TOMSK POLYTECHNIC UNIVERSITY ТОМСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

Министерство науки и высшего образования Российской Федерации
федеральное государственное автономное
образовательное учреждение высшего образования
«Национальный исследовательский Томский политехнический университет» (ТПУ)

Школа Инженерная школа информационных технологий и робототехники
Направление подготовки 09.04.03. Прикладная информатика
Отделение школы (НОЦ) Отделение информационных технологий

МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ

Тема работы
Управление рисками информационной безопасности нефтегазодобывающего предприятия

УДК 005.334:004.056.5:622.32

Студент

Группа	ФИО	Подпись	Дата
8КМ71	Прохоренко Ангелина Сергеевна		

Руководитель ВКР

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Доцент ОИТ ИШИТР	Ротарь Виктор Григорьевич	к.т.н.		

КОНСУЛЬТАНТЫ ПО РАЗДЕЛАМ:

По разделу «Финансовый менеджмент, ресурсоэффективность и ресурсосбережение»

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Профессор ОСГН ШБИП	Сосковец Любовь Ивановна	д.и.н.		

По разделу «Социальная ответственность»

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Старший преподаватель ООД ШБИП	Атепаева Наталья Александровна			

ДОПУСТИТЬ К ЗАЩИТЕ:

Руководитель ООП	ФИО	Ученая степень, звание	Подпись	Дата
Доцент ОИТ ИШИТР	Марухина Ольга Владимировна	к.т.н.		

Томск – 2019 г.

Планируемые результаты обучения

Код результата	Результат обучения (выпускник должен быть готов)
Р1	Применять базовые и специальные знания в области современных информационно-коммуникационных технологий для решения междисциплинарных инженерных задач.
Р2	Проводить теоретические и экспериментальные исследования, включающие поиск и изучение необходимой научно-технической информации, математическое моделирование, проведение эксперимента, анализ и интерпретацию полученных данных в области информатизации и автоматизации прикладных процессов и создания, внедрения, эксплуатации и управления информационными системами в прикладных областях.
Р3	Внедрять, сопровождать и эксплуатировать современные информационные системы, обеспечивать их высокую эффективность, соблюдать правила охраны здоровья и безопасности труда, выполнять требования по защите окружающей среды.
Р4	Активно владеть иностранным языком на уровне, позволяющем работать в иноязычной среде, разрабатывать документацию, презентовать и защищать результаты инновационной инженерной деятельности.
Р5	Владеть и применять методы и средства получения, хранения, переработки и трансляции информации посредством современных компьютерных технологий, в том числе глобальных компьютерных сетей.
Р6	Эффективно работать индивидуально, в качестве члена и руководителя группы, состоящей из специалистов различных направлений и квалификаций, демонстрирует ответственность за результаты работы и готовность следовать корпоративной культуре организации.
Р7	Самостоятельно учиться и непрерывно повышать квалификацию в течение всего периода профессиональной деятельности.
Р8	Применять глубокие профессиональные знания основ построения информационных технологий и систем, достаточные для решения научных и профессиональных задач производства. Знать современные проблемы и методы прикладной информатики и научно-технического развития информационных технологий.
Р9	Ставить и решать задачи комплексного анализа, связанные с информатизацией и автоматизацией прикладных процессов; созданием, внедрением, эксплуатацией и управлением информационными системами в прикладных областях, с использованием базовых и специальных знаний, современных аналитических методов и моделей.
Р10	Организовывать работы по моделированию прикладных ИС и реинжинирингу прикладных и информационных процессов предприятия и организации. Управлять проектами по информатизации прикладных задач и созданию ИС предприятий и организаций.

TOMSK POLYTECHNIC UNIVERSITY ТОМСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

Министерство науки и высшего образования Российской Федерации
федеральное государственное автономное
образовательное учреждение высшего образования
«Национальный исследовательский Томский политехнический университет» (ТПУ)

Школа Инженерная школа информационных технологий и робототехники
Направление подготовки 09.04.03 Прикладная информатика
Отделение школы (НОЦ) Отделение информационных технологий

УТВЕРЖДАЮ:
Руководитель ООП
_____ _____ Марухина О.В.
(Подпись) (Дата) (Ф.И.О.)

ЗАДАНИЕ
на выполнение выпускной квалификационной работы

В форме:

магистерской диссертации

(бакалаврской работы, дипломного проекта/работы, магистерской диссертации)

Студенту:

Группа	ФИО
8КМ71	Прохоренко Ангелине Сергеевне

Тема работы:

Управление рисками информационной безопасности нефтегазодобывающего предприятия	
Утверждена приказом директора (дата, номер)	07.03.19 г., №1787

Срок сдачи студентом выполненной работы:	

ТЕХНИЧЕСКОЕ ЗАДАНИЕ:

Исходные данные к работе *(наименование объекта исследования или проектирования; производительность или нагрузка; режим работы (непрерывный, периодический, циклический и т. д.); вид сырья или материал изделия; требования к продукту, изделию или процессу; особые требования к особенностям функционирования (эксплуатации) объекта или изделия в плане безопасности эксплуатации, влияния на окружающую среду, энергозатратам; экономический анализ и т. д.).*	Объектам исследования является процесс управления рисками информационной безопасности нефтегазодобывающего предприятия.

Перечень подлежащих исследованию, проектированию и разработке вопросов *(аналитический обзор по литературным источникам с целью выяснения достижений мировой науки техники в рассматриваемой области; постановка задачи исследования, проектирования, конструирования; содержание процедуры исследования, проектирования, конструирования; обсуждение результатов выполненной работы; наименование дополнительных разделов, подлежащих разработке; заключение по работе).*	- Изучение предметной области; - Анализ и сравнение методологий и инструментов киберзащиты; - Разработка классификации оценки рисков; - Выбор программных средств для процесса управления рисками информационной безопасности; - Разработка системы поддержки принятия решений; - Социальная ответственность; - Финансовый менеджмент, ресурсоэффективность и ресурсосбережение
Перечень графического материала *(с точным указанием обязательных чертежей)*	

Консультанты по разделам выпускной квалификационной работы
(с указанием разделов)

Раздел	Консультант
Финансовый менеджмент, ресурсоэффективность и ресурсосбережение	Л.И.Сосковец
Социальная ответственность	Н.А. Атепаева
Раздел, выполненный на английском языке	А.В. Диденко

Названия разделов, которые должны быть написаны на русском и иностранном языках:
Разработка методологии

Дата выдачи задания на выполнение выпускной квалификационной работы по линейному графику	04.02.2019 г.

Задание выдал руководитель:

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Доцент ОИТ ИШИТР	Ротарь Виктор Григорьевич	к.т.н., доцент		

Задание принял к исполнению студент:

Группа	ФИО	Подпись	Дата
8КМ71	Прохоренко Ангелина Сергеевна		

TOMSK POLYTECHNIC UNIVERSITY ТОМСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

Министерство науки и высшего образования Российской Федерации
федеральное государственное автономное
образовательное учреждение высшего образования
«Национальный исследовательский Томский политехнический университет» (ТПУ)

Школа Инженерная школа информационных технологий и робототехники
Направление подготовки 09.04.03 Прикладная информатика
Уровень образования Магистратура
Отделение школы (НОЦ) Отделение информационных технологий
Период выполнения весенний семестр 2018/2019 учебного года)

Форма представления работы:

Магистерская диссертация

(бакалаврская работа, дипломный проект/работа, магистерская диссертация)

КАЛЕНДАРНЫЙ РЕЙТИНГ-ПЛАН
выполнения выпускной квалификационной работы

Срок сдачи студентом выполненной работы:	

Дата контроля	Название раздела (модуля) / вид работы (исследования)	Максимальный балл раздела (модуля)
05.03.2019	Глава 1. Анализ рисков информационной безопасности нефтегазодобывающих предприятий	20
26.03.2019	Глава 2. Обзор стандартов, инструментов и методологий оценки рисков	15
16.04.2019	Глава 3. Разработка методологии	20
30.04.2018	Глава 4. Разработка программного продукта для помощи в процессе управления рисками информационной безопасности	20
14.05.2019	Глава 5. Финансовый менеджмент, ресурсоэффективность и ресурсосбережение	15
21.05.2019	Глава 6. Социальная ответственность	10

СОСТАВИЛ:
Руководитель ВКР

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Доцент ОИТ ИШИТР	Ротарь Виктор Григорьевич	к.т.н.		

