МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНО-ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ЮУрГГПУ»)
ПРОФЕССИОНАЛЬНО-ПЕДАГОГИЧЕСКИЙ ИНСТИТУТ

Кафедра Автомобильного транспорта, информационных технологий и методики обучения техническим дисциплинам

Проектирование информационной системы для электронного документооборота образовательной организации в условиях обеспечения информационной безопасности

Магистерская диссертация
по направлению: 44.04.04 Профессиональное обучение (по отраслям)
Направленность (профиль): Управление информационной безопасностью в профессиональном образовании
Форма обучения очная

Проверка на объем заимствований:
76,64% авторского текста

Работа рекомендована к защите
«8» 06 2022 г.
Зав. кафедрой АТИТ и МОТД
_____Руднев В.В.

Выполнила:
Студентка группы ОФ-209/210-2-1
Рыскулова Евгения Валерьевна

Научный руководитель:
Уварина Наталья Викторовна, д.п.н., профессор

Челябинск
2022

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Актуальность исследования. В условиях научно-технического, социально-экономического прогресса значительно улучшились условия и качество жизни общества. Данные процессы способствовали становлению и развитию информатизации в различных сферах деятельности. В образовании это повлекло за собой:

− изменение процесса взаимодействия между обучающим и обучаемым;

− изменение структуры представления учебного материала и формы учебно-методического обеспечения образовательного процесса;

− изменение учебной среды как условий взаимодействия между участниками образовательного процесса.

Однако те же процессы способствовали обострению проблем, связанных с информационной безопасностью передаваемых данных, сведений, защитой личности от информационного воздействия.

Развитие требовало комплексных решений, а именно внедрения средств технической и правовой защиты.

Под информационной безопасностью образовательной организации следует понимать состояние защищенности информационных ресурсов, технологий их формирования и использования, а также прав субъектов информационной деятельности.

Современная образовательная организация является сложным механизмом, в котором участники образовательного процесса используют различные средства обучения и воспитания. Помимо этого, в образовательной организации ведется учет, хранение, обработка и анализ информации об основных процессах в образовательной организации.

В условиях изменения подхода к процессам, связанным со взаимодействием в учебно-информационном пространстве, представлению

учебных материалов, очевидной становится задача по обеспечению информационной безопасности в образовательных организациях.

Наибольшее внимание уделяется защите персональным данным. К ним относятся: фамилия, имя, отчество, место и дата рождения, место регистрации, паспортные данные, СНИЛС, семейном положении, номер телефона, адрес электронной почты, фотография, сведения о родственниках, оценка навыков, личностных качеств, биометрические данные.

Впервые обратили внимание на необходимость защиты персональных данных в Организации по экономическому сотрудничеству и развитию. В дальнейшем принципы были детализированы.

На территории Российской Федерации осуществляется государственное регулирование, связанное с обеспечением безопасности обработки персональных данных (далее - ПДн). Правовое регулирование осуществляется в соответствии с Конституцией Российской Федерации, Федеральным законом от 27.07.2006 N 152-ФЗ «О персональных данных» и принятых во исполнение его положений, нормативно-правовых актов и методических документов.

Ключевыми факторами, обуславливающими проблему информационной безопасности данных обрабатываемых в университете, выступают:

− возрастающие темпы цифровизации ресурсов, усложняющейся структурой информационных систем университета;

− возрастающий объем обрабатываемых в университете данных;

− повышение востребованности сетевого доступа к цифровым ресурсам университета;

− добавление пользователей, пользующихся удаленным доступом;

− обновление состава внешних и внутренних угроз для безопасности данных.

К основным угрозам безопасности в университете относится:

− получение доступа третьими лицами к информационным сервисам;

− перехват третьими лицами аутентифицирующей информации;

− получение доступа во внутреннюю информационную подсистемы;

− кражи заинтересованными лицами личных персональных данных сотрудников и обучающихся;

− возможная подмена записей в документах;

− получение несанкционированного доступа к научным исследованиям и интеллектуальной собственности сотрудников;

− нарушение доступа к сайту университета.

Особое внимание уделяется вопросам защиты персональных данных в различных автоматизированных информационных системах. Соблюдению требований к защите в данных системах с учетом категории и количества получаемых, хранимых, обрабатываемых и передаваемых данных, решаемым задачам и ряду других показателей.

Из выше сказанного, можно сделать вывод, что тема исследования «Проектирование информационной системы для электронного документооборота образовательной организации (ФГБОУ ВО ЮУГМУ Минздрава России) в условиях обеспечения информационной безопасности» является актуальной, а полученные результаты имеют важное практическое значение.

Это определяет актуальность проектирования информационной системы документооборота ориентированной на основные угрозы безопасности, представленные в документах ФСТЭК и ФСБ России.

Цель исследования: спроектировать и внедрить информационную систему электронного документооборота образовательной организации, которая обеспечивает необходимый уровень информационной безопасности данных.

Объект исследования: информационная безопасность образовательной организации.

Предмет исследования: система документооборота образовательной организации.

Гипотеза исследования состоит в предположении того, что разработка и реализация информационной системы электронного документооборота образовательной организации, включающей модуль заказа и выдачи справок обучающимся повысит уровень информационной безопасности за счет передачи и обработки данных в защищенном контуре.

Для достижения поставленной цели были сформулированы следующие **задачи:**

1. Определить теоретические основы обеспечения информационной безопасности в образовательных организациях.
2. Проанализировать уровень обеспеченности информационной безопасностью образовательных организации в процессе их деятельности.
3. Выявить средства обеспечения информационной безопасности, учитываемые при проектировании информационных систем образовательных организаций в условиях обеспечения информационной безопасности.
4. Разработать и реализовать проект информационной системы электронного документооборота в условиях обеспечения информационной безопасности в ФГБОУ ВО ЮУГМУ Минздрава России.

Для решения поставленных задач были использованы следующие **методы исследования**:

− изучение и анализ теоретико-методической литературы по теме исследования;

− документоведческий метод как анализ документации образовательной организации;

− анализ и сопоставление имеющихся средств для защиты данных;

− анализ и классификация собранных данных с последующим моделированием и проектированием информационной системы в условиях обеспечения информационной безопасности;

− метод апробации результатов;

− метод экспертной оценки качества разработанных мер защиты.

Теоретической и методологической базой исследования явились нормативно-правовые акты законодательства Российской Федерации, а также труды следующих авторов: Астахова Л.В., Бадьина А., Богатырева Ю.И., Бурькова Е.В., Ильина К., Красноярского М.Н., Кузнецова Т.В., Мельникова Н.Ю., Милютина О.В., Параскевова А.В. Левченко А.В. Кухоива Ю.А., Пипиленко В.Ф., Привалова В.Ф. Богатыревой Ю.И. Романова В.А., Привалова В.Ф., Терещенко Л.К., Храмцовской Л.К., Чернова В.Н., Ярочкина В.Н.

База исследования*:* ФГБОУ ВО ЮУГМУ Министерства России.

На защиту выносятся следующие положения:

1. Проблема обеспечения информационной безопасности в образовательной сфере актуализируется посредством введения дистанционных технологий и необходимостью разной территориальной распределенностью участников образовательного процесса.

2. Электронный документооборот является формой современного делопроизводства в образовательных организациях, позволяет создавать базы данных, способные накапливать и хранить большие объемы информации, анализировать хранимые данные и принимать решения, основанные на данных.

3. В сфере образования системы электронного документооборота способствует повышению качества образовательного процесса, упрощение обучения и работы научно-педагогического персонала, совершенствованию контроля успеваемости обучающихся, упорядочению хранения и использования документации.

4. В сфере образования системы электронного документооборота способствует повышению качества образовательного процесса, упрощение обучения и работы научно-педагогического персонала, совершенствованию контроля успеваемости обучающихся, упорядочению хранения и использования документации.

5. Процесс разработки и реализации проекта информационной системы электронного документооборота в условиях обеспечения информационной безопасности включает: проектирование и разработку модуля выдачи справок в системе электронного документооборота.

Научная новизна исследования заключается в следующем:

1. Теоретически обоснована необходимость обеспечения информационной безопасности в образовательных организациях, а именно:

− создание совокупности мер и средств защиты, так как абсолютных способов обеспечения информационной безопасности не существует, систему защиты необходимо постоянно усовершенствовать, поскольку злоумышленники так же постоянно усовершенствуют свои методики;

− выявление проникновения злоумышленников на раннем уровне и тем самым снижения степени возможных вариантов проявления ущерба;

− наличие специалистов, представляющих себе принципы функционирования, как самой системы защиты, так и информационной среды образовательной организации в целом и в случае возникновения затруднительных ситуаций адекватно на них реагирующих.

2. Рассмотрена теория об электронном документообороте как форме современного делопроизводства в образовательных организациях и обоснована необходимость создания условий информационной безопасности при его функционировании.

3. На основе анализа существующей системы документооборота в исследуемой организации было обосновано решение о необходимости внедрения полноценной системы электронного документооборота, которая

будет не только организовать электронный документооборот, но и позволит связать между собой различные информационные системы университета и создавать условия для обеспечения информационной безопасности.

4. Спроектирован и внедрен модуль выдачи справок, в системе электронного документооборота, позволяющий передавать данные с учетом требований по информационной безопасности.

Теоретическая значимость исследования состоит в том, что:

1. Проведен анализ изучаемой проблемы и описаны классические методы обеспечивающие защиту электронного документооборота;

2. Определены средства, обеспечивающие информационную безопасность с учетом информационного взаимодействия;

3. Уточнены и конкретизированы понятия «информационная безопасность», «документооборот», «электронный документооборот «защищенная информационная система».

Практическая значимость работы заключается в проектирование информационной системы для электронного документооборота образовательной организации в условиях обеспечения информационной безопасности, разработанной на основе анализа системы документооборота и частной модели угроз ФГБОУ ВО ЮУГМУ Министерства России, которая может быть применено в других образовательных организациях высшего образования.

Ход исследования и его результаты докладывались и обсуждались на конференциях и конкурсах:

1. Двадцать второй международной научно-практической конференции «Новые информационные технологии в образовании» (Экосистема 1С для цифровизации экономики, организации учебного процесса и развития профессиональных компетенций), 01.02.2022 - 02.02.2022 г.;

2. Международной научно-практической конференции «Национальная безопасность и молодежная политика киберсоциализация и трансформация ценностей в VUCA-мире» 21-22 апреля 2021 г., г. Челябинск;

3. Международной научно-практической конференции «Модели и методы повышения эффективности инновационных исследований» 4 июля 2021 г. Воронеж;

4. Конкурсе «Лучшая научная статья студентов и аспирантов ФГБОУ ВО «Южно-Уральский государственный гуманитарно-педагогический университет» - 2021»;

5. XII внутривузовской научно-практической конференции «Оптимизация высшего медицинского и фармацевтического образования: менеджмент качества и инновации» 24 февраля 2021 г.;

6. XI внутривузовской научно-практической конференции «Оптимизация высшего медицинского и фармацевтического образования: менеджмент качества и инновации» 07 февраля 2020 г.

Структура магистерской диссертации состоит из введения, двух глав, заключения, списка использованных источников, состоящего из 88 наименований, приложения.

ГЛАВА 1. ПРОБЛЕМА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЙ В ТЕОРИИ И ПРАКТИКЕ ПЕДАГОГИКЕ

1.1. Теоретические основы обеспечения информационной безопасности в образовательных организациях

Защиты информации, а именно обеспечение сохранности и установление статуса ее использования является проблемой в любой сфере деятельности. В первые годы внедрения информационных технологий задача защиты информации решалась за счет организационных мер и программно - аппаратах средств.

С увеличением количества персональных компьютеров, сетей, спутниковых каналов связи обострилась проблема защиты информации, это было связанно с территориальной распределенностью. Развитие техники и технологий позволяло увеличивать число автоматизированных процессов, создавать базы данных способные накапливать и хранить большие объемы информации, анализировать хранимые данные и принимать решения, основанные на данных. Все это требовало изменения подходов к решению задач.

В сфере образования наименее защищенными пользователями являются дети и подростки. Одним из каналов получения ими информации является образовательный процесс. Связано это с внедрением федеральных государственных стандарты в образовании, которые были направлены на организацию регулирования учета образовательного и научного процессов. Это способствовало становлению и развитию информатизации образования, созданию предпосылок, констатирующие их необратимость:

− изменение процесса взаимодействия между обучающимся и обучаемым;

− изменение структуры представления учебного материала и формы учебно-методического обеспечения образовательного процесса;

− изменение учебной среды как условий взаимодействия между участниками образовательного процесса [74].

При проектировании системы информационной безопасности образовательной организации необходимо учитывать то, что она должна обеспечивать сохранность баз данных, массивов конфиденциальной информации, обеспечивать невозможность доступа пропаганды различного характера, которая может оказать воздействие на сознание обучающихся.

В понятие информационной безопасности образовательной организации входит два аспекта. Первым аспектом является система мер, направленная на защиту информационного пространства и персональных данных от случайного или намеренного проникновения с целью хищения каких-либо данных или внесения изменений в конфигурацию системы. Вторым аспектом понятия является защита образовательного процесса от любых сведений, носящих характер запрещенной законом пропаганды, или любых видов рекламы [65].

В своей деятельности образовательная организация обязана обеспечивать сохранность следующей информации:

- персональные сведения;

- оцифрованные архивы;

- методические пособия и технологии, используемые в образовательном процессе и относящиеся к интеллектуальной собственности;

- иные структурированные сведения.

Данная информация теоретически подвержена угрозам, которые связаны не только с хищением или повреждение, но и с деятельностью обучающихся, способных повредить оборудование или программное обеспечение.

Существует пять группы объектов, которые могут подвергнуться воздействию:

- компьютерная техника и другие аппаратные средства;
- программное обеспечение;
- хранимые данные;
- персонал;
- обучающиеся.

Угрозы могут носить случайный и преднамеренный характер. К случайным угрозам можно отнести:

- аварийные ситуации;
- ошибки персонала;
- сбои программного обеспечения;
- неисправность аппаратного обеспечения;
- проблемы в работе систем связи.

Данные угрозы являются временными, предсказуемы и могут быть устранены сотрудниками или специальными службами.

Преднамеренные угрозы являются опасными и в большинстве случаев не могут быть предвидены. Виновниками данных угроз могут быть обучающиеся, сотрудники, конкуренты, третьи лица с намерением на совершение преступления.

В образовательных организация подвергнуться атакам могут архивы, содержащие материалы, защищенные авторским правом, обучающиеся с целью воздействия на их сознание.

Для реализации угроз необходим доступ к ресурсам образовательной организации. Его возможно получить через:

− копирование, перенаправление и изменение данных нарушителем;

− использования специальных программ для копирования и перехвата паролей, информации, перенаправление трафика, дешифровку, внесение изменений в работу программ;

− использования технических средств, или с перехватом электромагнитного излучения по различным каналам связи.

Информационная безопасность - это предупредительные действия, которые позволяют защитить информацию и оборудование, от угроз и использования их уязвимых мест через повседневную практику и постоянную бдительность [38].

Для всесторонней защиты и борьбы с различными видами атак должна проводиться работа по обеспечению безопасности на различных уровнях, с использованием различных продуктов и носить комплексный характер.

При формировании системы защиты необходимо учитывать особенности информационного взаимодействия в образовательных организация, информационный обмен составляет значимую часть функционирования образовательной организации, при этом документооборот может быть реализована как в офлайн, так и в онлайн форматах.

Средствами обеспечения информационной безопасности с учетом информационного взаимодействия являются:

1. Нормативно-правовой способ.

На основе Федеральный закон от 29.12.2010 №436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» и Указа Президента Российской Федерации от 1 июня 2012 г. №761 «О Национальной стратегии действий в интересах детей на 2012 – 2017 годы» был создан ряд методических рекомендация для образовательных организаций.

В 2015 году принята «Стратегия развития воспитания в Российской Федерации на период до 2025 года», определяющая степень угроз и меры защиты безопасности детей, которая способствовала процессу анализа и доработки методических рекомендации, положений нормативных

правовых документов в части ограничения распространения информации для предотвращения агрессивного воздействия на сознание обучающихся.

В соответствии с частью 2 пункта 6 статьи 28 и частями 8 и 9 пункта 1 статьи 41 Закона «Об образовании» в обязанности образовательной организации входят вопросы, связанные с обеспечением безопасности и здоровья, обучающихся на территории образовательной организации.

Информационная безопасность детей согласно Федеральному закону №436-ФЗ - это состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию [52].

Образовательная организация должна обеспечивать информационную безопасность своих обучающихся. Это является одной из основных задач.

Образовательная организация обязана отслеживать изменения в законодательстве и нормативных актах, связанных с регулированием общественных отношений в сети Интернет.

Порядок защиты персональных данных определяется Конституцией Российской Федерации, федеральными законами об информации, информационных технологиях и о защите информации, в кодексах, ГОСТах, определяющие порядок защиты данных, и применяемые в этих целях методики и аппаратные средства.

2. Морально-этические средства обеспечения информационной безопасности.

Образовательная организация в своей деятельности должна анализировать информацию и источники получения данной информации с целью недопущения использование тех, которые могут травмировать психику обучающихся.

Заниматься просветительской работой с обучающимися и их родителями (законными представителями). Повышать культуру информационной безопасности через реализацию программ и

мероприятий, связанных с информационными технологиями и культурой их использования. Назначать ответственных, из числа сотрудников и педагогических работников образовательной организации, которые будут заниматься вопросам организации защиты обучающихся от видов информации, распространяемой посредством сети «Интернет».

3. Административно-организационные меры.

В образовательной организации должна быть разработана политика по информационной безопасности и внутренние регламенты, описывающие порядок обработки персональных данных; учета движения съемных носителей, доступа к информации и информационным системам, процесс резервного копирования, восстановления баз данных, работы с «Интернет» и другими процессами в соответствии с нормативными документами.

Сотрудники образовательной организации должны быть ознакомлены с данными документами. Документы необходимо хранить в доступном для ознакомления месте.

4. Физические меры.

За организацию физических мер отвечает руководство образовательной организации и сотрудники информационно-технического подразделений.

Для ее обеспечения необходимо создать условия для невозможности получения несанкционированного доступа, повреждения и воздействия в отношении помещений и информации образовательной организации.

Для обеспечения физической безопасности необходимо знать основные угрозы безопасности своей организации и методы их решения.

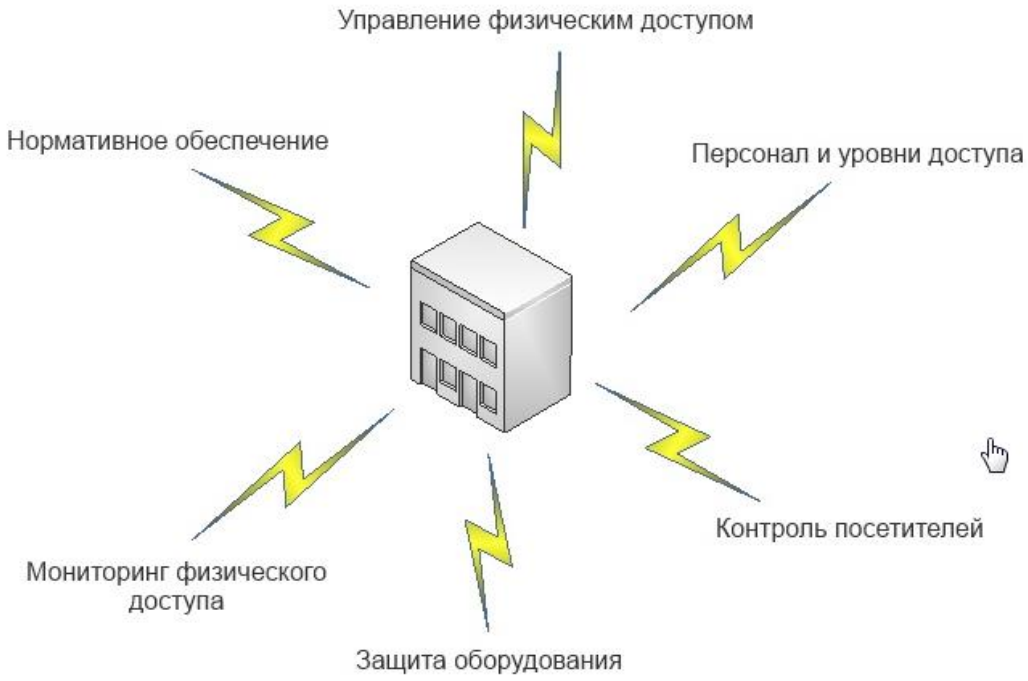

Рисунок 1 – Средства обеспечения физической безопасности информационных ресурсов в образовательной организации

На рисунке 1, представлены основные моменты, связанные с физической безопасностью информационных ресурсов.

Физическая безопасность информационных ресурсов – это комплекс информационно-технических мероприятий, соблюдение которых позволит эффективно защищать образовательную организацию от возможных внешних и внутренних атак, а также возможных стихийных бедствий [70].

5. Технические меры.

При выборе технических мер защиты образовательным организациям рекомендовано использовать профессиональные системы, входящие в список разрешенных и рекомендуемых программных мер защиты:

− антивирусное программное обеспечение;

− межсетевой экран (firewall);

− аутентификация личности;

− системы обнаружения вторжения (Intrusion Detection System, IDS) и системы предотвращения вторжения (Intrusion Prevention System, IPS).

− шифрование.

Совокупность всех перечисленных мер и средств, позволит создать условия для формирования безопасной информационной среды образовательной организации.

Специалисты, имеющие отношение к системе защиты должны полностью представлять себе принципы функционирования, как самой системы защиты, так и информационной среды образовательной организации и в случае возникновения затруднительных ситуаций адекватно на них реагировать. Для поддержания высокого уровня безопасности система защиты должна быть гибкой, быстро реагировать на изменения как внешних, так и внутренних факторов, на постоянной основе должен функционировать механизм тестирования для поддержания согласованности и целостности всех элементов.

1.2. Электронный документооборот как форма современного делопроизводства в образовательных организациях

В настоящее время наблюдается тенденция, связанная с переходом на электронную форму документооборота. Этому способствовало появление различных форм взаимодействия, как с внутренними участниками делопроизводства, так и внешними. Электронный документооборот позволяет ускорить процессы и сделать их более прозрачными. В образовательных организациях так же наблюдается переход от классической бумажной документации к электронной.

В сфере образования системы электронного документооборота будет способствовать повышению качества образовательного процесса, упрощение обучения и работы научно-педагогического персонала, совершенствованию контроля успеваемости обучающихся, упорядочению хранения и использования документации. Немаловажным является

переход от бумажных библиотек к электронным хранилищам документов, научных изданий и учебно-методической литературы [39].

Документооборот - это движение документов с момента входа в систему до выхода из нее. Под движением документов понимают работу над ними: формирование, прием, регистрация, рассылка, исполнение, хранение, повторное использование и другие операции.

Система электронного документооборота создана для управления данными процессами и реализуют концепцию безбумажного делопроизводства. Объектом в данной системе является электронный документ, сформированный средствами компьютерной техники и сохраненный на электронном носителе. Документы, созданные в системе, могут быть подписаны электронной подписью (аналог собственноручной подписи). Электронная подпись - средство защиты информации от незаконного изменения и служащее для контроля подлинности и целостности электронных документов.

Первоначальной задачей системы электронного документооборота являлась автоматизация делопроизводства, но ситуация изменилась, когда производители систем документооборота перестали просто копировать процессы движения документации, а стали учитывать задачи, поставленные как перед этими процессами, так и перед всем документооборотом в целом [39].

Для реализации более сложных задач разработчики систем электронного документооборота наделили системы свойствами:

- открытости;
- интегрируемости;
- интеллектуальности;
- маршрутизации;
- разграничения доступа;
- аннотирования;
- кросплатформенностью.

Данные свойства позволили добавлять в системы новые функции, совершенствовать и дополнять имеющиеся модули, выступать системе в качестве связующего звена между различными приложениями, создавая основу для организации делопроизводства и способствовать переходу к электронному документообороту в образовательных организация.

