НЕГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ ЧАСТНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ФИНАНСОВО-ПРОМЫШЛЕННЫЙ УНИВЕРСИТЕТ «СИНЕРГИЯ»

Институт Информационных технологий

Направление подготовки 09.03.02 Информационные системы и технологии
(шифр и наименование)

Департамент Цифровой экономики
(аббревиатура)

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

На тему:

Совершенствование системы защиты информации АО "ФИНТЕХ"

Обучающийся _____ _____
(ФИО полностью) (подпись)

Руководитель Стычук Алексей Александрович _____
(ФИО полностью) (подпись)

Директор Департамента _____ _____
(ФИО полностью) (подпись)

МОСКВА 2022 г.

Факультет электронного обучения

ЗАДАНИЕ

на выпускную квалификационную работу студента

(Ф.И.О. студента полностью)

1. Тема ВКР:
Совершенствование системы защиты информации АО "ФИНТЕХ"

2. Структура ВКР:

Введение

I Аналитическая часть

1.1. Технико-экономическая характеристика предметной области и предприятия (Установление границ рассмотрения).

1.1.1. Общая характеристика предметной области.

1.1.2. Организационно-функциональная структура предприятия.

1.2. Анализ рисков информационной безопасности

1.2.1 Идентификация и оценка информационных активов.

1.2.2. Оценка уязвимостей активов.

1.2.3. Оценка угроз активам.

1.2.4. Оценка существующих и планируемых средств защиты.

1.2.5. Оценка рисков.

1.3. Характеристика комплекса задач, задачи и обоснование необходимости совершенствования системы обеспечения информационной безопасности и защиты информации на предприятии

1.3.1. Выбор комплекса задач обеспечения информационной безопасности.

1.3.2. Определение места проектируемого комплекса задач в комплексе задач предприятия, детализация задач информационной безопасности и защиты информации.

1.4. Выбор защитных мер

1.4.1. Выбор организационных мер.

1.4.2. Выбор инженерно-технических мер.

II Проектная часть

2.1. Комплекс организационных мер обеспечения информационной безопасности и защиты информации предприятия.

2.1.1. Отечественная и международная нормативно-правовая основа создания системы обеспечения информационной безопасности и защиты информации предприятия.

2.1.2. Организационно-административная основа создания системы обеспечения информационной безопасности и защиты информации предприятия.

2.2. Комплекс проектируемых программно-аппаратных средств обеспечения информационной безопасности и защиты информации предприятия.

2.2.1 Структура программно-аппаратного комплекса информационной безопасности и защиты информации предприятия.

2.2.2. Контрольный пример реализации проекта и его описание.

III Обоснование экономической эффективности проекта

3.1 Выбор и обоснование методики расчёта экономической эффективности

3.2 Расчёт показателей экономической эффективности проекта

Заключение

Приложения

5. Основные вопросы, подлежащие разработке

В главе 1 необходимо представить обоснование актуальности выбора задачи обеспечения информационной безопасности, обосновать и изложить используемую стратегию действий по защите информационных ресурсов, результаты анализа предметной области, а также обоснование и результаты выбора административных и инженерно-технических мер.

В разделе 1.1. необходимо привести краткое описание компании и таблицу показателей ее деятельности, рисунок организационной структуры и его описание.

В разделе 1.2 следует провести анализ рисков информационной безопасности, для чего необходимо:

- идентифицировать информационные активы;
- ранжировать их по степени важности;
- определить активы, которые относятся к конфиденциальным;
- оценить уязвимость активов;
- оценить степень угроз выбранным информационным активам;
- дать характеристику действующей системе защиты информации на предприятии на предмет полноты и адекватности реагирования на угрозы информационной безопасности.
- провести обоснование выбора методики оценки рисков с последующим проведением оценки.

Требования по содержанию и форме представления информации (текстовая часть, таблицы, рисунки, схемы) изложены в соответствующем разделе Методических рекомендаций.

В разделе 1.3 необходимо кратко специфицировать комплекс задач, подлежащих дальнейшему решению. Необходимо отразить причину сделанного выбора и место задачи в комплексе задач.

В разделе 1.4 необходимо провести анализ и обоснование выбора:

- стратегии обеспечения информационной безопасности
- организационных и инженерно-технических мер обеспечения информационной безопасности;
- необходимых документов, регламентирующих проведение мероприятий по обеспечению информационной безопасности

В главе 2 необходимо представить проектные решения в соответствии с выбранным направлением обеспечения информационной безопасности.

В разделе 2.1 необходимо провести выбор нормативных актов отечественного и международного права, которые будут использоваться в качестве основы для разработки внутренних нормативных документов, а также разработать образцы документов в соответствии с выбранной темой.

Раздел 2.2 должен содержать описание внедряемых (разрабатываемых) программно-аппаратных средств информационной безопасности, а также описание контрольного примера применения выбранных средств информационной безопасности.

Требования по содержанию и форме представления информации (текстовая часть, таблицы, рисунки, схемы) изложены в соответствующем разделе Методических рекомендаций.

В главе 3 приводится методика расчета показателей экономической эффективности и расчеты, выполненные в соответствии с изложенной методикой. Расчетные данные следует представить в виде таблиц и диаграмм, отражающие сравнение величины ущерба до и после реализации мер по защите информации.

Приложение обязательно должно содержать формы внутренних нормативных документов. Кроме того, также могут быть приведены:

- схемы или таблицы из основной части выпускной квалификационной работы;
- результаты выполнения контрольного примера;
- схемы документооборота;
- примеры классификаторов;

- формы первичных и результатных документов;
- распечатки меню, экранных форм ввода, получаемых отчетов в разработанной системе;
- а также другие материалы выпускной квалификационной работы, кроме копий документов, не имеющих отношения к выпускной квалификационной работе, рекламных сообщений, скриншотов. В одном приложении нельзя размещать различные по смыслу таблицы или рисунки. Не допускается дублирование в приложении материала, размещенного в основной части выпускной квалификационной работе.

С детальным рассмотрением содержания каждого пункта, а также примерами схем и таблиц необходимо ознакомиться в «Методических указаниях по подготовке выпускной квалификационной работы для направления «Информационные системы и технологии», профиль «Информационная безопасность», размещенных на сайте МЕГАКАМПУСа в личном кабинете студента. При подготовке выпускной квалификационной работы вы можете пользоваться дополнительными литературными источниками, а также основной литературой, список которой приведен ниже.

3. Основные вопросы, подлежащие разработке.

Во введении рекомендуется обосновать актуальность выбранной темы, сформулировать цели и задачи работы, описать объект, предмет и информационную базу исследования.

В главе 1 необходимо представить обоснование актуальности выбора автоматизируемой задачи, проектных решений по информационному, программному и аппаратному обеспечению, дать ее развернутое описание, отразить взаимосвязь с другими задачами, изложить используемую стратегию автоматизации и способ приобретения информационной системы.

В разделе 1.1. необходимо привести краткое описание компании и таблицу показателей ее деятельности, рисунок организационной структуры и его описание, рисунки программной и технической архитектуры, а также их описание.

В разделе 1.2 следует обосновать актуальность выбора автоматизируемой задачи, для этого необходимо провести анализ организационной, программной и технической архитектуры с целью определения перечня задач, которые необходимо автоматизировать и выбора наиболее приоритетной из них. С целью определения информационных потоков выбранной задачи необходимо привести соответствующие IDEF диаграммы. Далее необходимо привести рисунок, отражающий документооборот автоматизируемой задачи, таблицу прагматических характеристик соответствующих документов (периодичность, время на обработку и так далее) и определить комплекс программно-аппаратных средств, обеспечивающих информационную безопасность и защиту информации в рамках решаемой задачи.

В разделе 1.3 необходимо провести анализ готовых программных решений автоматизируемой задачи (в виде сравнительной таблицы наиболее интересных решений), определить стратегию автоматизации и способ приобретения информационной системы.

В разделе 1.4 необходимо провести анализ и обосновать выбор средств, используемых для автоматизации задачи: технического обеспечения (компьютеры и периферия, сетевое оборудование, офисная техника, дополнительные устройства), программного обеспечения (операционная система, СУБД, среда разработки, другое прикладное ПО), информационного обеспечения (классификаторы, справочники, документы, информационные базы).

В главе 2 необходимо представить проектные решения в соответствии с выбранной моделью жизненного цикла: начиная с анализа рисков на всех этапах разработки системы и закачивая примером ее опытной эксплуатации.

В разделе 2.1 необходимо провести выбор стандарта и модели жизненного цикла, соответствующих автоматизируемой задаче, а также стратегии внедрения проектируемой информационной системы. После этого следует перечислить риски для каждого этапа выбранной модели жизненного цикла и определить пути их снижения, в том числе посредством разработки средств информационной безопасности и защиты информации проектируемой системы.

Раздел 2.2 отражает процесс проектирования информационного обеспечения задачи и должен содержать:

- рисунок информационной модели и ее описание;
- таблицу используемых систем кодирования и описание классификаторов;
- описание входных и оперативных документов, файлов и экранных форм;
- описание результатных документов, файлов и экранных форм;
- таблицы входных и результатных показателей, а также их описание.

Раздел 2.3 отражает процесс проектирования программного обеспечения задачи и должен содержать:

- рисунки дерева функций и сценария диалога, а также их описание;
- рисунок ER – модели (количество таблиц в ER модели должно быть равно количеству таблиц в информационной модели), описание структуры записей каждой таблицы;
- рисунок дерева вызова программных модулей, а также таблицу с перечнем и назначением модулей;
- блок-схема основного/расчетного модуля, описание блок-схем алгоритмов основных расчетных модулей.

В разделе 2.4 следует представить экранные формы, демонстрирующие работу системы (не менее 7) и их описание.

В главе 3 приводится методика расчета показателей экономической эффективности и расчеты, сделанные в соответствии с изложенной методикой. Расчетные данные следует представить в виде таблиц и диаграмм, отражающие сравнение базового и предлагаемого вариантов.

Приложение обязательно должно содержать фрагмент листинга программного кода (распечатка на исходном языке программирования отлаженных основных расчетных модулей - около 400 операторов языка высокого уровня или адаптированных программных средств, использованных в работе), также могут быть приведены:

- схемы или таблицы из основной части выпускной квалификационной работы;
- результаты выполнения контрольного примера;
- диаграммы потоков данных, демонстрирующих существующую технологию решения задач («КАК ЕСТЬ»);
- диаграммы потоков данных, демонстрирующих предлагаемую технологию решения задач («КАК ДОЛЖНО БЫТЬ»);
- схемы документооборота;
- примеры классификаторов;
- формы первичных и результатных документов;
- распечатки меню, экранных форм ввода, получаемых отчетов в разработанной системе;

- а также другие материалы выпускной квалификационной работы, кроме текстов договоров с клиентами и иных "шаблонных документов" (в тех случаях, когда для их существенных реквизитов проектируется форма, а по результатам ввода и сохранения в информационную базу имеется возможность распечатки документа "по шаблону").

В одном приложении нельзя размещать различные по смыслу таблицы или рисунки. Не допускается дублирование в приложении материала, размещенного в основной части выпускной квалификационной работы.

С детальным рассмотрением содержания каждого пункта, а также примерами схем и таблиц необходимо ознакомиться в «Методических указаниях по подготовке выпускной квалификационной работы» для направления «Информационные системы и технологии» профиль «Информационная безопасность», размещенных на сайте МЕГАКАМПУСа в личном кабинете студента. При подготовке выпускной квалификационной работы вы можете пользоваться дополнительными литературными источниками, а также основной литературой, список которой приведен ниже.

4. Исходные данные по ВКР:

Основная литература:

1. Доктрина информационной безопасности Российской Федерации – URL: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102161033
2. Федеральный закон РФ от от 27.07.2006 г. N 149-ФЗ Об информации, информационных технологиях и о защите информации – URL: http://pravo.gov.ru/proxy/ips/?docbody&nd=102108264
3. Н.Скабцов. Аудит безопасности информационных систем – СП-б.:Питер, 2018
4. А.Бирюков. Информационная безопасность. Защита и нападение – М.:ДМК Пресс, 2017
5. С.Нестеров. Информационная безопасность. Учебник и практикум – М.:Юрайт, 2017

Дополнительная литература:

6. Д.А.Мельников. Организация и обеспечение безопасности информационно-технологических сетей и систем. Учебник – М.:КДУ, 2015
7. Нестеров, С.А. Основы информационной безопасности : учебное пособие / С.А. Нестеров ; Министерство образования и науки Российской Федерации, Санкт-Петербургский государственный политехнический университет. - СПб. : Издательство Политехнического университета, 2014. - 322 с. : схем., табл., ил. - ISBN 978-5-7422-4331-1 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=363040(22.10.2017).
8. Аверченков, В.И. Аудит информационной безопасности : учебное пособие для вузов / В.И. Аверченков. - 3-е изд., стереотип. - М. : Флинта, 2016. - 269 с. - Библиогр. в кн. - ISBN 978-5-9765-1256-6 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=93245 (22.10.2017).

Руководитель ВКР: _____/ А.А. Стычук
подпись расшифровка

Студент задание получил: «01» июня 2026 г.

Студент: _____/
подпись расшифровка

СОДЕРЖАНИЕ

Введение……..…11
1. Аналитическая часть…….14
1.1 Технико-экономическая характеристика предметной области и предприятия……...14
1.1.1 Общая характеристика предметной области……...14
1.1.2 Организационно-функциональная структура предприятия……..….22
1.2 Анализ рисков информационной безопасности…….24
1.2.1 Идентификация и оценка информационных активов……..…24
1.2.2 Оценка уязвимостей активов……..……...27
1.2.3 Оценка угроз активам……...….31
1.2.4 Оценка существующих и планируемых средств защиты……...34
1.2.5 Оценка рисков…….37
1.3 Характеристика комплекса задач и обоснование необходимости совершенствования системы обеспечения информационной безопасности и защиты информации на предприятии……..44
1.3.1 Выбор комплекса задач обеспечения информационной безопасности……...…44
1.3.2 Определение места проектируемого комплекса задач в комплексе задач предприятия, детализация задач информационной безопасности и защиты информации……45
1.4 Выбор защитных мер……46
1.4.1 Выбор организационных мер……46
1.4.2 Выбор инженерно-технических мер……49
2. Разработка комплекса мер по обеспечению защиты информации……..53
2.1 Комплекс организационных мер обеспечения информационной безопасности и защиты информации предприятия……53
2.1.1 Нормативно-правовая основа создания системы обеспечения информационной безопасности и защиты информации предприятия…….53

2.1.2 Организационно-административная основа создания системы обеспечения информационной безопасности и защиты информации предприятия……...57

2.2 Комплекс проектируемых программно-аппаратных средств обеспечения информационной безопасности и защиты информации предприятия……...60

2.2.1 Структура программно-аппаратного комплекса информационной безопасности и защиты информации предприятия……60

2.2.2 Контрольный пример реализации проекта и его описание……..72

3. Обоснование экономической эффективности проекта……..78

3.1 Выбор и обоснование методики расчёта экономической эффективности……...78

3.2 Предварительный расчет экономической эффективности и окупаемости……...80

Заключение…….86

Список литературы……88

Приложения……89

ВВЕДЕНИЕ

С каждым часом увеличивается значимость информации в современном обществе. Информация является важным ресурсом, товаром, распаряжение которым будет приносить большую прибыль. Информация несет кое-какие адвалорные характеристики и потребительские свойства. Принимая это во внимание, особо актуальной имеет быть проблема защиты информации.

С разным информационным объектом имеют все шансы быть связаны конкретные опасности. Все угрозы могут быть случайными, и намеренными. Так, служащий организации имеет возможность невзначай выслать весомую информацию в основе, расстроить носитель данных, сделать промахи при вводе или же передаче инфы. Впрочем, случайные опасности появляются не часто, и современные программные и технические способы оберегают информацию от случайных сбоев и промахов.

Больше небезопасными считаются намеренные опасности информационной защищенности, в ходе коих нарушается единство, достоверность или же конфиденциальность инфы. Список этих опасностей с всегда увеличивается, в следствие этого для их предотвращения нужно улучшать способы обнаружения опасностей и обороны данных.

Арсенал и изощренность этих опасностей непреклонно растет, в следствие этого для их выявления нужно предвидеть не лишь только вероятные цели нарушителя, но и его возможности.

Впрочем, при организации системы защищенности данных принципиально не дожидаться, когда опасности проявятся, а уметь предвидеть их и выполнить профилактику. Для таких целей в организации обязана быть разработана политика защиты информации, которая учитывает появление опасностей разными носителям и каналам данных, а еще предусматривает меры для их выявления и исправления.

Для реализации политики защиты информации применяются всевозможные способы, методы и возможности. К ним относятся, в частности, правовые

нормы, организационные меры, инженерно-технические и программно-аппаратные возможности, методы шифрования данных.

На безопасность данных фирмы влияет много моментов. По этому действенное решение проблемы безопасности информации на предприятиях возможны только комплексными и систематическими мерами.

На сегодняшний день, вопросам защиты данных тратится очень много внимания. По этому идут множественные исследования, разрабатывают алгоритмы защиты данных, выпускаются новейшие технические и программные решения защищенности данных.

В современном мире защиты данных имеется множество отдельных инженерно-технических, программно-аппаратных, криптографических СЗИ. В литературе по ЗИ имеются описания методов и средств на данной основе, теоретических моделей защиты. Но, для создания на объекте эффективной ЗИ, требуется объединять отдельные средства защиты в систему. Проектирование СЗИ не будет являться первостепенной задачей фирмы, как, например, производство продуктов и получение зароботка. Поэтому разробатываемая СЗИ не должна сказаться на общей работе предприятия, а разработка СЗИ должна быть выгодной предприятию. Но вместе с этим, СЗИ должно обеспечивать сохранность и защиту важных данных фирмы от всех предусмотренных угроз.

Целью дипломной работы является совершенствование системы защиты информации АО «ФИНТЕХ». Для достижения цели смодулированны такие задачи:

- изучение точечной области и выявление дефектов в имеющейся системе обеспечения безопасности данных и их защите, определяющих надобность разработки проекта;
- подготовка постановки задачи проектирования;
- обоснование основных проектных решений;
- подгатовка всех видов обеспечивающих систем;
- обоснование экономической составляющей проекта.

Предметом выпускной работы будет является совершенствование систе-

мы защиты информации, на базе информационной системы АО «ФИНТЕХ».

При проектировании и написании ВКР применялись методы, анализ различных информационных источников, системные методы анализа, экономические и математические методы метод функционального моделирования.

Предложенная в работе политика защиты информационных данных может быть использована для работы в АО «ФИНТЕХ», что определяет практическую значимость работы.