СОГЛАСОВАНО:
Руководитель ООП

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Доцент ОИТ ИШИТР	Марухина Ольга Владимировна	к.т.н.		

ЗАДАНИЕ ДЛЯ РАЗДЕЛА
«ФИНАНСОВЫЙ МЕНЕДЖМЕНТ, РЕСУРСОЭФФЕКТИВНОСТЬ И РЕСУРСОСБЕРЕЖЕНИЕ»

Студенту:

Группа	ФИО
8КМ71	Прохоренко Ангелине Сергеевне

Школа	Инженерная школа информационных технологий и робототехники	**Отделение школы (НОЦ)**	Отделение информационных технологий
Уровень образования	Магистратура	**Направление/специальность**	09.04.03 Прикладная информатика

Исходные данные к разделу «Финансовый менеджмент, ресурсоэффективность и ресурсосбережение»:	
1. Стоимость ресурсов научного исследования (НИ): материально-технических, энергетических, финансовых, информационных и человеческих	1. Оклад руководителя 23264,86 руб., исполнителя 6976,22 руб.
2. Нормы и нормативы расходования ресурсов	1. Норматив потребления электроэнергии 4 руб/кВтч
3. Используемая система налогообложения, ставки налогов, отчислений, дисконтирования и кредитования	1. Отчисления во внебюджетные фонды 27,1% 2. Районный коэффициент 30% 3. Коэффициент дополнительной заработной платы 12%
Перечень вопросов, подлежащих исследованию, проектированию и разработке:	
1. Оценка коммерческого и инновационного потенциала НТИ	Оценка потенциальных потребителей исследования, оценка конкурентоспособности, SWOT-анализ
2. Планирование процесса управления НТИ: структура и график проведения, бюджет, риски и организация закупок	Планирование этапов работ, определение трудоемкости и построение календарного графика, формирование бюджета, определение рисков НТИ
3. Определение ресурсной, финансовой, экономической эффективности	Сравнительный анализ интегральных показателей эффективности
Перечень графического материала *(с точным указанием обязательных чертежей):*	
1. Карта сегментирования рынка 2. Карта оценки конкурентоспособности проекта 3. Карта оценки конкурентных разработок 4. Матрица SWOT 5. Альтернативы проведения НИ 6. График проведения и бюджет НИ 7. Оценка ресурсной, финансовой и экономической эффективности НИ	

Дата выдачи задания для раздела по линейному графику	01.03.2019

Задание выдал консультант:

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Профессор ОСГГ ШБИП	Сосковец Любовь Ивановна	д. и. н.		01.03.2019

Задание принял к исполнению студент:

Группа	ФИО	Подпись	Дата
8КМ71	Прохоренко Ангелина Сергеевна		01.03.2019

ЗАДАНИЕ ДЛЯ РАЗДЕЛА
«СОЦИАЛЬНАЯ ОТВЕТСТВЕННОСТЬ»

Студенту:

Группа	ФИО
8КМ71	Прохоренко Ангелине Сергеевне

Школа	Инженерная школа информационных технологий и робототехники	**Отделение школы (НОЦ)**	Отделение информационных технологий
Уровень образования	Магистр	**Направление/специальность**	09.04.03 Прикладная информатика

Исходные данные к разделу «Социальная ответственность»:	
1. Характеристика объекта исследования (вещество, материал, прибор, алгоритм, методика, рабочая зона) и области его применения.	Объект исследования – процесс управления рисками информационной безопасности нефтегазодобывающих предприятий; программное обеспечение и методологии для управления рисками информационной безопасности. Области применения – нефтегазодобывающие предприятия. Характеристики рабочего места. Основное оборудование ПЭВМ.
Перечень вопросов, подлежащих исследованию, проектированию и разработке:	
1. Правовые и организационные вопросы обеспечения безопасности: – специальные (характерные при эксплуатации объекта исследования, проектируемой рабочей зоны) правовые нормы трудового законодательства; – организационные мероприятия при компоновке рабочей зоны.	Трудовой кодекс Российской Федерации от 30.12.2001 N 197-ФЗ, СанПиН 2.2.2/2.4.1340-03 Гигиенические требования к персональным электронновычислительным машинам и организации работы; ГОСТ 12.2.032-78 «ССБТ. Рабочее место при выполнении работ сидя. Общие эргономические требования», ГОСТ 12.2.061-81 «ССБТ. Оборудование производственное. Общие требования безопасности к рабочим местам».
2. Производственная безопасность. 1.1. Анализ выявленных вредных и опасных факторов. 1.2. Обоснование мероприятий по снижению воздействия	– Недостаточная освещенность рабочей зоны и отсутствие или недостаток естественного света – Отклонение показателей микроклимата – Превышение уровня шума – Повышенный уровень электромагнитных излучений – Повышенное значение напряжения в электрической цепи, замыкание которой может произойти через тело человека

	– Меры по соблюдению норм освещенности – Способы и средства нормализации микроклимата – Меры по снижению уровня шумового загрязнения – Организационные и технические меры электробезопасности
3. Экологическая безопасность.	- Анализ негативного воздействия на окружающую природную среду: утилизация компьютеров и другой оргтехники
4. Безопасность в чрезвычайных ситуациях.	– Пожары

Дата выдачи задания для раздела по линейному графику	**01.03.2019**

Задание выдал консультант:

Должность	**ФИО**	**Ученая степень, звание**	**Подпись**	**Дата**
Старший преподаватель ООД ШБИП	Атепаева Наталья Александровна	нет		

Задание принял к исполнению студент:

Группа	**ФИО**	**Подпись**	**Дата**
8КМ71	Прохоренко Ангелина Сергеевна		

РЕФЕРАТ

Выпускная квалификационная работа содержит 133 страницы, 14 рисунков, 29 таблиц, 40 источников, 1 приложение.

Ключевые слова: информационная безопасность, нефтегазодобывающие предприятия, управление рисками, классификация рисков, система поддержки принятия решений.

Объект исследования – процесс управления рисками информационной безопасности нефтегазодобывающих предприятий.

Цель исследования – повышение эффективности методов информационной защиты нефтегазодобывающих предприятий.

В процессе исследования были изучены основные аспекты процесса управления рисками информационной безопасности. Во введении приведено обоснование актуальности исследования, выявлена проблема, описаны цель, задачи, предмет и объект исследования. В первой главе проведен анализ рисков информационной безопасности нефтегазодобывающих предприятий. Во второй главе описаны актуальные стандарты, методологии и инструменты управления рисками информационной безопасности. Третья глава посвящена описанию разработки метода классификации оценки рисков. В четвертой главе описана разработанный программный продукт для помощи в процессе управления рисками информационной безопасности. В пятой главе была обоснована экономическая эффективность проводимого исследования, а шестая содержит описание социальной ответственности.

Введение

Основу безопасности и надежности функционирования наиболее важных объектов инфраструктуры составляют системы управления производственными процессами организации (ICS). Инженерно-технические специалисты успешно разрабатывают и внедряют ICS-системы с учетом требований безопасности труда и надежности, но не всегда – информационной безопасности. Данный факт объясняется тем, что изначально потребность в обеспечении информационной безопасности таких систем была небольшой. Наибольшим спросом для управления производственными процессами пользовались изолированные, узкоспециализированные системы. Учитывая, что прежде такие системы не внедрялись в бизнес-процессы организаций и даже не взаимодействовали между собой, риск возникновения масштабных каскадных аварий в случае виртуальных и иных атак рассматривался отдельно от прочих рисков организаций.

Однако спустя 20 лет значительного развития информационных технологий – и распространенность объединенных в сети IoT-устройств значительно изменило представления об информационной безопасности. Сегодня все виды производственных активов, включая нефтяные месторождения, нефтепроводы и нефтеперерабатывающие предприятия, становятся уязвимыми для кибератак. В наше время операционные системы, вне зависимости от их локализации, подвержены внешним и внутренним рискам, которые могут привести к нарушениям безопасности или производственным сбоям и тем самым увеличить размер коммерческого риска. Несмотря на то что ICS-системы, как правило, призваны обеспечить безопасность в аварийных ситуациях, постоянное совершенствование методов, применяемых киберпреступниками, ведет к росту риска возникновения катастроф и масштаба их последствий, которые проявляются в виде затрат, нарушения безопасности, ущерба для репутации и коммерческих или финансовых потерь.

