МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Тольяттинский государственный университет»

Институт математики, физики и информационных технологий
(наименование института полностью)

Кафедра «Прикладная математика и информатика»
(наименование)

09.03.03 «Прикладная информатика»
(код и наименование направления подготовки, специальности)

Бизнес-информатика
(направленность (профиль)/ специализация)

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА (БАКАЛАВРСКАЯ РАБОТА)

на тему «Разработка системы обеспечения информационной безопасности»

Обучающийся Р.О. Брусенцов
(Инициалы Фамилия) (личная подпись)

Руководитель Н.Н. Казаченок
(ученая степень (при наличии), ученое звание (при наличии), Инициалы Фамилия)

Консультант (ы) к.ф.н., доцент Н.В. Андрюхина
(ученая степень (при наличии), ученое звание (при наличии), Инициалы Фамилия)

Тольятти 2022

Аннотация

Бакалаврская работа выполнена на тему «Разработка системы обеспечения информационной безопасности». Работа размещена на 83 страницах, содержит 7 таблиц и 31 рисунок.

Цель работы заключается в разработке системы обеспечения информационной безопасности Управления государственной экспертизы Ленинградской области и рекомендаций по их применению.

Во введении представлены: актуальность темы, объект и предмет исследования, методы исследования, цель работы, а также задачи, решение которых необходимо для достижения поставленной цели.

В первой главе рассмотрены теоретические аспекты информационной безопасности организации, исследованы информационные угрозы и их виды.

Во второй главе представлен анализ мероприятий по обеспечению информационной безопасности предприятия, рассмотрены три типа мер по информационной безопасности – организационные, технические и правовые.

В третьей главе представлены организационные, аппаратно-программные и криптографические средства обеспечения информационной безопасности предприятия. Разработан комплекс мер по обеспечению информационной безопасности для Управления негосударственной экспертизы.

В заключении приводятся оценки результатов исследования, выводы и рекомендации по практическому использованию материалов работы.

Abstract

The bachelor's work was carried out on the topic "Development of an information security system". The work is placed on 83 sheets and contains 7 tables and 31 figures.

The purpose of the work is to develop an information security management system for the State Expertise of the Leningrad Region and recommendations for their application.

The introduction presents: the relevance of the topic, the object and subject of the study, research methods, the purpose of the work, as well as the tasks that need to be solved to achieve the goal.

In the first chapter, the theoretical aspects of information security of the organization are considered, information threats and their types are investigated.

The second chapter presents an analysis of measures to ensure the information security of the enterprise, three types of information security measures are considered – organizational, technical and legal.

The third chapter presents organizational, hardware-software and cryptographic means of ensuring information security of the enterprise. A set of measures has been developed to ensure information security for the Management of non-governmental expertise.

In conclusion, the evaluation of the results of the study, conclusions and recommendations on the practical use of the materials of the work are given.

Оглавление

Введение

Информация является важнейшим ресурсом развития и всегда играла в истории человечества значительную роль. Накопление знаний способствовало росту благосостояния народов и развитию владеющей этим знанием культуры. Так обстояли дела у древних народов, так обстоят дела и сегодня. Изменились технологии информационных процессов, но не значимость информации. Наряду с ростом роли информации в обществе постепенно возникла и потребность в ее защите.

Появление и развитие новых информационных технологий, создание мощных систем и сетей хранения и обработки данных увеличили требования к уровню защиты информации и обусловили необходимость формирования эффективных механизмов защиты информации, приспособленной к современной архитектуре хранения данных. В процессе развития технологий, экономики, бизнеса и предпринимательства защита важной информации становится обязательной: создаются всевозможные рекомендации по защите информации; разрабатываются документы по защите информации; принимаются законы и иные нормативно-правовые акты, характеризующие проблемы обеспечения информационной безопасности и задачи по организации ее защиты.

«Обеспечение информационной защиты в организации является системным непрерывным процессом. Он предполагает использование современных методов защиты, позволяющих контролировать внешнюю и внутреннюю среды компании, организацию и реализацию мероприятий по поддержке устойчивого функционирования локальной сети и вычислительной техники, а также минимизацию потерь, связанных с утечкой информации. Для реализации защиты информации в организации формируют определенный свод правил и нормативных документов, регламентирующих действия сотрудников по обеспечению безопасности и описывающий технические и

программные средства для защиты информации. Такой свод документов называется политикой информационной безопасности» [18].

Политика информационной безопасности направлена на минимизацию рисков утечки информации на предприятии, а также для устойчивого функционирования информационной структуры предприятия. Вопросам информационной безопасности необходимо уделять самое пристальное внимание, так как ее нарушение может привести к финансовым и репутационным потерям, иногда невосполнимым. Комплексная система защиты информации предполагает внедрение организационных, программных и инженерно-технических мер, которые обеспечат неприкосновенность конфиденциальной информации и минимизирует риски реализации угроз информационным активам.

Наличие потенциальных угроз информации, периодическая их реализация и размеры понесенных отдельными компаниями потерь обусловили важнейшую роль системы защиты информации для любой организации. Меры по защите информации принимают в целях изоляции эффективно функционирующей информационной системы от «несанкционированных управляющих воздействий и доступа посторонних лиц или программ к данным с целью хищения или нанесения ущерба их целостности» [5].

Объектом исследования являются методы и средства защиты данных управления государственной экспертизы Ленинградской области.

Предметом исследования является система обеспечения информационной безопасности в управлении государственной экспертизы Ленинградской области.

Цель выпускной квалификационной работы – разработка системы обеспечения информационной безопасности для управления государственной экспертизы Ленинградской области.

Для достижения поставленной цели необходимо решить следующие задачи:

– провести исследование текущего состояния системы информационной безопасности управления государственной экспертизы Ленинградской области;
– определить уязвимости в системе информационной безопасности организации при их наличии, а также обозначить информационные угрозы с наибольшей вероятностью их наступления;
– исследовать проблемы защиты информации, изучить принципы и методы ее защиты;
– сформировать комплекс предложений по реализации административных, программно-аппаратных и инженерно-технических мер по предотвращению угроз информационной безопасности, тем самым разработать систему безопасности;
– оценить эффективность разработанной для управления государственной экспертизы Ленинградской области комплексной системы защиты информации.

Практическая значимость работы состоит в том, что предложенная модель комплексной системы защиты информации может быть использована в практике информационной защиты действующих предприятий.

Выпускная квалификационная бакалаврская работа состоит из следующих структурных элементов: введения, трех глав, заключения, списка использованной литературы.

В первой главе введены основные понятия информационной безопасности, рассмотрены и классифицированы информационные угрозы.

Во второй первой главе выполнен анализ имеющейся в управлении государственной экспертизы Ленинградской области системы защиты данных и выявлены основные проблемы в этой сфере.

Во третьей главе выполнено проектирование комплексной системы защиты информации предприятия.

В заключении подведены итоги работы, сделаны выводы по ее результатам.

Глава 1 Анализ системы защиты данных на предприятии

1.1 Технико–экономическая характеристика Управления государственной экспертизы Ленинградской области

В апреле 1988 года экспертно-технический отдел Архитектурно-планировочного управления Ленинградского облисполкома был преобразован в Управление государственной вневедомственной экспертизы при Главном управлении архитектуры и градостроительства облисполкома и принято Положение о Леноблсэкспертизе.

Задачи, которые были поставлены перед учреждением:

- проведение экспертизы технико-экономических расчетов, технико-экономических обоснований, проектов, рабочих проектов и смет на строительство всех объектов производственного и непроизводственного назначения, строящихся на территории Ленинградской области;
- выдача заключений по планировочной проектной документации для застройки Ленинградской области;
- проведение выездных экспертиз технического состояния жилых, общественных и других зданий и сооружений, а также оценки их общей стоимости;
- обобщение результатов экспертиз, анализ уровня проектирования, внесение предложений по совершенствованию проектно-сметного дела, его нормативной базы и экспертизы;
- внесение предложений в облисполком и финансирующие учреждения банков о применении мер финансово-кредитного воздействия к заказчикам и проектным организациям, а также о наказании должностных лиц, виновных в низком качестве разработанной проектной документации;

– проведение заседаний архитектурно-технической комиссии и градостроительного совета по рассмотрению сложных архитектурно-объемных решений и планировочных работ [18].

В ходе реорганизаций и переподчинений организация неоднократно меняла наименование и управляющие структуры. Последнее к настоящему моменту изменение произошло в декабре 2007 года (соответствующие изменения в ЕГРЮЛ внесены в апреле 2008 года). С этого момента создано Государственное автономное учреждение «Управление государственной экспертизы Ленинградской области» (далее – Управление), каковым оно я является сегодня.

Управление находится в подчинении Комитета государственного строительного надзора и государственной экспертизы Ленинградской области.

Учредителем организации является Российская Федерация.

Регистрационные данные современного состояния Управление государственной экспертизы Ленинградской области представлены на рисунке 1.

№ п/п	Наименование показателя	Значение показателя
1	2	3
Наименование		
1	Полное наименование на русском языке	ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ УЧРЕЖДЕНИЕ "УПРАВЛЕНИЕ ГОСУДАРСТВЕННОЙ ЭКСПЕРТИЗЫ ЛЕНИНГРАДСКОЙ ОБЛАСТИ"
2	ГРН и дата внесения в ЕГРЮЛ записи, содержащей указанные сведения	2124703157885 27.12.2012
3	Сокращенное наименование на русском языке	ГАУ "ЛЕНОБЛГОСЭКСПЕРТИЗА"
4	ГРН и дата внесения в ЕГРЮЛ записи, содержащей указанные сведения	2124703157885 27.12.2012
Место нахождения и адрес юридического лица		
5	Место нахождения юридического лица	ЛЕНИНГРАДСКАЯ ОБЛАСТЬ, Р-Н ВСЕВОЛОЖСКИЙ, Г. ВСЕВОЛОЖСК
6	ГРН и дата внесения в ЕГРЮЛ записи, содержащей указанные сведения	2194704363643 10.10.2019
7	Адрес юридического лица	188640, ЛЕНИНГРАДСКАЯ ОБЛАСТЬ, Р-Н ВСЕВОЛОЖСКИЙ, Г. ВСЕВОЛОЖСК, ПР-КТ ВСЕВОЛОЖСКИЙ, Д. 17, КОМ. 436

Рисунок 1 – Фрагмент выписки из ЕГРЮЛ

Организационная структура ГАУ «Управление государственной экспертизы Ленинградской области» представлена на рисунке 2.

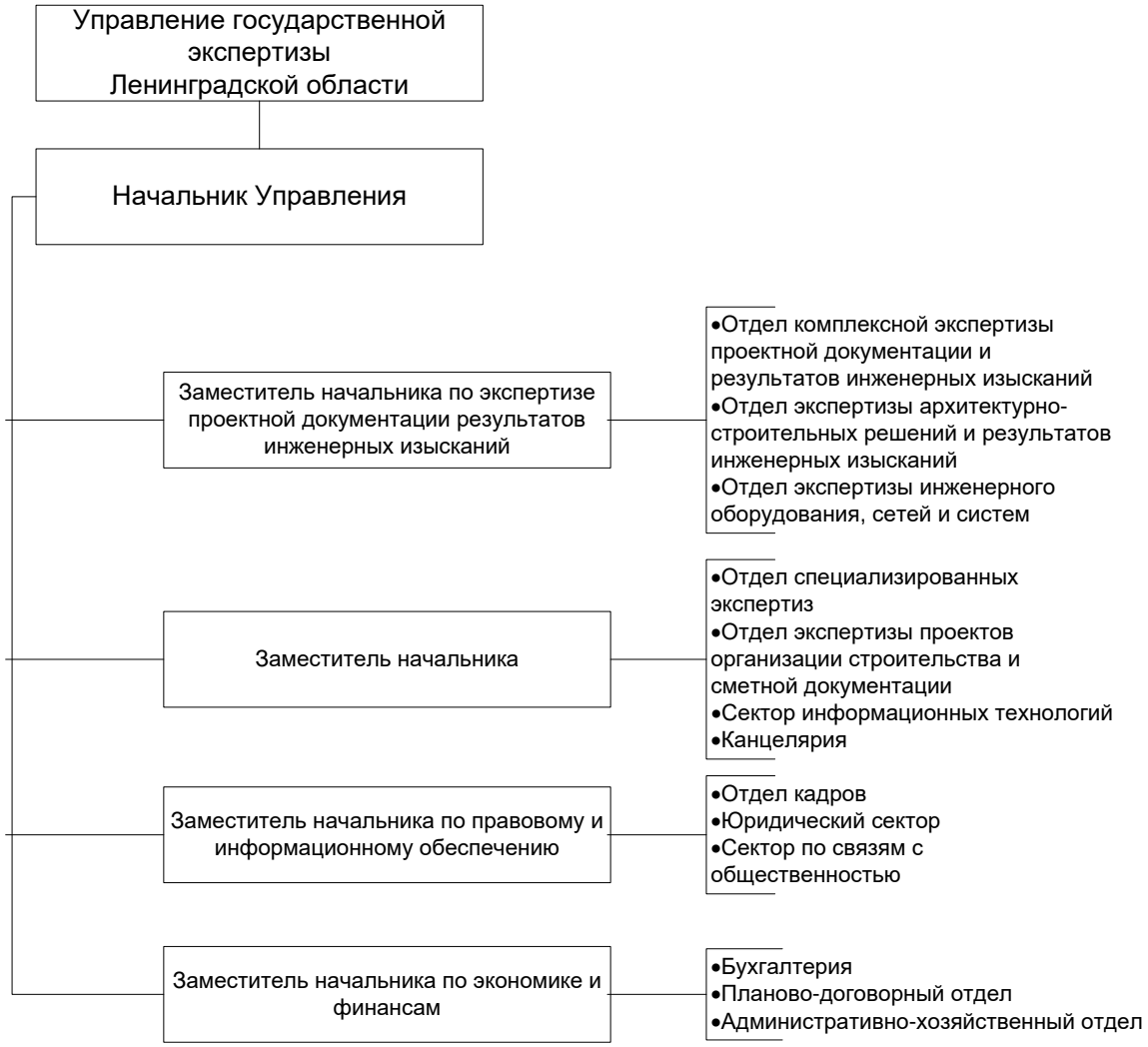

Рисунок 2 – Организационная структура Управления

Основным видом деятельности организации по ОКВЭД является:

71.20.61 – Экспертиза проектной документации, запасов полезных ископаемых и подземных вод, геологической информации о предоставляемых в пользование участках недр, результатов инженерных изысканий государственная [19].

Дополнительные виды деятельности:

63.11.1 – Деятельность по созданию и использованию баз данных и информационных ресурсов [19];

71.11 – Деятельность в области архитектуры [19].

71.12 – Деятельность в области инженерных изысканий, инженерно-технического проектирования, управления проектами строительства, выполнения строительного контроля и авторского надзора, предоставление технических консультаций в этих областях [19];

71.20.62 – Экспертиза проектной документации и результатов инженерных изысканий негосударственная [19].

Функциональная схема сектора информационных технологий представлена в нотации UML (диаграмма вариантов использования) на рисунке 3.

Рисунок 3 – Функциональная модель сектора информационных технологий

Модель демонстрирует обобщенные задачи, стоящие перед специалистами секции информационных технологий Управления. Полный перечень решаемых ими задач намного шире.

Деятельность государственного автономного учреждения «Управление государственной экспертизы Ленинградской области» осуществляется на основании Устава. Устав организации согласован Ленинградским областным комитетом по управлению государственным имуществом и утвержден распоряжением комитета государственного строительного надзора и государственной экспертизы Ленинградской области от 11 декабря 2012 года № 319. В настоящее время действует редакция с дополнениями и изменениями, внесенными в феврале 2022 года.

Государственная услуга по проведению государственной экспертизы проектной документации и (или) результатов инженерных изысканий предоставляется ГАУ «Леноблгосэкспертиза» в соответствии в Административным регламентом, утвержденным приказом комитета государственного строительного надзора и государственной экспертизы Ленинградской области от 29 ноября 2016 года № 7.

1.2 Основные проблемы и задачи защиты информации на предприятии

В Управлении государственной экспертизы Ленинградской области есть сектор информационных технологий, но в нем работают всего 3 человека, которые осуществляют поддержку имеющейся инфраструктуры, настройку программного обеспечения и оказывают коллегам помощь при возникновении проблем в использовании компьютерной техники. При необходимости выполнить какой-либо значительный объем работы, связанный с установкой компьютерной техники или программного обеспечения, привлекаются внешние специалисты. Текущим обслуживанием компьютеров занимаются IT-специалисты, которые есть в составе каждого подразделения компании.

Кроме того, в секторе информационных технологий числится сетевой администратор, в обязанности которого входит обслуживание локальной сети предприятия.

Решение задач по защите информации поручено специалистам отдела информационных технологий и руководителям подразделений.

Управление осуществляет экспертизу архитектурных и строительных проектов на основе заявлений, подаваемых организациями. Образец заявления представлен в регламенте оказания услуг. Блок–схема полного цикла предоставления услуги представлена на рисунке 4.

Рисунок 4 – Блок–схема полного цикла предоставления услуги

Услуги по проведению экспертизы являются платными. Ориентировочную стоимость услуг потребитель может рассчитать самостоятельно, воспользовавшись интерактивным калькулятором, размещенным на странице официального сайта Управления (URL: http://www.loexp.ru/), перейдя по ссылке Расчет стоимости с любой его страницы. Фрагмент использования калькулятора представлен на рисунке 5.

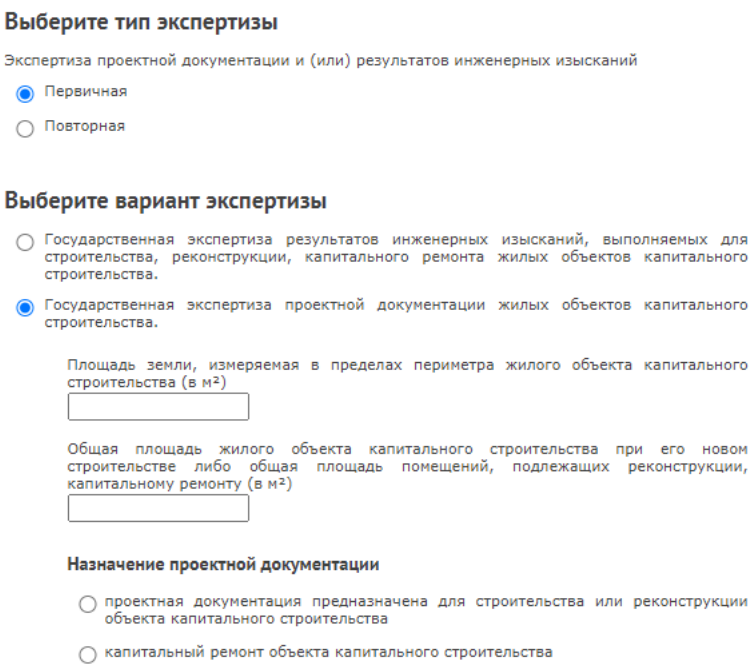

Рисунок 5 – Фрагмент калькулятора для расчета стоимости экспертизы

Деятельность специалистов Управления в первую очередь связана с проведением различного вида экспертиз. Это требует оформления большого количества документации, в том числе и конфиденциальной, оформленной в соответствии со всеми действующими стандартами и не допускающей ошибок, так как цена ошибок при реализации строительных проектов слишком высока.

