Федеральное государственное автономное
образовательное учреждение
высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Институт управления бизнес-процессами и экономики
Кафедра экономики и информационных технологий менеджмента

УТВЕРЖДАЮ
Заведующий кафедрой
_____ А.А. Ступина
подпись
«____» _____ 2019 г.

МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ

Моделирование бизнес-процесса информационной безопасности персональных данных корпоративных систем

09.04.03 Прикладная информатика
09.04.03.02 «Реинжиниринг бизнес-процессов»

Научный руководитель _____ доцент, канд.техн.наук М.В.Карасева
подпись, дата

Выпускник _____ Я.О.Шишкина
подпись, дата

Рецензент _____ доцент, канд. техн. наук В.А.Федоров
подпись, дата

Красноярск 2019

РЕФЕРАТ

Магистерская диссертация по теме «Моделирование бизнес-процессов информационной безопасности персональных данных корпоративных систем» содержит 87 страниц текстового документа, 5 таблиц, 80 использованных источников, 24 рисунка.

ИНФОРМАЦИОННАЯ БЕЗОПАСТНОСТЬ, АНТИВИРУСНАЯ ЗАЩИТА ПЕРСОНАЛЬНЫЕ ДАННЫЕ, ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ, БИЗНЕС-ПРОЦЕСС, РЕИНЖИНИРИНГ БИЗНЕС-ПРОЦЕССА, ИНФОРМАЦИОННАЯ СИСТЕМА, ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ.

Цель работы: разработка информационной технологии взаимодействия и обмена данными между подразделениями, с обеспечение безопасности персональных данных согласно законодательству Российской Федерации.

Объектом исследования является Федеральное Государственное Автономное образовательное учреждение высшего образования «Сибирский федеральный университет» в городе Красноярск.

В первом разделе рассмотрены современные тенденции информационной безопасности в Российской Федерации, а также возможные проблемы, которые встречаются при обеспечении информационной безопасности персональных данных.

Во втором разделе рассмотрен объект исследования, организационная и функциональная модели объекта исследования, проанализирован выбранный для совершенствования процесс, освещен выбор и обоснование необходимости реинжиниринга бизнес-процесса.

В третьем разделе спроектирована и разработана информационная технология для реинжиниринга бизнес-процесса, представлена реализация информационной технологии и разработана методика аттестации информационных систем согласно мерам по защите информации персональных данных.

ESSAY

Master's thesis on "Modeling business processes of information security of personal data of corporate systems" contains 87 pages of a text document, 5 tables, 80 sources used, 24 figures.

INFORMATION SECURITY, ANTI-VIRUS PROTECTION PERSONAL DATA, PERSONAL DATA PROCESSING, BUSINESS PROCESS, BUSINESS PROCESS RE-ENGINEERING, INFORMATION SYSTEM, INFORMATION TECHNOLOGY.

Objective is to develop information technology for interaction and data exchange between departments, with ensuring the security of personal data in accordance with the legislation of the Russian Federation.

The object of the research is the Federal State Autonomous Educational Institution of Higher Education "Siberian Federal University" in the city of Krasnoyarsk.

The first section considers current trends in information security in the Russian Federation, as well as possible problems encountered in ensuring the information security of personal data.

In the second section, the object of study, the organizational and functional model of the object of study are examined, the process selected for improvement is analyzed, the selection and justification of the need for business process reengineering is highlighted.

The third section developed an information technology for business process reengineering, presented the implementation of information technology and developed a methodology for certifying information systems according to measures to protect personal data information.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Современные тенденции развития информационного общества диктуют необходимость внедрения информационных технологий в различные сферы жизни общества, не исключением являются и сфера работы с персональными данными. Развитие технологий вычислительной техники и цифровых телекоммуникаций все сильнее влияет на виды взаимодействия при работе с персональными данными, особое место в которых занимает их передача.

Научно-технический прогресс с течением времени превратил информацию в продукт, с которым можно производить различные действия, например, купить, продать, обменять. Нередко стоимость данных в несколько раз превышает цену всей технической системы, которая хранит и обрабатывает информацию. Качество и достоверность коммерческой информации обеспечивает необходимый экономический эффект для компании, поэтому важно охранять критически важные данные от неправомерных действий.

Необходимость обеспечения информационной безопасности в настоящее время – объективная реальность. Современный человек не может самостоятельно противодействовать посягательству не только на его частную жизнь, но и на работу. Возросшие технические возможности по сбору и обработке персональной информации, развитие средств электронной коммерции и социальных сетей делают необходимым принятие мер по информационной безопасности.

Применение информационных технологий при работе с персональными данными имеет ряд уязвимостей. К таковым можно отнести возможность несанкционированного проникновения в информационные системы, возникновения ошибок при занесении больших объемов персональных данных, несоответствия компетенции сотрудников для работы с информационными технологиями, которые работают с системами, а также нескоординированность работы между различными структурными подразделениями.

Актуальность магистерской диссертации состоит в том, что при нынешних объемах потоков персональных данных между подразделениями необхо-

димо обеспечивать их сохранность согласно законодательству Российской Федерации.

Новизна данной магистерской диссертации заключается в том, что впервые для объекта исследования на примере реинжиниринга бизнес-процесса разработана и будет реализована детальная методика проведения аттестации информационной системы по требованиям защиты персональных данных, которые отвечают нынешнему законодательству Российской Федерации.

Основой для выполнения данной работы является:

- общенаучные методы, такие как системный, диалитический, классификационный;
- методы анализа, обработки и обобщения информации;
- методы анализа и сравнения информации из научных и учебных источников литературы.

Целью данной работы является разработка информационной технологии взаимодействия и обмена данными между подразделениями, с обеспечение безопасности персональных данных согласно законодательству Российской Федерации.

Для достижения поставленной цели были сформулированы следующие задачи:

- исследовать теоретический аспект информационной безопасности персональных данных;
- выделить проблемы и определить направления совершенствования обеспечения информационной безопасности персональных данных;
- изучить деятельность объекта исследования и выделить бизнес-процесс для реинжиниринга;
- обосновать актуальность и необходимость предлагаемого решения;
- спроектировать и реализовать информационную технологию работы с персональными данными.

Объектом исследования является Федеральное Государственное Автономное образовательное учреждение высшего образования «Сибирский федеральный университет» в городе Красноярск.

Таким образом, необходимость обеспечения информационной безопасности имеет большое значение для эффективной работы организаций и является важным вопросом, который регулируется на законодательном уровне.

1 Современные тенденции информационной безопасности

1.1 Аппаратная и программная информационная безопасность

В настоящее время происходит глобальная цифровизация общества и всех сфер его жизнедеятельности, что коренным образом меняет не только привычные устои, но также и привычные механизмы работы по всему миру, не исключением является и Российская Федерация. Эти изменения носят не поверхностный характер, они затрагивают практически все сферы жизни общества [1,2].

Информатизация общества – это организованный социально-экономический и научно-технический процесс, который создает оптимальные условия для обеспечения информационных потребностей общества и реализации прав граждан, органов государственной власти, органов местного самоуправления, организаций, общественных объединений на основе формирования и использования информационных ресурсов [2].

Информатизацию общества также можно считать своего рода формой развития общества, а также ее можно сравнить с двигателем прогресса. Сейчас информационные технологии задают темп, направление и ритм развития каждой сферы жизни общества [3].

Информационные технологии в настоящее время развиваются достаточно интенсивно, не случайно многие производители электроники с мировым именем выразили желание проинвестировать именно российские компании, поскольку считают их динамичными на рынке. Но кроме инвестиций от зарубежных компаний существует необходимость в поддержке дотациями из бюджета. Пока подобные программы осуществляются, но не всегда в достаточном объеме. Индустрия информационных услуг уже давно прошла стадию становления и представляет собой достаточно налаженную и разветвленную инфраструктуру [4, 5, 6].

В процессе информатизации все большее значение уделяется информации. С такими большими объемами на первый план выходит необходимость обеспечения безопасности при работе с такой информации.

Обеспечение информационной безопасности Российской Федерации одна из ключевых задач информатизации российского общества. Ее решение предполагает обеспечение информационной безопасности граждан в условиях информационного окружения, а также самой информационной инфраструктуры.

Такие области постоянно развиваются, поэтому всегда полезно знать о последних достижениях отрасли, даже если для этого необходимо находить варианты взаимодействия с конкурентами. Существуют официальные нормативные правовые акты, которые отражают современное состояние, как информационной инфраструктуры страны, так и тенденции отрасли обеспечения защиты информации [7,8].

Такие вопросы как: что происходит сегодня, что ожидается в будущем, связаны с ошибками планирования отраслевые объединения, помогающие получать необходимую информацию для решения вопросов информационной безопасности. Ив настоящее время 37% компаний принимают участие в работе над ними. В целом 58% организаций, так или иначе, поддерживают связь с другими компаниями [9].

Рассмотрим более распространенные технологии информационной безопасности.

Можно сказать, что среди первых технологий, которые до сих пор востребованы на рынке (как для корпоративных, так и домашних пользователей), самой распространенной для обеспечения информационной безопасности является антивирусная защита (антивирусные программы), появившиеся еще лет 40-50 назад. Именно тогда берут начало первые вирусные сканеры, фаги и мониторы. Но если на заре активного развития вычислительных сетей широкое распространение получили антивирусы, обнаруживавшие и лечившие зараженные файлы, и вирусы, которые распространялись через дискеты и BBS, то есть

при помощи человеческих ресурсов, то сейчас таких вирусов практически не существует. Но все равно они представляют угрозу для информации, которая находится на персональных компьютерах.

Сегодня распространение получили такие классы вредоносных программ, как троянцы и черви, распространяющиеся не от файла к файлу, как было раньше, а от компьютера к компьютеру. Вирусные вспышки превратились в настоящие эпидемии и пандемии, а ущерб от них измеряется десятками миллиардов долларов [10, 11]. Кроме потерь денежных ресурсов стоит учитывать и потерю времени на восстановление и работу большого количества сотрудников для лечения от вирусных атак.

Первые антивирусы были сконцентрированы на защите только отдельных компьютеров. О защите сети или тем более о централизованном управлении или о системе защиты информации и речи быть не могло, что, разумеется, затрудняло использование этих решений на корпоративном рынке. К сожалению, сегодня положение дел в этом вопросе тоже встречает ряд трудностей, так как современные антивирусные компании уделяют этому аспекту отнюдь не первостепенное внимание, концентрируясь в основном на пополнении базы сигнатур вирусов. Исключением являются лишь некоторые зарубежные фирмы, например, TrendMicro, Symantec, Sophos, которые заботятся также о корпоративном пользователе. Что же касается Российских производителей, то они не уступают своим иностранным коллегам по качеству и количеству обнаруживаемых вирусных атак, но пока проигрывают по части централизованного управления [12, 13].

Ежегодно сравнивается большое количество антивирусных программ, по результатам подобных исследований составляются рейтинги. Так согласно сайту Софткаталог лучшими признаны [14]: Avast Free Antivirus, AVG Anti-virus Free, Advanced SystemCare Ultimate с антивирусом, Panda Antivirus Pro, IObit Malware Fighter, 360 Total Security, антивирус ESET NOD32 Smart Security, бесплатный Антивирус Касперского 2019, AviraFree Antivirus.

Для примера на рисунках 1 и 2 представлены интерфейсы антивируса ESET NOD32 Smart Security. Как видно из рисунка, современные антивирусные программы имеют в наборе настроек защиту различных каналов поступления информации (сеть, Интернет). Также немаловажным аспектом является обеспечение защиты в реальном времени, что повышает эффективность защиты [15].

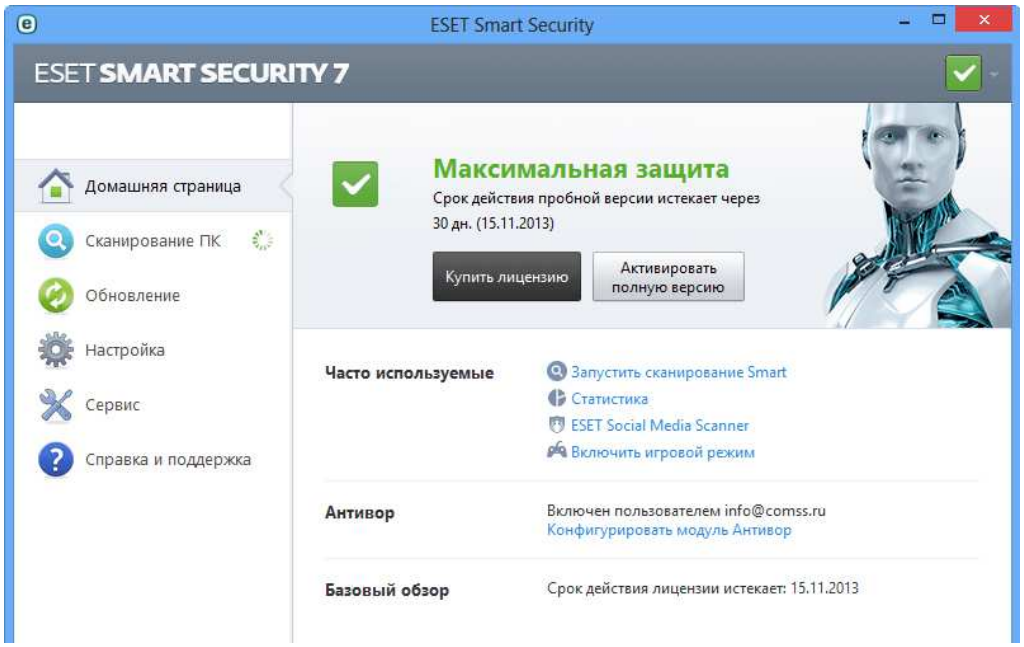

Рисунок 1 – интерфейс антивируса ESET NOD32 Smart Security

Рисунок 2 – Интерфейс настроек антивируса ESET NOD32 Smart Security

Для обеспечения информационной безопасности недостаточно только обеспечить защиту от вирусов на конечных рабочих станциях, также необходимо позаботиться о безопасности сети.

В конце 80-х – начале 90-х годов повсеместно началось развитие компьютерных сетей, вследствие чего возникла необходимость в их защите. По этой причине были разработаны межсетевые экраны, устанавливаемые между защищаемой и не защищаемой сетью. Свое начало они получили от обычных пакетных фильтров, постепенно подобные решения превратились в многофункциональные комплексы, решающие задачи от межсетевого экранирования и балансировки нагрузки до контроля пропускной способности и управления динамическими адресами. В межсетевой экран может быть встроен также модуль построения VPN, обеспечивающий защиту передаваемого между участками сети трафика [16].

Развитие межсетевых экранов отличается от истории развития антивирусов. Если последние развивались от персональной защиты к защите целых сетей, то первые – с точностью да наоборот. Долгое время никто и подумать не мог, что именно межсетевые экраны способны будут защитить что-то еще, кроме корпоративного периметра (поэтому его и называют межсетевым), но с увеличением количества персональных компьютеров, которые имеют доступ в Интернет, стала актуальной защита отдельно стоящих узлов, что и является прародителем технологии персональных межсетевых экранов, активно развивающейся в настоящее время. Некоторые производители развиваются и в таких направлениях, как предложение потребителю межсетевых экранов приложений, защищающие не сети и даже не отдельные компьютеры, а программы, запущенные на них [17].

Несмотря на почтенный возраст использования, межсетевые экраны до сих пор является часто используемым средством усиления традиционных средств защиты от несанкционированного доступа и активно применяется для обеспечения защиты данных при организации межсетевого взаимодействия

[18]. Стоит отметить такие востребованные сейчас функциональные требования межсетевых экранов как:

- фильтрация на сетевом уровне;
- фильтрация на уровне приложения;
- определение правил фильтрации и администрирования;
- инструменты сетевой проверки подлинности;
- внедрение газет и бухгалтерского учета.

Важным элементом концепции межсетевого экрана является аутентификация (авторизация пользователя), то есть пользователь получает право использовать конкретную услугу только после того, как было установлено и подтверждено, что он действительно тот, под чьим логином собираются производится операции. Услуга для этого пользователя считается авторизованной (процесс определения того, какие службы разрешены для конкретного пользователя, называется авторизацией или аутентификацией) [19].

Аутентификация позволяет сопоставить вводимые пользователем пароль и имя (логин) с информацией, хранящейся в базе системы защиты. При совпадении вводимых и эталонных данных разрешается доступ к запрашиваемым ресурсам. Стоит отметить, что, кроме пароля, аутентификационной информацией могут служить и другие уникальные элементы, которыми обладает пользователь, например, биометрические данные, брелоки и другое.

Элементы, которые могут послужить аутентификации, могут быть разделены на категории, соответствующие трем принципам [20]:

- «я знаю что-то» – классические парольные схемы;
- «я имею что-то» – в качестве уникального элемента может выступать таблетка Touch Memory, смарт-карта, брелок eToken, бесконтактная proximity-карта или карточка одноразовых паролей SecurID;
- «я обладаю чем-то» – уникальным элементом служит отпечаток пальца, геометрия руки, почерк, голос или сетчатка глаза, то есть биометрические персональные данные.

У системы защиты информации, которая включает на периметре корпоративной сети межсетевые экраны и антивирусы, все-таки некоторые атаки не сможет отразить. Подобные атаки получили название гибридных, и к ним можно отнести все последние нашумевшие эпидемии – Code Red, Nimda, SQL Slammer, Blaster, MyDoom и др. Для защиты от них предназначена технология обнаружения атак. Однако история этой технологии началась гораздо раньше, примерно, в 1980 году, когда Джеймс Андерсон предложил использовать для обнаружения несанкционированных действий журналы регистрации событий. Дальше понадобилось еще лет десять, чтобы стал возможен переход от анализа журналов регистрации к анализу сетевого трафика, где велись поиски признаков атак.

К настоящему моменту ситуация несколько изменилась – нужно не только обнаруживать атаки, но и блокировать их до момента, как они достигнут своей цели. Таким образом, системы обнаружения атак стали прорывом и, объединив в себе, знакомые по межсетевым экранам технологии, стали пропускать весь сетевой трафик (для защиты сегмента сети) или системные вызовы (для защиты отдельного узла), что позволило достичь 100% блокирования обнаруженных атак [21].

Дальше история повторилась: появились персональные системы, защищающие рабочие станции и мобильные компьютеры, а потом произошло закономерное слияние персональных межсетевых экранов, систем обнаружения атак и антивирусов, и это стало почти идеальным решением для защиты компьютера [22].

Всем известно, что катастрофу легче предупредить, чем предотвратить. То же можно сказать и о информационной безопасности: чем бороться с атаками, гораздо лучше устранить дыры информационной безопасности, используемые злоумышлинниками. Иными словами, надо обнаружить все уязвимости и устранить их до того, как их обнаружат злоумышленники. Этой цели служат сканеры безопасности (их также называют системами анализа защищенности), работающие как на уровне сети, так и на уровне отдельного узла. Первым ска-

нером, ищущим дыры в операционной системе UNIX, стал COPS, разработанный Юджином Спаффордом в 1991 году, а первым сетевым сканером – Internet Scanner, созданный Кристофером Клаусом в 1993-м.

В настоящее время происходит постепенная интеграция систем обнаружения атак и сканеров безопасности, что позволяет практически полностью исключить из процесса обнаружения и блокирования атак человека, сосредоточив его внимание на более важной деятельности. Интеграция заключается в следующем: сканер, обнаруживший дыру, дает команду сенсору обнаружения атак на отслеживание соответствующей атаки, и наоборот: сенсор, обнаруживший атаку, дает команду на сканирование атакуемого узла [23].

Лидерами рынка систем обнаружения атак и сканеров безопасности являются такие компании, как Internet Security Systems, Cisco Systems и Symantec. Среди российских разработчиков тоже есть свои герои, решившие бросить вызов своим более именитым зарубежным коллегам. Такой компанией является, например, Positive Technologies, выпустившая первый российский сканер безопасности – XSpider [24].

Итак, от вирусов, червей, троянских коней и атак мы нашли средства защиты. А что делать со спамом, утечкой конфиденциальной информации, загрузкой нелицензионного ПО, бесцельными прогулками сотрудников по Интернету, чтением анекдотов, онлайн-играми? Все вышеописанные технологии защиты могут помочь в решении этих проблем лишь частично. Впрочем, это и не их задача. На первый план здесь выходят другие решения – средства мониторинга электронной почты и Web-трафика, контролирующие всю входящую и исходящую электронную корреспонденцию, а также разрешающие доступ к различным сайтам и загрузку с них (и на них) файлов (в том числе видео- и аудиофайлов) [25].