1. АНАЛИТИЧЕСКАЯ ЧАСТЬ

1.1 ТЕХНИКО-ЭКОНОМИЧЕСКАЯ ХАРАКТЕРИСТИКА ПРЕДМЕТНОЙ ОБЛАСТИ И ПРЕДПРИЯТИЯ

1.1.1 ОБЩАЯ ХАРАКТЕРИСТИКА ПРЕДМЕТНОЙ ОБЛАСТИ

Основная деятельность предприятия АО «ФИНТЕХ» заключается в предоставлении профессиональных услуг в области информационных технологий, разработки ПО и создания новых автоматизированных комплексов.

Виды выпускаемой продукции:

- разработка и производство цифровых платформ (примером служит действующая и сертифицированная цифровая платформа «СитезМ»;
- разработка средств и систем контроля (такие как Автоматический пропускной модуль (одно и двунаправленные), портативное техническое средство паспортного контроля, считыватели паспортно-визовых документов и т.д.);
- разработка бюджетных систем (автоматизированная информационная система управления общественными финансами «СКИФ-БП».

Отрасль информационных технологий в России развивается и набирает обороты в связи с определенным причинам, и в том числе – в связи с высокой стоимостью иностранных технологий. Для получения прибыли, необходимо использовать современное оборудование для разработки и тестирования новой продукции, при этом цена современных серверов и комплексов защиты, ПО составляет миллионы рублей.

Начальные вложения для разработки конкурентоспособной фирмы в сфере информационных технологий на сегодняшний день составляет не менее ста миллионов рублей. Время освоения и выхода на рынок – не менее двух лет, срок окупаемости составляет не менее четырёх-пяти лет. Однако в России умеренно развит рынок с предложениями подержанного оборудования для разработки и тестирования создаваемой продукции. Всвязи с этим можно начать разработку и внедрение производимых продуктов с минимальными затратами.

По быстрее и с наименьшими затратами получется открыть дело в сфере

технической поддержки и обслуживания предприятий.

В общем, для развития отрасли информационных технологий в текущее время существует некоторые препятствия:

1. Большая зависимость от иностранного оборудования: малое присутствие российского оборудования, отвечающее современным требованиям; производство комплектующих частей инностранными производителями.

2. Несовершенное таможенное законодательство: постоянный рост пошлины на ввоз компьютерной техники и комплектующих материалов.

Можно отметить, что в текущее время заграничные поставщики, которые трудятся в сфере информационных технологий, преобладают конкурентными преимуществами перед российскими производителями, поскольку их цены достаточно ниже российских. И одна из причин этому – несовершенная налоговая система Российской Федерации.

3. Износ и моральное устаревание оборудования.

Износ серверного оборудования по всей сфере составляет около 70%. Техническое развитие в разных регионах нашей страны доходит до крайне низкого уровня. Повышение конкурентоспособности сферы возможно привлечением дополнительных инвестиций. Некоторые эксперты утверждают, что для решения данной проблемы требуется создание предприятий для оснащения серверного и компьютерного оборудования основными комплектующими от заграничных производителей.

По этому возможно отметить, что в сфере информационных технологий есть конкуренция, IT-компании выживают не только за счет качества своей продукции, но и за счет истребления своих конкурентов. По этому в IT-сфере имеется кража данных, ее фальсификация или по простому вывод из строя техники и сети фирмы.

Всвязи с этим, конкуренция в сфере информационных технологий очень большая, что провоцирует попытки захвата и взломам информации с данными, а также попыткам выведения из строя компьютерных систем. По этому особое внимание еделяется информационной безопасности предприятия.

Для проектирования системы информационной безопасности фирмы необходимо произвести ее аудит, а также входящую и исходящую информацию. Для анализа проблем предприятия подготовим функциональную модель на основе метода IDEF0. Эта метод позволяет проектировать функциональные схемы, показывающие предметную область. Функциональная модель показывает функциональную структуру фирмы. Функциональная модель состоит из схем, части текстов и глоссария, предоставляющих ссылки друг на друга.

Для анализа текущей технологии обработки информации на объекте требуется разобрать структурно-функциональную схему.

На рисунке 1 представлена контекстная схема деятельности компании АО «ФИНТЕХ».

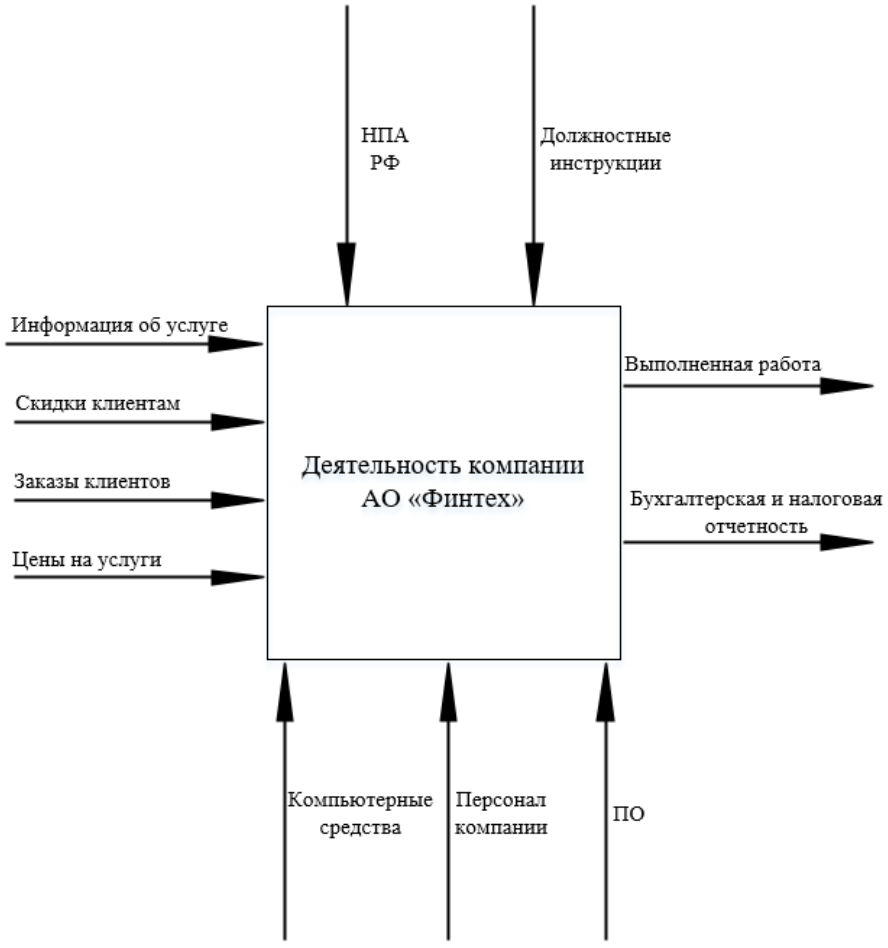


Рис. 1. Контекстная схема

Исходя зи рисунка 2, главной функцией, поподающей под наш анализ, будет деятельность фирмы. Для реализации этой функции требуется получение некоторых данных или документов:

- заказ клиента его требования (заполняется на бланке установленного образца);
- прайс с ценами и услугами;
- информация об предоставляемых услугах (полное описание услуг с указанием сроков, стоимости и дополнительной информацией);
- програма лояльности;

Эта информация является входной группой. В результате выполнения функции будут получены следующие результаты:

- проделанная работа;
- управленческая и бухгалтерская отчетность.

Эта информация является выходной группой. Как управление используются следующие механизмы:

- должностная инструкция сотруднике;
- НПА РФ.

Для реализации данного механизма требуется персонал компании, компьютерная техника и ПО. При этом контекстная схема отражает общую функцию, поэтому для улучшения понимания, о функционировании фирмы требуется произвести декомпозицию контекстной схемы.

Декомпозиция контекстной схемы выделяет основные функций, которые должны быть реализованы для выполнения основной функции. При выполнении декомпозиции стоит уделить внимание, что все входы, выходы, управление и механизмы, используемые на контекстной схеме, требуется отразить и на схеме, получившейся в результате декомпозиции. Полученный результат представлен на на рисунке 2.

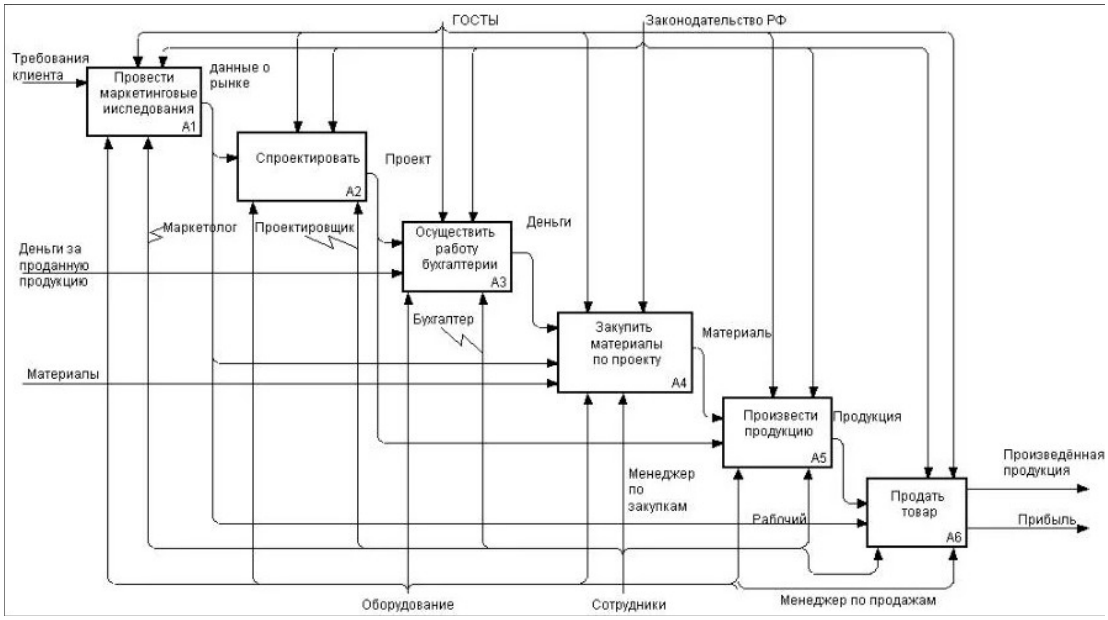


Рис. 2. Функциональная схема первого уровня

Стоит отметить, что в результате декомпозиции основного процесса было выделено пять подпроцессов:

1. Формирование заказов. Если клиент соглашается заключить договор на оказание услуг (по написанию ПО или проведению разработки), тогда все данные вносятся в клиентскую базу. При обращении заказчика в фирму повторно, его данные будут иметься в базе, тем самым облегчая процесс работы. После того, как клиент определится с нужными ему услугами, происходит формулировка и прием заказа: клиентские данные, вид предостаавляемых услуг, сроки выполнения работы, инные данные уточняющиее формулировку заказа. На основании этих данных выполняется расчет стоимости и заполнение договора с заказчиком.

2. Реализация работ. На этом этапе подрозумевается реализация работ на основании утвержденного договора.

3. Закупка необходимых материалов. Если в этом есть необходимость, то для реализации работы производится закупка необходимых материалов.

4. Бухгалтерская и налоговая отчетность.

Так же может быть полезным выполнение поведенческого моделирования

некоторых процессов. Данное моделирование необходимо для понимания происходящих процессов в системе.

Поведенченское моделирование основывается на имитаци моделирования систем массового обслуживания, сети Петри, возможно применение конечно-автоматных моделей, описывающих поведение системы, как последовательности смены состояний.

Поведенческие аспекты отражает методика IDEF3. Если она связана с функциональными аспектами, то в IDEF3 детализируются и конкретизируются IDEF0-функции.

В IDEF3 входит пара описаний:

− процесс-ориентированные, последовательность операций (Process Flow Description Diagrams, PFDD);

− объект-ориентированные, выражаемые схемами перехода состояний (Object State Transition Network, OSTN).

Процесс оформления и регистрации заявки заказчика представлен на рисунке 3. Здесь операции приведены в виде прямоугольника с чертой, отделяющей верхнюю часть (с названием функции) от нижней части, содержащей порядковый номер функции. Связь, отражающая последовательность риализации функций, изображаются сплошными линиями-стрелками.

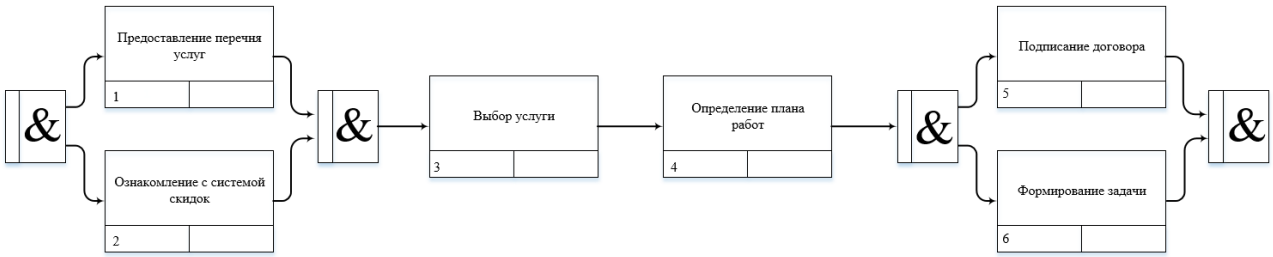


Рис. 3. Модель IDEF 3

По данному методу, были разработаны функциональная и поведенческая модели предметной области. Эти модели разрешают выявить важные информационные потоки и документы, которые являются активами фирмы и подлежат охране. Помимо того, с помощью этих моделей возможно выявить процессы,

которые исполняют обработку конфиденциальной информации. В работу процессов нужно внедрять спецтехнологии защиты данных.

Помимо этого можно выделить еще один не менее важный аспект, с использованием созданных моделей – эксперты, принимающие участие в обработке данных. Для этих экспертов нужно создать алгорифмы работы с данными, создать инструкции и провести инструктаж. Помимо этого в обработке данных применяются компьютерная техника, для которой тоже необходимо разработать систему защиты: организационные, программно-технические либо физические.

Следовательно, созданные модели предметной области являются основой для обзора информаионных активов и создания СИБ.

С помощью моделирования предметной области, выявлены важные документы и данные, которые подлежат охране. Впрочем, дабы верно оценивать нужные затраты на разработку СЗИ, необходимо верно оценивать число этих документов и обычный объем информации.

Приведённые основные свойства будут являтся последующей основой для обоснования необходимости решения задачи защиты информации, а ещё для расчёта общей экономической рузультативности проектного плана (таблица 1).

Таблица 1

Показатели компании в период с марта 2022 по апрель 2022

№	Наименование характеристики (показателя)	Значение
1	Число заказов (зак./мес.)	286
2	Число поставок комплектующих (пост./мес.)	3
3	Число обработанных документов (док./мес.)	1658
4	Трудоемкость на оформление заказов (час./мес.)	85
5	Трудоемкость на оформление поставок комплектующх (час./мес.)	2
6	Трудоемкость формирования документации (час./мес.)	180
7	Число итоговых отчетов (док.в/мес.)	50
8	Трудоемкость на оформление периодичной отчетности (час./мес.)	12
9	Количество сотрудников (чел.)	60
10	Отделы компании (шт.)	6

С помощью свойств, приведенных в таблице, будет происходить оценка уровня угроз, которые могут нанести ущерб тому либо другому потоку данных, вероятность появления той либо другой угрозы, а ещё надобность использования СЗИ.

Помимо этого, при создании способов защиты будет внятно, какой объем данных проходит через то либо другое программное, техническое средство, что поспособствует правильному выбору техники и ПО.

1.1.2 ОРГАНИЗАЦИОННО-ФУНКЦИОНАЛЬНАЯ СТРУКТУРА ПРЕДПРИЯТИЯ

К текущему моменту фирма АО «ФИНТЕХ» имеет все нужные источники для насыщенного роста, улучшения и достижения поставленных целей.

Структура управления показывает важные отделы, а ещё должности. По-

мимо того, в ней проведены вертикальные и горизонтальные связи. Вертикальные связи отображают должности находящиеся на одной ступени. Горизонтальные связи указывают на подчиненость сотрудников в нутри подразделений. Схема общей структуры управления фирмой АО «ФИНТЕХ», отражающая содержание структуры управления и объекта управления на предприятии, указана на рисунке 4.



Рис. 4. Схема общей структуры управления

На текущей день в организации АО «ФИНТЕХ» работает около 58 сотрудников.

Непосредственное общение с заказчиками организации АО «ФИНТЕХ» производится офис-менеджерами. Офис-менеджер назначается на должность и отстраняется от должности согласно действующим трудовым законодательством, приказом директора компании по предоставлению соответствующих документов начальником отдела. К основным обязанностям и задачам офис-менеджера относятся:

- Консультирование заказчиков по вопросам разнообразия продукции;
- Оказание помощи заказчику при формировании задания к продук-

ту;

- Проверка заказов на соответствие комплектации и упаковки;
- Информирование заказчика о предоставляемых фирмой услугах;
- Оповещение покупателя о скидках, правилах (порядке) оплаты и получения продукции;

Офис-менеджеры делают всё, для реализации плана продаж, установленного управлением организации АО «Финтех».

Руководство бухгалтерией организации АО «ФИНТЕХ» осуществляется главным бухгалтером. К функциям и задачам данного направления принадлежат:

- Провод денежных расчётов с заказчиками за приобретенную ими продукцию;
- Составление и соправождение бухгалтерской и налоговой отчетности;
- Начисление заработной платы сотрудникам фирмы.

К основным функциям и задачам отдела управления проектами и отдела разроботок фирмы АО «ФИНТЕХ», в котором проходилась практика на должности инженера, относятся:

- Диагностика неисправностей и их устранение;
- Установка и настройка ПО;
- Установка и настройка САЗ;
- Установка драйверов и настройка устройств;
- Проведение всех видов ТО;
- Внедрение и сопровождение ПО;
- Разработка и сопровождение ПО;
- Разработка и сопровождение автоматизированных систем;
- Тестирование разработанного ПО и оборудования;
- Разработка и внедрение корпоративной политики безопасности;
- Поддержка пользователей и офисных приложений.

К основным функциям и задачам юридического отдела относится состав-

ление и подписание договоров с заказчиками организации. Руководство производственно-хозяйственной и финансово-экономической деятельностью организации АО «ФИНТЕХ» осуществляется директором и его заместителем.

