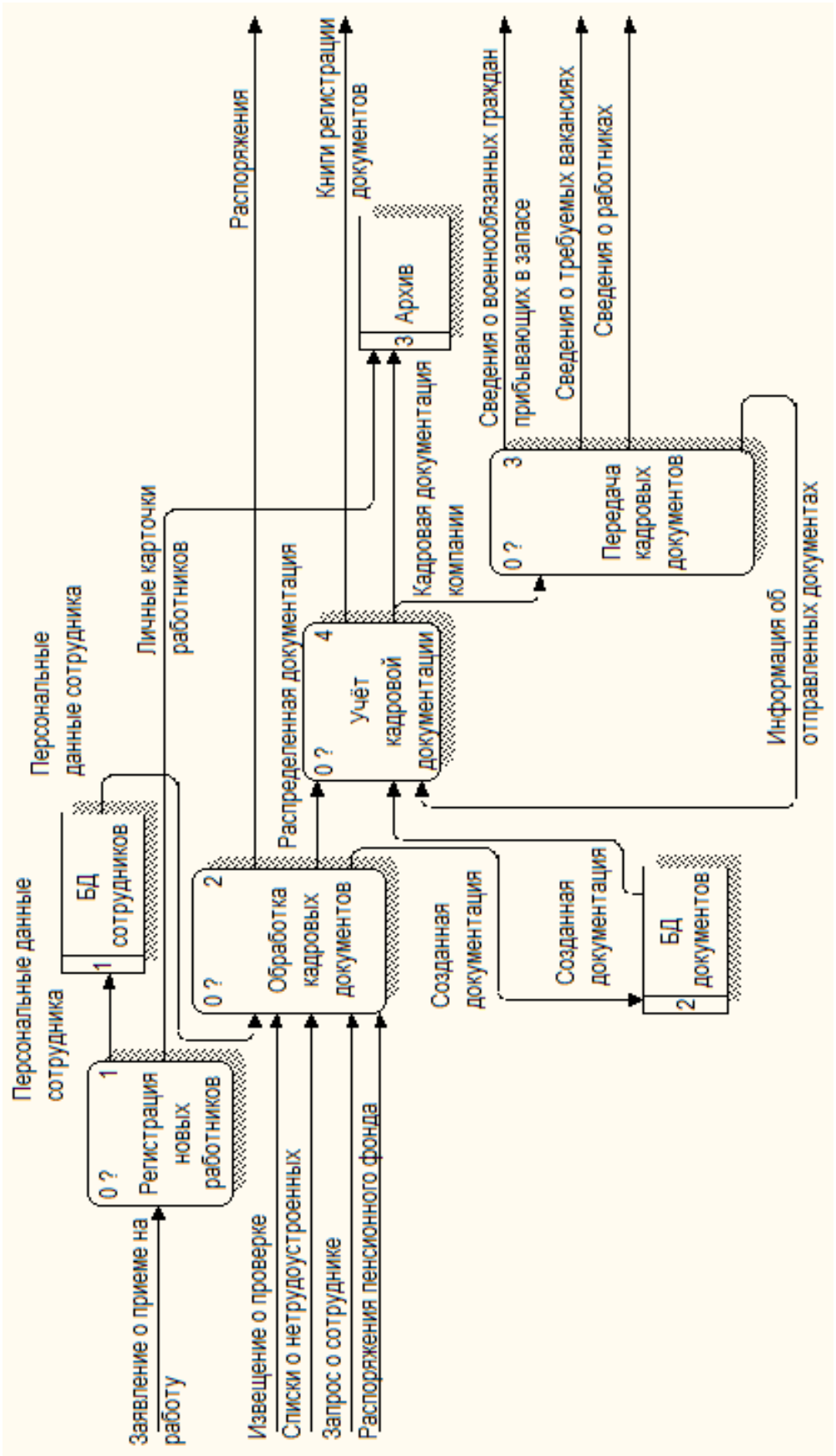


Рисунок В.2 – Внутренний документооборот

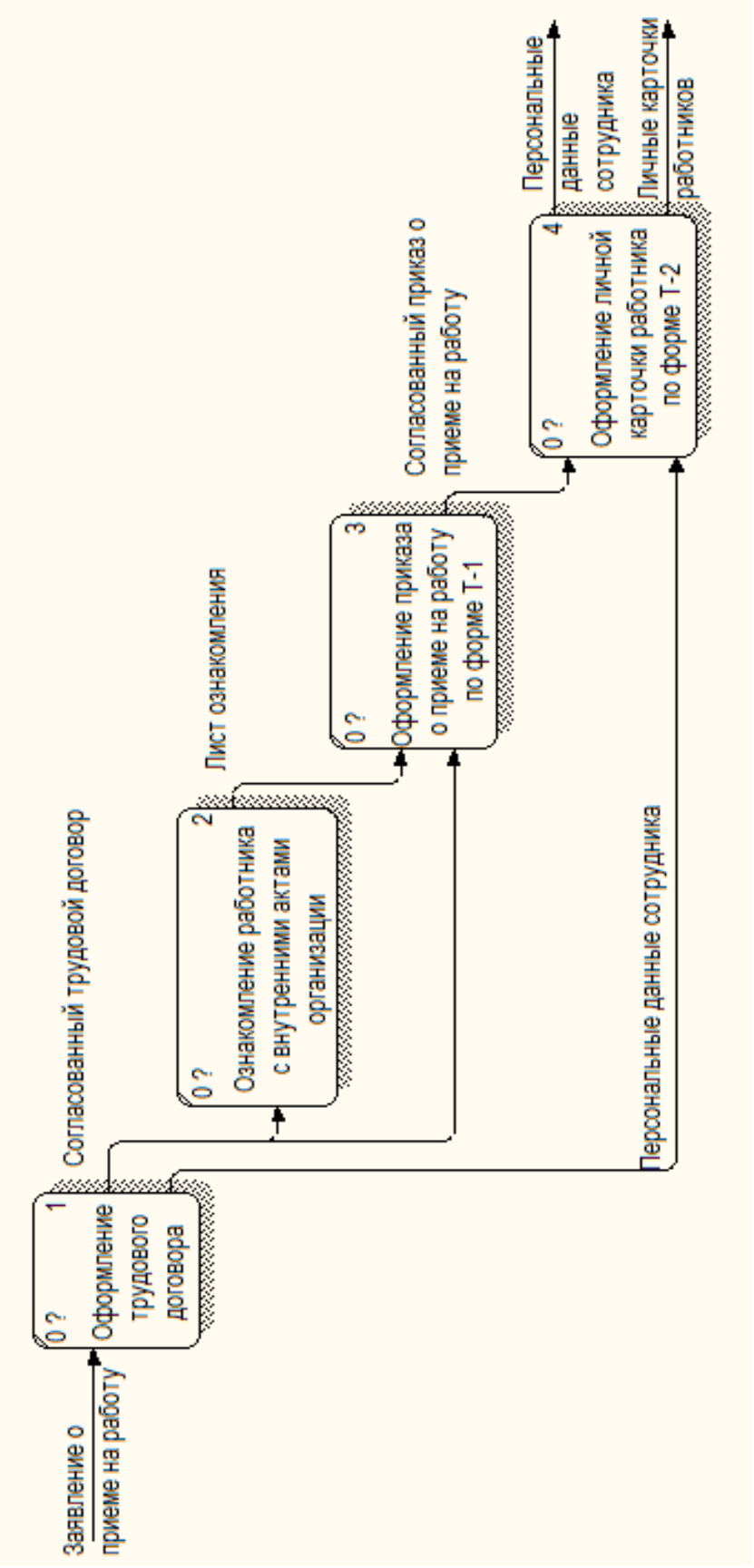


Рисунок В.3 – Декомпозиция процесса регистрации новых работников