В корпоративных сетях нашли применение и некоторые другие защитные технологии, хотя и очень перспективные, но пока что мало распространенные. К таким технологиям можно отнести PKI, системы корреляции событий безопасности и системы единого управления разнородными средствами защиты.

Данные технологии востребованы только в случаях эффективного применения и межсетевых экранов, и антивирусов, и систем разграничения доступа и т.д., а это в нашей стране пока еще редкость. Лишь единицы из тысяч российских компаний доросли до использования технологий корреляции, PKI и т.п., но ведь мы находимся только в начале пути.

Таким образом, отрасль информационной безопасности начитывает большое количество передовых технологий, например, антивирусная защита, межсетевые экраны, сканеры безопасности. Кроме этого существует тенденция развития, потому что угрозы информационной безопасности совершенствуются, что задает тенденции для развития отраслей информационной безопасности.

1.2 Актуальность информационной безопасности персональных данных корпоративных систем

В настоящее время в законодательстве Российской Федерации большое значение уделяется разработке нормативных актов, которые регулируют отрасли информационной безопасности и задают для нее стандарты и направление развития.

Согласно положениям Доктрины информационной безопасности Российской Федерации, можно сказать, что ее основные постулаты используют общие принципы для организации системы информационной безопасности, как в государственных, так и коммерческих структурах. Положения отражают цели, которые должны быть достигнуты в части защиты информации [26]:

- целостность;
- доступность;
- конфиденциальность.

Рассмотрим данные понятия подробно в разрезе информационной безопасности.

Конфиденциальность – это гарантирование того, что данные может быть прочитаны и проинтерпретированы только теми людьми и процессами, которые авторизованы это делать. Обеспечение конфиденциальности включает процедуры и меры, предотвращающие раскрытие информации неавторизованными

пользователями. Информация, которая может считаться конфиденциальной, также называется чувствительной. Примером может являться почтовое сообщение, которое защищено от прочтения кем бы то ни было, кроме адресата [27].

Целостность – это гарантия, что информация остается неизменной, корректной и аутентичной. Обеспечение целостности предполагает предотвращение и определение неавторизованного создания, модификации или удаления информации. Примером могут являться меры, гарантирующие, что почтовое сообщение не было изменено при пересылке [27].

Доступность – это гарантия того, что авторизованные пользователи могут иметь доступ и работать с информационными активами, ресурсами и системами, которые им необходимы, при этом обеспечивается требуемая производительность. Обеспечение доступности включает меры для поддержания доступности информации, несмотря на возможность создания помех, включая отказ системы и преднамеренные попытки нарушения доступности. Примером может являться защита доступа и обеспечение пропускной способности почтового сервиса [27].

Следом за целями указаны задачи, посредством решения которых они могут быть достигнуты:

- защита информации от несанкционированного доступа или изменения;
- организация защищенного доступа в открытые сети связи, в том числе в Интернет или по другим каналам;
- защита от воздействия компьютерных атак и вирусов.

Обеспечение информационной безопасности само по себе технически сложное и трудоемкое мероприятие, при этом одной из существенных проблем является установление связи между технической составляющей обеспечения информационной безопасности и обеспечением экономико-правовой и информационной безопасности личности в современных условиях [28].

Любой дееспособный член общества имеет свои персональные данные, которые он должен предоставлять: имя, адрес места регистрации и жительства, контактный телефон, адрес электронной почты, идентификационные данные своего удостоверения личности (серия и номер паспорта) и др. Подобные данные можно долго перечислять, но объединяет их то, что при их помощи можно идентифицировать конкретного гражданина. Персональных данных большое количество, это может быть и биометрическая информация, личные идентификационные признаки, сведения о различных персональных документах (водительское удостоверение, свидетельство о праве собственности на материальный объект, документы об образовании и др.). Несанкционированное или даже просто ошибочное использование персональных данных может принести существенный вред личности. Кроме этого незаконные махинации с персональными данными граждан могут повлечь за собой как административную, так и уголовную ответственность.

Стоит отметить, что согласно законодательству Российской Федерации, принято такое определение персональных данных. Персональные данные - любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных) [29].

Каждую составляющую персональных данных можно рассматривать с точки зрения её приоритета и статуса. Приоритет определяет значимость конкретных данных, а статус – её возможности. Так получается, что в зависимости от приоритета и статуса вред от неправомерного использования может разнится [28].

Обрабатываемые персональные данные подразделяются на группы [30]:

– первая группа – это специальные категории персональных данных, которые относятся к информации о национальной и расовой принадлежности субъекта, о религиозных, философских, либо политических убеждениях, а также информация о здоровье и интимной жизни субъекта.

– вторая группа – это биометрические персональные данные, т.е. данные, которые характеризуют биологические или физиологические особенности субъекта, например, фотография или отпечатки пальцев.

– третья группа – это общедоступные персональные данные, сведения о субъекте, полный и неограниченный доступ к которым предоставлен самим субъектом;

– четвертая группа – иные категории персональных данных, не представленные в трёх предыдущих группах.

Для обеспечения информационной безопасности организации, учреждения, предприятия должны быть созданы такие условия, при которых использование, потеря или искажение любой информации о состоянии организации, в том числе персональных данных, работниками организации или внешними лицами (пользователями) с высокой степенью вероятности не приведут в обозримом будущем к возникновению угроз прерывания деятельности организации или даже к прекращению работы компании, судебным разбирательствам [31].

Одной из составляющих национальных интересов Российской Федерации в информационной сфере является защита информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории России.

Национальными интересами в информационной сфере являются [26]:

а) обеспечение и защита конституционных прав и свобод человека и гражданина в части, касающейся получения и использования информации, неприкосновенности частной жизни при использовании информационных технологий, обеспечение информационной поддержки демократических институтов, механизмов взаимодействия государства и гражданского общества, а также применение информационных технологий в интересах сохранения культурных, исторических и духовно-нравственных ценностей многонационального народа Российской Федерации;

б) обеспечение устойчивого и бесперебойного функционирования информационной инфраструктуры, в первую очередь критической информационной инфраструктуры Российской Федерации (далее – критическая информационная инфраструктура) и единой сети электросвязи Российской Федерации, в мирное время, в период непосредственной угрозы агрессии и в военное время;

в) доведение до российской и международной общественности достоверной информации о государственной политике Российской Федерации и ее официальной позиции по социально значимым событиям в стране и мире, применение информационных технологий в целях обеспечения национальной безопасности Российской Федерации в области культуры;

г) содействие формированию системы международной информационной безопасности, направленной на противодействие угрозам использования информационных технологий в целях нарушения стратегической стабильности, на укрепление равноправного стратегического партнерства в области информационной безопасности, а также на защиту суверенитета Российской Федерации в информационном пространстве.

Целью российского законодательства в области обеспечения информационной безопасности персональных данных является защита прав и свобод гражданина при обработке его персональных данных, в том числе защита прав на неприкосновенность частной жизни, а также личную и семейную тайну. Законодательством регулируются отношения, которые связанны с обработкой персональных данных, которая осуществляется государственными органами власти, органами местного самоуправления, юридическими лицами и физическими лицами.

Для обеспечения защиты персональных данных государство способствует развитию современных информационных технологий, отечественной индустрии информации, в том числе индустрии средств информатизации, телекоммуникации и связи, обеспечение накопления, сохранности и эффективного использования отечественных ресурсов [4].

Для достижения этого требуется [4, 5, 6]:

– развивать и совершенствовать инфраструктуру единого информационного пространства Российской Федерации;

– развивать отечественную индустрию информационных услуг и повышать эффективность использования государственных информационных ресурсов;

– развивать пространство в Российской Федерации конкурентоспособных средств и систем информатизации, телекоммуникации и связи, расширять участие России в международной кооперации производителей этих средств и систем;

– обеспечить государственную поддержку отечественных и прикладных исследований, разработок в сфере информатизации, телекоммуникации и связи.

Стоит отметить, что законодательство Российской Федерации задает направление в сферах защиты персональных данных. Систематически обновляется законодательная база, которая включает в себя нормативные акты различных уровней: государственные, региональные, районные. Для того чтобы обеспечение безопасности соответствовало требуемому уровню необходимо совершенствовать технический, нормативный, информационные аспекты защиты персональных данных.

Мероприятия по защите информации трудоемки и могут привести к значительным финансовым затратам, что обусловлено необходимостью [32, 33]:

– получать (по необходимости) лицензию на деятельность по технической защите конфиденциальной информации ФСТЭК России;

– привлекать лицензиата ФСТЭК России для осуществления мероприятий по созданию системы защиты ИСПДн и/или ее аттестации по требованиям безопасности информации;

– отправлять сотрудников, ответственных за обеспечение безопасности информации, на курсы повышения квалификации по вопросам защиты информации и/или нанимать специалистов по защите информации;

– устанавливать сертифицированные по требованиям ФСТЭК средства защиты информации, сертифицированные ФСБ средства криптографической защиты информации в зависимости от класса информационной системы.

Оператор при обработке персональных данных обязан принимать необходимые организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

Суммируя вышесказанное можно заключить, что обеспечением безопасности персональных данных занимается не только оператор, но и уполномоченные на это органы власти. Система регулирования отношений, связанных с обработкой персональных данных и обеспечением их безопасности между заинтересованными субъектами представлена на рисунке 3 [34].

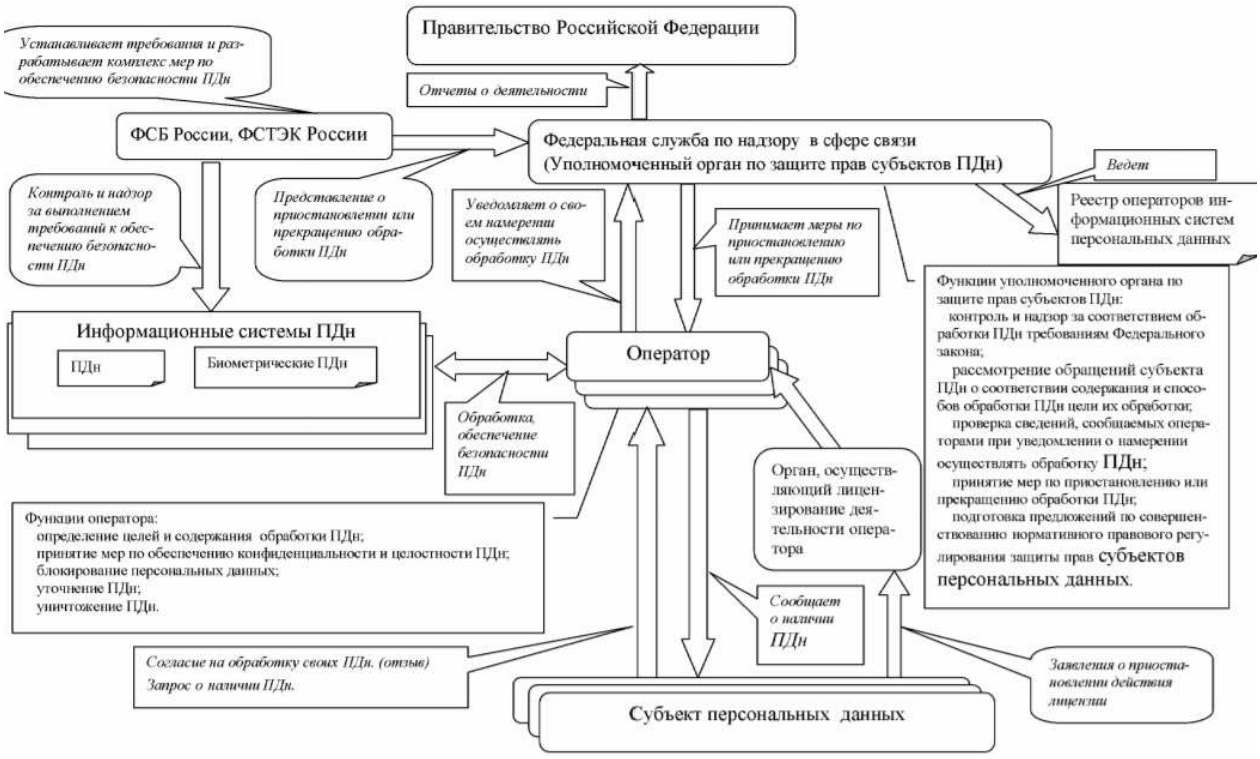

Рисунок 3 – Система регулирования отношений, связанных с обработкой персональных данных и обеспечением их безопасности

Таким образом, необходимость обеспечения безопасности персональных данных в наше время – объективная реальность. Современный компании долж-

ны не только самостоятельно противодействовать посягательству на сохранность персональных данных, но и с привлечением органов власти Российской Федерации. Возросшие технические возможности по сбору и обработке персональной информации, развитие средств электронной коммерции и социальных сетей делают необходимым принятие мер по защите персональных данных.

1.3 Проблемы при работе с техническим обеспечением информационной безопасности

Интенсивное развитие информационных технологий предполагает различные аспекты их использования. Информатизация работы с персональными данными предполагает облегчение работы с ними, что является несомненным плюсом. Но также включает ряд отрицательных моментов, которые непосредственно ввязаны с обеспечением безопасности этих данных.

Важными вопросами для организаций, осуществляющих обработку персональных данных на своих серверах, являются большие объемы данных граждан в информационных системах, широкое использование сетевых технологий, которое может привезти к утечке, уничтожению или модификации с возможностью возникновения значительных последствий [34].

Согласно данным на 2017 год в результате утечек скомпрометировано 7,78 млрд. записей (персональных и платежных данных) – номера социального страхования, реквизиты пластиковых карт, иная критически важная информация. Доля утечек персональных данных составила 65,8% от общего количества утечек. При этом было зафиксировано 20 «мега-утечек». В результате каждой «утекло» более 10 млн. персональных данных. На «мега-утечки» пришлось 98% всех скомпрометированных записей [35]. Подобная статистика лишь доказывает, что мало внимания уделяется вопросам информационной безопасности персональных данных, а если и уделяются, то принимаемые меры являются недостаточно эффективными.

Носители персональных данных встречаются как электронные, так и бумажные. Каждый из этих видов имеет ряд своих угроз сохранности.

Например, одним из основных минусов хранения в электронном виде (использования информационных технологий) является невозможность качественного обеспечения безопасности информации. Факторами утраты необходимой информации могут служить [36]:

1. Потеря документации, что может случить невосполнимой утратой персональных данных.

Каналы утери документированной информации или документов на бумажных носителях имеются на всех стадиях и этапах движения документов, при выполнении любых процедур и операций. К ним можно отнести [37]:

- кража (хищение) документа или отдельных его частей (листов, приложений, копий, схем, фотографий и др.), носителя чернового варианта документа или рабочих записей [36];
- несанкционированное копирование бумажных и электронных документов, баз данных, фото-, видео - и аудиодокументов, запоминание злоумышленником или его сообщником текста документа;
- тайное или разрешенное ознакомление сотрудника организации с документом и сообщение информации злоумышленнику лично или по линиям связи, прочтение текста документа по телефону или переговорному устройству, разглашение информации с помощью мимики, жестов, условных сигналов [38];
- подмена документов, носителей и их отдельных частей с целью фальсификации или сокрытия факта утери, хищения;
- дистанционный просмотр документов и изображений дисплея с помощью технических средств визуальной разведки;
- ошибочные (умышленные или случайные) действия персонала при работе с документами (нарушение разрешительной системы доступа, правил обращения с документами, технологии их обработки и хранения);
- случайное или умышленное уничтожение ценных документов и баз данных, несанкционированная модификация и искажение текста, реквизитов;
- считывание данных в чужих массивах за счет использования остаточной информации на копировальной ленте, бумаге, дисках;

– утечка информации по техническим каналам при обсуждении и диктовке текста документа, работе с компьютером и другой техникой;

– гибель документов в условиях экстремальных ситуаций;

– уничтожение документации раньше окончания установленного срока хранения [36].

Кроме вышеперечисленных опасностей существует еще и угрозы для конфиденциальной информации из электронных источников.

2. Неисправность оборудования, что может не только обеспечить потерю информации, но и быть причиной простоя в работе организации или неправильного сохранения необходимых данных.

В настоящее время документооборот подразумевает необходимость использования информационных технологий для составления, хранения, использования документов. Но иногда аппаратное обеспечение, которое обеспечивает использование информационных технологий, дает свои в работе. Для подобного существуют ряд причин [38]:

– ошибки при проектировании, разработке и эксплуатации программно-аппаратного обеспечения;

– преднамеренные действия по внесению уязвимостей в ходе проектирования, разработки и эксплуатации программно-аппаратного обеспечения;

– неправильные настройки оборудования и ПО, недопустимое изменение режимов работы устройств и программ;

– несанкционированное внедрение и использование неучтенных программ с последующим необоснованным расходованием ресурсов (например, загрузка процессора, захват оперативной памяти, памяти на внешних носителях);

– внедрение вредоносных программ, создающих уязвимости в программном и программно-аппаратном обеспечении;

– несанкционированные неумышленные действия пользователей;

– сбои в работе оборудования и ПО (вызванные сбоями в электропитании, выходом из строя аппаратных элементов в результате старения и сниже-

ния надежности, внешними воздействиями электромагнитных полей технических устройств и др.).

Особенности любого документооборота таковы, что сбои в работе могут возникать из-за ошибок пользователей, пиковых нагрузок, возникновения ошибок в самой системе после очередного поднятия версии [39].

3. Сбой работы в программе, что может привести к безвозвратной потере конфиденциальной информации.

Существует ряд факторов, которые обуславливают утрату конфиденциальной информации, обрабатываемой и хранящейся с помощью информационных технологий [37]:

- непреднамеренные ошибки пользователей, операторов, референтов, управляющих делами, работников службы конфиденциальной документации, системных администраторов, врачей, медицинских сестёр и других лиц, работающих и обслуживающих информационные системы (самая часто встречающаяся опасность);
- кражи и подлоги информации;
- угрозы, исходящие от стихийных ситуаций внешней среды;
- угрозы заражения вирусами;
- угрозы выхода из строя аппаратного обеспечения.

Вышеперечисленные угрозы не так страшны и опасны при использовании в компании резервного копирования, но не каждая компания способна позволить себе подобное.

4. Отсутствие резервного копирования (сбой резервного копирования).

Система резервного копирования – подсистема информационной системы, которая предназначена для создания резервных копий и восстановления данных [40, 41, 43].

Целью резервного копирования является предотвращение потери информации при сбоях оборудования, программного обеспечения, в критических ситуациях и так далее [44, 45].

5. Внесение информации в ручном режиме.

Использование аппаратного обеспечения и информационных технологий для ввода информации в базы данных, заполнение шаблонов документов, ведение и внесении информации для составления отчетности.

Последствия утраты информации могут быть различными: от необходимости восстановления своими силами до необходимости привлечения сторонних специалистов для устранения возникшей неисправности [46, 47, 48].

Еще существует возможность несанкционированное проникновение в информационное пространство организации. Как сказано в ГОСТе Р 50922-96 «Защита информации. Основные термины и определения» несанкционированный доступ к информации – это деятельность, которая направлена на получение защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к информации [49, 50]. Это можно отнести к возможности потери или кражи конфиденциальных данных.

Также не стоит недооценивать еще один из отрицательных моментов, которым являться так называемый человеческий фактор. Но данный аспект скорее относится не к информационным технологиям, но он всегда будет сопровождать их использование [51].

Все вышеперечисленные ошибки доставляют неудобство в большей своей части субъектам персональных данных, ведь им приходится приложить усилия для их устранения [52].

Одним из основных электронных способов обработки персональных данных являются различные информационные системы. Стоит обратить внимание конкретно на информационные системы персональных данных.

Информационная система персональных данных – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с

использованием средств автоматизации или без использования таких средств [47].

Для информационных систем персональных данных устанавливается 3 типа актуальных угроз [52]:

- угрозы 1 типа – угрозы, связанные с наличием не декларированных возможностей в системном программном обеспечении, используемом в информационной системе персональных данных;
- угрозы 2 типа – угрозы, связанные с наличием не декларированных возможностей в прикладном программном обеспечении, используемом в информационной системе персональных данных;
- угрозы 3 типа – угрозы, не связанные с наличием не декларированных возможностей в системном и прикладном программным обеспечением, используемом в информационных системах персональных данных.

Система защиты персональных данных должна обеспечить [53]:

- защиту информации от утраты, утечки, уничтожения, искажения, подделки и блокирования доступа к ней за счет несанкционированного доступа и воздействия;
- защиту информации от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи;
- резервное копирование и архивирование информации, а также программного обеспечения с целью оперативного восстановления утраченных данных вследствие несанкционированного воздействия на них;
- постоянный контроль за обеспечением защищенности информации и программного обеспечения, своевременное обнаружение фактов несанкционированного доступа к информации и воздействия на нее;

Особое внимание следует обратить на обеспечение целостности информации, содержащейся в базах данных информационных систем, а также на точность, полноту и правильность данных, вводимых в систему.