Данный переход позволить получить ряд преимуществ:

− увеличить производительность труда сотрудников;

− улучшить контроль исполнительской дисциплины;

− сократятся затраты на хранения, обработку, передачу и поиск документов;

− появлению возможности коллективной работы над документами;

− повышению безопасности хранения информации за счет ограничения доступа к ней и сохранности документов.

Но при внедрении системы электронного документооборота помимо положительного эффекта возникает и ряд факторов, которые оказывают отрицательное влияние на процессы, протекающие в делопроизводстве:

− человеческий;

− нестабильность структуры организации;

− отсутствие документооборота;

− способ взаимодействия с «внешним миром»;

− перевод документов из бумажной формы в электронную;

− угрозы информационной безопасности.

Более пристального внимания требуют такие факторы как человеческий и угрозы информационной безопасности. Человеческий фактор связан с тем, что многие сотрудники образовательных организация являются людьми консервативными и с недоверием относятся к технологиям. Переход необходимо проводить плавно, приучая персонал к новым технологиям, идти от автоматизации простых процессов и заканчивать полноценной системой документооборота.

Угрозы информационной безопасности проявляются не самостоятельно, через взаимодействие со слабыми звеньями системы защиты, через факторы уязвимости.

Данные факторы необходимо определить и разработать по ним сценарии предупреждения наступления данных событий или их разрешения в случаи наступления.

Таким образом, системы автоматизации документооборота – достаточно сложный механизм, включающий в себя множество подсистем, построенных с помощью различных программных продуктов. В процессе функционирования данного механизма возникает ряд проблем и сложностей, но они носят весьма условный характер и легко поддаются решению при грамотном подходе. Более того, количество и вес преимуществ, получаемых организацией, использующей систему электронного документооборота, перекрывают недостатки и неудобства.

Данные системы находят широкое применение именно по причине того, что эффект от них заключается не только в экономии ресурсов, но и в том, что повышается качество работы организации в целом.

Для образовательных организаций - это возможность более эффективно решать поставленные задачи, реализовать возможность оперативного взаимодействия с различными субъектами и с ведомствами. Системы электронного документооборота позволяют сделать управление в образовательных организациях более прозрачным, оперативным и информативным.

1.3. Требования к проектированию систем электронного документооборота в условиях обеспечения информационной безопасности

Система электронного документооборота решает множество прикладных задач, связанных с информацией:

- обеспечение высокой доступности и безопасности;
- поддержка работы ключевых систем;
- сокращение расходов на хранение и управление;
- снижение убытков из-за потерь документов.

При разработке необходимо учитывать существующую организационную структуру, систему делопроизводства, необходимость интеграции с внутренними и внешними информационными системами и специфические особенности отрасли.

В образовании специфика связана с тем, что документы могут формироваться в различных специализированных информационных системах, которые не связаны между собой.

Нет возможности полностью отказаться от бумажного способа, так как данный вариант закреплен законодательно.

Наличие специфических объектов, которые требуют определенного подхода к автоматизации.

При проектировании системы электронного документооборота необходимо учитывать все выше перечисленные особенности и обеспечить надлежащий уровень безопасности.

Требования для обеспечения надлежащего уровня информационной безопасности формируются на основе анализа угроз и критериев.

Разработчики различных систем приводят примеры реализованных защищенных систем электронного документооборота, но точных критериев нет в изученной литературе, так как постоянно меняется правовое поле, нет необходимого количества стандартов. [35-37].

Из-за этого очень сложно дать точную формулировку понятию защищенного электронного документооборота (далее – ЗЭД) и создать рекомендации по формированию системы электронного документооборота в условии обеспечения информационной безопасности.

В настоящее время, используются классические методы, обеспечивающие защиту электронного документооборота, такие как:

- аутентификация и разделение прав доступа;
- подтверждение авторства;
- контроль целостности;
- конфиденциальность;
- обеспечение юридической значимости.

Если раньше обеспечивалась защита непосредственно самих электронных документов или информационных ресурсов, содержащих документы, то теперь изменяется основной вектор атак и, соответственно, объект защиты кроме традиционных атак на информационные ресурсы все чаще их объектом становится взаимодействие «человек – электронный документ», «человек – информационный ресурс» [31].

Из этого следуют, что защищать нужно в большей степени системы передачи, обработки и хранения документов.

На рисунке изображена модель ЗЭД, позволяющая провести анализ существующих угроз безопасности (рис. 2).

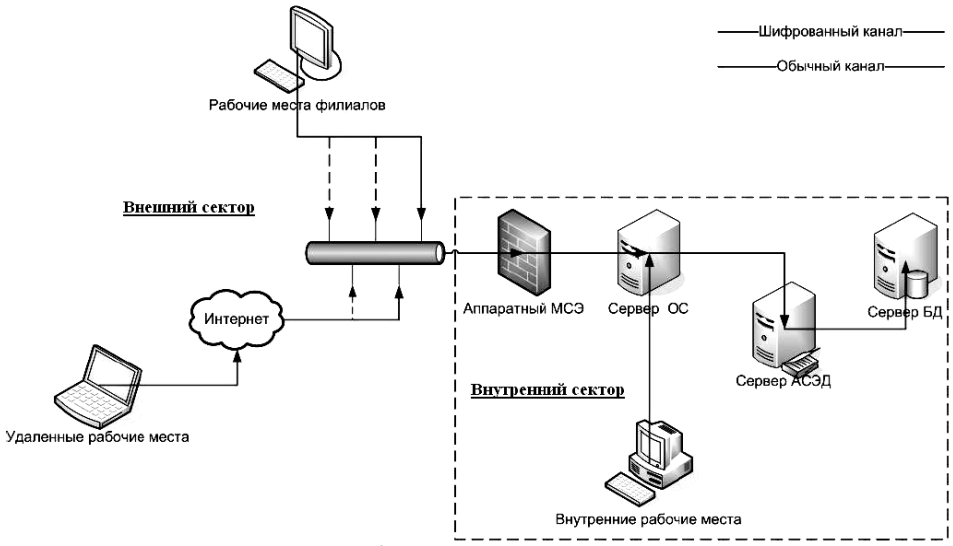

Рисунок 2 - Модель защищенной системы электронного документооборота

Все существующие угрозы можно сгруппировать по нарушаемым свойствам безопасности:

− угроза конфиденциальности (кража, перехват или изменение маршрутов следования информации);

− угроза целостности (потеря заранее определенных системой вида и качества передаваемой информации);

− угроза доступности (потеря доступа к информации в системе в любой момент времени).

Таки образом, при проектировании системы электронного документооборота образовательной организации необходимо учитывать особенности отрасли, опираться на классические методы обеспечения информационной безопасности, что позволит сформулировать требования, позволяющие в дальнейшем оценить степень защищенности внедренной системы.

ВЫВОДЫ ПО ПЕРВОЙ ГЛАВЕ

По итогам первой главы магистерской диссертации можно сделать следующие выводы.

1. Раскрыты теоретические основы обеспечения информационной безопасности в образовательных организациях.

Совокупность мер и средств, направленных на противодействие угрозам безопасности с целью сведения к минимуму возможности ущерба, образуют систему защиты, предназначенную для формирования безопасной информационной среды образовательной организации.

Специалисты, имеющие отношение к системе защиты должны полностью представлять себе принципы функционирования, как самой системы защиты, так и информационной среды образовательной организации и в случае возникновения затруднительных ситуаций адекватно на них реагировать.

Для поддержания высокого уровня безопасности система защиты должна быть гибкой, быстро реагировать на изменения как внешних, так и внутренних факторов, на постоянной основе должен функционировать механизм тестирования для поддержания согласованности и целостности всех элементов.

2. Рассмотрена теория о электронном документооборот как форме современного делопроизводства в образовательных организациях.

Системы автоматизации документооборота – достаточно сложный механизм, включающий в себя множество подсистем, построенных с помощью различных программных продуктов. В процессе функционирования данного механизма возникает ряд проблем и сложностей, но они носят весьма условный характер и легко поддаются решению при грамотном подходе. Более того, количество и вес преимуществ, получаемых организацией, использующей систему электронного документооборота, перекрывают недостатки и неудобства.

Данные системы находят широкое применение именно по причине того, что эффект от них заключается не только в экономии ресурсов, но и в том, что повышается качество работы организации в целом.

Для образовательных организаций - это возможность более эффективно решать поставленные задачи, реализовать возможность оперативного взаимодействия с различными субъектами и с ведомствами. Системы электронного документооборота позволяют сделать управление в образовательных организациях более прозрачным, оперативным и информативным.

3. Описаны требования к проектированию систем электронного документооборота в условиях обеспечения информационной безопасности.

Любая система должна обеспечивать защиту от угроз, связанных с конфиденциальность, доступностью, целостностью.

Системы электронного документооборота не является исключением. При ее проектировании в образовательной организации необходимо учитывать особенности отрасли, опираться на классические методы обеспечения информационной безопасности, это позволит сформулировать требования, позволяющие в дальнейшем оценить степень защищенности внедренной системы.

В целом решение проблемы обеспечения информационной безопасности образовательных организациях в теории педагогики видится в обобщении полученного опыта через создание научных объединений, проведения тематических встреч, конференций и отражении его в научной литературе в виде методических рекомендаций, научных статей, монографий, диссертаций [74].

В свою очередь, решение проблемы обеспечения информационной безопасности образовательных организациях в практике видится в подготовке не только квалифицированных технических специалистов, способных спроектировать, внедрить и обслуживать информационные

системы с высоким уровнем безопасности, но и педагогов через добавление специальных дисциплин в учебные планы, повышения квалификации работающих педагогов и персонала по средствам обучающих курсов, инструктажей, организации безопасной информационно-образовательной среды образовательной организации.

ГЛАВА 2. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ СИСТЕМЫ ДОКУМЕНТООБОРОТА ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ (на примере ФГБОУ ВО ЮУГМУ Минздрава России)

2.1 Разработка и реализация проекта информационной системы электронного документооборота в условиях обеспечения информационной безопасности в ФГБОУ ВО ЮУГМУ Минздрава России

Базой исследования является федеральное государственное бюджетное образовательное учреждение высшего образования «Южно-Уральский государственный медицинский университет» Министерства здравоохранения Российской Федерации (далее – ФГБОУ ВО ЮУГМУ Минздрава России), располагающийся по адресу: г. Челябинск, ул. Воровского, 64.

Исполняющий обязанности ректора — доктор медицинских наук, профессор, академик РАН Важенин Андрей Владимирович.

ФГБОУ ВО ЮУГМУ Минздрава России — высшее учебное заведение федерального подчинения, реализующее многоуровневую непрерывную систему подготовки специалистов: довузовская подготовка, обучение в колледже, университете, последипломная подготовка, повышение квалификации и переподготовка врачей, а также сертификация специалистов и подготовка научно-педагогических кадров [58].

Важнейшим направлением образовательной политики университета является совершенствование практической подготовки обучающихся. Ее основу составляют клиника, клинические базы, центр практических навыков.

Организационная структура ФГБОУ ВО ЮУГМУ Минздрава России представлена на рисунке 3.

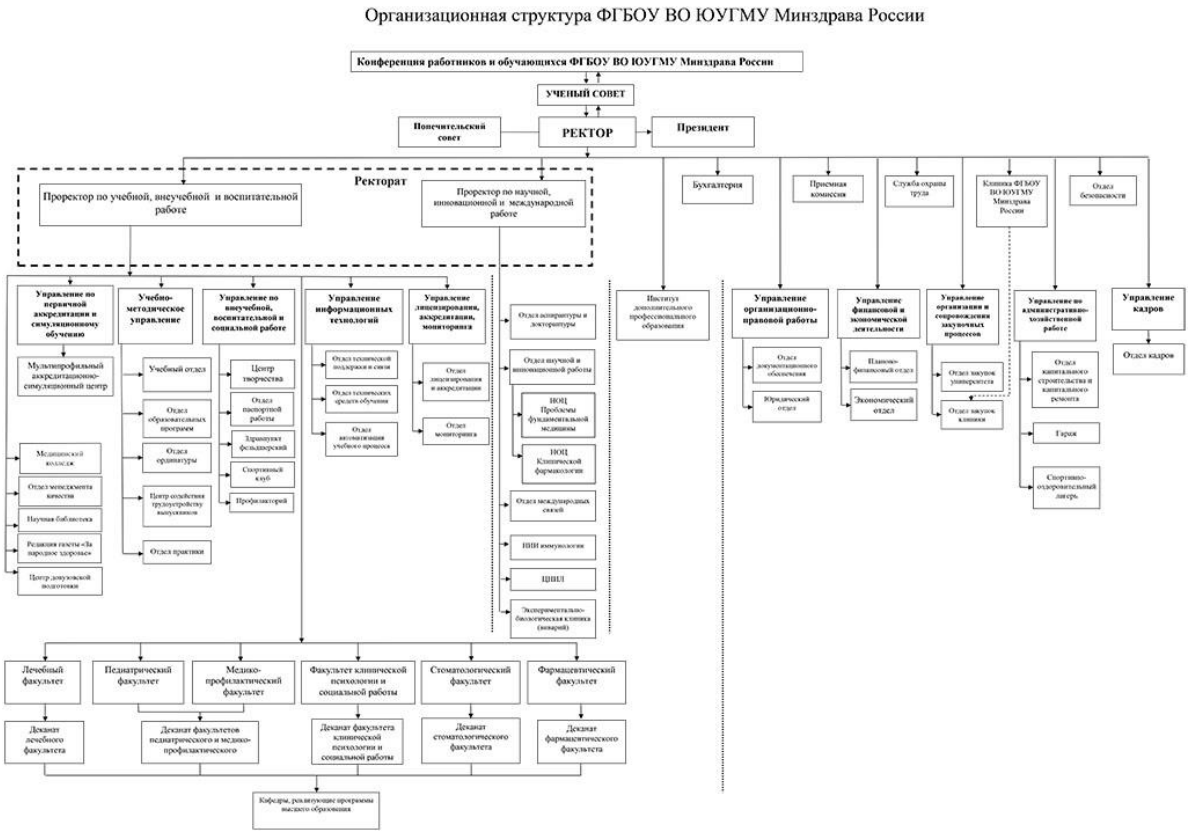

Рисунок 3 – Организационная структура ФГБОУ ВО ЮУГМУ Минздрава России

Университет располагается в 4 корпусах, первый корпус расположен по адресу ул. Воровского 64, там же находится административные подразделения. В этих корпусах расположены теоретические кафедры, обучающие студентов первых трех курсов. Студенты после третьего курса приступают к обучению на клинических кафедрах, расположенных в больницах города Челябинска. Так же в распоряжении университета имеются общежития для обучающихся, хозяйственные постройки и корпус центральной научно-исследовательской лаборатории, в котором ведется научно-исследовательская работа.

Основные виды деятельности ФГБОУ ВО ЮУГМУ Минздрава России:

1. образовательная деятельность;

2. научная деятельность в части осуществления фундаментальных поисковых и прикладных научных исследований;

3. деятельность, связанная с правовой охраной и использованием результатов интеллектуальной деятельности;

4. деятельность по обороту наркотических средств, психотропных веществ и их прекурсоров, культивированию наркосодержащих растений;

5. медицинская деятельность в части оказания населению медицинской помощи;

6. фармацевтическая деятельность;

7. и иные виды деятельности [58].

Организацией системы защиты данных в ФГБОУ ВО ЮУГМУ Минздрава России занимается «Управление информационных технологий».

Управление расположено по адресу: 454092, г. Челябинск, ул. Воровского, 64. Начальник управления информационных технологий - Муратов Иван Иванович.

В структуру управления информационных технологий университета входят:

1. Отдел технической поддержки и связи.

2. Отдел технических средств обучения.

Основные задачи управления:

1. Развитие информационных технологий в рамках административно-управленческих процессов.

2. Поддержание компьютерной сети университета в работоспособном состоянии.

3. Обеспечение бесперебойной работы компьютерного оборудования.

4. Организация освоения и применения новых программных и технических средств, информационных технологий, накопление и систематизация общего и тематического прикладного программного обеспечения.

5. Техническое обеспечение работ по вопросам лицензирования и аккредитации университета, ежегодной отчетности.

6. Анализ эффективности использования программных средств.

Функции управления:

1. Обеспечение подразделения университета доступом к ресурсам сети «Интернет».

2. Поддержание в рабочем состоянии и совершенствование компьютерной сети, комплексная защита сети от компьютерных вирусов разных видов, обеспечение сотрудников университета услугами электронной почты, назначение пользователям сети прав доступа.

3. Установка, настройка и управление программными и аппаратными системами университета.

4. Обеспечение бесперебойной работы компьютеров и периферийного оборудования.

5. Анализ и учет случаев отказа системы.

6. Развитие информационных технологий в рамках административно-управленческой деятельности.

7. Анализ и изучение проблем автоматизированных систем управления университета и ее подразделений.

8. Разработка и проведение мероприятий по повышению качества и надежности автоматизированных систем управления университета.

9. Разработка и реализация проектов по внедрению систем автоматизированного управления университетом.

10. Модернизация применяемых технических средств.

11. Составление заявок на необходимое оборудование, ведение учета его поступлений и использования средств, выделенных на эти цели. Подготовка документации на проведение конкурсов и аукционов при закупке компьютерной и оргтехники для нужд университета.

12. Обеспечение системами внутренней автоматической телефонной связи городка университета.

13. Консультации пользователей информационно-вычислительной системы университета по вопросам использования компонентов системного программного обеспечения.

14. Техническая поддержка учебных компьютерных классов.

Ответственным за обеспечение безопасности данных является начальник отдела технической поддержки и связи управления информационных технологий.

Управление информационными технологиями выполняет возложенные на него функции в тесном сотрудничестве и взаимодействии со всеми кафедрами и структурными подразделениями университета и другими образовательными организациями: центрами дистанционного образования, центрами Интернет-тестирования, учебно-научными центрами по проблемам информационной безопасности в системе высшей школы.

В университете введены в эксплуатацию информационные системы:

- СТЭК-Бухгалтерия (хозрасчеты);
- СТЭК-Заработная плата (бюджет);
- 1С: Аренда и управление недвижимостью для 1С: Бухгалтерия государственного учреждения;
- 1С: Розница 8 ПРОФ;
- 1С: Университет ПРОФ;
- портал вуза от 1С: Университет ПРОФ;
- 1С: Колледж ПРОФ;
- 1С: Управление учебным центром;
- 1С: Производственная безопасность. Охрана труда;
- ИРБИС – система автоматизации библиотек;
- сайт вуза;
- почтовый клиент;
- IP-телефония,

образующие единую электронную информационно-образовательную среду университета.

Документы, сопровождающие образовательную, научную и управленческую деятельность, формируются в различных и информационных системах, данный факт приводит к дублированию информации по причине отсутствия полноценной интеграции используемых систем в общую систему документооборота.

Жизненный цикл документации организации закреплен в Положении по управлению документированной информации СМК П 7.5-2018 и Положении о делопроизводстве СМК П 03-2014.

Целью управления документированной информацией является своевременное обеспечение структурных подразделений университета необходимой документацией в объеме и состоянии достаточном для осуществления процессов и их взаимодействия [58].

Управление документами университета включает в себя этапы:

- разработка проекта документа;
- согласование проекта документа;
- утверждение (принятие) документа и ввод его в действие;
- регистрация документа;
- копирование документа;
- рассылка документа;
- учет;
- ознакомление;
- хранение документа;
- актуализация документа;
- вывод документа из обращения;
- уничтожение документа.

Документы университета имеют четыре структурных уровня. Документы первого уровня:

- миссия и политика в области качества;

− цели в области качества;

− руководство по качеству.

В этих документах определены основные направления деятельности и цели в области качества, которые ставит руководство университета; задачи, которые нужно решить, чтобы достичь поставленных целей.

Документы второго уровня устанавливают порядок или способ выполнения различных видов деятельности университета. К документам второго уровня относятся:

− положения,

− правила, распространяющиеся на деятельность всего университета.

К документам третьего уровня относятся:

− инструкции;

− правила;

− организационные, распорядительные, информационно-справочные документы (приказы, распоряжения, положения о структурных подразделениях, должностные инструкции, и т.д.);

− документация по планированию (учебные планы, индивидуальные планы работы преподавателей, планы работ в структурных подразделениях и т.п.);

− записи, которые ведутся в структурных подразделениях университета.

К документам четвертого уровня относятся внешние нормативные документы:

− Федеральные законы;

− указы Президента Российской Федерации;

− постановления Правительства Российской Федерации;

− постановления и распоряжения Правительства Челябинской области;

− национальные и международные стандарты;

− федеральные государственные образовательные стандарты,

− типовые (примерные) программы;

− и иные.

Официальными являются документы на бумажном носителе. После утверждения и введения документа в действие специалистом отдела менеджмента качества создается электронная версия документа в формате pdf, которая размещается на сайте университета в сети «Интернет» в «Личном кабинете» – разделе доступном только работникам университета. На электронной версии документа имеется соответствующая надпись: «Электронная версия», «Для ознакомления».

Каждое структурное подразделение университета имеет доступ к актуальным версиям документов, необходимым в подразделения. Ответственность за использование актуальных документов в работе подразделения возложена на руководителя подразделения. Каждое подразделение может использовать в работе, как бумажный экземпляр, так и электронный.

Инструментами системы внутреннего обмена информацией являются:

− обмен информацией и данными на совещаниях различного уровня;

− обмен информацией и данными в рабочем порядке между подразделениями и должностными лицами;

− доведение информации до работников организации методом наглядной агитации, размещением информации на официальном сайте в сети Интернет;

− издание и рассылку приказов, выписок из протоколов ученого совета по средствам электронной почты или информационных систем;

− обратная связь руководства университета с персоналом осуществляется в ходе личных встреч.

Информационные системы наполнены различными данными, часть из которых относится к персональным данным, для данных такого типа используются информационные системы персональных данных (далее -

ИСПДн) с использованием средств криптографической защиты информации (далее - СКЗИ, криптосредства):

– ИСПДн «ФГБОУ ВО ЮУГМУ Минздрава России. ФИС ФЦТ»;

– ИСПДн «Обучающиеся и абитуриенты» ФГБОУ ВО ЮУГМУ;

– ИСПДн «Сотрудники» ФГБОУ ВО ЮУГМУ;

– ИСПДн «Библиотека» ФГБОУ ВО ЮУГМУ.

Для всех перечисленные ИСПДн разработаны и утверждены модели угроз безопасности персональных данных при их обработке в информационной системе персональных данных. Согласно моделям угроз ИСПДн установлено, что:

– ИСПДн являются информационными системами, обрабатывающей иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

– для ИСПДн актуальны угрозы 3-го типа;

– 3-ий и 4-ий уровень защищенности персональных данных при их обработке в ИСПДн.

Для защиты информации в ИСПДн университета используются СКЗИ:

– «ViPNet Coordinator HW 1000», сертификат соответствия ФСБ России;

– «ViPNet Client 4», сертификат соответствия ФСБ России;

– «КриптоПро CSP 4.0», сертификат соответствия ФСБ России;

– «Тунель-TLS», сертификат соответствия ФСБ России.

Приказом ректора университета № 552-л/вр от 13.08.2019 в ИСПДн: «ФИС ФЦТ», «Обучающиеся и абитуриенты», «Сотрудники» и «Библиотека» ответственным пользователем СКЗИ назначен оператор ЭВМ отдела технической поддержки и связи управления информационных технологий.

В Университете разработана «Инструкция ответственного пользователя СКЗИ» № б/н от 15.08.2019.

Процесс хранения оригиналов документов в университете организован на бумажных носителях, хранящихся в архиве организации. Систематизация осуществляется за счет составления номенклатуры дел.

Номенклатура дел составляется для обеспечения порядка формирования и учета дел в делопроизводстве структурных подразделений. Она намечает группировку исполненных документов в дела, систематизацию дел, индексацию и сроки хранения дел, является основой для составления описей дел постоянного и временного (свыше 10 лет) срока хранения и основным учетным документом в делопроизводстве.