1.2 АНАЛИЗ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.2.1 ИДЕНТИФИКАЦИЯ И ОЦЕНКА ИНФОРМАЦИОННЫХ АКТИВОВ

Активы – это все, что имеет ценность или находит полезное применение для организации, ее деловых операций и обеспечения их непрерывности. Надлежащее управление и учет активов должны являются одной из основных обязанностей руководителей всех уровней [1]. К основным активам относятся непосредственно информация, инфраструктура, персонал, имидж и репутация компании. Без инвентаризации активов на уровне бизнес-деятельности невозможно ответить на вопрос, что именно нужно защищать. На основе функциональной модели были ыявлены следующие потоки информации:

- заказы клиентов (заполняется на бланке установленного образца);
- цены на товары и услуги;
- информация об услугах (полный перечень услуг с указанием примерных сроков и стоимости);
- скидки клиентам;
- бухгалтерская и управленческая отчетность.

Оценка информационных активов компании представлена в таблице 2.

Таблица 2

Оценка информационных активов компании

Вид деятельности	Наименование актива	Форма представления	Владелец актива	Критерии определения стоимости	Размерность оценки	
					Количественная оценка (ед. изм.)	Качественная
Информационные активы						
Реализация услуг	Заказы клиентов	Устная информация	Офис-менеджер	Утрата доступности	6	средняя
Реализация услуг	Переписка внутри компании	Текстовая информация	Офис-менеджер, инженера	Потери в результате перехвата данных	9	критическое значение
Реализация услуг	Скидки клиентов	Документ	Офис-менеджер	Утрата доступности	0,5	очень малая
Реализация услуг	Цены на товары и материалы	Прайс-лист	Офис-менеджер	Утрата доступности	7	высокая
Реализация услуг	Расходные накладные	Документ	Офис-менеджер	Утрата доступности	6	средняя
Реализация услуг	Наряд на выполнение работ	Документ	Офис-менеджер	Утрата доступности	6	средняя
Реализация услуг	Инвентаризационная ведомость	Документ	Инженер	Утрата доступности	9	критическое значение
Закупка расходных материалов	Приходные накладные	Документ	Инженер	Утрата доступности	8	высокая
Бухгалтерский и налоговый учет	Бухгалтерская и налоговая отчетность	Документ	Бухгалтер	Утрата доступности	1,5	малая
Активы программного обеспечения						
Реализация услуг	Программное обеспечение	Информация на электронном носителе	Програмист	Первоначальная стоимость актива	32	средняя

Физические активы						
Реализация услуг	Персонал компании	Материальный объект	Програмист	Первоначальная стоимость	17	малая
Реализация услуг	Компьютерные средства	Материальный объект	Инженер	Первоначальная стоимость	23	средняя
Услуги						
Реализация услуг	Информационные услуги	Устная информация	Офис-менеджер	Утрата доступности	6	средняя

Перечень информационных активов, обязательное ограничение доступа, к которым регламентируется действующим законодательством РФ, сведены в таблицу 3.

Таблица 3

Перечень сведений конфиденциального характера

№ п\п	Наименование сведений конфидециального характера	Присвоенный гриф конфиденциальности	Документ, регламентирующий конфидециальность
1	Сведения, раскрывающие характеристики и настройки СЗИ ЛВС фирмы от несанкционированного доступа.	Коммерческая тайна	Устав фирмы АО «Финтех»
2	Требования к сотрудникам фирмы, для обеспечения комерческой тайны.	Коммерческая тайна	Гражданский кодекс РФ ст. 1465
3	Персинифицированные данные о сатрудниках фирмы	Коммерческая тайна	Федеральный закон 152-ФЗ
4	Данные заказчиков	Коммерческая тайна	Федеральный закон 152-ФЗ

Результат выстраивания активов имеет вид интегрированной оценки степени необходимости актива для фирмы, расчитываемую по пятибалльной шкале и приведенную в таблице 4.

Таблица 4

Результаты выстраивания активов

Наименование актива	Ценность актива (ранг)
Состав заказа(включая сам заказ и его подробное описание)	4
Скидочная программа	1
Ценовая политика товаров и комплектующих	5
Накладные по приходу комплектующих	4
Акты выполненых работ	4
Отчеты об инвентаризации	5
Отчетность фирмы (бухгалтерская, нологовая)	4
ПО используемое фирмой	3
Сотрудники фирмы	1
Техническое оснащение фирмы	2
Предоставляемые информационные услуги	4
Внутреняя переписка фирмы	5

Тем самым, выявлены активы, относящиееся к более важным: ценовая политика товаров и комплектующих, отчеты об инвентаризации, внутреняя переписка фирмы, состав заказа(включая сам заказ и его подробное описание), накладные по приходу комплектующих, акты выполненых работ, отчетность фирмы (бухгалтерская, нологовая), предоставляемые информационные услуги.

1.2.2 ОЦЕНКА УЯЗВИМОСТЕЙ АКТИВОВ

Оценка уязвимости активов расмотрена на основании регламентирующего документа ГОСТ Р ИСО/МЭК 27005-2010 [].

Уязвимость – это событие, возникающее в результат стечения обстоятельств, в силу каких-либо причин, выявленное в системах обработки информации СЗИ и не в состоянии дать должного сопротивления всевозможным дестабилизирующим моментам вредоносного действия на данные, подлежащие защите.

В ИБ, термин уязвимость употребляется для разъяснения уязвимости в

ИС, используя который, можно преодалеть её целостность и навредить в ее работе. Уязвимость может может быть образована в результате допущения ошибок при разработки ПО, неточностей, допущенных при начальном и последующих проектированиях ИС, паролей малой сложности, вирусных файлов и программ. Можно сказать – уязвимость – это вероятная уязвимость в СЗИ.

Уязвимости ИС фирмы выявляются такими способами как:

- Описание сотрудником компании (инженер, администратор ИБ или специалист ДИБ) исходя из опыта приобретённого ранее.

- Сотрудники специализированных фирм занимающихся технологическим аудитом информационной системы и выявлением уязвимостей в ней.

За частую сотрудники специализированных фирм более независимо проведут аудит существующующей СЗИ и обнаружить все (или большую часть) уязвимостей, существующих в фирме.

Показателем уязвимости некого актива является степень уязвимости в порядковой шкале оценок (пример степеней: высокая, средняя, низкая).

Перечень уязвимостей, с оценками возможной уязвимости активов, указаны в таблице 5.

Таблица 5

Оценка уязвимости активов

Группа уязвимостей	Внутренняя переписка	Цены на товары	Инвен--ведомость	Приходные накладные	Заказы клиентов	Расходные накладные	Наряд на выполнение работ	Бух. и налоговая отчетность	Инф-я о продукции	ПО
1. Среда и инфраструктура										
Перебои в электропитании										низкая
2. Аппаратное обеспечение										
Не своевременное обслуживание	высокая	средняя	средняя	средняя	средняя	средняя	средняя	средняя	низкая	средняя
Отсутствие учёта внесения изменений в конфигурации	высокая	высокая	высокая	высокая	высокая	высокая	высокая	низкая	низкая	высокая
3. Программное обеспечение										
Отсутствие способов идентификации	высокая	высокая	высокая	высокая	высокая	высокая	высокая	низкая	низкая	высокая
Общий доступ к паролям	высокая	высокая	высокая	высокая	низкая	высокая	низкая	низкая	низкая	высокая
Несвоевременная смена паролей	высокая	высокая	высокая	высокая	высокая	высокая	низкая	низкая	низкая	высокая
Не корректное разграничение прав доступа	высокая	высокая	средняя	средняя	низкая	средняя	низкая	низкая	низкая	средняя
Отсутствие регистрации пользованием компьютерной техникой	высокая	высокая	высокая	высокая	низкая	высокая	низкая	низкая	низкая	средняя

Отсутствие эфективности учёта внесения изменений в конфигурации	высокая	высокая	средняя	средняя	средняя	средняя	низкая	низкая	низкая	высокая
Отсутствие резервного копирования и бэкапов	высокая	высокая	средняя	средняя	высокая	средняя	средняя	низкая	низкая	средняя
4. Коммуникации										
Некоректное управление сетью	высокая	низкая	низкая	низкая	низкая	низкая	низкая	низкая	низкая	низкая
Незащищенные подключения к сетям общего пользования	высокая	средняя	средняя	средняя	средняя	средняя	средняя	средняя	средняя	средняя
5. Документы (документооборот)										
Хранение документации в открытом доступе	низкая	высокая	высокая	высокая	высокая	высокая	средняя	низкая	низкая	
Безконтрольность при уничтожении документации	низкая	высокая	высокая	высокая	высокая	высокая	средняя	низкая	низкая	
Копирование документов без регистрации копий	низкая	высокая	высокая	высокая	высокая	высокая	средняя	низкая	низкая	
6.Персонал										
Использование СВТ в личных нуждах	высокая	средняя	средняя	средняя	средняя	средняя	средняя	низкая	средняя	средняя
7. Общие уязвимые места										
Неправильное (некомпитентное) провидение ТО	высокая	низкая	низкая	низкая	низкая	низкая	низкая	низкая	низкая	низкая

1.2.3 ОЦЕНКА УГРОЗ АКТИВАМ

Угроза – это некая причина события, которая с большей долей вероятности может спровацировать ущерб как самой системе так и фирме в целом. Инцидент ИБ – это любое неожиданное или неприятное происшествие, которое вероятнее всего спровацирует нарушение деятельности в организации или в ИБ.

Существует несколько видов угроз. Одни из них это пассивные угрозы направленые в большей мере на неправомерное использование информационных ресурсов информационной системы, но при этом не оказывают влияния на сами данные, так же пассивные угрозы не искажают и не нарушают информацию. К примеру такой угрозы возможно отнести прослушивание каналов связи и просмотр информации из БД.

Вторые, это так называемые активные угрозы, нарушающие нормальную работу информационной системы. Она целенаправленно действует на состовляющей данной системы. Данные угрозы искожают информацию, порожают саму информационную систему. К данным угрозам можно отнести искажение данных, вывод из строя СВТ, заражение системы вирусами.

Так же существуют умышленные угрозы которые делятся на два типа: внутренние (происходящие в нутри фирмы) и внешние (предшевствующие из вне). Внутренние угрозы более вероятны со стороны неблагонадежного и чем-либо расстроенного сотрудника со стороны фирмы. Также не исключюены внутренние экономией средства на разработки СЗИ. Внешние угрозы чаще всего справоцированы конкурентами на рынке, зависят от экономических условий и иных причин.

По данным интернет издательств, широко распространяется промышленный шпионаж — это недобрасовестная конкуренция, при которой конкурент незаконным путем получает служебную, комерческую и иные виды информации подлежащую защите действующим законодательством и указами фирмы.

Таким образом была проведена оценка угроз активам на основании ГОСТ Р ИСО/МЭК 27005-2010 []. Перечень угроз, с указанием их оценки, приведены

в таблице 6.

Таблица 6

Оценка угроз активам

Перечень уязвимостей по группам	Внутренняя переписка	Цены на товары	Инвентари-зационная ведомость	Приходные накладные	Заказы клиентов	Расходные накладные	Наряд на выполнение работ	Бухгалтерская и налоговая отчетность	Инф-я о продукции	ПО
1. Угрозы, от преднамеренных действий										
ПО считающиеся вредоносным	высокая	низкая	низкая	низкая	низкая	низкая	низкая	низкая	низкая	низкая
Доступ неликвидных пользователей к системе	высокая	средняя	средняя	средняя	средняя	средняя	средняя	средняя	средняя	средняя
Использование ПО неликвидными пользователями	высокая	высокая	высокая	высокая	высокая	высокая	высокая	низкая	высокая	высокая
2. Угрозы, возникшие от случайных действий										
Ошибка персонала	высокая	высокая	высокая	высокая	высокая	высокая	высокая	средняя	средняя	низкая
Неподобающее распоряжение ресурсами	средняя	высокая	высокая	высокая	средняя	высокая	средняя	низкая	средняя	высокая
Допуск ошибок при ТО	высокая	средняя	средняя	средняя	низкая	средняя	средняя	средняя	средняя	средняя
3. Угрозы, природного и техногенного характера										
Износ систем и носителей данных	низкая	высокая	высокая	высокая	средняя	высокая	высокая	средняя	средняя	высокая
Не стабильность электропитаня	низкая	высокая	высокая	высокая	высокая	высокая	низкая	средняя	средняя	высокая

1.2.4 ОЦЕНКА СУЩЕСТВУЮЩИХ И ПЛАНИРУЕМЫХ СРЕДСТВ ЗАЩИТЫ

Задачи по защите информации возложены на сотрудников IT-отдела компании, а также на начальников отделов.

Компания оснащена необходимыми ТС, характеристики которых приведены на схеме технической архитектуры ИС фирмы на рисунке 5.

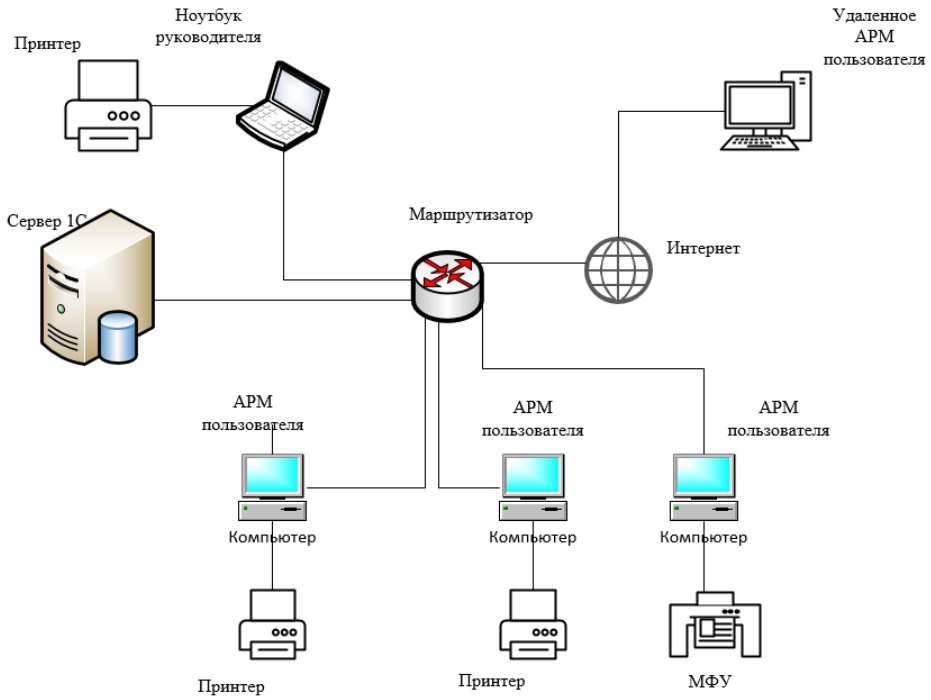


Рис. 5. Техническая архитектура ИС фирмы АО «ФИНТЕХ»

Сервер 1С установлен на сервере IBM x3650, который имеет характеристики следующего вида: Intel Xeon 6C X5675 3.06 GHz Макс. объем памяти: 32 Гб x 8 шт. Типы памяти: DDR3-1333 MHZ.

Все отделы фирмы оснащены рабочими станциями со следующими параметрами: Intel core i5 (2.6 ГГц) / RAM 16 ГБ / HDD 1 Тб / NVIDIA GeForce RTX 2060 (6 Гб) / DVD+/-RW Slim.

Для печати документов в отделах компании установлены принтеры, HP LJ P3015DN с лазерной технологией печати (ч/б), скорость печати составляет 40 стр./мин.

Руководство фирмы использует ноутбук, с характеристиками: AMD Ryzen 5 Ryzen 5 5600H 3.2 ГГц / RAM 8 Гб / SDD 512 Гб / GeForce RTX 3050 / LAN / Wi-Fi / Bluetooth / веб-камера.

Все АРМ фирмы объеденены в локальную сеть по топологии звезда, с помощью технологии передачи данных Ethernetc. Для маршрутизации применяется маршрутизатор типа Cisco 3945 SPE150 K9.

На текущий момент налоговая и бухгалтерская отчетность в фирме осуществляется на базе программного обеспечения «1С: Бухгалтерия 8.3». Данное програмное обеспечение гарантирует большой уровень автоматизированного ведения бухгалтерского и налогового учета. А так же отлично подходит для подготовки и ведения обязательных (регламентированных компанией и законодательством) отчетных документов. Программная архитектура ИС фирмы представлена схемой на рисунке 6.

Сервер 1С – это сервер с ПО, который обеспечивает непрерывную работу и доступ к данному продукту. Сервер 1С состоит из набора процессов для оптимальной работы в сфере решаемых задач фирмой []:

- Серверный агент (ragent.exe) – является основой для сервера 1С. Он производит хранение данных и идентификацию кластеров 1С.
- Кластер 1С (rmngr.exe) – рабочие процессы 1С, объединенные в группу. Осуществляют обработку информации. Его работа заключается в управлении рабочими процессами.
- Рабочий процесс 1С (rphost.exe) – некое ПО, которое занимается обработкой пользовательских сеансов.

Система типа «1С: Бухгалтерия 8.3» обеспечивает своевременной и конструктивное решение всех поставленных задач для отдела бухгалтерии.

Подготовка документальных отчетов, а также иной необходимой документации в фирме составляется при помощи программных продуктов пакета Microsoft Office 2016:

- Microsoft Office Word позволяет создовать, редактировать, просматривать тексты статей и деловых бумаг, в фирме применяется для составления и

ведения документации в надлежащем виде.

- Microsoft Office Excel позволяет работать с электронными таблицами, в фирме применяется для анализирования и визуализирования данных.
- Microsoft Office Outlook персональный информационный менеджер с функциями почтового клиента, в фирме используется для служебной переписки между сотрудниками. Так же присутствует возможность создавать расписания, контакты и задачи.
- Microsoft Office InfoPath используется как полнофункциональная среда для проектирования, разработки, развертывания, размещения, сбора, объединения и интеграции электронных форм.
- Microsoft Office PowerPoint используетсчя для подготовки презинтаций, показываемых заказчику и руководству.

Веб-браузер Google Chrome используется всеми подразделениями фирмы для предоставления доступа в интернет среду (поиска информации, работа с электронной почтой, чтение новостей для развития компании).

В фирме так же используются дополнительное ПО, такое как Adobe Acrobat и др.

Для предостережения от угроз исходящих из вне ОС фирмы АО «ФИНТЕХ» оснащается лицензионным ПО «Kaspersky Total Security Plus для бизнеса». Данное ПО установленно в ОС Microsoft Windows 10 (Корпоративная версия), установленна на всех АРМ фмрмы.