Таким образом, обеспечение информационной безопасности персональных данных встречает такие проблемы как потеря, порча электронной и бу-

мажной документации, неисправность оборудования, сбои в работе программного обеспечения, отсутствие или нежелание работников проведения работ по резервному копированию информации, человеческий фактор. Создается впечатление, что, например, информационные системы персональных данных смогут позволить решить подобные вопросы, но это не всегда так. Только информационные системы с налаженной системой защиты информации будут способствовать минимизировать потери персональных данных.

2 Анализ и оценка деятельности Отдела защиты информации Департамента по режиму и безопасности жизнедеятельности Сибирского федерального университета

2.1 Анализ деятельности Отдела защиты информации Департамента по режиму и безопасности жизнедеятельности Сибирского федерального университета

Сибирский Федеральный университет – российский федеральный университет, расположенный в Красноярске. Крупнейший университет восточной части России. Основан в 2006 году путём объединения четырёх высших учебных заведений города. В 2012 году к нему также были присоединены Красноярский государственный торгово-экономический институт и НИИЦ «Кристалл» [35].

Миссией университета являются создание передовой образовательной, научно-исследовательской и инновационной инфраструктуры, продвижение новых знаний и технологий для решения задач социально-экономического развития Сибирского федерального округа, а также формирование кадрового потенциала – конкуренто-способных специалистов по приоритетным направлениям развития Сибири и Российской Федерации, соответствующих современным интеллектуальным требованиям и отвечающих мировым стандартам [54].

СФУ насчитывает 21 институт и 3 филиала: Военно-инженерный институт; Гуманитарный институт; Инженерно-строительный институт; Институт архитектуры и дизайна; Институт горного дела, геологии и геотехнологий; Институт гастрономии; Институт инженерной физики и радиоэлектроники; Институт космических и информационных технологий; Институт математики и фундаментальной информатики; Институт нефти и газа; Институт педагогики, психологии и социологии; Институт управления бизнес-процессами и экономики; Институт физической культуры, спорта и туризма; Институт филологии и языковой коммуникации; Институт фундаментальной биологии и биотехнологии; Институт цветных металлов и материаловедения; Институт экологии и

географии; Институт экономики, управления и природопользования; Политехнический институт; Торгово-экономический институт; Юридический институт; Лесосибирский педагогический институт – филиал СФУ; Саяно-Шушенский филиал СФУ; Хакасский технический институт – филиал СФУ.

Структура и руководство. Первый ректор университета – академик РАН Евгений Александрович Ваганов. 26 октября 2017 года исполняющим обязанности ректора назначен Владимир Иннокентьевич Колмаков.

Президент СФУ – Александр Викторович Усс, доктор юридических наук, врио губернатора Красноярского края, председатель красноярского отделения Ассоциации юристов России [54].

Рассмотрим структуру Сибирского Федерального университета.

Для начала хотелось бы отметить, что организационная структура – совокупность управленческих звеньев, расположенных в строгой сосредоточенности и обеспечивающих взаимосвязь между управляющей и управляемой системами [55].

Основными элементами организационной структуры являются состав, соотношение, расположение и взаимосвязь отдельных подсистем организации [55].

Структура Сибирского Федерального университета достаточно обширна и масштабна, поэтому в ней нет возможности учесть всех сотрудников и все подразделения, поэтому на рисунке 4 представлена укрупненная структура на 16 мая 2019 года.

В структуре Сибирского Федерального университета отдельное место занимает Отдел защиты информации Департамента по режиму и безопасности жизнедеятельности (ДРиБЖД) [54].

Рассмотрим подробнее работу отдела защиты информации (ОЗИ).

Отдел по защите информации, являясь самостоятельным структурным подразделением предприятия, создается и ликвидируется приказом ректора.

Отдел непосредственно подчиняется руководителю департамента по режиму и безопасности жизнедеятельности.

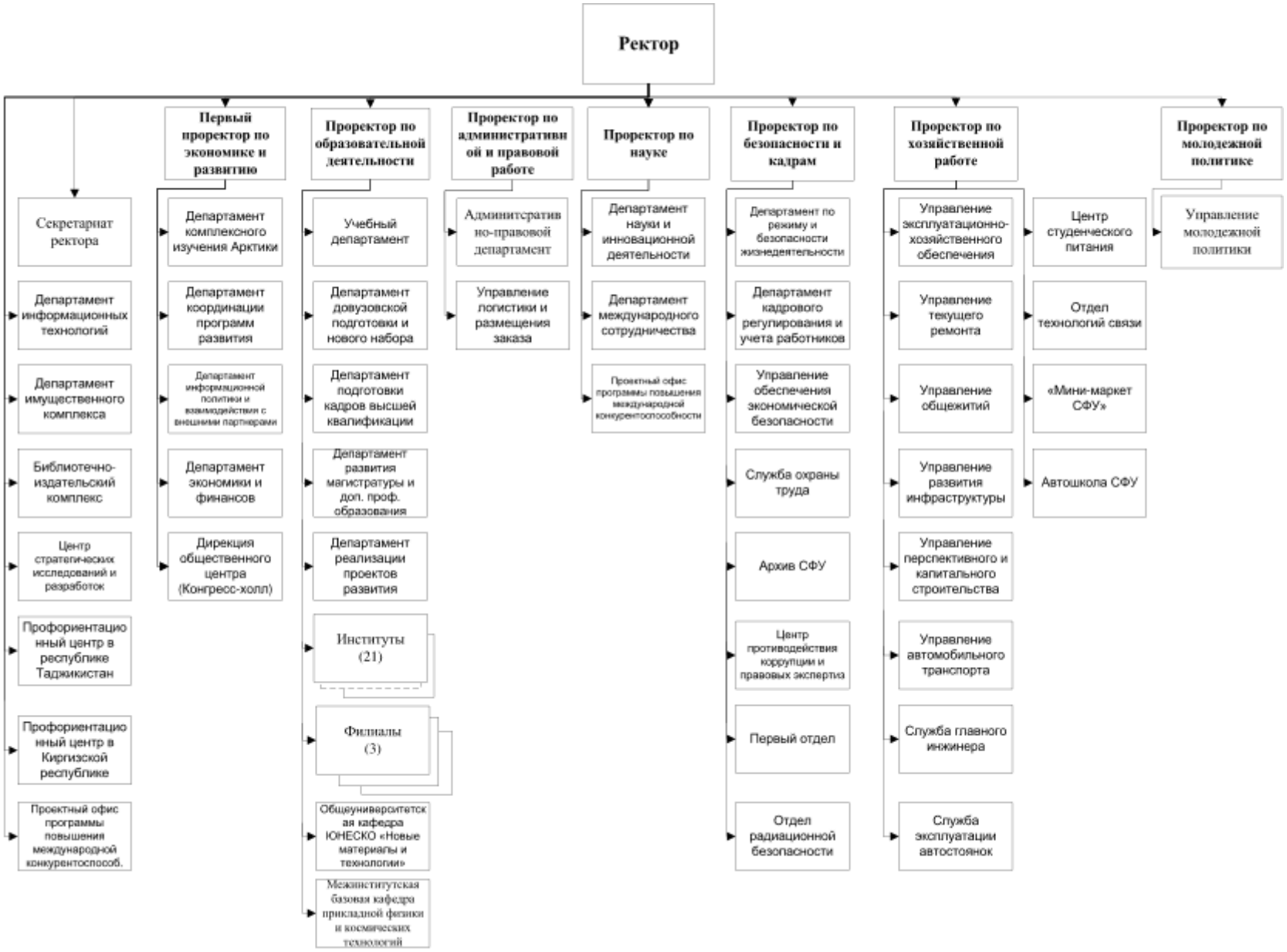

Рисунок 1 – Организационная структура Сибирского Федерального университета

Отдел подчиняется начальнику, назначенным на должность приказом ректора университета по представлению проректора по безопасности и кадрам.

В своей деятельности сотрудники отдела руководствуются:

- Уставом университета;
- приказами и распоряжениями ректора университета, проректора по безопасности и кадрам и руководителя департамента по режиму и безопасности жизнедеятельности;
- нормативно-распорядительными и нормативно-методическими документами Министерства науки и высшего образования РФ;
- нормативно-распорядительными и нормативно-методическими документами Федеральной службы по техническому и экспортному контролю;
- нормативно-распорядительными и нормативно-методическими документами Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций
- нормативно-распорядительными и нормативно-методическими документами Федеральной службы безопасности РФ
- нормативно-распорядительными и нормативно-методическими документами других федеральных ведомств;
- документами системы менеджмента качества университета
- положением об отделе;
- должностными инструкциями.

Состав и штатную численность отдела по защите информации утверждает ректор, исходя из конкретных условий и особенностей деятельности предприятия. В состав отдела входят группа специалистов, состоящая из 5 человек, в том числе начальник отдела защиты информации.

Распределение обязанностей между работниками отдела осуществляется начальником отдела по защите информации.

Масштаб деятельности отдела распространяется на все институты, филиалы и подразделения университета. Отдел работает в сотрудничестве со всеми подразделениями.

Отдел располагается на 2 площадке Сибирского федерального университета по адресу г. Красноярск ул. Киренского, 26А, корпус № 15 (Д). Географическое местоположение можно увидеть на 5 рисунке [54].

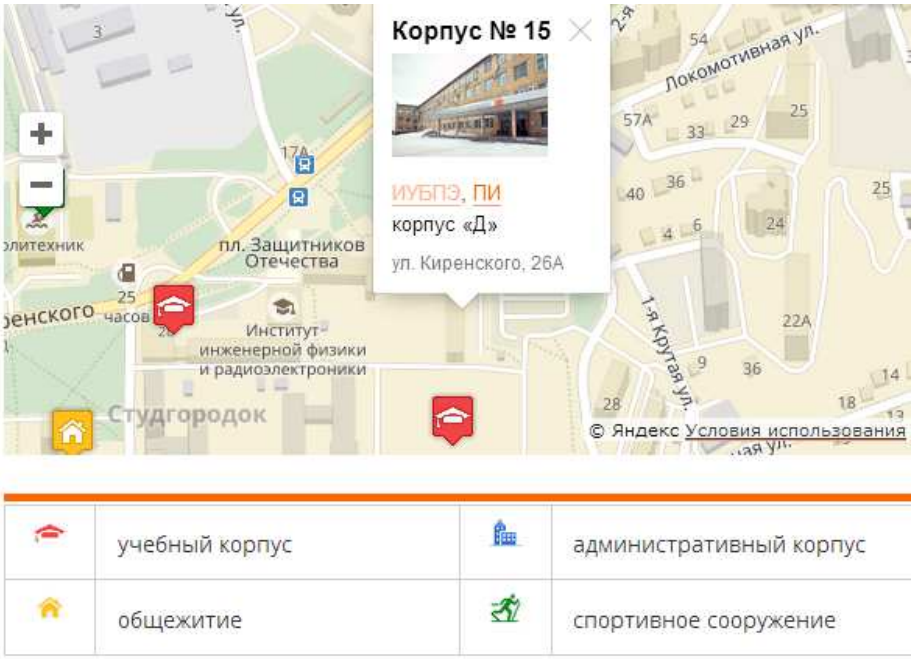

Рисунок 5 – Месторасположение объекта исследования

Отдел защиты информации Департамента по режиму и безопасности жизнедеятельности находится в подчинении у проректора по кадровой и социальной работе.

Рассмотрим структуру отдела отдельно. На рисунке 3 видно, что в отделе работают 5 сотрудников: начальник отдела и 4 специалиста отдела.

Рисунок 5 – Организационная структура ОЗИ

У каждого специалиста есть определенный, закрепленный за ним функциональный набор, который определяется распространением полномочий сотрудника:

– начальник отдела относится к категории административно-управленческого персонала и осуществляет методическое руководство организацией мероприятий по защите информации в подразделениях университета и контроль за эффективностью предусмотренных мер защиты информации;

– ведущий специалист по защите информации относится к категории административно-управленческого персонала и осуществляет координацию работ по нормативному и методическому обеспечению мероприятий по защите информации, контроль за выполнением требований по защите информации в подразделениях;

– специалист по защите информации относится к категории административно-управленческого персонала и осуществляет нормативное и методическое обеспечение мероприятий по защите информации, контроль за выполнением требований по защите информации в автоматизированных системах, вычислительных сетях и средствах вычислительной техники;

– специалист по защите информации относится к категории административно-управленческого персонала и осуществляет нормативное и методическое обеспечение мероприятий по защите информации, контроль за выполнением требований по защите информации в подразделениях;

– специалист по защите информации относится к категории административно-управленческого персонала и осуществляет нормативное и информационное обеспечение мероприятий по организации защиты информации в подразделениях, в автоматизированных системах, вычислительных сетях и средствах вычислительной техники университета.

Таким образом, функциональный набор специалистов отличается друг от друга, поэтому каждый из специалистов вынесен в отдельную ячейку организационной структуры.

Функциональная модель отображает функциональную структуру объекта, т.е. производимые им действия и связи между этими действиями [56].

Весь функциональный набор отдела зафиксирован в должностных инструкциях специалистов отдела, которые не предоставляются для общего пользования, по-

этому функции отражены в функциональной структуре отдела, которая представлена на рисунке 6.

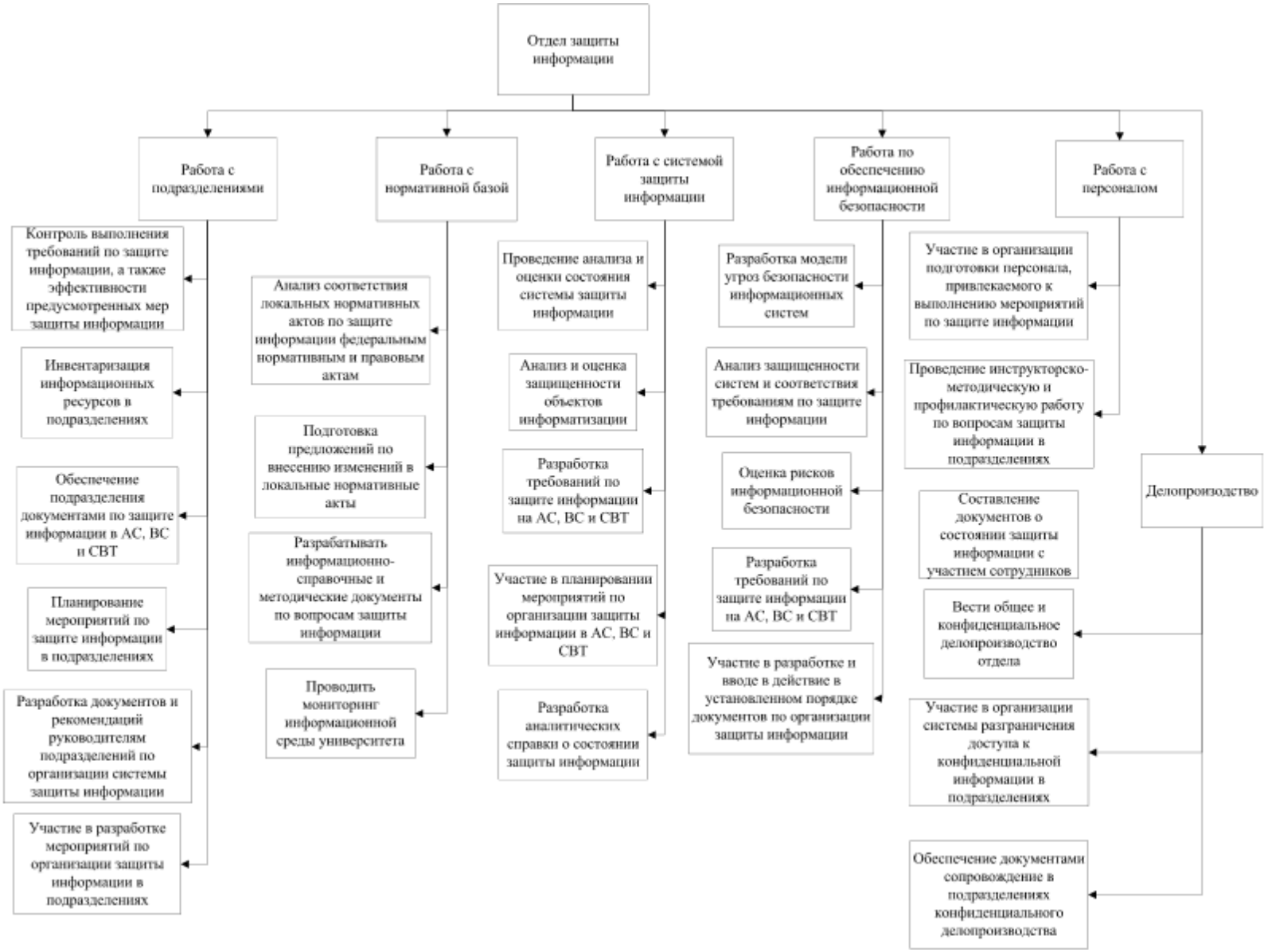

Рисунок 6 –Функциональная структура отдела защиты информации

На рисунке 6 видно, что каждый сотрудник имеет определенный функционал и он взаимосвязан с работой других специалистов. Например, ведение делопроизводства отдела влияет на составление актов, служебных записок и иных локальных нормативных документах, в которых приходится ссылаться на предыдущие документы о деятельности отдела.

Дерево функций отражает все функции, которые сотрудники выполняют отдела. Они четко определены и разделены между сотрудниками, что способствует отсутствию перенагрузки.

Функциональная структура данного отдела является эффективной, потому что функции распределены между сотрудниками равномерно и взаимозавязаны между собой.

Функциональное дерево представляет собой совокупность взаимодействий сотрудников, так как сотрудники отдела обслуживания отвечают за отдельные функции процесса. Согласно функциональной структуре представим распределение бизнес-процессов для отдела, непосредственно связанных с основной задачей отдела. В таблице 1 представлены бизнес-процессы и подпроцессы работы отдела.

Таблица 1 – Табличное представление системы бизнес-процессов отдела защиты информации

Группа процессов	Процесс	Ответственный исполнитель
Работа с подразделениями	Контроль выполнения мер по защите информации (ЗИ)	Курбатов А. Ф. (Начальник отдела); Кокшарова Н. В. (институты и филиалы), Сизых В. С. (административные подразделения)
	Разработка локальных нормативных актов по ЗИ	
	Инвентаризация информационных ресурсов в подразделениях	
	Обеспечение подразделений необходимыми документами	
	Планирование мероприятий по организации ЗИ	

Окончание таблицы 1

Группа процессов	Процесс	Ответственный исполнитель
	Консультирование подразделений по вопросам ЗИ	
Работа с нормативной базой	Анализ соответствия локальных нормативных актов по ЗИ с федеральными нормативными актами	Курбатов А. Ф. (Начальник отдела); Шишкина Я. О.
	Разработка методических документов по ЗИ	
	Мониторинг федеральной информационной среды	
Работа с системой защиты информации (СЗИ)	Проведение анализа и оценки состояния СЗИ	Курбатов А. Ф. (Начальник отдела); Котельникова С. В.
	Анализ защищенности объектов информатизации	
	Планирование мероприятий по организации ЗИ в автоматизированных системах, вычислительных сетях и средствах вычислительной техники (АС, ВС и СВТ)	
Работа по методическому обеспечению информационной безопасности университета	Разработка и анализ модели угроз безопасности информационной системы	Курбатов А. Ф. (Начальник отдела)
	Анализ защищенности системы и соответствия требованиям по ЗИ	
	Разработка требований по ЗИ для АС, СВ и СВТ	

Таким образом, в рамках обеспечения информационной безопасности отделом выполняют 4 глобальных бизнес-процесса. За каждым закреплен определенный специалист, а контроль за выполнением возложен на начальника отдела.

Стоит обратить внимание не такие блоки работы отдела защиты информации как:

- работа системой защиты информации;

– работа по методическому обеспечению информационной безопасности университета.

Данные блоки являются важными, потому что сейчас киберпреступность не стоит на месте и попытки шифрования, взлома и других неправомерных действий могут происходить ежечасно. Целью попыток проникнуть в сеть организации чаще всего является кража персональных данных.

В настоящее время ценность персональных данных велика, ведь это идентификаторы личности, с помощью которых можно совершать преступления от другого лица. По этой причине сложно преуменьшать необходимость обеспечения информационной безопасности персональных данных.