Номенклатура дел является частью сводной номенклатуры дел университета и составляется лицом, ответственным за ведение делопроизводства в структурном подразделении на бланке установленной формы и в соответствии с установленными требованиями, согласованными с заведующим архивом, подписанными руководителем структурного подразделения и представленными в архив до 01 октября текущего года.

Вновь созданное подразделения обязано в месячный срок разработать номенклатуру дел подразделения при методической помощи заведующего архивом.

На основе номенклатур дел подразделений заведующий архивом составляет сводную номенклатуру дел, которая согласовывается с экспертной комиссией университета, экспертно-проверочная комиссия Государственного комитета по делам архивов Челябинской области, утверждается приказом ректора и вводимого в действие с 1 января следующего календарного года.

Сводная номенклатура дел университета составляется в трех экземплярах:

– первый хранится в архиве университета;

– второй передается в Государственный комитет по делам архивов Челябинской области;

– третий передается в ЭПК Государственного комитета по делам архивов Челябинской области.

Утвержденная номенклатура дел университета действует в течение 5 (пяти) лет. В конце каждого года её уточняют, при необходимости корректируют.

Номенклатура университета составляется вновь и переутверждается лишь в случае коренного изменения функций и структуры университета (или структурных подразделений).

Названиями разделов номенклатуры дел университета являются наименования подразделений, разделы располагаются в соответствии с утвержденной структурой.

После утверждения сводной номенклатуры дел университета подразделения получают выписки из соответствующих разделов для использования в работе. Выписки регистрируются в журнале и передаются заведующим архивом ответственным по делопроизводству в подразделении под подпись. Наличие выписок из сводной номенклатуры дел университета обязательно в каждом подразделения.

Электронные письма – файл, формируемый адресантом с помощью почтового клиента, предназначенный для передачи адресату посредством электронной почты после получения изображения документа (электронного письма) на экране персонального компьютера переводятся в бумажный формат при помощи принтера [58].

Данные документы проходят прием, регистрацию и передаются ректору или проректорам для рассмотрения. Ректор или проректора, изучив полученные документы, ставят резолюцию, где указывают срок и исполнителей, которым через отдел документооборота и управления организационно-правовой работы университета передаются в структурные подразделения. В архив данная документация не сдается, в качестве самостоятельного документа, но может быть передана в составе пакета документов, подготовленного на основе данного электронного сообщения.

Электронная почта используется для передачи сообщений структурным подразделениям как внутри университета, так и между различными организациями, имеющими соответствующие аппаратные и программные средства, фиксация отправленных сообщений по средствам электронных писем на бумажном носителе не ведется.

Факсимильные сообщения отправляются только для полностью оформленных и вступившие в действие документов. Отправляемые документы должны быть выполнены черным цветом, иметь четкое и контрастное изображение. В нижнем левом углу лицевой стороны последнего листа документа должна быть указана фамилия и номер телефона исполнителя.

Факсограммы на иностранных языках отправляются при наличии перевода, заверенного лицом, подписавшим факсограмму. Тексты документов с пометкой «Для служебного пользования» передавать запрещается [58].

Официальные документы, предназначенные для отправки, подлежат регистрации в журнале писем. После передачи информации подлинники документов возвращаются исполнителю.

Поступившие в отдел документооборота управления организационно-правовой работы факсограммы считаются входящей корреспонденцией и фиксируются как подлинник документа и направляется в соответствующее подразделение – исполнитель.

Электронные копии документов хранятся на персональных компьютерах сотрудников организации, сетевых папках, электронной почте, информационных системах и серверах организации, находящихся на территории университета или клинических базы.

Охрану специальных помещений университета, находящихся на территории университета осуществляют: Общество с ограниченной ответственностью Частная охранная организация «СпецОхрана», контракт

№93/2018 от 16.11.2018, Общество с ограниченной ответственностью Частная охранная организация «Ягуар», контракт №94/2018 от 07.12.2018.

Охрану специальных помещений университета, находящихся вне территории кампуса осуществляют организации на территории, которых находятся клинические базы на основании договоров, заключенных между университетом и клиническими базами.

Анализ состояния разработанности информационной системы электронного документооборота университета показал наличия ряда отклонения от классического электронного документооборота.

В организации смешанный тип с привилегией бумажного варианта, что затрудняет процессы направленные, на повышение качества образовательного процесса и упрощения работы научно-педагогического и административного персонала, совершенствование контроля успеваемости обучающихся, упорядочение хранения и использования документации, а также процессов коммуникаций между участниками внутри и вне университета.

Одним из немаловажных фактов, замедляющих процессы, является отсутствие полноценного электронного архива, существуют частичный переход от бумажных библиотек к электронным хранилищам документов. Реализован он только при хранении научных изданий и учебно-методической литературы по средствам система автоматизации библиотеки.

Университет проводит научные исследования, данный процесс сопровождаются большим количеством документации, и без использования полноценной системы электронного документооборота добиться высоких показателей производительности достаточно сложно.

Структуризация процессов, протекающих в электронной информационно-образовательной среде, контроль работы персонала, безопасное хранение документов, оптимизация создания документации – это задачи, которые частично решены, но в существующей системе

электронного документооборота недоучтена как внутренняя структуру университета, так и специфические особенности процессов. Остро стоит проблема гармоничной интеграции, необходимости введение дополнительных ограничений, требований к информационным системам, пересмотра подходов к проектированию, разработке и использованию системы электронного документооборота.

В настоящее время не только программные продукты оказывают существенное влияние на функционирование системы документооборота, но и участники процессов: пользователи, документы и операции, производимые с ними. Постоянное исследование внутренних процессов движения документации внутри университета, поиск закономерностей и выявление правил необходим для создания общей стабильности, качества и удовлетворенности пользователей работой электронной информационно-образовательной среды.

Для решения выявленных проблем было принято решение о разработке и реализации проекта по созданию информационной системы электронного документооборота, в котором основной информационной системой, которая объединит все процессы, связанные с движением и хранением документов будет: система автоматизации электронного документооборота и делопроизводства «1С: Документооборот» (далее - СЭД).

Данный проект разрабатывается и реализуется с привлечением организаций-подрядчиков, экспертов, имеющих опыт в данной сфере.

В рамках технического задания выделены функциональные контуры:

1. Регистрация входящих, исходящих, внутренних документов.

2. Управление договорной деятельностью.

3. Управление организационно-распорядительной документацией (приказы, распоряжения, локальные нормативные акты, справки и др.).

4. Претензионная работа.

5. Служебные записки.

6. Совещания и протоколы.

7. Поручения и их исполнение.

8. Интеграция с другими информационными системами.

9. Электронный архив документов.

10. Внедрение электронной подписи.

11. Контроль исполнительской дисциплины в рамках процессов согласования, подписания и исполнения документов.

12. Прогнозирование угроз информационной безопасности системы электронного документооборота.

13. Подбор и внедрением методов обеспечивающих информационной безопасности системы электронного документооборота.

14. Контроль соблюдения методов обеспечивающих информационную безопасность системы электронного документооборота.

Сформулирована цель создания системы и поставлены задачи, которые должна решать выбранная информационная система.

Система электронного документооборота разрабатывается с целью повышение эффективности работы университета. Достичь этого возможно будет за счет сокращения времени исполнения процессов; прозрачности процесса согласования; обеспечения основных требований по достоверности, целостности и актуальности информации; улучшения контроля исполнительской дисциплины [80].

Система документооборота должна решать следующие задачи:

− регистрация и хранение копий документов.

− обеспечение полного жизненного цикла документов.

− поддержка свойства многопользовательской работы с документами.

− хранение документов в базе, с возможностью поиска.

− возможность реализации механизма согласования документов по заданному маршруту.

− возможность создания системы поручений.

− создание аналитических отчетов.

− интеграция с различными информационными системами.

− обеспечения информационной безопасности.

Определены требования к системе, по следующим параметрам:

− к структуре и функционированию системы;

− к численности и квалификации персонала;

− информационному обеспечению системы;

− к аппаратно-программному обеспечению;

− к функциональным блокам.

Требования к структуре и функционирования системы:

Система должна функционировать на базе программного обеспечения с открытым исходным кодом, и поддерживать возможность работы с MS SQL Serve. Обеспечивать возможность подключения к системе с использованием технологии WEB-доступа и содержать интеграционные механизмы, позволяющие включить данную систему в единое информационное пространство университета и предусматривать развитие по трем направлениям:

− территориальное масштабирование;

− функциональное масштабирование;

− наращивание аппаратных ресурсов.

Требования к численности и квалификации персонала:

В процессе внедрения и на этапе опытной эксплуатации должно быть проведено обучение персонала.

Требования информационному обеспечению системы:

Система должна быть сдана в опытную эксплуатацию с реализованным механизмом разграничения прав доступа.

Настроенным регламентом резервного копирования и восстановления данных.

Требования к аппаратно-программному обеспечению:

Количество одновременно работающих пользователей до 150 человек. Количество пользователей при пиковой нагрузке 550 человек. Конфигурация – «1С:Документооборот КОРП». Платформа – «1С:Предприятие 8.3».

Для работы СЭД должен использоваться программно-аппаратный комплекс, которые закупает заказчик с учетом рекомендации организации подрядчика.

Требования к функциональным блокам:

1. Входящие документы.

2. Исходящие документы.

3. Управление внутренними документами.

Внедряемые функциональные блоки системы электронного документооборота должны функционировать в соответствии со схемами, представленными в Приложениях 1-3.

В данном параграфе была рассмотрена существующая система документооборота в ФГБОУ ВО ЮУГМУ Минздрава России. Проанализированы её сильные и слабые стороны. На основе данного анализа было принято решение о необходимости внедрения полноценной системы электронного документооборота при помощи «1С:Документооборот», который будет не только организовать электронный документооборот, но и позволит связать между собой различные информационные системы университета. Это наладит процессы, обеспечить контроль исполнения задач, регламентирует управленческую деятельность и повысить ее эффективность.

2.2 Прогнозирование угроз информационной безопасности системы электронного документооборота (на примере ФГБОУ ВО ЮУГМУ Минздрава России)

Внедрение системы электронного документооборота позволит изменить подход к делопроизводству в университете, сделать ее более гибкой в отношении обработки и хранения документов. В тоже время появление новой системе в едином информационном пространстве породит новые риски, которые могут привести к новым угрозам конфиденциальности [40].

Базовым элементом любой системы документооборота является документ, в электронной системе это файл или запись в регистре. При формировании требований к защищенности от информационных угроз часто подразумевают только защиту документов и защиту информации, которую они содержат. При таком подходе все сводится к защите данных от несанкционированного доступа.

Но данный подход не покроет все угрозы, так как система электронного документа оборота это не только документы, но система обеспечивающая функционирование различных процессов, связанных с делопроизводством и именно систему в целом необходимо защищать, а не только данные внутри нее.

Базируюсь на данном подходе, при формировании требований, необходимо помимо задач, связанных с защитой данных, ставить задачи по защите работоспособность системы, обеспечению быстрого восстановление после повреждений, сбоев и уничтожения.

Все требования можно разделить на требования к:

− аппаратным элементам систем (серверы, элементы компьютерной сети и сетевое оборудование);

− файловой системе (файлы программного обеспечения и базы данных);

− документам и информации, находящиеся внутри системы.

При формировании системы защиты необходимо предусмотреть угрозы, связанные с поломкой и доступом к оборудованию, отключения питания и иные ситуации. Проработать варианты возможного влияния злоумышленников или обстоятельствами на файлы из вне. Разработать механизм подтверждение авторства и юридической значимости, контроля целостности и конфиденциальности документов [35].

Использование данных методов позволит спрогнозировать угрозы на каждом из уровней и построить систему с их учетом.

При прогнозировании угроз, которые могут наступить при использовании системы электронного документооборота в ФГБОУ ВО ЮУГМУ Минздрава России, были взяты за основу стандартные угрозы и классифицированы следующим образом:

– угроза целостности;

– угроза конфиденциальности;

– угроза работоспособности системы.

Данные угрозы могут привести к повреждению, уничтожению или искажению информации, перехвату информации, изменению ее маршрутов следования, нарушению или прекращению работы системы как не намеренно, так и спланировано.

Источником перечисленных угроз могут быть ошибки пользователей, которых можно разделить на группы:

– легальные пользователи системы;

– административный персонал;

– внешние злоумышленники.

Пользователь системы - это потенциальный злоумышленник, он может сознательно или не сознательно нарушить конфиденциальность информации [26].

Легальные пользователи могут совершать ряд ошибок, которые носят различный характер. От повреждения аппаратных частей системы до кражи информации.

Административный персонал специализированных подразделений имеет неограниченные полномочия и доступ к данным, они являются более квалифицированными пользователями и могут совершать злодеяния, наносящие серьезный урон системе.

К внешним злоумышленникам можно отнести конкурентов, партнеров, обучающихся.

Для обеспечения защиты от данных угроз необходимо использовать средства защиты, встроенные в СЭД, сетевые устройства, компьютерные сети, файловые и операционные системы.

Выбранная университетом система электронного документооборота может обеспечить защиту от основных угроз: обеспечение сохранности документов, обеспечение безопасного доступа, обеспечение подлинности документов, протоколирование действия пользователей [27].

Для этого должен быть разработан регламент резервного копирования, описан механизм восстановление не только данных, но и самой системы в случае ее повреждения.

Безопасный доступ к данным внутри СЭД должен быть обеспечен аутентификацией. Пароли должны генерироваться по заранее определенному алгоритму, изменяться после первого входа пользователем, не сохраняться в памяти устройств, если они предназначены для использования совместно, не передаваться другим пользователям.

При разработке должна быть создана гибкая и детальная структура, предусматривающая разграничение прав пользователя. Предпочтительней реализовать комбинированный вариант: подсистема, созданная разработчиками СЭД и подсистема безопасности СУБД, которую использует СЭД.

Наибольший уровень защиты обеспечить криптографический метод защиты данных, который позволит не нарушать конфиденциальность документов.

Сотрудниками информационных подразделений должны быть разработаны организационные меры защиты: разработаны модели угроз, составлены инструкции по безопасному использованию информационной системы, проводиться первичные и повторные инструктажи.

Для обеспечения подлинности документов необходимо использовать электронно-цифровую подпись (далее - ЭЦП). При реализации данного механизма защиты необходимо руководствоваться Федеральным законом №63-ФЗ «Об электронной подписи» и подзаконными актами.

В системе должен быть реализован механизм протоколирование действий пользователей, который позволит отследить все неправомерные действия и найти виновника, а при оперативном вмешательстве даже пресечь попытку неправомерных или наносящих вред действий.

Абсолютных способов для обеспечения безопасности информационной среды от угроз не существует, систему защиты необходимо постоянно усовершенствовать, поскольку злоумышленники тоже усовершенствуют свои методики [29]. На сегодняшний день не существует универсальных способов, которые подходят каждому и дают стопроцентную защиту. Важно остановить проникновение злоумышленников на раннем уровне и тем самым снизить степень возможные варианты проявления ущерба.

2.3 Проектирование и разработка модуля выдачи справок в системе электронного документооборота в ФГБОУ ВО ЮУГМУ Минздрава России

В соответствии с выбранной стратегией движение и согласование основного потока документов будет реализовано через систему

электронного документооборота «1С:Документооборот». Информационные системы семейства 1С, имеющие механизм бесшовной интеграции будут объединены данным методом. Иные системы будут взаимодействовать между собой через обработки позволяющие создавать как одностороннее, так и двухстороннее взаимодействие.

В рамках проекта создания ЭДО было принято решение об автоматизации процесса заказа и выдачи справок обучающимися по средствам личного кабинета обучающегося и «1С:Университет ПРОФ». Причинами инициализации стали требования законодательства, эпидемиологическая ситуация и современные реалии.

Для реализации проекта была создана рабочая группа, состоящая из сотрудников университета и организации подрядчика, группа состояла из заказчика, руководителя проекта, процессного аналитика, аналитика данных, проектировщика структуры, специалиста по тестированию и программиста.

Для реализации стратегии был выбран метод SWOT-анализа, где были подробно рассмотрены сильные и слабые стороны планируемого к реализации проекта, определены возможности, которые откроются перед университетом после реализации с учетом выделенных угроз (таб.1).

Таблица 1 - SWOT-анализ деятельности ФГБОУ ВО ЮУГМУ Минздрава России

СИЛЬНЫЕ СТОРОНЫ (STRENGHT)	СЛАБЫЕ СТОРОНЫ (WEAKNESS)
− кадровое обеспечение (наличие специалистов); − наличие технической базы для создания продукта; − наличие реальной потребности; − комплексный подход к реализации проекта; − суперсервис.	− недостаточная квалификация пользователей; − отсутствие хранилища; − зависимость от точности данных; − уникальность специалиста.

Окончание таблицы 1

ВОЗМОЖНОСТИ (OPPORTUNITIES)	УГРОЗЫ (THREATS)
− возможности удаленного получения документов; − оптимизация бумажного документооборота; − переход к системе ЭДО; − повышение удовлетворенности потребителя; − освобождение времени для выполнения других видов работы сотрудниками подразделения; − возможность создания уникального продукта.	− задержка поставок технического оборудования; − отсутствие бюджетного финансирования.

На этапе анализа были выявленные проблемы:

− необходимость автоматизации процесса заказа и выдачи справок об обучении с целью высвобождения рабочего времени сотрудников для выполнения других видов работ;

− необходимость оптимизации бумажного документооборота, создание предпосылок для перехода к системе ЭДО и повышению уровня удовлетворенности потребителей.

Команда выбрала S-O действия, это стратегия роста, представляющая собой мероприятия или программы, использующие сильные стороны для охвата каждой из возможностей.

Конечным результатом проекта, как решением данных проблем является создание раздела «Справки (для студентов)» в «1С:Университет ПРОФ» и личном кабинете обучающегося.

После проведения анализа цель была переформулирована с использованием метода SMART. Данный подход к постановке целей помогает выбрать формулировку желаемого результата, дает чувство направления и помогает организовать и достичь целей.

Цель проекта: сокращение временных потерь обучающихся и сотрудников университета при получении и выдачи справок с 09.01.2022

года с применением личного кабинета обучающегося и «1С:Университет ПРОФ» в условиях обеспечения информационной безопасности.

Задачи, которые необходимо было решить для достижения поставленной цели:

- определение шаблонов справок;
- сбор и анализ данных, необходимых для формирования справок;
- описание процесса создания и выдачи справки;
- описание методов обеспечения информационной безопасности;
- реализация программными средствами;
- апробация и тестирование;
- внедрение, запуск и сопровождение.

Для реализации задач была применена теория управления стейкхолдерами. В данном проекте внешними являются обучающиеся, внутренними - сотрудники университета и организация подрядчик.

В настоящее время используется механизм вовлечения стейкхолдеров по стратегиям «Поддержка» и «Консультанты». В рамках данных стратегий стейкхолдеры вовлечены в процесс реализации проекта, в зависимости от их уровня важности и уровня влияния.

На основе ранее реализованных проектов университетом было принято решение о необходимости использования дополнительной стратегии - «Партнеры», которая заключается в максимальном вовлечении и применяется к стейкхолдерам с высоким уровнем важности и влияния. Принцип партнерства использовался в коммуникации при ведении переговоров по проекту с этой группой.

На первых этапах реализации проекта был описан процесс выдачи справки «как есть» (рис. 3).

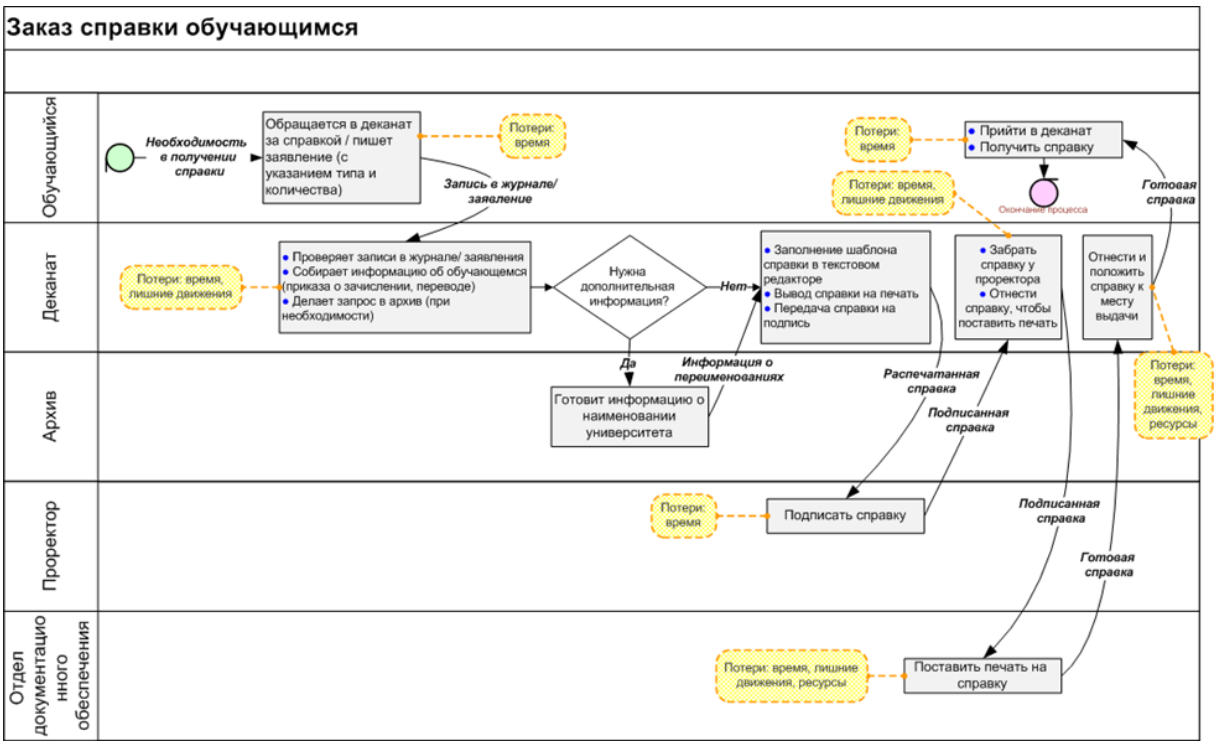

Рисунок 3 – Заказ справки обучающимся «Как есть»

Данный процесс является сложным из-за большого количества участников, что приводит к увеличению времени его протекания. Так же данный процесс является трудоемким для сотрудников, так как требует обращения к архивам, хранящимся на бумажных носителях.

Еще одним немаловажным фактором, способствующим переходу на электронный способ заказа и выдачи справок обучающимися, была сложившейся эпидемиологической ситуация. Министерство здравоохранения рекомендовало снизить уровень личных контактов между участниками различных процессов. В нашем случаи, это было возможно за счет изменения способа заказа и выдачи справок обучающимся.

После трансформации процесс заказа и выдачи справок значительно сократился по причине уменьшения количества участников данного процесса (рис. 4).

Рисунок 4 – Заказ справок обучающихся через личный кабинет

Это дало возможность:

− сократить сроки исполнения;

− уменьшить финансовые затраты;

− обеспечить необходимый уровень информационной безопасности;

− повысить уровень удовлетворённости всех участников существующего процесса.

Для реализации процесса автоматизации заказа и выдачи справок об обучении была разработана «Дорожная карта» (таб. 2).

Таблица 2 – «Дорожная карта» по достижению целевых показателей

Задачи	Мероприятия	Сроки	Отвеянные
Выявление потребностей; обследование состояния	Сбор данных о текущем состоянии; анализ данных; изучение опыта других организации	3 недели	Проректор, УМУ, УИТ
Создание технического задания	Написание ТЗ, корректировка, окончательное оформление	2 недели	Аналитики, тестировщики
Реализация	Создание программного продукта с использованием технических средств для реализации	1,5 месяца	УИТ, подрядчик
Тестирование, внедрение	Апробация, внедрение, сопровождение	2 недели ...	Тестировщик

В ней выделены задачи, спланированы мероприятия для исполнения задач, определены сроки реализации с назначением ответственных лиц. На основании «Дорожной карты» был составлен проект финансового плана (таб. 3).