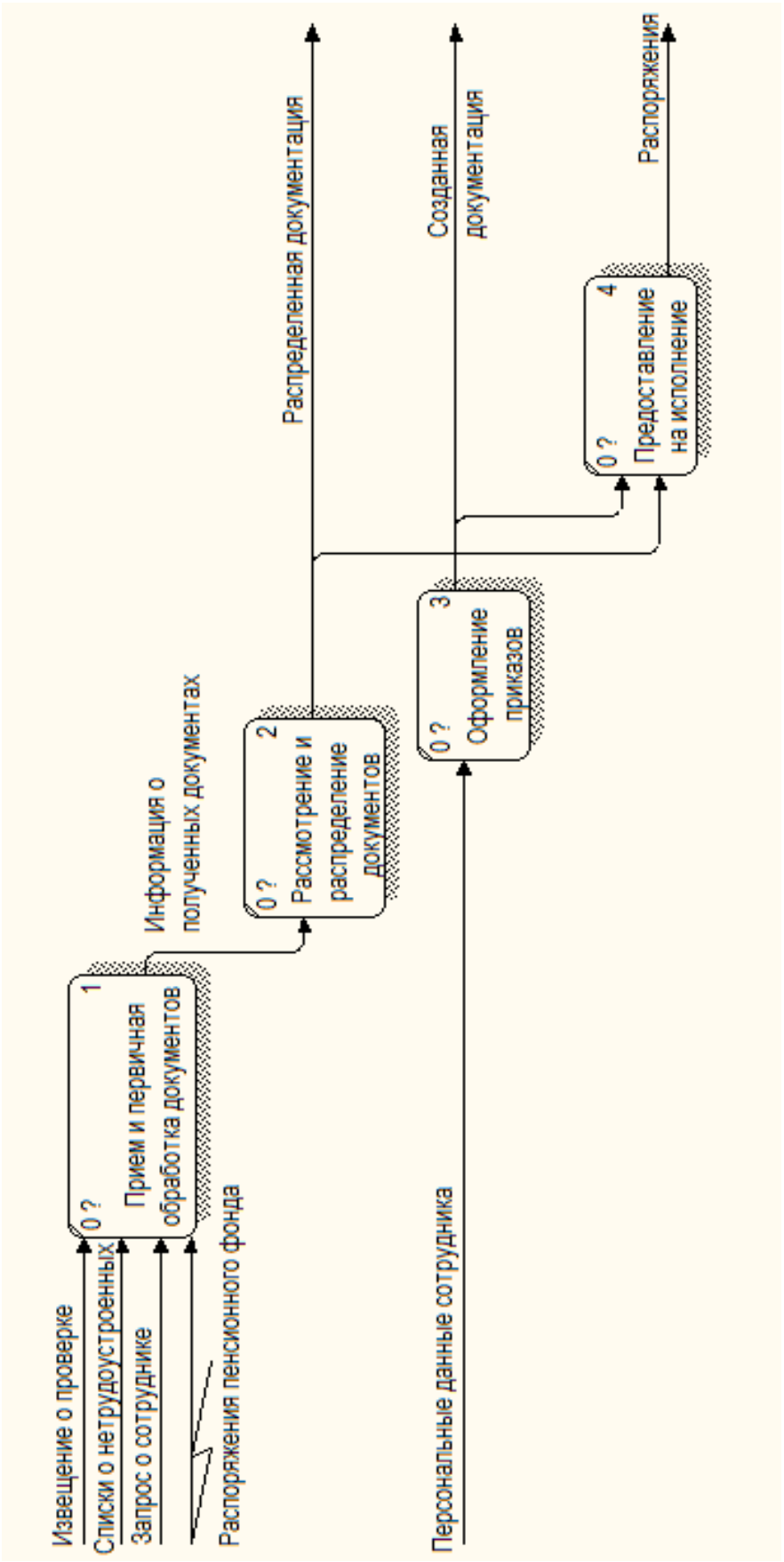


Рисунок В.4 – Декомпозиция процесса обработки кадровых документов

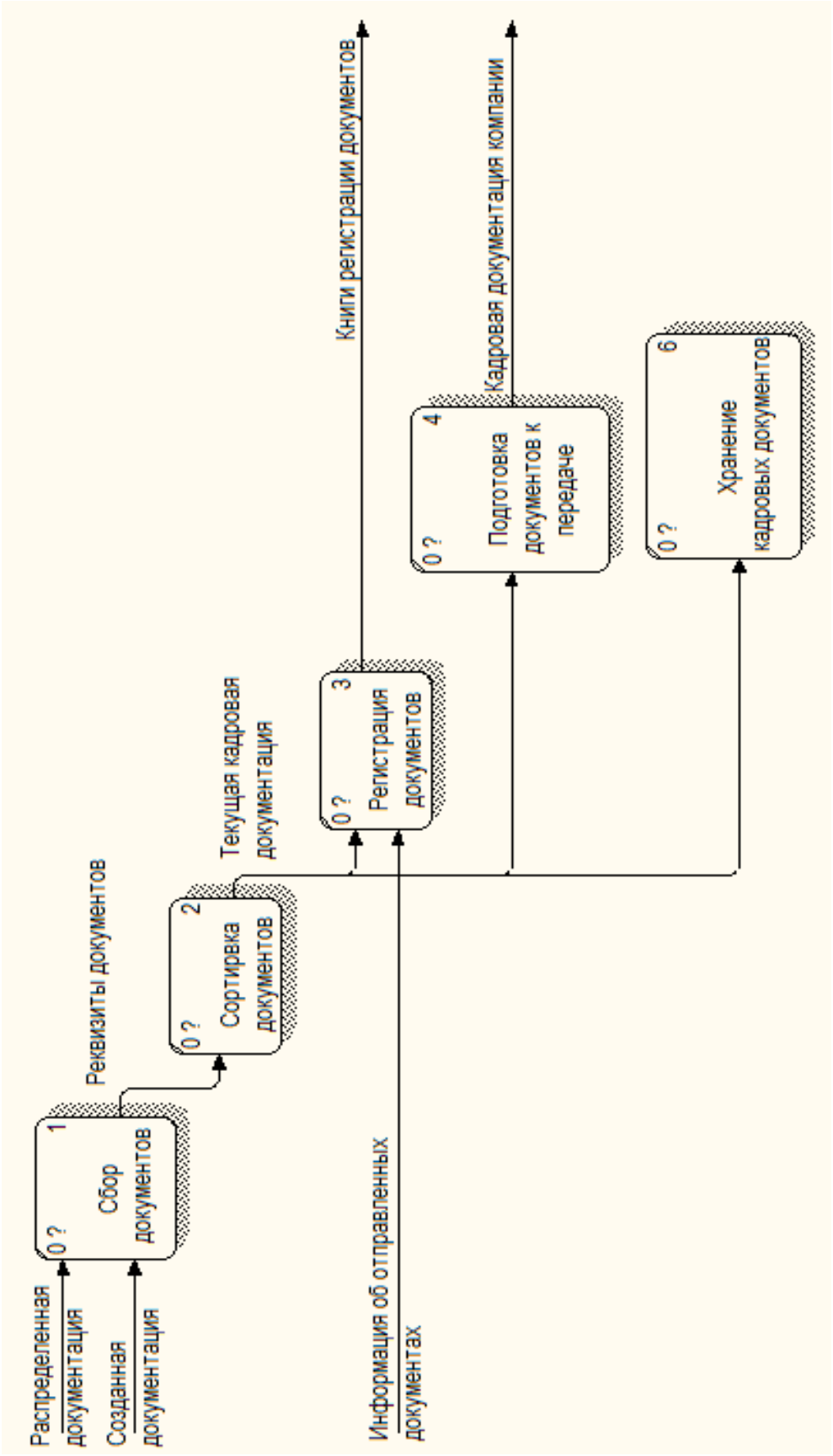