Общая схема делопроизводства в Управлении представлена на рисунке 6.

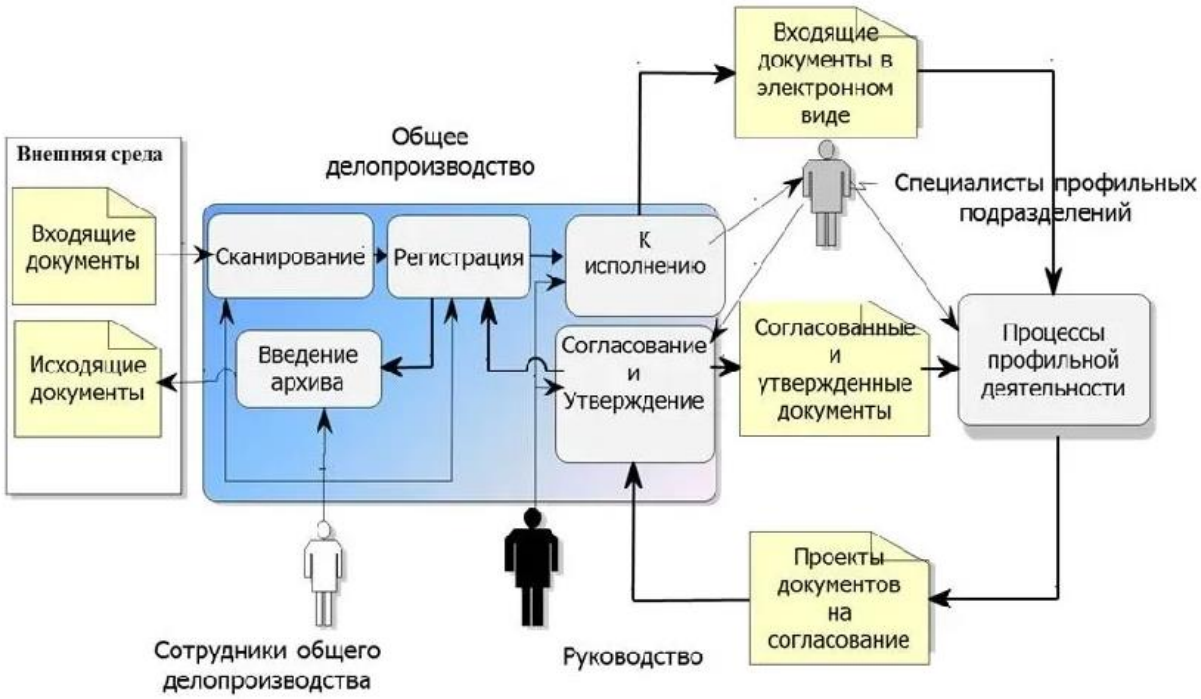

Рисунок 6 – Общая схема делопроизводства

Управление является участником межведомственного обмена электронными документами. «Система межведомственного электронного документооборота представляет собой федеральную информационную систему, предназначенную для организации взаимодействия систем электронного документооборота между его участниками (органами государственной власти РФ, федеральными органами исполнительной власти, органами исполнительной власти субъектов РФ и иными государственными органами и организациями)» [15].

Ярким примером межведомственного документооборота является известный сайт Госуслуги, который предлагает пользователям много удобных удаленных сервисов. Например, можно записаться на прием к врачу, не выходя из дома; можно удаленно подать заявление на оформление внутреннего или заграничного паспорта; можно оформить пособие.

Схематически система межведомственного электронного документооборота представлена на рисунке 7.

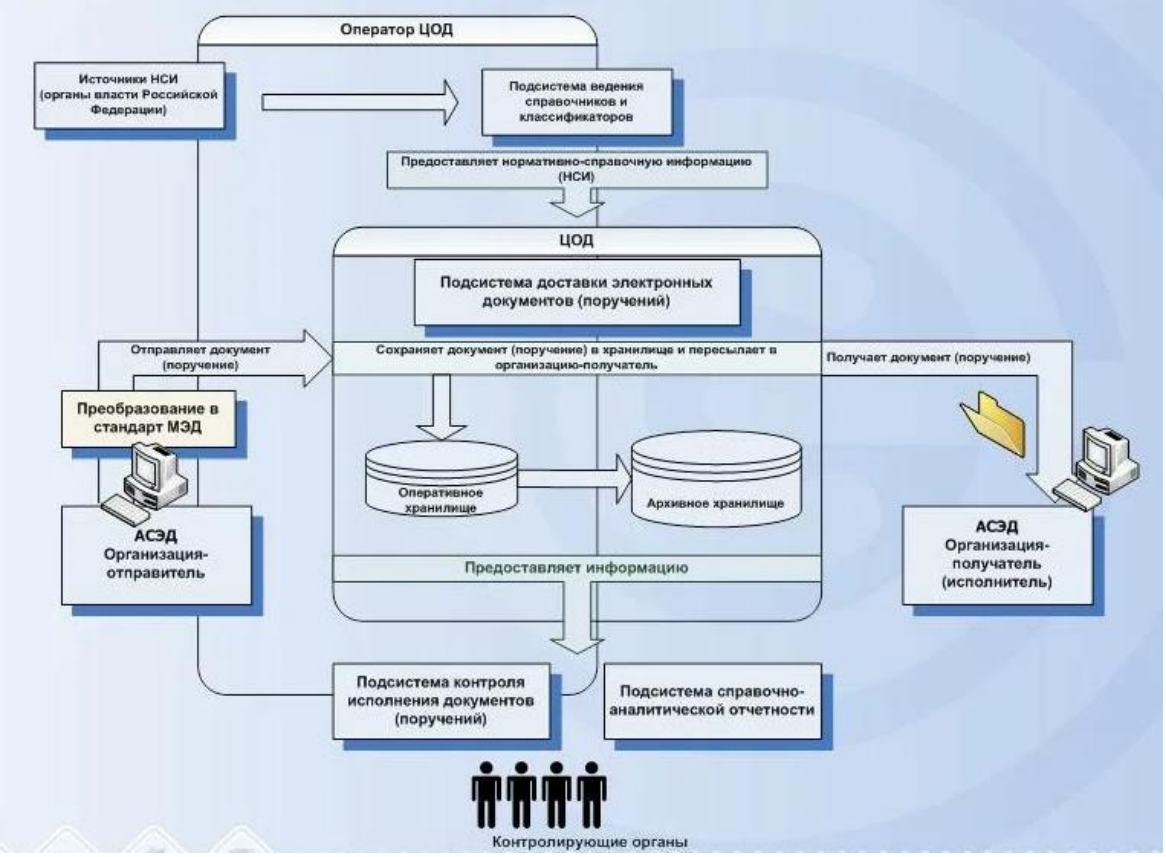

Рисунок 7 – Схема системы межведомственного электронного документооборота

«Взаимодействие организаций в рамках электронного документооборота понимается обмен электронными сообщениями, содержащими:

– документы – метаданные (реквизиты) документов и их файлы;
– уведомления – информацию о ходе рассмотрения и исполнения документов получателями» [10].

Поступив системы межведомственного электронного документооборота, в рамках Управления электронные документы передаются по локальной сети организации.

Так как все важные документы хранятся в Управлении в электронной форме (отдельные документы, согласно государственным регламентам, дублируются и в твердой копии), то работа сотрудников ИТ–службы очень

важна и ответственна. Рассмотрим более подробно деятельность сектора информационных технологий.

Организационная структура сектора информационных технологий представлена на рисунке 8.

Рисунок 8 – Организационная структура сектора информационных технологий

Сектор информационных технологий выполняет следующие задачи:

- подготовка и реализация ИТ–проектов;
- поддержание работы информационных систем;
- обеспечение информационной безопасности организации;
- устранение неполадок в аппаратном и программном обеспечении компьютерной техники;
- обновление компьютерного парка в соответствии с современными требованиями по согласованию с администрацией Управления;
- организация и сопровождение электронного делопроизводства;

– организация обучения сотрудников работе с новыми автоматизированными информационными системами.

В организации используется большое количество компьютерной техники, оснащенной разнообразным программным обеспечением, что связано со спецификой реализуемых услуг.

Анализ аппаратного и программного обеспечения в государственном автономном учреждении «Управление государственной экспертизы Ленинградской области» представлен в таблице 1.

Таблица 1 – Анализ аппаратного и программного обеспечения

Техническое/ программное обеспечение	Требует обновления (Да /Нет)
Техническое обеспечение	
Ноутбук ASUS Laptop 15 X515JA-BQ041T 90NB0SR1-M09150 (4 шт) Характеристики: - процессор: Intel Core i3 1005G1 (2x1200 МГц); - оперативная память: 8 ГБ DDR4 3200 МГц; - накопитель: SSD 256 ГБ; - встроенная видеокарта: Intel UHD Graphics.	Нет
Рабочие станции HP Desktop Pro 300 G3 MT (9LC19EA)/Windows 10 Pro (20 шт) Характеристики: - процессор: Intel Core i5-9400 (6x2900 МГц); - оперативная память: 8 ГБ DDR4 2666 МГц; - накопитель: SSD 256 ГБ; - встроенная видеокарта: Intel UHD Graphics 630.	Частично
Принтер Pantum P3010D с черно-белой лазерной печатью со скоростью 30 листов в минут;	Да
Многофункциональное устройство HP Neverstop Laser 1200w, которое выполняет три операции – печать, копирование и сканирование. Печать – черно-белая, скорость – 20 листов в минуту	Да
Сервер HPE Proliant DL380 Gen10	Нет
Сетевое оборудование: маршрутизатор TP-LINK TL-R470T маршрутизатор MikroTik RB4011iGS+RM	Да
Программное обеспечение	
Операционная система Windows 10 Pro	Нет
Серверная ОС Microsoft Windows Server 2019	Нет
Офисный пакет Microsoft Office 365 Business по подписке	Нет
1С: Документооборот 8	Нет

Продолжение таблицы 1

Техническое/ программное обеспечение	Требует обновления (Да /Нет)
1С Бухгалтерия 8.3	Нет
Браузеры: Google Chrome FireFox	Нет
Антивирусная программа Kaspersky Internet Security multi–Device	Нет
Специальное ПО	Частично

Как показал анализ аппаратного и программного обеспечения, профессиональная деятельность Управления достаточно хорошо оснащено компьютерным оборудованием и программным обеспечением, причем в большинстве своем в рамках имеющейся архитектуры ИТ–инфраструктуры поэтапная замена устаревшей аппаратуры и По производится практически незаметно для сотрудников.

Изменения требуется внести в подход к обеспечению информационной безопасности организации.

1.3 Обоснование необходимости совершенствования системы обеспечения информационной безопасности и защиты информации на предприятии

Анализ рисков информационной безопасности в Управлении ранее не проводился, так как все материальные и нематериальные ресурсы были до сих пор направлены на организацию деятельности, а в аудите ИБ не было ярко выраженной необходимости [23].

В настоящее время руководством организации принято решение о систематизации деятельности по усилению информационной безопасности организации, первым шагом которой является аудит информационных активов.

Исследование области деятельности предприятия позволило выявить следующие информационные активы, содержащие коммерческую тайну и/ или иные виды данных, подлежащих защите:

- информация/данные (в том числе информация, представляющая собой коммерческую тайну – технологические карты производства работ, договоры с потребителями услуги, проектная документация, а также персональные данные сотрудников);
- документы в твердой копии (договоры, чертежи и схемы технологических процессов, выписки из государственных реестров и др.);
- аппаратное обеспечение (персональные компьютеры, хранилище данных, используемая в компании оргтехника, сетевая аппаратура);
- программные средства, (операционные системы, прикладное программное обеспечение, в том числе средства САПР и офисное ПО, сетевое программное обеспечение);
- программно-аппаратные средства (флеш–накопители и внешние жесткие диски для хранения информации);
- конфиденциальность и доверие при оказании услуг;
- персонал организации.

При формировании перечня информационных активов были учтены положения Федерального закона от 29.07.2004 N 98-ФЗ (в редакции от 09.03.2021) «О коммерческой тайне» [20].

Анализ и оценка информационных активов выполнена на основе экспертного мнения руководителей и сотрудников компании.

«Для эффективной деятельности организации информационные объекты должны обладать следующими свойствами:

- доступность;
- своевременность доступа;
- достоверность;
- конфиденциальность;

– разграничение ответственности;

– защищенность от нежелательных искажений, утраты.

Безопасность произвольного информационного объекта может быть обеспечена за счет трех основных характеристик: конфиденциальность, доступность и достоверность» [7].

Конфиденциальность информации – субъективно определяемая характеристика (свойство) информации, указывающая на необходимость введения ограничений на круг субъектов (лиц), имеющих доступ к данной информации, и обеспечиваемая способностью системы (среды) сохранять указанную информацию в тайне от субъектов, не имеющих полномочий на доступ к ней [22].

«Целостность информации – защита от несанкционированного изменения или разрушения информации и программно-технической информационно среды.

Доступность информации – защита от несанкционированного сокрытия информации» [7].

Для оценки информационных активов использованы как количественные, так и качественные оценки.

Выполним моделирование процесса организации информационной безопасности в Управлении. Для моделирования бизнес–процессов выберем графическую нотацию IDEF0, так как она наиболее наглядно представляет процессы, их взаимосвязь и предполагает детализацию процессов любого уровня. Для разработки модели воспользуемся CASE–средством MS Visio.

MS Visio является векторным графическим редактором, в котором реализованы элементы многих графических нотаций моделирования бизнес–процессов – например, DFD, UML, IDEF0, eEPC и т.п.

Концептуальная модель предметной области «как есть» представлена на рисунке 9. Декомпозиция контекстной диаграммы предметной области представлена на рисунке 10.

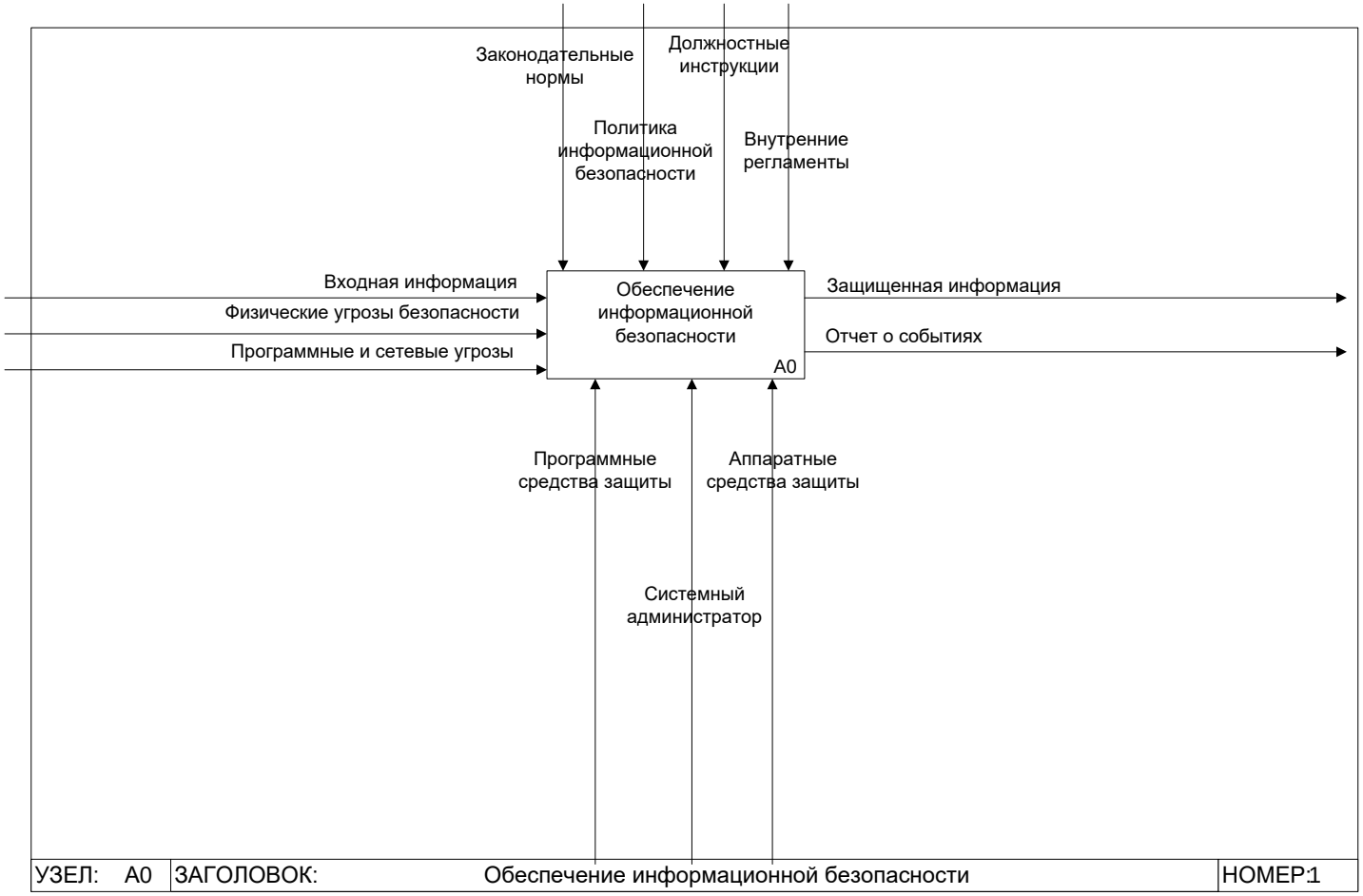

Рисунок 9 – Концептуальная модель предметной области (как есть)