У каждого пользователя «1С: Бухгалтерия 8.3» имеется персональный логин и пароль. В связи с этим достаточно свободно и легко определить кем и когда были внесены какие-либо изменения в отчетную документацию.

Оценив действующую СИБ, возможно отразить на сколько полно выполняются однотипные функции при решении поставленных задач обеспечения защиты данных (таблица 7).

Таблица 7

Анализ выполнения задач по обеспечению информационной безопас-

ности

№ п/п	Основные задачи по обеспечению ИБ	Степень
1.	обеспечение безопасности производственно-торговой деятельности, защита информации и сведений, являющихся коммерческой тайной;	средняя
2.	организация работы по правовой, организационной и инженерно-технической (физической, аппаратной, программной и математической) защите коммерческой тайны;	средняя
3.	организация специального делопроизводства, исключающего несанкционированное получение сведений, являющихся коммерческой тайной;	низкая
4.	предотвращение необоснованного допуска и открытого доступа к сведениям и работам, составляющим коммерческую тайну;	средняя
5.	выявление и локализация возможных каналов утечки конфиденциальной информации в процессе повседневной производственной деятельности и в экстремальных (техногенных, природных) ситуациях;	средняя
6.	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
7.	обеспечение охраны территории, зданий помещений, с защищаемой информацией.	высокая

1.2.5 ОЦЕНКА РИСКОВ

Активы, составляющие ценность для компании с некой степенью уязвимости, за чистую могут подлежать уязвимости при возникновении той или иной угрозы. При аудите риска ставится задача об определении и оцениванию рисков, подвергающимся при эксплуатации систем ИТ и ее активов. Цель этой задачи определение и выбор оптимальных СЗИ. Для оценки рисков выбран метод, предполагающий таблицы «штрафных баллов» для каждой комбинации ценности активов, уровня угроз и уязвимостей (таблица 8).

Таблица 8

Таблица «штрафных баллов»

Ценность актива	Уровень угрозы								
	Низкий			Средний			Высокий		
	Уровень уязвимости			Уровень уязвимости			Уровень уязвимости		
	Н	С	В	Н	С	В	Н	С	В
0	0	1	2	1	2	3	2	3	4
1	1	2	3	2	3	4	3	4	5
2	2	3	4	3	4	5	4	5	6
3	3	4	5	4	5	6	5	6	7
4	4	5	6	5	6	7	6	7	8
Обозначение: Н - низкий, С - средний, В - высокий.									

Ценности активов в совокупности с уровнем угроз, а так же уязвимости, определенные каждому типу влияния вносят в матрицу для анализирования каждого сочетания соответствующих мер риска по 8-ми бальной системе. Значения величин вносят в матрицу в структурирной форме согласно таблице 8.

Для всех активов предусматривают уязвимые места и сопутствующие им угрозы. В случае нахождения новых уязвимых мест без определенной угрозы или угрозы без соответствующего уязвимого места, определяется отсутствие риска на тикущий момен. Далее сопостовляют ряд матриц по ценности актива, а соответствующие поля – по важности угрозы и уязвимости. Ценность настоящего метода состоит в выстраивание по порядку соответствующих рисков (таблица 9).

Таблица 9

Результаты оценки рисков информационным активам фирмы

Риск	Актив	Ранг риска
Утрата доступности	Цены на товары и материалы	65
Утрата доступности	Информационные услуги	58
Утрата конфиденциальности	Внутренняя переписка	57
Утрата конфиденциальности	Приходные накладные	52
Утрата конфиденциальности	Расходные накладные	49
Утрата конфиденциальности	Инвентаризационная ведомость	34
Утрата конфиденциальности	Заказы клиентов	26
Утрата доступности	Скидки клиентов	23

Нарушение целостности	ПО	23
Утрата доступности	Акты выполненых работы	22
Утрата доступности	Бухгалтерская и налоговая отчетность	7

Приведенная выше таблица содержит риски наиболее ценным информационным активам, ранжированные в порядке убывания. Выводы оценки рисков это основание для дальнейшей разроботки и усовершенствования СИБ.

Так же методом оценки ИБ может являться оценка защищенности объектов защиты по отдельности. К таким объектам относится:

- АРМ персонала;
- серверное оборудование;
- информация конфедициального характера (документы);
- сетевые и кабельные линии;
- помещения для обработки конфендициальной информации;
- БД фирмы.

Информационные риски следует расчитывать для каждого объекта индивидуально. Понятия используемые прт расчетах.

Критичность ресурса (D) – влияние реализации угрозы на работу информационной системы (степень значимости ресурса). Определяют специалисты фирмы на основе экспертных оценок.

Критичность реализации угрозы (ER) – это влияния выполнения угрозы на ресурс, указывается в %. Определяют на основании статистической информации, опубликованных на сайтах компаний – интеграторов.

Вероятность осуществления угрозы через некую уязвимость в течении колендарного года (P(v)) – возможность исполнения угрозы, через указанную уязвимость в неких ситуациях, указывается в %.

Объект защиты – АРМ сотрудника.

В фирме имеется порядка 80 АРМ сотрудников. Для доступа в помещения фирмы используются именные пластиковые карты, тем самым исключая доступ посторонних лиц. Каждый сотрудник имеет персональный

логин и пароль, групповой политикой для исключения при отлучении сотрудника с рабочего места АРМ блокируется через 10 минут. На практике пароли зачастую меняются редко, а некоторые пользовотили и вовсе оставляют записи с ними у рабочего места.

Вся документация отправляемая и получаемая на предприятии через электронную почту проходит через сервер, где контролируются все письма, поэтому личная переписка запрещена. Все образцы документов находятся в общем доступе для сотрудников на сервере, заполненные документы хранятся непосредственно на АРМ сотрудников. Критерий критичности (D) приравнен к 49 347 рублям.

Проведем аудит основных угроз, типичный для выбранного инстанса и уязвимостей, для реализации данных угроз (таблица 10).

Таблица 10.

Таблица угроз и уязвимостей.

Угроза	Уязвимости
1.Физический доступ нарушителя к АРМ	1. Отсутствие системы контроля доступа служащих к чужим АРМ (оставление компьютера без присмотра в не заблокированном виде)
	2.Отсутствие видеонаблюдения в кабинетах (имеется только в серверном помещении)
	3.Отсутствие алгоритма смены паролей
2.Сбои в работе АРМ	1. Отсутствие АПО на АРМ
	2.Человеческий фактор
3.Разрушение конф. информации при помощи специальных программ и вирусов	1.Отсутствие АПО на АРМ
	2.Не ограниченый доступ сотрудников к внешней среде

Таблица вероятности реализации данной угрозы через уязвимость в течение года(P(V)) и критичности реализации угрозы (ER).

Таблица 11.

Таблица вероятности реализации угрозы

Угроза/уязвимость	P(V), %	ER,%
1/1	10	50
1/2	10	50
1/3	20	90
2/1	40	80
2/2	10	20
3/1	50	80
3/2	20	60

Таблица уровня угрозы по некой уязвимости (Th) и по уровню угроз по всем уязвимостям (CTh).

Таблица 12.

Таблица уровня угрозы

Угроза/уязвимость	Th	CTh
1/1	0,05	0,260
1/2	0,05	
1/3	0,18	
2/1	0,32	0,334
2/2	0,02	
3/1	0,4	0,472
3/2	0,12	

Th=P(V)/100*ER/100

CTh=1-П(1-Th)

Расчет общего уровня угрозы по ресурсу:

CThR=1-П(1-CTh)=0,740

Расчет риска по ресурсу:

R= CThR*D=0,740*49 347 = 36 516,78 (руб.),

с одного автоматизированного рабочего места => 80*36 516,78 = 2 921 342,4

Исходя из этого, уровень риска, с использованием АРМ сотрудника, высок – 74%, потери в денежном эквиваленте 36 516,78 руб. Основными проблемами являются:

- отсутствие антивируса на АРМ

- отсутствие регламента паролей
- халатное отношение пользователей

Объект защиты – локальный сервер.

Критерий критичности (D) равен 1 040 800 рублей.

Данный сервер располагается в специальном помещении, с ограниченым доступом. На сервере расположены общие ресурсы, доступны сотрудникам с рабочих мест. В основном это образцы документов и общая информация дла всех сотрудников фирмы. В связи с этим появляется проблема угрозы разглашения и изменения информации конфендициального характера, но при всем этом такие угрозы проявляются достаточно редко и описываются схемами внутреннего нарушителя. Чаще всего, это это случается не преднамеренно. Как и со всяким оборудованием, на сервере так же возможны сбои в его работе, однако это случается достаточно редко.

Сервер электронной почты установлен непосредственно на самом сервере, тем самым имеется возможность отслеживать получателей и отправителей. Там же находится прокси-сервер, контролирующий выход в Интернет. Для определенных сотрудников имеется УД к ресурсу, что делает возможным утечку и порчу информации на сервере.

Проведем анализ основных угроз, характерных для выбранного объекта и уязвимостей, через которые эти угрозы могут быть реализованы (таблица 13).

Таблица 13.

Таблица угроз и уязвимостей.

Угроза	Уязвимости
1.Разглашение, уничтожение или разглашение КИ, хранящейся на сервере	1. Доступ к информации с АРМ
	2. Наличие удаленного доступа
2.Выход сервера из строя	1.Большое количество подключений
	2.Сбои электричества

Таблица вероятности реализации данной угрозы через уязвимость в течение года(P(V) и критичности реализации угрозы (ER).

Таблица 14

Таблица вероятности реализации угрозы

Угроза/уязвимость	P(V), %	ER,%
1/1	10	60
1/2	10	20
2/1	20	20
2/2	10	40

Таблица уровня угрозы по определённой уязвимости (Th) и по уровню угроз по всем уязвимостям (CTh).

Таблица 15

Таблица уровня угрозы по определённой уязвимости

Угроза/уязвимость	Th	CTh
1/1	0,06	0,079
1/2	0,02	
2/1	0,04	0,078
2/2	0,04	

Th=P(V)/100*ER/100

CTh=1-П(1-Th)

Рассчитаем общий уровень угроз по ресурсу:

CThR=1-П(1-CTh)= 0,151

Рассчитаем риск по ресурсу:

R=CTh*D=0,151*1 040 800=157 160, 13 (руб.).

Таким образом приходим к выводу, что риск по этому ресурсу не большой по сравнению с АРМ – всего 15,1 % и потери – 157 160,13 руб. Но следует взять во внимание угрозы, наличие УД, отсутствие групповых политик безопасности.

Объект защиты – помещения с ограниченной информацией и комуника-

ционные системы.

В связи с тем, что доступ на фирму осуществляется по именным пропускам, то проникнуть в здание фирмы, посторонним лицам невозможно.

1.3 ХАРАКТЕРИСТИКА КОМПЛЕКСА ЗАДАЧ И ОБОСНОВАНИЕ НЕОБХОДИМОСТИ СОВЕРШЕНСТВОВАНИЯ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЗАЩИТЫ ИНФОРМАЦИИ НА ПРЕДПРИЯТИИ

1.3.1 ВЫБОР КОМПЛЕКСА ЗАДАЧ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

После проведения оценки рисков наиболее важным ИА были определены основные задачи по совершенствованию ИБ.

Выделим 3 группы задач разрабатываемой СИБ:

1. Обеспечивание доступности надлежащих активов: стоимоть услуг и комплектующих, программы скидок, информационные предложения, отчетность компании, акты выполненых работ.

2. Обеспечивание конфиденциальности надлежащих активов: приходные накладные, инвентаризационная ведомость, служебная переписка, расходные накладные, заявки покупателей.

3. Обеспечивание целостности надлежащих активов: ПО.

Основной целью разработки СИБ, является понижение вероятности риска по всем активам (по раздельности) и по всем информационным объектам в частности. В связи с этим считаю нужным решить следующие задачи:

1. Возможность пользовотеля в привычной форме запрашивать, согласовывать и получать доступ к ИР через web-портал.

2. Возможность работы с документацией без нарушения уровня конфиденциальности.

3. Возможность круглосуточно держать под контролем все конфигурации

прав доступа к ИР фирмы и иные изменения необходимых конфигураций оборудования; владеть всей нужной информацией для быстрого иследования инцидентов, связанных с неисполнением правил политики безопасности.

Главной задачей фирмы считается привлечение новых заказчиков и расширение на рынке, обеспечение клиентов своевременной информацией по продукции и обслуживанию. Реализация данных задач возможна счет реализации ИБ на фирме.

Внедрением СЗИ на фирме скорее всего займется системный администратор, а также начальник СБ и руководитель фирмы.

1.3.2 ОПРЕДЕЛЕНИЕ МЕСТА ПРОЕКТИРУЕМОГО КОМПЛЕКСА ЗАДАЧ В КОМПЛЕКСЕ ЗАДАЧ ПРЕДПРИЯТИЯ, ДЕТАЛИЗАЦИЯ ЗАДАЧ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЗАЩИТЫ ИНФОРМАЦИИ

Обеспечение ИБ является неотъемлемой частью для функционирования предприятия. Утеря информации приведет к краху всей системы, уменьшение, либо и вовсе потери прибыли, уходу постоянных заказчиков.

Учитываемый комплекс мер для обеспечения ИБ фирмы:

I. Технические

1. Аппаратные:

1) Закупить ИБП для сервера и АРМ пользователей.

2) Дополнительно установить видеокамеры.

3) Закупить металлические шкафы и сейфы для хранения документации с ограниченым доступом.

2. Программные:

1) Установить систему КУБ.

2) Установить программное средство Secret Net LSP.

3) Переустановить антивирусную систему по принципу, на сервере устанавливается серверная часть антивирусной программы, далее создаем задачи для установки АПО на клиентские АРМ, так же все БД будут обновляться централизованно с сервера, в то же время администратор сможет

управлять и мониторить всеми АРМ сотрудников.

4) Переработать политику паролей. Требовать смены пароля пользователем раз в месяц с набором определенных символов.

5) Настроить разграничение прав пользователей к информации хранящейся на сервере;

Так же обязать работников дать письменное согласие об соглашении с правилами работы на местах, в частности с информацией и АРМ, провести дополнительные инструктажи. В дальнейшем включить эти пункты в трудовой договор или дополнительное соглашение.

1.4 ВЫБОР ЗАЩИТНЫХ МЕР

1.4.1 ВЫБОР ОРГАНИЗАЦИОННЫХ МЕР

Меры для физической защиты безопасности содержут характеристики по обеспечение прочности внутренних стенок постройки, использование цифровых, кодовых замков (лучше установить СКУД), план систем пожаротушения и инструкции СБ. Безопасность персонала содержит определенную проверку лиц при трудоустройстве на работу (особенно лиц, которым предстоит работать с информацией ограниченого и конфедициального характера), контроль работы персонала и проверку знаний мер защиты.

Административная безопасность содержит безопасные способы ведения и оформления отчетной документации, методы разработки и дальнейшего принятия прикладных программ, а также механизм реализации обработки инцидентов в случаях нарушения СИБ.

Предполагается 3 стратегии обеспечения ИБ:

- оборонительная;
- наступательная;
- упреждающая.

В данной фирме выбрана наступательная стратегия ИБ. Наступательная

стратегия включает активное противодействие всевозможным известным угрозам, влияющим на ИБ системы. Данная стратегия так же подразумевает возможную установку дополнительных программно-аппаратных средств авторизации пользователей, внедрение более совершенных технологий, повышение отказоустойчивости системы.

Функционирование системы фирмы должно обеспечивать круглосуточный доступ к ней пользователей не зависимо от праздников и выходных.

В состав сотрудниковобеспечивающий эксплуатацию ИС в рамках данной фирмы входит практически весь персонал, исключая руководящий состав. Техническая поддержка и администрирование системы ведется инженерами и програмитами, входящими в состав сотрудников фирмы.

Сотрудники, эксплуатирующим данную систему, должны соответствовать таким требованиям как:

- Менеджеры – умение работы с заказчиками при оформлении и формировании заказа; знание инструкций по работе с ИС (руководство пользователя).
- Инженера и програмисты – знание методологии проектирования хранилищ данных; знание 1С; опыт администрирования 1С; опыт в архивирование и восстановление данных; знание и навыки оптимизации работы 1С; умение управлением СИБ; знание и навыки администрирования приложения; знание инструментов разработки.

Надежность на предприятии должена достигаться согласованным действиями организационно-технических мероприятий и программно-аппаратных средств. Отказоустойчивость должна обеспечиваться за счет:

- применения ТС, системного и базового ПО, надлежащих классу решаемых задач;
- своевременного администрирования процессов;
- соблюдения правил эксплуатации и ТО программно-аппаратных средств;
- проведения обучения сотрудников.

Для соблюдения безопасности при использовании ИС сотрудники фирмы

обязаны соблюдать установленные требования мер безопасности при работе с АРМ. Технические средства, используемые для функционирования ИС, в свою очередь должны отвечать требованиям СанПиН 2.2.2/2.4.1340-03 «Гигиенические требования к персональным электронно-вычислительным машинам и организации работы», утверждённый Главным государственным санитарным врачом РФ, первым заместителем Министра здравохранения РФ 30 мая 2003 г.

В части диалога с пользователем:

- для наиболее частых операций, для ускорения рабочего процесса должны быть предусмотрены «горячие» клавиши;
- при возникновении ошибок в работе, на экране монитора должно отображаться сообщение с текстом ошибки и с необходимыми действиями по её устранению на русском языке.

Для реализации сохранности при непредвиденных ситуациях проработать следующие меры по восстановлению работоспособности системы:

- Резервное копирование БД – копия данных, структур и объектов безопасности, содержащихся в БД. Запускается ежедневно в 21:00 автоматически, а так же при инициировании запуска администратором системы в ручном режиме.
- Восстановление из резервной копии – операция проводится исключительно администратором системы.

Расположение единой БД для работы с ИС будет находиться на отдельном сервере с предустановленной СУБД «1С: Предприятие».

Сотрудники будут подключаться и работать с системой с помощью клиентского приложения. Для работоспособности данного сценария на серверном оборудовании необходимо установить такое ПО как:

- ОС Windows Server 2016;
- СУБД «1С: Предприятие»;
- Почтовый сервер Microsoft Office Exchange;

На АРМ пользователя предпологается установить:

- ОС Windows 10;

- Офисный пакет Microsoft Office 2016;
- Клиентская часть «1С: Предприятие»;

Для обеспечения безопасности ИС предусматривается разграничение прав доступа, всвяз с чем определены две категории пользователей, описанные в таблице 18.