2.2 Модель бизнес-процесса «Обеспечение работы с персональными данными проживающих в общежитиях СФУ»

В Сибирском федеральном университете для работы с персональными данными работников и обучающихся используются информационные системы и человеческие ресурсы. В отделе защиты информации проводятся проверки подразделений, которое кроме отслеживания соблюдений правил и норм обеспечения защиты информации еще и помогают составлять общую картину работы с персональными данными в подразделениях.

К сожалению, но на данный момент не все хранимые персональные данные защищены и обрабатываются только системами. Как и любой другой российской организации обеспечение информационной безопасности персональных данных имеет ряд прорех, которые с течением времени закрываются.

В рамках выбранных процессов отдела защиты информации на данный момент выявлено, что в общежитиях нет информационной системы для работы с персональными данными, но она ведется. Поэтому необходимо заострить внимание именно на этом бизнес-процессе.

Сбор персональных данных и дальнейшая работа с ними осуществляется при заселении сотрудника или обучающегося в общежитие, поэтому бизнес-

процесс «Обеспечение работы с персональными данными проживающих в общежитиях СФУ» буде рассмотрен в момент заселения.

Рассмотрим данный бизнес-процесс детально.

Заселяющийся приходит в свое общежитие. Заполняется договор, куда вносятся такие персональные данные как Ф. И. О., паспортные данные, адрес прописки. После заполнения договора ему присваивается номер согласно журналу регистрации. Каждый из заселяющихся проходит необходимый инструктаж, за прохождение которого он расписывается в журналах. После чего происходит заселение. После всех заселений происходит формирование статистики этого дня, в которой необходимо учесть количество заселившихся, их комнаты и договоры. Для ведения статистики пустых и заселенных комнат используется еще один журнал, в котором распределены все комнаты и указано количество мест в них. Если комната заселена, то в соответствующей ячейке написано кем.

После заполнения всех журналов, внесение данные в документ Excel формируемся отчет для Управления общежитий. Далее этот отчет отправляется по электронной почте.

Данный вид взаимодействия между общежитиями и Управлением общежитий (п электронной почте) имеет постоянный характер. На протяжении года правление запрашивает необходимые данные, а заведующие составляются необходимую статистику из документов на компьютере и имеющихся журналов. А получившийся отчет отправляется по электронной почте. Такой тип взаимодействия имеет постоянный характер, но особое внимание стоит уделить именно заселению, потому что набор персональных данных в нем максимален, но это также является работой с персональными данными проживающих в общежитии.

Для отражения всех нюансов бизнес-процесса ««Обеспечение работы с персональными данными проживающих в общежитиях СФУ» необходимо представить бизнес-процесс при помощи моделирования в разных нотациях. Для представления выбраны нотации:

- DFD;

– IDEF0;

– EPC.

Рассмотрим графическое представление модели «как есть» в нотации DFD, которая представлена на рисунке 7.

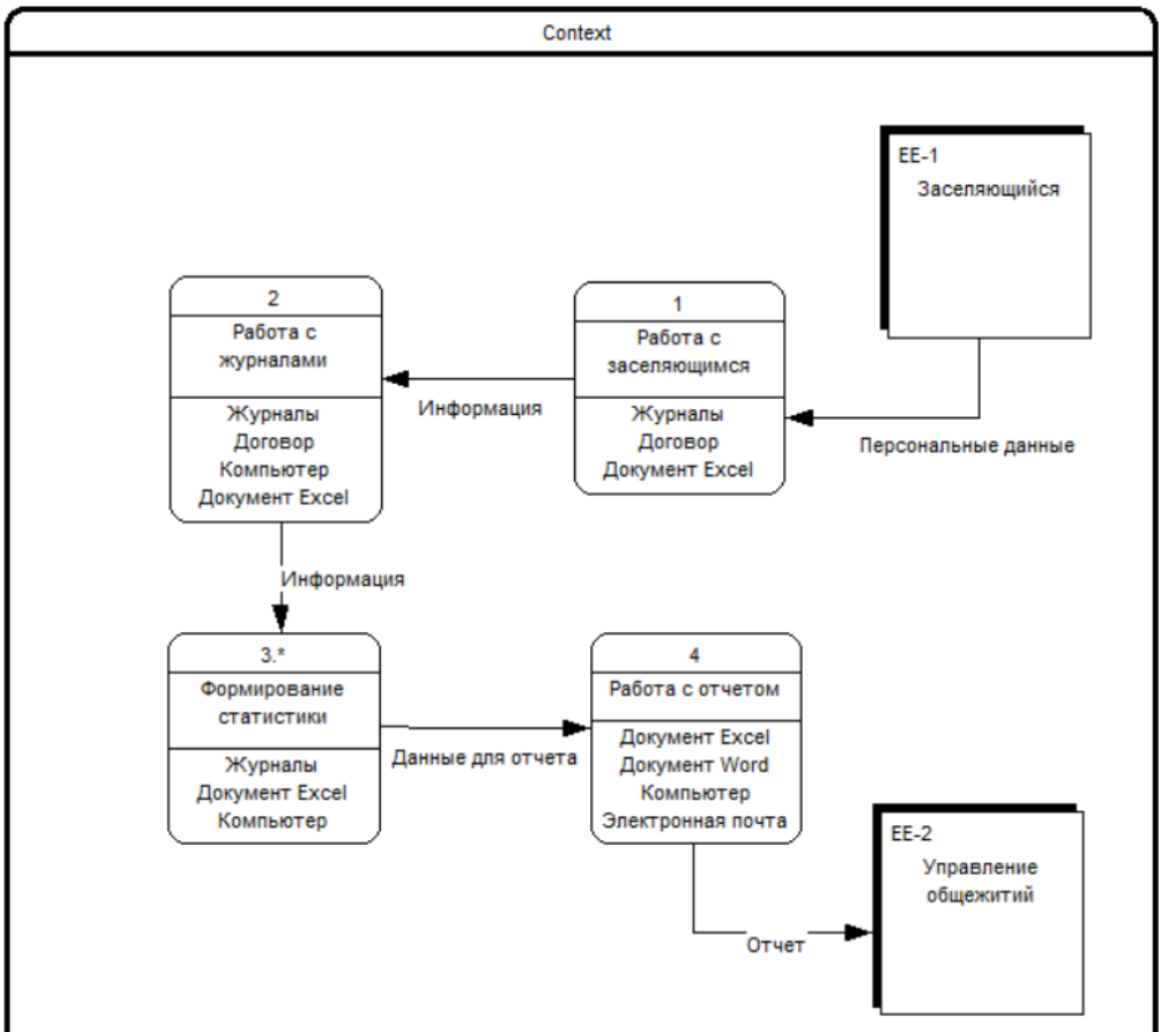

Рисунок 7 – Модель «как есть» бизнес-процесса «Обеспечение работы с персональными данными проживающих в общежитиях СФУ»

Модель содержит:

– 2 внешние сущности (заселяющийся, управление общежитий);

– 4 процесса (работа с заселяющимся, работа с журналами, формирование отчетности, работа с отчетом);

– 6 вариантов используемых ресурсов (журналы, договор, документ Excel, компьютер, документ Word, электронная почта).

Модель «как есть» имеет детализацию процессов, это можно определить по наличию звёздочки около процесса. Как видно из рисунка 7 модель имеет детализации процесса «Формирование статистики». Детализация представлена на рисунке 8.

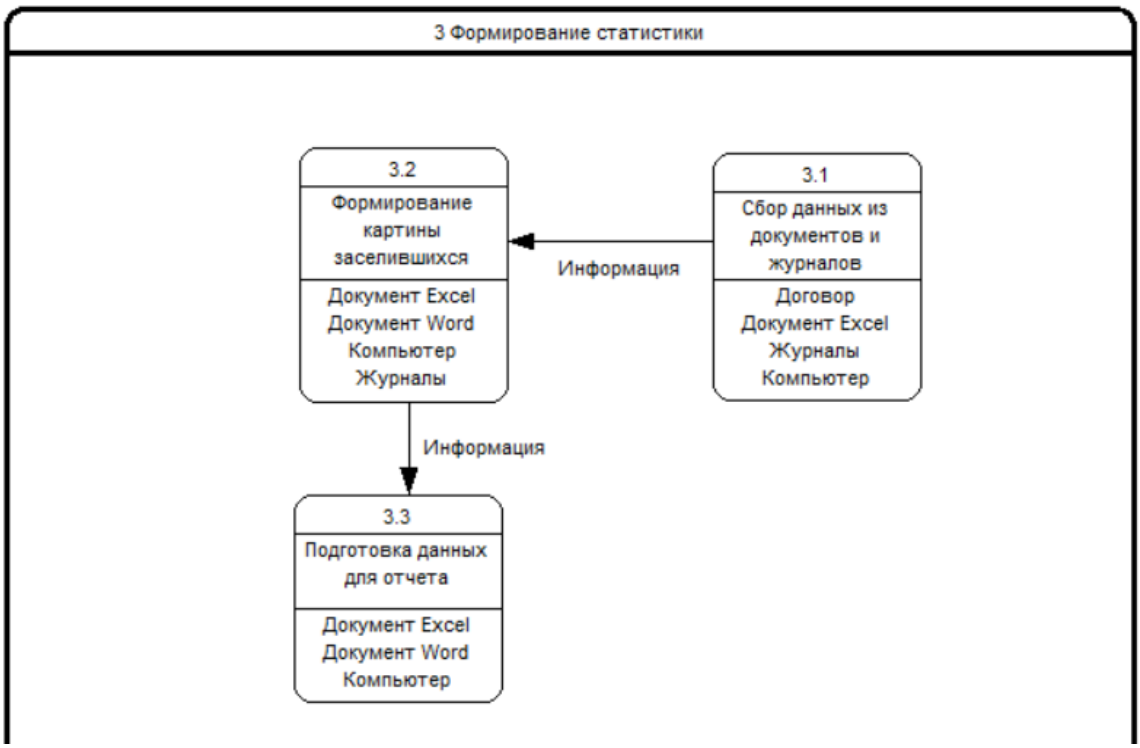

Рисунок 8 – Детализация блока 3 в модели бизнес-процесса «Обеспечение работы с персональными данными проживающих в общежитиях СФУ»

Модель содержит:

– 3 процесса (сбор данных из документов и журналов, формирование картины заселившихся, подготовка данных для отчета);

– 5 вариантов используемых ресурсов (журналы, договор, документ Excel, компьютер, документ Word).

Данная DFD модель показывают циркуляцию информации между процессами, используемые ресурсы на каждом этапе процесса, внешние сущности, которые являются частью процесса.

Диаграмма, представленная в нотации IDEF0, которая позволяет составить одну модель, которая будет отражать процесс со всеми нюансами взаимодействия, распределения ресурсов, входящих и исходящих потоков.

На рисунке 9 представлена контекстная диаграмма бизнес-процесса «Обеспечение работы с персональными данными проживающих в общежитиях СФУ».

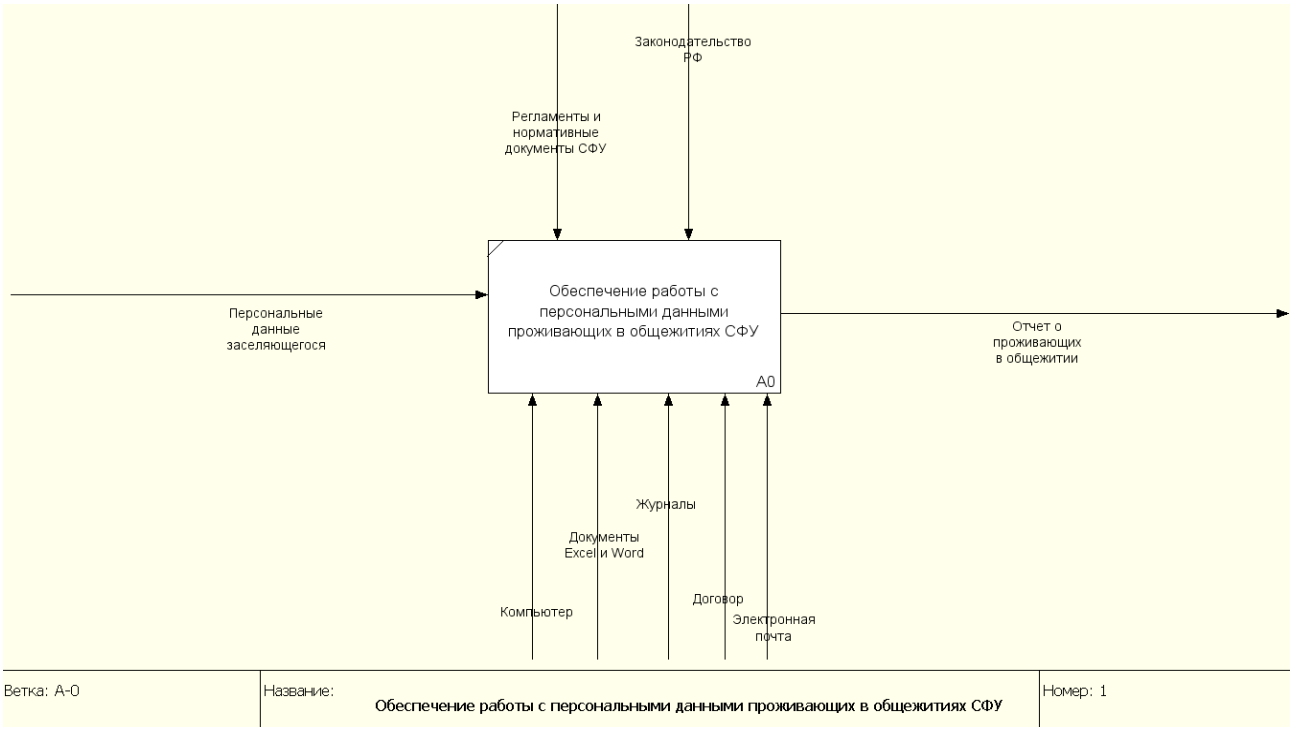

Рисунок 9 – Контекстная диаграмма бизнес-процесса «Обеспечение работы с персональными данными проживающих в общежитиях СФУ»

Как видно из рисунка 9 на входе в процесс персональные данные заселяющегося, на выходе – отчет о проживающих в общежитии. Также управление: регламенты и нормативные документы Сибирского федерального университета, контролирующие организацию, законодательные документы, а механизмы – компьютер, документы, разработанные в программах Microsoft .Excel и Word, договор, который заключается при заселении, электронная почта, по каналам которой отправляется информация.

Данная контекстная диаграмма имеет детализацию, которая представлена на рисунке 10. Как и в прошлой диаграмме в нотации DFD, данная нотация позволяет отражать регуляторы процесса.

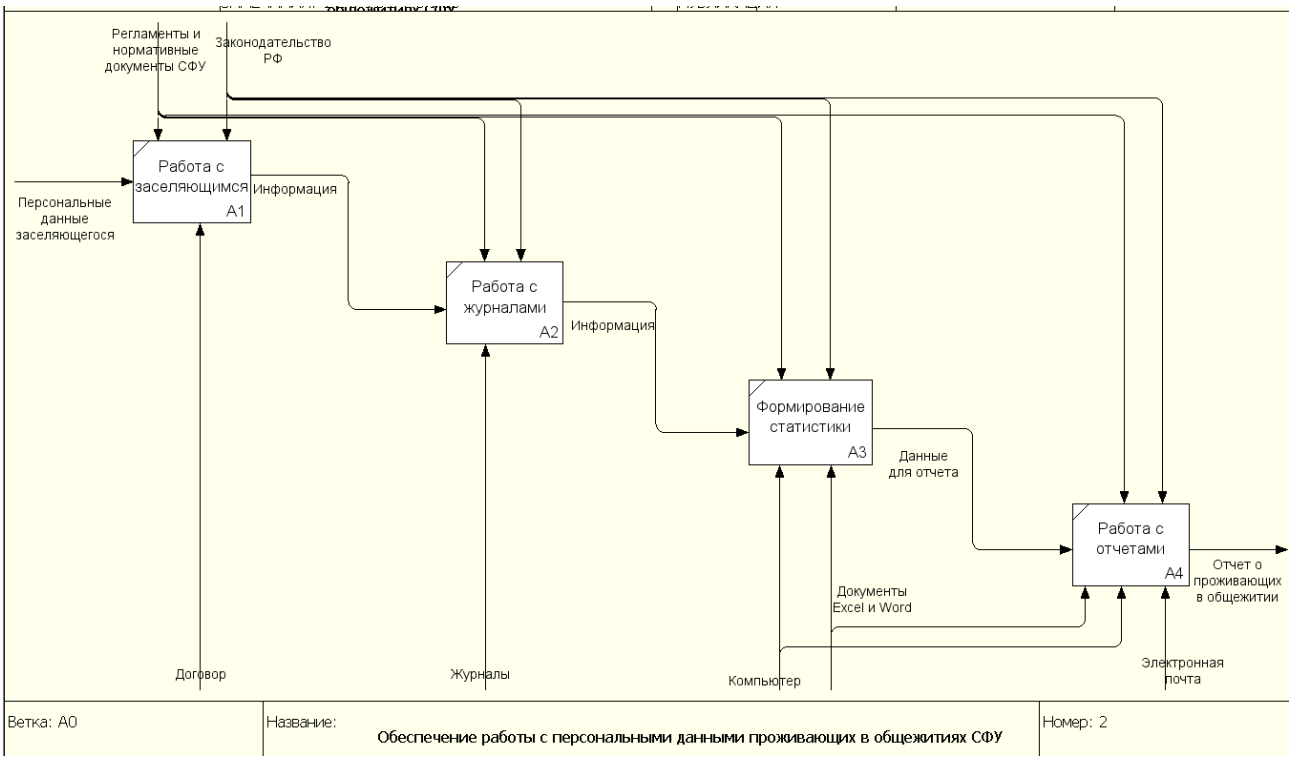

Рисунок 10 – Детализация контекстной диаграммы

На данной представлена детализация контекстной диаграммы. Как и в нотации DFD на рисунке 11 приставлена детализация блока 3 «Формирование статистики».

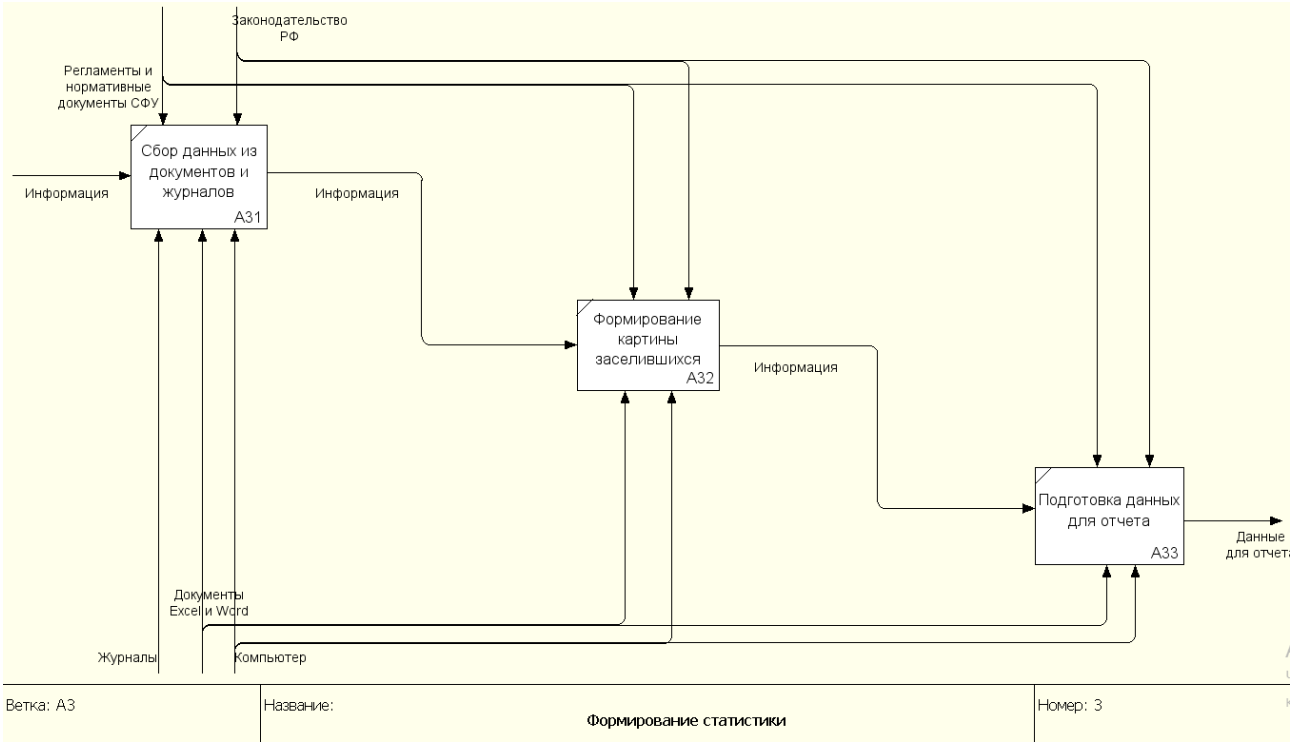

Рисунок 11 – Детализация блока «Формирование статистики»

Как и в нотации DFD, детализация контекстной диаграммы имеет 4 блока, а детализация для блока «Формирование статистики» имеет 3 блока.