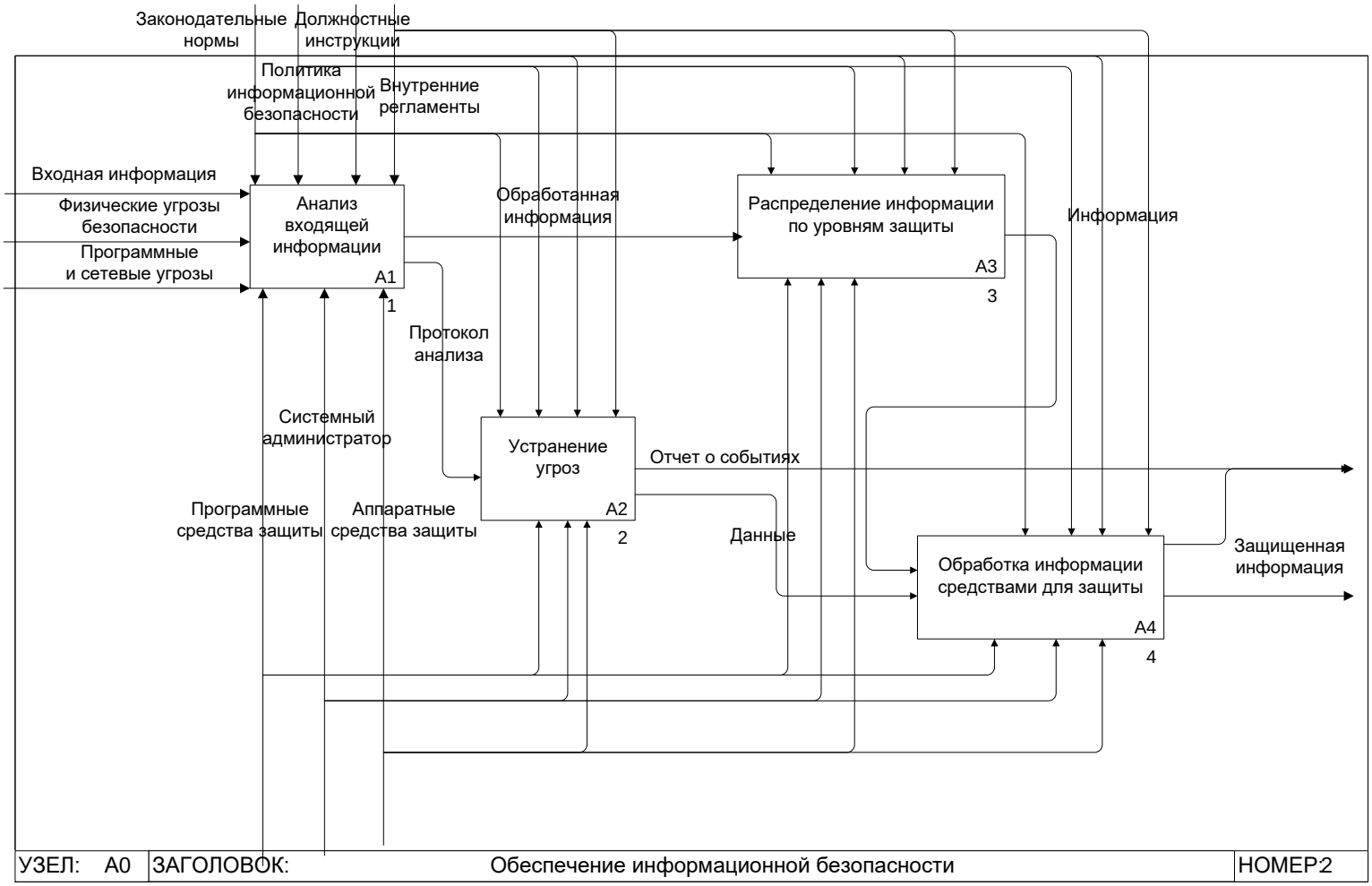

Рисунок 10 – Декомпозиция концептуальной модели предметной области (как есть)

Представленная модель «Как есть» показывает, что в Управлении государственной экспертизы Ленинградской области средства обеспечения информационной системы применяются, но они не составляют единый комплекс, поэтому требуется ее совершенствование.

1.4 Оценка существующих и планируемых средств защиты на предприятии

Все компьютеры Управления государственной экспертизы Ленинградской области функционируют под управлением операционной системы Windows 10. В качестве защиты от внешних угроз в компании используется антивирус Kaspersky Internet Security Multi-Device 2 устройства, выполняющий функции антивируса и брандмауэра. Программный продукт обеспечивает защиту сразу двух устройств – персонального компьютера или ноутбука, работающего под управлением операционной системы Windows и смартфона под управлением ОС Android. Таким образом решается вопрос защиты индивидуальных устройств сотрудников, которые иногда используются в решении профессиональных задач.

Для работы с базами данных, которые формируются и поддерживаются программами «1С: Бухгалтерия», каждый пользователь имеет логин и пароль для входа. Права пользователей разграничены по нескольким категориям.

Одной из уязвимостей при использовании паролей является человеческий фактор. Сотрудники, как правило, небрежно относятся к мероприятиям по защите данных, считают, что никто не сделает попытку получить доступ к конфиденциальным данным, поэтому можно отключить запрос логина и пароля на входе в систему, чтобы лишний раз не вводить их. Часто, отлучаясь из кабинета, сотрудники оставляют включенный компьютер с осуществленным в него входом и не запирают двери кабинета. Также сотрудники могут доверять друг другу пароли, электронные ключи, подписи и иные аутентифицирующие данные.

Анализ выполнения основных задач по обеспечению информационной безопасности Управление государственной экспертизы Ленинградской области представлена в таблице 2.

Таблица 2 – Анализ выполнения основных задач по обеспечению информационной безопасности

Основные задачи по обеспечению информационной безопасности	Степень выполнения
Обеспечение безопасности производственно-торговой деятельности, защита информации и сведений, являющихся коммерческой тайной	Средняя
Организация работы по правовой, организационной и инженерно-технической (физической, аппаратной, программной и математической) защите коммерческой тайны	Средняя
Организация специального делопроизводства, исключающего несанкционированное получение сведений, являющихся коммерческой тайной	Низкая
Предотвращение необоснованного допуска и открытого доступа к сведениям и работам, составляющим коммерческую тайну	Низкая
Выявление и локализация возможных каналов утечки конфиденциальной информации в процессе повседневной производственной деятельности и в экстремальных (авария, пожар и др.) ситуациях	Средняя
Обеспечение режима безопасности при осуществлении таких видов деятельности, как различные встречи, переговоры, совещания, заседания и другие мероприятия, связанные с деловым сотрудничеством на национальном и международном уровне	Высокая
Обеспечение охраны территории, зданий помещений, с защищаемой информацией.	Высокая

Расчет рисков необходим для выявления наиболее вероятных угроз для объекта информации и уязвимостей, через которые они могут быть реализованы. Это один из важнейших этапов защиты информации в организации [24].

Сегодня специалисты предлагают две основные методики оценки рисков информационной безопасности:

– метод, основанный на построении модели угроз и уязвимостей;
– метод, основанный на построении модели информационных потоков.

В качестве методики оценки рисков важных объектов в работе использована методика оценки риска ГРИФ 2006 из состава Digital Security Office, позволяющей проанализировать угрозы, действующие на каждый информационный ресурс организации на основе модели угроз и уязвимостей.

Алгоритм расчета рисков.

Рассчитать уровень угрозы по уязвимости Th по формуле

$$Th = \frac{ER}{100} \cdot \frac{P(V)}{100}, \quad (1)$$

где ER – критичность реализации угрозы в %;

P(V) – вероятность реализации угрозы через уязвимость Th.

Уровень угрозы демонстрирует степень критичности воздействия изучаемой угрозы на ресурс с учетом вероятности ее реализации [9].

Расчет выполняется по трем базовым угрозам – конфиденциальность, доступность и целостность [21].

Рассчитать уровень угрозы по всем уязвимостям CTh с учетом всех уязвимостей по формуле

$$CTh = 1 - \prod_{i=1}^{n} (1 - Th_i), \quad (2)$$

Рассчитать общий уровень угроз по ресурсу CThR с учетом всех угроз, применимых к ресурсу, по формуле

$$CThR = 1 - \prod_{i=1}^{n} (1 - CTh_i), \quad (3)$$

где CTh – уровень угрозы по всем уязвимостям.

Рассчитать риск по ресурсу по формуле

$$R = CThR \times D, \quad (4)$$

где D – критичность ресурса в денежных единицах

Оценка риска на основе данной методики позволяет получить наиболее полную и точную картину для формулировки задач по обеспечению информационной безопасности организации.

Выполним оценку рисков по представленной методике для отдельных объектов защиты. В качестве таких объектов экспертами выделены:

- автоматизированные рабочие места (АРМ) сотрудников;
- сервер локальной сети;
- базы данных;
- конфиденциальная информация;
- помещения, в которых обрабатывается и хранится конфиденциальная информация.

Данные для расчета критичности и вероятности реализации угроз представлены в таблице 3.

Таблица 3 – Вероятность и критичность реализации угроз

Угроза	Уязвимость	P(V), %	ER, %
АРМ сотрудников, обрабатывающих сведения, составляющие коммерческую тайну			
Физический доступ злоумышленника к АРМ	Отсутствие системы видеонаблюдения в офисных помещениях	10	50
	Отсутствие системы контроля доступа служащих к АРМ (например, оставление компьютера без выхода из сеанса работы)	10	40
	Неоптимальная политика паролей	15	80
Сбои в процессе эксплуатации АРМ	Человеческий фактор	15	20
	Отсутствие эффективной антивирусной защиты непосредственно АРМ	40	75

Продолжение таблицы 3

Угроза	Уязвимость	P(V), %	ER, %
Нарушение конфиденциальной информации с помощью вирусов и специальных программ	Неконтролируемый доступ сотрудников в Интернет	10	50
	Отсутствие эффективной антивирусной защиты непосредственно АРМ	50	80
Серверы локальной сети			
Уничтожение или разглашение информации, составляющей коммерческую тайну, хранящейся на сервере	Доступ к информации с автоматизированного рабочего места	10	50
	Наличие удаленного доступа	10	10
Выход сервера из строя	Нарушения электроснабжения	10	50
	Критически большое количество подключений	30	20
Конфиденциальная информация			
Физический доступ нарушителя к документам	Отсутствие видеонаблюдения в офисных помещениях	20	40
	Несоблюдение регламента работы с конфиденциальными документами	20	10
Несанкционированное манипулирование (печать, копирование, размножение) конфиденциальных документов	Неэффективный регламент работы с конфиденциальными документами	20	20
	Неконтролируемый доступ к оргтехнике (печатным и копировальным устройствам)	20	30

Уязвимости и риски для баз данных могут быть совмещены с оценкой рисков для серверов локальной сети, так как в организации для баз данных используется клиент-серверная архитектура.

Рисками для помещений, в которых обрабатывается и хранится конфиденциальная информация, можно пренебречь, так как допуск сотрудников в офисные и производственные помещения осуществляется по индивидуальным пропускам. На входе в офисный центр и в производственной группе имеется видеонаблюдение. В совокупности эти факторы исключают проникновение на территорию организации посторонних лиц.

Определим уровни угроз и оценим риски по каждому ресурсу по формулам 1–4. Вычисления выполнены в Excel. Результаты расчетов представлены на рисунке 11.

	A	B	C	D	E	F	G	H	I	J
1	**Угроза**	**Уязвимость**	**P**	**ER**	**Th**	**CTh**	**CThR**	**D, тыс. руб.**	**Кол-во**	**R, тыс. руб.**
2	**АРМ сотрудников, обрабатывающих сведения, составляющие коммерческую тайну**									
3	1	1	10	50	0,05	0,19744	0,689385	62,7	35	1512,86
4	1	2	10	40	0,04					
5	1	3	15	80	0,12					
6	2	1	15	20	0,03	0,321				
7	2	2	40	75	0,3					
8	3	1	10	50	0,05	0,43				
9	3	2	50	80	0,4					
10	**Серверы локальной сети**									
11	1	1	10	50	0,05	0,0595	0,160134	1260	2	403,54
12	1	2	10	10	0,01					
13	2	1	10	50	0,05	0,107				
14	2	2	30	20	0,06					
15	**Конфиденциальная информация**									
16	1	1	20	40	0,08	0,0984	0,186396	400	1	74,56
17	1	2	20	10	0,02					
18	2	1	20	20	0,04	0,0976				
19	2	2	20	30	0,06					

Рисунок 11 – Результаты оценки рисков

Таким образом, самый высокий уровень риска связан с использованием АРМ. Он достигает 69%, уровень потерь в денежном эквиваленте на одно АРМ составляет 42, 22 тысяч рублей.

В качестве основных проблем можно выделить:

– отсутствие эффективной антивирусной защиты непосредственно АРМ;

– неоптимальную политику паролей;

– человеческий фактор.

Риск для серверов локальной сети составляет 16%, что ниже, чем для АРМ, потери в расчете на один сервер достигают 201, 77 тысяч рублей.

Уязвимости, которые должны быть учтены при планировании задач обеспечения информационной безопасности:

– удаленный доступ к локальным сетям;

– разграничение операций пользователей.

Риск, связанный с хранением и использованием конфиденциальной информации, составляет 19%, потери (согласно оценке экспертов компании) – 74,56 тысяч рублей. Риск относительно невысокий, но следует отметить, как главные проблемы:

- неэффективный регламент работы с конфиденциальными документами;
- отсутствие видеонаблюдения в офисных помещениях;
- неконтролируемый доступ к оргтехнике.

Исключить выявленные проблемы и систематизировать вопросы информационной безопасности в управлении можно путем выстраивания комплексной системы защиты, которая включает организационно-административные меры и программно-аппаратные средства.

Комплексная система защиты информации подразумевает одновременное использование нескольких инструментов обеспечения информационной безопасности для снижения вероятности возникновения информационных угроз и их реализации. В выпускной квалификационной работе рассматриваются три основных вида инструментов:

- административно–организационные меры;
- инженерно-технические мероприятия;
- аппаратно-программные комплексы.

Концептуальная модель предметной области «как должно быть» в графической нотации IDEF0 представлена на рисунке 12. Декомпозиция контекстной диаграммы предметной области представлена на рисунке 13.

Изменения, внесенные в модель, выделены красным цветом.

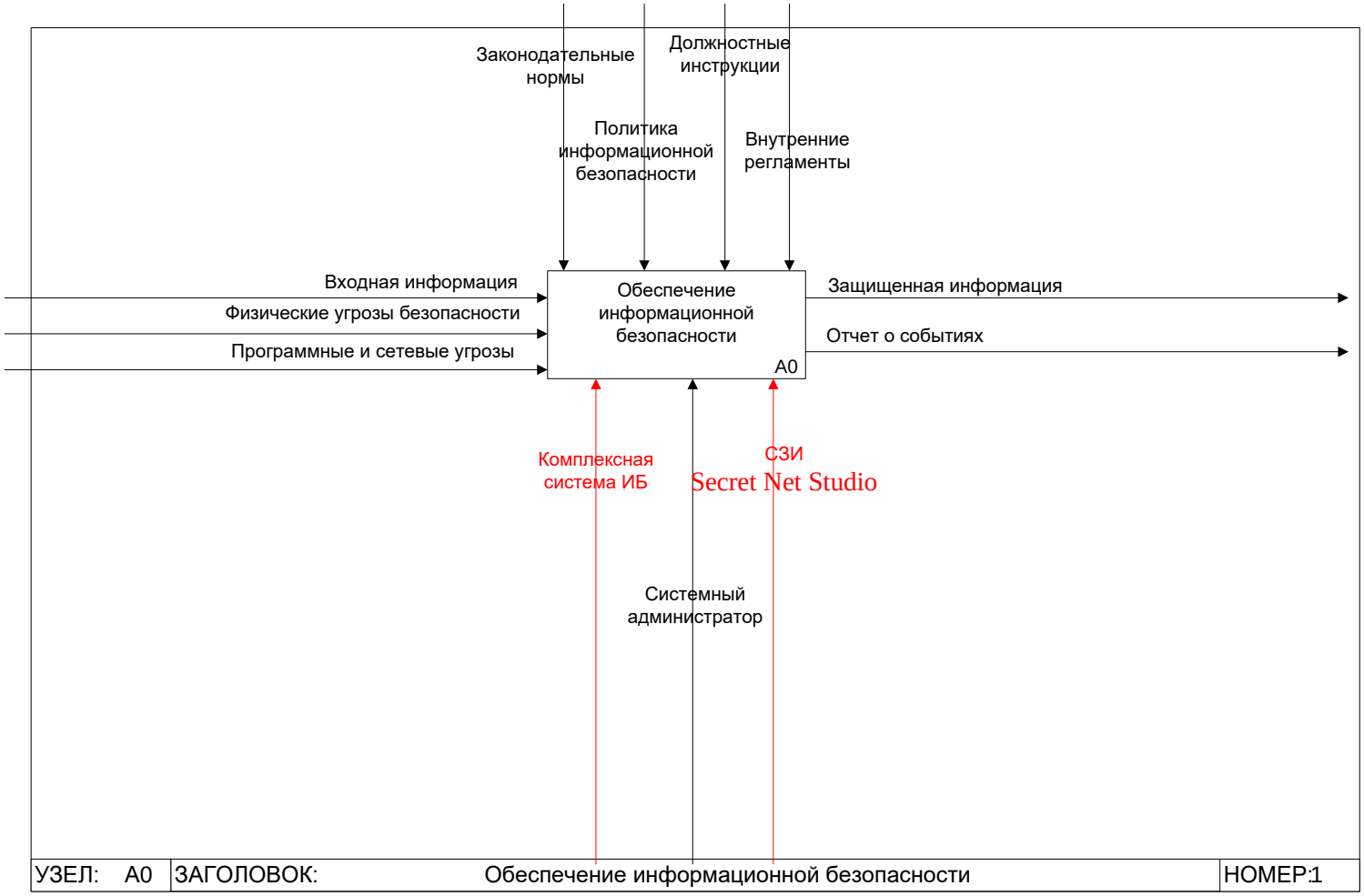

Рисунок 12 – Концептуальная модель предметной области (как должно быть)

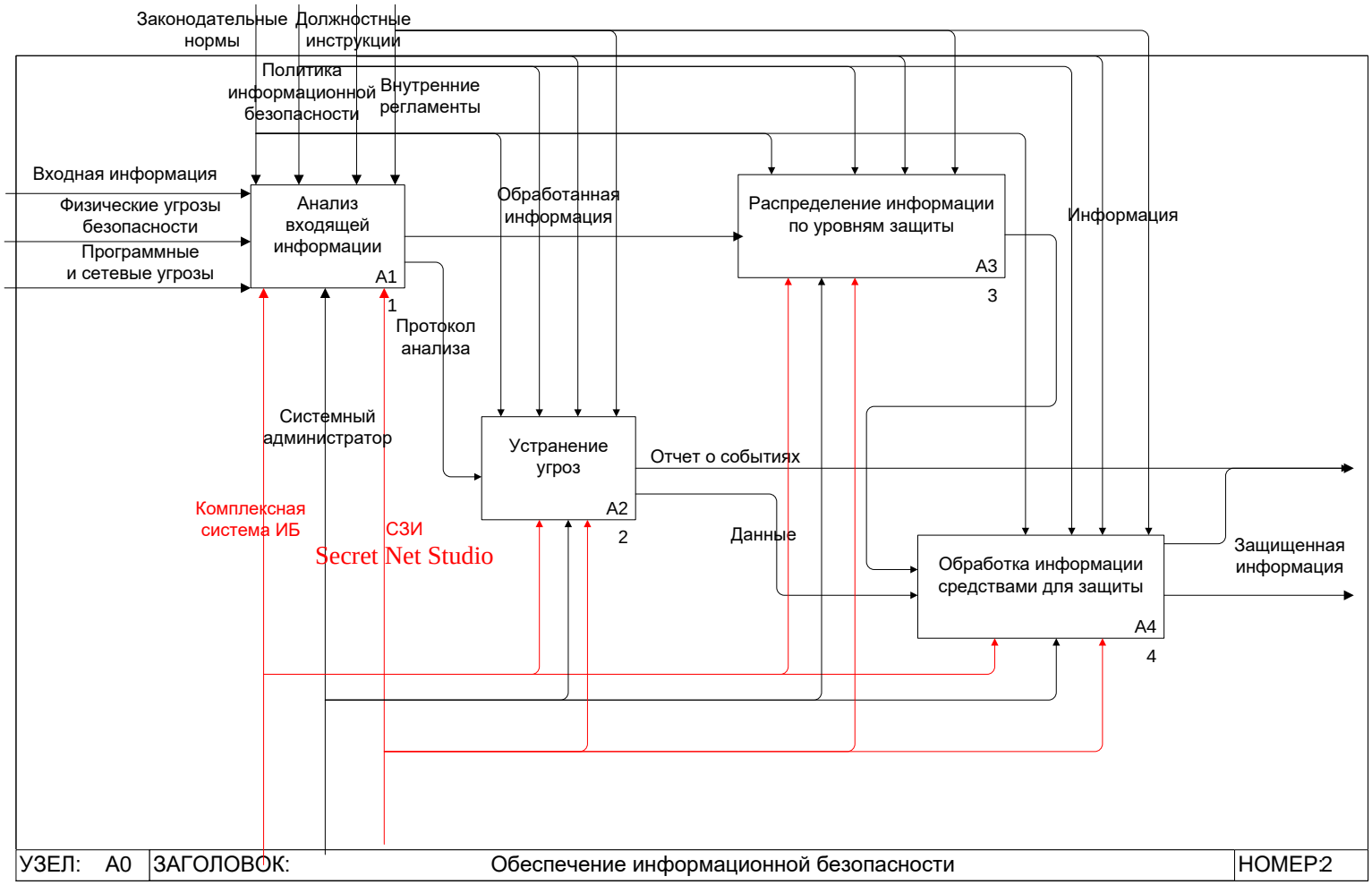

Рисунок 13 – Декомпозиция концептуальной модели предметной области (как должно быть)

Модель «Как должно быть» демонстрирует, что для формирования комплексной системы информационной безопасности в Управлении государственной экспертизы Ленинградской области должен быть принят ряд мер – организационных, инженерно-технических и программно-аппаратных.