Таблица 18

Разграничение прав пользователей

Пользователи	Справочники	Документы	Отчеты
Администратор	Полный доступ	Полный доступ	Полный доступ
Остальные сотрудники фирмы	Чтение Добавление Редактирование	Формирование Предварительный просмотр Печать	Формирование Предварительный просмотр Печать

В первую очередь востановлению подлежат функции и приоритеты, необходимые для обработки данных, которые необходимо востанавливать в случае сбойных ситуаций системы.

К документации, которая будет разработана, возможно отнести:

- инструкция о пропускном, внутреобъектовом режиме;
- регламент обработки документов, подлежащих защите;
- порядок действий при инцендентах в фирме;
- ТЗ для разработки ИС;
- руководство пользователя;
- руководство администратора;
- руководство программиста.

1.4.2 ВЫБОР ИНЖЕНЕРНО-ТЕХНИЧЕСКИХ МЕР

СЗИ в частности предотвращения преднамеренных атак, зависящие от метода реализации можно поделить на несколько группы:

Аппаратные (технические) средства — средства защиты информации и информационных систем, реализованные на аппаратном уровне. Эти устройства различны по типу устройства, но все они препятствуют доступу к данным, а так

же москтруют их. По типам устройств они делятся на механические (сигнализация, засовы, замки, решетки на стеклянном покрытии здания), элекромеханические (генераторы шума (ГШ), сетевые фильтры, сканирующие радиоприемники, устройство «Дух» и т.д.). Преимущества таких средств в надежности, высокой устойчивости к модернизации. Недостаток — недостаточная гибкость, сравнительно не маленький объем и вес, дороговизна.

Программные средства — программы для аутентификации сотрудников, СКУД, шифровка (дешифровка) данных, очистка временных файлов, и др. Преимущества данных средств — универсальность, гибкость, надежность, простота установки, способность к модификации и развитию. Недостатки — задействует часть ресурсов сервера и АРМ, достаточно высокая чувствительность к незначительным или преднамеренным внесениям изменений, некоторые из них не сопостовимы с «железом».

Так же можно пременить аппаратно-программные средства реализующие функции, аппкратных и програмных средств одновременно. В данных средствах реализуется полноценный комплекс СЗИ в пример этому можно привести крипто - маршрутизатор с функциями МСЭ.

Наиболее востребованными и распространеными в настоящее время являются программные СЗИ. Программные СЗИ классифицируются как:

Встроенные СЗИ в сетевых ОС. Данные подсистемы обеспечения безопасности при текущем развитии информационного рынка являются обязательными, но отличаются в зависимости от вида ОС, в каждой ОС они могут так или иначе отличаться, однако присутствуют в большинстве распространенных ОС. Примером данных подсистем являются:

Сетевые ОС, позволяющие осуществить «эшелонированную» защиту инфы от аппаратных сбоев и повреждений с помощью системы «System Fault Tolerance» (система устойчивости к отказам) компании Micro Focus (ранее известной ка Novell). В сетевой ОС присутствует кодирование информации по принципу так называемого «открытого ключа» (алгоритм RSA) с приминением

электронной подписи для транслируемых по сети пакетов. В ОС Linux фактическим стандартом служит система межсетевого экранирования Netfilter/IPTables. Еще одним не плохим механизмом является операция «chroot», она изменяет корневой каталог, таким образом программа запущенная с измененным котологом, не будет иметь доступ к другим каталогам. В ОС Windows, используются СЗИ такие как МСЭ он же «Брандмауэр Windows» служит для предотвращения, удаления и карантирования шпионского ПО в ОС Microsoft Windows.

Конечно для СЗИ лучше использовать специальное ПО оно обладает лучшими возможностями и характеристиками, чем встроенные средства ОС. Наиболие распространенными программными решениями СЗИ следует ометить:

Криптографические и шифровальные программы СЗИ. Шифрование представляет собой преобразование данных, делающее ее нечитаемой для посторонних лиц (неавторизованных в системе фирмы). В свою очередь авторизованным пользователям предоставляются права на чтение шифровонных данных согласно допуску данного пользователя. Так же при получении злоумышленником шифровонной информации он не сможет её дишифровать пока не получит ключ авторизации.

Firewalls – брандмауэр, МСЭ. Защищает локальную сеть от неавторизованного доступа из недоверенных сетей, он функцианирует на 3 (сетевом) уровне модели OSI (The Open Systems Interconnection model). Принцип работы заключается в фильтрации проходящего через него сетевого трафика в соответствии с задаными правилами. Чаще всего встречающееся разновидностью метода является «Маскарадинг (Masquerading)» заключающееся в динамической подстановке сетевого адреса отправителя. Метод характерен для маршрутизаторов «Cisco».

Прокси-сервер – промежуточный сервер между пользователем и серверами с которых запрашиваются данные. Из этого следует то, что обращения из глобальной сети в локальную в принципе становятся невозможными. Но такой метод не эфективен на более высоком уровне, такого как приложение.

VPN (Virtual Private Network «виртуальная частная сеть») позволяет со-

здавать тунелирование через которое можно передавать зашифрованную информацию, даже если трафик прослушивается злоумышлиниками. VPN работает по принципу шифрования трафика с осуществлением аутентификация удаленного хоста, так же они поддерживают протоколы используемые технологиями PPTP, PPPoE, IPSec. Таким образом соединение обеспечивается только между двумя клиентами.

Intrusion Detection System (IDS) - система обнаружения вторжений, выявляет несанкционированные и вредоносные активности в сети или на отдельном хосте. Intrusion Prevention System (IPS) - системы предотвращения вторжений. Система компьютерной и сетевой безопасности, обнаруживает вторжения или нарушения безопасности с возможностью последующей автоматической защитой от них. Для данных систем характерно обнаружение не всех атак, предпринимаемым к сетям, а так же ложные срабатывания.

2. РАЗРАБОТКА КОМПЛЕКСА МЕР ПО ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ИНФОРМАЦИИ

2.1 КОМПЛЕКС ОРГАНИЗАЦИОННЫХ МЕР ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЗАЩИТЫ ИНФОРМАЦИИ ПРЕДПРИЯТИЯ

2.1.1 НОРМАТИВНО-ПРАВОВАЯ ОСНОВА СОЗДАНИЯ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЗАЩИТЫ ИНФОРМАЦИИ ПРЕДПРИЯТИЯ

В РФ к НПА в области ИБ относятся:

Акты федерального законодательства:

Международные договора РФ;

- конституция РФ;
- законы федерального уровня;
- Указы Президента РФ;
- Постановления правительства РФ;
- НПА федеральных министерств и ведомств;
- НПА субъектов РФ, органов местного самоуправления и т. д.

К нормативно-методическим документам можно отнести

1. Методические документы государственных органов России:

- Доктрина ИБ РФ;
- Руководящие документы ФСТЭК;
- Приказы ФСБ России;

2. Стандарты ИБ, из которых выделяют:

- Международные стандарты;
- Государственные (национальные) стандарты РФ;
- Рекомендации по стандартизации;
- Метод рекомендации.

Самым главным документом, согласно которому предприятия разрабаты-

вают структуру защиты данных, относящихся к ограниченой информации, является Закон № 98-ФЗ «О коммерческой тайне» от 29 июля 2004 г. Закон предписывает, что коммерческая тайна – 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 (п. 1 ст. 3 Закона № 98-ФЗ).

Под разглашение информации, составляющей коммерческую тайну, согласно ФЗ понимается - действие или бездействие, в результате которых информация, составляющая коммерческую тайну, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору (п.1 ст.3 Закона № 98-ФЗ).

Так же в ст.5 Закона № 98-ФЗ присутствует перечень сведений , которые не могут составлять комерческую тайну. В соответствии с законом режим коммерческой тайны не может быть установлен лицами, осуществляющими предпринимательскую деятельность, в отношении следующих сведений:

1) содержащихся в учредительных документах юридического лица, документах, подтверждающих факт внесения записей о юридических лицах и об индивидуальных предпринимателях в соответствующие государственные реестры;

2) содержащихся в документах, дающих право на осуществление предпринимательской деятельности;

3) о составе имущества государственного или муниципального унитарного предприятия, государственного учреждения и об использовании ими средств соответствующих бюджетов;

4) о состоянии противопожарной безопасности, санитарно-эпидемиологической и радиационной обстановке, безопасности пищевых продуктов и других факторах, оказывающих негативное воздействие на обеспечение безопасного

функционирования производственных объектов, безопасности каждого гражданина и безопасности населения в целом;
(в ред. ФЗ от 09.03.2021 N 39-ФЗ)

5) о численности, о составе работников, о системе оплаты труда, об условиях труда, в том числе об охране труда, о показателях производственного травматизма и профессиональной заболеваемости, и о наличии свободных рабочих мест;

6) о задолженности работодателей по выплате заработной платы и социальным выплатам;
(в ред. ФЗ от 18.04.2018 N 86-ФЗ)

7) о нарушениях законодательства Российской Федерации и фактах привлечения к ответственности за совершение этих нарушений;

8) об условиях конкурсов или аукционов по приватизации объектов государственной или муниципальной собственности;

9) о размерах и структуре доходов некоммерческих организаций, о размерах и составе их имущества, об их расходах, о численности и об оплате труда их работников, об использовании безвозмездного труда граждан в деятельности некоммерческой организации;

10) о перечне лиц, имеющих право действовать без доверенности от имени юридического лица;

11) обязательность раскрытия которых или недопустимость ограничения доступа к которым установлена иными федеральными законами;

12) составляющих информацию о состоянии окружающей среды (экологическую информацию).
(п. 12 введен ФЗ от 09.03.2021 N 39-ФЗ)

Ст.10 Закон № 98-ФЗ «О коммерческой тайне» от 29.07.2004 г. Об «Охрана конфиденциальности информации» предписывается:

1. Меры по охране конфиденциальности информации, принимаемые ее обладателем, должны включать в себя:

1) определение перечня информации, составляющей коммерческую тайну;

2) ограничение доступа к информации, составляющей коммерческую тайну, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;

3) учет лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана;

4) регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;

5) нанесение на материальные носители, содержащие информацию, составляющую коммерческую тайну, или включение в состав реквизитов документов, содержащих такую информацию, грифа "Коммерческая тайна" с указанием обладателя такой информации (для юридических лиц - полное наименование и место нахождения, для индивидуальных предпринимателей - фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства).

(п. 5 в ред. Федерального закона от 11.07.2011 N 200-ФЗ)

2. Режим коммерческой тайны считается установленным после принятия обладателем информации, составляющей коммерческую тайну, мер, указанных в части 1 настоящей статьи.

3. Индивидуальный предприниматель, являющийся обладателем информации, составляющей коммерческую тайну, и не имеющий работников, с которыми заключены трудовые договоры, принимает меры по охране конфиденциальности информации, указанные в части 1 настоящей статьи, за исключением пунктов 1 и 2, а также положений пункта 4, касающихся регулирования трудовых отношений.

4. Наряду с мерами, указанными в части 1 настоящей статьи, обладатель информации, составляющей коммерческую тайну, вправе применять при необходимости средства и методы технической защиты конфиденциальности этой информации, другие не противоречащие законодательству Российской Федерации меры.

5. Меры по охране конфиденциальности информации признаются разумно достаточными, если:

1) исключается доступ к информации, составляющей коммерческую тайну, любых лиц без согласия ее обладателя;

2) обеспечивается возможность использования информации, составляющей коммерческую тайну, работниками и передачи ее контрагентам без нарушения режима коммерческой тайны.

6. Режим коммерческой тайны не может быть использован в целях, противоречащих требованиям защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

2.1.2 ОРГАНИЗАЦИОННО-АДМИНИСТРАТИВНАЯ ОСНОВА СОЗДАНИЯ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЗАЩИТЫ ИНФОРМАЦИИ ПРЕДПРИЯТИЯ

Организационно-административные меры защиты - это меры, согласно которым функционируют процессы автоматизированной системы обработки экономической информации (АСОЭИ), такие как, деятельности персонала, использование ресурсов, также предписывает порядок использования системы так, чтобы максимально эффективно застопорить или вовсе избежать возможности осуществления угроз ИБ.

Данные меры описывают процессы создания и эксплуатации информационных объектов, таким образом чтоб взаимодействие пользователя и системы исключало несанкционированный доступ к данным. Организационно-

административные способы защиты данных включают все без исключения элементы АИС в абсолютно всех стадиях их актуального цикла (проектирования систем, помещений и сооружений, постройки зданий, пусконаладочные работы, эксплуатации и модернизации систем). К организационно-административным событиям защиты данных соответствует:

- выделение специализированных защищенных помещений с целью размещения электронно-вычислительных машин (ЭВМ), а также средств связи и содержание носителей информации;
- категорирование специализированых АРМ для обработки сведений составляющих конфиденциальную информацию;
- организация хранения информации, составляющая конфиденциальный характер, на зарегистрированных МНИ;
- использование в работе с информацией, несущей конфиденциальный характер, ТС и ПС, имеющих соответствующии сертификаты безопасности и установленных в защищенных помещениях прошедших аттестацию;
- организация особого делопроизводства для установления порядка учёта, обработки, хранения, использования и уничтожения документированной информации конфедициального характера;
- организация соответствуещего права доступа сотрудников к работе на АРМ, средствах связи и к архивам с конфиденциальными данными;
- создание запрета на передачу конфедициальной информации с использованием открытых каналов связи;
- разработка, а также введение специализированных нормативно-правовых документов по реализации защиты информации конфедициального характера, регламентирующие деятельность всего объекта защиты в процессе манипуляций с информацией;
- регулярный контроль за соблюдением требований по защите данных.

После анализа действующей СБ было принято решение об реализации административных мер безопасности таких, как:

1) Создать и утвердить приказом по фирме:

- положение касательно защите сведений, в той или иной степени содержащих коммерческую тайну, и иных данных для ограниченного использования, предписанные законодательством РФ;

- список сведений, относящихся к коммерческой тайне;

- инструкцию по правилам работы со сведениями, содержащими коммерческую тайну;

- руководство по ведению, хранению и обработки информации ограниченного пользования.

2) Опубликовать приказ по фирме, которым:

- начальникам отделов поручить обязательство выполнения мероприятий, по обеспечению целостности и сохранности сведений составляющих коммерческую тайну;

- установить административное наказание за несоблюдение правил работы с информацией, относящейся к коммерческой тайне;

- СБ поручить мероприятия по выявлению нарушений, в следствии которых возможна утечка охраняемых данных.

3) Запретить на АРМ хранить информацию личного характера.

4) Установить правила размножения документации, недопускающих создание копий конфедициальных документов, без резолюции начальника.

5) При заключении трудового договора, по должности связвнной с ограничеными сведениями, брать письменные обязательства о неразглашении с сотрудников. А также в случае окончания трудовой деятельности сотрудником фирмы, востребовать от него сдачи всевозможных носителей информации, содержащих ограниченную информацию, выданные предприятием в его пользование.

6) Подготовить выдержки, содержащие положения об информации конфедициального характера с целью приминения их сотрудниками в обыденной работе;

7) Составить журнал учета индивидуальной информации;

8) Разработать принцип работы с почтовым ящиком.

9) При запуске АРМ, прежде чем будет введен пароль, автоматически выводить сообщение, напоминающее о правилах работы с АРМ.

2.2 КОМПЛЕКС ПРОЕКТИРУЕМЫХ ПРОГРАММНО-АППАРАТНЫХ СРЕДСТВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЗАЩИТЫ ИНФОРМАЦИИ ПРЕДПРИЯТИЯ

2.2.1 СТРУКТУРА ПРОГРАММНО-АППАРАТНОГО КОМПЛЕКСА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЗАЩИТЫ ИНФОРМАЦИИ ПРЕДПРИЯТИЯ

Для выполнения задачи по обеспечению ИБ, выбрана система КУБ. Система КУБ позволяет осуществлять тесную интеграцию технологий, процессов и людей, одновременно повышая доступность сервиса службы автоматизации и эффективность деятельности службы ИБ. Данная система позволяет реализовать механизм контролируемого и упорядоченного доступа к системе, в строгом соответствии с политикой ИБ.

Комплексный подход к решению трудностей позволяет решать задачи основных пользователей:

1. Бизнес-подразделения. Может легко обеспечить своевременный и необходимый доступ персонала отделов к ресурсам ИС, а также открыть свою информацию другим отделам для объединенной работы, сохраняя непрерывный контроль доступа к ним.

2. Служба информационных технологий/автоматизации. Помогает обеспечивать возможность своевременного внесения в ИС изменений, нужных для решения отделами задач, соответствующих положениям политики безопасности организации. При помощью данной системы унифицированное, приведенное к стандарту управление доступом сотрудников ко всем прикладным подсистемам ИС, доводящее до минимума вероятность конфликта со службой ИБ.

3. Служба ИБ. Получают возможность для мониторинга всех изменений в ИС и аудита функционирования ИС. С помощью системы КУБ они могут осуществлять проверку и согласование предложенных изменений в ИС на

корректность и соответствие требованиям политики безопасности.

Возможности КУБ

1. Управление:

− Электронный документооборот, осуществление электронной подписи, определяет порядок подписания документов.

− Основная модель управления.

− Автоматизированное создание модели ИС.

− Множество отчетов для разных подразделений.

2. Безопасность:

− Проверка на соответсвие, изменений в правах доступа, установленные политикой ИБ.

− Постоянный мониторинг контроля несанкционированных попыток изменения прав доступа.

− Согласованность управления в логическом и сетевом доступе.

− Позволяет управлять необходимыми цифровыми сертификатами и осуществлять контроль конфигурация программно-аппаратных средств.

3. Автоматизация:

− Динамическое создание маршрутов согласовывания заявок на внесение изменений прав доступа.

− Позволяет своевремено управлять учетными записями и вносить изменения в права доступа пользователей, согласно кадровым корректировкам.

− Автоматическое исполнение инструкций на изменение прав доступа.

При использовании системы КУБ процесс управления доступом представлен на рисунке 6.