Таблица 3 - Проект финансового плана

Основные статьи расходов	Источники доходов/ финансирования	Прогноз по затратам	Выводы по эффективности задуманного
Техническое задание	Университет	ч/часы	сокращение временных затрат, ресурсов, мест хранения за счет автоматизации процесса, дружественность, масштабируемость, безопасность, перспективность
Создание ПП	Университет, подрядчик	тыс. руб	
Тестирование	Университет	ч/часы	
Обучение персонала	Университет, подрядчик	ч/часы	
Обслуживание		ч/часы	

При работе над проектом были учтены риски. Это вероятные для проекта события, наступление которых может как отрицательно, так и положительно отразиться на параметрах и результатах проекта.

Нами были выделены риски, которые могут носить отрицательный характер. К ним относятся:

- неверные и неполные первичные данные;
- уязвимость системы;
- недостаточность и несвоевременность финансирования;
- саботаж реализации проекта;
- наличие несоответствий внутренним нормативным документам;
- перебои с электричеством в университете;
- ошибки интеграции.

При работе с рисками необходимо учитывать влияние риска на проект и вероятность его наступление. Это дает возможность оперативно и

адекватно реагировать при его наступлении. В рамках проекта у обозначенных рисков были проанализированы причины, обозначены триггеры и определены последствия после их наступления (таб. 4).

Таблица 4 - Перечень рисков, влияющих на проект по разработке и проектированию модуля

Наименование	Причина	Триггеры	Последствия
Неверные и неполные первичные данные	Технические ошибки	Человеческий фактор (усталость, невнимательность)	Недостоверность данных, указанных в документе
Уязвимость системы	Программно-аппаратные ошибки, внешние атаки	Устаревшее оборудование, недостаточная квалификация работников	Полная или частичная потеря данных
Недостаточность и несвоевременность финансирования	Особенности бюджетного финансирования	Долгий процесс согласования	Приостановка проекта, срыв сроков выполнения, ограничение функционала
Саботаж реализации проекта	Отсутствие понимания среди работников, страхи	Наличие жалоб и недовольство работников	Неработоспособность ПП
Наличие несоответствий внутренним нормативным документам	Несогласованность действий различных подразделений	Наличие нескольких ответственных лиц, не оперативный обмен информацией	Документ, требующий переоформления, недействительный, срыв сроков

В процессе реализации проекта команда подготовила ряд мер, которые могли бы обеспечить серию «быстрых побед»:

− удаление лишних этапов из процессов (уменьшение количества участников, «живых обращений»);

− трансформация неэффективных процедур/процессов (создание электронного реестра, перенос информации из электронного реестра путем печатных форм в архив);

− улучшение коммуникации между участниками процесса (обучающийся и сотрудник подразделения);

− уменьшение издержек (сокращение расходов на канцелярию);

− использование доступных функций программного обеспечения, которые не использовались ранее (обращение через ЛК).

Данные меры позволили в короткие сроки показать ощутимый результат пользователю и повысить его лояльность к трансформации существующих процессов. При подготовке данных мер необходимо учитывать особенности отрасли, в которой реализуется данный проект. Без учета уровня влияние невозможно создать проект, который бы на 100% покрывал все потребности заказчиков, а в дальнейшем и пользователей.

В нашем проекте отраслевыми особенностями являлись:

1. Особенности реализации образовательных программ медицинского и фармацевтического образования (ст. 82 ФЗ-273).

Особенность заключается ограниченности возможности переводов, обучающихся внутри укрупненных групп специальностей.

2. Множественность индивидуальных образовательных траекторий.

Особенность заключается в том, что данный факт влияет на итоговое содержание выдаваемого документа.

3. Моно - и полинаправленность образовательных программ разного уровня.

Особенность заключается в том, что, если неверно указаны специальности и продолжительность обучения, то будет неверно создан документ.

Уровень воздействия на проект отраслевых особенностей отражен в таблице 5.

Таблица 5 - Уровень воздействия на проект «Отраслевые особенностей»

Наименование	Степень проявления (0-10)	Уровень воздействия на проект (0-10)	Последствия (1 и 2 порядков)
Особенности реализации образовательных программ медицинского и фармацевтического образования (ст. 82 ФЗ-273)	10	5	2 - перевод внутри УГСН
Множественность индивидуальных образовательных траекторий	10	10	1 - влияние на итоговое содержание документа
Моно - и полинаправленность образовательных программ разного уровня	10	10	1 - неверно указаны специальности и продолжительность обучения и в результате неверно создан документ

Так же на протяжении всего жизненного цикла проекта должны реализовываться меры для формирования положительного имиджа.

Нами были выбраны следующие меры:

1. Создание коротких обучающих роликов о сервисе.

2. Информирование обучающихся посредством размещения информации о сервисе в личном кабинете, на сайте университета и в социальных сетях.

3. Регулярный аудит баз данных.

4. Актуализация обновлений системы.

5. Получение оценок обратной связи от пользователей сервиса.

6. Обмен опытом среди участников.

С учетом всех перечисленных мероприятий был создан модуль выдачи справок в системе электронного документооборота путем интеграции личного кабинета и «1С:Университет ПРОФ».

На рисунках 5 представлен раздел для заказа справок в личном кабинете обучающегося.

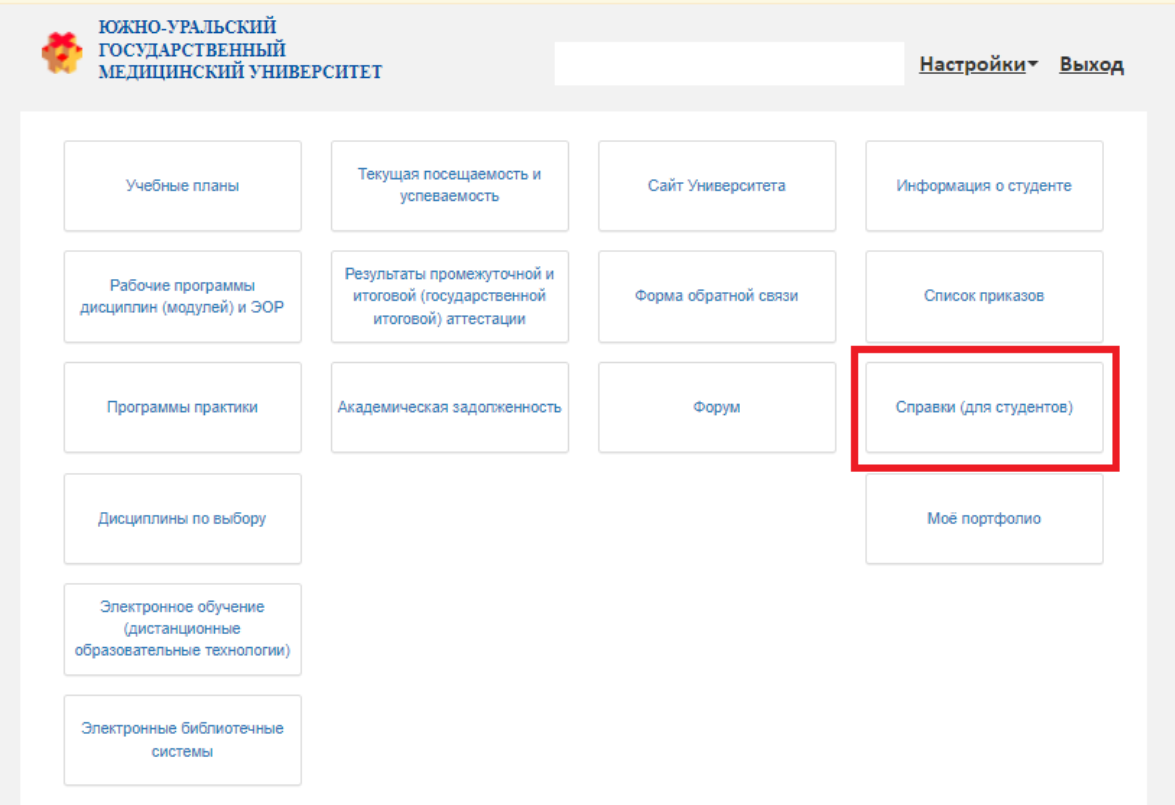

Рисунок 5 – Раздел «Справки (для студентов)» в личном кабинете

На рисунках 6 представлен непосредственно раздел для заказа справок в личном кабинете обучающегося по выбранным параметрам. В данном разделе обучающийся может отслеживать статус заказанной справки (рис. 6).

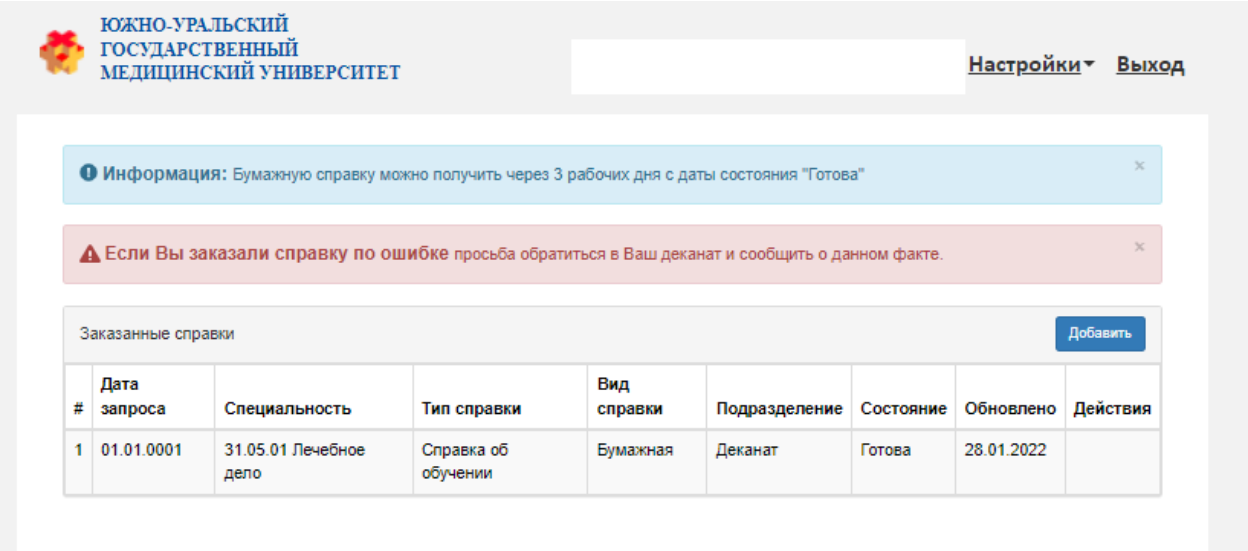

Рисунок 6 – Страница раздела для заказа и получения справок обучающимся

На рисунках 7 представлен раздел «Справки обучающихся» предназначенный для работы сотрудников университета. Данный раздел предполагает фиксацию информации о справках об обучении, которые выдаются двумя подразделениями (деканатами и учебным отделом).

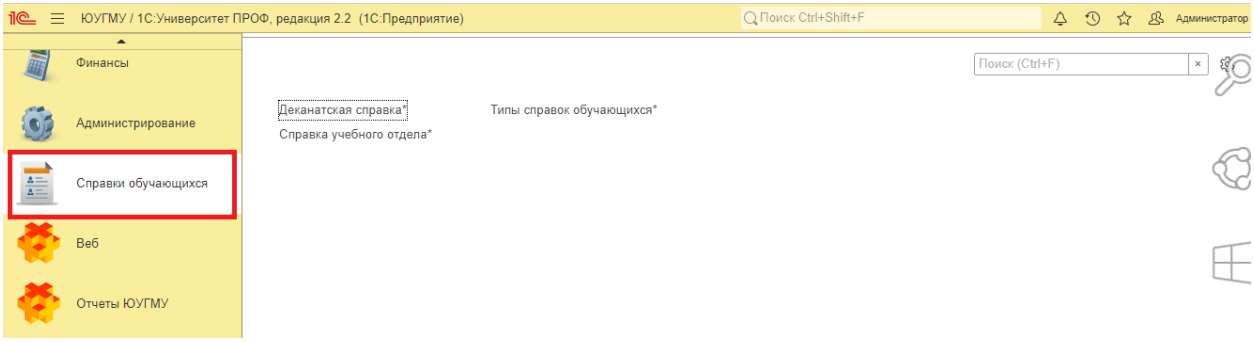

Рисунок 7 – Раздел «Справки обучающихся»

Деканат выдает справку о факте обучения в университете. На рисунке 8 представлен журнал, в котором фиксируются все заказанные и выданные справки.

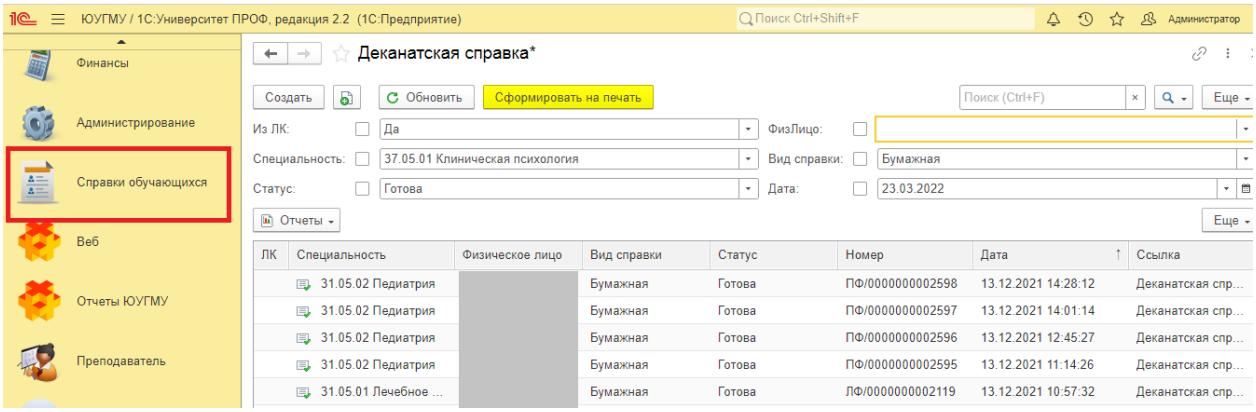

Рисунок 8 – «Деканатская справка»

Учебный отдел выдает справку о периоде обучения. На рисунке 9 представлен журнал, в котором фиксируются все заказанные и выданные справки.

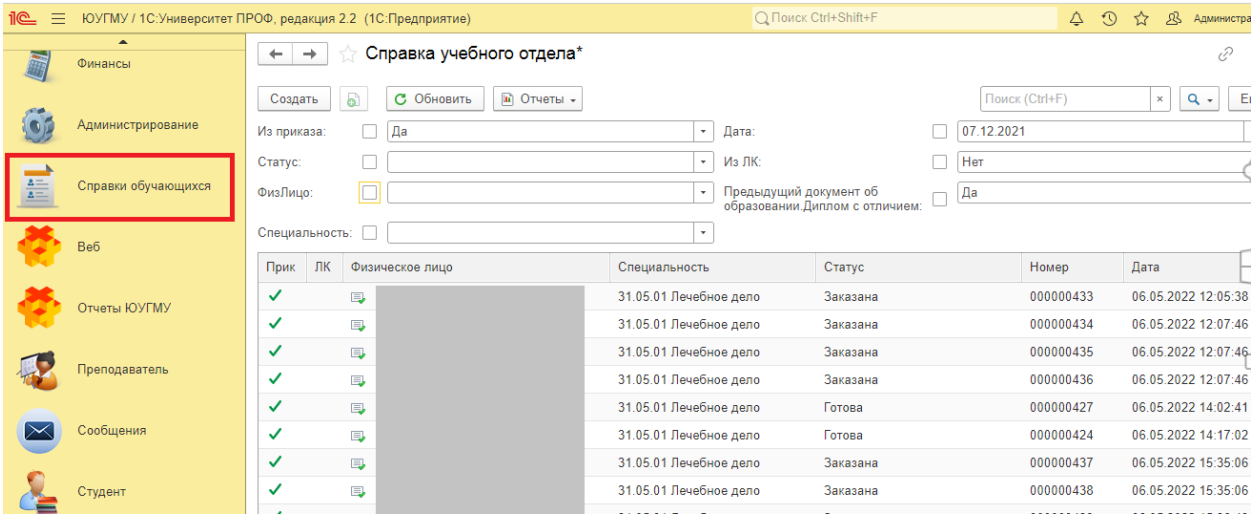

Рисунок 9 – «Справка учебного отдела»

Формирование справок о факте обучения в «1С:Университет ПРОФ» происходить двумя способами:

– запрос со стороны личного кабинета;

- в «1С:Университет ПРОФ» сотрудником деканата.

Формирование справок о периоде обучения в «1С:Университет ПРОФ» происходит тремя способами:

– запрос со стороны личного кабинета;

– автоматически после создания приказа на отчисление обучающегося;

- в «1С:Университет ПРОФ» сотрудником учебного отдела.

Процесс выдачи справок может быть осуществлен двумя способами:

− возврат справки в формате pdf подписанный ЭЦП;

− на бумажные носители.

Механика выдачи справок и шаблон справки деканатом представлены на рисунке 10.

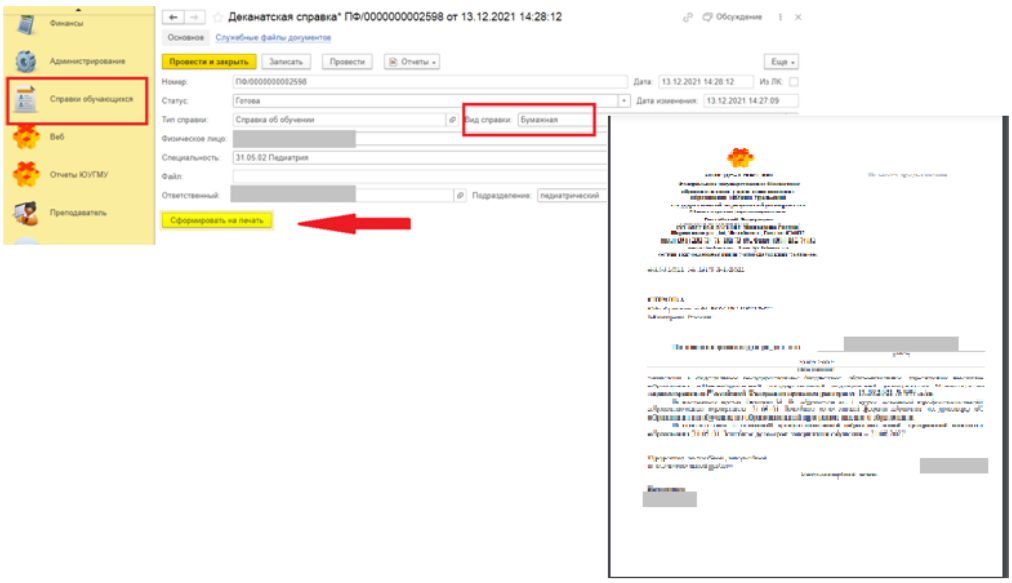

Рисунок 10 – Процесс выдачи справок деканатом

Механика выдачи справок и шаблон справки учебным отделом представлены на рисунке 11.

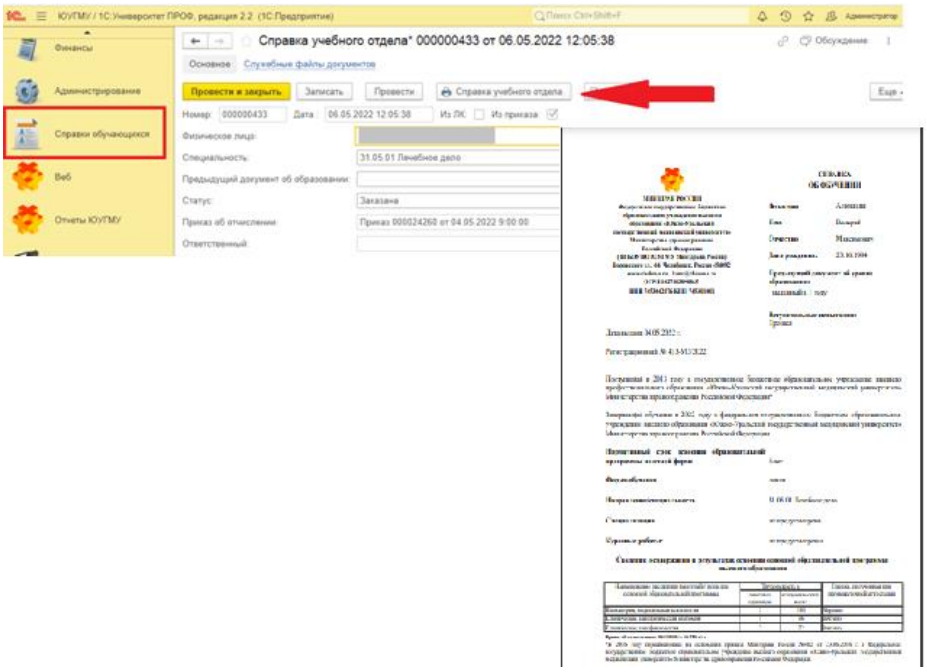

Рисунок 11 - Процесс выдачи справок учебным отделом

В настоящее время справки выдаются только вторым способом, так как процесс выдачи справок путем возврата, в личный кабинет обучающегося с ЭЦП программно реализован, но не утвержден документально в университете.

При реализации данного модуля были соблюдены условия информационной безопасности. Для обмена данными между личным кабинетом и «1С:Университет ПРОФ» приобретен SSL-сертификат.

SSL-сертификат - это цифровая подпись сайта. С её помощью подтверждается его подлинность. Перед тем как установить защищённое соединение, браузер запрашивает этот документ и обращается к центру сертификации, чтобы подтвердить легальность документа. Если он действителен, то браузер считает этот сайт безопасным и начинает обмен данными [41].

Обмен данными происходит по протоколу https. Это безопасный протокол передачи данных, который поддерживает шифрование посредством криптографических протоколов SSL и TLS, и является расширенной версией протокола HTTP [41].

В «1С:Университет ПРОФ» встроен механизм «настройки пользователей и прав», с помощью которого обеспечивается защита персональных данных в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и ведется учет обращений к ним.

Применены разработанные и утвержденные в университете модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных «Обучающиеся и абитуриенты», «Сотрудники».

Разработаны инструкциии по работе с модулем выдачи справок в системе электронного документооборота.

Подготовлен обучающий курс по обучению пользователей правилам работы с средствами криптографической защиты информации (Приложение 4), который необходимо будет пройти сотрудникам, которые будут подписывать справки ЭЦП.

Проектирование и разработка модуля выдачи справок в системе электронного документооборота в ФГБОУ ВО ЮУГМУ Минздрава России была реализована в установленные регламентом сроки, но представленный вариант не является итоговым. Данный модуль проходит стадию опытной эксплуатации, которая будет длиться до 30.06.2022 года. В данный период будут собрана информация о работе данного модуля путем анкетирования пользователей, анализа обращений в техническую поддержку и итогов встреч рабочей группы.

На основании полученных данных будет разработана программа по устранению обнаруженных недочетов и совершенствованию функциональных возможностей.

2.4 Оценка эффективности модуля выдачи справок в системе электронного документооборота в ФГБОУ ВО ЮУГМУ Минздрава России

Эффективность проекта – это такая мера соответствия проекта ожидаемым целям, задачам и выгодам всех сторон, которые принимали участие в его оценки и реализации.

В целях определения меры соответствия применяется оценка эффективности проекта.

Оценка эффективности проекта – это процедура расчета затрат и анализа капитальных затрат на исполнение проекта и итоговых достижений, показывающая, насколько он отвечает намеченным ориентирам и планам участвующих сторон [45].

Можно оценивать проект по двум показателям:

– эффективность проекта в целом;

– эффективность участия в проекте.

Целью проекта было проектирование информационной системы для электронного документооборота образовательной организации в условиях обеспечения информационной безопасности.

Достижение данной цели должно способствовать повышение эффективности работы университета.

Предполагается сокращения сроков протекания и повышения прозрачности процессов. Обеспечения высокого уровня достоверности, целостности и актуальности согласуемой информации.