Основными составляющими комплексной системы защиты информации являются организационное обеспечение информационной безопасности, а также программно-аппаратные средства, исключающие несанкционированный доступ к защищаемой информации.

Организационное обеспечение — это регламентация производственной деятельности, функционирования системы обработки данных, деятельности сотрудников организации с целью предотвращения или затруднения несанкционированного доступа к конфиденциальной информации.

Совокупность программно-аппаратных средств обеспечивает необходимую защиту информации от несанкционированного доступа.

Выводы по главе 1

В первой главе представлена технико-экономическая характеристика Управления государственной экспертизы Ленинградской области, описаны основные бизнес–процессы организации и построена функциональная модель защиты информации на предприятии «как есть». Модель разработана в графической нотации IDEF0.

Выполненный в первой главе анализ предметной области позволил оценить сегодняшнее состояние системы обеспечения информационной безопасности и защиты информации, выявить слабые места системы, ее уязвимости и возможность осуществления угроз.

На основании проведенного мониторинга системы информационной безопасности было принято решение о разработке и внедрении в Управлении комплексной программы защиты информации. Представлена функциональная модель «Как должно быть».

Глава 2 Логическое проектирование системы информационной безопасности организации

2.1 Основные понятия информационной безопасности экономического объекта

«Появление новых информационных технологий и развитие мощных компьютерных систем хранения и обработки информации повысили требования к уровню защиты информации и определили необходимость разработки эффективных механизмов защиты информации, адаптированной под современные архитектуры хранения данных» [6].

Защита информации в современном мире имеет высокий приоритет и является одной из самых важных тем в сфере IT-деятельности. Инструменты защиты информации необходимы как государственным и коммерческим организациям, так и каждому отдельно взятому человеку. Жизнедеятельность общества протекает сегодня в условиях, когда информация циркулирует в огромных количествах, она быстро распространяется по информационным каналам и доступна большому количеству людей. Обработка информации осуществляется с помощью компьютеров, ускоряющих и оптимизирующих этот процесс во много раз и в то же время уязвимых для всевозможных влияний как на данные, так и на устройства, их содержащие.

Для большинства информационных систем свойственны некоторые факторы, которые могут создать уязвимости: большой объем информации, внушительное количество пользователей в системе, которые работают с некоторой информацией, анонимность доступа, передача информации по каналам связи, а также возможность «информационных диверсий». Все эти и многие другие факторы создают задачу поддержания безопасности информационных систем и сетей.

«Активное развитие информационных технологий обуславливает актуальность изучения проблем информационной безопасности: угроз для

информационных ресурсов, различных средств и мер защиты, барьеров для проникновения, а также уязвимостей в системах защиты информации» [19].

Под информационной безопасностью в более общем виде «следует понимать совокупность средств, методов и процессов (процедур), обеспечивающих защиту информационных активов и, следовательно, гарантирующих сохранение эффективности и практической полезности как технической инфраструктуры информационных систем, так и сведений, которые в таких системах хранятся и обрабатываются» [3].

Под угрозой информационной безопасности «понимают события или действия, которые могут привести к искажению, несанкционированному использованию или даже к разрушению информационных ресурсов управляемой системы, а также программных и аппаратных средств» [13].

«Составные элементы информационной безопасности:

- формирование защищенности информационного пространства от всевозможных угроз для обеспечения его развития в интересах всех его пользователей;
- формирование информационной инфраструктуры, при которой использование информации строго регламентировано по назначению и категориям пользователей» [12];
- формирование информационной среды, в которой значительно затруднено или полностью исключено нарушение доступности, целостности или конфиденциальности информации;
- экономическая безопасность – системы сбора, накопления и обработки информации экономических подразделений, систем управления, системы экономического анализа, принятия решений, управление энергосистемами и др.;
- финансовая безопасность – автоматизированные информационные системы банков, системы обмена финансовой информацией, системы финансовых расчетов.

Обобщенная структура понятия «Информационная безопасность» представлена на рисунке 14.

Рисунок 14 – Структура понятия «Информационная безопасность»

В узком смысле под информационной безопасностью понимают:

- обеспечение надежности и безотказности в работе персонального компьютера;
- обеспечение сохранности и конфиденциальности информации, хранящейся в компьютере;
- обеспечение допуска к информации только тех лиц, для которых эта информация предназначена;
- обеспечение тайны личной переписки в социальных сетях и электронной почте.

В работе в качестве объекта информационной безопасности рассматривается некоммерческое предприятие. По отношению к организации понятие «информационная безопасность» подразумевает защиту информационных интересов учредителей предприятия, исключение несанкционированного доступа к информации, представляющей государственную и/ или коммерческую тайну и иным видам информации, определенным менеджерами компании, минимизацию информационных потерь от пересылки информации по каналам передачи.

Разработка системы защиты информации предприятия требует детального знакомства с бизнес-процессами организации, ее IT-инфраструктурой и стратегическими планами руководителей.

2.2 Информация как товар и объект безопасности

«Информационное пространство (инфосфера) - сфера человеческой деятельности связанная: с созданием, преобразованием и потреблением информации и включающая в себя:

- индивидуальное и общественное сознание
- информационные ресурсы, то есть информационную инфраструктуру (комплекс организационных структур, технических средств, программного и другого обеспечения для формирования, хранения, обработки и передачи информации), а также собственно информацию и ее потоки» [13].

«Прогресс в новейших информационных технологиях делает весьма уязвимым любое общество. Каждый прорыв человечества в будущее не освобождает его от груза прошлых ошибок и нерешенных проблем» [13].

Рассмотрим основные термины, относящиеся к информационной безопасности.

«Информационная преступность – проведение информационных воздействий на информационное пространство или любой его элемент в

противоправных целях. Как ее частный вид может рассматриваться информационный терроризм, то есть деятельность, проводимая в политических целях» [13].

«Информационное оружие – комплекс технических и других средств, методов и технологий, предназначенных для:

- установления контроля над информационными ресурсами потенциального противника;
- вмешательство в работу его систем управления и информационных сетей, систем связи и т.п. в целях нарушения их работоспособности, вплоть до полного выведения из строя, изъятия, искажения содержащихся в них данных или направленного введения специальной информации» [13];
- «распространение выгодной информации и дезинформации в системе формирования общественного мнения и принятия решений» [13];
- «воздействие на сознание и психику политического и военного руководства, личного состава вооруженных сил, спецслужб и населения противостоящего государства, используемых для достижения превосходства над противником или ослабления проводимых им информационных воздействий» [13].

«Стремительное и агрессивное развитие информационных технологий значительно усиливает актуальность исследования и изучения проблем информационной безопасности и их причин:

- угроз для информационных ресурсов,
- разнообразных средств и мер защиты, барьеров для проникновения;
- уязвимостей в системах защиты информации» [7].

«Под информационной безопасностью в более общем виде понимают совокупность средств, методов и процессов (процедур), обеспечивающих защиту информационных активов и, следовательно, гарантирующих сохранение эффективности и практической полезности как технической

инфраструктуры информационных систем, так и сведений, которые в таких системах хранятся и обрабатываются» [13].

Данные, которые использует в своей практической деятельности любая организация, в обязательном случае содержат экономическую информацию, которая относится к области экономических знаний. Этот вид информации характеризует процессы снабжения, производства, распределения и потребления материальных благ.

В процессе функционирования экономических объектов, их развития и управления ими всегда происходит преобразование экономической информации.

Если исходить из положений кибернетически – науки об общих свойствах управления в живых и неживых системах – любой процесс управления возможно свести к взаимодействию управляемого объекта и системы управления этим объектом. В процессе такого взаимодействия вырабатывается управляющая информация как результат соотнесения полученной от объекта управления информации о его состоянии и проанализированной системой управления.

Деятельность любой современной компании опирается, в том числе, и информационные ресурсы, которые сегодня зачастую оцениваются выше, чем материальные блага. К информационным ресурсам относят бумажные и электронные документы, базы данных и другие источники и носители как внутренней, так внешней информации, относящейся к деятельности компании (рисунок 15).

Информационные ресурсы, а также их производные – информационные услуги и продукты, представляют ценность в некоторой предметной области, то их рассматривают в качестве товара (за исключением случаев, когда информационные ресурсы законодательно отнесены к государственной тайне или другим видам информации, охраняемым государством).

Отмечают следующие качества информации как товара:

– неисчерпаемость – запасы информации с развитием общества растут;

– сохраняемость – информация при использовании не только сохраняется, ее количество может в процессе использования даже возрасти;
– несамостоятельность – информация имеет ценность и проявляет свои качества только при взаимодействии с другими ресурсами (человеческими, вычислительными и другими).

Рисунок 15 – Информационные ресурсы компании

Информация представляет ценность для компании, в которой она хранится, используется, генерируется, обрабатывается. Любая ценность нуждается в защите, информационные ресурсы организации не являются исключением. Имеется множество видов и градаций информации, доступ к которой ограничен не только профессиональными интересами использующей

ее компании, но и на законодательном уровне. К таким видам информации можно, например, отнести следующие виды данных:

- персональные данные [1];
- врачебная тайна;
- тайна усыновления;
- адвокатская тайна; тайна частной жизни человека и др.

Кроме несанкционированного доступа, информация должна быть защищена и от других видов угроз – таких, как внешние атаки, вирусы, технические сбои.

Вопросы защиты информации являются очень важным направлением в деятельности большинства современных компаний, так как ущерб, вследствие порчи, утери или опубликования конфиденциальной информации может быть очень велик.

2.3 Информационные угрозы и их виды

Согласно ГОСТ Р ИСО/МЭК 27005-2010 «Методы и средства обеспечения безопасности»:

«Уязвимости могут быть связаны со свойствами актива. Способ и цели использования актива могут отличаться от планируемых при приобретении или создании актива. Необходимо учитывать уязвимости, возникающие из разных источников, например те, которые являются внешними или внутренними по отношению к активу» [8].

Понятие «уязвимость» можно отнести к свойствам или атрибутам актива, которые могут использоваться иным образом или для иных целей, чем те, для которых приобретался или изготавливался данный актив.

В ГОСТ Р 56546-2015 «Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем» [6] представлены следующие типы уязвимостей информационных систем:

– уязвимость кода;
– уязвимость конфигурации;
– уязвимость архитектуры;
– организационная уязвимость;
– многофакторная уязвимость.

Термин «уязвимость» применяют в информационной безопасности для определения изъяна информационной системы, который может стать источником нарушения целостности и нарушить правильность работы. Уязвимость представляет собой потенциальную возможность проявления угрозы безопасности информационных ресурсов [12].

Уязвимость может возникнуть вследствие разных причин – например, в результате ошибок проектирования информационной системы или разработки программного кода, недостатков, допущенных при проектировании информационной системы, вредоносных программ, недостаточно сложных паролей и др.

Выявление уязвимостей возможно осуществить различными способами. Перечень уязвимости может быть представлен как изнутри организации, например, сотрудником IT-службы, инженерным работником, сетевым администратором, так и представителем внешней по отношению к исследуемой компании – специалистом, приглашенным для реализации информационного аудита и выявления уязвимостей.

«Под угрозой информационной безопасности понимается потенциально возможные действия или же процессы, которые способны оказать нежелательные воздействия на саму систему или информацию, находящуюся в ней. Такие угрозы могут привести к искажению, копированию, незаконному распространению или же ограничению доступа к данным системы» [18].

Угрозы информационной безопасности могут быть классифицированы по различным основаниям. Классификация угроз по источнику представлена на рисунке 16.

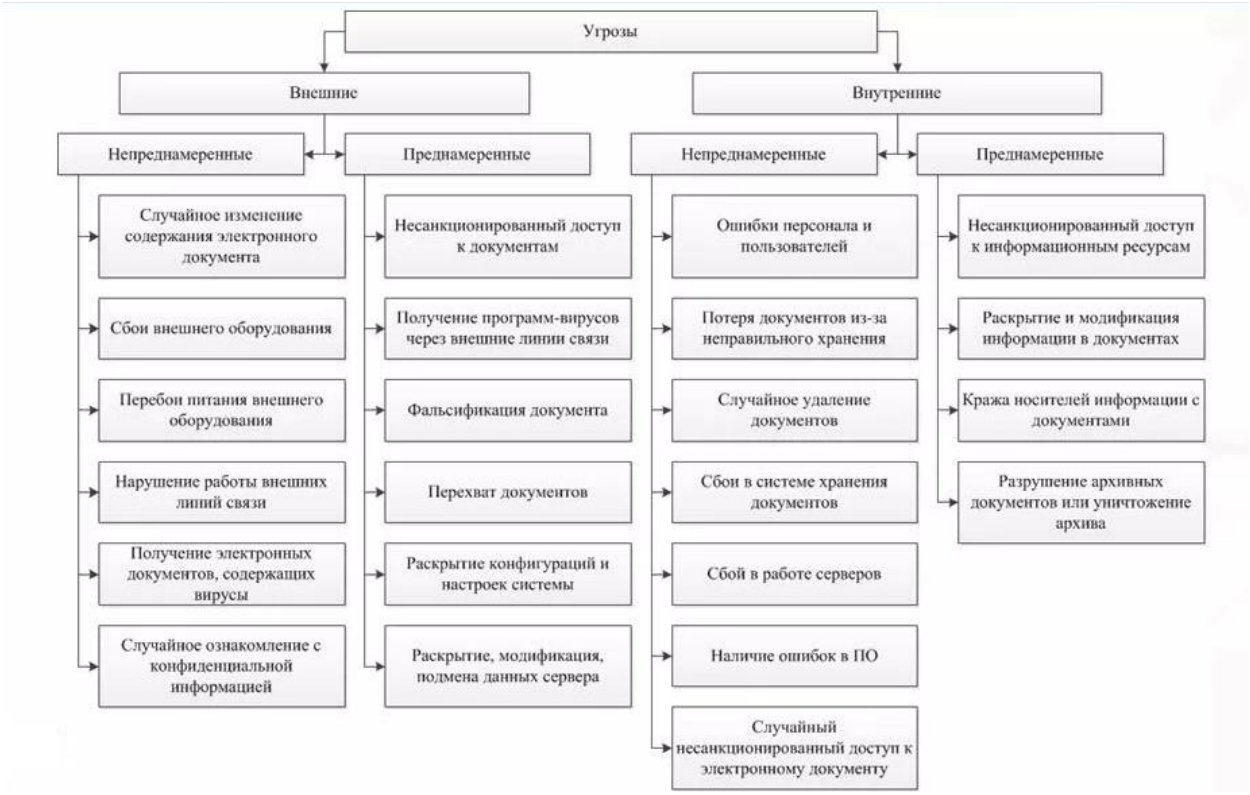

Рисунок 16 – Классификация угроз информационной безопасности по источникам

«Сущность информационной безопасности в широком понимании заключается в выявлении и устранении негативных источников воздействия на информацию. Методы и цели защиты информационного ресурса также могут определять ее сущность» [10]. Как правило, «специалисты определяют сущность информационной безопасности как отсутствие какой-либо возможности источнику угрозы оказать негативное воздействие на объект защиты информации, которое может также нанести ущерб также его функциональной деятельности или самим свойствам» [12].

Выполним моделирование системы информационной безопасности в графической нотации UML, позволяющей выполнить модель бизнес-процесса на всех стадиях его протекания. При моделировании информационной системы унифицированный язык моделирования UML позволяет в некоторых CASE–средствах даже сгенерировать скелетный код системы на выбранном языке моделирования.

Диаграмма прецедентов системы информационной безопасности для Управления государственной экспертизы Ленинградской области представлена на рисунке 17.