В последнее время нефтегазодобывающие компании, как и компании из других отраслей экономики работают над укреплением информационной безопасности, поскольку, по мнению высшего руководства и членов советов директоров, эта задача является одной из первоочередных.

Актуальность данной работы обусловлена тем, что в настоящее время наблюдается интенсивное применение робототехники, цифровизации и Интернета вещей (IoT) в операционной среде нефтегазодобывающих предприятий и, как следствие, возникают новые риски информационной безопасности в данных предприятиях.

Целью работы является повышение эффективности применяемых методов информационной защиты в нефтегазодобывающих предприятиях.

Задачи, решаемые в ходе данной работы: выполнение всестороннего анализа и сравнение различных подходов и методов защиты информации, применяемых на нефтегазодобывающих предприятиях, анализ недостатков и преимуществ каждого метода, а также разработка системы классификации оценки рисков, для поддержки принятия решений по мерам защиты информации.

Результат проделанной работы можно будет применять в нефтегазодобывающих предприятиях с целью повышения эффективности применяемых мер информационной защиты.

1. Анализ рисков информационной безопасности нефтегазодобывающих предприятий

Одной из основных причин, затрудняющих обеспечение безопасности ICS-систем, является то, что при их создании не предполагалась возможность их объединения в сети, однако сегодня происходит именно это. Цифровизация операционных процессов в нефтегазовом секторе привела к тому, что перед компаниями открываются новые возможности для повышения производительности и сокращения затрат. Однако слияние производственных и бизнес-процессов делает организации уязвимыми для широкого спектра новых киберрисков. Рассмотрим возможные сценарии, которых несколько лет назад вовсе не существовало (Таблица 1).

Таблица 1. Влияние киберугроз на цепочку создания стоимости в нефтегазовом секторе.

<table>
<tr><th colspan="2">Геологоразведка и добыча</th></tr>
<tr><th>Геологоразведка</th><th>Добыча</th></tr>
<tr><td>Геофизическая оценка и моделирование
Разработка месторождений
Буровые работы</td><td>Извлечение нефти</td></tr>
<tr><td>Геологоразведка и добыча: сценарий 1.
Незаконное присвоение служебной коммерческой информации о динамике эксплуатации пласта и скважин.
Риски:
утрата конкурентных преимуществ оператора на месторождении.</td><td>Геологоразведка и добыча: сценарий 2.
Превышение стандартных эксплутационных параметров или полная остановка работы ключевого оборудования, обеспечивающего управление работами в скважинах, и безопасность рабочих.
Риски:
риск остановки работ и возникновения финансовых потерь, а также инцидентов в сфере безопасности на месторождениях из-за неисправностей в работе оборудования.</td></tr>
<tr><th colspan="2">Транспортировка и хранение</th></tr>
<tr><th colspan="2">Транспортировка</th></tr>
<tr><td colspan="2">Сбор и транспортировка (трубопроводы, танкеры, грузовики)</td></tr>
<tr><td>Транспортировка и хранение: сценарий 1.
Несанкционированный доступ и управление системами трубопроводов.
Риски:
риск возникновения взрыва, утечки, нанесения ущерба окружающей среде и системам, а также создания опасных</td><td>Транспортировка и хранение: сценарий 2.
Нарушение или прерывание процесса мониторинга, создающее угрозу для бесперебойной работы оборудования.
Риски:
риск остановки функционирования системы, обеспечивающей проведение внутренних расследований, что может привести к сбоям</td></tr>
</table>

условий для персонала и населения близлежащих территорий.	при доставке продукции и финансовым потерям.
Переработка и сбыт	
Переработка	**Сбыт**
• Переработка сырой нефти для получения нефтепродуктов • Смешение нефтепродуктов	• Розничные продажи • Трейдинг
Переработка и сбыт: сценарий 1. Хищение данных о запасах сырой нефти и очищенных нефтепродуктов. **Риски:** риск несоблюдения деловых обязательств и утраты репутации.	**Переработка и сбыт: сценарий 2.** Нарушение/умышленное нарушение функционирования средств осуществления контроля за операционной деятельностью. **Риски:** риск несоблюдения условий эксплуатации и простоя оборудования, приводящий к сбоям в поставках и потере доходов.

1. Если организации пользуются незащищенным удаленным доступом для взаимодействия, это позволяет киберпреступникам получить контроль над системой, управляющей производственными процессами, и вызвать перегрузку производственного оборудования.

2. Неэффективные методы обеспечения безопасности, применяемые сторонними контрагентами, позволяют вирусам проникнуть в производственную программную среду, что приводит к остановке работы ключевых систем SCADA (системы диспетчерского управления и сбора данных) и созданию небезопасных условий труда.

3. Некорректное проведение тестирования информационных систем перед развертыванием приводит к их полному отказу и, как следствие, к сбоям или остановке производственных процессов.

4. Если предприятие приобретает какие-либо технологические продукты без полноценного предварительного тестирования и оценки, то все имеющиеся в таком программном обеспечении ошибки остаются неисправленными, что делает предприятие уязвимым и позволяет враждебно настроенным лицам получить удаленный доступ к программируемым устройствам управления (PLC) и возможность умышленно дестабилизировать производственные процессы.

Приведенные примеры показывают, что существует множество источников киберугроз, в том числе в лице сотрудников компании, стремящихся организовать диверсию на производстве; конкурентов, желающих нанести ущерб бренду компании; а также третьих лиц (например, групп активистов, призывающих к остановке работ).

Не все уязвимости обуславливаются исключительно использованием технологий. Поведенческие аспекты также могут играть свою роль. Так, недостаточное понимание значения мер по обеспечению безопасности в рамках организации может подвергнуть корпоративные системы риску возникновения кибератак (например, это может случиться, если сотрудники используют собственные мобильные носители информации, зараженные вредоносными программами). Более того, многие производственные работники полагают, что используемые ими системы не представляют интереса для злоумышленников, а потому неохотно признают необходимость изменения привычного образа действий и внедрения новых протоколов безопасности. В конце концов, еще недавно можно было с уверенностью предполагать, что все элементы оборудования заслуживают полного доверия. Сегодня все изменилось. Ведь показания цифровых сенсоров и контроллеров можно сфальсифицировать с целью предоставления ложной информации о состоянии оборудования. Другая устаревшая аксиома гласит, что сбои в процессах в основном объясняются погодными условиями, человеческим фактором и износом оборудования и не обязательно вызваны злонамеренным вмешательством в работу систем со стороны лиц, желающих причинить ущерб компании.

Вне зависимости от того, произошла ли утечка данных по недосмотру самой компании или в результате атаки злоумышленников, ее последствия могут быть очень серьезными: от нарушения конфиденциальности данных до отказа или полной остановки работы систем. А это может повлечь за собой уменьшение объемов выручки, нанесение ущерба репутации компании,

происхождение экологической катастрофы, принятие правовых мер или – в худшем случае – гибель людей.

Легко понять, почему внедрение комплексных, эффективных средств контроля информационной безопасности в ICS-системы организаций в наше время становится насущной необходимостью, если не сказать обязательным требованием. Вместе с тем для выполнения этой задачи компании должны найти способ принять во внимание противоположные точки зрения на информационные системы и операционные процессы, поскольку специалисты по управлению производственными процессами не всегда в полной мере понимают специфику текущих рисков информационной безопасности, а специалисты в области информационной безопасности часто не разбираются в производственных процессах, управляемых ICS-системами.

Анализ типа bowtie – популярный метод, широко используемый в инженерно-технической области для оценки отказов оборудования. Любой анализ можно провести с учетом специфики организации. На рис. 1 показан анализ киберрисков с помощью метода bowtie применительно к нефтегазодобывающей компании.