Рисунок В.5 – Декомпозиция процесса учета кадровой документации

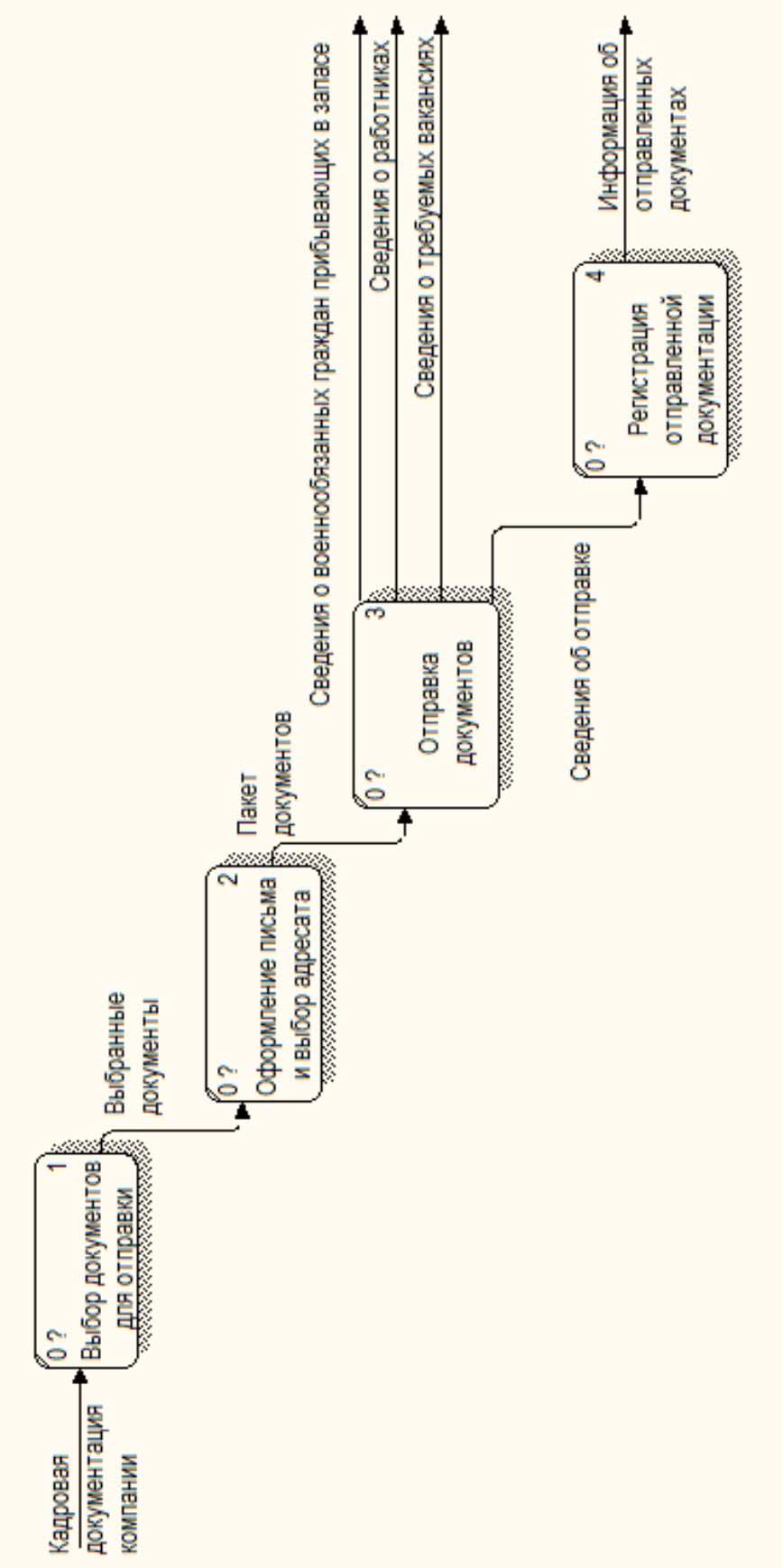


Рисунок В.6 – Декомпозиция процесса передачи кадровых документов