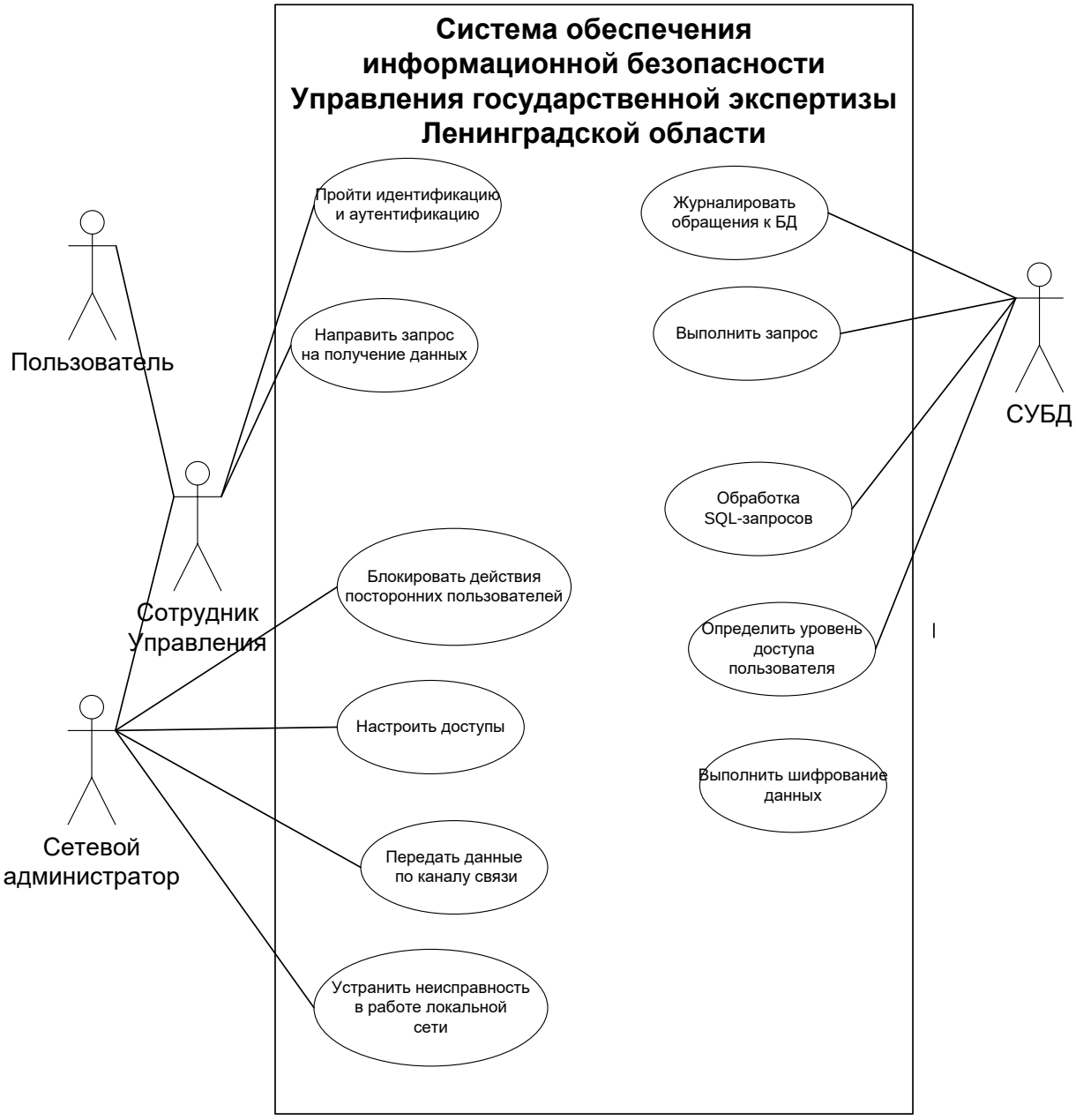

Рисунок 17 – Диаграмма вариантов использования системы информационной безопасности

Диаграммы активности управления инцидентами системы информационной безопасности представлены на рисунках 18–19.

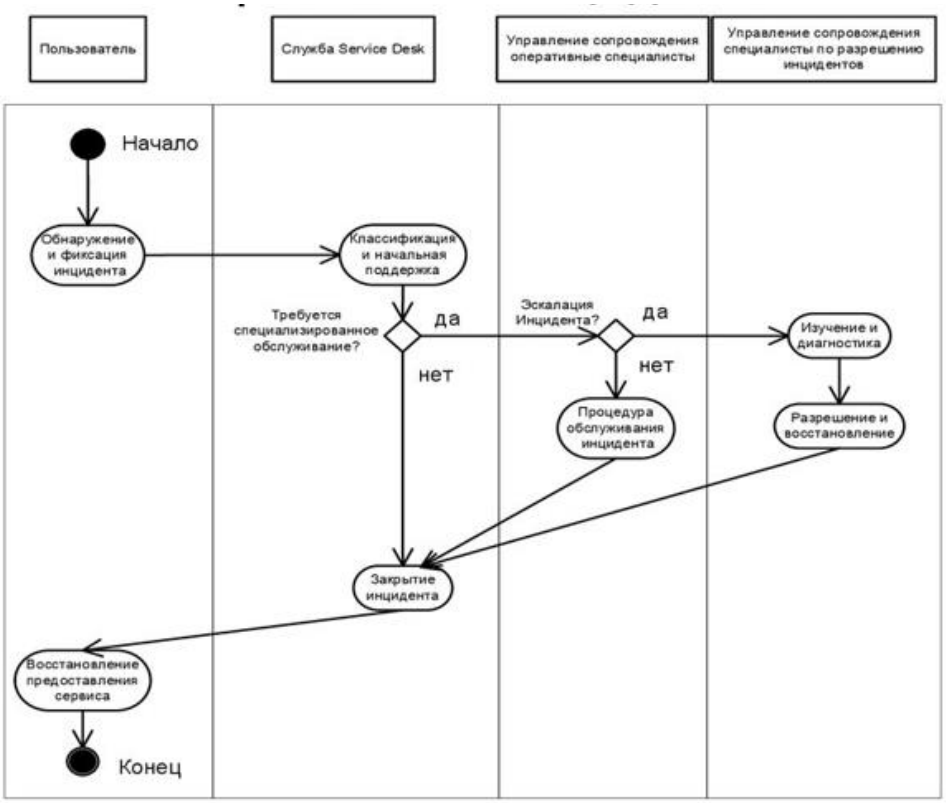

Рисунок 18 – Диаграмма активности системы при обнаружении инцидента

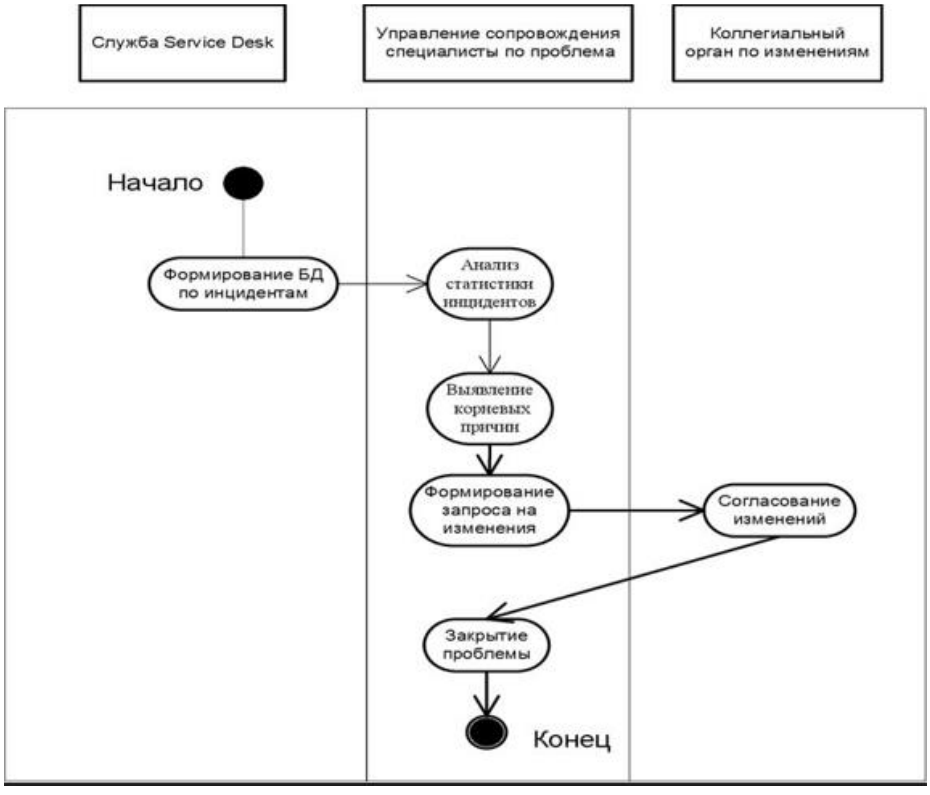

Рисунок 19 – Диаграмма активности Формирование БД инцидентов

Диаграмма последовательностей прецедента Пройти идентификацию и аутентификацию представлен на рисунке 20.

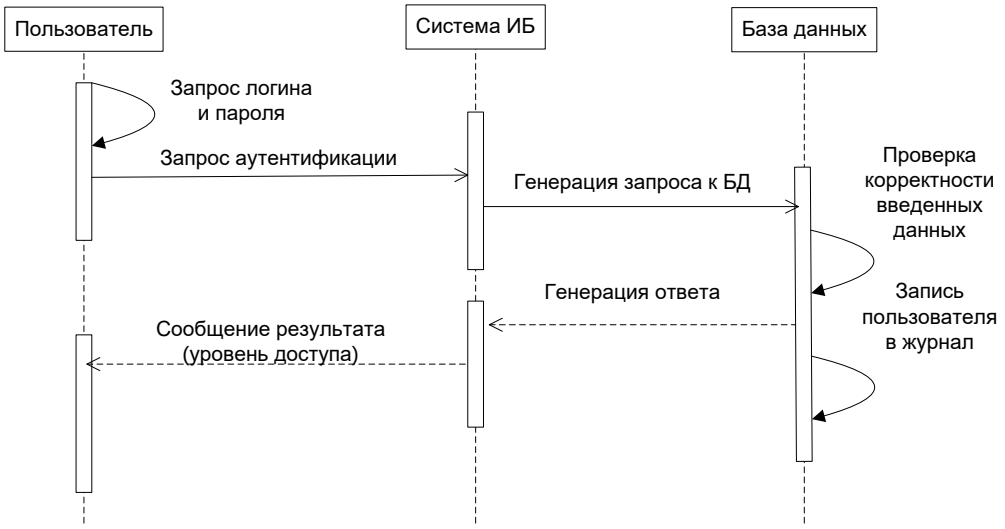

Рисунок 20 – Диаграмма последовательностей

Рассмотрены основные аспекты моделирования системы обеспечения безопасности на предприятии.

Выводы по главе 2

Во второй главе представлены основные понятия информационной безопасности. Рассмотрены понятия уязвимостей информационной безопасности, представлены и классифицированы угрозы.

В главе изучены с точки зрения обеспечения информационной безопасности активы Управления государственной экспертизы Ленинградской области, сделана оценка их уязвимости. Особенное внимание уделено несанкционированному доступу к информации, а также вирусным атакам, которые могут угрожать локальной сети организации.

Сформулировано наиболее общее определение информационной безопасности в широком понимании и показано, что ее роль заключается в выявлении и устранении негативных источников воздействия на информацию.

Глава 3 Физическое проектирование системы обеспечения информационной безопасности предприятия

3.1 Организационные меры обеспечения политики информационной безопасности предприятия

Развитие современного мира движется в направлении информационного общества. Информационное общество представляет собой такую стадию развития общества, при которой использование информационно-коммуникационных технологий оказывает существенное влияние на все социальные институты и сферы жизни.

«Наличие нормативно-правовой базы, регулирующей взаимоотношения субъектов в сфере информационных отношений, является обязательным условием для эффективного функционирования современного общества. С помощью правовой базы, соответствующей актуальным проблемам и тенденциям информационного характера, становится возможным предотвратить угрозу или защитить свои права на тот или иной вид информации. Правовое регулирование принимает принципиально важное значение в сфере безопасности федеральной и государственной службы, включающей гражданскую, военную и правоохранительную. Необходимо проанализировать вопрос актуальности нормативно-правовой базы обеспечения информационной безопасности с целью выявления сильных и слабых сторон защиты прав граждан на территории Российской Федерации» [15].

Информационные технологии активно развиваются, постоянно обновляется как аппаратная составляющая компьютерных устройств, так и программное обеспечение. Появляются новые уязвимости и новые угрозы информационной безопасности. Нормативно-правовая база, определяющая и регулирующая основные положения информационной безопасности, также находится в процессе постоянного обновления. Развитие новых возможных

правоотношений в области информационной безопасности также является причиной постоянной модернизации правового регулирования.

К нормативно-правовым актам (НПА) в части обеспечения информационной безопасности могут быть отнесены следующие основные документы:

- Конституция Российской Федерации;
- Гражданский Кодекс Российской Федерации;
- Уголовный Кодекс Российской Федерации;
- Доктрина информационной безопасности;
- ФЗ №128 – «О лицензировании отдельных видов деятельности»;
- ФЗ №149 – «Об информации, информационных технологиях и защите информации»;
- ФЗ №98 «О коммерческой тайне»;
- ФЗ №152 – «О персональных данных».

Важными регламентирующими документами являются стандарты в сфере информационной безопасности (международные и национальные), а также рекомендации и методические указания.

В Конституции РФ безопасность упоминается как по отношению к государству, обществу, так и к личности. Основное обращение к понятию «государственная безопасность» содержится в статьях 13, 55, 82 и 114. Вообще в Конституции Российской Федерации помимо государственной безопасности можно встретить понятия безопасности граждан, общественных видов безопасности, экологический безопасности.

«Наиболее часто упоминаемым в Конституции РФ термином, связанным с видами безопасностью, является «безопасность личности». Этот вид безопасности означает защищенность прав и свобод индивида и гражданина, в том числе право на информационную безопасность.

Наиболее приоритетным направлением на современной фазе развития правового регулирования информационной безопасности стала

своевременность разрабатываемых предложений по эффективной защите прав человека в области информационного пространства» [1].

«Активно прогрессирующее развитие информационно-коммуникационной значительно влияет на важнейшие отрасли безопасности страны – военную, политическую и экономическую. Комплекс национальной безопасности страны существенно зависит от уровня информационной защищенности и качественной реализации обеспечения информационной безопасности» [16].

Доктрина национальной безопасности Российской Федерации утверждена Указом Президента РФ от 05.12.2016 г. № 646 и является основополагающим документов в вопросах безопасности государственного и персонального характера.

В Доктрине прямо указывается, что недостаточный уровень организации системы защиты у федеральных органов государственной власти, государственных органов власти и органов местного самоуправления может повлечь за собой ряд тяжких последствий, так как процесс их работы напрямую связан с накоплением и хранением большого количества данных, в том числе персональных [3].

В Уголовном кодексе РФ предусмотрено наказание за незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, в том числе с использованием служебного положения, а также за незаконное распространение в публичном выступлении и публичную демонстрацию информации, указывающей на личность несовершеннолетнего потерпевшего, не достигшего шестнадцатилетнего возраста, по уголовным делам (статья 137. Нарушение неприкосновенности частной жизни) [4].

На рисунке 21 представлена динамика роста преступлений, связанных с нарушением неприкосновенности частной жизни за последние 5 лет. Диаграмма построена на основе официальной судебной статистики, представленной на портале «Судебная статистика РФ» [17].

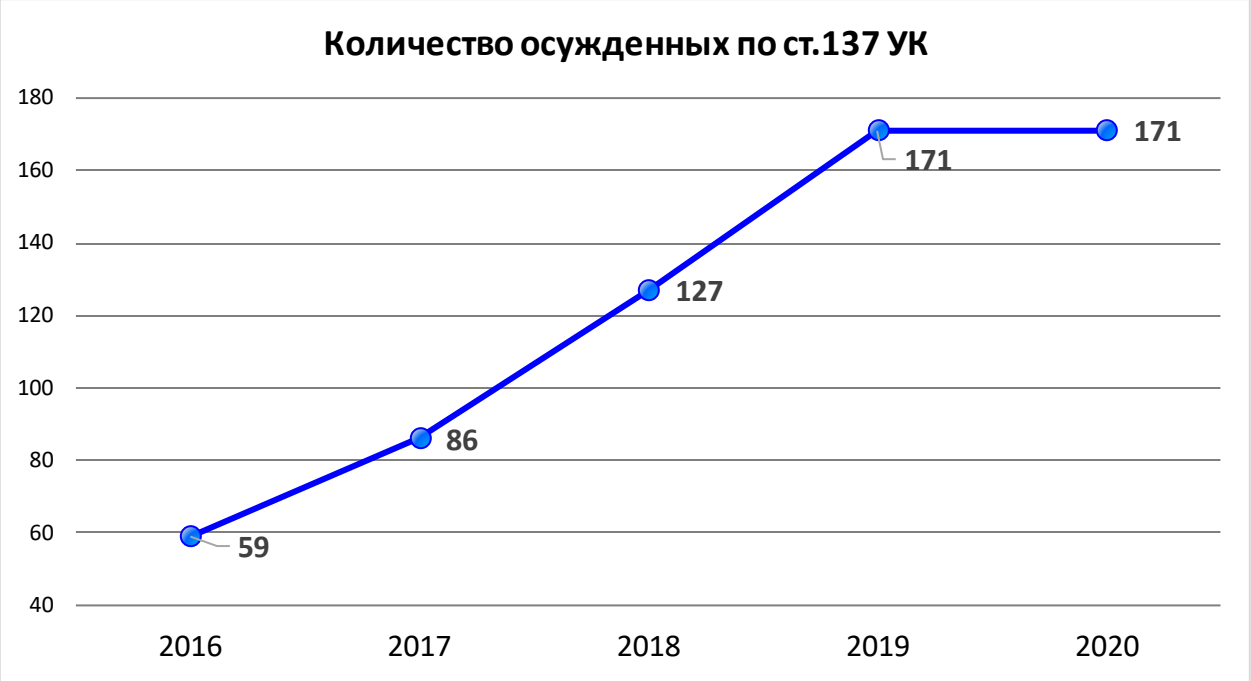

Рисунок 21 – Динамика роста преступлений, связанных с нарушением неприкосновенности частной жизни

Представленная диаграмма может быть демонстрацией обобщенной картины преступлений против информационной безопасности и в других сферах жизнедеятельности человека, которые также упоминаются в Уголовном кодексе РФ.

Видно, что количество преступлений против информационной безопасности растет и требует общего усиления и систематизации защитных мер. В связи с этим особенное внимание требуется уделить созданию единого комплекса нормативно-правовых актов региональных органов власти, органов местного самоуправления, а также собственно организаций и предприятий.

Федеральный Закон № 98-ФЗ «О коммерческой тайне» является основным нормативно-правовым документом, на основании которого коммерческие организации создают собственную систему защиты данных, представляющих закрытую информацию разной степени секретности.

Коммерческой тайной закон определяет «режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных

расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду».

«Информация, составляющая коммерческую тайну, – сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность» [2].