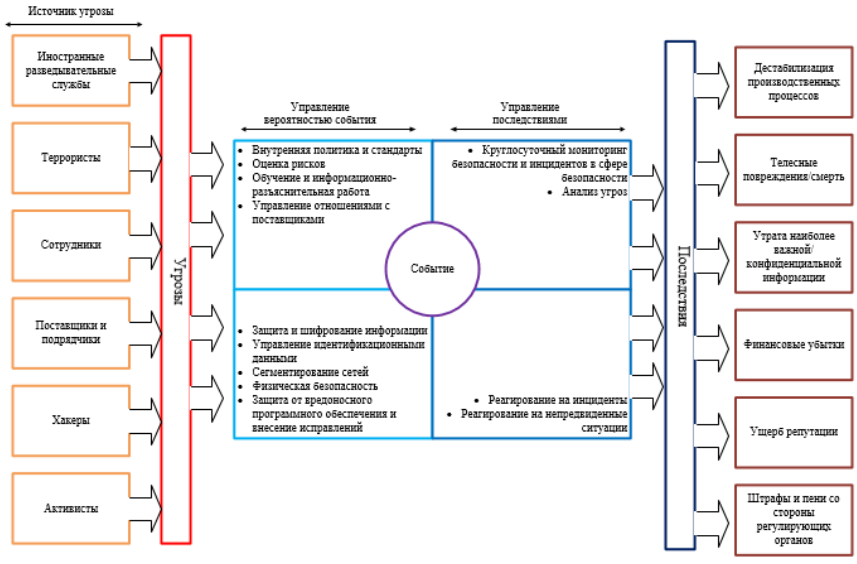

Рисунок 1. Анализ киберрисков нефтегазодобывающей компании.

После получения полной картины рисков нефтегазодобывающая компания должна провести оценку зрелости существующих средств обеспечения контроля за информационной безопасностью производственных процессов.

И пусть не все риски можно минимизировать, важно понимать, какие виды контрольных процедур существуют в организации и над чем еще необходимо работать. Речь идет о необходимости уделять достаточное количество внимания анализу взаимосвязей между рисками, связанными со взломом ICS-систем, и бизнес-рисками в целом. На рисунке 2 представлена модель проведения оценки зрелости средств обеспечения информационной безопасности предприятия.

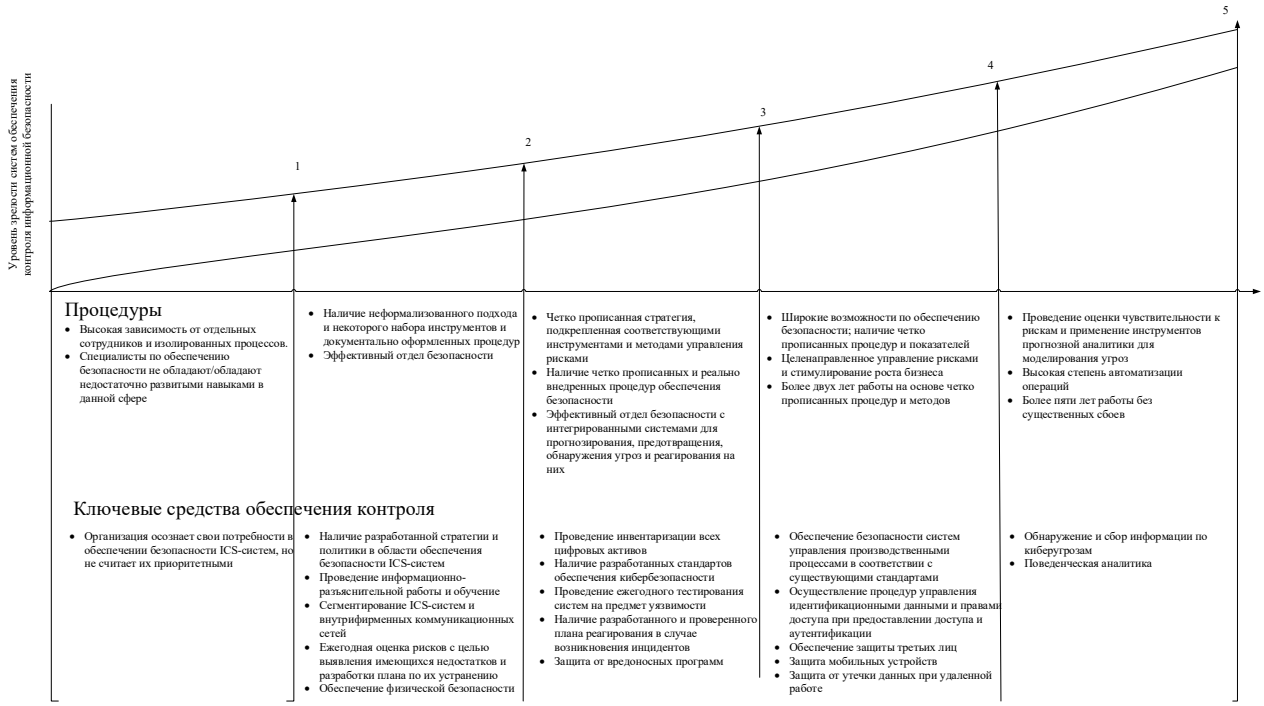

Рисунок 2. Оценка зрелости средств обеспечения контроля за киберрисками.

Помимо оценки зрелости, организации в рамках текущего мониторинга должны регулярно анализировать определенные активы, причем не только те, в которых были выявлены факторы уязвимости, но и те, в отношении которых обнаружены потенциальные угрозы безопасности, постоянные угрозы повышенной сложности (advanced persisent threats − APT) или подозрительные действия, а также заблаговременно отслеживать уязвимые активы до возникновения реальной угрозы безопасности.

2. Обзор стандартов, инструментов и методологий оценки рисков

Стандарты информационной безопасности необходимы для определения подходов к оценке уровня рисков ИБ, а также для описания требований к безопасности информационной системы. Инструменты управления рисками информационной безопасности являются системными решениями и процедурами, которые позволяют провести оценку рисков. Методологии управления рисками информационной безопасности в основном являются свободными и фундаментальными подходами к оценке рисков, некоторые из них касаются определенной части процесса управления рисками, а другие охватывают весь процесс. Инструменты управления рисками обычно разрабатываются на основе нескольких методик.

Данные инструменты и методологии имеют два основных подхода − количественный и качественный, однако в некоторых из них используется смешанный подход в зависимости от среды использования и структуры процесса.

2.1. Стандарты

Для оценки и управления рисками информационной безопасности разработаны различные стандарты. Наиболее распространенными являются следующие стандарты: государственный стандарт ГОСТ Р ИСО/МЭК 27005-2010, определяющий инструменты и методику оценки безопасности информационных продуктов и систем; ISO 31000, ISO 27001:2013 (ранее известный как BS 7799); ISO 27002:2013 (ранее известный как 17799); последние два стандарта относят к семейству ISO/IEC 27000, которое включает стандарты по информационной безопасности, опубликованные совместно Международной Организацией по Стандартизации.

Семейство стандартов ISO 27000 произошло от британского стандарта BS 7799 (позже с несколькими обновленными версиями ISO 17799). Процесс развития включал экспертные мнения из различных областей, включая правительство, научно-исследовательские организации, промышленные ассоциации и международные предприятия. Данные стандарты и сейчас

продолжают обновляться и расширяться с учетом новых тенденций в быстро развивающихся областях техники. Стандарты ИСО 27000 были адаптированы многими странами и являются одними из наиболее общепризнанных стандартов управления рисками информационной безопасности во всем мире. Причина в том, что они обеспечивают эффективные, полномасштабные меры по управлению рисками информационной безопасности. В отличие от других традиционных подходов и стандартов, основанных на техническом понимании, серия ISO 27000 обеспечивает систематическую, процедурную и документационную основу для процесса управления рисками информационной безопасности. Он охватывает вопросы риска от организационного высокого уровня до подробного оперативного и технического уровня.

ISO 31000 является еще одним популярным стандартом в области управления рисками. Он обеспечивает принципы, границы и процесс управления рисками, и может быть интегрирован с ISO 27001. ISO 31000 не дает каких-либо конкретных рекомендаций, по оценке рисков информационной безопасности. Поэтому при решении проблем информационной безопасности необходимо учитывать и другие более узконаправленные стандарты, такие как ISO 27005. Однако ISO 31000 может быть хорошим дополнением для разработки стратегической основы общих вопросов управления рисками информационной безопасности.