ПРИЛОЖЕНИЕ Г

Функциональная диаграмма разрабатываемой подсистемы

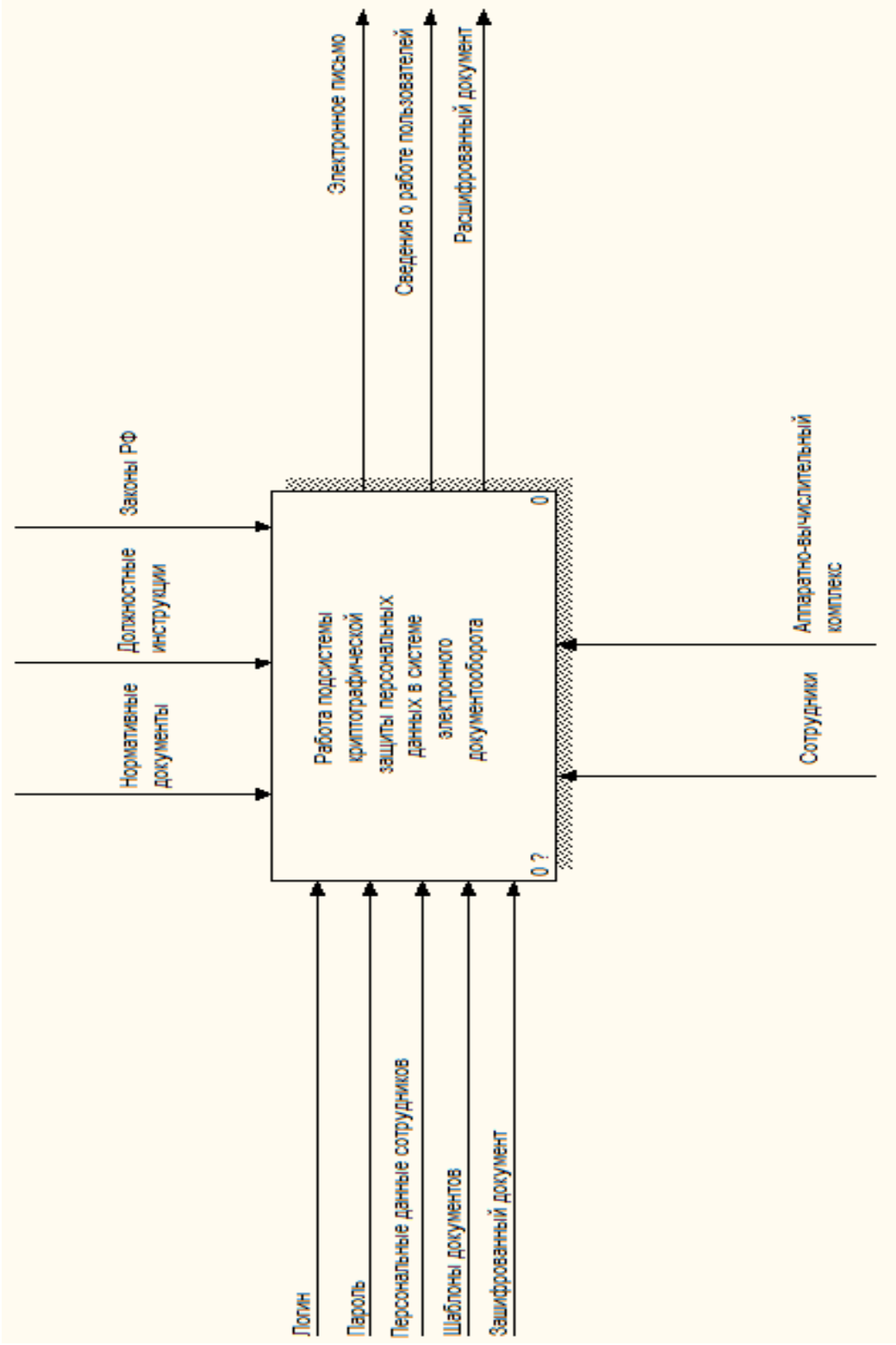


Рисунок Г.1 – Контекстная диаграмма

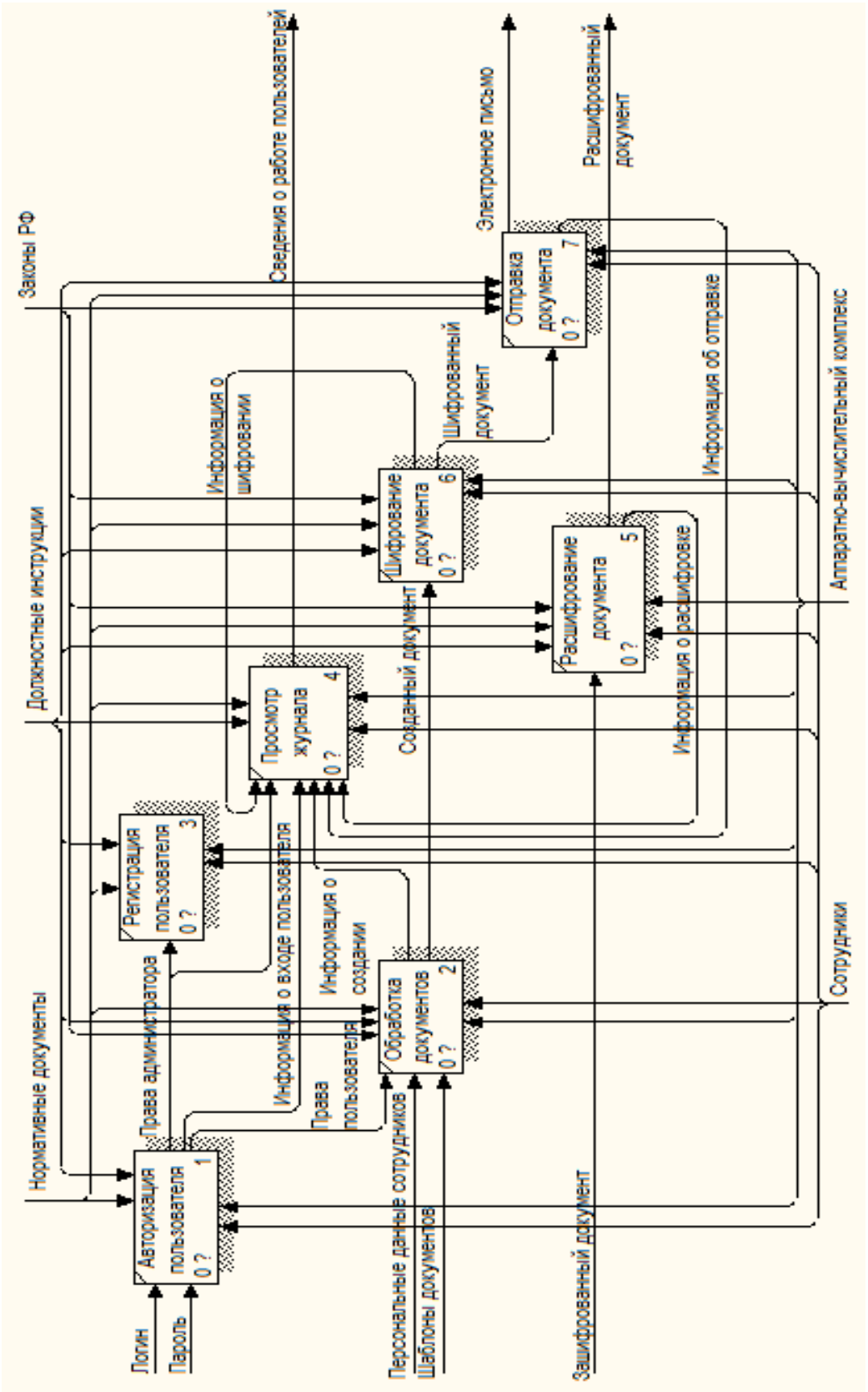