Данные диаграммы доступны и понятны, но не отражают процесс детально, поэтому для описания в подробностях использована нотация EPC. На рисунке 12 представлена графическая схема в данной нотации.

Рисунок 12 _ Модель «как есть» бизнес-процесса в нотации EPC, лист 1

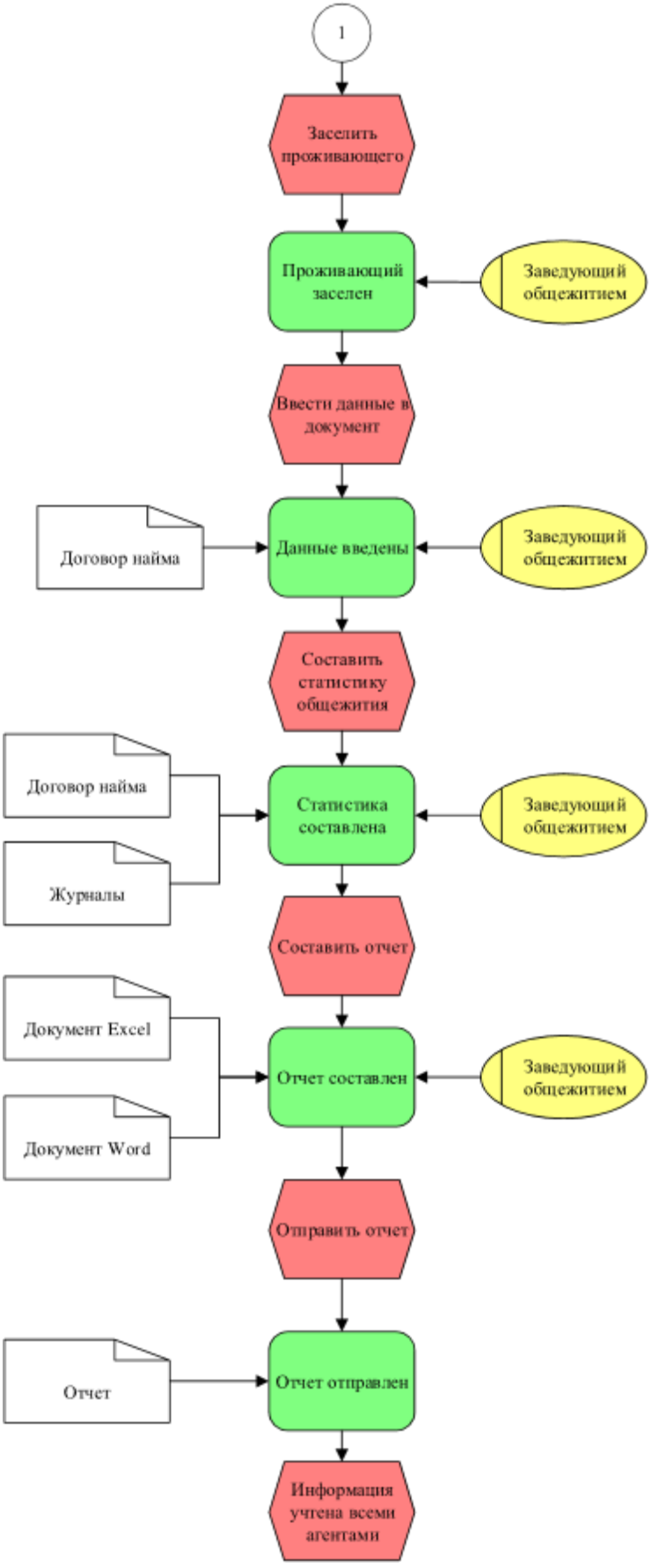

Рисунок 12, лист 2

Таким образом, в данном разделе представлены модели бизнес-процесса «как есть» в нотациях DFD, IDEF0, EPC.

2.3 Анализ и обоснование необходимости реинжиниринга бизнес-процесса «Обеспечение работы с персональными данными проживающих в общежитиях СФУ»

Сибирский федеральный университет является оператором персональных данных зарегистрированных официально, потому с 12 декабря 2006 года внесен в реестр операторов персональных данных Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций [63].

В Сибирском федеральном университете регламентированные такие действия с персональными данными, как сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение.

Цели обработки [63]:

- обеспечение соблюдения законов и иных нормативных правовых актов, договоров;
- обеспечение предоставления образовательных услуг, учебной, научной, инновационной и административно-хозяйственной деятельности;
- содействие работникам и обучающимся в трудоустройстве, обучении и продвижении по службе;
- обеспечение личной безопасности работников и обучающихся;
- контроле количества и качества выполняемой работы;
- получение образовательных услуг;
- обеспечение сохранности имущества; проведения праздничных мероприятий.

Стоит обратить внимание на соблюдение цели про личную безопасность работников и обучающихся. В рамках этой цели большую роль играет информационная безопасность, что уже было указано ранее.

Рассмотрим важные характеристики бизнес-процесса «Обеспечение работы с персональными данными проживающих в общежитиях СФУ».

В таблице 2 представлен перечень основных характеристик бизнес-процесса и конкретные примеры по изучаемому бизнес-процессу, таких как цель, владелец процесса, его границы, участников, ресурсы. Некоторые из характеристик можно увидеть на моделях, например, ресурсы, но не все.

Таблица 2 – Характеристики бизнес-процесса «Обеспечение работы с персональными данными проживающих в общежитиях СФУ»

Характеристика процесса	Описание
Цель процесса	Обеспечение актуальности информации о состоянии заселенности общежитий, хранение персональных данных
Владелец процесса	Управление общежитий
Границы процесса	Верхняя граница: заселение сотрудника, обучающегося СФУ. Нижняя граница: выселение сотрудника, обучающегося СФУ
Последовательность операций процесса	Работа с заселяющимся _ работа с журналами _ формирование статистики _ работа с отчетом
Участники процесса	Заведующие общежитиями, Управление общежитий, сотрудники, учащиеся заселяющиеся и в последствии живущие в общежитии
Входящая информация	Персональные данные сотрудников, учащихся заселяющихся и в последствии живущих в общежитии
Исходящая информация	Данные для отчета
Поставщики информации	Сотрудники, учащиеся заселяющиеся и в последствии живущие в общежитии
Потребители информации	Управление общежитий
Ресурсы процесса	Журналы, договор, документ Excel, компьютер, документ Word, электронная почта

В таблице 2 представлено описание бизнес-процесса «Обеспечение работы с персональными данными проживающих в общежитиях СФУ», где выделены ключевые характеристики процесса. Взаимодействие административного персонала общежитий с управлением общежитий происходит постоянно, но методика взаимодействия не меняется. Согласно внутренним документам Си-

бирского федерально университета взаимодействие между удаленными подразделениями должно осуществляться с помощью корпоративной почты, и согласно российскому законодательству еще существует метод личного или почтового предоставления информации на дальние расстояния.

Что касается электронной почты, то по личным соображениям некоторых сотрудников они пользуются не корпоративным доменом. Это создает угрозы утечки информации и персональных данных, что является одной из причин для реинжиниринга данного бизнес-процесса.

Также во внутренних документах Сибирского федерального университета по части защиты информации особое внимание уделяется резервному копированию. Это создают предпосылки к утере важной электронной информации в случае реализации угроз безопасности (технические сбои, воздействие вирусов, и др.), восстановление которой потребует дополнительное время, технические и людские ресурсы.

Еще угрозами для обеспечения информационной безопасности является отсутствие утвержденного единого комплекта документов по учету проживающих. В общежитиях количество учетных документов различно и колеблется до трех-четырех, они могут иногда дублировать друг друга, при этом также отсутствуют единые формы документов, часто ведутся просто списки проживающих на отдельных неучтенных листах, после изменения данных эти листы уничтожаются неустановленным порядком, чаще всего просто рвутся и выбрасываются. Документы, содержащие персональные данные, не всегда учитываются, передаются без соответствующих записей в журналах учета, например на вахту ДДС.

На данный момент важным ресурсом данного бизнес-процесса являются человеческие ресурсы. Управление общежитий насчитывает десятки сотрудников: заведующие общежитий, тьютеры, кастелянши, а также административный персонал (специалисты) управления общежитий, начальник. Все сотрудники

территориально разбросаны по городу Красноярску, как показано на рисунке 13 [54].

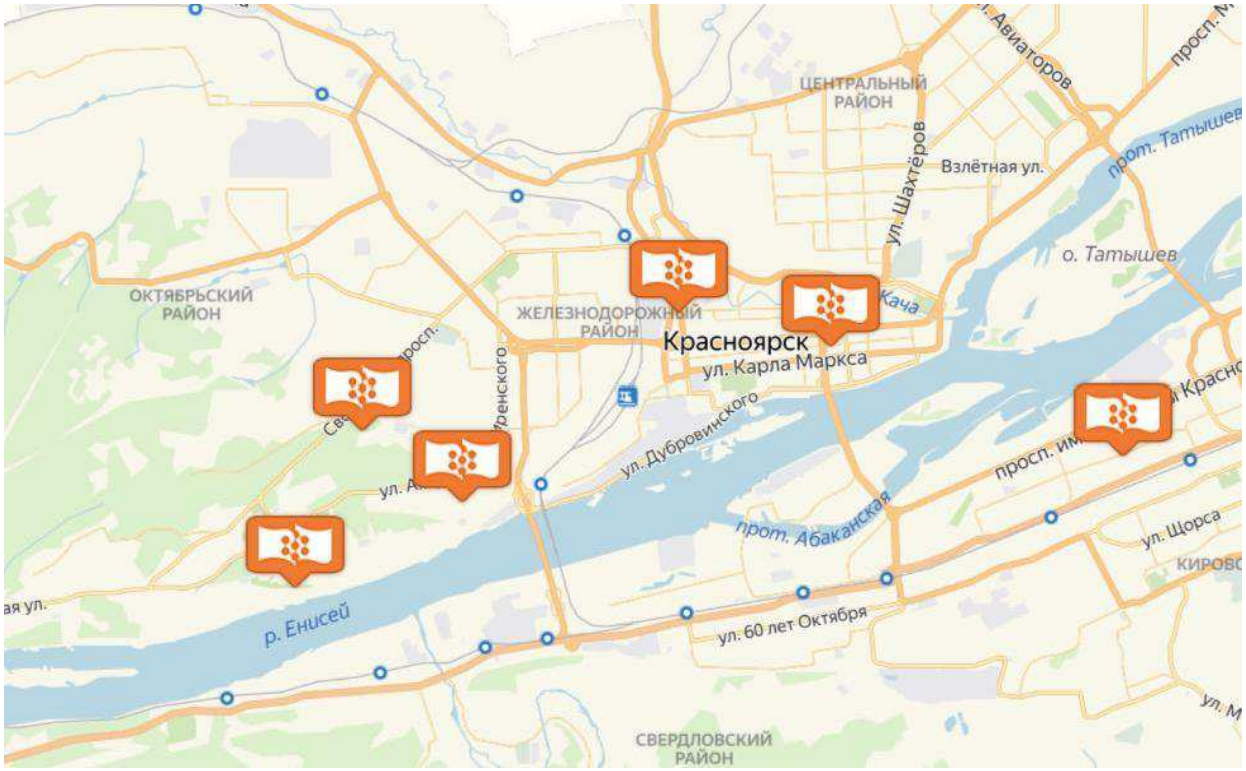

Рисунок 13 – территориальное распределение подразделений управления общежитий

На рисунке 13 не показано конкретное расположение, а представлено распределение площадок, на которых есть несколько общежитий.

Такое территориальное расположение также является основанием для реинжиниринга, потому что взаимодействие на расстоянии необходимо регламентировать и обеспечивать.

Человеческие ресурсы в данном процессе представлены большим количеством людей – это и заселяющиеся, и сотрудники управления общежитий. Для более четкого представления взаимодействия между ними проведем качественный анализ бизнес-процесса.

Качественный анализ бизнес-процесса «Обеспечение работы с персональными данными проживающих в общежитиях СФУ» будет выполнен с помощью:

– картирования взаимодействий – это представление того, кто участвует в процессе и как они взаимодействуют друг с другом и с окружающим миром;

– межфункциональной блок-схемы. Данное графическое представление дает дополнительную возможность установить, кто выполняет то или иное действие, к какому функциональному отделу принадлежат исполнители [64].

На рисунке 14 представлена карта взаимодействия внутри бизнес-процесса «Обеспечение работы с персональными данными проживающих в общежитиях СФУ», на котором видны задействованные сотрудники и циркулирующие документы.

Рисунок 14 – Карта взаимодействий бизнес-процесса «Обеспечение работы с персональными данными проживающих в общежитиях СФУ»

В данном бизнес-процессе задействованы:

– сотрудники управления общежитий, отдельно выделены заведующие общежитий, потому что они первыми получают персональные данные заселяющихся;

– сотрудники, обучающиеся, которые заселяются и в последствии будут жить в общежитии.

Как видно из 14 рисунка взаимодействие основывается на персональных данных, а это взаимодействие необходимо защищать согласно законодательст-

ву Российской Федерации, что не предполагает использование незащищенных каналов, некорпоративной электронной почты.

Межфункциональная блок-схема дает дополнительную возможность установить, кто выполняет то или иное действие, к какому функциональному отделу принадлежат исполнители [65]. Межфункциональная блок схема бизнес-процесса «Обеспечение работы с персональными данными проживающих в общежитиях СФУ» можно увидеть на рисунке 15.

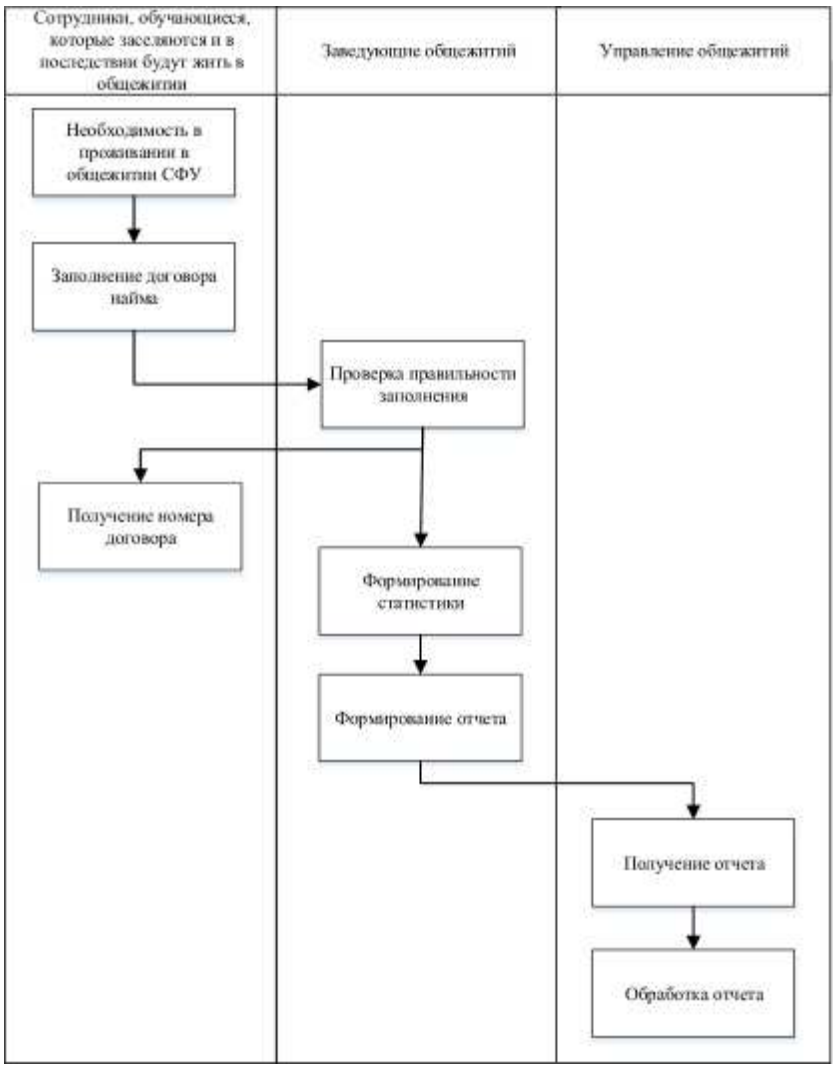

Рисунок 15 – Межфункциональная схема бизнес-процесса « Обеспечение работы с персональными данными проживающих в общежитиях СФУ»

Как видно из 15 рисунка, данный процесс включает 3 функциональных подразделения, сотрудники которых задействованы в процессе. То показывает распределение функциональных действий между людьми, и оно не совсем равноправно разделено.

Стоит отметить, что согласно вышеперечисленному необходимо подвергнуть реинжинирингу бизнес-процесс «Обеспечение работы с персональными данными проживающих в общежитиях СФУ» по причине необоснованной нагрузка заведующих общежитий, которое можно заменить автоматизированной работой информационной системы. Также важной причиной является соблюдение российского законодательства по части защиты информации, потому что для подобного рода бизнес-процессов необходимо использование только корпоративной почтой и только по защищенным корпоративным каналам.

3 Разработка информационной технологии для бизнес-процесса «Обеспечение работы с персональными данными проживающих в общежитиях СФУ»

3.1 Модель реинжиниринга бизнес-процесса «Обеспечение работы с персональными данными проживающих в общежитиях СФУ»

Как было установлено в предыдущем разделе для бизнес-процесса «Обеспечение работы с персональными данными проживающих в общежитиях СФУ» нуждается в реинжиниринге.

Было установлено, что в настоящее время в данном бизнес-процессе имеются такие проблемные вопросы, как:

- резервное копирование;
- обеспечение информационной безопасности персональных данных сотрудников, обучающихся, заселяющихся и в последствии проживающих в общежитиях;
- формирование статистки проживающих;
- обеспечение информационной безопасности персональных компьютеров;
- возможность коммуницировать на дальние расстояния.

В настоящее время база по проживающим в Управлении общежитий ведется в программе Excel, а заведующие общежитиями ведут базу вручную отмечая в журнале проживающих, что затрудняет получать точные данные о проживающих и создает предпосылки реализации угроз информационной безопасности.

В качестве реинжиниринга для бизнес-процесса «Обеспечение работы с персональными данными проживающих в общежитиях СФУ» выбрана разработка информационной технологии.

Информационная технология – использование совокупности средств и методов организации информационных процессов, сформированных на основе

современной системы научных и инженерных знаний, в интересах получения информации нового качества о состоянии объекта, процесса или явления [73].

Информационная технология, разрабатываемая при реинжиниринге – система управления проживающими в общежитиях (далее СУПО).

Информационная система обеспечит получение своевременной и точной информации за счет оперативного ввода данных о заселении, переселении, выселении, задолженности за проживание у сотрудников и студентов. Информационная система является многопользовательской, предназначена для использования всеми подразделениями Управления общежитий, централизованно хранит данные о всех общежитиях и проживающих, что позволит оперативно формировать отчеты, необходимые для ежедневной работы инженерам, заведующим общежитий и тьютерам Управления общежитий.

Учитывая, что информационная система будет обрабатывать персональные данные проживающих в общежитиях, она будет создаваться с учетом требований по защите персональных данных и должна обеспечить информационную безопасность системы.

Внедрение программы обеспечит оперативное и своевременное получение информации, ускорит планирование и контроль исполнения задач в Управлении общежитий.

Рассмотрим модели бизнес-процесса «Обеспечение работы с персональными данными проживающих в общежитиях СФУ» с использованием новой информационной технологии.

Как и в предыдущем разделе для графического представления данного бизнес-процесса будет использованы нотации DFD, IDEF0 и EPC. Модели «как должно быть» включают в себя действия с новой информационной технологией. Данная система буде иметь название «Система управления проживающими в общежитиях» или СУПО. Система соответственно будет иметь свою база данных – БД СУПО, которая будет содержать все персональные данные проживающих, из-за чего пропадет необходимость в журналах.