ГОСТ Р ИСО/МЭК 27005-2010 поддерживает общие концепции, определенные в ИСО/МЭК27001, и предназначен для содействия адекватного обеспечения информационной безопасности на основе подхода, связанного с менеджментом риска.

2.2. Инструменты управления рисками информационной безопасности

2.2.1. Программные продукты

А. Оценка операционных угроз, активов и уязвимостей (OCTAVE)

OCTAVE – это подход к управлению рисками информационной безопасности, разработанный Массачусетским технологическим институтом

и широко используемый во всем мире. В отличие от других ориентированных на технологии подходов, OCTAVE в большей степени ориентирован на стратегическую оценку/планирование и организационные риски, а также на достижение баланса между операционным риском, практикой обеспечения безопасности и технологией.

OCTAVE состоит из трех этапов:

1) создание профиля угроз, связанных с активами;

2) идентификация уязвимостей инфраструктуры;

3) разработка стратегии и планов безопасности.

Профиль угрозы включает в себя указания на актив (asset), тип доступа к активу (access), источник угрозы (actor), тип нарушения или мотив (motive), результат (outcome) и ссылки на описания угрозы в общедоступных каталогах. По типу источника, угрозы в OCTAVE делятся на:

1. угрозы, исходящие от человека-нарушителя, действующего через сеть передачи данных;
2. угрозы, исходящие от человека-нарушителя, использующего физический доступ;
3. угрозы, связанные со сбоями в работе системы;
4. прочие.

Результат может быть раскрытие (disclosure), изменение (modification), потеря или разрушение (loss/destruction) информационного ресурса или разрыв подключения. Отказ в обслуживании (interruption).

B. Консультативный, объективный и двухфункциональный анализ рисков (COBRA)

Система COBRA (Consultative Objective and Bi-functional Risk Analysis), созданная компанией Risk Associates, предоставляет средства анализа рисков и позволяет оценить соответствие ИС стандарту ISO 27002:2013. В COBRA реализованы методы количественной оценки рисков.

В состав продукта входят также инструменты для консалтинга и проведения обзоров безопасности, разработанные на основании принципов

построения экспертных систем. Инструменты используют обширную базу знаний по угрозам и уязвимостям, а также множество вопросников, успешно применяющихся на практике. В комплект ПО входят модули COBRA ISO 17799 Security Consultant, COBRA Policy Compliance Analyst и COBRA Data Protection Consultant.

C. @RISK (Монте-Карло)

Данный программный продукт выполняет анализ рисков с использованием моделирования по методу Монте-Карло, показывая большое количество результатов в модели на базе электронной таблицы, учитывая вероятность возникновения каждого из рисков. Программа с полной объективностью вычисляет и отслеживает множество возможных будущих сценариев и выдает связанные с ними вероятности и риски. Таким образом можно оценить, на какие риски организация готова пойти, а каких лучше избежать, и принять лучшее решение в условиях неопределенности.

D. CORAS

Методология Coras, предназначенная для анализа рисков безопасности, представляет собой инструмент для моделирования рисков и угроз, используемый на протяжении всей работы. ПО использует язык UML − язык графического описания для объектного моделирования в области разработки ПО. Методология оценки рисков CORAS основывается на HAZOP, FTA, FMECA и обеспечивает поддержку целостности, доступности, подотчетности, подлинности и надежности ИТ-систем. Методология CORAS включает в себя 7 этапов: вводная встреча (во время этой встречи аналитики собирают информацию, основанную на представлениях заказчика); отдельная встреча с представителями заказчика (идентифицируются первые угрозы, уязвимости, сценарии угроз и нежелательные инциденты); усовершенствованное описание той ситуации, которую необходимо проанализировать; четвертый этап включает в себя идентификацию всех возможных потенциальных нежелательных инцидентов, а также угроз и уязвимостей; на этом этапе оцениваются последствия, которые будут в случае осуществления

нежелательных инцидентов, а также вероятность этих инцидентов; на шестом этапе получают первичную полную картину рисков, которую редактируют; в конце следует обоснование и описание действий, предотвращающих угрозы.

F. Упрощенный процесс анализа рисков (FRAP)

Этот качественный метод в основном ориентирован на процесс РА с ограниченными временными и бюджетными рамками, поэтому он обычно быстрее и проще по сравнению с другими методами. Проводятся четыре основных этапа: мозговой штурм для выявления угроз, присвоение каждой угрозе оценки вероятности воздействия, определение и назначение средств контроля и управление риском. Метод только фильтрует и оценивает риск тех действий, которые являются наиболее необходимыми. Данный продукт не рассчитывает вероятность риска и ALE (ожидаемая годовая потеря). Каждый член группы по оценке рисков должен принять решение о важности каждого риска на основе своего опыта. Таким образом, этот метод может контролировать процесс управление рисками с использованием относительно небольших временных затрат.

G. RiskWatch

RiskWatch − это инструмент оценки рисков, сочетающий количественные и качественные методы оценки. Он поддерживает ISO 27000 и другие стандарты оценки рисков и может быть использован для анализа организаций, объектов, систем, приложений или сетей, в малом или большом масштабе. Инструмент содержит 5 продуктов, которые сосредоточены на различных областях. Risk Watch имеет такие преимущества, как удобный пользовательский интерфейс, использование предопределенных моделей оценки рисков и баз данных экспертных знаний, чтобы пользователь мог эффективно оценивать риски и уязвимости. Определение риска в RiskWatch заключается в рассмотрении аспектов активов, потерь, угроз, уязвимостей и защиты. Результатом наблюдения за рисками является достижение двух целей − выявление рисков в текущей ситуации, а также поиск или рекомендация мер по снижению или снижению рисков и доказательство их эффективности.

2.2.2. Технические средства

A. Сканер уязвимостей

Сканеры уязвимостей − это инструменты, которые оценивают безопасность сетей или систем и могут выявлять и сообщать об их уязвимостях. Они сканируют сети, серверы, брандмауэры, маршрутизаторы, приложения и т. д., чтобы найти нарушения безопасности в системах и оценить серьезность угрозы. Сканирование производится на разных уровнях системы: оценка уровня сети, работы системы оценки, базы оценки, и оценки уровня приложения. Сканирование необходимо проводить регулярно, чтобы пользователи могли быть в курсе потенциальных рисков. Типичными сканерами уязвимостей являются Сканеры портов (Nmap, Nessus), Сканеры веб-приложений, хост-сканеры (второй сканер), сканеры баз данных и т.д.

B. Тестирование на проникновение

Тестирование на проникновение является мерой предосторожности для проверки негативных последствий уязвимости системы, с целью устранения уязвимостей до реальных атак. Тестирование обычно проводится путем проведения моделирования атак, похожих на реальные, однако ими можно управлять и, в случае чего, с легкостью восстановить систему. Тестировщики могут использовать либо белый ящик, либо черный ящик. Во многих случаях тестирование на проникновение может проводиться совместно со сканерами уязвимостей. Сканеры уязвимостей более эффективны, однако при обнаружении сложных проблем безопасности возможны ложные срабатывания оборудования. С другой стороны, тестирование на проникновение требует больше времени и ресурсов, но способно справиться с более глубокими уязвимостями.

2.3. Методологии

A. Hazop

Hazop – это структурированный, основанный на командной работе метод определения опасных факторов при эксплуатации существующих процессов и проектировании новых объектов. В основе исследования лежит

искусственное создание отклонений производственных характеристик от указанных в проекте данных. Все узлы пропускаются через «отклонения», таким образом вырисовывая потенциальные сценарий рисков для дальнейшего исследования. Главная задача мероприятий заключается в проверке надежности и наличия мер защит, предусмотренных в определённых узлах для незапланированных «отклонений», которые повышают вероятность возникновения аварийной ситуации и её последствий. Результатом использования методологии является список угроз. Для каждой угрозы потребуется дополнительная оценка причин и последствий.