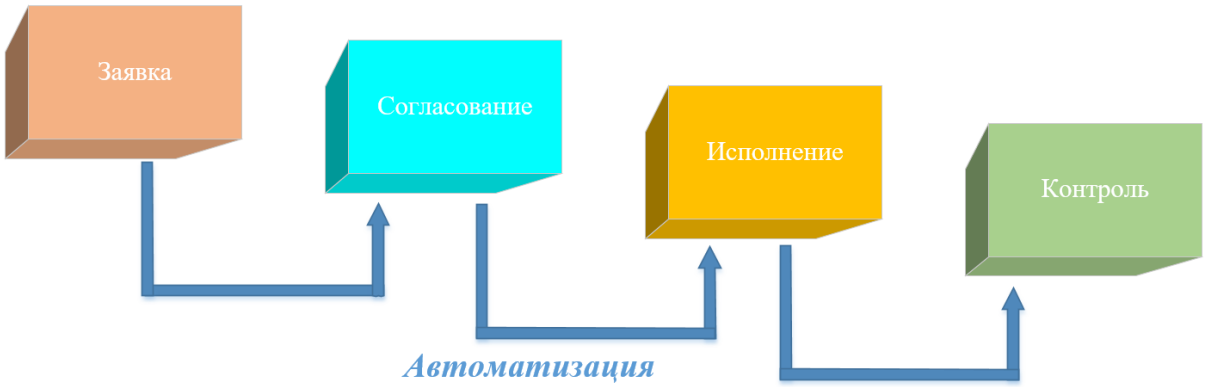


Рисунок 6. Процесс управления доступом

Эксплуатация системы КУБ дает возможность совокупно решать все проблемы, сопреженные с управлением доступом и учетными данными пользователей. При этом КУБ выполняет роль формирования и согласования заявок на доступ, а также реализацует и осуществляет контроль доступа. Непосредственноданные задачи считаются ключевыми для единого управления доступом.

Типовая архитектура решения задач управления доступом представлена на рисунке 7.

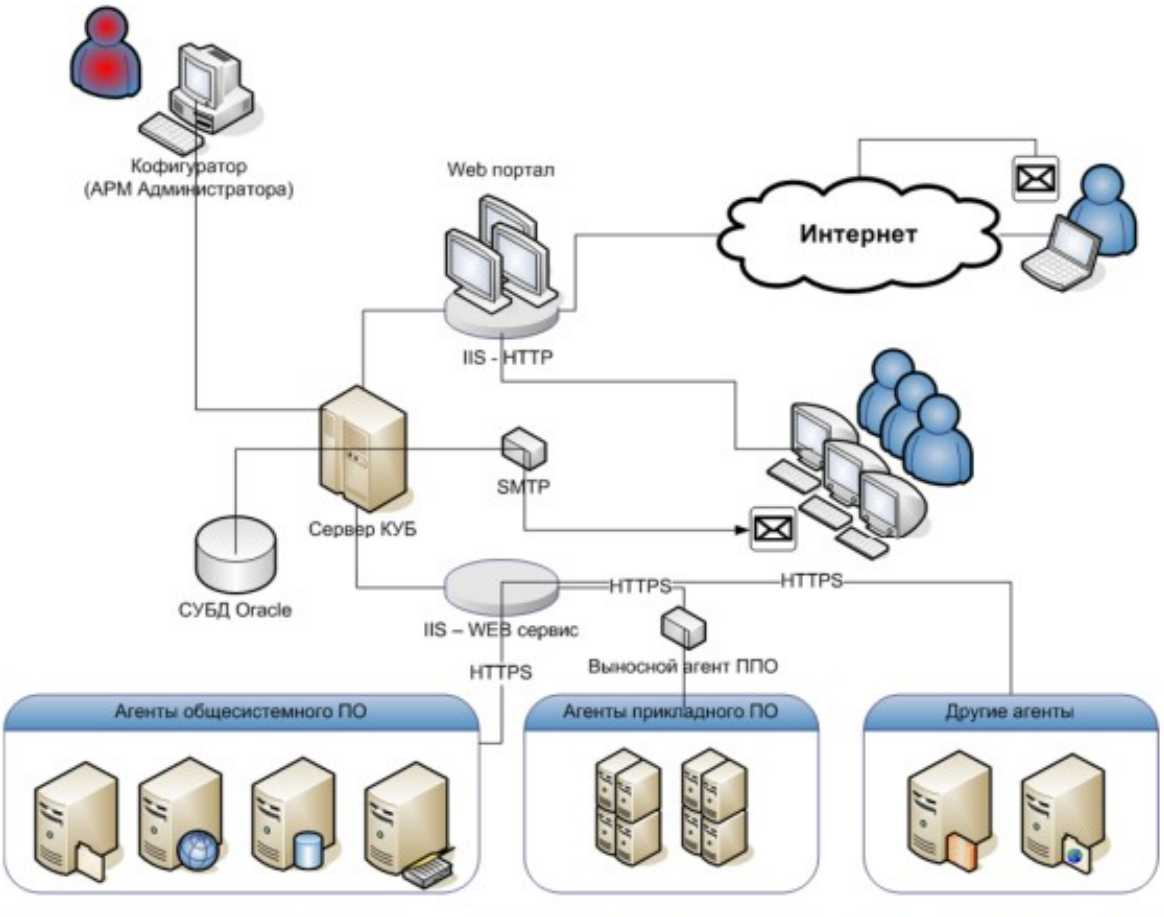


Рисунок 7. Типовая архитектура управления доступом

КУБ обладает преимуществами, приведенными далее:

1. Обеспечение безопасности. Это редкоповторимая система, целиком выполняющая задачу обеспечения ИБ фирмы в добавок к функциональности стандартной IDM. Данная система помимо управления логическим доступом, может обеспечивать управление и сетевым доступом, а также осуществлять контроль над цифровыми сертификатами конфигураций программно-аппаратных средств. Контроль над соответствием запрошенных реализованных прав доступа, данной системой осуществляется непрерывно.

2. Расследование инцидентов. При нарушении политики безопасноти фирмы, для эффективного и оперативного расследования предусмотренно полное хранение всех историй изменений прав пользователей. Также при помощи ЭЦП продуманна защита электронных заявок и проводимых с ними

операций.

3. Оптимизация технических ресурсов. Оперативность выявления несанкционированных изменений, заключается в логике работы информационных систем, которые в свою очередь заложены в процессе настройки. Так же оптемизирует работу IT-отделов, минимизирует ошибки зависящие от человеческого фактора так, как автоматически обрабатывает заявоки на изменение доступа.

4. Обучение и поддержка клиентов. По всем интересующим вопросам можно обратиться на горячую линию поддержки как по телефону так и по email. Так же в поставку системы КУБ входит подробная документация.

5. Развитие. Ситстема КУБ обладает гибкой архитектурой, которая позволяет интегрировать внешнии системы, обеспечивая широкие возможности по расширению функциональности.

По результатам аудита ИБ фирмы, были обнаружены недостатки в системе видеонаблюдения. По данным недостаткам были, предложены меры с целью увеличения продуктивности системы видеонаблюдения компании:

1. Обновить изжитые себя, видеокамеры.
2. Установить видеокамеры в кабинетах и на прилегающей к зданию территории.
3. Заменить монитора видеонаблюдения.
4. Установить сервер с видеонаблюдением в защищенное от несанкционированого доступа помещение.
5. Заменить ПО вывода видеосигнала.
6. Заменить устарелые кабеля .

Вследствии рекомендованных мероприятий, система видеонаблюдения фирмы будет модернизирована. Более подробное описание предложенных мероприятий преведено ниже.

1. Обновление видеокамер.

Нормативный срок полезного использования для видеокамер составляет 5

лет. На фирме установлены камеры производства «Mintron», согласно документации об установке систем видеонаблюдения, данные камеры были закуплены на вторичном рынке. Таким образом можно сделать вывод что срок использования видеокамерами составляет более 5 лет, так как они могли использоваться ранее и неизвестно как долго.

После анализа рынка было принято решение выбрать камеры видеонаблюдения серии DS-T201. Данные видеокамеры обеспечивают качественную съёмку с записью 25 кадров в секунду.

2. Установка камер в помещениях.

Камеры серии DS-T201 имеют высокое разрешение и повышенную чувствительность. Данная модель камеры показала себя как весьма надежная и неприхотливая. Данная камера предоставляет довольно таки четкое и контрастное изображение с углом обзора в 103˚, имеет не большие габариты. Изготовитель «Hangzhou Hikvsion Digital Techology CO., Ltв» (Китай).

3. Выбор видеокамер наблюдения за прилегающей территорией.

Для выбора камер за наблюдением прилегающего периметра необходимо решить следубщие проблемы.

- Защита камер от воздействия внешней среды.

- Повышение информативности при наблюдении за въездом на территорию фирмы.

Для устойчивости камер от низких температур, различных осадков и т.д. возможно использование специальных кожухов, либо преобретение камер предусматривающих условия эксплуатации.

Для реализации видеонаблюдения за прилегающей территорией фирмы были выбраны камеры Для этого были выбраны камеры HiWatch DS-I250L. Цветная видеокамера с защитой от влаги и пыли по IP67, диапазон рабочих температур от -40°C до +60°C, угол обзора 107°, запись 30 кадр./сек

Данная камера установлены по всему периметру здания, а так же на против шлагбаума для распознования госномеров автотранспортных средств. Она позволяет получать четкое изображение объекта, обладает высокой степенью

надежности и небольшими габаритами.

4. Замена монитора видеооператоров.

Для комфортного наблюдения за общей обстановкой через камеры наружнего и внутреобъектового видеонаблюдения следует установить улучшенный монитор.

Выбирая тип монитора следует отдать предпочтение мониторам с повышеной частотой обновления. В современных моделях мониторов, используемых для систем наблюдения, величина этого параметра варьируется в пределах от 82 до 100 Гц. Меньшие значения этой характеристики будут приводить к более быстрой утомляемости глаз.

Для выбора монитора так же делался упор на его диагональ и разрешение. Чем выше эти показатели, тем четче и качественней будет картинка, для просмотра. Выбирая диагональ монитора можно следовать правилу приведенному ниже:

- 15″ – для систем с количеством камер 1-2;
- 17″ – для систем, которые имеют 4 камеры;
- от 19″ до 22″ – для систем, имеющих от 4 до 9 камер;
- от 22″ до 40″ – для систем с 16-ю камерами;
- от 32″ и больше – для систем, имеющих до 20-ти камер.

5. Замена соединительного кабеля.

Состояние кабеля связывающего элементы системы видеонаблюдения оценивается, как неудовлетворительное. Всвязи с этим велик риск искажений и потерь в качестве передоваемой картинки. При замене было решено испоьзовать обыкновенный коаксиальный кабель с волновым сопротивлением 75 Ом. От качества кабеля зависит и выводимое изображение, но также стоит обратить внимание , что удаленность расположения видеокамер от поста наблюдения не должна привышать 200-300 метров. Если растояние будет большим, то необходимо устанавливать магистральные видеоуселители, для компенсации потерь. При этом данные уселители следует устанавливать как можно ближе к камерам, для повышения отношения сигнал/шум.

Большинство кабинетов фирмы имеют прямоугольную форму. И по этому принято решение устанавливать по две камеры на кабинет, на противоположных стенках, для избегания так называемых «мертвых зон». Схема расположения камер приведена на рисунке 8.

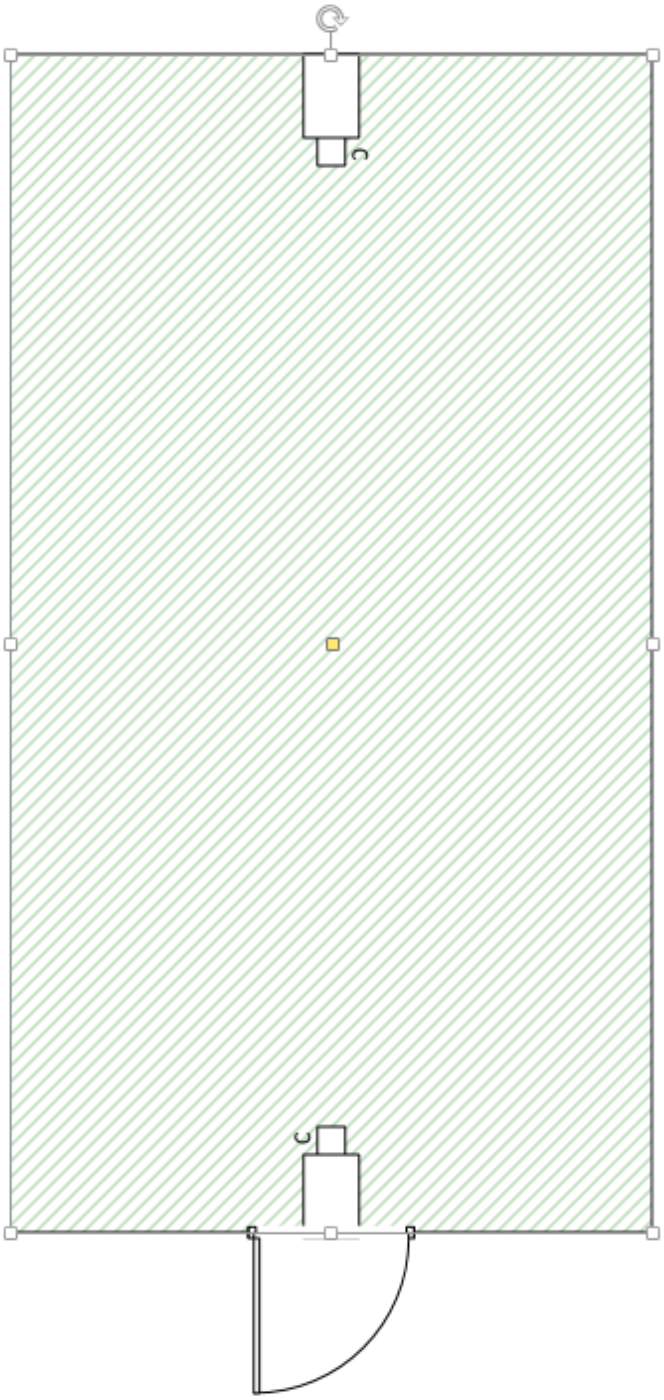


Рис. 8. Встречное расположение камер

Данное расположение камер, позволяет делать дублирование, а так же с

помощью камеры на против появляется возможность возможность просматривать ближнюю зону этой камеры, тем самым ликвидируются «мертвые зоны».

Вместе с этим видеосервер будет находится в режимном помещении, там же будут находится и органы управления. Монитор для просмотра видеокамер будет дублироваться и выведен на пункт охраны.

С целью недопущения несанкционированного доступа к АРМ пользователей рационально установить СЗИ Secret Net LSP. Данное СЗИ соответствует требованиям ФСТЭК России в результате чего минимизирует финансовые и репутационные риски, связанные с невыполнением требований регуляторов, а также проводит ИС в соответствие с требованиями нормативных документов. И имеет сертификацию с возможностью применяться:

- 5-й класс защищенности СВТ
- 4-й класс защиты МЭ типа «В»
- 4-й уровень доверия
- Применяется для защиты значимых объектов КИИ 1 категории, ИМПДН до У31, ГИС до К1 и АСУ ТП до К1 включительно

Комплектация СЗИ Secret Net LSP-С имеет сертификацию:

- 2-й уровень контроля отсутствия НДВ
- Технические условия
- Применяется для защиты АС, обрабатывающих государственную тайну до уровня «Совершенно секретно»

СЗИ Secret Net LSP вместе с ОС Windows гарантируе идентификацию и аутентификацию пользователя, контролируя вход пользователя в систему по логину/паролю, либо с использованием электронных идентификаторов.

Разгроничение доступа к ресурсам происходит по средствам механизма дискреционного разграничения доступа для контроля и управления правами доступа пользователей и групп пользователей к объектам файловой системы – файлам и каталогам, а так же реализует МСЭ уровня узла.

СЗИ Secret Net LSP контролирует целостность критических объектов файловой системы. Также контролирует замкнутую программную среду, по

средствам настройки режимов реакции на нарушенияцелостности объектов, запрещает запук модулей, явно не разрешенных администратором ИБ.

Контролю могут подлежать файлы, каталоги, элементы реестра ОС и секторы дисков. Соответственно каждый тип перечисленных ранее объектов имеет индивидуальный набор контролируемых конфигураций. При обнаружении несоответствия контралируемых конфигураций на целостность содержимого, прав доступа, а также на существование файлов по задонному пути, существует несколько вариантов развития событий, а именно:

- регистрация журнале Secret Net LSP данных событий;
- блокировка АРМ;
- возвращение к надлежащему виду повреждённой/измененной информации;
- отказать в приминение либо принять изменения.

Система Secret Net LSP записывает все события, происходящие на компьютере: от включения АРМ до вывода информации ограниченого доступа на бумажные либо отчуждаемые носители информации.

В фирме обоснованно требуется использование МСЭ, который разграничивает зоны на сети с обработкой информации конфиденциального характера, обработку и содержанием персонифицированными данными персонала, а также информации открытого характера.

Для реализации МСЭ прекрасно подойдет МСЭ ССПТ-2 производства ЗАО «НПО РТК». Данный МСЭ отвечает требованиям современных стандартов безопасности для устройств 3-го класса защиты и имеют сертификаты ФСБ России № СФ/СЗИ-0369.

МСЭ ССПТ-2 реализует функции контроля и разграничения доступа в компьютерных сетях, оставаясь при этом «прозрачным» для обрабатываемого трафика и любых тестовых воздействий. Это достигается за счет отсутствия физических и логических адресов на его фильтрующих интерфейсах (решение защищено патентами РФ 2214623, US 7281129). Скрытность функционирования

межсетевого экрана повышает надежность системы защиты в целом, значительно упрощает процедуру установки ССПТ-2 в существующие компьютерные сети и функционирующие на их основе информационные и телематические системы.

Данный МСЭ имеет следующии функциональные характеристики:

- Многоуровневая скрытная фильтрация пакетов по совокупности критериев.
- Контроль виртуальных соединений (одновременно до 40000 сессий) на основе проверки соответствия каждого пакета контексту сессии.
- Трансляция сетевых адресов (режим NAT) в режиме «стелс» для сокрытия структуры внутренней сети с выделением «демилитаризованной зоны».
- Блокировка компьютерных flood-атак на основе фильтрации аномальной активности сетевых потоков данных.
- Регистрация системных событий и полных заголовков обработанных пакетов на всех уровнях межсетевого взаимодействия.
- Ведение журналов регистрации пакетов и их выгрузка по запросам администратора сети с использованием протоколов FTP и SYSlog.
- Аутентификация и авторизация администратора с помощью протокола RADIUS.
- Контроль доступа к интерфейсу управления на основе списка доверенных сетевых адресов.
- Синхронизация системного времени по протоколу NTP.

Для оперативного востановления как самих данных так и програм, после выхода из строя АРМ либо сервера, необходимо иметь резервные копии, создоваемые средствами резервного копирования.

Резервное копирование (РК) – процесс создания и хранения копий данных на не учавствующем в ежедневных процессах носителях, предназначенных для восстановления данных в оригинальном, либо же новом месте их расположения в случае их повреждения или разрушения.