Теперь бизнес-процесс будет выглядеть так: заселяющийся сотрудник, обучающийся также приходит на заселение и получает договор для заполнения. В договор вносятся персональные данные, в последствии ему будет присвоен свой идентификационный номер. После завершения заселения и работы с вселяющимся начинается работа с информационной системой. В систему вносятся все необходимые данные, к которым имеют доступ как заведующие, так и специалисты управления общежитий.

На рисунке 16 представлен бизнес-процесс «Обеспечение работы с персональными данными проживающих в общежитиях СФУ» в нотации DFD в интерпретации «как должно быть».

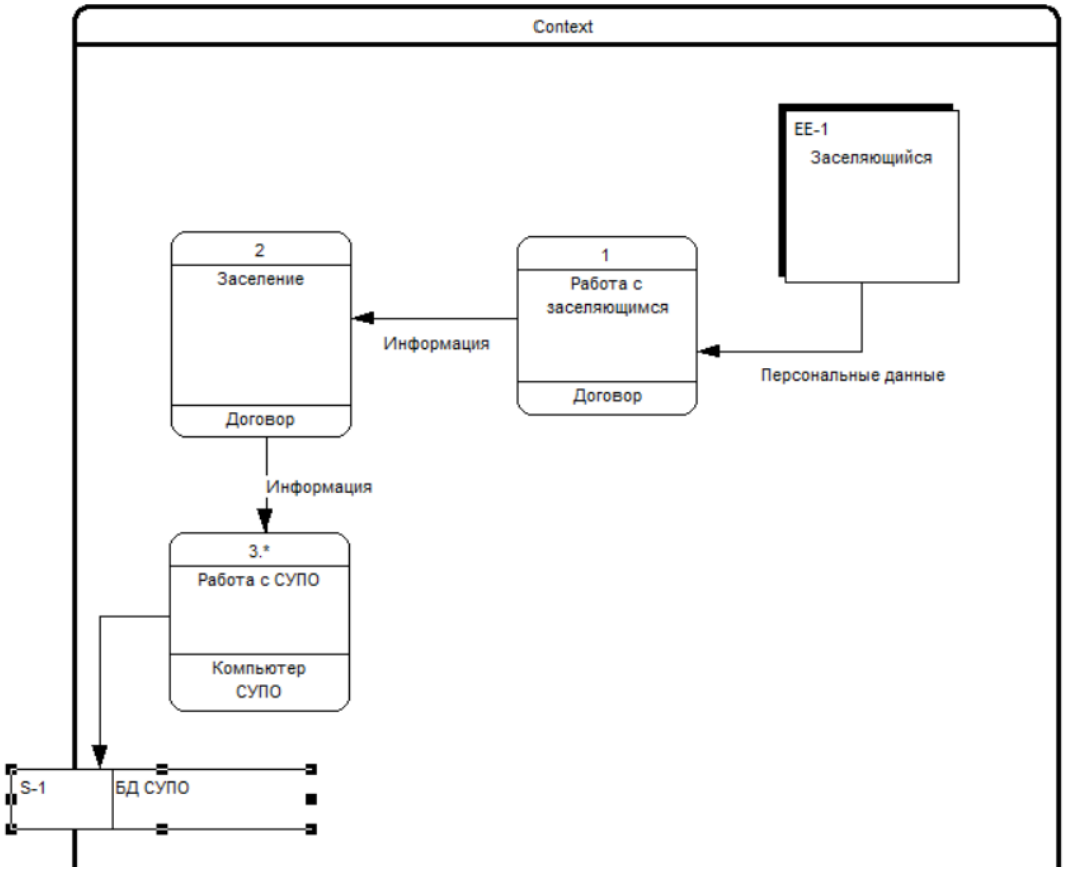

Рисунок 16 – Модель «как должно быть» бизнес-процесса «Обеспечение работы с персональными данными проживающих в общежитиях СФУ» в нотации DFD

Как видно из рисунка 16 данная модель теперь содержит:

– 1 внешнюю сущность (заселяющийся);

- 3 процесса (работа с заселяющимся, заселение, работа с СУПО);
- 1 накопитель данных (база данных СУПО).

Теперь диаграмма не нуждается в детализации, потому что все действия с системой производятся просто и не требуют регламентации, только необходимо обучение сотрудников для работы с системой.

На рисунках 17 представлено графическое представление «как должно быть» контекстной диаграммы бизнес-процесса «Обеспечение работы с персональными данными проживающих в общежитиях СФУ» в нотации IDEF0.

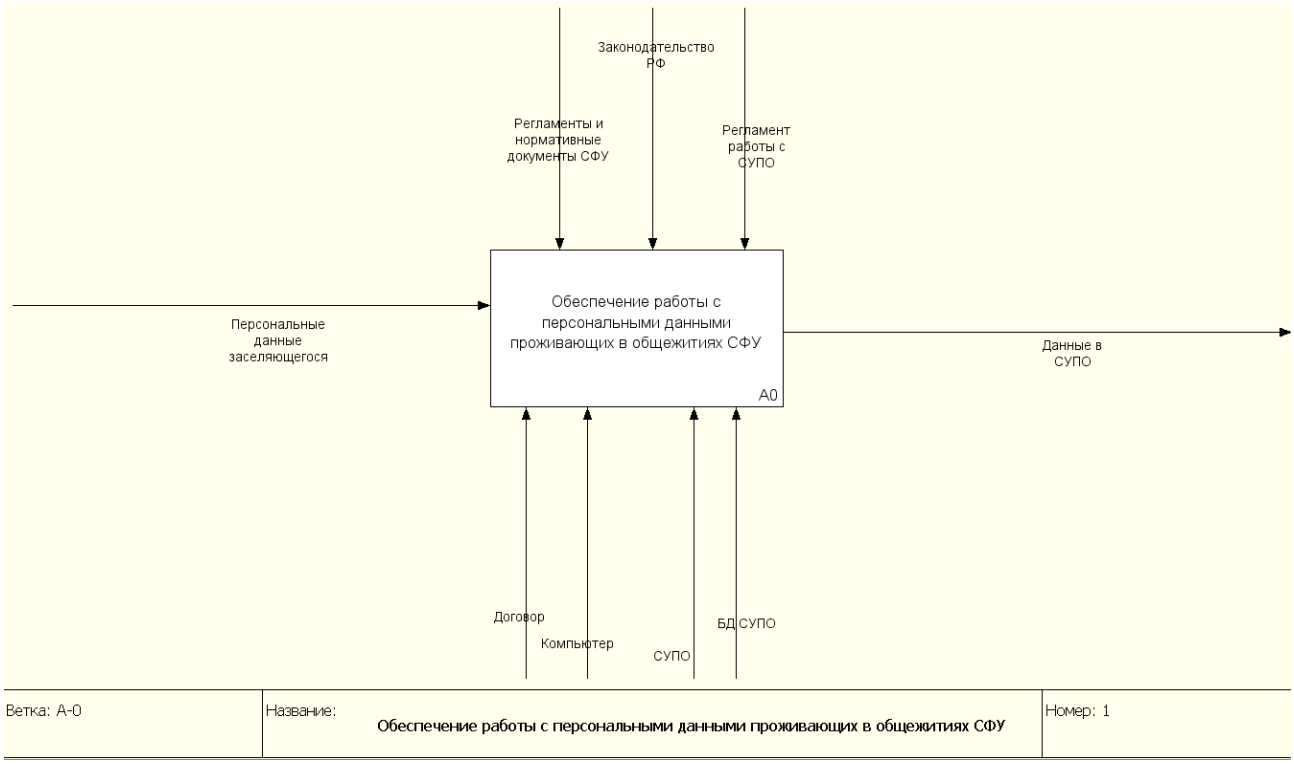

Рисунок 17 – Контекстная диаграмма модели «как должно быть» бизнес-процесса «Обеспечение работы с персональными данными проживающих в общежитиях СФУ» в нотации IDEF0

Данная контекстная диаграмма в ресурсах имеет базу данных СУПО и саму систему, и учитывает отдельно регламент ля работы с данной системой, потому что после ввода в использование сначала нужно будет обращаться к нему.

На рисунке 18 представлена детализация контекстной диаграммы бизнес-процесса «Обеспечение работы с персональными данными проживающих в общежитиях СФУ» в нотации IDEF0.

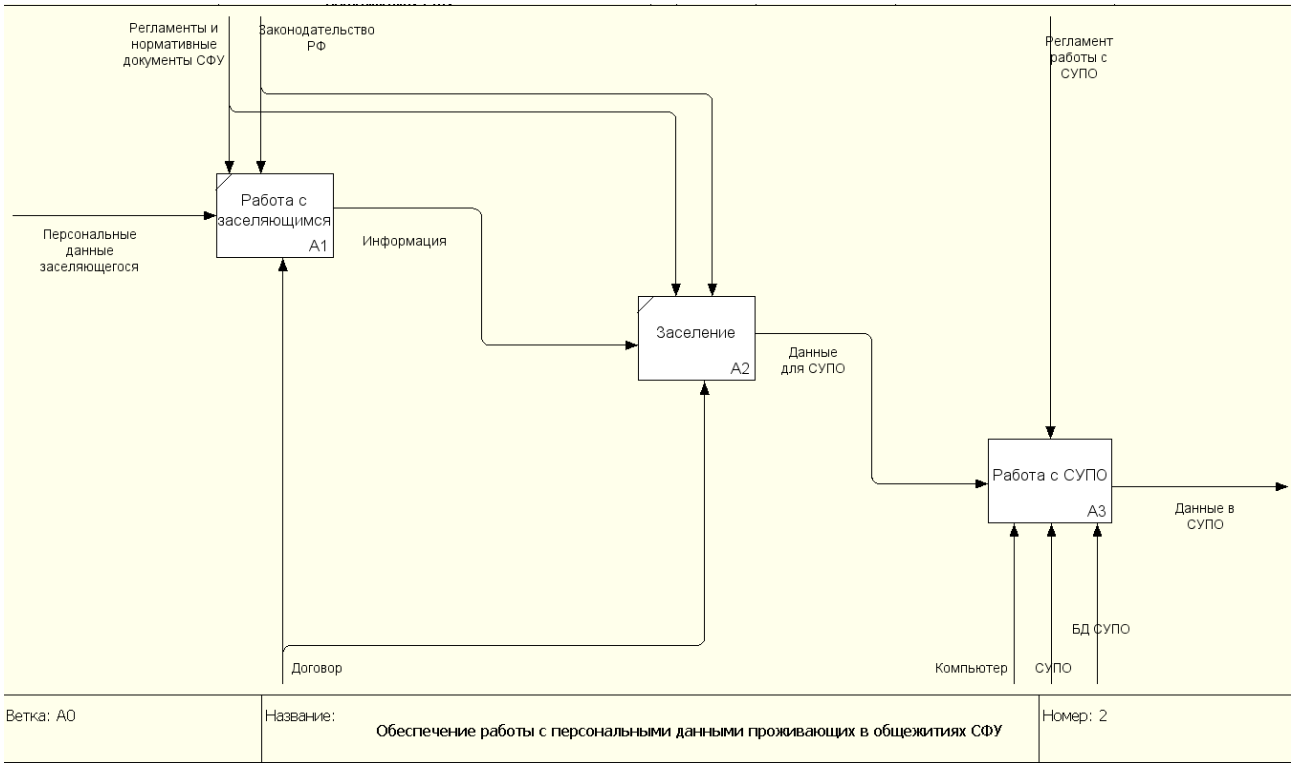

Рисунок 18 _ Детализация контекстной диаграммы модели «как должно быть» бизнес-процесса «Обеспечение работы с персональными данными проживающих в общежитиях СФУ» в нотации IDEF0

Как видно из представленных графических моделей «как должно быть» введение СУПО в работу административного персонала общежитий и управления общежитий упростит взаимодействие между административным персоналом и специалистами управлениями.

Как и раньше, работа с персональными данными не ограничивается только заселением, в период проживания также необходимо запрашивать определенный набор персональных данных, поэтому работа с системой актуальна на всем периоде проживания заселившегося.

Далее на рисунке 19 бизнес-процесс «Обеспечение работы с персональными данными проживающих в общежитиях СФУ» представлен в нотации EPC.

Рисунок 19 _ Модель «как должно быть» в нотации EPC

Управление общежитий насчитывает большое количество помещений и сотрудников, в таблице 3 представлен перечень необходимых мест для внедрения данной информационной технологии.

№	Месторасположение	Помещение
1.	Управление общежитий, начальник	пр. Свободный, д. 80, пом.7
2.	Управление общежитий, приемная	пр. Свободный, д. 80, пом.7
3.	Управление общежитий, хоз. отдел	пр. Свободный, д. 80, пом. 6
4.	Управление общежитий, отдел по воспитательной работе	пр. Свободный, д. 80, пом.4
5.	Управление общежитий, специалист	пр. Свободный, д. 80, пом.5
6.	Управление общежитий, инженер	пр. Свободный, д. 80, пом.8
7.	Общежитие № 1	ул. Академгородок, д. 8, пом. 106
8.	Общежитие № 2	пр. Свободный, д. 81, пом. 118, 122
9.	Общежитие №3	пр. Свободный, д. 83, пом. 121, 122
10.	Общежитие № 4	пр. Свободный, д. 81 В, пом. 113
11.	Общежитие № 5	ул. Борисова, д. 24, пом. 100
12.	Общежитие № 6	ул. Борисова, д. 14А, пом.71
13.	Общежитие №7	ул. Борисова, д. 1, пом. 105
14.	Общежитие № 8	ул. Борисова, д. 6, пом. 107, 106
15.	Общежитие № 9	ул. Борисова, д. 8, пом. 105
16.	Общежитие № 10	ул. Борисова, д. 10,
17.	Общежитие № 11	ул. Борисова, д. 22, пом. 121
18.	Общежитие № 12	ул. Вавилова, д. 64, пом. 128
19.	Общежитие № 13	ул. Вавилова, 60, пом.117
20.	Общежитие № 14	пер. Вузовский, д. 8, пом. 104
21.	Общежитие № 15	пер. Якорный, д. 4, пом.112, 111
22.	Общежитие № 16	ул. Вавилова, д. 47 «Б», пом.116

Окончание таблицы 3

№	Месторасположение	Помещение
23.	Общежитие № 17	пр. Свободный, д. 80, пом.45-46, 56
24.	Общежитие № 18	пр. Свободный, д. 78, пом. 143,
25.	Общежитие № 19	пр. Свободный, д. 76, пом.111
26.	Общежитие № 20	пр. Свободный, пом. 107,109
27.	Общежитие № 21	пр. Свободный, пом. 102
28.	Общежитие № 22	пр. Свободный, пом. Кабинет заведующей
29.	Общежитие № 23	ул. Железнодорожников, пом. 122
30.	Общежитие № 24	ул. Судостроительная, д. 38 «А», пом. 108
31.	Общежитие № 25	пр. Свободный, д. 76 «Ж», пом. кабинет заведующей
32.	Общежитие № 26	пр. Свободный, д. 76 «И»
33.	Общежитие № 27	пр. Свободный, д. 76 «К»
34.	Общежитие № 28	пер. Вузовский, д, 6 «Д», пом. 201
35.	Общежитие № 29	пер. Вузовский, д. 6 «Д», пом. 122, 126
36.	Общежитие № 30 (корпус 1)	ул. Борисова,3, пом. 5
37.	Общежитие № 30 (корпус 2)	ул. Борисова, д. 5, пом. 010

Кроме обеспечения информационной безопасности самой системы на персональных компьютерах административных сотрудников общежитий установлены антивирусные программы. Например, на некоторых стоит антивирус ESET NOD32 Smart Security, который представлен на рисунках 1 и 2 в первом разделе.

Таким образом, в трех нотациях представлены графические модели «как должно быть» бизнес-процесса «Обеспечение работы с персональными данными проживающих в общежитиях СФУ». Рассмотрены возникающие изменения

после введения в бизнес-процесс информационной технологии и приставлен перечень мест, где будет внедрено данное решение.

3.2 Разработка и описание информационной технологии для бизнес-процесса «Обеспечение работы с персональными данными проживающих в общежитиях СФУ»

Как было сказано ранее для реинжиниринга бизнес-процесса «Обеспечение работы с персональными данными проживающих в общежитиях СФУ» выбрана разработка информационной технологии СУПО.

Рассмотрим этапы разработки системы.

Разработка и внедрение новой системы происходит ряд основных этапов: формирование требований к системе; разработка концепции системы; создание технического задания; создание технического проекта; создание рабочей документации; разработка системы; ввод в действия; сопровождение.

В государственных учреждениях, а Сибирский федеральный университет таким и является, данные этапы иногда могут затянуться. Обычно это происходит по причине прохождения большого количества инстанций для одобрения документации и действий.

В программном продукте Microsoft Project возможно учитывать все нюансы работы с разработкой системы и вносить изменения. В частности, рассмотрим возможности программного продукта для временного ресурса. На данный момент распределение этапов по времени представлена на рисунках 20 и 21.

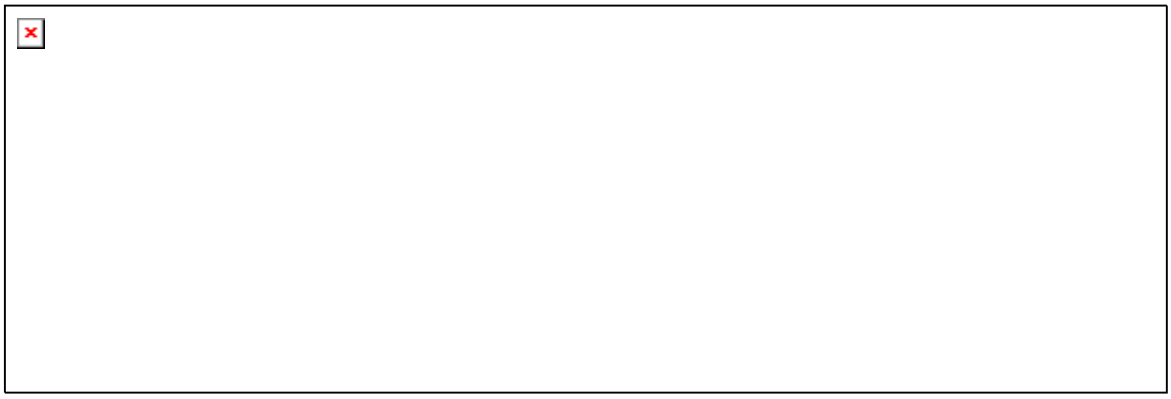

Рисунок 20 Распределение этапов проектирования системы по времени

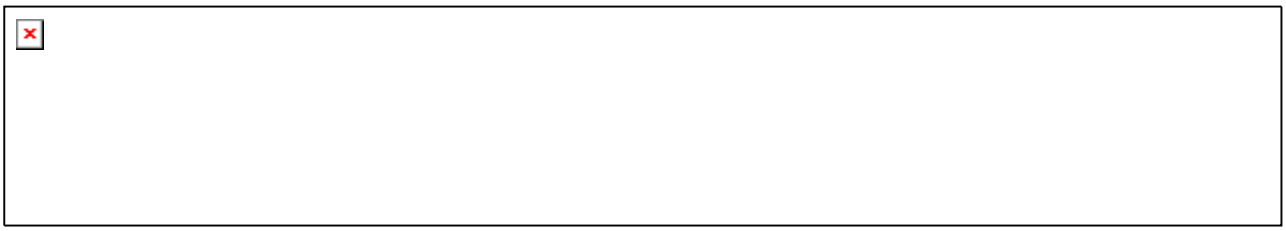

Рисунок 21 Графическое представление этапов проектирования системы

Таким образом, на данный момент проектирование этой системы должно завершится к концу этого года, точнее к 22 ноября.

Каждый этап имеет подэтапы. Это можно увидеть в 4 таблице.