B. Вероятностная оценка риска (PRA)

PRA − это модель для анализа частоты и последствий наступления рисковых событий. Она сочетает в себе как количественные, так и качественные методы оценки рисков. PRA состоит из следующих этапов:

- выявление событий, которые могут нарушить информационную безопасность, данные события являются профилями риска;

- оценка профилей рисков с учетом их роли в системе и внутренних логических связей;

- формирование дерева рисков системы, оценка последствий и частоты возникновения рисков;

- использование логических и математических подходов, чтобы получить окончательную оценку риска.

На первом этапе PRA идентификация осуществляется либо путем общей инженерной оценки, основанной на предыдущем опыте, либо с помощью более формального подхода, такого как предварительный анализ рисков и анализ последствий.

C. Предварительный анализ опасности (PHA)

PHA применяется на начальных этапах проекта, когда данных и информации недостаточно. Для выявления событий или опасностей проводится контрольное исследование с учетом последовательностей событий, превращающих опасности в нарушения информационной

безопасности. Последствия наступления рисковых событий будут ранжированы в соответствии с серьезностью нанесенного ущерба.

D. Режимы и эффекты отказов и анализ критичности (FMECA)

FMECA состоит из двух частей: FMEA (анализ режимов отказов и эффектов) и CA (анализ критичности). FMECA − это метод анализа, направленный на отказы систем и оборудования. Первая часть, FMEA, представляет собой метод исследования режимов отказов отдельных компонентов системы. Для того, чтобы выполнить процесс FMEA, необходимо сначала проанализировать работу системы. Затем будет создан рабочий лист для определения режимов отказа каждого компонента, основанный на пяти аспектах: 1) как происходит сбой компонента, 2) каковы причины сбоя, 3) каковы последствия сбоя, 4) насколько они серьезны и 5) как обнаруживается сбой.

Этот метод является достаточно трудоемким и дорогостоящим из-за большого объема информации и обработки данных. Однако его применение может улучшить надежность и качество информационной безопасности, сделать возможным более раннее выявление и устранение отказов и минимизировать издержки. CA является расширенной частью FMEA, из-за двух дополнительных шагов. Первый шаг определяет и ранжирует серьезность последствий сбоя, оценивает вероятность возникновения сбоя и частоту обнаружения сбоя с помощью текущего механизма безопасности системы. Вторым шагом на основе предыдущего анализа будет рассчитан приоритет риска (RPN).

Получаем RPN=(серьезность)*(вероятность)*(обнаружение). Чем выше значение RPN, тем больше внимания следует уделить данному риску.

E. Анализ деревьев неисправностей (FTA)

Анализ дерева отказов является графическим методом анализа с 1960-х годов, который в основном используется для анализа надежности и безопасности сложных систем. Это нисходящий подход. С помощью анализа различных частей системы, таких как аппаратные средства, программное обеспечение, окружающая среда или человеческий фактор, можно нарисовать

древовидный график, который включает в себя различные комбинации рисковых событий и вероятности их наступления.

F. Анализ дерева событий (ETA)

ETA является еще одним методом графического анализа, который используется для выявления последствий, вызванных наступлением рисковых событий. С его помощью можно количественно оценить возможные последствия возникновения угрозы. Логика анализа ETA противоположна логике анализа FTA, так как анализ начинается с последствий наступления данного события. В каждом узле дерева событий, следствием может быть как угроза, так и возможности. Основываясь на экспертном опыте и большом количестве статистических исследований, получаем вероятность наступления каждого возможного результата.

G. Причинно-следственный анализ (CCA)

CCA − это метод, который сочетает в себе FTA и ETA. Таким образом, она включает в себя анализ причин и следствий. Использование данного метода поможет определить цепь событий, которые могут привести к неожиданным последствиям. С помощью анализа вероятности возникновения различных событий в графе CCA может быть достигнута вероятность всех возможных последствий. А общий уровень риска можно определить с учетом вероятности наступления и серьезности последствий каждого из рисков.

H. Delphi

Delphi − это типичный качественный метод, которые был изобретен для того, чтобы максимально использовать опыт экспертов. Учитывая то, что метод Дельфи представляет собой метод экспертного оценивая, основными его особенностями являются анонимность, многоуровневость и заочность. Базовой предпосылкой служит идея о том, что если должным образом произвести обобщение и обработку индивидуальных оценок экспертов по поводу конкретной ситуации, можно получить общее мнение, которое будет обладать максимальной степенью надёжности и достоверности.

I. Процесс аналитической иерархии (AHP)

Метод анализа иерархий (Analytic Hierarchy Process - AHP), или подход аналитической иерархии предполагает декомпозицию проблемы на простые составляющие части и обработку суждений ЛПР. В результате определяется относительная значимость исследуемых альтернатив для всех критериев, находящихся в иерархии. Относительная значимость выражается численно в виде векторов приоритетов. Полученные таким образом значения векторов являются оценками в шкале отношений и соответствуют так называемым жестким оценкам.

Процесс AHP включает в себя 4 этапа:

1. Структуризация задачи виде иерархической структуры с несколькими уровнями: цели – критерии – альтернативы;
2. Попарное сравнение элементов каждого уровня лицом, принимающим решения. Результаты сравнения имеют числовой характер;
3. Вычисление коэффициентов важности для элементов каждого уровня. Проверка согласованности суждений ЛПР;
4. Подсчет количественной оценки качества альтернатив. Выбор лучшей альтернативы.

3. Разработка методологии

После того, как будет выбран подходящий метод оценки рисков, специалистам необходимо приступить непосредственно к самой оценке рисков. Однако, как было выявлено в предыдущих разделах, каждый метод имеет недостатки. Поэтому необходимо адаптировать какой-либо из методов, или же комбинировать несколько методов, с целью разработки наиболее подходящего решения. В настоящее время на практике все чаще применяют гибридные методы, а для оценки рисков используются теория ИИ, машинное обучение, нейросети и методы, основанные на нечеткой логике. Существует множество гибридных методов, которые можно использовать для различных целей, и в которых акцент делается на совершенно разные аспекты. Представленная структура гибридного режима дает возможность проводить стандартные процедуры для определения рисков, которые бы соответствовали общепринятым стандартам информационной безопасности.

3.1. Основа метода

3.1.1. Концепция Систем оценки рисков

Система оценки рисков (СОР) – это стратегия для обмена и обзора потоков информаций о рисках различных организаций. Хорошая СОР должна быть одинаково понятна как профессионалам, так и новичкам. Она должна полностью охватывать организацию, и не фокусироваться на одном активе или системе. Также необходимо учитывать элементы, связанные с работой компании, например, ее цель, структуру, документацию и т.д. Хорошая система оценки рисков позволяет организации определить потенциальные риски, общий уровень рисков, а также помочь в разработке мероприятий реагирования на возможные наступления рисковых событий, создании стратегии развития и финансовых планов, а также развитии бизнес-культуры.

В настоящее время достаточно распространены следующие СОР: ISO 27000, NIST, OCTAVE и т.д. Организации могут применять их как напрямую, так и видоизменять для того, чтобы адаптировать под конкретные требования ИБ.

3.1.2. Интеграция с серией стандартов 27000

Разработанный метод оценки рисков в основном соответствуют серии стандартов ISO 27000, однако часть идей были взяты из стандартов ISO 31000 и NIST 800-30. Серия ISO 27000 соответствует СМИБ (система менеджмента информационной безопасности), основанной на модели PDCA, поэтому имеет возможность постоянного улучшения.

Рисунок 3. Модель PDCA, определенная в ISO 27000

СМИБ постоянно улучшает процесс оценки рисков и поддерживает безопасность системы. На этапе планирования организация определяет активы, требующие защиты, требования к безопасности, риски, связанные с доступом к информации, а также выбирает методы контроля. На этапе выполнения организация применяет политику безопасности, выбранную раннее, с целью контроля рисков. На этапе проверки организация проверяет и оценивает эффективность реализованного метода. На этапе воздействия организация предпринимает корректирующие действия и превентивные меры для повышения эффективности.

3.1.3. Основные проблемы, которые необходимо решить

Основные задачи, возникающие в процессе оценки рисков – идентификация рисков, с которыми может столкнуться организация, определение вероятности и возможных воздействий риска, определение устойчивости организации к рискам, определение мер по противостоянию рискам и ответные действия при их наступлении. Необходимо ответить на несколько важнейших вопросов:

1. Какие ключевые активы необходимо защитить? Какова их потребительская стоимость?