Для реализации данного решения прекрасно подойдет Veritas Backup Exec 16, данный продукт утсанавливается на серверное оборудование и администрируется администратором системы. С помощью данного ПО возможна настройка планового РК для компьютеров по управление Windows, находящихся в сети.

Данное решение сводится к уменьшению круга лиц, имеющих доступ к резервным копиям, так как все администрирование происходит удаленно администратором системы.

Для хранения резервных копий используется сервер в сегменте сети с ограниченым доступом, запуск служб РК осуществляется из под специального пользователя служб и приложений, у данного пользователя имеется ряд ограничений одним из них является запрет на авторизацию в системе как обыкновенный пользователь, тем самым исключая противоправные действия под данным пользователем

От сервера, предназначенного для хранения РК, не требуется высокой показателей производительности, первостепенным требованием является сравнительно большой объем дискового пространства, из расчета по 300-500 Гб на один АРМ, в зависимости от хранимой информации на самом АРМ.

Администратор системы самостоятельно настраивает расписание РК. На основе календаря он может легко запланировать обработку операций РК в часы пониженной нагрузки. Управление контрольными точками резервирования и дисковым пространством, выделенным под резервные копии, происходит автоматически.

Администратор обязан постоянно контролировать ход РК, по средствам просмотра отчетов по результатам завершения РК. Следить за состоянием резервных архивов.

2.2.2 КОНТРОЛЬНЫЙ ПРИМЕР РЕАЛИЗАЦИИ ПРОЕКТА И ЕГО

ОПИСАНИЕ

После проведенного аудита ИБ на фирме, выявлены некоторые проблемы и рассчитан средний риск по всем объектам защиты, который составил 25,1 %. Однако самый высокий показатель риска уязвимости принадлежит АРМ пользователя – 74%. Данные результаты привели к определенным мероприятиям по обеспечению ИБ.

Исходя из вышесказанного, в ходе ВКР была разработана определенная система мер для обеспечения ИБ фирмы:

I. Технические

1. Аппаратные:
   1) Закупить ИБП для сервера и АРМ пользователей.
   2) Дополнительно установить видеокамеры.
   3) Закупить металлические шкафы и сейфы для хранения документации с ограниченым доступом.

2. Программные:
   1) Установить систему КУБ.
   2) Установить программное средство Secret Net LSP.
   3) Переустановить антивирусную систему по принципу, на сервере устанавливается серверная часть антивирусной программы, далее создаем задачи для установки АПО на клиентские АРМ, так же все БД будут обновляться централизованно с сервера, в то же время администратор сможет управлять и мониторить всеми АРМ сотрудников.
   4) Переработать политику паролей. Требовать смены пароля пользователем раз в месяц с набором определенных символов.
   5) Настроить разграничение прав пользователей к информации хранящейся на сервере;

Так же обязать работников дать письменное согласие об соглашении с правилами работы на местах, в частности с информацией и АРМ, провести

дополнительные инструктажи. В дальнейшем включить эти пункты в трудовой договор или дополнительное соглашение.

После данных мероприятий выполним перерасчет рисков ИБ после внедрения приведенных выше мер.

1. Объект защиты –АРМ пользователя. Критерий критичности (D) равен 49 347рублей.

Однако надо принять во внимание, что для защиты АРМ пользователя были предприняты меры:

− Установка параметров автоматической блокировки компьютера в режиме бездействия более чем 10 минут.

− Замена старых и закупка новых видеокамер, с последующим монтажем и подключением к системе видеонаблюдения.

− Переодичная смена пароля, по определенным критериям сложности.

− Установка АПО и их активация.

− Рекомендации по работе с ПО и АРМ пользователя, а также отключение USB-портов.

− Создание групповых политик для ограничения прав пользователей.

После проведения данных мероприятий, таблица угроз и уязвимостей выглядит иначе, результаты приведены в таблице 19.

Таблица 19

Таблица угроз и уязвимостей после проведения мероприятий.

Угроза	**Уязвимости**	**Мероприятия**
1.Физический доступ нарушителя к АРМ	1. Отсутствие системы контроля доступа служащих к чужим АРМ (оставление компьютера без присмотра в не заблокированном виде)	Установка параметров автоматической блокировки компьютера в режиме бездействия более чем 10 минут.
	2.Отсутствие видеонаблюдения в кабинетах (имеется только в серверном помещении)	Замена старых и закупка новых видеокамер, с последующим монтажем и подключением к системе видеонаблюдения.
	3.Отсутствие алгоритма смены паролей	Переодичная смена пароля, по

		определенным критериям сложности.
2.Сбои в работе АРМ	1. Отсутствие АПО на АРМ	Установка АПО и их активация.
	2. Человеческий фактор	Рекомендации по работе с ПО и АРМ пользователя, а также отключение USB-портов.
3.Разрушение конф. информации при помощи специальных программ и вирусов	1.Отсутствие АПО на АРМ	Установка АПО и их активация.
	2.Не ограниченый доступ сотрудников к внешней среде	Создание групповых политик для ограничения прав пользователей.

Таблица вероятности реализации данной угрозы через уязвимость в течение года(P(V)) и критичности реализации угрозы (ER). После проведенных мероприятий по обеспечению ИБ снизится вероятность возникновения угроз, данные приведены в таблице 20.

Таблица 20

Таблица вероятности реализации угрозы

Угроза/уязвимость	P(V), %	ER,%
1/1	0	50
1/2	0	50
1/3	0	90
2/1	1	80
2/2	5	20
3/1	1	80
3/2	0	60

Таблица уровня угрозы по некой уязвимости (Th) и по уровню угроз по всем уязвимостям (CTh).

На основе данной таблицы необходимо рассчитать уровень угроз по каждой уязвимости. Эти значения помогут оценить, какие уязвимости наиболее вероятны, а также рассчитать общее значение уязвимости ресурса.

Таблица 21

Таблица уровня угрозы

Угроза/уязвимость	Th	CTh
1/1	-	0
1/2	-	
1/3	-	
2/1	0,01	0,018
2/2	0,01	
3/1	0,01	0,008
3/2	-	

Th=P(V)/100*ER/100

CTh=1-П(1-Th)

Рассчитаем общий уровень угроз по ресурсу:

CThR=1-П(1-CTh)=0,026

Рассчитаем риск по ресурсу:

R= CThR*D=0,026*49 347=1 283, 02 (руб.).

Всвязи с этим, уровень риска снизится и будет составлять 2,6% и потери в год упадут на 35 233, 76 руб.

Эффективность проведенных мероприятий рассчитывается по формуле:

$$E = \frac{R_{old} - R_{new}}{R_{old}}$$

В нашем случает она равна 97%.

2. Объект защиты – локальный сервер.

Таблица угроз и уязвимостей после проведенных мероприятий.

Таблица 22

Таблица угроз и уязвимостей

Угроза	Уязвимости	Контрмеры
1.Разглашение, уничтожение или разглашение КИ, хранящейся на сервере	1. Доступ к информации с АРМ	Создание групповых политик для ограничения прав пользователей.
	2. Наличие удаленного доступа	Создание групповых политик для ограничения прав пользователей.
2.Выход сервера из строя	1.Большое количество подключений	Обновление конфигураций сервера сервера.
	2.Сбои электричества	Создание групповых политик для ограничения прав пользователей.

Таблица вероятности реализации данной угрозы через уязвимость в течение года(P(V) и критичности реализации угрозы (ER).

Таблица 23

Таблица вероятности реализации угрозы

Угроза/уязвимость	P(V), %	ER,%
1/1	0	60
1/2	5	20
2/1	0	20
2/2	0	40

Таблица уровня угрозы по определённой уязвимости (Th) и по уровню угроз по всем уязвимостям (CTh).

Таблица 24

Таблица уровня угрозы по определённой уязвимости

Угроза/уязвимость	Th	CTh
1/1	-	0,01
1/2	0,01	
2/1	-	0
2/2	-	

Th=P(V)/100*ER/100 CTh=1-П(1-Th)

Рассчитаем общий уровень угроз по ресурсу:

CThR=1-П(1-CTh)= 0,01

Рассчитаем риск по ресурсу:

R=CTh*D=0,01*1 040 800= 10 408 (руб.).

Всвязи с этим, уровень риска снизится и будет составлять 1%, экономия в год на 146 752, 13 руб., эффективность контрмер – 93,4%.

3. ОБОСНОВАНИЕ ЭКОНОМИЧЕСКОЙ ЭФФЕКТИВНОСТИ ПРОЕКТА

3.1 ВЫБОР И ОБОСНОВАНИЕ МЕТОДИКИ РАСЧЁТА ЭКОНОМИЧЕСКОЙ ЭФФЕКТИВНОСТИ

Экономическая эффективность – эффективность, расчитанная основании полученных результатов производства труда, деятельности сотрудников и затрат труда, средств на производство.

«Результаты» и «затраты» являются немаловажными понятиями, они связанны с определением экономической эффективности инвестиционных проектов.

Результаты отображают определенные глобальные задачи, которые необходимо решить в инвестиционном проекте, при помощи которых достичь основной цели экономического развития. Результаты непосредственно зависят от поставленных целей и задач инвесторами. В инвестиционной разработке доводится иметь дело как с экономическими, так и внеэкономическими результатами.

Для достижения определенных целей и ожидаемых результатов в проекте подразумевается затраты, они могут быть, как текущими, так и единовременными.

Единовременные затраты на две группы, первая это затраты которые в конечном счете суммирутся в основном капитале (закупка оборудования, ТС, приобритение и строительство зданий и сооружений), вторая группа входит в состав оборотного капитала (запасы комплектующих, незавершенное производство и т.п.).

Текущие затраты в свою очередь будут формировать себестоимость услуг и продукции.

Разница оценок результатов и расходов сформировывают эффект, по которому можно судить, что получит инвестор в следствии реализации плана.

Эффект по сути представляется двумя выражениями:

1) Разность между суммарного результата и суммарных затрат.

2) Разность между суммарных результатов и только текущих издержек.

Эффективность – позволяет увидить (просчитать) соотношение затрат на ресурсы с достигнутым результатом.

Эффективность инвестиционного проекта определяется с целью решения некоторых задач:

1) просчет возможной рентабельности реализации проекта, т.е. просчитать как суммарные результаты превосходят все произведенные затраты инвесторов;

2) анализ преимуществ проекта в сравнении с иными проектами;

3) ранжирование проектов по показателям эффективности, так как при условии ограничения финансовых и других ресурсов, проекты необходимо внести в инвестиционную программу.

Срок окупаемости – промежуток времени от момента начала инвистирования проекта до момента, когда доход (или прыбль) от реализации проекта превысит единовременные капитальные вложения в проект. Данное значение определяется последовательным вычислением чистого дохода для каждого этапа проекта. Точка, в которой PV примет положительное значение, будет являться точкой окупаемости.

При расчете дисконтированного срока окупаемости проекта могут быть применены такие понятия как:

- DPBP (англ. Discounted Pay-Back Period);
- DPB (англ. Discounted Pay-Back).

PBP рассчитывается по формуле:

$$PBP = \frac{\text{Инвестиции}}{\text{Денежный поток за еденичный период + амортизация}}$$

Окупаемость капитальных вложений, один из показателей эффективности капитальных вложений, их отношение к экономическому эффекту, получаемому благодаря данным инвестициям.

Период окупаемости можно рассчитывается пблагодоря формуле:

$$T_{ОК} = \frac{КЗ_А}{Э_М} \quad (1)$$

где $Т_{ОК}$ – период окупаемости (мес.);

$КЗ_А$ – капитальные затраты автоматизации;

$Э_М$ – месячная экономия.

Капитальные затраты автоматизации вычисляются по формуле:

$$КЗ_А = Ц_{ПО} + К_{ТЕХ} + К_{РМ} + К_{ПР} + К_Н \quad (2)$$

где $Ц_{ПО}$ – капитальные затраты на закупку ПО;

$К_{ТЕХ}$ – капитальные затраты на закупку технического оснащения;

$К_{РМ}$ – капитальные затраты на формирование рабочего места сотрудника;

$К_{ПР}$ – капитальные затраты на закупку (приобритение) и установку ПО;

$К_Н$ – капитальные затраты на настройку ПО.

$$Э_М = З_{АВТ(ДО)} - З_{АВТ(ПОСЛЕ)} \quad (3)$$

3.2 ПРЕДВАРИТЕЛЬНЫЙ РАСЧЕТ ЭКОНОМИЧЕСКОЙ ЭФФЕКТИВНОСТИ И ОКУПАЕМОСТИ

Очевидным предположением экономической эффективности является то, что с одной стороны, при уязвимости защищенности данных причиняется некий ущерб, со второй - защита информации связанна с расходом денежных средств. Общую планируемую стоимость защиты можно представить суммой

расходов денежных средст на защиту и потерь от нарушения данной защиты.

Из этого следуют очивидные выводы:

- минимизировать общую стоимость выполненных работ по защите данных;
- определение экономической эффективности мероприятий по обеспечению защиты данных следует через объем предотвращенного ущерба или величину понижения риска для информационных активов фирмы.

Для реализации данного подхода к решению проблемы требуется определять или знать:

1) планируемые потери при несакционированном доступе к защищаемой информации;
2) зависимость между уровнем защищенности и средствами, затрачиваемыми на защиту информации.

При определении уровня затрат ROI (Return ON Investment) предостовляющих необходимый уровень защищенности данных, надо знать:

1) максимально полный список информационных угроз;
2) для защищаемой информации проанализировать каждую из угроз;
3) затраты, которые понадобятся для реализации защиты от каждой из угроз.

Целесообразный уровень затрат на защиту информации состоит в том, что данный уровень должен быть приравнен к уровню ожидаемых потерь при нарушении защиты, Вполне достаточно рассчитать уровень потерь. Данный уровень потерь по каждому объекту защиты, оценивался в пункте 1.2. Имеющиеся данные сведены в таблицу 25.

Таблица 25.

Величина рисков для критичных информационных данных до модернизации СЗИ

Актив	Угроза	Величина потерь (руб.)
Утрата конфиденциальности	Персональные данные персонала	50 000
Утрата конфиденциальности	Данные о проделанной работе	100 000
Утрата доступности, целостности	Документация фирмы (Устав, Положения, Локальные акты)	20 000
Утрата доступности, целостности	Перечень дополнительных услуг	10 000
Утрата целостности	Отчетность фирмы	500 000
Нарушение целостности	ПО	300 000
Утрата доступности	Техническая оснащенность	450 000
Итого:		1 680 000

Исходя из этого общий объём прогнозиру емых потерь, от выполнения угроз ИБ составляет 1 680 000 тыс. руб.

Выполним рассчёт затрат на внедрение СЗИ. Некоторые предложенные мероприятия реализуются с помощью действующих сотрудников согласно их служебному регламенту и не потребуют дополнительных финансовых затрат. Служба безопасности и IT-подразделения осуществлят следующие работы:

- подключение и настройку к системе видеонаблюдения камер;
- разграничат права доступа пользователей;
- разработают политику доступа на внешнии ресурсы;
- разработают порядок работы с информацией конфиденциального характера.

От уровня инженерно-технической защиты информации, зависит риск владельца информации, который в свою очередь, определяется ресурсами системы.

Выделяемый ресурс на защиту данных, имеет разовый и постоянный характер.

Разовый тратится на закупку, установку и настройку дорогостоящего оборудования.

Постоянный, на заработную плату сотрудников и поддержание установленного уровня безопасности, как показывает практика, путем эксплуатации ТС и контроля эффективности защиты.

Данные, необходимые для определения экономической эффективности СЗИ фирмы:

- расходы на модернизацию (в нашем случае) текущей системы и поддержание её в надлежащем состоянии;
- величина рисков, определенных угрозами информационным активам после модернизации СЗИ;

Таблица 26

Содержание и объем разового ресурса, затрачиваемого на защиту информации

Организационные мероприятия				
№ п\п	**Выполняемые действия**	**Среднечасовая зарплата специалиста (руб./час)**	**Трудоемкость операции (чел.час)**	**Стоимость, всего (тыс.руб.)**
1	Доставка технических средств	500	10	5
2	Установка технических средств	435	120	52,2
Стоимость проведения организационных мероприятий, всего				57,2
Мероприятия инженерно-технической защиты				
№ п/п	Номенклатура ПиАСИБ, расходных материалов	Стоимость, единицы (тыс.руб)	Кол-во (ед.измерения)	Стоимость, всего (тыс.руб.)
1	Монитор видеонаблюдения	14	4	56
2	Видеокамера DS-T201	2,41	7	16,87
3	Видеокамера DS-I250L	5,22	5	26,1
7	Коаксиальный кабель (м)	0,3	200	60
Стоимость проведения мероприятий				158,97
Объем разового ресурса, выделяемого на защиту информации				216,17

Всвязи с тем, что в фирме трудятся сотрудники обеспечивающие ИБ, выделение средств по статье постоянног ресурса не требуется.

Суммарные затраты выделяемые на защиту данных составили 216 170 руб.

Предложенная СЗИ экономически эффективна, т.к. потраченные ресурсы и финансы на ее осуществление существенно ниже, чем потери от угроз ИБ. После модернизации СЗИ прогназируемые суммы потерь приведены в таблице 27.

Таблица 27

Величины рисков для критичных информационных ресурсов после модернизации СЗИ

Актив	Угроза	Величина потерь (руб.)
Утрата конфиденциальности	Персональные данные персонала	40 000
Утрата конфиденциальности	Данные о проделанной работе	85 000
Утрата доступности, целостности	Документация фирмы (Устав, Положения, Локальные акты)	5 000
Утрата доступности, целостности	Перечень дополнительных услуг	5 000
Утрата целостности	Отчетность фирмы	450 000
Нарушение целостности	ПО	250 000
Утрата доступности	Техническая оснащенность	410 000
Итого:		1 245 000

После проведенных мероприятий можно расчитать срок окупаемости СЗИ ($Т_{ок}$). Выполняется аналитическим путём, с использованием формулы:

$$Т_{ок} = R_{\sum} / (R_{ср} - R_{прогн})$$

$$Т_{ок} = \frac{216170}{(1680000 - 1245000)} = 0{,}49 \text{ года} = 5 \text{ мес.}$$

Это также выполняется графическим способом, как это представлено на рис. 9.