Таблица 4 Детализация этапов проекта системы

№	Название этапа	Подэтапы
1	Формирование требований и разработка концепции системы	Системно-аналитическое обследование объекта
		Анализ и обработка полученной информации
		Концептуальная модель данных
2	Создание технического проекта	Разработка технического задания и приложения к нему
		Согласованное и утвержденное технического задания
3	Создание эскизного проекта	Определение общей функциональной и технической архитектур
		Разработка логической модели данных
		Разработка предварительного регламента взаимодействия
		Эскизное проектирование
		Эскизное проектирование интерфейсов пользователя
		Оформление эскизного проекта
		Согласование и утверждение
4	Создание технического проект	Определение функциональной и технической архитектур
		Формирование плана развертывания системного ландшафта
		Разработка физической модели данных
		Разработка и согласование регламентов взаимодействия системы
		Проектирование процессов
		Проектирование интерфейсов пользователя
		Оформление технического проекта
		Согласование и утверждение

Окончание таблицы 4

	Название этапа	Подэтапы
5	Создание рабочей документации	Разработка рабочей документации
		Разработка или адаптация программ
		Согласование и утверждение
6	Разработка системы	Разработка и адаптация системы
		Согласование и утверждение
7	Ввод в действие	Подготовка объекта к вводу в действие
		Подготовка персонала
		Комплектация системы подставляемыми изделиями
		Проведение предварительных испытаний
		Поведение опытной эксплуатации
		Проведение приемных испытаний
		Завершение работ
8	Сопровождение	Контроль за работой системы
		Проведение профилактических и ремонтных работ

Функционал данной системы можно разработать не только для заведующих общежитий, но и для другого административного персонала общежитий тьютеров и кастилянш. Система позволит и их задачи автоматизировать, ведь эта технология может позволить по-новому выполнять работу административного персонала общежитий.

Система должна обеспечить:

- гибкое планирование индивидуальной структуры общежития;
- учет проживающих в общежитиях (заезд, перемещение, выезд);
- формирование договоров с проживающими;
- учет лиц, дополнительно проживающих на жилплощади совместно с лицом, заключившим договор с общежитием;
- учет наличия койко-мест и их характеристик;
- расчет и контроль осуществления оплаты за проживание, предоставление дополнительных услуг;

- анализ динамики движения денежных средств при предоставлении услуг проживания в разрезе различных показателей и требований;
- отчетность по численности проживающих и дополнительно проживающих, взаиморасчетам и задолженности проживающих, наличию свободных койко-мест, материальным средствам.

Также система позволит:

- обеспечивать контроль за проживающими и организовать оперативный учет заездов/выездов/переселений в 30 и более общежитиях;
- вести учет материальных ценностей, числящихся за общежитием или закрепленных за проживающими;
- вести учет материальных ценностей, находящихся в комнате/номере;
- давать возможность вести учет предоставления дополнительных услуг (прачечная, телефон, …) в общежитии;
- формировать необходимую отчетность в разных аналитических разрезах;
- получать актуальную информацию об оплатах, наличии мест, количестве проживающих, материальных средствах и т.д.;
- все изменения должны указываться на дату, с которой вступает соответствующее изменение, а система формирования отчетов должна учитывать эту информацию при выполнении отчета на указанную дату/период.

Особое внимание в изучаемом бизнес-процессе уделялось затруднениям с отчетность, с которой работают сотрудники управления общежитий, поэтому отметим список генерируемых отчетов:

- закрепление мест в общежитиях за каждым институтом в соответствии с приказом;
- списки проживающих по институтам;
- списки выезжающих на конкретную дату;
- списки проживающих каждого курса;

- свободные места в общежитиях на конкретную дату;
- список живущих на местах не своего общежития;
- места незакреплённые за каким-либо институтом (резерв);
- справка о проживающих на конкретную дату;
- список выселившихся из общежитий на конкретную дату;
- общая и жилая площадь каждой комнаты;
- справка о проживающих в общежитиях СФУ на определённое число;
- сводка о выговорах и поощрениях за период;
- отчёт о наличии отчисленных и не выселенных студентов;
- отчёт о долгах оплаты общежития по проживающим.

Представим проект внешнего вида системы с ключевыми для бизнес-процесса «Обеспечение работы с персональными данными проживающих в общежитиях СФУ» элементами. На рисунке 22 представлено окно создания проживающего при его заселении.

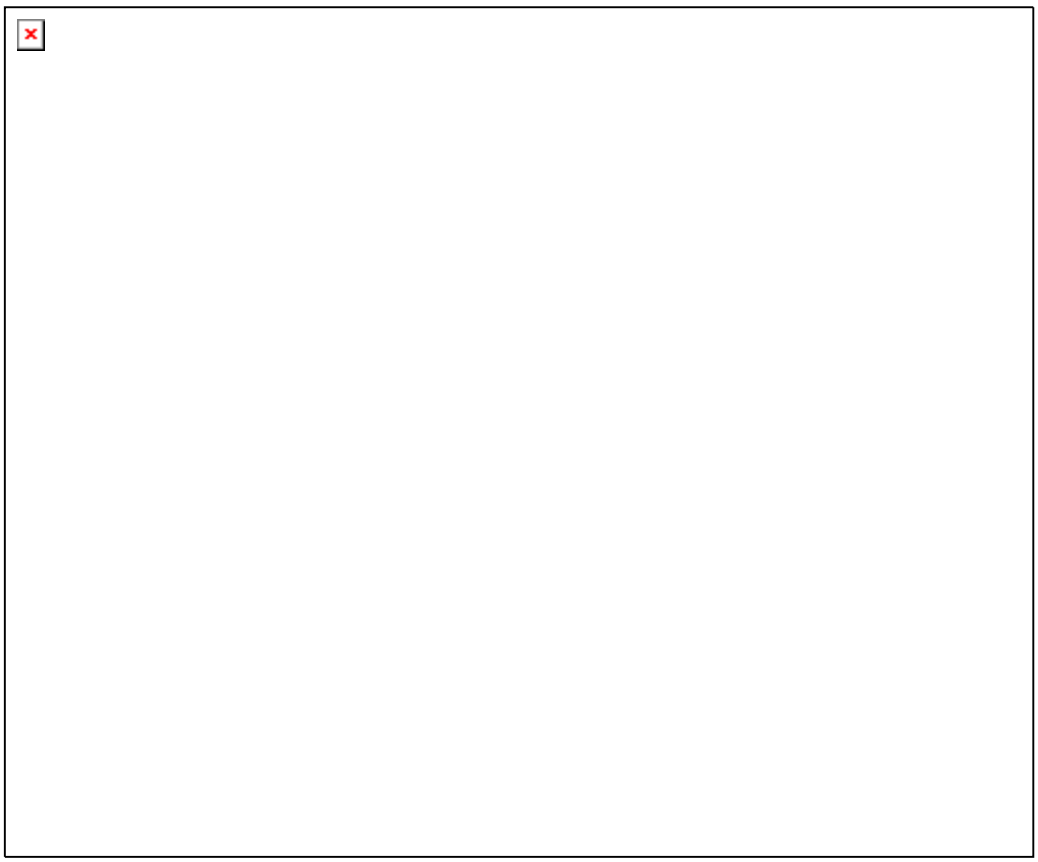

Рисунок 22 – Окно создания/редактирования проживающего

На данном рисунке видно, что в данную форму вносятся персональные данные:

- Ф. И. О.;
- пол;
- гражданство;
- семейное положение;
- социальная категория;
- тип проживающего;
- форма финансирования обучения;
- группа обучения;
- статус обучения;
- дата рождения;
- страна, регион, район и населенный пункт, где проживающий родился;
- паспортные данные;
- фотография.

Также на рисунке 23 представлено окно выселения по договору найма, которое содержит номер договора, что является конфиденциально.

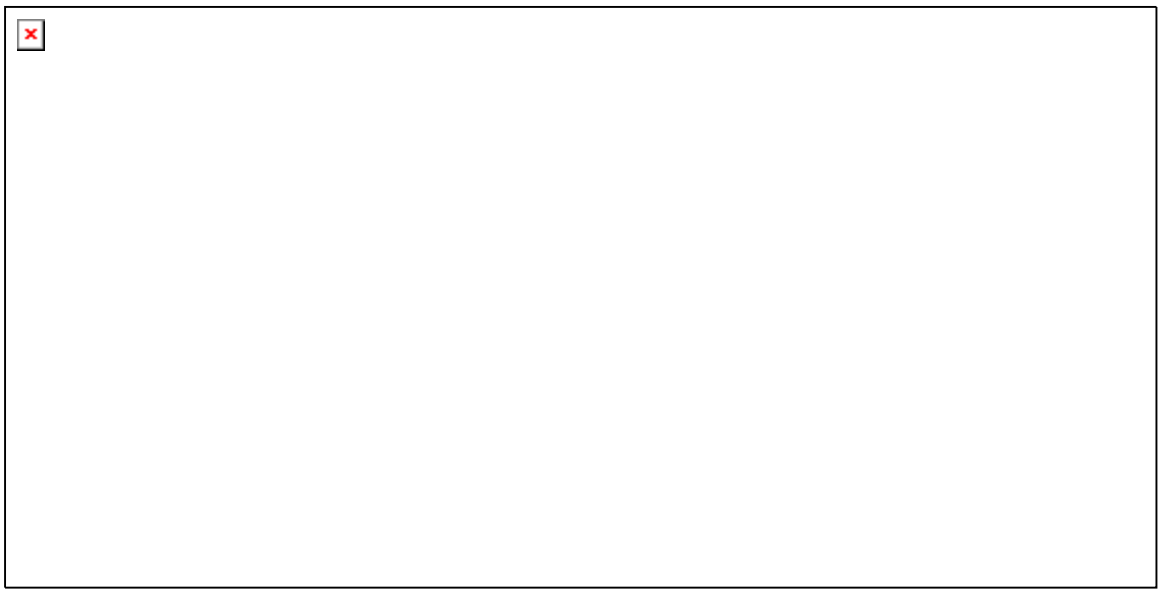

Рисунок 23 – Выселение жителей вселенных по договору найма

Данная система позволяет видеть информацию по комнатам. Пример такого интерфейса представлен на рисунке 24

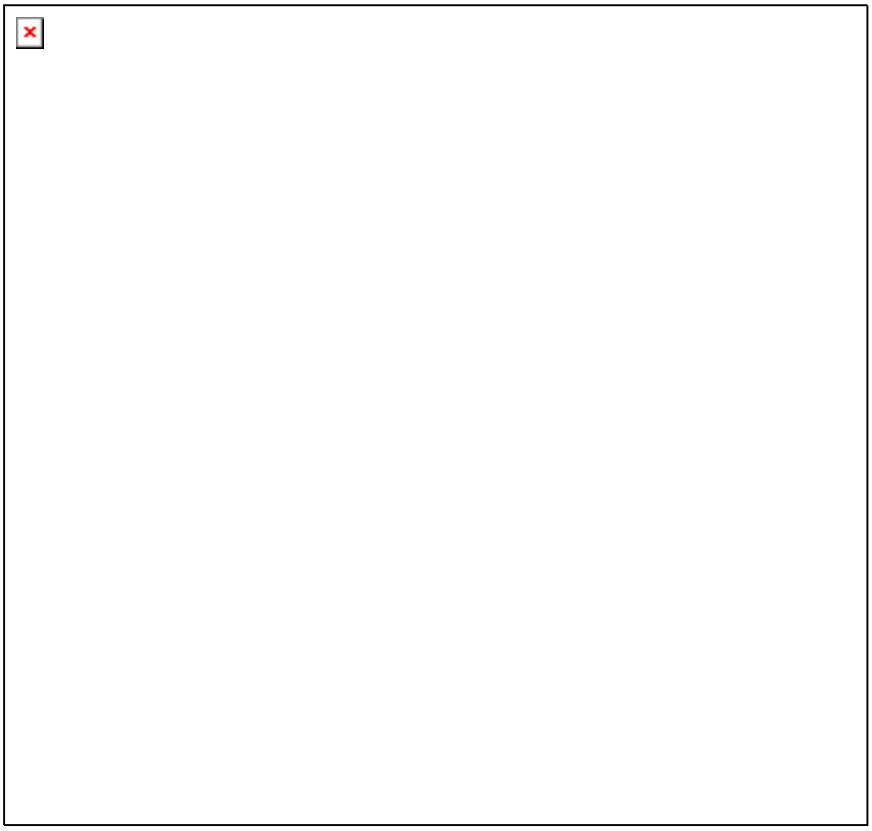

Рисунок 24 – Окно редактирования комнаты после сохранения информации о вселении

Таким образом, данная система позволит не только изменить бизнес-процесс процесса «Обеспечение работы с персональными данными проживающих в общежитиях СФУ», но и кардинально изменить работу всех сотрудников управления общежитий.

Но данную систему необходимо обезопасить согласно нормам информационной безопасности, поэтому необходимо соблюсти ряд мероприятия по аттестации информационной системы.

Так как в Сибирском федеральном университет нет методики аттетации информационных систем далее предлагаю разработанную методику аттестации информационных систем по требованиям защиты персональных данных.

3.3 Требования к информационной безопасности системы и методика проведения аттестации корпоративной информационной системы по требованиям защиты персональных данных

Как и для любой системы, которая работает с персональными данными, по российскому законодательству необходимо обеспечить качественную информационную безопасность системы. С их перечнем можно ознакомится в Постановлении Правительства Российской Федерации № 1119 от 1 ноября 2012 года «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» [78] и в приказе Федеральной службы по техническому и экспортному контролю № 17 от 11 февраля 2013 года «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

Для СУПО рассмотрим некоторые основные характеристики, которые должны быть учтены в системе защиты информации данной информационной технологии.

Система защиты персональных данных должна обеспечить:

- защиту информации от утраты, утечки, уничтожения, искажения, подделки и блокирования доступа к ней за счет несанкционированного доступа и воздействия;
- защиту информации от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи;
- резервное копирование и архивирование информации, а также программного обеспечения с целью оперативного восстановления утраченных данных вследствие несанкционированного воздействия на них;
- постоянный контроль за обеспечением защищенности информации и программного обеспечения, своевременное обнаружение фактов несанкционированного доступа к информации и воздействия на нее.

Требования к системе защиты персональных данных.

При построении системы защиты персональных данных должны учитываться следующие принципы:

- выделение для работы системы сегмента корпоративной сети посредством VPN;
- межсетевое экранирование: фильтрацию принимаемых и передаваемых пакетов по различным критериям;
- защита внутренних сегментов сети от несанкционированного доступа от внешних и внутренних нарушителей;
- масштабируемость (возможность системы адаптироваться к расширению предъявляемых требований и возрастанию объемов решаемых задач);
- оповещение администратора (в реальном режиме времени) о событиях, требующих оперативного вмешательства;
- защита информации посредством электронной подписи от нарушения ее целостности при передаче ее по каналам связи.

Состав и содержание технических мер по обеспечению безопасности персональных данных.

Идентификация и аутентификация субъектов доступа и объектов доступа:

- идентификация и аутентификация пользователей, являющихся работниками оператора;
- управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов;
- управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации.
- защита обратной связи при вводе аутентификационной информации "система - субъект доступа" в процессе аутентификации должна обеспечиваться исключением отображения для пользователя действительного значения аутентификационной информации и (или) количества вводимых пользователем символов аутентификационной информации;

- идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей).

Регистрация событий безопасности:

- определение событий безопасности, подлежащих регистрации, и сроков их хранения;
- определение состава и содержания информации о событиях безопасности, подлежащих регистрации;
- сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения;
- защита информации о событиях безопасности (записях регистрации (аудита)) должна обеспечиваться применением мер защиты информации от неправомерного доступа, уничтожения или модифицирования, определенных в соответствии с настоящим методическим документом, и в том числе включает защиту средств ведения регистрации (аудита) и настроек механизмов регистрации событий).

Антивирусная защита:

- должна реализовываться применением сертифицированных антивирусных программных средств;
- базы данных признаков вредоносных компьютерных программ (вирусов) должны автоматически обновляться.

По итогам реинжиниринга разработана единая методика проведения аттестации информационной системы по требованиям защиты персональных данных.

Требование по проведению аттестации информационных систем в настоящий момент в действующем законодательстве явно нигде не прописано. Федеральная служба по техническому и экспертному контролю и Федеральная служба безопасности России уполномочены проводить мероприятия по контролю или надзору за выполнением требований по технической защите персональных данных.

Однако самостоятельно проведенный аудит не дает гарантии того, что у проверяющих органов не возникнет вопросов. Преимущество аттестации в том, что аттестат, выданный организацией-лицензиатом Федеральной службой по техническому и экспертному контролю и Федеральной службой безопасности России, дает гарантию соответствия требованиям по защите персональных данных.

Декларирование соответствия (аттестация) это документальное подтверждение соответствия свойств и характеристик информационной системы предъявляемым к ней требованиям, которые установлены законодательством РФ о персональных данных, а также нормативными и методическими документами Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, Федеральной службы по техническому и экспертному контролю и Федеральной службы безопасности России.

Целью аттестационных испытаний является проверка соответствия требованиям по защите персональных данных объекта информатизации.

В таблице 5 представлены возможные вариант этапов и подэтапов декларирования соответствия информационных систем требованиям информационной безопасности.

Таблица 5 Этапы аттестации системы

№	Этап	Подэтапы
1	Разработка программы и методики оценки	Описание объекта оценки
		Порядок проведения оценки
		Перечень процедур оценки
		Требования к содержанию проверок и испытаний
		Критерии оценки, характеризующей успешное прохождение проверок и испытаний
2	Оценка соответствия системы организационно-техническим требованиям по защите персональных данных	Анализ структуры системы и технологического процесса обработки информации
		Оценка достаточности разработанных внутренних нормативных актов и соответствия их содержания требованиям по безопасности информации

Окончание 5 таблицы

№	Этап	Подэтапы
		Оценка правильности выбора уровней защищенности персональных данных и мер защиты
		Оценка соответствия состава и структуры программно-технических средств системы представленной документации
		Оценка состояния организации работ и выполнения организационно-технических требований по защите информации
		Оценка достаточности мер физической охраны технических средств информационной системы
		Оценка уровня подготовки кадров и распределения ответственности персонала

Отчет по декларированию соответствия должен содержать:

- наименование и местонахождение оператора персональных данных;
- информацию, позволяющую идентифицировать информационную систему персональных данных;
- перечень нормативно-правовых актов, нормативных и методических документов, на соответствие требованиям которых производится декларирование;
- описание информационной системы, в том числе описание принятых оператором мер по обеспечению безопасности персональных данных в соответствии с необходимыми требованиями;
- сведения и копии документов, служащих основанием для подтверждения соответствия системы требованиям по безопасности информации;
- срок действия декларации соответствия. Срок действия декларации, как и аттестата, не должен превышать трёх лет.

В случае выявления несоответствия системы установленным требованиям по защите информации необходимо разработать предложения по устранению

выявленных недостатков и нарушений по возможности до окончания оценки. При этом могут применяться следующие меры:

- доработка организационно-распорядительной документации;
- исключение отдельных средств из состава системы;
- внесение дополнительных настроек в системе защиты персональных данных и изменение рабочей и эксплуатационной документации;
- применение дополнительных организационно-технических мер защиты;
- применение дополнительных сертифицированных средств защиты информации.

По результатам оценки оформляется заключение**.** К заключению прилагаются протоколы оценки, подтверждающие полученные при оценке результаты и обосновывающие приведенный в заключении вывод.

Протоколы испытаний подписываются экспертами – членами комиссии по оценке, проводившими испытания.

Таким образом, представлена информационная технология, с помощью которой произведен реинжиниринг бизнес-процесса процесса «Обеспечение работы с персональными данными проживающих в общежитиях СФУ», представлены модели процесса в трех разных нотациях, отражены основные характеристики обеспечения информационной безопасности разработанной системы и возможная методика декларирования (аттестации) соответствия системы требования по защите информации.

ЗАКЛЮЧЕНИЕ

В рамках написания магистерской диссертации рассмотрены некоторые аспекты обеспечения информационной безопасности персональных данных, которые обрабатываются с помощью корпоративных информационных систем.

В качестве взаимодействия между подразделениями Сибирского федерального университета рассмотрен обмен информацией о проживающих в общежитиях сибирского федерального университета в рамках работы управления общежитий. Также представлены некоторые проблемные места подобного взаимодействия.

На примере некоторых подразделений Сибирского федерального выделен бизнес-процесс, который подлежал реинжинирингу в ходе выполнения магистерской диссертации. Также представлена разработанная информационная технология, которая является основой оптимизации взаимодействия между подразделениями Сибирского федерального университета.

Для достижения постеленной цели были выполнены сформулированные ранее задачи, а результаты представлены в магистерской диссертации.

В рамках первой задачи представлены тенденции обеспечения информационной безопасности персональных данных в Российской Федерации согласно законодательству страны. Представлена схема системы регулирования отношений, связанных с обработкой персональных данных и обеспечением их безопасности в Российской Федерации.

В рамках второй задачи изучены возможные и возникающие проблемы аппаратного и программного обеспечения информационной безопасности. Представлены и разделены по видам актуальные угрозы информационной безопасности для корпоративных систем, также отражен перечень национальных интересов в данной области.

В рамках третьей задачи представлены результаты изучения деятельности отдела защиты информации департамента по режиму и безопасности жизнедеятельности, которые включают рассмотрение обязанностей и функций отдела.