Рисунок Г.2 – Декомпозиция контекстной диаграммы

ПРИЛОЖЕНИЕ Д

Концептуально-инфологическая модель

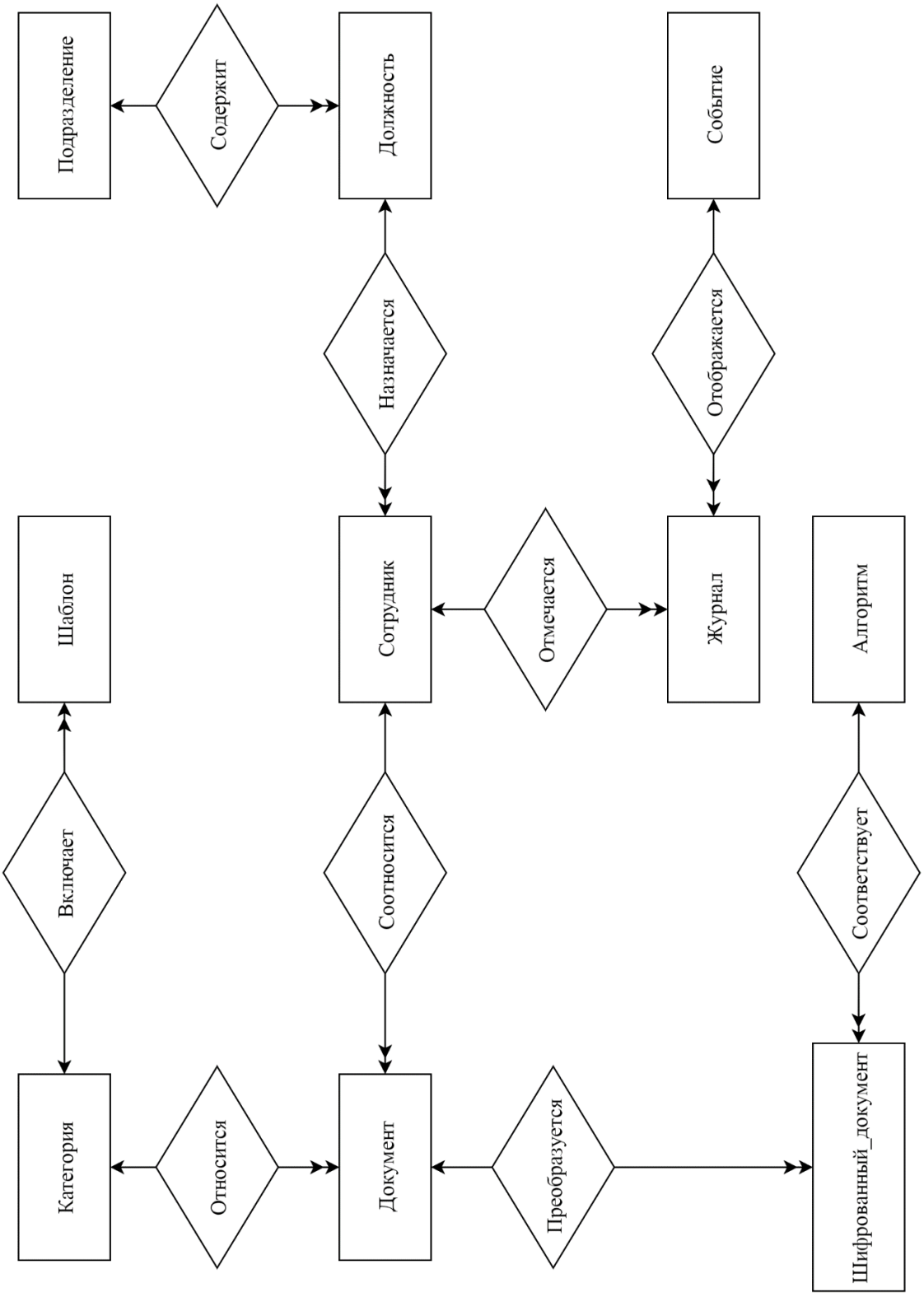