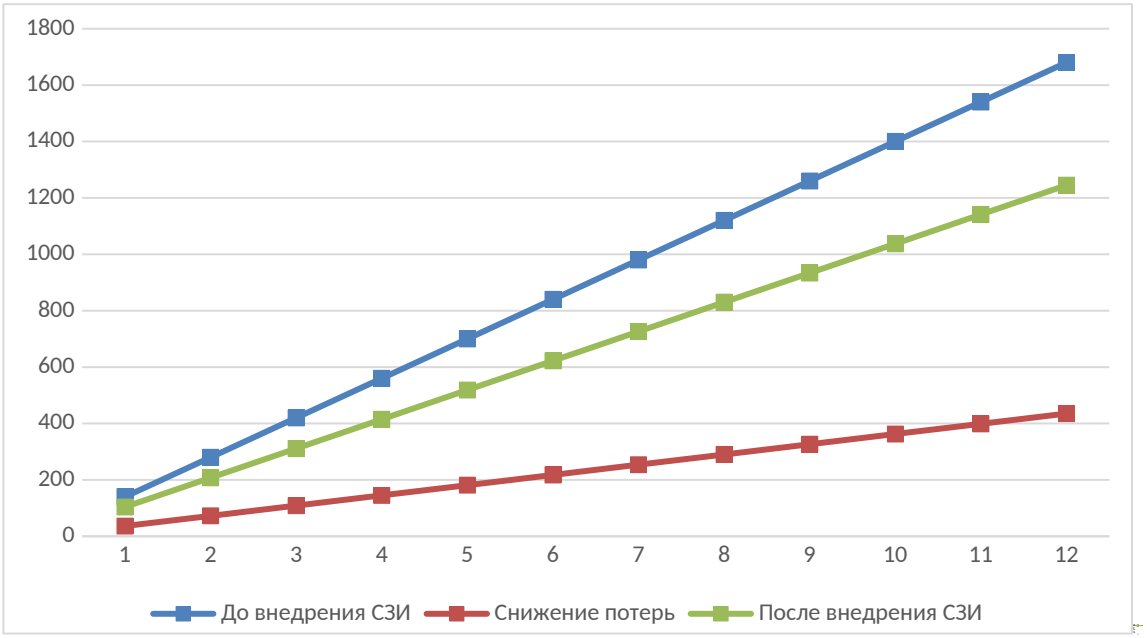


Рис. 9. Динамика потерь

Срок окупаемости проекта составит менее полугода (около 5 месяцев). Таким образом, предложенные средства защиты очень эффективны.

ЗАКЛЮЧЕНИЕ

Внедрение СИБ окажется результативным, если будет поддерживаться надёжное соблюдение политик безопасости. Основная цель создания политики безопасности системы и описания ее в виде формальной модели — это определение условий, которым должно подчиняться поведение системы, выработка критерия безопасности и проведение формального доказательства соответствия системы этому критерию при соблюдении установленных правил и ограничений.

Первоочередными мерами обеспечения сохранности коммерческой тайны являются правовые, данные меры должны обеспечить гаррантирванное функционирование предпринятых мер, для обеспечения сохранения информацтт конфедициального характера. С данной точки зрения по отношению к остальным мерам правовые меры являются основными.

Вся документация проходит согласование с юридическим подразделением фирмы, а также утверждается начальством и вводится в действие приказом по фирме. Также учитывается, соответствие документов законам и НПА и документам РФ в данной области, в связи с тем, что к сотрудникам фирмы применяются определенные ограничения, а также ложится ответственность, вплоть до уголовной за нарушение правил работы с ддокументами относящимися к комерческой тайне.

В фирме подразумевается внедрение системы КУБ. Данная система позволяет комплексно решить все задачи, связанные с управлением доступом и учетными данными пользователей. А также осуществляет роль в формировании заявок на доступ, реализацию и контроль доступа. Тем самым реализуя ключевые задачи для комплексного управления доступом.

В результате аудита фирмы предложен проект усовершенствования существующей системы видеонаблюдения. Усовершенствованная система реализует основательную защиту фирмы от несанкционированного доступа и целиком соответствует условиям систем безопасности в сфере видеонаблюдения. При

подборе ТС внимательно изучались характеристики и совместимость оборудования. Данная система соответствует требованиям ТЗ и готова к внедрению в фирме.

Таким образом, в ВКР были предложены меры по СЗИ, позволяющие избежать рисков и потерь. Затраты на реализацию мер составляют 1 455 000 рублей. Данная система принятия мер по обеспечению ИБ оправдает себя через 5 лет.

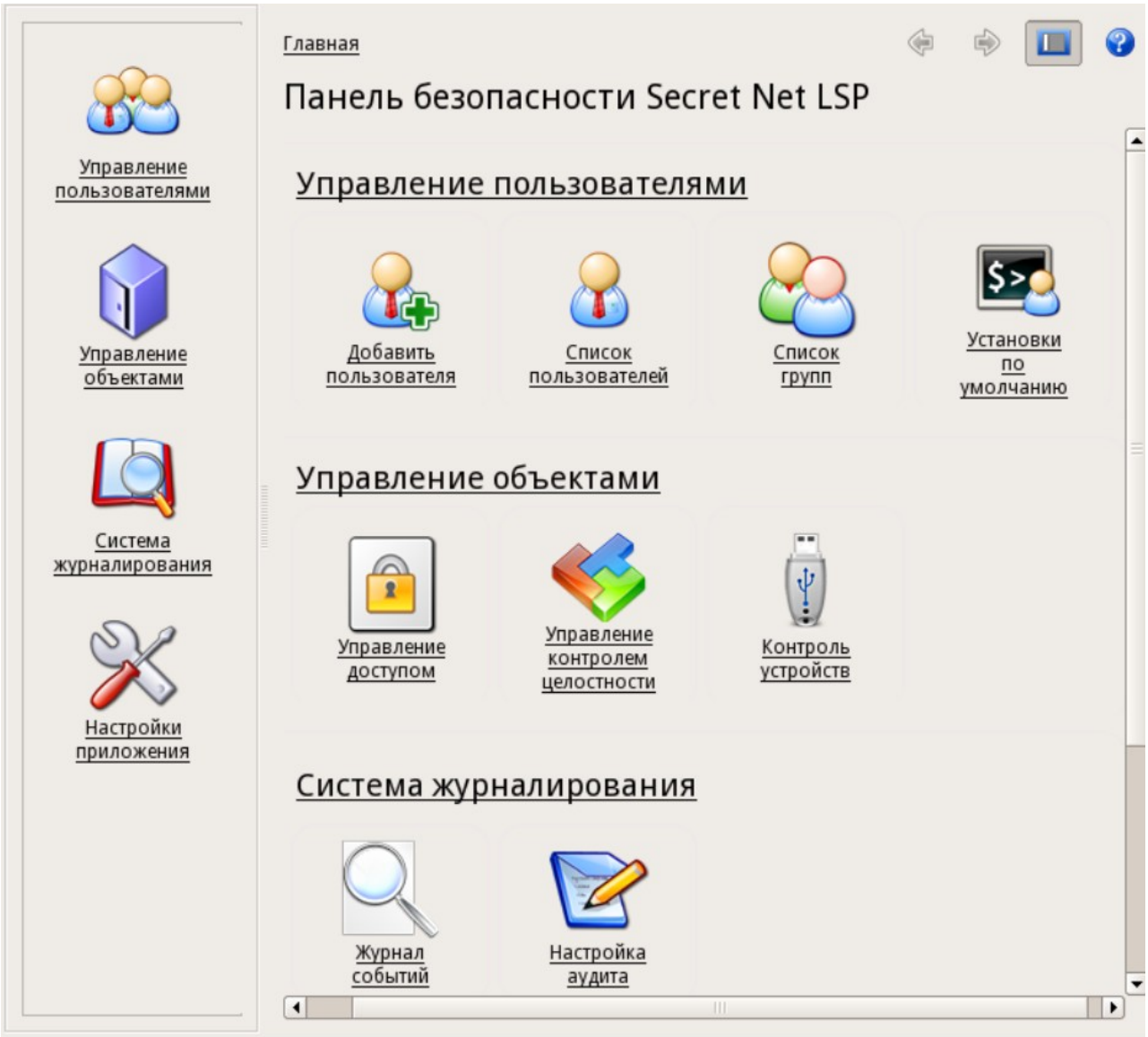
СПИСОК ЛИТЕРАТУРЫ

1. Доктрина информационной безопасности Российской Федерации – URL: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102161033
2. Федеральный закон РФ от от 27.07.2006 г. N 149-ФЗ Об информации, информационных технологиях и о защите информации – URL: http://pravo.gov.ru/proxy/ips/?docbody&nd=102108264
3. Н.Скабцов. Аудит безопасности информационных систем – СП-б.:Питер, 2018
4. А.Бирюков. Информационная безопасность. Защита и нападение – М.:ДМК Пресс, 2017
5. С.Нестеров. Информационная безопасность. Учебник и практикум – М.:Юрайт, 2017
6. Д.А.Мельников. Организация и обеспечение безопасности информационно-технологических сетей и систем. Учебник – М.:КДУ, 2015
7. Нестеров, С.А. Основы информационной безопасности : учебное пособие / С.А. Нестеров ; Министерство образования и науки Российской Федерации, Санкт-Петербургский государственный политехнический университет. - СПб. : Издательство Политехнического университета, 2014. - 322 с. : схем., табл., ил. - ISBN 978-5-7422-4331-1 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=363040(22.10.2017).
8. Аверченков, В.И. Аудит информационной безопасности : учебное пособие для вузов / В.И. Аверченков. - 3-е изд., стереотип. - М. : Флинта, 2016. - 269 с. - Библиогр. в кн. - ISBN 978-5-9765-1256-6 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=93245 (22.10.2017).
9. Электронный ресурс сайта ФСТЭК России URL:https://fstec.ru/
10. Электронный ресурс сайта ООО «Код Безопасности» URL:https://www.securitycode.ru/

    Руководство администратора «Месетовой экран ССПТ-2» ЗАО «НПО РТК» г. Санкт-Петербург.

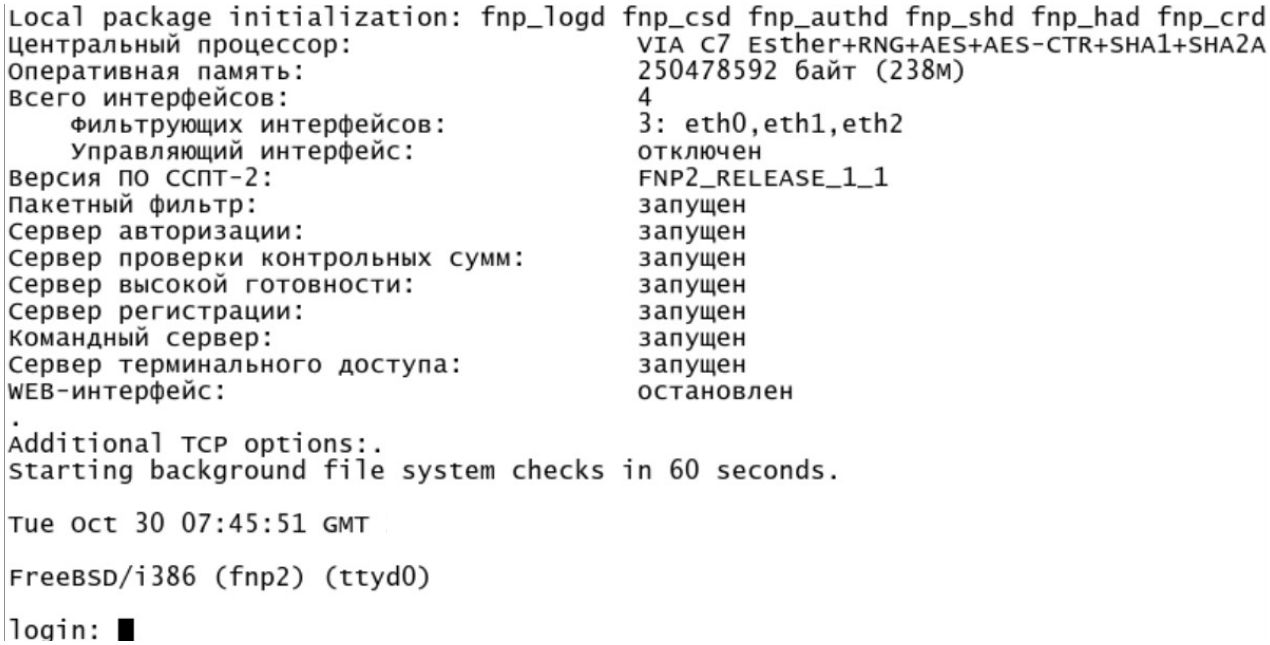
ПРИЛОЖЕНИЕ 1

Изображение панели безопасности Secret Net LSP



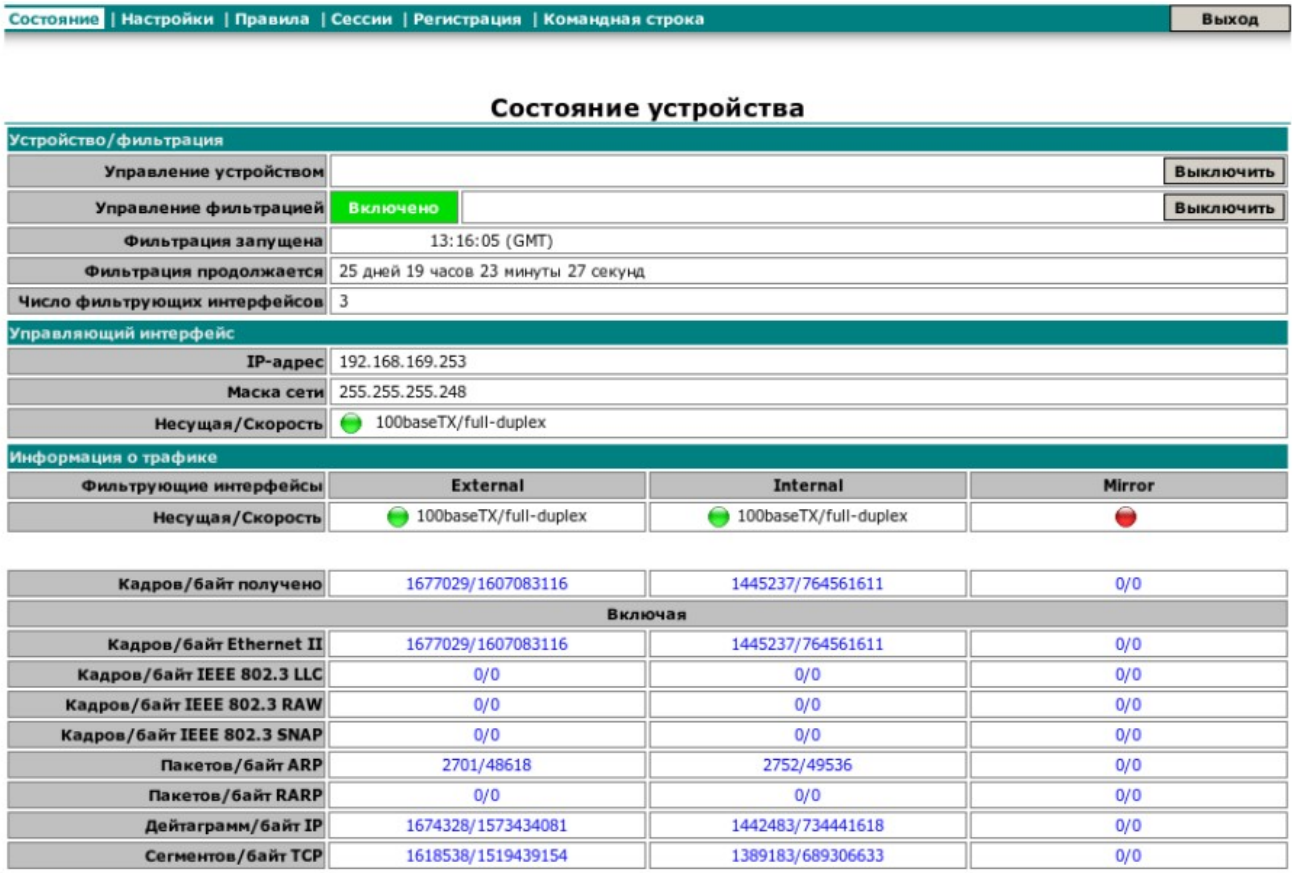
ПРИЛОЖЕНИЕ 3

Вид экрана после загрузки ОС ССПТ-2



ПРИЛОЖЕНИЕ 3

Рабочий интерфейс ССПТ-2



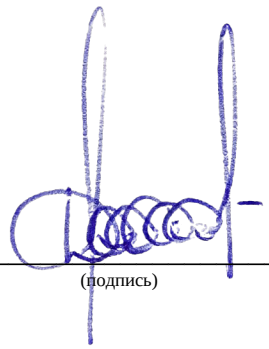
Состояние | Настройки | Правила | Сессии | Регистрация | Командная строка — Выход

Состояние устройства

Устройство/фильтрация			
Управление устройством			Выключить
Управление фильтрацией	Включено		Выключить
Фильтрация запущена	13:16:05 (GMT)		
Фильтрация продолжается	25 дней 19 часов 23 минуты 27 секунд		
Число фильтрующих интерфейсов	3		
Управляющий интерфейс			
IP-адрес	192.168.169.253		
Маска сети	255.255.255.248		
Несущая/Скорость	100baseTX/full-duplex		
Информация о трафике			
Фильтрующие интерфейсы	External	Internal	Mirror
Несущая/Скорость	100baseTX/full-duplex	100baseTX/full-duplex	
Кадров/байт получено	1677029/1607083116	1445237/764561611	0/0
Включая			
Кадров/байт Ethernet II	1677029/1607083116	1445237/764561611	0/0
Кадров/байт IEEE 802.3 LLC	0/0	0/0	0/0
Кадров/байт IEEE 802.3 RAW	0/0	0/0	0/0
Кадров/байт IEEE 802.3 SNAP	0/0	0/0	0/0
Пакетов/байт ARP	2701/48618	2752/49536	0/0
Пакетов/байт RARP	0/0	0/0	0/0
Дейтаграмм/байт IP	1674328/1573434081	1442483/734441618	0/0
Сегментов/байт TCP	1618538/1519439154	1389183/689306633	0/0

Выпускная квалификационная работа выполнена мной совершенно самостоятельно. Все использованные в работе материалы и концепции из опубликованной научной литературы и других источников имеют ссылки на них. Выпускная квалификационная работа прошла проверку на корректность заимствования в системе «Антиплагиат.ру».

Настоящим подтверждаю, что даю разрешение Университету «Синергия» на размещение полного текста моей выпускной квалификационной работы и отзыва на мою выпускную квалификационную работу в электронно-библиотечной системе Университета «Синергия».



_____ / Д.О. Юрасов
(подпись) (ФИО)

« 05 » октября 2022 г.