Повышение эффективности исполнения заданий и документов, за счет улучшения контроля исполнительской дисциплины.

Все это планировалось достичь через поставленные перед внедряемой системой задачи.

Для эффективной реализации задач были выделены функциональные контуры, одним из которых является «Управление организационно-

распорядительной документацией (приказы, распоряжения, локальные нормативные акты, справки и др.)».

В рамках данного контура был реализован проект по проектированию и разработке модуля выдачи справок в системе электронного документооборота в ФГБОУ ВО ЮУГМУ Минздрава России, эффективность которого и будет оценена в данном параграфе.

Оценка эффективности проекта будет производиться по показателю эффективность проекта в целом:

1. После внедрения данного модуля сократился срок протекания процесса заказа и выдачи справок с трех до одного рабочего дня из-за уменьшения количества участников, которым требовалось время для решения поставленных задач в рамках данного процесса. Количество участников до реализации проекта пять, после два.

2. Повысилась прозрачность процесса согласования документа за счет уменьшения количества участников и обращения к системе за архивной информацией об обучающимся.

3. Уменьшилось количество времени и трудозатрат на подготовку и поиск необходимых документов. Система обращается к данным в базе «1С:Университет ПРОФ». Нет необходимости использовать бумажные архивы. Время формирование справки при обращении к базе 30 секунд, обращение к бумажным архивам занимало до 2 рабочих дней.

4. Повышения эффективности исполнения заданий и документов за счет:

– автоматизации процесса, способствующего уменьшения затрачиваемого времени на заказ, формирования и выдачи справок;

– уменьшения количества ошибок, связанных с искажение и неполной данных, путем шаблонизации форм справок и обращений к базе.

5. Улучшения контроля исполнительской дисциплины за счет внедрения системы состояний справок (Заказана, Готова) и фиксации даты и времени изменения состояний.

6. Повышения уровня информационной безопасности за счет перехода на заказ и выдачу справок через личный кабинет обучающегося и 1С:Университет ПРОФ», которые спроектированы с учетом всех информационных угроз и применением необходимых программных средств защиты и проходит регулярный контроль в соответствии с разработанной в университете инструкцией.

С 2020 года существовало два способа заказа и выдачи справок:

− личное обращение в деканат (официально закрепленный);

− заказ справок был возможен по средствам электронный почты, который не обеспечивает достаточный уровень информационной безопасности.

7. Формирование имиджа цифровой трансформации.

При реализации проекта рабочая группа придерживалась принципов работы с имиджем цифровой трансформации и понимала, что она является частью системы государственной трансформации, которая с каждым годом приобретает большую значимость и актуальность.

В этих условиях формируется образ нового, «цифрового» университета и всё больше возрастает научно-исследовательский интерес к проблемам формирования позитивного цифрового имиджа образовательных организаций.

Реализуемый проект частично разрешил имеющиеся проблемы в университете и поставленные задачи в сфере цифровой трансформации в управлении и развитии, так как носит практическую значимость, которая обоснована и достигает социального или экономического эффекта, как для самого университета, так и для системы образования в целом.

Положительным эффектом от реализации является улучшение процессов и показателей работы образовательной организации (таб. 6).

Таблица 6 – Основные принципы работы с имиджем цифровой трансформации

Как можно использовать проект для формирования имиджа ЦТ	Какие способы возможно использовать для формирования имиджа ЦТ	На что следует особо обратить внимание при формирования имиджа ЦТ
– способствует продвижению внедрения цифровых технологий в повседневную деятельность университета; – совершенствованию цифровой инфраструктуры, цифровизации административно-управленческих процессов; – способствует переходу к управлению на основе данных.	Цифровизация процесса получения справок.	Качество создаваемых цифровых услуг, инфраструктуры

8. Переход к управлению на основе данных. Данная технология является новой в управленческой деятельности. Носителями этой технологии становятся не только эксперты, консультанты и аналитики образования, но и управленцы, государственные служащие, то есть специалисты, принимающие решения в системе образования.

Технология анализа больших данных и управления на основе данных – одна из сквозных технологий Национальной технологической инициативы, задачи которой интегрированы в национальные проекты «Образование» и «Наука» [29].

Данные показатели позволяют утверждать об эффективности внедренного модуля. Но для закрепления убежденности в рамках исследовательской работы мы приняли решение о необходимости подкрепления достоверности пункта шесть - «Повышения уровня информационной безопасности» методом экспертной оценки, так как

основным условием нашей работы было проектирование информационной системы в условиях обеспечения информационной безопасности.

Экспертная оценка – основана на компетентном мнении экспертов, знающих данную область и имеющих научно-практический потенциал для принятия решения [35].

В процессе проведения экспертизы, условия информационной безопасности оценивались по следующим критериям:

1. Нормативно-правовая составляющая: соответствие требованиям действующих в России законодательных и нормативных документов по обеспечению безопасности данных.

2. Содержательная и функциональная валидность реализованных мер, полнота их разработанности.

3. Технологическая составляющая: характер предложенных технических и физических мер защиты данных.

Данные критерии были преобразованы в информационно-оценочную карту, которая представлена в таблице 6.

Перед проведением экспертизы была согласована система баллов, которые выставлялись экспертом при заполнении информационно-оценочной карты. Это было сделано для того, чтобы получаемая оценка обладала свойством надежности. То есть, чтобы разные эксперты, получив одни и те же данные, используя единую систему баллов и методы для их анализа, приходили к близким или одинаковым выводам.

Таблица 6 – Показатели оценки эффективности условий информационной безопасности при проектировании и разработке модуля выдачи справок в системе электронного документооборота в ФГБОУ ВО ЮУГМУ Минздрава России

Показатели оценки эффективности	**Эксперты**		
	Эксперт 1	Эксперт 2	Эксперт 3
	Критерии качества эффективности: высокий уровень (полностью соответствует показателю) средний уровень (в основном соответствует показателю) низкий уровень (в основном не соответствует показателю)		
1. Нормативно-правовая составляющая: соответствие требованиям действующих в России законодательных и нормативных документов по обеспечению безопасности данных.			
2. Содержательная и функциональная валидность реализованных мер, полнота их разработанности.			
3. Технологическая составляющая: характер предложенных технических и физических мер защиты данных.			
Итоговая оценка экспертов:			

Каждому эксперту был предоставлен доступ к модулю заказа и выдачи справок и информационно-оценочный лист с одинаковыми показателями оценки.

По итогам оценки эксперт представляет отчет, который содержит следующие сведения:

– заполненную информационно-оценочную карту;

– общие выводы.

В состав экспертной комиссии вошли: начальник управления информационных технологий, начальник учебного отдела учебно-методического управления, представитель от деканатов в лице заместителя

декана лечебного факультета, который является одним из самых многочисленных по контингенту.

Результаты экспертной оценки представлены в таблице 7.

Таблица 7 – Результаты экспертной оценки эффективности модуля заказа и выдачи справок обучающимся

Показатели оценки эффективности	Эксперты		
	Эксперт М.И.	Эксперт К.С.	Эксперт З. Г.
	Критерии качества эффективности: высокий уровень (полностью соответствует показателю) средний уровень (в основном соответствует показателю) низкий уровень (в основном не соответствует показателю)		
1. Нормативно-правовая составляющая: соответствие требованиям действующих в России законодательных и нормативных документов по обеспечению безопасности данных.	Высокий уровень	Высокий уровень	Высокий уровень
2. Содержательная и функциональная валидность реализованных мер, полнота их разработанности.	Средний уровень	Средний уровень	Высокий уровень
3. Технологическая составляющая: характер предложенных технических и физических мер защиты данных.	Высокий уровень	Средний уровень	Высокий уровень
Итоговая оценка экспертов:	*Высокий уровень эффективности условий обеспечения информационной безопасностью внедренного модуля*		

Результаты экспертной оценки эффективности представлены на результирующей диаграмме (рис. 11).

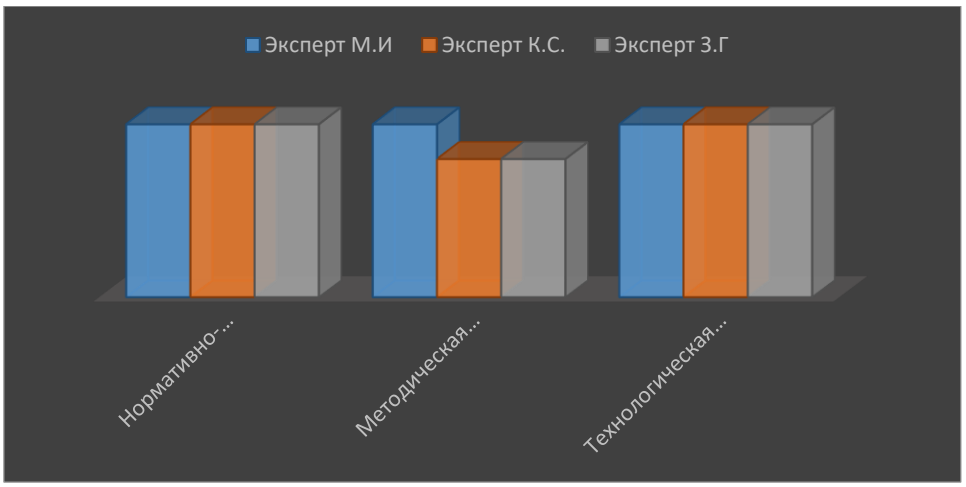

Рисунок 11 – Сводные результаты экспертной оценки эффективности условий информационной безопасности модуля заказа и выдачи справок обучающимся

Проведенный анализ позволяет сделать вывод, что мнения экспертов относительно совпадают и используемые условия являются эффективными для обеспечения информационной безопасности в процессе заказа и выдачи справок обучающимся.

Проект по проектированию и разработке модуля выдачи справок в системе электронного документооборота в ФГБОУ ВО ЮУГМУ Минздрава России, реализованный в рамках проекта по разработке и реализации проекта информационной системы электронного документооборота в условиях обеспечения информационной безопасности в ФГБОУ ВО ЮУГМУ Минздрава России создан и реализуется не только для автоматизации существующих процессов, но и для использования накопленных данных в принятия управленческих решений. А любые решения должны быть подкреплены безопасными и проверяемыми данными, так как успех данного подхода, зависит от качества собранных данных и эффективности их анализа и интерпретации.

ВЫВОДЫ ПО ВТОРОЙ ГЛАВЕ

По итогам второй главы магистерской диссертации можно сделать следующие выводы:

1. В первом параграфе была рассмотрена существующая система документооборота в ФГБОУ ВО ЮУГМУ Минздрава России. Проанализированы её сильные и слабые стороны. На основе данного анализа было принято решение о необходимости внедрения полноценной системы электронного документооборота при помощи «1С:Документооборот», который будет не только организовать электронный документооборот, но и позволит связать между собой различные информационные системы университета. Это наладит процессы, обеспечить контроль исполнения задач, регламентирует управленческую деятельность и повысить ее эффективность.

2. При разработке системы документооборота необходимо создавать условия для обеспечения информационной безопасности. Абсолютных способов не существует, систему защиты необходимо постоянно усовершенствовать, поскольку злоумышленники тоже усовершенствуют свои методики. На сегодняшний день не придуман универсальный способ, который подходит каждому и дает стопроцентную защиту. Важно остановить проникновение злоумышленников на раннем уровне и тем самым снизить степень возможных вариантов проявления ущерба.

3. В рамках магистерской диссертации по проектирование информационной системы для электронного документооборота образовательной организации в условиях обеспечения информационной безопасности подробно был рассмотрен процесс проектирования и разработки модуля выдачи справок в системе электронного документооборота в ФГБОУ ВО ЮУГМУ Минздрава России. Он был реализован в установленные регламентом сроки, но представленный вариант не является итоговым. Данный модуль проходит стадию опытной

эксплуатации, которая будет длиться до 30.06.2022 года. В данный период будут собрана информация о работе данного модуля путем анкетирования пользователей, анализа обращений в техническую поддержку и итогов встреч рабочей группы.

На основании полученных данных будет разработана программа по устранению обнаруженных недочетов и совершенствованию функциональных возможностей.

4. Проект по проектированию и разработке модуля выдачи справок в системе электронного документооборота в ФГБОУ ВО ЮУГМУ Минздрава России создан и реализуется не только для автоматизации существующих процессов, но и для использования накопленных данных в принятия управленческих решений. А любые решения должны быть подкреплены безопасными и проверяемыми данными, так как успех данного подхода, зависит от качества собранных данных и эффективности их анализа и интерпретации.

ЗАКЛЮЧЕНИЕ

Информационная безопасность основана на предупредительных действиях, они позволяют защитить информацию и оборудование от угроз и использования их уязвимых мест.

За годы использования информационных систем в различных сферах деятельности было установлено, что объединение всех способов защиты может обеспечить максимальный уровень защищенности.

Надежная физическая защита обеспечивает сохранность материальных активов. Защита коммуникаций позволяет обеспечить безопасность при передаче информации. Защита излучения необходима, если есть вероятность прочтения электронной эмиссии от компьютерных систем. Компьютерная безопасность ограничивает доступ в компьютерных системах, а безопасность сети доступность к локальным сетям. В совокупности все виды защиты обеспечивают информационную безопасность информационного пространства образовательной организации.

Высокий уровень безопасности достигается через повседневную практику, постоянную бдительность, анализ наступивших событий и изучение практик других участников глобального информационного пространства.

Использование опыта других участников позволит улучшить систему защиты, избежать или значительно уменьшить вероятность наступления событий, которые не были учтены при формировании требований к информационным системам в условиях информационной безопасности.

Нельзя полагаться на один вид защиты для обеспечения безопасности информационного пространства в целом или отдельной информационной системы. Не существует и продукта, который реализует все способы защиты.

Многие разработчики претендуют на то, что их продукт может справиться с задачей по обеспечению тотальной безопасности, но данное заявление легко подвергнуть критики, если опираться на минимальные требования к обеспечению уровня информационной безопасности. Для всесторонней защиты информационных ресурсов требуется множество различных продуктов.

Образовательная организация должна учитывать данный факт и при планировании расходов на создание системы электронного документооборота и закладывать необходимый финансовые ресурсы.

В рамках нашего исследования были проанализированы теоретические основы обеспечения информационной безопасности в образовательных организациях.

Рассмотрена теория об электронном документообороте как форме современного делопроизводства в образовательных организациях.

Изучены требования к проектированию систем электронного документооборота в условиях обеспечения информационной безопасности.

На основании полученных знаний нами был разработан проект информационной системы электронного документооборота в условиях обеспечения информационной безопасности в ФГБОУ ВО ЮУГМУ Минздрава России.

Спрогнозированы угрозы, которым может подвергнуться система электронного документа оборота в университете.

Введен в опытную эксплуатацию модуль выдачи справок в системе электронного документооборота в ФГБОУ ВО ЮУГМУ Минздрава России и проведена оценка эффективности использования внедренного модуля.

Оценка эффективности проводилась по показателю эффективность проекта в целом, которая позволила утверждать, что сократился срок протекания процесса заказа и выдачи справок, повысилась прозрачность процесса согласования документов, уменьшилось количество времени и трудозатрат на подготовку и поиск необходимых документов, улучшился

контроль исполнительской дисциплины и повысился уровень информационной безопасности.

При реализации проекта были учтены принципы работы с имиджем цифровой трансформации, которые позволяют формировать образ нового, «цифрового» университета и осуществлять переход к управлению на основе данных.

При данном способе управления любые решения должны быть подкреплены безопасными и проверяемыми данными. В нашем исследовании при проектирование системы электронного документооборота было принято решение о том, что конфигурация «1С:Документооборот» будет основополагающей системой в едином информационном пространстве университета и следовательно будет, является основным источником и инструментом для работы с данными и создание условий для обеспечения информационной безопасности является важнейшим критерием для определения успешности проекта.

Данный проект включен в общую стратегию развития университета до 2030 года. Проект является масштабным и поделен на части, в рамках нашего исследования был рассмотрен модуль заказа и выдачи справок, который является частью создаваемой системы. Одной из задач при реализации данного модуля была задача повышения уровня информационной безопасности за счет передачи и обработки данных в защищенном контуре.

По результатам выполненного исследования мы можем утверждать, что цель работы достигнута, задачи выполнены, гипотеза исследования подтвердилась.

ОСНОВНЫЕ ПОЛОЖЕНИЯ ДИССЕРТАЦИИ ОПУБЛИКОВАНЫ В СЛЕДУЮЩИХ РАБОТАХ

1. Статья. Рыскулова Е. В. «Заполнение данных в системе «1С: Университет ПРОФ»: типовые ошибки» / Рыскулова Е.В., Худякова О.Ю. В сборнике: Оптимизация высшего медицинского и фармацевтического образования: менеджмент качества и инновации. Материалы XII внутривузовской научно-практической конференции. 2021. С. 48-51.

2. Статья. Рыскулова Е. В. «Проблемы обеспечения информационной безопасности образовательной организации» Рыскулова Е.В., Уварина Н.В. В сборнике: НАЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ И МОЛОДЕЖНАЯ ПОЛИТИКА: КИБЕРСОЦИАЛИЗАЦИЯ И ТРАНСФОРМАЦИЯ ЦЕННОСТЕЙ В VUCA-МИРЕ. материалы Международной научно-практической конференции. Челябинск, 2021. С. 376-379.

3. Статья. Рыскулова Е. В. «Мотивирование сотрудников образовательной организации на соблюдение информационной безопасности» Чераева О.А., Рыскулова Е.В., Якупов О.А.В сборнике: МОДЕЛИ И МЕТОДЫ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ИННОВАЦИОННЫХ ИССЛЕДОВАНИЙ. Сборник статей по итогам Международной научно-практической конференции. Стерлитамак, 2021. С. 70-74.

4. Научная статья. Рыскулова Е.В. «Проблема обеспечения информационной безопасности образовательных организаций в теории и практике педагогики» / Е.В. Рыскулова // Вестник совета молодых ученых и специалистов Челябинской области. - 2020. Т. 2, № 4 (31). - с. 69 – 72.

Статья. Рыскулова Е. В. «Новые возможности Электронной информационное образовательной среды университета» / Е. В. Рыскулова // В сборнике: Оптимизация высшего медицинского и фармацевтического образования: менеджмент качества и инновации. Материалы XI внутривузовской научно-практической конференции. 2020. С. 60-62.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

Нормативно – правовые акты

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020), URL - http://www.consultant.ru/. Дата обращения: 15.01.2022.

2. Гражданский кодекс Российской Федерации: ФЗ от 18 декабря 2006 г. № 230-ФЗ // СЗ РФ. - 2006. - №52. Ч. 1. Ст. 5496.

3. Доктрина информационной безопасности Российской Федерации от 09.09.2000: утверждена Президентом РФ В. Путиным // Известия. - 10 декабря 2002. - С.2.

6. О персональных данных: ФЗ от 27 июля 2006 № 152 - ФЗ // Бюллетень нормативных актов министерств и ведомств. - № 7. - 2006. - С.15.

7. Об архивном деле в Российской Федерации: ФЗ от 01 октября 2004 № 125 - ФЗ // Собрание актов Президента и Правительства РФ. - № 11. - С.12.

8. Об информации, информационных технологиях и о защите информации: федер. закон от 27 июля 2006 № 149 - ФЗ // СЗ РФ. – 2006. - №31

9. Об утверждении Перечня сведений конфиденциального характера от 06.03.97 № 188: указ Президента РФ // Собрание актов Президента и Правительства РФ. - 1993. - № 23. С.12 – 14.

11. Об утверждении положения о государственной системе защиты информации от иностранной технической разведки и от ее утечки по техническим каналам от 15.09.93 № 912 - 51: постановление Правительства РФ // Собрание актов Президента и Правительства РФ. - 1993. - № 15. - 125 с.

12. Об утверждении Положения о лицензировании деятельности по технической защите конфиденциальной информации от 30.04.02. № 290: постановление Правительства РФ // Собрание актов Президента и Правительства РФ. - 2002. - № 8. - С.102.

13. Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных: постановление Правительства РФ от 17 ноября 2007 г. № 781. URL - https://base.garant.ru/192223/. Дата обращения: 21.04.2022.

16. Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти: постановление Правительства РФ от 3 ноября 1994 г. № 1233. // Собрание актов Президента и Правительства РФ. - 1995. - № 10. - С.56.

17. Трудовой кодекс Российской Федерации: федер. закон от 30.12.2001 N 197-ФЗ (ред. от 25.05.2020). URL - https://clck.ru/B8yGj. Дата обращения: 14.12.2020.

18. ГОСТ Р 51141. - 98. Делопроизводство и архивное дело. Термины и определения. - М.: Изд-во стандартов, 2003.

19. ГОСТ РВ 50600-93. Защита секретной информации от технической разведки. Система документов. Общие положения. - М.: Изд-во стандартов, 1993.

20. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. – Введ. 2006-12-27. – М.: Изд-во стандартов, 2006. – 9 с.

21. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. – Введ. 2006-12-27. – М.: Изд-во стандартов, 2006. – 7 с.

22. ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности. Основные термины и определения. – URL: http://www.opengost.ru/iso/35_gosty_iso/35020_gost_iso/11522-gost-

r-53114-2008-zaschita-informacii.-obespechenie-informacionnoy-bezopasnosti.-osnovnye-terminy-i-opredeleniya.html. Дата обращения: 16.12.2020.

23. ГОСТ Р ИСО/МЭК 15408-2002. Методы и средства обеспечения безопасности критерии оценки безопасности информационных технологий (КОБИТ). Части 1, 3-5.

24. ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью.

25. ГОСТ Р ИСО/МЭК ТО 13335-3-2007. [Электронный ресурс]. - URL: http://www.opengost.ru/iso/13_gosty_iso/13110_gost_iso/4958-gost-r-iso_mek-to-13335-3-2007-it.-metody-i-sredstva-obespecheniya-bezopasnosti.-chast-3.-metody-menedzhmenta-bezopasnosti-informacionnyh-tehnologiy.html. Дата обращения: 16.12.2021.

Литература

26. Аскеров Т.М. Защита информации и информационная безопасность / под общ. ред. К.И. Курбакова. – М.: Российская экономическая академия, 2001. – 386 с.

27. Астахова Л.В., Завадский А.О. Особенности организации защиты персональных данных в образовательной организации // Вестник УрФО. Безопасность в информационной сфере. – 2013 – № 3(9). – С.4-10.

28. Бадьина А. Обработка, порядок хранения и передвижения персональных данных // Кадровик. Кадровое делопроизводство. 2012. №1. С. 162 – 171.

29. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка) [Электронный ресурс]: [Утверждена заместителем директора ФСТЭК РФ 15.02.2008 г.]. - Режим доступа: www.fstec.ru. Дата обращения: 15.01.2022.

30. Бархатова Е.Ю. Комментарий к Конституции Российской Федерации (постатейный). 2-е изд., перераб. и доп. Москва: Проспект, 2015. 272 с.

31. Богатырева, Ю.И. Информационная безопасность образовательных организаций: проблема и пути ее решения [Текст] / Ю.И. Богатырева // Новые информационные технологии в образовании, IX международной научно-практической конференции. 2016 Издательство: Российский государственный профессионально-педагогический университет (Екатеринбург), с. 125-130.

32. Бугров А. Международные стандарты для построения системы информационной безопасности / А. Бугров // Финансовая газета. - 2017. - №10.

33. Бурькова Е.В. Система защиты персональных данных в высшем учебном заведении // Интеллект. Инновации. Инвестиции. – 2017. – № 7. – С. 69-74.

34. Галатенко В.А. Основы информационной безопасности: курс лекций / В.А. Галатенко. URL - https://www.intuit.ru/studies/courses/10/10/info. Дата обращения: 20.10.2021.

35. Защита электронного документооборота. [Электронный ресурс]: Режим доступа: https://revolution.allbest.ru/programming/00779901_0.html Дата обращения: 08.01.2022.

36. Ильгова О. Этапы организации защиты ПДн в ОО (для администратора). – URL: https://help.dnevnik.ru/hc/ru/articles/203475268. Дата обращения: 16.12.2021.