Рисунок Д.1 – Концептуально-инфологическая модель БД

ПРИЛОЖЕНИЕ Е

Логическая модель БД

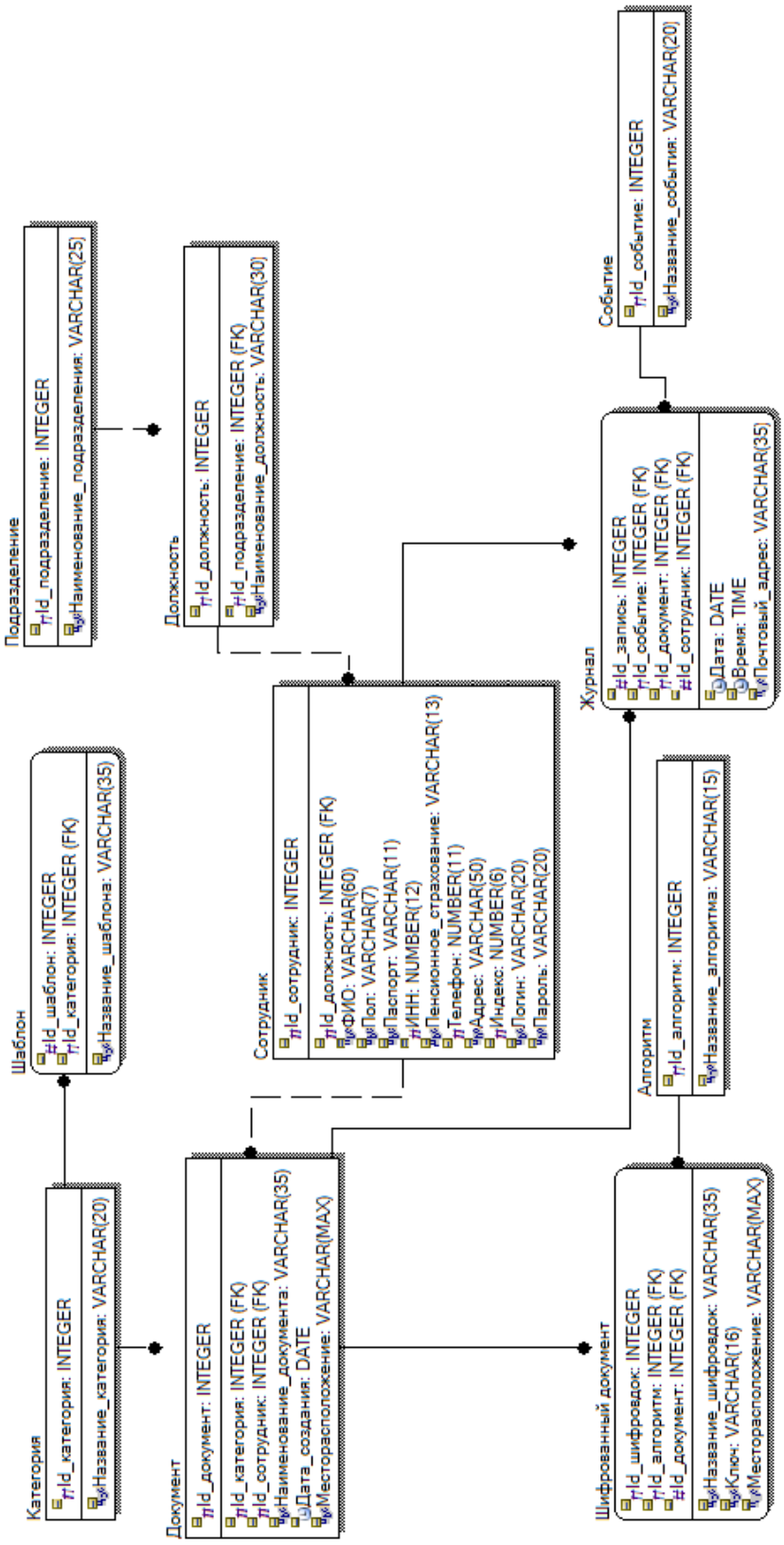


Рисунок Е.1 – Логическая модель базы данных

ПРИЛОЖЕНИЕ Ж