2. С какими потенциальными угрозами могут столкнуться активы? Каков источник этих угроз? Какова вероятность, что эти угрозы действительно возникнут?

3. Какие уязвимости есть у активов? Чем можно воспользоваться? Насколько легко это осуществить?

4. Если с активами что-то произойдет, какой урон это нанесет организации? С какими последствиями она столкнется?

5. Какие меры безопасности должна предпринять организация для контроля и снижения риска до приемлемого уровня?

3.2. Структура разработанной методологии

Метод будет разрабатываться на основе инструкции стандартов ISO серии 27000, ключевые определения будут взяты из документации стандартов. В этой части будет подробно описаны процесс и модель.

Цель работы данной модели – нахождение всех видов информационных рисков для определенной организации. В разрабатываемой модели будет задействована концепция ERM (управление рисками предприятия). ERM помогает сформировать представление об организации с трех разных уровней: уровня предприятия, бизнес-уровня и операционного уровня. Согласно модели COSO ERM, для каждого уровня мы рассматриваем восемь компонентов риска, которые также соответствуют модели PDCA стандартов ISO. В инструкции ISO 27005 также говорится: “Оценка риска часто

проводится за две (или более) итерации. Сначала проводится высокоуровневая оценка для идентификации потенциально высоких рисков, служащих основанием для дальнейшей оценки. Следующая итерация может включать дальнейшее углубленное рассмотрение потенциально высоких рисков. В тех случаях, когда полученная информация недостаточна для оценки риска, проводится более детальный анализ, возможно, по отдельным частям сферы действия, и, возможно, с использованием иного метода».

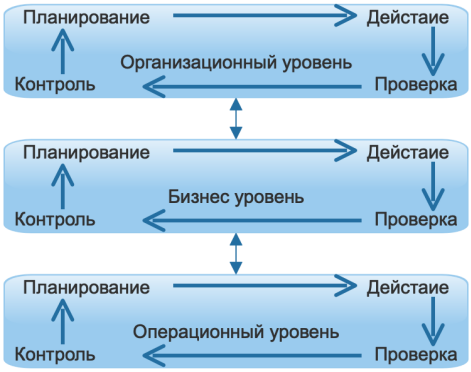

Рисунок 4. Поток данных между различными уровнями ИТ-систем в процессе оценки рисков

Процесс можно представить следующим образом: поток данных, идущий от верхнего уровня к нижнему, определяет информацию и руководство. Также он включает в себя информацию, полученную с помощью обратной связи, которая помогает улучшать процесс оценки, от нижнего к верхнему уровню.

3.3. Реализация метода

После того, как была определена структура метода оценки рисков, необходимо перейти непосредственно к его реализации. Разрабатываемый метод будет соответствовать инструкциям стандартов на всех трех уровнях организации проведения оценки рисков. В данной работе в качестве примера, иллюстрирующего процесс оценки рисков, будет рассмотрен операционный уровень. Согласно ISO 27005 процесс оценки рисков состоит из четырех частей: 1) идентификации риска, 2) анализа риска, 3) оценки риска и 4) предотвращения риска. В процессе идентификации рисков необходимо

определить активы, которые наиболее подвержены рискам, угрозы, существующие меры контроля, уязвимости и возможные последствия. В процессе анализа риска будут принято решение, какой тип методологии идентификации рисков необходимо использовать – качественный или количественный. Затем необходимо будет определить последствия и вероятность наступления рисковых событий, а также вычислить их общий уровень. Для того, чтобы объединить мнения нескольких экспертов, произвести сравнение критериев оценки, а также учесть факторы, имеющие отношение к оценке, в разрабатываемом методе будет использована нечеткая логика. Последним шагом является предотвращение рисков. На данном этапе происходит модификация рисков, их сдерживание, попытки избежать наступления рисковых событий, а также разделение рисков с внешними сторонами.

3.3.1. Подготовительный этап

В самом начале процесса оценки рисков организации необходимо определить цель, с которой проводится оценка рисков. Данная цель должна соответствовать требованиям конфиденциальности, неприкосновенности и доступности объекта, а также поддерживать бизнес стратегию на более высоком уровне. После того, как была определена цель процесса оценки рисков, организации необходимо выполнить следующие шаги:

- определить сферу оценки риска;

- разработать критерии оценки риска информационной системы;

- выбрать подходящую основу и стандарт для оценки риска. В данной работе будут использованы следующие инструменты: COSO ERM, метод анализа иерархии, метод нечеткой логики и стандарты ISO серии 27000.

– наладить или построить коммуникационные связи между руководством и техническими командами, для того чтобы специалисты могли оперативно получать информацию, необходимую для процесса оценки рисков.

Очень важным моментом является создание компетентной команды для процесса оценки рисков. Команда состоит из лидера проекта, который имеет все необходимые знания в области оценки рисков и обладает управленческими навыками. Затем в команде должны быть специалисты, обладающие опытом в технической сфере и в процессе оценки рисков. При наличии возможности, в команде должен быть сертифицированный специалист со знаниями стандартов информационной безопасности и имеющий опыт работы с необходимыми инструментами. В случае необходимости возможна помощь стороннего консультанта, обладающего нужными знаниями.

Для того, чтобы определить необходимость привлечения сторонних консультантов, нужно выбрать наиболее подходящий подход для конкретного проекта по оценке рисков – инсорсинг, частичный аутсорсинг или полный аутсорсинг. Инсорсинг подразумевает работу только внутренних специалистов, при полном аутсорсинге необходимо будет нанять достаточное количество специалистов для работы над всем проектом. В случае частичного аутсорсинга необходимо нанять небольшое количество специалистов, в зависимости от требований проекта. Иногда в работу включены несколько экспертов, которые на одни и те же аспекты оценки рисков высказывают разные точки зрения. Для того, чтобы сбалансировать полученные в данном случае результаты, применяется метод нечеткой логики. Подробнее это будет рассмотрено в пункте 1.3.3.

3.3.2. Идентификация рисков

Процесс идентификации рисков заключается в определении активов, которые необходимо защитить, потенциальных угроз и уязвимостей информационной системы. Во время процесса идентификации происходит сбор необходимых данных для последующего анализа рисков. В приложении В стандарта ISO 27005 привоеден пример идентификации и оценки активов, а также проводится оценка влияния наступления угроз. На этапе сбора данных для идентификации активов крайне важно мнение экспертов. Для того, чтобы получить наиболее точные результаты необходимо использовать метод

«Делфи». В иных случаях могут применяться общие методологии исследования, такие как опросники, интервью с персоналом и пользователями, физический осмотр или анализ документов. Далее подробно рассмотрим процесс идентификации рисков.

a. Анализ компонентов системы. На данном шаге необходимо проанализировать информационную систему (в рамках диссертации будет рассмотрен операционный уровень системы) и различные подсистемы, касающиеся процесса оценки рисков и определенных на предыдущих этапах. Все должно соответствовать организационной структуре и бизнес-процессам. Для более точной картины можно составить карту топологии системы. Хорошим примером являются сетевые топологии. Для того, чтобы идентифицировать все риски информационной системы необходимо учитывать не только сетевые компоненты, но и программное обеспечение, рабочую среду и прочие элементы. Четкая структура системы и определенный уровень требований к защите для различных частей системы упрощает процесс идентификации активов и управления рисками.

b. Идентификация активов: Список активов может быть составлен на основе данных, собранных на этапе анализа. После составления списка, для каждого из актива необходимо определить его ценность. Оценка происходит на основе трех атрибутов: конфиденциальности, неприкосновенности и доступности. Существуют качественные и количественные методы оценки. В приложении B стандарта ISO 27005 приведен пример того, как проводить данную оценку.

c. Идентификация угроз: В приложении B3 стандарта ISO 27005 представлены типичные виды угроз для информационных систем. В данном списке также отображены источники угроз и возможные последствия наступления рисковых событий. На данном этапе лучше всего обратиться к этой или другим профессиональным библиотекам / базам данных и сравнить предложенные примеры с активами, список которых был составлен ранее. Основные методы исследований, которые были представлены в начале главы