37. Ильин К. Вопросы информационной безопасности при электронном документообороте / К. Ильин // Защита информации. INSIDE. - 2016. - № 4. - С.18 - 25.

38. Информационная безопасность образовательных учреждений. – URL: https://searchinform.ru/resheniya/otraslevye-resheniya/informatsionnaya-bezopasnost-obrazovatelnykh-uchrezhdenij/. Дата обращения: 11.05.2022.

39. Краснянский М.Н. Проектирование информационных систем управления документооборотом научно-образовательных учреждений: монография / М. Н. Краснянский, С. В. Карпушкин, А. В. Остроух и др. –

Тамбов : Изд-во ФГБОУ ВПО «ТГТУ», 2015. – 216 с. – 400 экз. – ISBN 978-5-8265-1477-1.

40. Контур Диадок. Безопасность электронного документооборота. [Электронный ресурс]: Режим доступа: https://kontur.ru/diadoc/spravka/21935-bezopasnost_elektronnogo_dokumentooborota. Дата обращения: 05.01.2022.

41. Кузнецова Т. В. Организация работы с персональными данными // Делопроизводство. 2011. №2. С. 3 – 8; Трудовое право. 2011. №5. С. 77 – 83.

42. Лушников А. Защита персональных данных работника: сравнительно-правовой комментарий гл. 14 Трудового кодекса РФ // Трудовое право. 2014. № 9. С. 93–101; № 10. С. 77–82. СПС «КонсультантПлюс», 2014. Версия 4015.00.09, сборка 208002 (дата обращения: 13.01.2022).

43. Медведева Т. М. О работе с персональными данными работников // Актуальные вопросы бухгалтерского учета и налогообложения. 2014. №21. С. 77 – 88.

44. Международный стандарт ИСО/МЭК 27001. Первое издание 2005-10-15. Информационные технологии. Методы защиты. Системы менеджмента защиты информации.

45. Мельник Н.Ю. Защита персональных данных в профессиональном образовании // Современные технологии: актуальные вопросы, достижения и инновации. – 2018. – С. 55-57.

46. Мельников, В.П. Информационная безопасность и защита информации [Текст]: учеб. пособие / В.П. Мельников, С.А. Клейменов, А.М. Петраков. – М.: Издательский центр «Академия», 2013. – 336 с.

47. Меры по защите от угроз нарушения доступности [Электронный ресурс]. - URL: www.sha-danis.narod.ru. Дата обращения: 20.12.2021.

48. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах

персональных данных (утв. ФСТЭК РФ 14.02.2008) Электронный документ. Режим доступа: http://fstec.ru/. Дата обращения: 20.12.2021.

49. Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке информационных системах персональных данных с использованием средств автоматизации [Электронный ресурс]: [Утверждены руководством 8 центра ФСБ России 21.02.2008 г. №149/54-144]. - Режим доступа: www.consultant.ru. Дата обращения: 15.01.2022.

50. Методические рекомендации по применению приказа Роскомнадзора от 5 сентября 2013 г. N 996 «Об утверждении требований и методов по обезличиванию персональных данных» (утв. Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций 13 декабря 2013 г.).

51. Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности (утв. ФСБ России 31.03.2015 N 149/7/2/6-432). Электронный документ. Режим доступа: http://docs.cntd.ru/document/420336137. Дата обращения: 16.01.2022.

52. Методические рекомендации по ограничению в образовательных организациях доступа обучающихся к видам информации, распространяемой посредством сети "Интернет", причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования (утв. Министерством просвещения РФ, Министерством цифрового развития, связи и массовых коммуникаций РФ, Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций 16 мая 2019 г.). Электронный документ. Режим доступа: https://www.garant.ru/products/ipo/prime/doc/72145832/. Дата обращения 06.08.2021.

53. Методический документ. Меры защиты информации в государственных информационных системах (утв. ФСТЭК России 11.02.2014). Электронный документ. Режим доступа: http://fstec.ru/. Дата обращения: 16.01.2022.

54. Методы организации защиты информации [Текст]: учебное пособие для студентов 3–4 курсов всех форм обучения направлений подготовки 230400.55, 230701.51, 090300.65, 220100.55 / Ю.Ю. Громов и др. – Тамбов: Изд-во ФГБОУ ВО «ТГТУ», 2013. – 80 с.

55. Милютина О.В. Особенности защиты информации в образовательном учреждении [Текст] / О.В. Милютина. – URL: http://www.fcoit.ru/internet_conference/information_security_training_process/features_information_security_in_an_educational_institution.php. Дата обращения: 10.12.2021.

56. Модели угроз информационной безопасности [Электронный ресурс]. - Режим доступа: www.arinteg.ru. Дата обращения: 19.12.2021.

57. Обеспечение безопасности в системах электронного документооборота [Электронный ресурс]: Режим доступа: https://it-iatu.ru/is/informacionnaya-bezopasnost-i-zaschita-informacii/obespechenie_bezopasnosti_v_sistemah_elektronnogo_dokumentooborota Дата обращения: 08.01.2022.

58. Официальный сайт ФГБОУ ВО «Южно-Уральский государственный медицинский университет» Министерства здравоохранения Российской Федерации. – URL: http://www.chelsma.ru/. Дата обращения: 16.05.2022.

59. Параскевов А.В., Левченко А.В., Кухоль Ю.А. Сравнительный анализ правового регулирования защиты персональных данных в России и за рубежом. // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета, 2015. – № 110. –С. 866-894.

60. Пилипенко В.Ф. Обеспечение комплексной безопасности в образовательном учреждении. Теория и практика [Текст] / В.Ф. Пилипенко, Н.В. Ерков, А.А. Парфенов. – М.: Издво «Айрис-пресс», 2006. – 192 с.

61. Постановление Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

62. Постановление Правительства РФ от 03.02.2012 N 79 (с изм. от 15.06.2016) «О лицензировании деятельности по технической защите конфиденциальной информации». [Электронный ресурс]. Режим доступа: http://www.garant.ru/. Дата обращения: 16.12.2021.

63. Постановление Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» // «Российская газета», № 200, 24.09.2008.

64. Привалов А.Н., Богатырева Ю.И., Романов В.А. Методологические подходы к организации безопасной информационно-образовательной среды вуза // Образование и наука. – 2017. – Т. 19. – № 4. – С. 169-183.

65. Привалов А.Н. Основные угрозы информационной безопасности субъектов образовательного процесса [Текст] /А.Н. Привалов, Ю.И. Богатырева // Известия Тульского государственного университета. Гуманитарные науки – Тула, 2012. Выпуск 3. – С. 427-431. информационной безопасности учащихся [Текст]: монография – Тула: ТулГУ, 2014. – 224 с.

66. Приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК России) Федеральной службы безопасности Российской Федерации (ФСБ России) Министерства информационных технологий и связи Российской Федерации (Мининформсвязи России) от

13 февраля 2008 г. N 55/86/20 г. Москва «Об утверждении Порядка проведения классификации информационных систем персональных данных» // «Российская газета», № 4637, 12.04.2008.

67. Приказ Федеральной службы по техническому и экспортному контролю, ФСБ России и Министерства связи и массовых коммуникаций РФ от 31 декабря 2013 г. № 151/786/461 «О признании утратившим силу приказа Федеральной службы по техническому и экспортному контролю, Федеральной службы безопасности Российской Федерации и Министерства информационных технологий и связи Российской Федерации от 13 февраля 2008 г. № 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных». - Режим доступа: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/110-prikazy/815-sovmestnyj-prikaz-fstek-rossii-fsb-rossii-i-minkomsvyazi-rossii-ot-31-dekabrya-2013-g-n-151-786-461. Дата обращения: 16.12.2021.

68. Приказ ФСБ России от 10 июля 2014 г. N 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в ИСПДн при использовании средств криптографической защиты информации» // «Российская газета» от 17 сентября 2014 г. N 211.

69. Приказ ФСТЭК России от 18.02.2013 N 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» // «Российская газета», № 107, 22.05.2013.

70. Проблемы внедрения системы электронного документооборота. [Электронный ресурс]: https://wiseadvice-it.ru/o-kompanii/blog/articles/ (дата обращения 10.05.2022).

71. Пугачев В.П. Руководство персоналом организации: учеб. пособие / В.П. Пугачев. - М.: Аспект-Пресс, 2015. - 279 с.

72. Роберт И.В., Козлов О.А. Концепция комплексной, многоуровневой и многопрофильной подготовки кадров информатизации образования. М.: ИИО РАО, 2005. 50 с. URL: https://docplayer.ru/86331326-Podgotovka-nauchno-pedagogicheskih-kadrov-informatizacii-obrazovaniya.html. Дата обращения: 15.04.2022.

73. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации [Электронный ресурс]: [Утвержден решением председателя Гостехкомиссии при Президенте РФ 30.03.1992 г.]. - Режим доступа: www.consultant.ru. Дата обращения: 17.12.2021.

74. Рыскулова Е.В. «Проблема обеспечения информационной безопасности образовательных организаций в теории и практике педагогики» / Е.В. Рыскулова // Вестник совета молодых ученых и специалистов Челябинской области. - 2020. Т. 2, № 4 (31). - с. 69 – 72

75. Сабанов А.А. Некоторые аспекты защиты электронного документооборота // Connect! Мир связи. – 2010. – № 7. – С. 62–64.

76. Терещенко Л. К. Отдельные вопросы применения законодательства о персональных данных // Комментарий судебной практики / под ред. К. Б. Ярошенко. М.: КОНТРАКТ, 2014. Вып. 19. С. 3 – 13.

77. Фионова Л.Р Положение о защите персональных данных работников / Л.Р. Фионова, О.В. Касперская // Секретарское дело. - 2015. - № 10. - С.40 - 49.

78. Физическая безопасность информационных ресурсов. Электронный ресурс https://efsol.ru/articles/physical-security.html. Дата обращения: 10.08.2021.

79. Храмцовская Н.А. Закон о персональных данных: последствия для делопроизводства / Н.А. Храмцовская // Делопроизводство и документооборота на предприятии. - 2017. - № 2. - С.12 – 30.

80. Чернов. В. Н. Системы электронного документооборота / В. Н. Чернов. – М. : РАГС, 2009. – 84 с.

81. Ярочкин В.Н. Информационная безопасность / В.Н. Ярочкин. - М.: Трикста, Академ. проект, 2015. - 542 с.

ПРИЛОЖЕНИЯ

Приложение 1

ОПИСАНИЕ СХЕМЫ ВНУТРЕННЕГО ДОКУМЕНТООБОРОТА В «1С: ДОКУМЕНТООБОРТ»

Данный документ описывает предполагаемую схему документооборота для внутренних документов при помощи системы «1С:Документооборот»:

– Приказ (для видов приказов настраиваются шаблоны);

– Распоряжение;

– Докладные и служебные записки;

– Выписка из приказа.

Схема процесса представлена на рисунке 12.

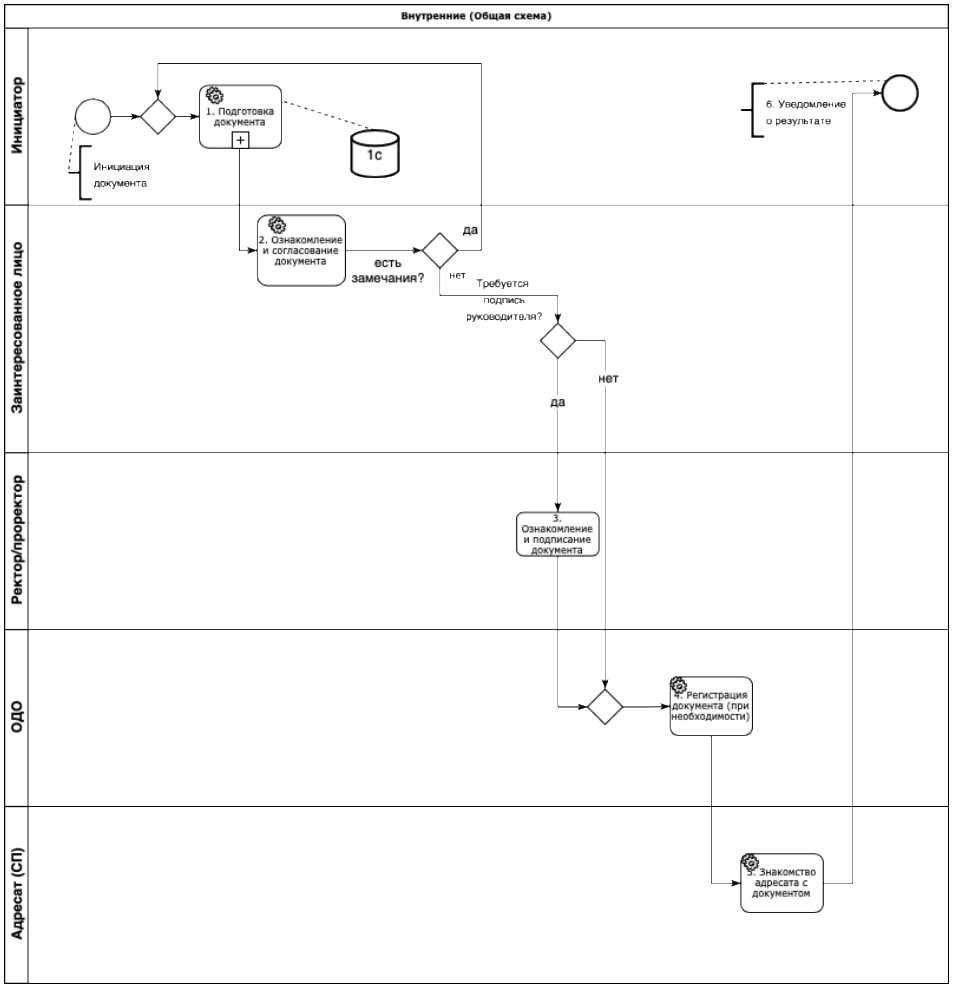

Рисунок 12 - Схема документооборота для внутренних документов при помощи системы «1С:Документооборот»

Инициатор процесса переходит в реестр внутренних документов и создает документ (рис. 13).

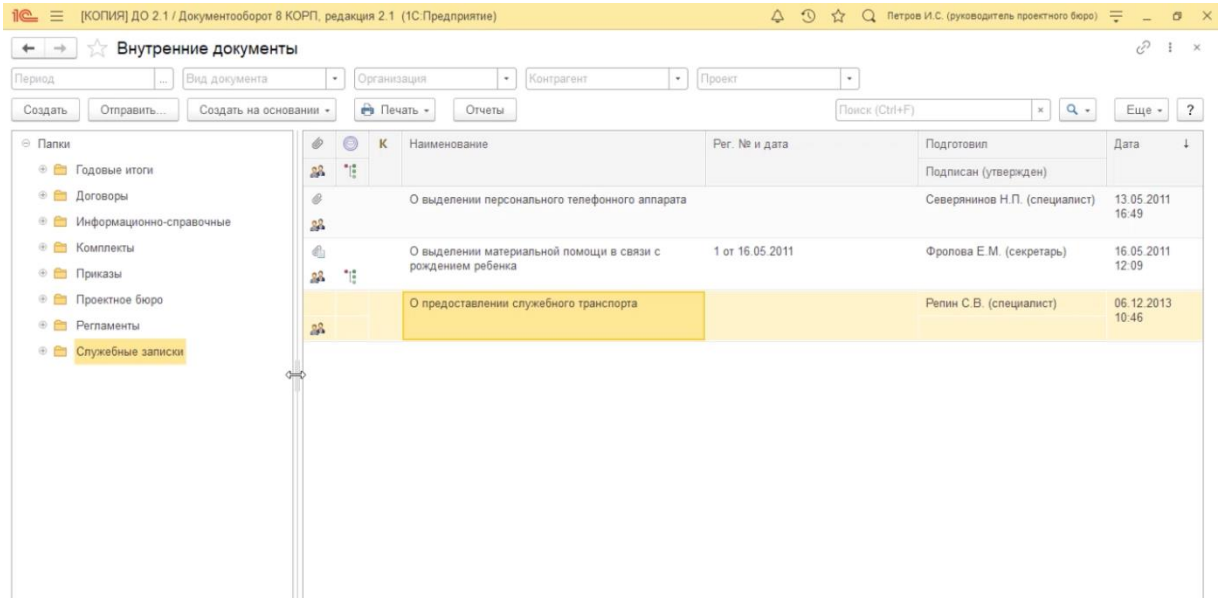

Рисунок 13 – Внутренние документы

Далее выбирает нужный вид документа, шаблоны документов загружены заранее (рис. 14).

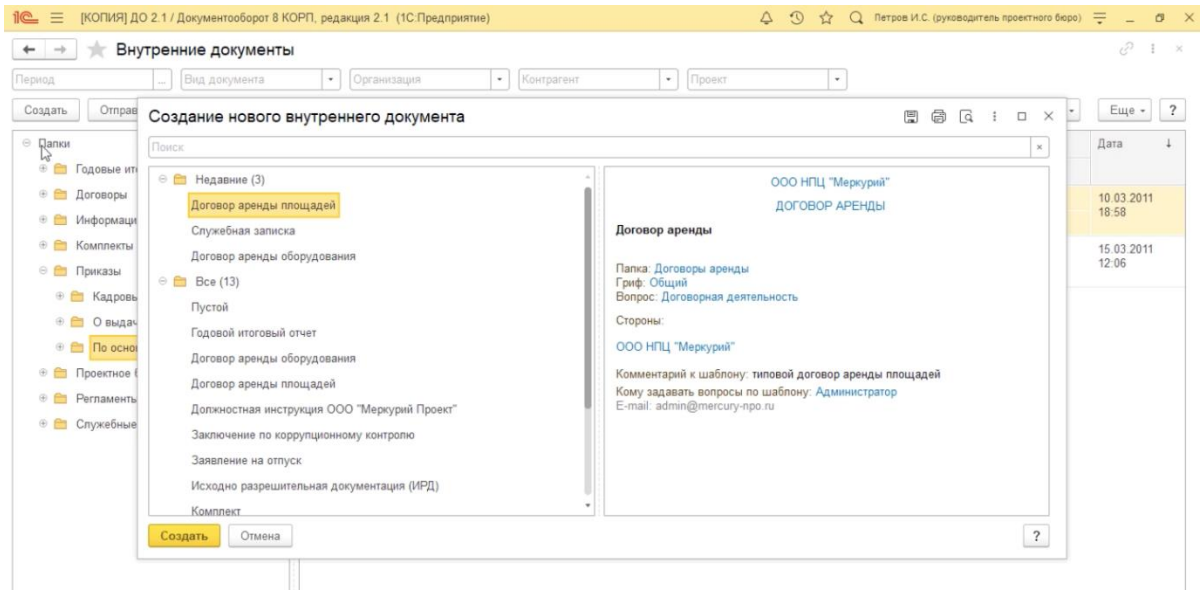

Рисунок 14 – Создание нового внутреннего документа в системе

В открывшемся окне заполняются основные реквизиты документа (рис. 15).

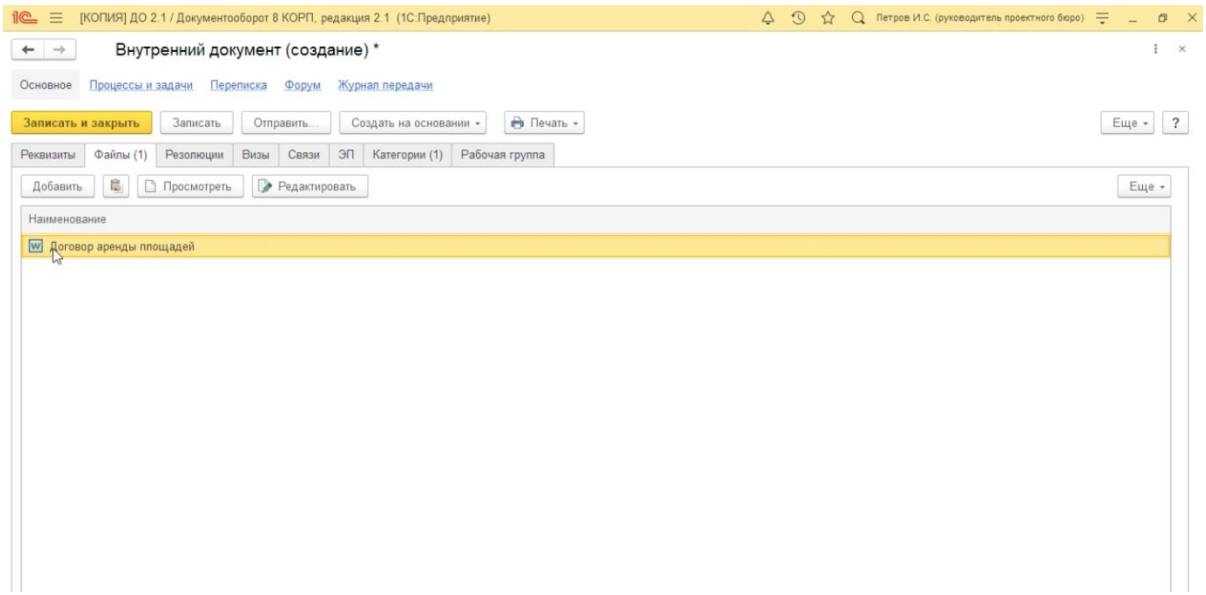

Рисунок 15 – Заполнение основных реквизитов документа

После отправки на печать в шаблоне документа все ранее заполненные реквизиты будет вставлены в шаблон автоматически (рис. 16).

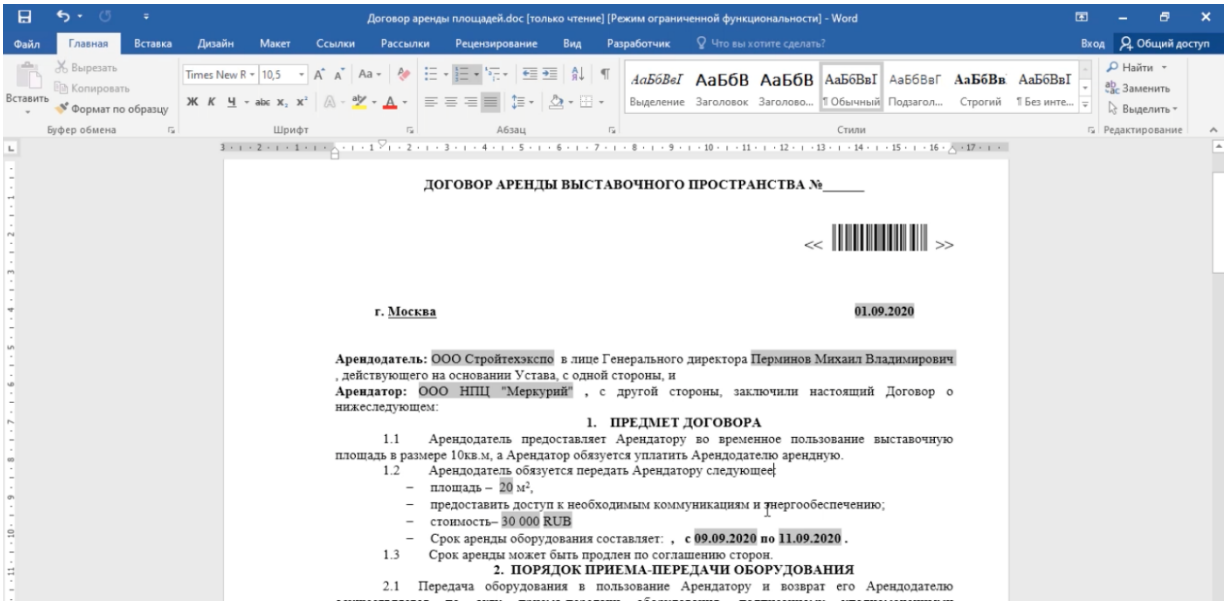

Рисунок 16 – Шаблон документа с автоматическим заполнением реквизитов

В зависимости от выбранного вида документа определяется заранее настроенный процесс согласования в системе, при внедрении описываются процессы согласования в системе (рис. 17).