Помимо определения коммерческой тайны статья 3 Закона о коммерческой тайне трактует понятия доступа, передачи, представления и разглашения информации, составляющей коммерческую тайну.

В то же время закон определяет сведения, не подлежащие засекречиванию организацией ни при каких условиях (статья 5):

- данные учредительных документов и правоустанавливающих субъектов предпринимательской деятельности;
- состав имущества муниципальных и государственных учреждений;
- сведения о противопожарной безопасности, радиационной и санитарно-эпидемиологической обстановке на предприятии;
- состав и численность сотрудников, система оплаты труда и др.;
- сведения о нарушениях законодательства и т.п.

Свод правил защиты конфиденциальной информации представлены в статье 10 «Охрана конфиденциальности информации». Среди предложенных законом мер:

- определение перечня информации, составляющей коммерческую тайну;
- ограничение доступа к информации, составляющей коммерческую тайну;
- учет лиц, получивших доступ к информации, составляющей коммерческую тайну;

– регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;
– нанесение на материальные носители, содержащие информацию, составляющую коммерческую тайну, грифа «Коммерческая тайна» [2].
– Закон определяет оценку достаточности мер по охране конфиденциальности информации (п.5 статьи 10):
– исключение доступа к конфиденциальной информации без согласия ее обладателя;
– обеспечение соблюдения режима коммерческой тайны всеми сотрудниками организации.

На основе проанализированных и иных нормативно-правовых актов и в соответствии с ними на предприятии разрабатывается комплекс нормативных документов, регулирующих функционирование организации и взаимодействие персонала в части обеспечения информационной безопасности.

Комплексный план мероприятий, направленный на сокращение угроз информационной безопасности предполагает разработку нормативно-правовой базы, регулирующей деятельность ответственных сотрудников организации по работе с угрозами, внедрение нового, более подходящего к специфике организации, программного обеспечения в качестве инструментов контроля, мониторинга и устранение уязвимостей, а также разработку регламентов, памяток и методических рекомендаций, которые обеспечат работников предприятия, ответственных за информационную безопасность, достаточным количеством информации по работе с выявлением и устранением угроз, а также мероприятия, направленные на обучение специалистов и администраторов, которые включают протокол оперативного совещания.

Организационно-распорядительная документация второго уровня в сфере обеспечения информационной безопасности оказывает существенное влияние на обеспечение безопасности компании. К документации второго уровня относят регламенты, инструкции и методические рекомендации, позволяющие установить методы и порядок деятельности по защите от угроз информационной безопасности.

Принятие отдельных внутренних нормативных актов регламентируется требованиями законодательства, к ним относится, например, положение об обработке персональных данных, которое должен разработать и разместить на своем сайте каждый оператор персональных данных.

К организационным мерам обеспечения информационной безопасности в организации также относят:

- определение уровней доступа сотрудников к информации, содержащей коммерческую тайну;
- формирование группы лиц (подразделений), ответственных за обеспечение информационной безопасности;
- регулярное информирование и обучение персонала в части информационной безопасности, включая действия по работе с информационной системой в критических условиях;
- обеспечение технической защиты помещений и оборудования с дальнейшей сертификацией классов защиты, определение их соответствия нормативно-правовым требованиям;
- внедрение и поддержка пропускной системы для сотрудников, обеспечение их электронными средствами идентификации;
- выполнение всех требований законодательства по защите персональных данных;
- формирование системы взаимодействия с государственными органами в части обмена конфиденциальной информацией.

Меры защиты информации с технической точки зрения должны базироваться на модели построения информационной системы организации,

которая позволит выстроить защиту против несанкционированного доступа и повреждения конфиденциальных данных.

В качестве таких принципов можно принять:

- простоту архитектуры информационной системы, использование в ней только необходимых аппаратно-программных компонентов, избавление от избыточных функций;
- уменьшение количества каналов и протоколов межсетевого взаимодействия;
- внедрение надежных лицензионных программных решений, протестированных и получивших положительные рекомендации от использующих их организаций;
- использование в системе надежных компонентов, застрахованных от неожиданной поломки и нарушения работы системы;
- простоту администрирования как системы, так и используемого ПО, минимизация сторонней техподдержки.

Для выполнения указанных принципов реализуют следующие «организационно-административные мероприятия защиты информации:

- выделение специальных защищенных помещений для размещения компьютеров и средств связи и хранения носителей информации;
- выделение специальных компьютеров для обработки конфиденциальной информации;
- использование в работе с конфиденциальной информацией технических и программных средств, имеющих сертификат защищенности и установленных в аттестованных помещениях;
- применение специальной маркировки на носителях для хранения конфиденциальной информации;
- организация для конфиденциальной информации специального делопроизводства, определяющего порядок подготовки, использования, хранения, уничтожения и учета документированной информации;

– запрещение использования открытых каналов связи для передачи конфиденциальной информации;
– организация регламентированного доступа пользователей к работе на компьютерах, средствам связи и к хранилищам носителей конфиденциальной информации;
– разработка и внедрение специальных нормативно-правовых и распорядительных документов по организации защиты конфиденциальной информации, которые регламентируют деятельность всех звеньев объекта защиты в процессе обработки, хранения, передачи и использования информации;
– регулярный контроль соблюдения введенных требований к защите информации» [14].

По результатам анализа используемой в Управлении государственной экспертизы Ленинградской области системы обеспечения информационной безопасности принято решение о реализации следующих административных мер обеспечения информационной безопасности:

а) Разработать (усовершенствовать) и утвердить следующий перечень нормативных документов в рамках организации:

1) перечень сведений, содержащих конфиденциальную информацию в ГАУ «Управление государственной экспертизы Ленинградской области» (Перечень);

2) положение о порядке организации и проведения работ по защите конфиденциальной информации в ГАУ «Управление государственной экспертизы Ленинградской области» (Положение);

3) инструкция о порядке обращения с документированной служебной информацией ограниченного распространения в ГАУ «Управление государственной экспертизы Ленинградской области» (Инструкция);

4) журнал учета носителей информации (Журнал).

б) Разработать и утвердить приказ по ГАУ «Управление государственной экспертизы Ленинградской области», в котором:

1) определить круг лиц, на которых возлагается обязанность выявления потенциальных опасностей утечки сведений, составляющих коммерческую тайну и ответственность за организацию и реализацию мероприятий, направленных на обеспечение информационной безопасности предприятия, в том числе – сохранности конфиденциальной информации;

2) конкретизировать меры административной ответственности за нарушение регламентов, определенных в ГАУ «Управлении государственной экспертизы Ленинградской области» для работы с конфиденциальной информацией.

в) Ввести на запрет хранения на компьютерах, предназначенных для обработки сведений, содержащих коммерческую тайну, личной информации.

г) При принятии на работу сотрудников, которым по долгу службы необходимо работать с конфиденциальной информацией, одновременно с заключением трудового договора оформлять письменное обязательство о неразглашении секретных сведений.

д) При увольнении с работы сотрудников, которым по долгу службы необходимо работать с конфиденциальной информацией, организовать возврат всех имеющихся у них в распоряжении специальных маркированных носителей.

е) Разработать для каждого уровня доступа и передать для служебного использования каждому сотруднику, работающему с конфиденциальной информацией, памятку с положениями Инструкции.

Рассмотрим далее аппаратные и программные средства обеспечения информационной безопасности.

3.2 Аппаратные и программные средства обеспечения информационной безопасности предприятия

«Под программно-аппаратным комплексом понимают совокупность технических и программных средств, совместно работающих для выполнения одной или нескольких близких задач» [3].

Программный комплекс Управления государственной экспертизы Ленинградской области включает следующие компоненты:

- операционная система Windows 10;
- антивирусный комплекс Kaspersky Internet Security Multi-Device;
- браузер Google Chrome;
- облачное решение для офисной работы «Microsoft 365»;
- программа бухгалтерского учета «1С: Бухгалтерия».

«В программном комплексе парольная защита организована посредством стандартного разграничения доступа пользователей ОС Windows, передача данных осуществляется в интернет без использования защищенного соединения.

Для более расширенного функционирования комплекса на сервере необходимо произвести:

- настройку межсетевого экрана;
- установку прокси сервера;
- установку почтового сервера» [16].

Защиты сегментов локальной сети и отдельных хостов от несанкционированного доступа через уязвимые места в протоколах и программном обеспечении в настоящее время используется антивирусный комплекс Kaspersky Internet Security Multi-Device, выполняющий функции антивирусной защиты и межсетевого экрана. Это устройство уже контролирует входящий и исходящий сетевой трафик, но требуется его дальнейшая настройка [25].

Для реализации угрозы несанкционированного доступа к автоматизированным рабочим местам (АРМ) сотрудников «нарушителем могут быть использованы следующие уязвимости:

- отсутствие регламента доступа к АРМ;
- отсутствие пломбирования корпуса АРМ;
- отсутствие авторизации на аппаратном уровне;
- наличие программного обеспечения, которое может создать условия для НСД» [13];
- наличие вредоносного программного обеспечения в системе;
- нарушение пропускного режима.

Исключение нерегламентированного доступа к АРМ решается внедрением в практику работы сотрудников соответствующих пунктов Положения. Также следует разработать матрицу доступа, в которой представлен список сотрудников, имеющих доступ к информации, содержащей конфиденциальные сведения, с указанием этих прав. Для контроля выполнения этого мероприятия должно быть назначено ответственное лицо.

Опломбирование корпусов персональных компьютеров, на которых ведется обработка информации, содержащей коммерческую и конфиденциальную информацию, или установлены средства криптографической защиты информации следует выполнить в соответствии с рекомендациями приказа ФАПСИ от 13 июня 2001 г. N 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну» [5]. Для пломбирования целесообразно приобрести одноразовые пломбы – наклейки с серийным номером.

Установка аппаратной авторизации на рабочие компьютеры сотрудников является ресурсозатратным и дорогим мероприятием.

Вероятность возникновения данной уязвимости в Управлении государственной экспертизы Ленинградской области оценивается как маловероятная, поэтому ей решено пренебречь и принять вытекающие риски с последующей ликвидацией последствий в случае их возникновения.

Для определения, какое аппаратно-программное средство будет оптимальным для внедрения в организации, рассмотрим и сравним несколько программных продуктов данного класса. На рынке представлено большое количество программ, предлагающих сходные функции. Рассмотрим сравнение наиболее популярных средств защиты по цене (автономный вариант, цена за 1 рабочее место) представлено на диаграмме (рисунок 22).

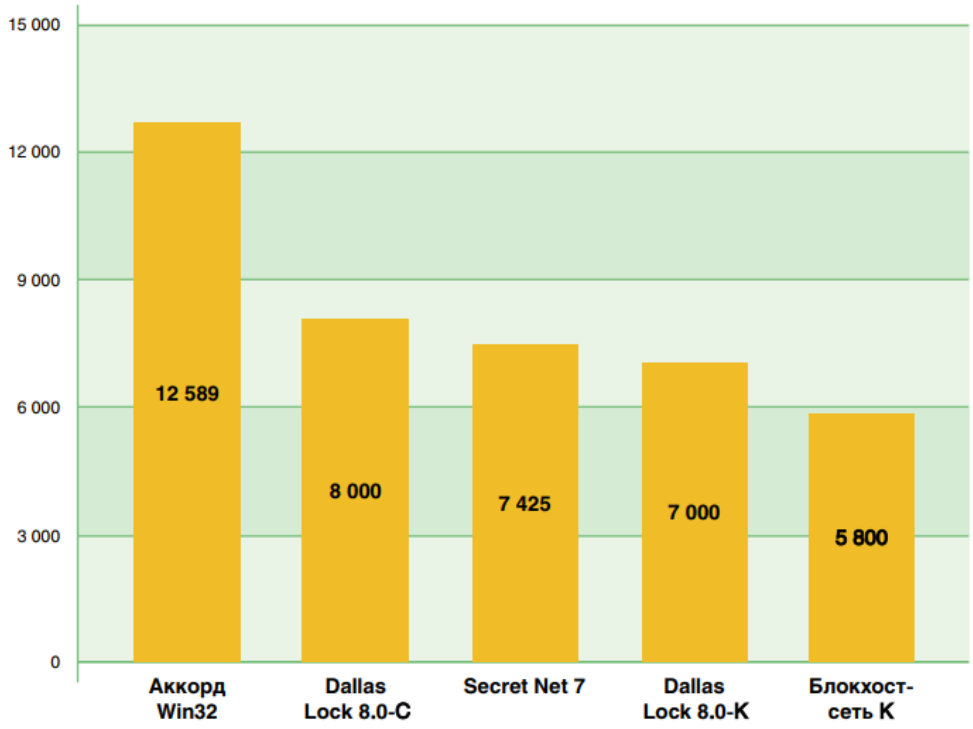

Рисунок 22 – Сравнение по цене

Дальнейший выбор средств информационной защиты происходил между Secret Net Studio, Dallas Lock 8 и Аккорд – Win32/ Win64 (ПАК) на основании сравнения функциональных возможностей. Результаты сравнения представлены в таблице 4.

Таблица 4 – Сравнение средств защиты информации по функциональности

Функция	Secret Net Studio	Dallas Lock 8	Аккорд
Сертификат ФСТЭК России	3СВТ, 2НДВ, защита АС до 1Б	5СВТ, 4НДВ, защита АС до 1Г (3СВТ, 2НДВ, защита АС до 1Б)	3СВТ, 2НДВ, защита АС до 1Б
Другие сертификаты	Минобороны России: 3НСД, 2НДВ	-	-
Варианты установки	Автономный, сетевой	Автономный, сетевой	Автономный, сетевой
Windows	+	+	+
База данных	MS SQL или Oracle	Встроенная	Встроенная
Возможность централизованной установки на рабочие станции	+	+	-
Идентификация и аутентификация пользователей при входе в систему	+	+	+
Возможность блокировки сессии пользователя по периоду неактивности	+	-	+
Возможность восстановления объектов при нарушении целостности	+	+	-
Блокировка запуска при нарушении целостности контролируемых модулей	+	-	-
Контроль доступа к физическим дискам	+	+	+
Контроль появления новых сетевых интерфейсов	+	-	-
Возможность ограничения категорий конфиденциальности документов, выводимых на принтер	+	-	-
Контроль вывода конфиденциальной информации на внешние носители	+	-	+

Продолжение таблицы 4

Функция	Secret Net Studio	Dallas Lock 8	Аккорд
Локальное оповещение пользователя о событиях НСД	+	+	+
Централизованное управление СЗИ	+	+	+
Возможность управления политиками на уровне организационных подразделений	+	+	-
Экспорт/импорт типовых настроек для ускорения развертывания			
Удаленный контроль состояния рабочей станции	+	+	+
Возможность автоматического оповещения о событии НСД по электронной почте	+	+	-
Получение отчета по всем настройкам СЗИ на рабочей станции	+	+	-
Централизованный сбор журналов СЗИ с рабочих станций	+	+	+
Автоматическое архивирование журналов	+	+	-

По совокупности характеристик в качестве одной из инженерно-технических мер предусмотрено внедрение программно-аппаратного средства – системы защиты информации от несанкционированного доступа «Secret Net Studio».

Для решения задачи обеспечения защиты от несанкционированного доступа к информации было выбрано аппаратно-программное средство Secret Net Studio.

«Система Secret Net Studio предназначена для обеспечения безопасности информационных систем на компьютерах, функционирующих под управлением операционных систем MS Windows 10/8/7 и Windows Server 2019/2016/2012/2008» [11].

«Средство Secret Net Studio представляет комплексное решение для обеспечения безопасности рабочих станций и серверов на уровне данных, приложений, сети, операционной системы и периферийного оборудования» [11].

Концепция продукта представлена на рисунке 23.

Рисунок 23 – Концепция Secret Net Studio

Secret Net Studio обеспечивает практически все виды защит информации от различных угроз.

«Система Secret Net Studio реализует следующие основные функции:

а) контроль входа пользователей в систему (идентификация и аутентификация пользователей);

б) дискреционное разграничение доступа к файловым ресурсам, устройствам, принтерам;

в) мандатное (полномочное) разграничение доступа к файловым ресурсам, устройствам, принтерам, сетевым интерфейсам, включая:

1) контроль потоков конфиденциальной информации в системе;

2) контроль вывода информации на съемные носители;

г) контроль состояния устройств компьютера с возможностями:

3) блокирования компьютера при изменении состояния заданных устройств;

4) блокирования подключения запрещенного устройства (устройства из запрещенной группы).

д) теневое копирование информации, выводимой на внешние носители и на печать;

е) автоматическая маркировка документов, выводимых на печать;

ж) контроль целостности файловых объектов и реестра;

з) создание замкнутой программной среды для пользователей (контроль запуска исполняемых модулей, загрузки динамических библиотек, исполнения скриптов по технологии Active Scripts);

и) очистка оперативной и внешней памяти при ее перераспределении;

к) изоляция процессов (выполняемых программ) в оперативной памяти;

л) защита содержимого локальных жестких дисков при несанкционированной загрузке операционной системы;

м) создание доверенной среды (внешний по отношению к ОС контроль работы ОС и системы защиты, установленных на компьютере);

н) антивирусная защита компьютеров;

о) обнаружение вторжений;

п) межсетевое экранирование сетевого трафика;

р) авторизация сетевых соединений;

с) управление ПАК «Соболь» (управление пользователями, контролем целостности, получение событий безопасности).

т) функциональный контроль ключевых защитных подсистем;

у) самозащита от несанкционированных воздействий на ключевые защитные подсистемы;

ф) регистрация событий безопасности;

х) централизованное и локальное управление параметрами работы механизмов защиты;

ц) централизованное и локальное управление параметрами работы пользователей;

ч) мониторинг и оперативное управление защищаемыми компьютерами;

ш) централизованный сбор, хранение и архивирование журналов» [11].

Средство защиты информации Secret Net Studio обеспечивает комплексную защиту на пяти уровнях (рисунок 24).

Рисунок 24 – Пять уровней защиты информации

На уровне данных обеспечивается:

– шифрование данных в контейнерах;
– хранение ключей;
– автоматическое подключение;
– настраиваемые права доступа;
– резервное копирование;
– копирование на съемные носители;

– хранение копий в защищенном хранилище;
– контроль заполнения хранилища;
– маркировка при выводе на печать;
– маркеры по уровням конфиденциальности.

На уровне приложений обеспечивается:

– список разрешенных приложений;
– контроль целостности;
– автопостроение зависимостей приложений;
– контроль скриптов Active Script.

На уровне сети обеспечивается:

– фильтрация сетевого трафика;
– реакции на срабатывание правила;
– время действия правил;
– режим обучения;
– шаблоны для различных сетевых служб;
– правила для отдельных пользователей и групп;
– создание программных VLAN;
– сокрытие сетевого трафика;
– эвристический анализ;
– сигнатурный анализ;
– временная блокировка атакующих хостов;
– команда оперативного снятия блокировки.