Отдельно выделена функция обеспечения безопасности персональных данных, которые обрабатываются в рамках работы университета. Представлены модели бизнес-процесса «Обеспечение работы с персональными данными проживающих в общежитиях СФУ» в нотациях DFD, IDEF0 и EPC.

В рамках реализации четвертой задачи проанализированный бизнес-процесс «как есть». Представлены карта взаимодействий и межфункциональная схема изучаемого бизнес-процесса.

В рамках реализации пятой задачи разработан реинжиниринг процесса, представлены модели в нотациях DFD, IDEF0 и EPC. В рамках бизнес-процесса «как должно быть» разработана информационная система система учета проживающих в общежитиях, которая имеет свою систему защиты информации согласно нормативным стандартам, отражённым в российском законодательстве. Представлены интерфейсы системы учета проживающих в общежитиях, которые отражают функции изучаемого бизнес-процесса. Также проработаны этапы реализации информационной технологии и представлены временные сроки реализации этапов разработки.

Представленный реинжиниринг бизнес-процесса «Обеспечение работы с персональными данными проживающих в общежитиях СФУ» является основой для разработки методики декларирования (аттестации) соответствия информационной системы требованиям по защите информации.

Таким образом, данная бакалаврская работа отражает тенденции обеспечения информационной безопасности персональных данных, которые заложены в законодательных актах Российской Федерации.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Колин, К. К. Информационная цивилизация, какой она будет? /К. К. Колин // Библиотековедение. 2001. №5. С. 40 45.
2. Колин, К.К. Информационная цивилизация / К. К. Колин. М.:ИПИ РФН, 2002. 112 с.
3. Черников, Б. В. Информационные технологии управления: учебник / Б. В. Черников. М.: ИД «ФОРУМ»: ИНФРА-М, 2014. 368 с.
4. Лопатин, Ю. Н. Информационная безопасность в России. Проблемы, поиски решений / Ю. Н. Лопатин / Гуманитарные исследования в восточной Сибири и на Дальнем Востоке // Дальневосточный федеральный университет. Владивосток, 2008. № 2. С. 51-57
5. Важорова, М. А. Соотношение понятий «Информация о частной жизни» и «Персональные данные» / М. А. Важорова / Вестник Саратовской юридической академии // Саратовская государственная юридическая академия. Саратов, 2012. № 2. с. 55-59
6. Горошко, И. В. Персональные данные: возможные пути реализации федерального закона / И. В. Горошко, В. Н. Лебедев / Труды академии управления МВД России // Академия управления Министерства внутренних дел Российской Федерации. Москва, 2011. № 3. С. 60-66
7. Гагарина, Л. Г. Информационные технологии : учебное пособие / Л.Г. Гагарина, Я.О. Теплова, Е.Л. Румянцева М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2015. 320 с.
8. Юдина, Н. Ю. Информационные технологии: учебное пособие / Н.Ю. Юдина – Воронеж : ВГЛТУ им. Г.Ф. Морозова, 2013. 235 с.
9. Черников, Б. В. Информационные технологии управления : учебник / Б.В. Черников. М.: ИД ФОРУМ: НИЦ Инфра-М, 2013. 368 с.
10. Семченков, А. С. Информационная безопасность и политическая стабильность России / А. С. Семченков / Вестник российской нации // Обще-

российский союз общественных объединений содействия укреплению государственного единства «Российская нация». Москва, 2017. С. 134-146

11. Касперский, Евгений Валентинович. Компьютерное зловредство / Е. В. Касперский . Санкт-Петербург : Питер, 2009. 208 с

12. Денисов, Д. В. Безопасность в Интернете: защита от внешних угроз / Д. В. Денисов / Прикладная информатика // Московский финансово-промышленный университет «Синергия». Москва, 2016. Т. 11, № 2. С. 57-64

13. Медведев, В. В. Возможность выборки требований к системе защиты от вредоносных программ / В. В. Медведев / Прикладная информатика // Московский финансово-промышленный университет «Синергия». Москва, 2015. Т.10, № 3. С. 76-87

14. Электронный каталог СофтКаталог.info [Электронный ресурс]: информационный ресурс. Режим доступа: http://softcatalog.info/ ru/obzor/reyting-antivirusov

15. Официальный сайт компании ESET [Электронный ресурс]: информационный ресурс. Режим доступа: https://www.esetnod32.ru/

16. Орлов, С. Межсетевые экраны: расширение функционала / С. Орлов / Журнал сетевых решений LAN // Издательство «Открытые системы». Москва, 2013. № 6. С. 44-49

17. Башкирцев, А. С. Межсетевые экраны как элемент архитектуры информационной безопасности систем управления современными телекоммуникационными сетями и центрами обработки данных / А. С. Башкирцев, Н. В. Михайличенко, И. Б. Паращук // Региональная информатика и информационная безопасность // Издательство: Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления. Санкт-Петербург, 2017. С. 37-39

18. Альтерман, А. Д. Межсетевые экраны / А. Д. Альтерман, А. С. Парфенова // Современные научные исследования и разработки // Научный центр «Олимп». Астрахань, 2018. № 12(29). С. 112-114

19. Крутохвостов, Д. С. Парольная и непрерывная аутентификация по клавиатурному почерку средствами математической статистики / Д. С. Крутохвостов, В. Е. Хиценко / Вопросы кибербезопасности // Закрытое акционерное общество «Научно-производственное объединение «Эшелон»». Москва, 2017. № 5. С. 91-99

20. Актаева, А. У. Искусственные интеллектуальные системы для обнаружения вторжений: перспективы развития инновационных технологий / Современные информационные технологии и ИТ-образование / А. У. Актаева, Р. Ниоязова, Н. Гагарина, Н. Бижигитова, У. Кусаноинова, А. Даутов, Г. Шатенова / Современные информационные технологии и ИТ-образование // Фонд содействия развитию интернет-медиа, ИТ-образования, человеческого потенциала «Лига интернет-медиа». Москва, 2017. Т. 13, № 3. С. 44-52

21. Шуваев, П. В. Автоматизированные системы обнаружения / П. В. Шуваев, М. Д. Кузнецов, А. Г. Анисимов, Т. С. Емашкина, В. А. Трусова / Труды международного симпозиума надежность и качество // Пензенский государственный университет. Пенза, 2017. № 2. С. 59-62

22. Лапонина, О. Р. Использование сканера уязвимостей ZAP для тестирования веб-приложений / О. Р. Лапонина, С. А. Малаховский / International journal of open information technologies / Лаборатория Открытых Информационных Технологий факультета ВМК МГУ им. М.В. Ломоносова. Москва, 2017. Т. 5 № 8 С. 18-26

23. Описание программного продукта «XSpider» [Электронный ресурс]: Официальный сайт программного продукта «XSpider».Режим доступа: https://www.ptsecurity.com/ru-ru/products/xspider/

24. Мишин, А.В. Информационные технологии в профессиональной деятельности : учебное пособие / А.В. Мишин, Л.Е. Мистров, Д.В. Картавцев. М.: РАП, 2011. 311 с.

25. Гвоздева, В. А. Информатика, автоматизированные информационные технологии и системы : учебник / В.А. Гвоздева. М.: ИД ФОРУМ: ИНФРА-М, 2011. 544 с

26. Об утверждении Доктрины информационной безопасности Российской Федерации [Электронный ресурс] : указ Президента Российской Федерации от 05.12.2016 № 646 // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/ document/cons_doc_LAW_208191/

27. Официальный сайт национального открытого университета «Интуит» [Электронный ресурс] : Триада безопасной ИТ-инфраструктуры – Конфиденциальность, Целостность, Доступность. Режим доступа: https://www.intuit.ru/studies/courses/14250/1286/lecture/24236

28. Сиротский, А. А. Информационная безопасность личности и защиты персональных данных в современной коммуникативной среде /А. А. Сиротский / Технологии техносферной безопасности / Академия Государственной противопожарной службы Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий. Москва, 2013. № 4(50) С. 3-10

29. Об информации, информационных технологиях и о защите информации [Электронный ресурс] : федер. закон от 14.07.2006. № 149-ФЗ // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/

30. Хестанова, Л. А. Информационная безопасность. Технологии защиты персональных данных / Л. А. Хестанова, М. А. Марков / Сборник научных докладов международной научно-практической конференции «Актуальные проблемы науковедения, культуры, образования, экономики, информатики и социальные трансформации – 2017» / Полиграф сервис. Москва, 2017. С. 287-292

31. Хасанов, Ш. А. Безопасность информационных систем персональных данных / Ш. А. Хасанов, Т. Х. Агишев / Мир компьютерных технологий / Федеральное государственное автономное образовательное учреждение высшего образования «Севастопольский государственный университет». Севастополь, 2018. С. 144-147

32. Дорожкин, А. В. Информационная безопасность как инструмент обеспечения экономической безопасности хозяйствующего субъекта / А. В. Дорожкин, В. Н. Ясенев / Экономика и предпринимательство // Редакция журнала «Экономика и предпринимательство». Москва, 2015. № 5-1. С. 812-816

33. Арабенко, В. А. Основные направления предупреждения преступлений, связанных с разглашением государственной тайны и утратой документов, содержащих государственную тайну / В. А. Арабенко // Общество и право / Федеральное государственное казенное образовательное учреждение высшего профессионального образования «Краснодарский университет Министерства внутренних дел Российской Федерации» Краснодар, 2009. №5 С. 201 203

34. Назаров, И. Г. Особенности организации обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных / И. Г. Назаров, Ю. К. Язов, С. Е. Остроухова / Информация и безопасность // Воронежский государственный технический университет. Воронеж, 2009. Т. 12, № 1. С. 71-76

35. Аналитический центр InfoWatch. Глобальное исследования утечек конфиденциальной информации в I полугодии 2017 года [Электронный ресурс]. Электрон. дан. – Режим доступа: https://www.infowatch.ru/report2017_half

36. Башкатова, Л. И. Пропажа, утрата, уничтожение, восстановление документов / Л. И. Башкатова // Бухгалтерский учет / Редакция журнала «Бухгалтерский учет» Москва, 2010. №3 С. 98 102

37. Муханова, А. Классификация угроз и уязвимостей информационной безопасности в корпоративных системах / А. Муханова, А. В. Ревнивых, А. М. Федотов // Вестник новосибирского государственного университета. Серия:

информационные технологии / Новосибирский национальный исследовательский государственный университет Новосибирск, 2013. №11 С. 55 72

38. Сабангурова, Л. Б. Анализ ошибок в системе документооборота / Л. Б. Сабангулова, Н. В. Гнусин // Молодежный вестник уфимского государственного авиационного технического университета / ГОУ ВПО «Уфимский государственный авиационный технический университет» Уфа, 2015. №1 (13) С. 23 26

39. Данилов, Ю. М. Защита и обработка конфиденциальных документов [Электронный ресурс] / Ю. М. Данилов // Журнал «Делопроизводство». 2008. №1. Режим доступа: http://www.top-personal.ru/officeworkissue.html?23

40. Таранин, С. М. Резервное копирование с хранением в базе данных / С. М. Татарин // Моделирование и анализ информационных систем / Ярославский государственный университет им. П.Г. Демидова Ярославль, 2016. №23 С. 479 491

41. Гордеева, Д. С. Резервное копирование как актуальный метод реализации политики информационной безопасности / Д. С. Гордеева, А. С. Мезенов // Управление инновациями в сфере науки, техники и технологий / НОО «Профессиональная наука» Екатеренбург, 2016. С. 59 65

42. Чистяков, И.А. Фрактальный подход к резервному копированию динамических данных / И.А. Чистяков // Глобальный научный потенциал. Тамбов. 2012. № 16. С. 47 50

43. Фйкашева, Ю. А. Резервное копирование и восстановление данных на предприятиях/ Ю.А. Айкашева // Актуальные проблемы авиации и космонавтики Красноярск, 2016. Т. 2. № 12. С. 7 8.

44. Гордеева, Д. С. Резервное копирование как актуальный метод реализации политики информационной безопасности / Д.С. Гордеева, А.С. Мезенов // Управление инновациями в сфере науки, техники и технологий сборник научных трудов по материалам I Международной научно-практической конференции. НОО «Профессиональная наука». Екатеринбург, 2016. С. 59-65.

45. Осипов, М. Ю. Виртуализация как технология повышения эффективности использования технических средств ИТ-инфраструктуры / М. Ю. Осипов, И. Л. Бондарь, Р. А. Семенов, Т. Ю. Серова // Вопросы атомной науки и техники. Серия: математическое моделирование физических процессов / Российский Федеральный ядерный центр Всероссийский научно-исследовательский институт экспериментальной физики Саров, 2011. №2. С. 78 84

46. Туранцев, Д. С. Организация пропускного режима первый шаг к обеспечению безопасности и конфиденциальности информации // Научно-технический вестник информационных технологий, механики и оптики/ Санкт-Петербургский национальный издательский университет информационных технологий, механики и оптики Санкт-Петербург, 2007. С. 244 252

47. ГОСТ Р 50922-96 Защита информации. Основные термины и определения. Взамен ГОСТ Р 50922 96 ; введ. 27.12.2006. Москва :Стандартинформ, 2006. 12 с

48. Лемещенко, Г. Л. Об исправлении ошибок в бухгалтерском учете и отчетности организации / Г. Л. Лемещенко, О. С. Темченко // Международный бухгалтерский учет / ООО «Издательский дом ФИНАНСЫ и КРЕДИТ» Москва, 2012. №14 С. 16 22

49. Шиленко, С. И. Классификация искажений и ошибок в бухгалтерской финансовой отчетности / С. И. Шиленко, А. А. Гордеева / Вестник белгородского университета кооперации, экономики и права // Белгородский университет кооперации, экономики и права Белгород, 2010. №1 С. 122 129

50. Гамбарян, Р. Г. Исправление ошибок в бухгалтерском учёте и бухгалтерской отчётности / Р. Г. Гамбарян, Ю. С. Зиновьев / Актуальные проблемы современной экономики // РИО АГПУ Армавир, 2015. С. 88 94

51. Кривенец, А. Н. Ошибки при составлении бюджетной отчетности / А. Н. Кривенец / Бухгалтерский учет // Редакция журнала «Бухгалтерский учет» Москва, 2010. №5 С. 88 91

52. Петухов, К. В. Организационные меры по защите информации при использовании средств криптографической защиты информации / Современные проблемы и пути их решения в науке, производстве и образовании // Кубанский казачий государственный институт пищевой индустрии и бизнеса (филиал) федерального государственного бюджетного образовательного учреждения высшего образования «Московский государственный университет технологий и управления им. К.Г. Разумовского (Первый казачий университет)» Темрюк №1 (1), 2016. С. 90 93

53. Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных: Приказ ФСТЭК от 18.02.2013г. №21 // Российская газета, 2013. - №107

54. Официальный сайт Сибирского Федерального университета [Электронный ресурс] : информационный ресурс. Режим доступа: http://about.sfu-kras.ru/general

55. Зайцев, М. Г. Методы оптимизации управления и принятия решений: примеры, задачи, кейсы: учебное пособие / М. Г. Зайцев, С. Е. Варюхин // Издательство «Дело» АНХ. – С. 664

56. Данилин, А. И., Основы теории оптимизации (постановки задач) [Электронный ресурс] : электрон. учеб. пособие / А. И. Данилин ; Минобрнауки России, Самар. гос. аэрокосм. ун-т им. С. П. Королева (нац. исслед. ун-т). - Электрон. текстовые и граф. дан. 57 с

57. Елиферов, В. Г. Бизнес-процессы: регламентация и управление: учебное пособие / В. Г. Елиферов,. В. В. Репин. Москва : НИЦ ИНФРА-М, 2015. - 319 с.

58. Абдикеев, Н. М. Управление знаниями и реинжиниринг бизнеса: учебник / Н. М. Абдикеев, А. Д. Киселев. М. : ИНФРА-М, 2013. 382 с.

59. Репин, В. В. Бизнес-процессы. Моделирование, внедрение, управление: учебное пособие для вузов / В. В Репин. – Москва: Экономистъ, 2013. – 238 с.

60. Бойхман, Е.Г. Реинжиниринг бизнеса/ Е.Г. Бойхман М. Финансы и статистика, 2010. 152 с.

61. . Гаврилюк, А. Л. Блок-схемы, комбинаторно симметричные графы и их автоморфизмы: / А. Л. Гаврилюк. Екатеринбург : Б. и., 2008. 21 с.

62. Богомолова, И. С. Инновационный и проектный менеджмент / И.С. Богомолова, С.В. Гриненко, Е.С. Едалова // Учебное пособие. – Ростов-на-Дону: Изд-во ЮФУ. – 2014. – 181 с.

63. Официальный сайт Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций [Электронный ресурс]: информационный ресурс. Режим доступа: https://rkn.gov.ru/personal-data/register/

64. Репин, В.В. Процессный подход к управлению. Моделирование бизнес-процессов / В.В. Репин. - М.: Манн, Иванов и Фербер, 2013. 512 с.

65. Казакова, Н. А Управленческий анализ в различных отраслях: Учеб. пособие / Н. А. Казакова. М. : ИНФРА-М, 2015. 288 с.

66. Понятие информационной системы (ИС): основные термины и определения. Этапы развития ИС. Соотношение между ИС и ИТ [Электронный ресурс]: статья. – Режим доступа: http://cde.osu.ru/demoversion/course157/text/1.5.html

67. Варфоломеева, А.О. Информационные системы предприятия : учебное пособие / А. О. Варфоломеева, А. В. Коряковский, В. П. Романов. – Москва : Академия, 2013 283 с

68. Заботина, Н. Н. Проектирование информационных систем: Учебник / Н. Н. Заботина М.: Москва ИНФРА-М, 2014. 331 с.

69. Гвоздева, В. А. Проектирование информационных систем: учебное пособие / В. А. Гвоздева М.: ИД «ФОРУМ»: ИНФРА-М, 2015. 544 с.

70. Емельянова, Н. З. Проектирование информационных систем: Учебник / Н. З. Емельянова, Т. Л. Пыртыка, И. И. Попов М.: ФОРУМ: ИНФРА-М, 2014. 432 с.

71. Гагарина, Л. Г. Разработка и эксплуатация информационных систем: учебное пособие / Л. Г. Гагарина ИД «ФОРУМ»: ИНФРА-М, 2013. 425 с.

72. Пинаев Д., Веретенников Д. Моделирование бизнес-процессов: доступно о сложном / Д. Пинаев, 2013. 496 с.

73. Федоров, О. Г. Информационные технологии в науке и образовании / О. Г. Федоров «Редакционно-издательский центр» Министерство обороны РФ, 2009. 630 с.

74. Андерсен, Б. Бизнес-процессы. Инструменты совершенствования / Б. Андерсен. М. : РИА «Стандарты и качество», 2003. 272 с.

75. Светлов, Н. М. Информационные технологии управления проектами: учебное пособие / Н. М. Светлов, Г. Н. Светлова. М.: ИД «ФОРУМ»: ИНФРА-М, 2015. 232 с.

76. Федотова, Е. Л. Информационные технологии в профессиональной деятельности : учебное пособие для среднего профессионального образования / Е. Л. Федотова М.: ИД «ФОРУМ»: ИНФРА-М, 2015. 368 с.

77. Шевцова, О. Н. Комплексный экономический анализ как инструментарий механизма управления экономической эффективностью организации / О.Н. Шевцова // Наукоемкие технологии и инновации / Белгородский государственный технологический университет им. В.Г. Шухова. Белгород, 2014. С. 375 379.

78. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных: Постановление Правительства РФ от 01.11.2012г. №1119 // Собрание Законодательства РФ, 2012. - №45

79. Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах: Приказ ФСТЭК от 11.02.2013г. №17 // Российская газета, 2013. – №136

80. СТО 4.2–0.7–2014 Система менеджмента качества. Общие требования к построению, изложению и оформлению документов учебной деятельности. Введ. впервые; дата введ. 30.12.2013. Красноярск: ИПК СФУ, 2014. –60 с.

Федеральное государственное автономное
образовательное учреждение
высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Институт управления бизнес-процессами и экономики
Кафедра экономики и информационных технологий менеджмента

УТВЕРЖДАЮ
Заведующий кафедрой
_____ А.А.Ступин
подпись инициалы, фамилия
«10» июня 20 19 г.

МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ

Моделирование бизнес-процессов информационной безопасности персональных данных корпоративных систем

09.04.03 Прикладная информатика

09.04.03.02 Реинжиниринг бизнес-процессов

Научный руководитель _____ доцент, канд. техн. наук М. В. Карасева
подпись, дата

Выпускник _____ Я. О. Шишкина
подпись, дата

Рецензент _____ доцент, канд. техн. наук В. А. Федоров
подпись, дата

Красноярск 2019