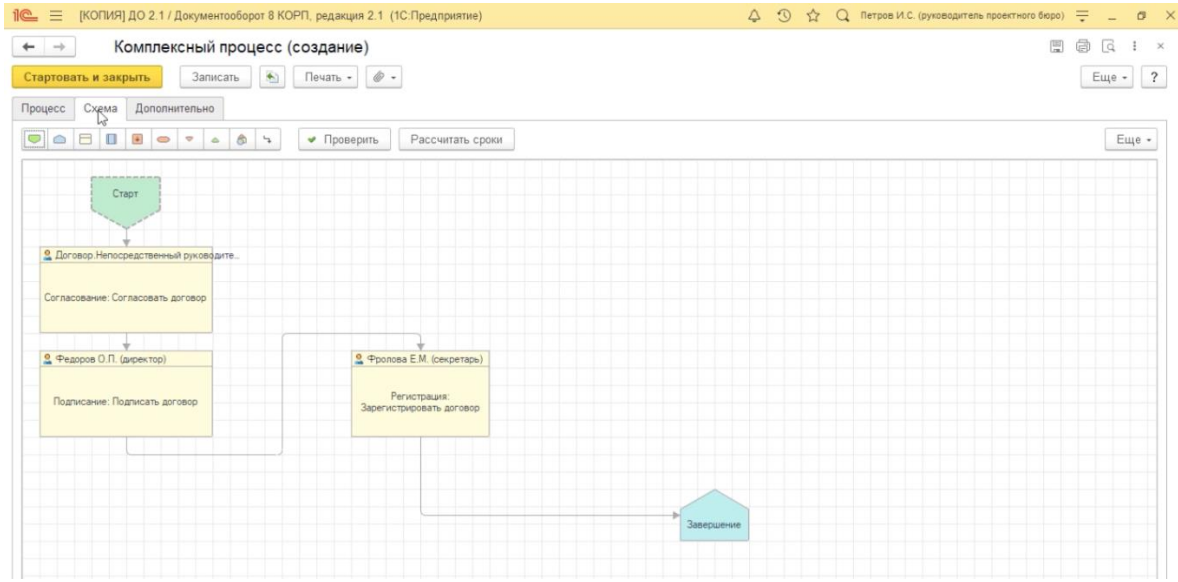

Рисунок 17 – Схема заполнения процесса согласования

В случае настройки процесса для вида документов подписанный документ направляется для ознакомления всем заинтересованным сотрудникам (согласно настройке). Результат согласования инициатор получает в список своих задач (рис. 18).

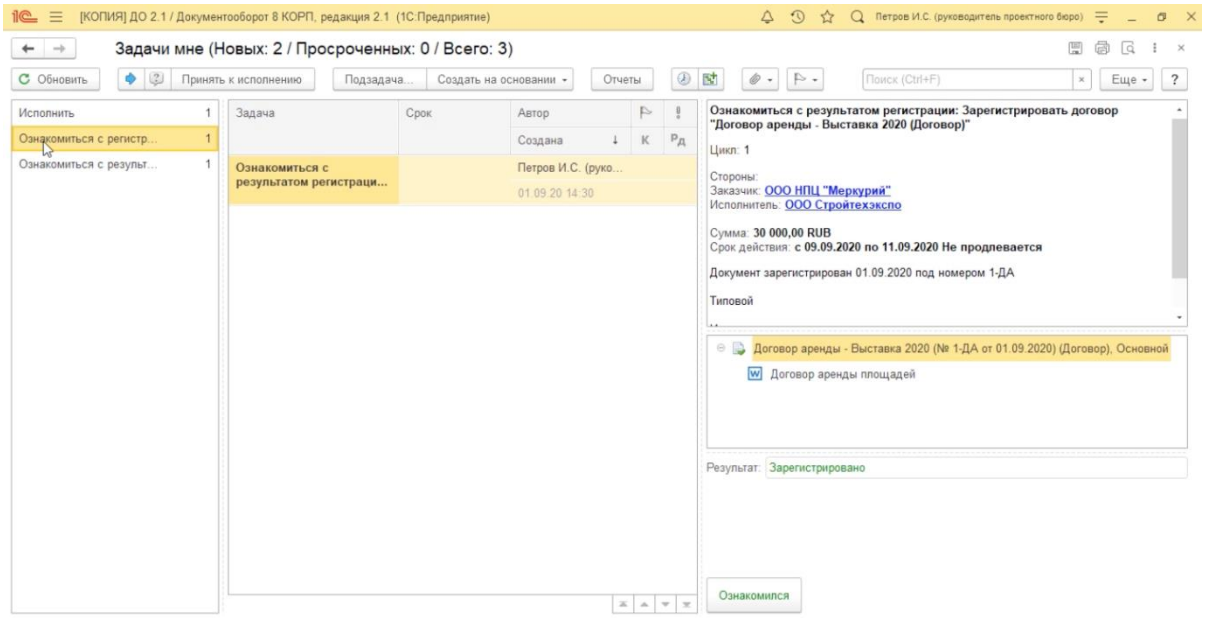

Рисунок 18 – Отражение списка задач в системе

Приложение 2

ОПИСАНИЕ ПРОЦЕССА ИСХОДЯЩЕГО ДОКУМЕНТООБОРОТА

Данный документ описывает предполагаемую схему документооборота для исходящих документов при помощи системы «1С:Документооборот»:

– Письмо;

– Переписка по договору.

Для бухгалтерских документов (счета-фактуры, акты и т.д.) регистрация исходящих документов на текущий момент не предполагается (отправка происходит напрямую от бухгалтерии без какой-либо отметки).

Схема процесса представлена на рисунке 19.

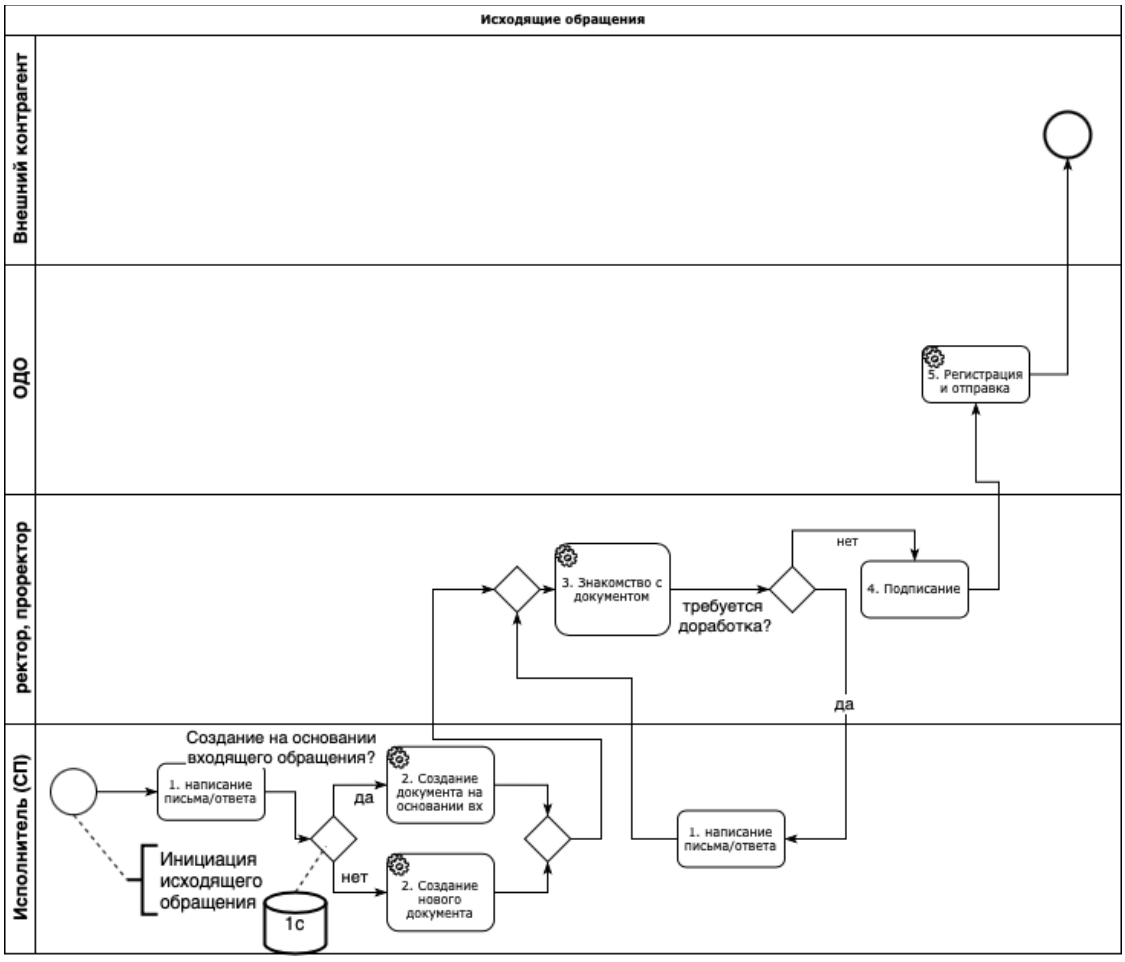

Рисунок 19 - Схему документооборота для исходящих документов при помощи системы «1С:Документооборот»

Инициатор (представитель структурного подразделения) пишет письмо (ответ) на бланках установленного образца. Передает документ в ОДО в бумажном или электронном формате.

Специалист (Инициатор) создает исходящий документ в журнале исходящих документов (рис. 20).

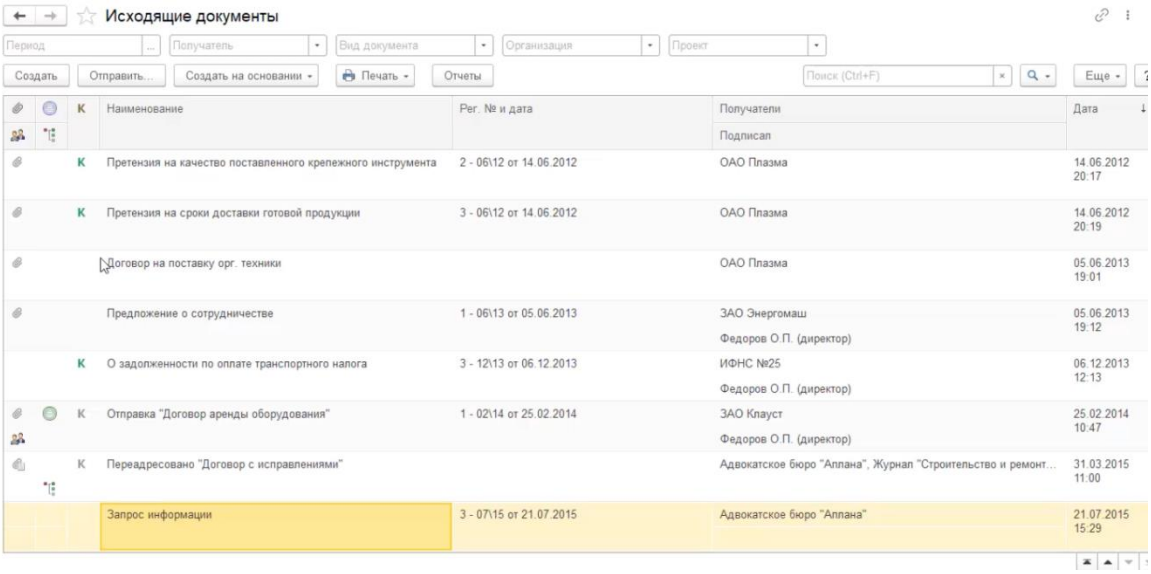

Рисунок 20 - Исходящий документ в журнале исходящих документов

или на основании входящего документа, если это ответ, с указанием вида документа (рис. 21).

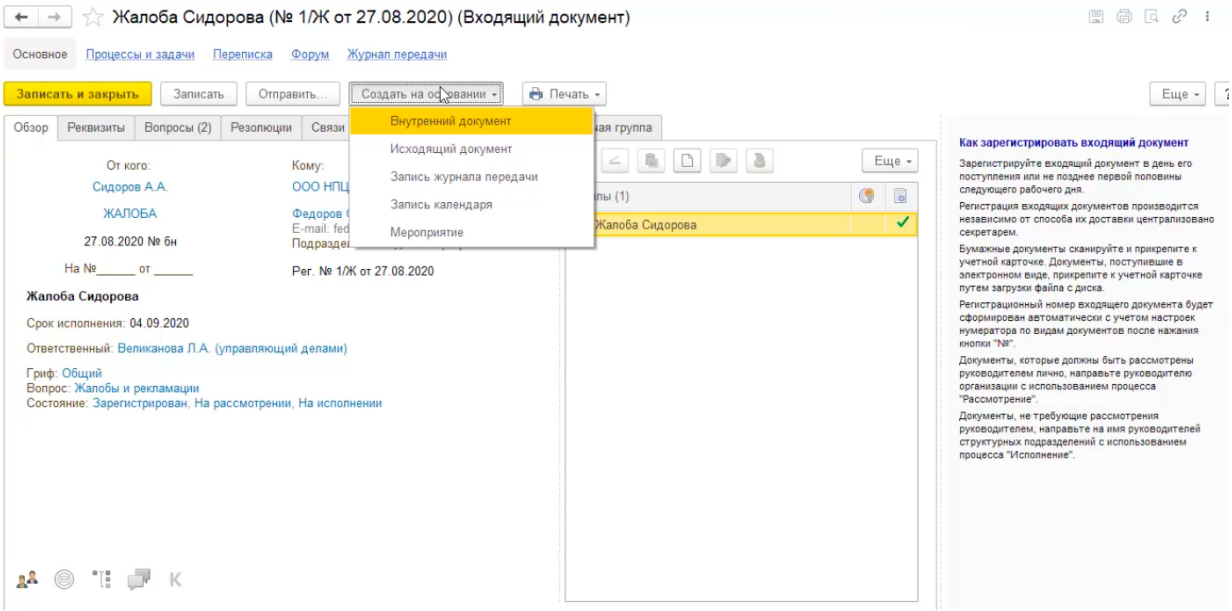

Рисунок 21 – Создание документа на основе входящего документа

С указанием всех необходимых реквизитов, в том числе кто должен подписать, документ, на который готовится ответ (рис. 22).

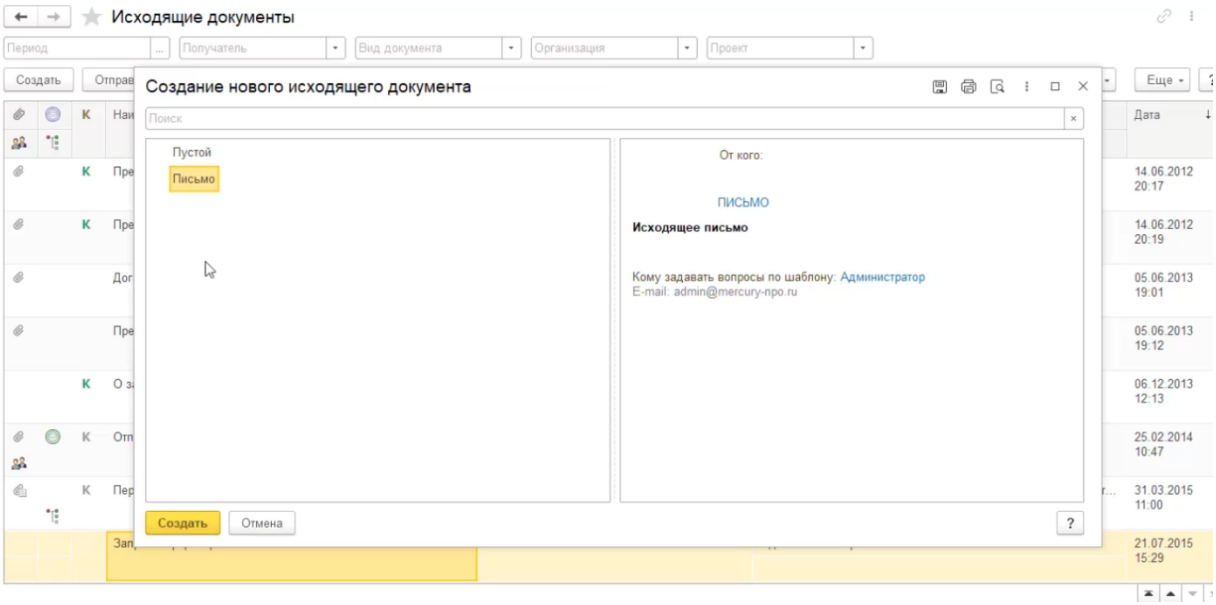

Рисунок 22 - Исходящий документ на основании входящего документа

Вкладывает в электронном виде к созданному документу электронный вариант документа. Отправляется документ на согласование (рис. 23).

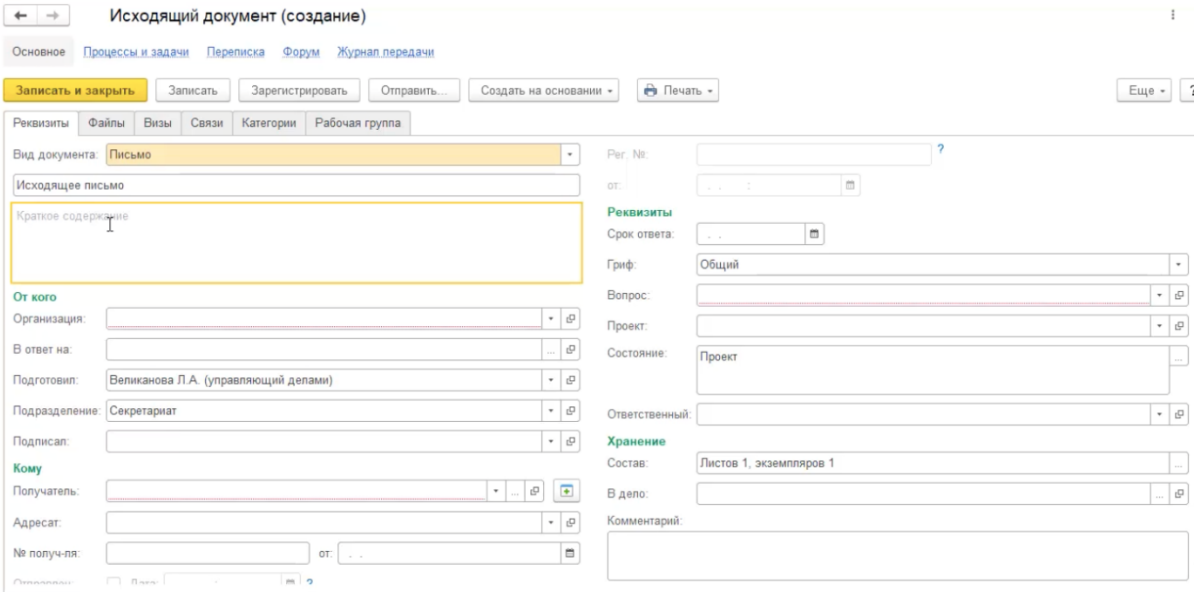

Рисунок 23 – Исходящий документ с указанием всех необходимых реквизитов

После создания документа инициатор промесса отправляет документ на согласование, которое проходит по ранее утвержденной и зафиксированной в системе схеме (рис. 24).

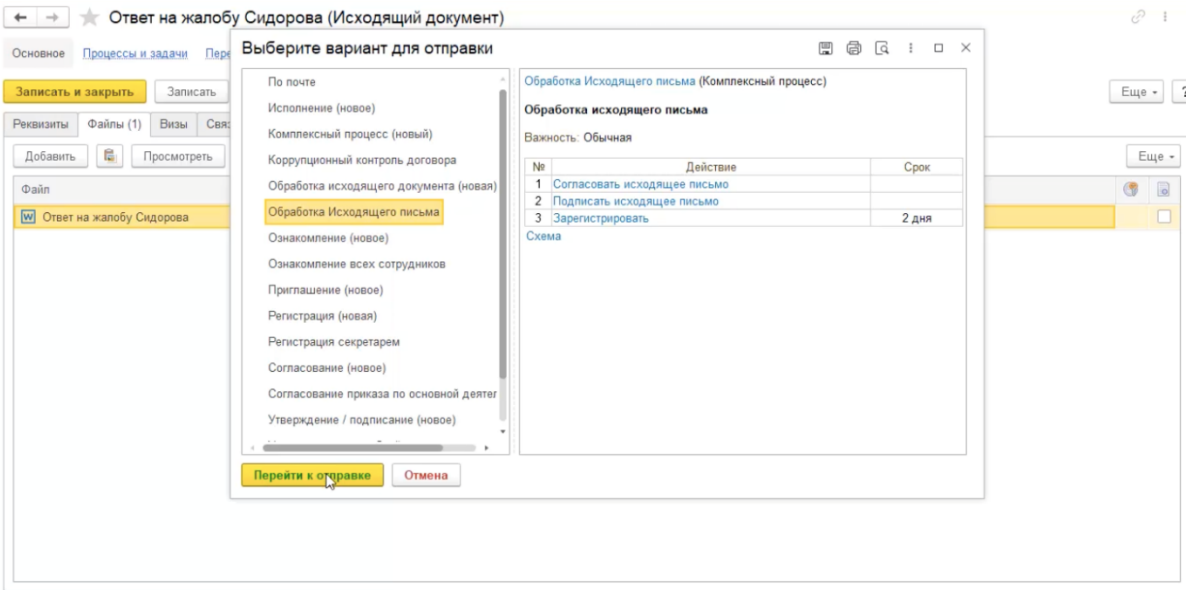

Рисунок 24 – Исходящий документ, отправленный на согласование

В случае, если требуется доработка документа, передается обратно исполнителю задача доработки (рис. 25).

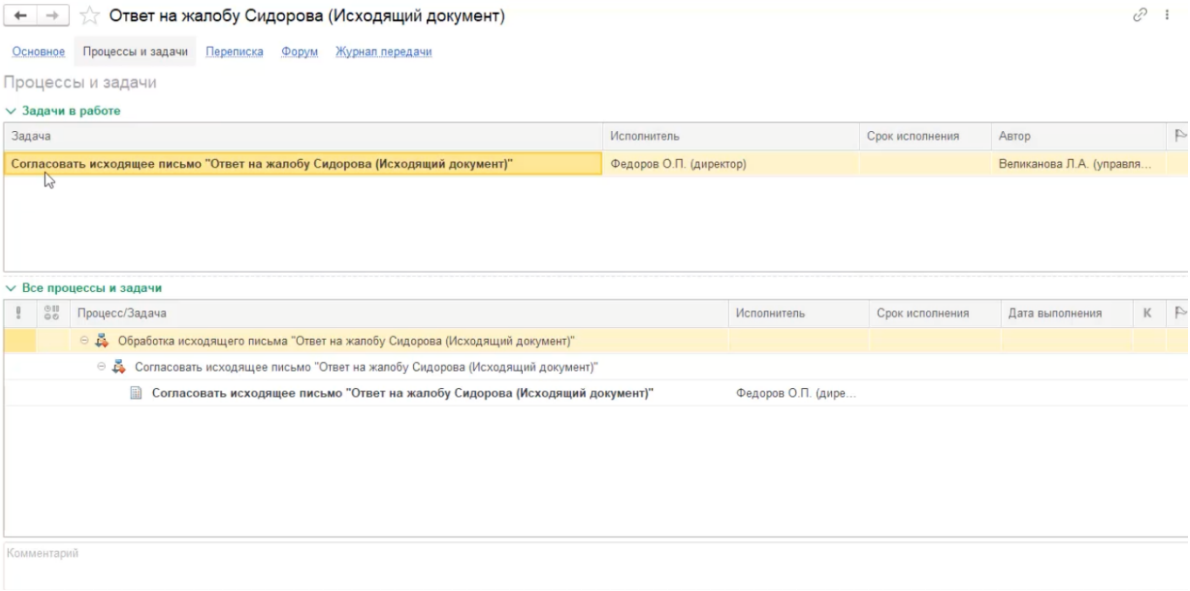

Рисунок 25 – Процесс подписания исходящего документа

В зависимости от формата подписания (электронная подпись, ручная) подписывается документ и передается в ОДО.