Блок-схемы алгоритма RC4

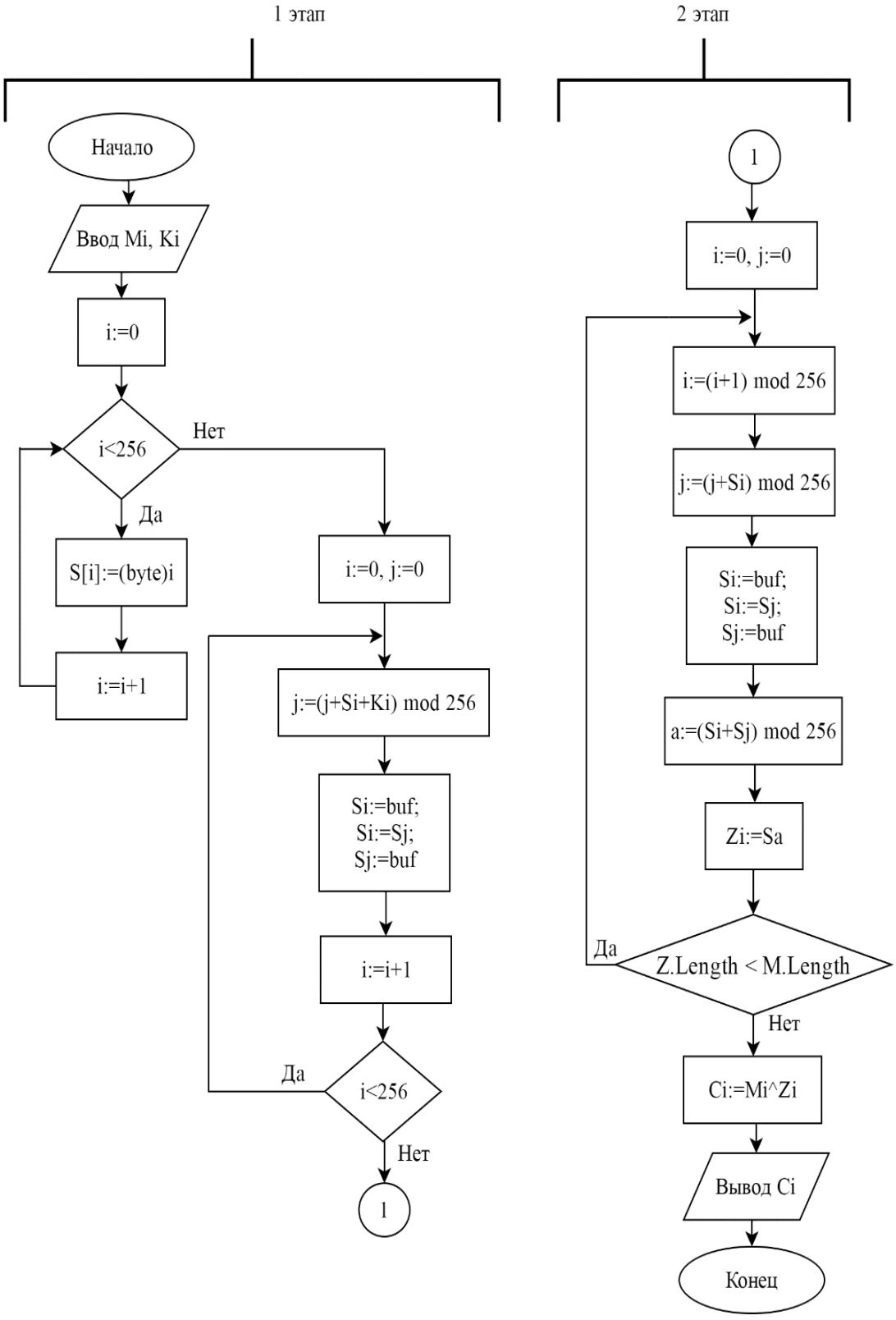


Рисунок Ж.1 – Зашифровка сообщения

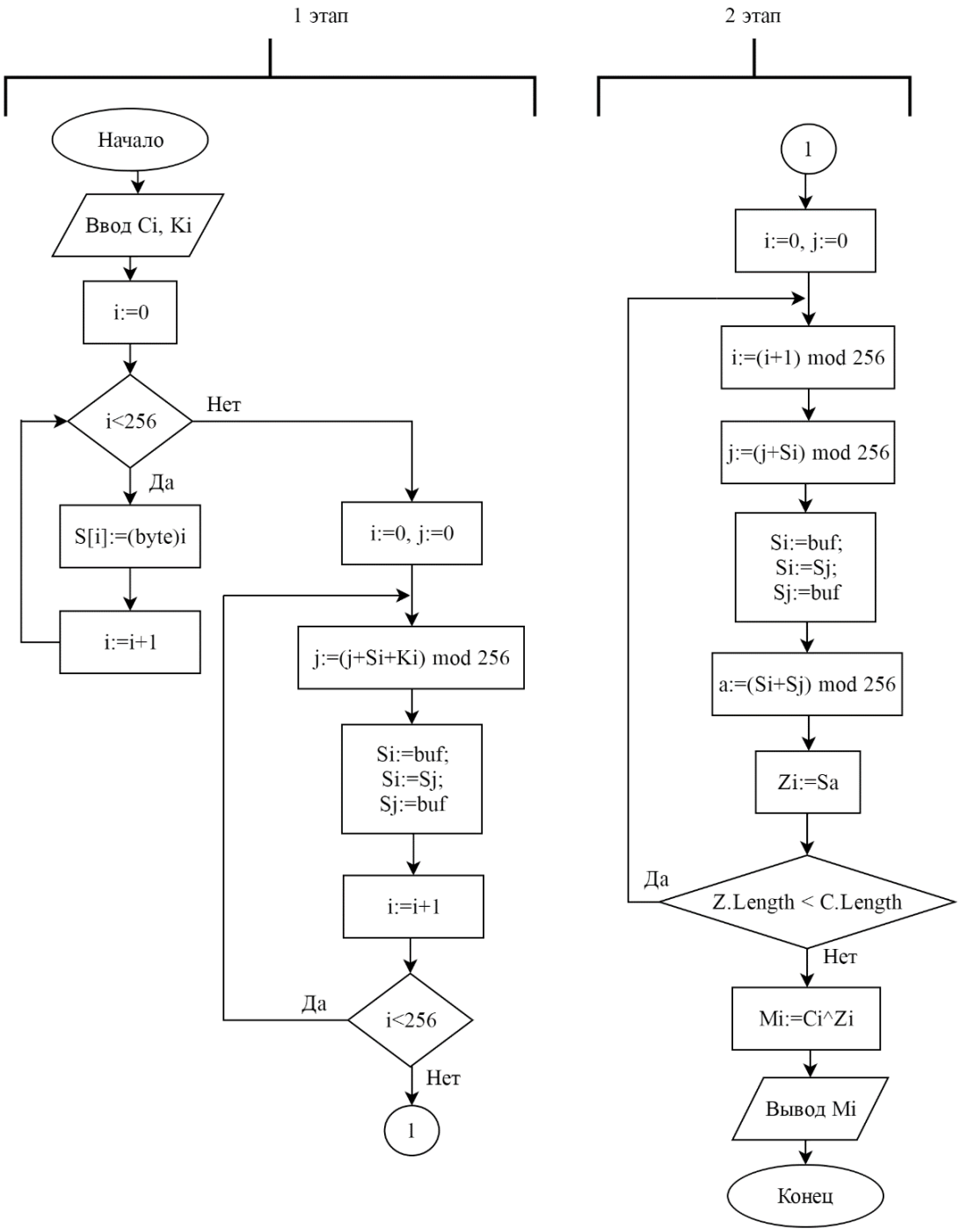


Рисунок Ж.2 – Расшифровка сообщения