На уровне операционной системы обеспечивается:

– двухфакторная аутентификация;
– усиленная парольная аутентификация;
– политики блокировки сеанса;
– работа с локальными и доменными учетными записями пользователей;
– гибкие настройки ограничения доступа;

– контроль файлов, директорий и реестра;
– настройка времени контроля;
– два антивирусных модуля на выбор;
– сигнатурные и эвристические методы контроля;
– выбор профилей сканирования;
– локальные серверы обновлений;
– работа в любой файловой системе;
– унифицированный интерфейс настройки;
– управление доступом к устройствам и принтерам;
– контроль потоков;
– автоматическое затирание;
– затирание по требованию;
– централизованный сбор и хранение паспортов.

На уровне периферийного оборудования обеспечивается:

– четыре уровня настроек;
– иерархическое наследование настроек;
– дискреционное и полномочное управление доступом;
– контроль подключений и отключений устройств;
– настройка отдельных принтеров;
– поддержка виртуальных принтеров;
– ограничение печати документов;
– сквозная аутентификация;
– единое управление;
– получение журналов из ПАК «Соболь».

При установке системы на персональных компьютерах устанавливаются следующие компоненты:

– клиент;
– сервер безопасности;
– центр управления.

«Клиент системы Secret Net Studio предназначен для реализации защиты компьютера, на котором установлен данный компонент. Защита реализуется путем применения защитных механизмов, расширяющих и дополняющих средства безопасности ОС Windows.

Сервер безопасности реализует возможности централизованного управления клиентами в сетевом режиме функционирования.

Программа управления используется для централизованного управления серверами безопасности и клиентами в сетевом режиме функционирования. Она обеспечивает:

- управление параметрами объектов;
- отображение информации о состоянии защищаемых компьютеров и произошедших событиях тревоги;
- загрузку журналов событий;
- оперативное управление компьютерами» [17].

Система обеспечивает два режима работы:

- автономный режим – только клиент;
- сетевой режим – клиент + сервер безопасности + центр управления.

Сетевой режим предполагает централизованное развертывание и обеспечивает централизованное управление и централизованный мониторинг.

Для установки программы управления на компьютере должно быть установлено следующее программное обеспечение: Internet Explorer версии 8 или выше. Программа установки также проверяет и при необходимости устанавливает в автоматическом режиме пакет Microsoft .NET Framework 4.5.

Компоненты системы Secret Net Studio можно устанавливать при работе на компьютере локально или в терминальных сессиях.

Кроме того, установка клиента в сетевом режиме функционирования может выполняться централизованно под управлением сервера безопасности.

Обобщенная структурная схема клиента представлена на рисунке 25.

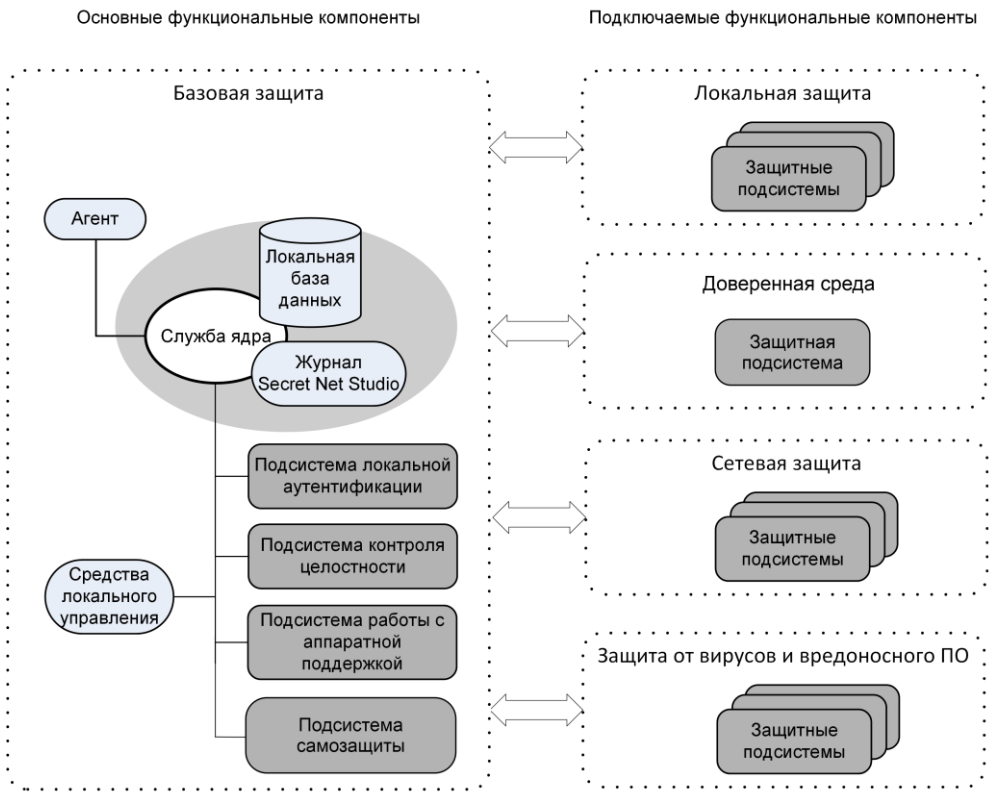

Рисунок 25 – Обобщенная структурная схема клиента

«Сетевая структура системы Secret Net Studio строится по принципу подчинения защищаемых компьютеров сети серверу безопасности. Для подчинения серверу безопасности компьютер должен быть в составе домена безопасности.

В рамках леса доменов можно организовать функционирование нескольких серверов безопасности с подчинением по иерархическому принципу. При этом иерархия подчинения серверов не обязательно должна соответствовать структуре доменов в лесу.

Каждый сервер контролирует работу своей группы защищаемых компьютеров и имеет свою базу данных. При этом некоторые операции доступны и в отношении объектов, относящихся к подчиненным серверам» [19].

На рисунке 26 представлен пример использования нескольких серверов.

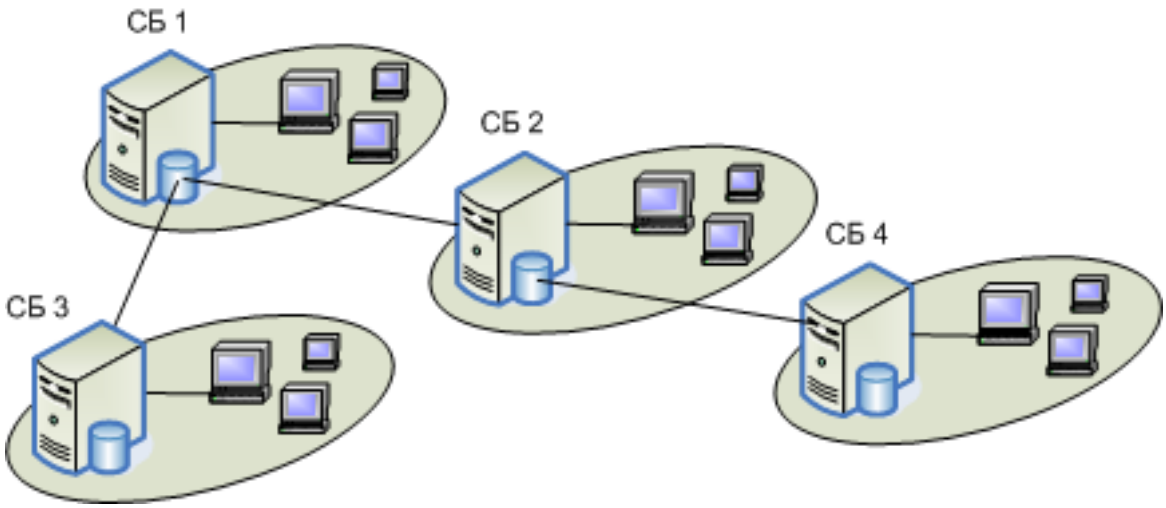

Рисунок 26 – Пример сетевой структуры Secret Net Studio

Централизованная установка программного обеспечения клиента под управлением сервера безопасности реализуется с помощью программы управления. В программе управления осуществляется формирование списка устанавливаемого программного обеспечения и заданий развертывания.

На клиентских компьютерах установка ПО выполняется автоматически в фоновом режиме. Пользователь оповещается о начале и завершении процесса установки. По окончании процесса пользователю предлагается перезагрузить компьютер [12].

Использование программно-аппаратного комплекса Secret Net Studio позволяет комплексно решить все ключевые задачи, связанные с управлением доступом и учетными данными пользователей.

Помимо обозначенных задач внедрение ПАК Secret Net Studio позволит решить и следующие поставленные задачи:

- упорядочение политики паролей в организации.
- упорядочение прав доступа сотрудников, в том числе удаленного, к конфиденциальной информации.
- оптимизация использования антивирусных программ на АРМ.

Как одна из задач формирования комплексной системы защиты информации организации поставлена задача монтажа видеонаблюдения в

офисных помещениях компании. Общий вход в офисный центр оборудован видеокамерами, но в офисных помещениях видеонаблюдение отсутствует. Для решения задачи обеспечения комплексной системы защиты информации в Управлении государственной экспертизы Ленинградской области необходимо обеспечить видеонаблюдение в офисных помещениях компании.

Выбор видеокамер выполнен на основе различных желательных характеристик: камера должна обеспечивать максимальный обзор офисного помещения, обеспечивать стандартное разрешение изображения, иметь возможность съемки в темноте (ИК-съемка), быть устойчивой к внешним воздействиям (антивандальный корпус) и доступной по цене. Камера должна иметь возможность удаленной передачи данных на смартфон.

В результате анализа характеристик различных вариантов камер для установки в офисных помещениях была выбрана купольная камера Uniview 3F22P-RB28.

Основные характеристики камеры:

- разрешение: 1920×1080;
- матрица: 2 МП;
- объектив: 2,8 мм;
- угол обзора: 112°;
- ИК-съемка в темноте: 30 м;
- поддержка MicroSD: до 128 Гб.

Камера поддерживает удаленный просмотр через приложение для смартфона (планшета), имеется функция отправки тревожных уведомлений при обнаружении движения в объективах камер. Возможен вывод изображения на любой современный экран.

Примерный план установки видеокамер для одного крыла представлен на рисунке 27.

В компании требуется установить всего 27 видеокамер, в том числе в представленном крыле 8:

– камеры № 1 и № 2 установлены в начале и в конце коридора, в который выходят все двери офисных помещений, в поле их обзора попадают все люди, входящие в офисы;
– камеры № 3 – № 8 установлены в офисных помещениях и в серверной таким образом, что фиксируют всех входящих в эти помещения людей и сотрудников, работающих за компьютерами

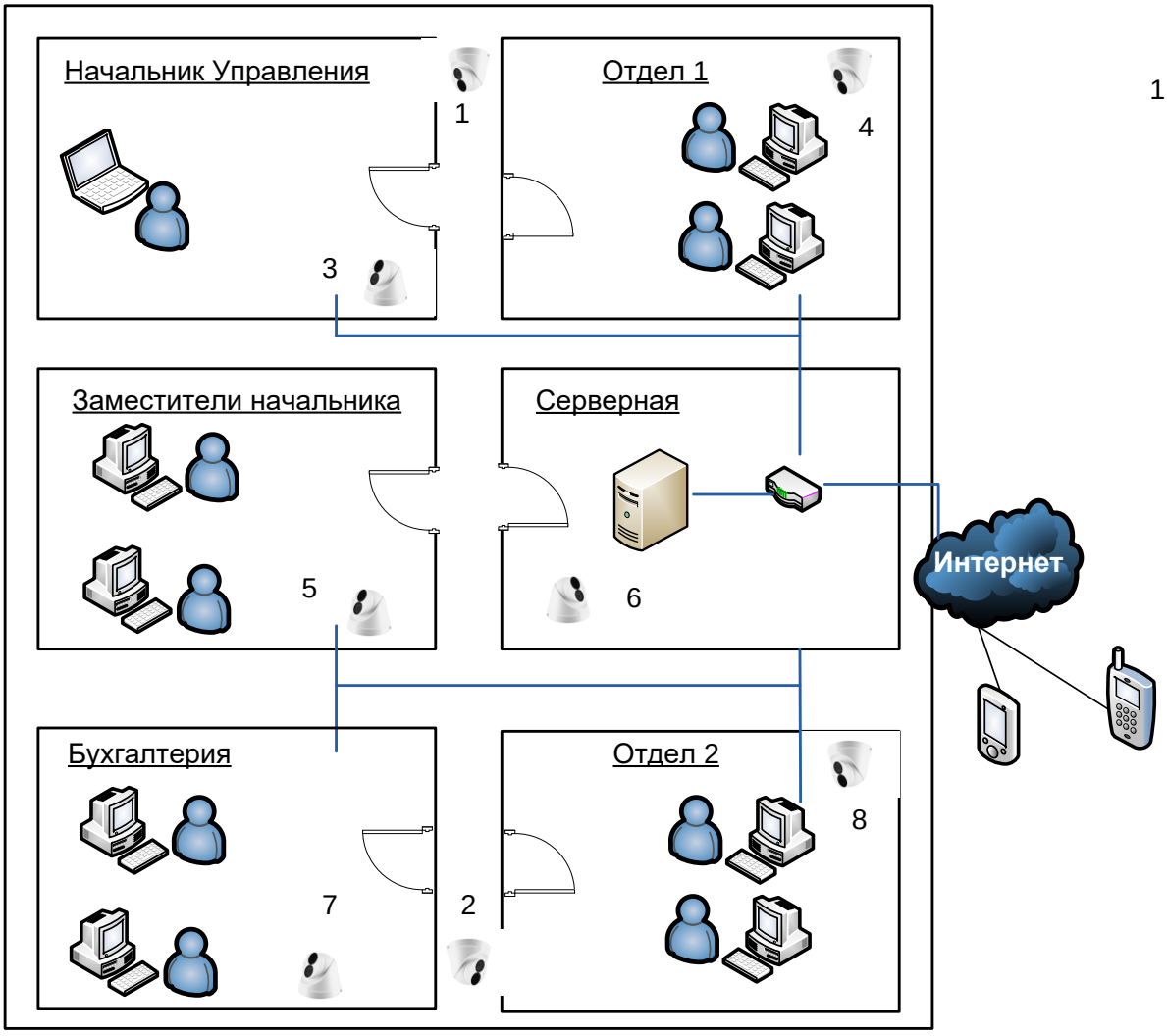

Рисунок 27 – Общий принцип установки видеокамер

Ансамблю установленных в помещениях видеокамер позволяет зафиксировать лица всех входящих из коридора людей, а также тех, кто

работает в офисных помещениях. Видеоданные с камер выводятся на монитор в серверной и записываются на специальный носитель информации с периодичностью перезаписи 14 дней.

Рассмотрим проект внедрения системы информационной безопасности организации. Проект разработан в программе MS Project и представлен на рисунке 28.

	Название задачи	Длительность	Начало	Окончание	Предшественники
1	**Разработка системы информационной безопасности**	**25 дней?**	**Ср 15.06.22**	**Вт 19.07.22**	
2	**Подготовка к реализации проекта**	**5 дней?**	**Ср 15.06.22**	**Вт 21.06.22**	
3	Формирование проектной группы	2 дней	Ср 15.06.22	Чт 16.06.22	
4	Планирование проекта	2 дней	Пт 17.06.22	Пн 20.06.22	3
5	Согласование плана с администрацие	1 день?	Вт 21.06.22	Вт 21.06.22	4
6	**Разработка мер по обеспечению ИБ**	**7 дней**	**Ср 22.06.22**	**Чт 30.06.22**	
7	Разработка нормативных регламентов и документов	7 дней	Ср 22.06.22	Чт 30.06.22	5
8	**Реализация инженерно-технических м**	**10 дней?**	**Ср 22.06.22**	**Вт 05.07.22**	**5**
9	Закупка материалов и оборудования	1 день?	Ср 22.06.22	Ср 22.06.22	
10	Монтаж видеокамер	3 дней	Чт 23.06.22	Пн 27.06.22	9
11	Проверка установленного оборудования	1 день?	Вт 28.06.22	Вт 28.06.22	10
12	Установка программного обеспечения (Kaspersky Internet Security	2 дней	Ср 29.06.22	Чт 30.06.22	11
13	Настройка межсетевого экрана	3 дней	Пт 01.07.22	Вт 05.07.22	12
14	**Реализация аппаратно-программного комплекса мер по обеспечению ИБ**	**6 дней?**	**Ср 06.07.22**	**Ср 13.07.22**	**13**
15	Приобретение лицензии Secret Net Stuc	1 день?	Ср 06.07.22	Ср 06.07.22	
16	Установка Secret Net Studio для сетев	3 дней	Чт 07.07.22	Пн 11.07.22	15
17	Тестирование АПК	2 дней	Вт 12.07.22	Ср 13.07.22	16
18	**Обучение персонала**	**3 дней?**	**Чт 14.07.22**	**Пн 18.07.22**	**17**
19	Проведение занятий с сотрудниками	2 дней	Чт 14.07.22	Пт 15.07.22	
20	Проверка результатов обучения	1 день?	Пн 18.07.22	Пн 18.07.22	19
21	Начало эксплуатации в штатном режиме	1 день?	Вт 19.07.22	Вт 19.07.22	20
22	Сопровождение системы	5 дней	Ср 15.06.22	Вт 21.06.22	

Рисунок 28 – Проект внедрения системы информационной безопасности

На реализацию проекта потребуется 30 рабочих дней с учетом параллельного выполнения отдельных видов работ. С учетом непредвиденных ситуаций, реализации рисков и возможных отклонений от графика следует при планировании заложить на проект 40 рабочих дней.

На рисунке 29 представлена диаграмма Ганта проекта. Красным цветом на диаграмме отмечен критический путь.