Специалист ОДО прикладывает к документу сканкопию, выбирает способ отправки и получателя. Указывает дату отправки и регистрирует исходящий документ (рис. 26). При необходимости отправляет копию электронной почтой.

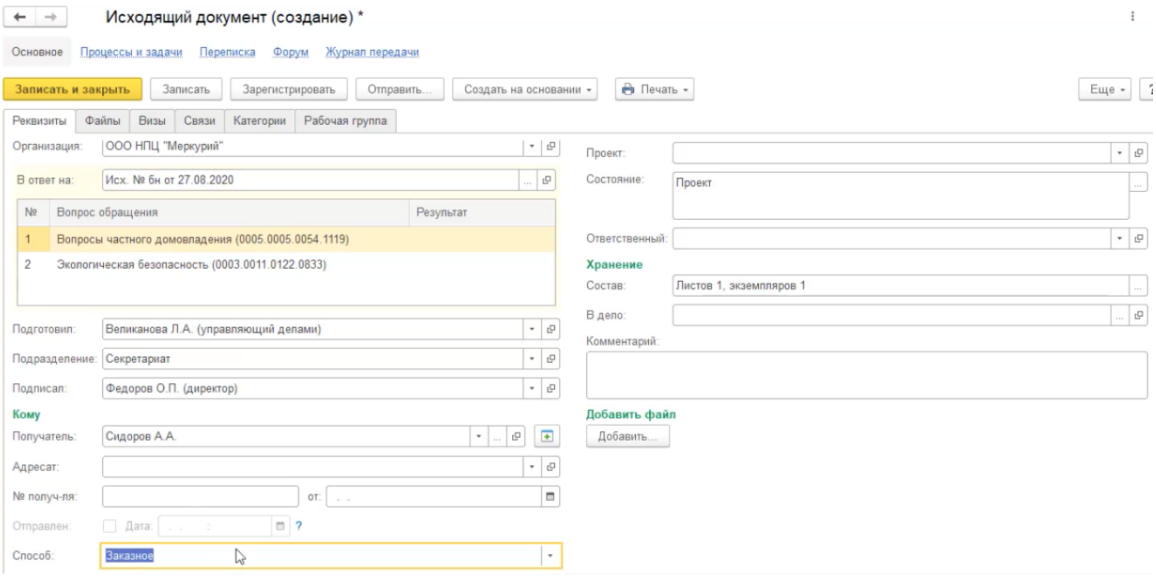

Рисунок 26 – регистрация и отправка исходящего документа

Приложение 3

ОПИСАНИЕ ПРОЦЕССА ВХОДЯЩЕГО ДОКУМЕНТООБОРОТА

Данный документ описывает предполагаемую схему документооборота для входящих документов при помощи системы «1С:Документооборот»:

– Запрос/Жалоба;

– Заявление;

– Переписка по договору;

– Письмо;

– Предложение.

Схема процесса отражена на рисунке 27.

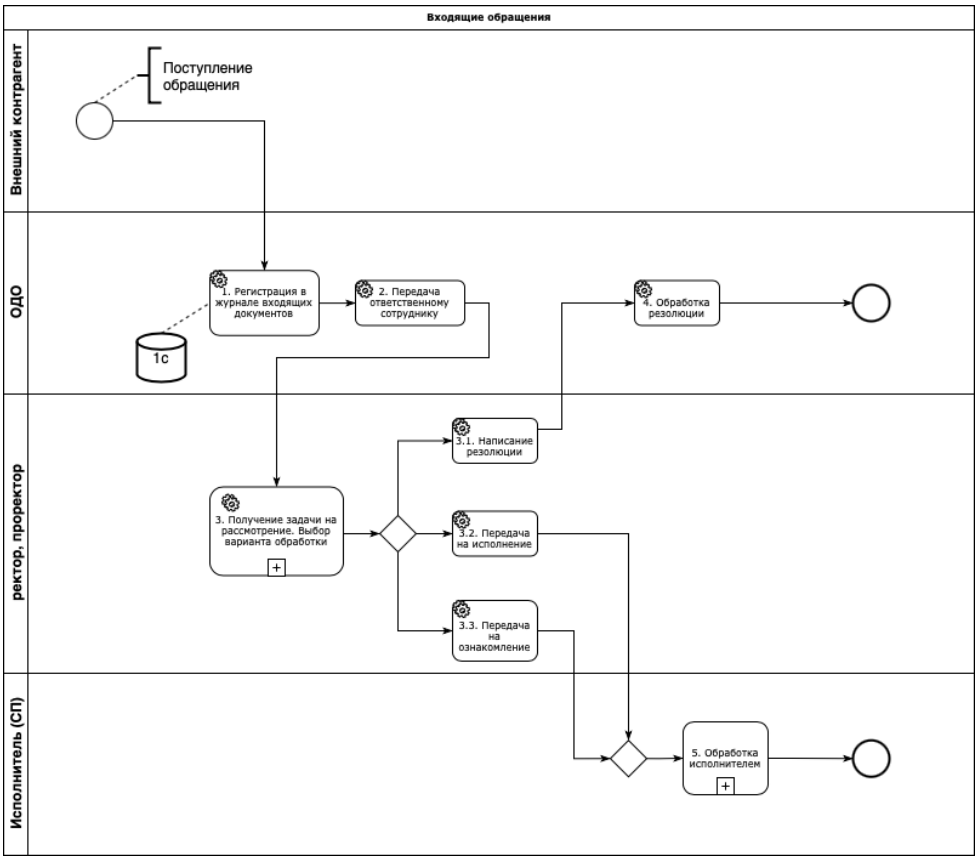

Рисунок 27 - Схема документооборота для входящих документов при помощи системы «1С:Документооборот»

От внешнего контрагента поступает документ, который регистрируется в журнале Входящих документов при помощи кнопки создать (рис. 28).

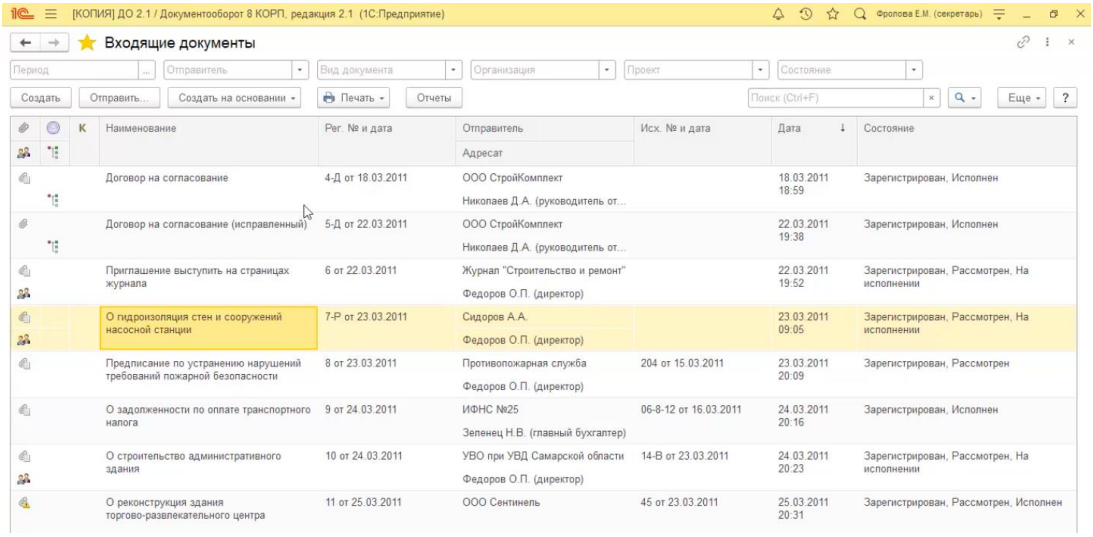

Рисунок 28 – Поступление входящего документа

Открывается форма регистрации входящего документа, в котором определяется вид документа и заполняются основные реквизиты, в том числе сроки рассмотрения (рис. 29).

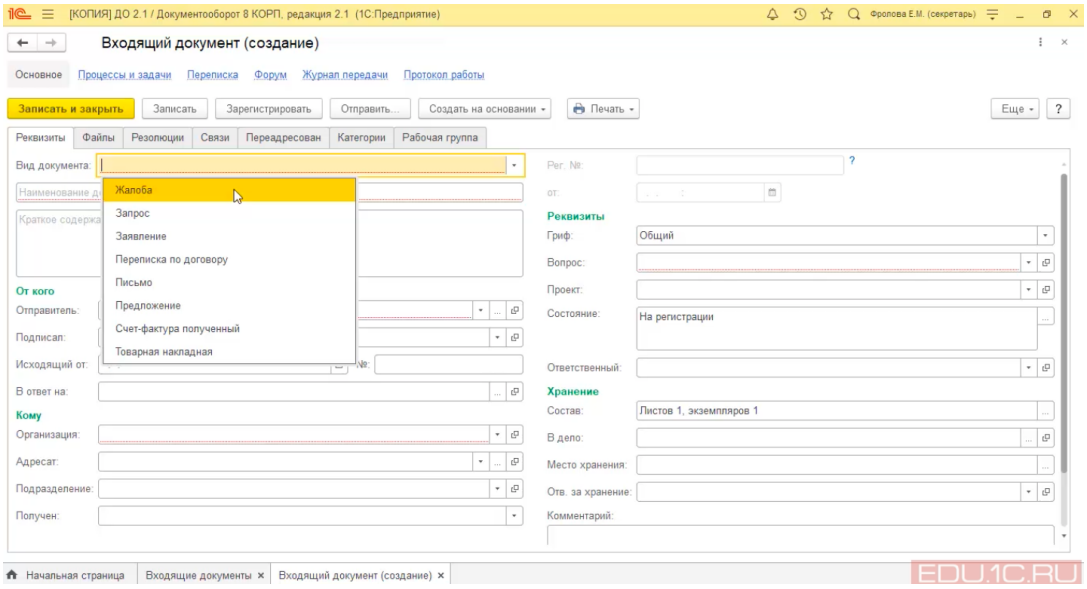

Рисунок 29 – Форма регистрации входящего документа

В данной форме прикрепляется скан-копия документа (рис. 30).

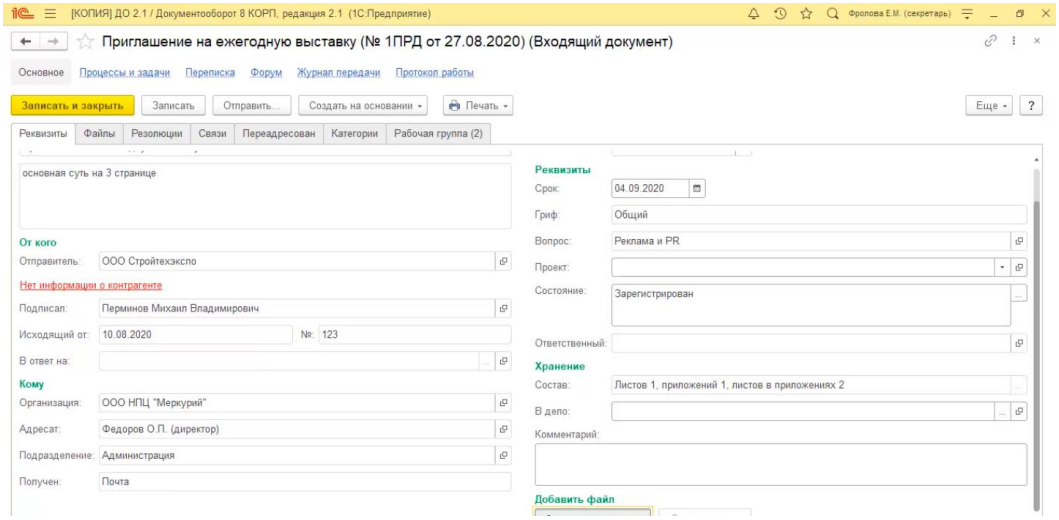

Рисунок 30 – Форма для прикрепления скан-копий

Далее при нажатии кнопки «Отправить» выбирается формат отправки и адресат (рис. 31).

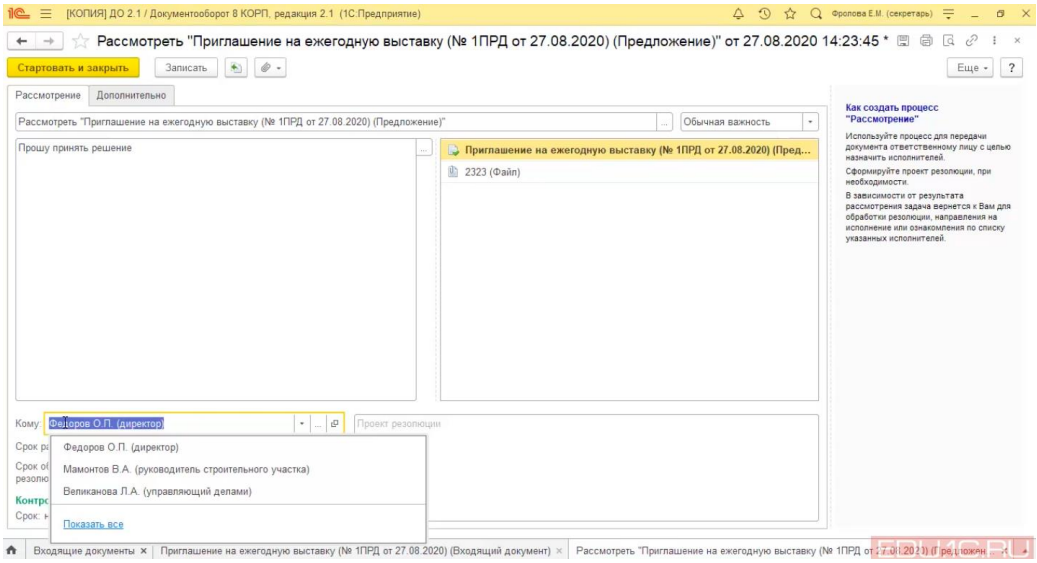

Рисунок 31 – Отправка документа адресату

Ответственное лицо (Руководитель) получает задачу на рассмотрение (рис. 32).

При открытии задачи возможны три варианта развития событий:

– рассмотреть: руководитель пишет резолюцию по данной задачи. Дальнейших действий не предусмотрено.

– на исполнение: передает задачу на исполнение ответственному сотруднику с дальнейшим контролем.

– на ознакомление: передает задачу на ознакомление. Дальнейших действий не предусмотрено.

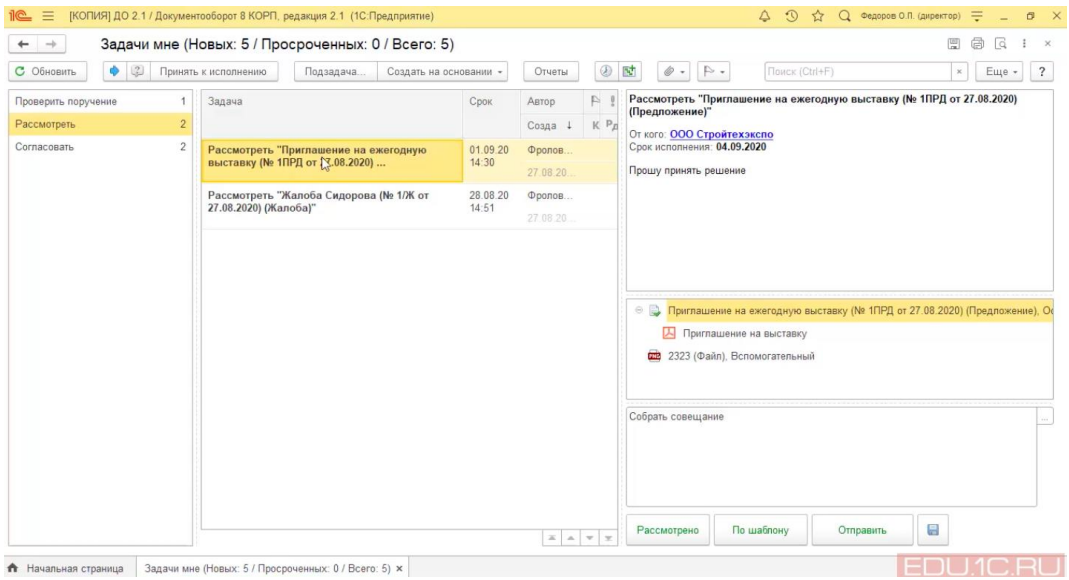

Рисунок 32 – Форма для отражения задач пользователя

При выполнении пункта 3 задача поступает в ОДО (сотруднику, создавшему входящий документ) для обработки резолюции (рис. 33).

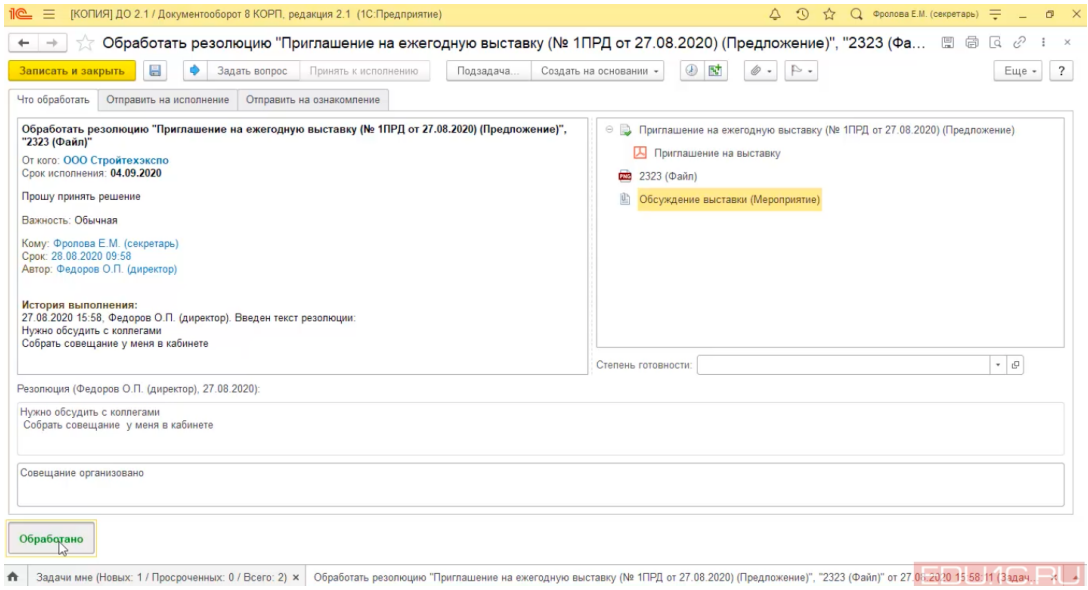

Рисунок 33 – Обработка резолюции сотрудником ОДО

Обработка исполнителем (ознакомление или выполнение определенных действий вне системы). В системе отображается факт выполнения поручения или ознакомления.

Приложение 4

ПРОГРАММА ПОДГОТОВКИ (ОБУЧЕНИЯ) ПОЛЬЗОВАТЕЛЕЙ ПРАВИЛАМ РАБОТЫ СО СРЕДСТВАМИ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

№ п/п	Тема
I.	**Основы безопасности информационных технологий**
1.1	Основные понятия информационной безопасности
1.2	Угрозы безопасности информационных технологий
1.3	Виды мер и основные принципы обеспечения информационной безопасности
II	**Обеспечение безопасности конфиденциальных данных**
2.1.	Федеральный закон от 04 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности»
2.2.	Федеральный закон от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации»
2.3	Положение «О разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденное Приказом ФСБ России от 9 февраля 2005 г. № 66;
III	**Правила работы с СКЗИ**
3.1.	Приказ ФАПСИ от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»
3.2.	Порядок использования СКЗИ КриптоПро CSP и ViPNet CSP
3.3.	Порядок использования электронной подписи
3.4.	Информационная система «ДелоPro». Делопроизводство и документооборот.
IV	**Тест для зачета**

Рисунок 34 – Программа подготовки (обучения) пользователей правилам работы со средствами криптографической защиты информации

Модуль 1. Основы безопасности информационных технологий

1.1 Основные понятия информационной безопасности

Что такое безопасность информационных технологий. Субъекты информационных отношений, их интересы и безопасность, пути нанесения им ущерба. Основные термины и определения. Конфиденциальность, целостность, доступность.

Определение НСД. Объекты, цели и задачи защиты информационных систем и циркулирующей в них информации.

1.2 Угрозы безопасности информационных технологий

Угрозы безопасности информации, информационных систем и субъектов информационных отношений. Основные источники и пути реализации угроз. Классификация угроз безопасности и каналов проникновения в автоматизированную систему и утечки информации. Основные непреднамеренные и преднамеренные искусственные угрозы. Классификация нарушителей информационной безопасности.

1.3 Виды мер и основные принципы обеспечения информационной безопасности

Виды мер противодействия угрозам безопасности (организационные, технические, физические). Достоинства и недостатки различных видов мер защиты. Основные принципы построения системы обеспечения безопасности информации в информационной системе.

Модуль 2. Обеспечение безопасности конфиденциальных данных

2.1. Федеральный закон от 04 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности»

Основные положения. Требования, предъявляемые к оператору конфиденциальной информации. Положение о лицензировании деятельности по технической защите конфиденциальной информации.

2.2. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

Сфера действия. Основные понятия. Информация как объект правовых отношений. Обладатель информации. Право на доступ к информации. Защита информации.

2.3. Положение «О разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденное Приказом ФСБ России от 9 февраля 2005 г. N 66

Общие положения. Порядок разработки СКЗИ. Порядок производства СКЗИ. Порядок реализации (распространения) СКЗИ. Порядок эксплуатации СКЗИ.

Модуль 3. Правила работы с СКЗИ

3.1. Приказ ФАПСИ от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с

ограниченным доступом, не содержащей сведений, составляющих государственную тайну»

Основные положения. Риски использования ЭП. Порядок обращения с ключевыми носителями. Инфраструктура открытых ключей. Управление своими сертификатами, их отзыв, приостановка и возобновление действия. Действия при истечении сертификата, компрометации ключей и прочих нестандартных ситуациях. Резервное копирование ключей, условия хранения и управления своими ключевыми данными.

3.2. Порядок использования СКЗИ КриптоПро CSP и ViPNet CSP

Установка и настройка СКЗИ. Хранение, использование, учет и контроль за использованием СКЗИ. Проверка срока действия сертификата ЭП.

3.3. Порядок использования электронной подписи

Основные понятия. Сфера регулирования отношений в области использования электронных подписей. Принципы использования электронной подписи. Виды электронной подписи. Признание квалифицированной электронной подписи. Средства электронной подписи. Удостоверяющий центр. Сертификат ключа проверки электронной подписи. Аккредитация удостоверяющего центра.

Модуль 4. Тест для зачета

Анкета для опроса пользователей СКЗИ

Заполняется персонально пользователем СКЗИ

ФИО _____

Для корректного заполнения просьба отметить один или несколько вариантов ответа

1. Какие свойства информации необходимо защищать?

a) коммерческую тайну;

b) целостность;

c) конфиденциальность;

d) полноту информации;

e) доступность.

2. Кто может быть нарушителем безопасности?

a) посетители;

b) сотрудники Вашей организации, не прошедшие обучение по работе с СКЗИ;

c) сотрудники Вашей организации, прошедшие обучение по работе с СКЗИ;

d) все вышеперечисленные.

…

15. Осуществляется ли обработка конфиденциальной информации в присутствии посторонних лиц?

a) да, если монитор расположен таким образом, что исключается возможность его обзора;

b) нет, ни в коем случае;

c) да, если это сотрудник лицензиата Управления Федеральной службы безопасности по Челябинской области.

Подпись _____

Дата _____

Результаты проверки

Всего ответов _____(кол-во)

Правильных ответов _____(кол-во)

(зачтено/не зачтено)

Проверил ФИО, подпись_____