ПРИЛОЖЕНИЕ К

Структура взаимодействия модулей подсистемы

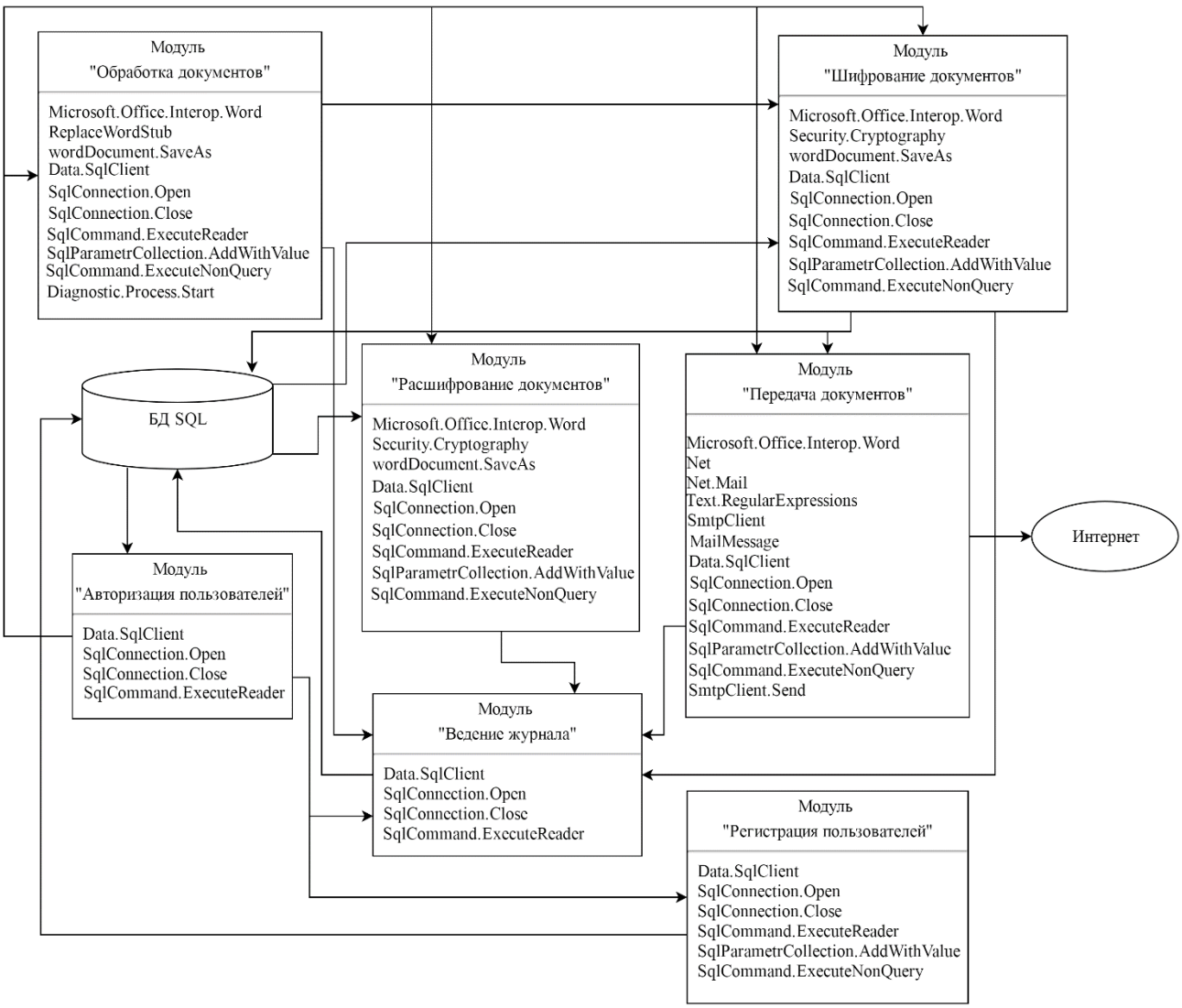


Рисунок К.1 – Структура взаимодействия модулей подсистемы