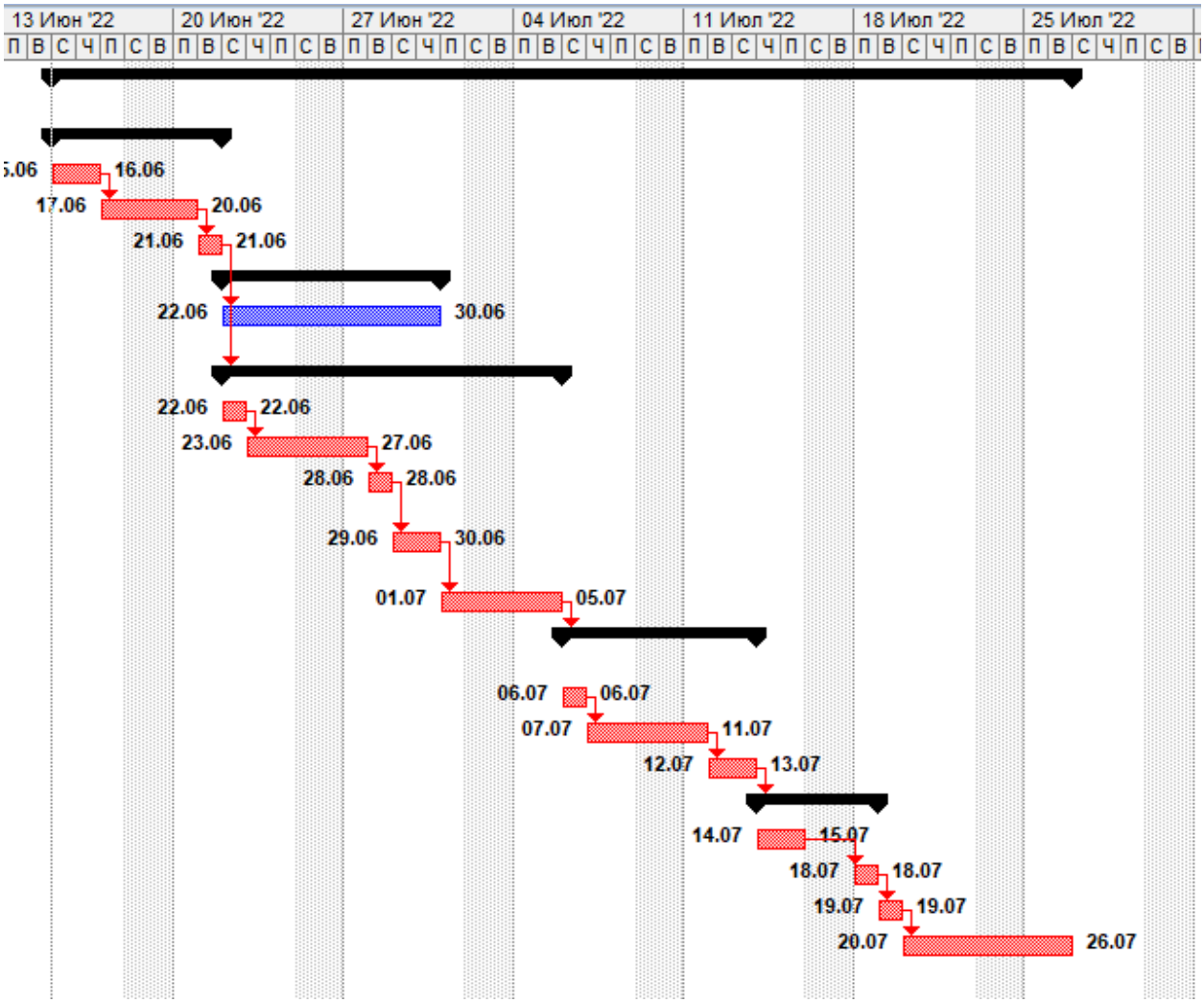

Рисунок 29 – Диаграмма Ганта

Диаграмма Ганта показывает, что практически все работы за исключением одной лежат на критическом пути. Это свидетельствует о том, что в проекте практически нет запасов времени между работами, поэтому предложение о выделении дополнительного времени выглядит разумным.

3.3 Экономический эффект от внедрения проекта

Оценим экономический эффект от внедрения проекта.

Проектирование и разворачивание комплексной системы защиты информации для любой организации предполагает, что будут задействованы значительные ресурсы – финансы (покупка аппаратного и программного

обеспечения, системы видеонаблюдения; оплата работы специалистов по монтажу и настройке), рабочее время сотрудников (разработка и внедрение новых правил работы, обучение персонала). Поэтому важно соблюсти баланс между возможным ущербом от нарушений защищенности информации и расходами на обеспечение ее защиты. Если расходы превысят ущерб, то систему нельзя будет признать экономически эффективной.

С одной стороны, любое предприятие старается минимизировать объем средств, выделяемых на то или иное мероприятие, с другой – выделенных средств должно быть достаточно на достижение запланированного эффекта. Оптимальной будет ситуация, при которой общая стоимость средств, выделенных Управлением государственной экспертизы Ленинградской области на защиту информации будет минимальна при гарантии выполнения задач, поставленных в процессе проектирования комплексной системы защиты информации.

Экономическая эффективность мероприятий по защите информации может быть определена через объем предотвращенного ущерба или величину снижения риска для информационных активов организации.

Для нахождения экономической эффективности защиты информации организации необходимо получить значения следующих показателей:

- ресурсы, запланированные на формирование и/или изменение спроектированной системы защиты информации и содержание ее в рабочем состоянии;
- величины потерь (рисков), вызванных угрозами информационным активам после внедрения/модернизации системы защиты информации.

Данные о содержании и объеме разового ресурса, выделяемого на защиту информации в Управления государственной экспертизы Ленинградской области, представлены в таблице 5.

Таблица 5 – Содержание и объем разового ресурса, выделяемого на защиту информации

Организационные мероприятия			
Выполняемые действия	Среднечасовая зарплата специалиста (руб.)	Трудоемкость операции (чел. час)	Стоимость всего (тыс. руб.)
Разработка локальных нормативных актов	180	12	2,16
Обучение персонала	180	10	1,8
Доставка технических средств	200	10	2,0
Установка технических средств	220	80	17,6
Стоимость проведения организационных мероприятий, всего			23,56
Мероприятия инженерно-технической защиты			
Номенклатура ПиАСИБ, расходных материалов	Стоимость единицы (тыс. руб.)	Кол-во (ед. измерения)	Стоимость всего (тыс. руб.)
Камеры видеонаблюдения	3,04	8	24,32
Система архивирования записей видеонаблюдения	7,2	1	7,2
Кабель коаксиальный	0,03	500	15,0
Лицензия на Secret Net Studio	8,019	24	192,456
Сейф для хранения конфиденциальных документов	10,49	2	20,98
Стоимость проведения мероприятий инженерно-технической защиты			259,956
Объем разового ресурса, выделяемого на защиту информации			283,516

Содержание и объем постоянного ресурса, выделяемого на защиту информации в Управления государственной экспертизы Ленинградской области», представлены в таблице 6.

Таблица 6 – Содержание и объем постоянного ресурса, выделяемого на защиту информации в Управлении

Организационные мероприятия			
Выполняемые действия	Среднечасовая зарплата специалиста (руб.)	Трудоемкость операции (чел. час)	Стоимость всего (тыс. руб.)
Инструктажи и тренинги персонала	180	20	3,6
Стоимость проведения организационных мероприятий, всего			3,6

Продолжение таблицы 6

Мероприятия инженерно-технической защиты			
Выполняемые действия	Среднечасовая зарплата специалиста (руб.)	Трудоемкость операции (чел. час)	Стоимость всего (тыс. руб.)
Номенклатура ПиАСИБ, расходных материалов	Стоимость единицы (тыс. руб.)	Кол-во (ед. измерения)	Стоимость всего (тыс. руб.)
Обслуживание камер видеонаблюдения	1	8	8,0
Обновление лицензий Secret Net Studio	0,5	24	12,0
Обслуживание ПО	10	1	10,0
Стоимость проведения мероприятий инженерно-технической защиты			30,0
Объем разового ресурса, выделяемого на защиту информации			33,6

Проведенные вычисления показали, что внедрение разработанного проекта системы информационной безопасности потребует вложения 283 516 руб., а ее поддержка – ежегодных расходов в размере 33 600 руб.

Для определения эффективности разработанной системы информационной безопасности требуется рассмотреть прогнозную информацию о величине потерь (рисков) для критичных информационных ресурсов после ее внедрения. Данные, полученные на основе опроса экспертов, представлены в таблице 7.

Таблица 7 –Величины потерь (рисков) для критичных информационных ресурсов Управления после внедрения системы защиты информации

Актив	Угроза	Величина потерь (тыс. руб.)
Технология экспертизы (документация, связанная с технологическими процессами)	Утеря конфиденциальности	50
Технология экспертизы (документация, связанная с технологическими процессами)	Утеря целостности	100
Технология экспертизы (документация, связанная с технологическими процессами)	Утеря доступности	2

Продолжение таблицы 7

Актив	Угроза	Величина потерь (тыс. руб.)
Бухгалтерская и налоговая отчетность	Утеря конфиденциальности	5
Бухгалтерская и налоговая отчетность	Утеря целостности	10
Бухгалтерская и налоговая отчетность	Утеря доступности	4
Персональные данные клиентов	Утеря конфиденциальности	20
Персональные данные клиентов	Утеря целостности	2
Персональные данные клиентов	Утеря доступности	2
Персональные данные сотрудников	Утеря конфиденциальности	10
Персональные данные сотрудников	Утеря целостности	1
Персональные данные сотрудников	Утеря доступности	1
Внутренняя переписка	Утеря конфиденциальности	20
Внутренняя переписка	Утеря целостности	2
Внутренняя переписка	Утеря доступности	2
Цены на услуги	Утеря конфиденциальности	0
Цены на услуги	Утеря целостности	5
Цены на услуги	Утеря доступности	1
Системное программное обеспечение	Утеря конфиденциальности	0
Системное программное обеспечение	Утеря целостности	5
Системное программное обеспечение	Утеря доступности	3
Прикладное программное обеспечение	Утеря конфиденциальности	0
Прикладное программное обеспечение	Утеря целостности	5
Прикладное программное обеспечение	Утеря доступности	3
	Суммарная величина потерь	***253***

Затраты на внедрение системы информационной безопасности существенно ниже, чем возможные потери в случае реализации угроз.

Определим срок окупаемости системы Ток по формуле:

$$T_{ок} = \frac{R_{\sum}}{R_{ср} - R_{прогн}}, \qquad (5)$$

$$T_{ок} = \frac{317116}{253000 - 25300} = 1,4$$

Срок окупаемости проекта составит 1,4 года, то есть приблизительно один год и 5 месяцев, что приемлемо для организации масштабов исследуемой организации. Представим динамику величин потерь за период 2 года (рисунки 30 и 31). Экономические расчеты показали эффективность внедрения комплекса информационной защиты.

	1 кв.	2 кв.	3 кв.	1 год	1 кв.	2 кв.	3 кв.	2 год
До внедрения СЗИ	580	1160	1740	2320	2900	3480	4060	4640
После внедрения СЗИ	58	116	174	232	290	348	406	464
Снижение потерь	522	1044	1566	2088	2610	3132	3654	4176

Рисунок 30 –Величины потерь за период 2 года

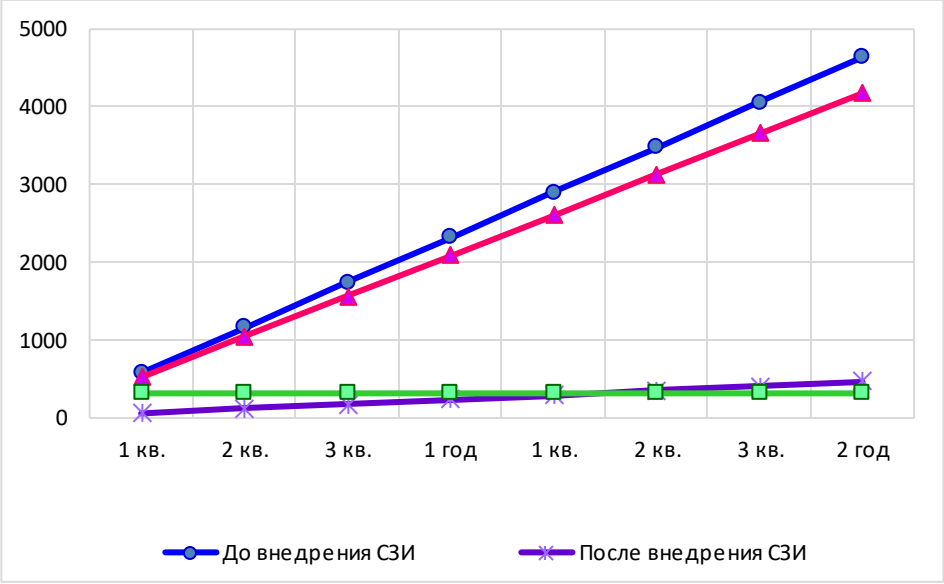

Рисунок 31 – Графическое определение срока окупаемости

Согласно проведенным исследованиям для Управления государственной экспертизы Ленинградской области внедрение разработанной системы является оптимальным вариантом технически и эффективным экономически.

Выводы по главе 3

В третьей главе представлены предложения по разворачиванию в Управлении государственной экспертизы Ленинградской области комплексной системы обеспечения информационной безопасности и защиты информации, так как имеющаяся система устарела и неэффективно для защиты от современных угроз. Представленное предложение содержит меры организационного характера (разработку нормативно–правовой базы) и внедрение аппаратно-программных мер соответствующей направленности, а также инженерно–технические решения (например, установка видеокамер в офисных помещениях и в коридорах для охвата всего периметра, расстановка периферийных устройств таким образом, чтобы они полностью находились в поле обзора камеры).

Расчет экономической выгоды комплекса мер на основе объема предотвращенного ущерба показал, что проект экономически оправдан.

Заключение

В процессе выполнения выпускной квалификационной работы была разработана комплексная система защиты информации Управления государственной экспертизы Ленинградской области.

В рамках выпускной квалификационной работы была разработана комплексная система защиты информации для Управления государственной экспертизы Ленинградской области. Процесс разработки был реализован в несколько этапов:

- выявление недостатков действующей информационной защиты организации;
- определение типов угроз, которые могут возникнуть в результате уязвимостей и недостатков в системе защиты информационных систем организации;
- предложение комплекса мер по формированию системы безопасности, предотвращающей возможность несанкционированного доступа к конфиденциальной информации и ее неправомерного использования, а также минимизирующей урон от реализации информационных угроз.

На основании проведенного системного анализа был разработан и предложен для внедрения Управления государственной экспертизы Ленинградской области комплекс организационных мер, инженерно-технических методов и средств, позволяющий обеспечить комплексную защиту данных на предприятии.

Оценка эффективности разработанной комплексной системы защиты информации в Управления государственной экспертизы Ленинградской области показала целесообразность их внедрения на предприятии. В выпускной квалификационной работе дано экономическое обоснование эффективности и окупаемости представленного проекта.

Список используемой литературы и используемых источников

1. Астахов А..М. Искусство управления информационными рисками. – М.: ДМК Пресс, 2018. – 312 с.
2. ГОСТ Р 56546-2015 «Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем». – Электронный фонд правовых и нормативно-технических документов. – URL: https://docs.cntd.ru/document/1200123702 (дата обращения 11.05.2022). – Текст: электронный.
3. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности. – Электронный фонд правовых и нормативно-технических документов. – URL: https://docs.cntd.ru/document/1200123702 (дата обращения 14.04.2022). – Текст: электронный.
4. ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. – База ГОСТов. – URL: https://allgosts.ru/35/040/gost_r_iso!mek_27005-2010 (дата обращения 11.03.2022). – Текст: электронный.
5. Доктрина информационной безопасности Российской Федерации. – Совет безопасности Российской Федерации. Официальный сайт – URL: http://www.scrf.gov.ru/security/information/document5/ (дата обращения 29.05.2022). – Текст: электронный.
6. Дурницын, И. Развитие права в сфере информационной безопасности. – Информационно-правовой портал Гарант.ру – URL: https://www.garant.ru/ia/opinion/author/durnicyn/1420282/ (дата обращения 29.05.2022). – Текст: электронный.
7. Методы организации защиты информации: учебное пособие / Ю. Ю. Громов и др. – Тамбов: Изд-во ФГБОУ ВПО «ТГТУ», 2013. – 80 с.

8. ОК 029–2014. Общероссийский классификатор видов экономической деятельности. – Правовой портал Консультатн-Плюс. – URL: http://www.consultant.ru/document/cons_doc_LAW_163320/ (дата обращения 15.03.2022). – Текст: электронный.

9. Официальный сайт единой информационной системы в сфере закупок в информационно-телекоммуникационной сети Интернет. – URL: https://zakupki.gov.ru/epz/main/public/home.html (дата обращения 15.03.2022). – Текст: электронный.

10. Официальный сайт Управления государственной экспертизы Ленинградской области [Электронный ресурс]. – Режим доступа: http://www.loexp.ru/inf/ob_uchrezhdenii/istoriya/ (дата обращения 15.03.2022)..

11. Приказ ФАПСИ от 13 июня 2001 г. N 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну» – Информационно-правовой портал Гарант – URL: https://base.garant.ru/183628/ (дата обращения 05.06.2022). – Текст: электронный.

12. Средство защиты информации Secret Net Studio. Руководство администратора. Принципы построения. – Компания «Код Безопасности», 2019. – 67 с.

13. Средство защиты информации Secret Net Studio. Установка, обновление и удаление. – Компания «Код Безопасности», 2019. – 45 с.

14. Уголовное судопроизводство. Данные о назначенном наказании по статьям УК. – Портал «Судебная статистика РФ». – URL: http://stat.xn---7sbqk8achja.xn--p1ai/stats/ug/t/14/s/17 (дата обращения 01.02.2022). – Текст: электронный.

15. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (действующая редакция). – Информационно-правовой портал

КонсультантПлюс – URL: http://www.consultant.ru/ (дата обращения 31.04.2022). – Текст: электронный.

16. Федеральный Закон «О персональных данных» от 27 июля 2006 года № 152 (действующая редакция).

17. Федеральный закон от 29.07.2004 N 98-ФЗ (ред. от 09.03.2021) «О коммерческой тайне». – Доступ из информационно-правовой системы «КонсультантПлюс». – URL: http://www.consultant.ru/ (дата обращения 07.05.2022). – Текст: электронный.

18. Федеральный закон от 29.07.2004 N 98-ФЗ (ред. от 09.03.2021) «О коммерческой тайне» [Электронный ресурс]. – Доступ из информационно-правовой системы «КонсультантПлюс»: http://www.consultant.ru/ (дата обращения 07.05.2022).

19. Ясенев В.Н., Дорожкин А.В. Информационная безопасность: Учебное пособие. / под общей редакцией проф. Ясенева В.Н. – Нижний Новгород: Нижегородский госуниверситет им. Н.И. Лобачевского, 2017. – 198 с.

20. TAdviser. Государство. Бизнес. ИТ. – Портал об информационных технологиях в госуправлении и бизнесе. – URL: https://www.tadviser.ru/ (дата обращения 10.04.2022). – Текст: электронный.

21. CompTIA Network+ Practice Tests: Exam N10-008, 2nd Edition.

22. Prakhar Prasad, Mastering Modern Web Penetration Testing. Packt Publishing Ltd, 2016.

23. METASPLOIT. David Kennedy, Jim O'Gorman, Devon Kearns, and Mati Aharoni. San Francisco, 2011.

24. B. B. Gupta. Cross-Site Scripting (XSS) attacks and defense mechanisms: classification and state-of-the-art. Int J Syst Assur Eng Manag, 2015.

25. Cybersecurity – Attack and Defense Strategies. Second Edition. Published by Packt Publishing Ltd., 2019.