6.3.2, также могут быть использованы. На этом этапе необходимо составить таблицу, включающую в себя активы и возможные угрозы. После этого для каждой из угроз необходимо определить вероятность ее наступления, которая определяется исходя из опыта экспертов или из статистических данных, собранных раннее.

d. Идентификация уязвимостей: идентификация уязвимостей будет проводится на основании определения, данного в пункте 3.1.3. Так как уязвимость не имеет значения до тех пор, пока не наступило рисковое событие, то данный шаг будет находиться после идентификации угроз. Помимо обычных методов исследований, упомянутых в начале данной главы, могут использоваться некоторые технические методы, такие как автоматизированное сканирование уязвимостей, тестирование и оценка безопасности, тестирование на проникновение, проверка кода. Сила воздействия будет определена для каждого уязвимого элемента в зависимости от серьезности последствий. После выполнения данного этапа необходимо составить таблицу зависимости между активами, угрозами и уязвимостями.

e. Идентификация способов контроля: Согласно стандарту ISO 27005, контроль существующих рисков определяется, исходя из документации по контролю и плану реализации предотвращения рисков. Существует два типа контроля рисков: 1) предотвращение потенциальных угроз, которые еще не наступили и 2) защита от уже существующих уязвимостей. Достаточно сложно оценить данный этап. Однако в конце будет составлен список способов контроля и методов реагирования на наступление рисковых событий. Выполнение данного этапа поможет лучше определить вероятность возникновения угрозы, а также ее влияние на систему, в том случае наступления рискового события. На рисунке 10 показана структура всех элементов, которые необходимо идентифицировать для оценки риска в информационной системе.

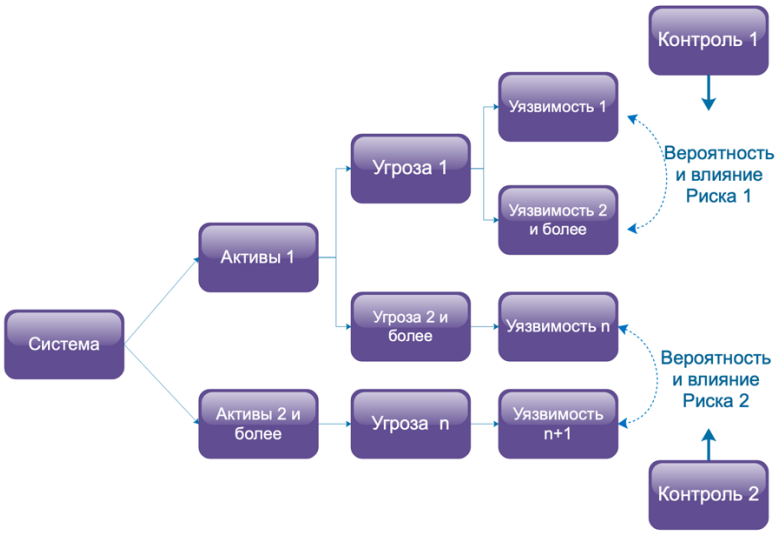

Рисунок 5. Структура критериев оценки рисков

После идентификации, необходимо перейти к следующим этапам – анализу и вычислению.

3.3.3. Анализ и оценка рисков

С помощью информации, полученной от выполнения предыдущих этапов, у команды по оценке рисков будет четкое понимание факторов, влияющих на риски для информационной системы. Далее необходимо провести индивидуальную и комплексную оценку влияния данных факторов. Это означает, что для факторов различной ценности необходимо провести стандартизацию значений, для того чтобы сравнить их и прийти к средневзвешенному значению. Существуют как количественные, так и качественные методы оценки факторов влияния. В данной работе для этого этапа был выбран метод нечеткой логики.

Для начала необходимо присвоить значения для каждого фактора влияния, после чего необходимо дать комплексную оценку всему риску в целом. Это стандартный подход при работе с качественными данными, значения которых варьируются в определенном диапазоне. Общий анализ собранных данных позволяет получить количественное значение для окончательной оценки. Детально процесс будет описан в дальнейших главах. Метод нечеткой логики хорошо подходит для унификации мнений различных экспертов. При использовании данного метода необходимо присвоить вес

каждому из мнений, основываясь на базовых требованиях. Таким образом будет получен наилучший теоретический результат при минимальном объективном вмешательстве. Существуют и другие способы количественной оценки, которые не были рассмотрены в диссертации.

Если рассматривать систему с точки зрения структуры, каждый фактор, оказывающий влияние на определенный уровень, также влияет на более высокие уровни системы. Поэтому необходимо определить вес влияния каждого фактора и для более высоких уровней. Для этих целей будет использован метод анализа иерархий (МАИ). Благодаря данному методу можно определить влияние факторов, расположенных на нижнем уровне, на конечную цель. Для этого необходимо создать матрицу оценки и сравнить факторы друг с другом. Построение матрицы поможет учесть взаимосвязь между факторами влияния и многоуровневыми проблемами.

Метод анализа иерархий – стандартный метод субъективной оценки, который очень зависит от опыта и мнения человека, принимающего решение. Метод «Делфи», схож с МАИ, в нем сочетаются экспертные мнения и вычисление весов. Существуют и объективные методы оценки. Например, метод перекрестной энтропии. Он более точен и гибок, но требует большего количества времени на вычисления.

Структура МАИ вне зависимости от рассматриваемой системы следующая:

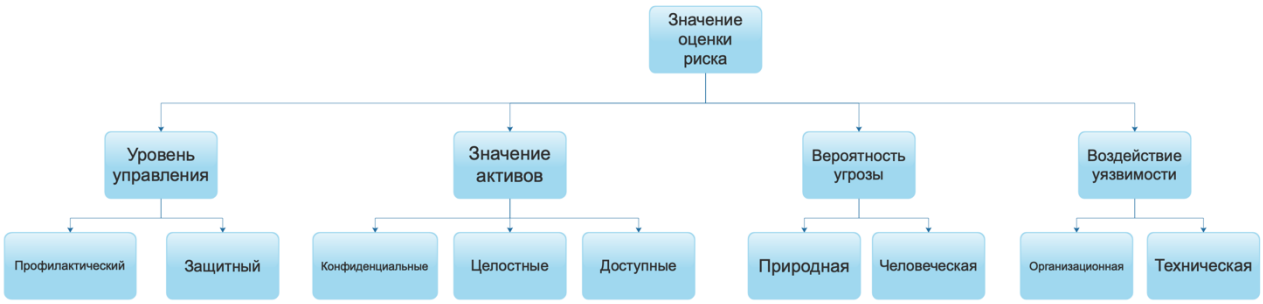

Рисунок 6. Структура оценки рисков МАИ

Первыми тремя уровнями МАИ являются – уровень цели, уровень критериев и уровень альтернатив. С помощью метода парных сравнений

определяются веса каждого из факторов влияния. Если для примера рассмотреть уровень критериев, то для каждого оцененного критерия можно составить матрицу суждений на основе мнения эксперта. Следуя методу, будет получена таблица сравнения, состоящая из девяти уровней.

Таблица 2. Сравнение факторов

Результат (M)	Значение
1	Оба фактора одинаково важны
3	Один немного более важен, чем другой
5	Один более важен, чем другой
7	Один значительно более важен, чем другой
9	Один гораздо более важен, чем другой
2, 4, 6, 8	Дополнительное медианное значение к предыдущему критерию
1, 1/2, 1/3, ... 1/9	Взаимообратное значение, по сравнению с предыдущим критерием

Далее мы можем составить матрицу суждений (таблица 3).

Таблица 3. Матрица суждений

	Контроль	Активы	Угрозы	Уязвимости
Контроль	1	M_1	M_2	M_3
Активы	1/ M_1	1	M_4	M_5
Угрозы	1/ M_2	1/ M_4	1	M_6
Уязвимости	1/ M_3	1/ M_5	1/ M_6	1

В матрице суждений M1 представляет уровень важности - Управляющий фактор по аналогии с Активным фактором при рассмотрении процесса оценки рисков. А 1 / M1 представляет обратные отношения, как показано на рисунке. Остальные параметры перечислены аналогично. Таким образом мы получаем матрицу расчета:

$$W = \begin{bmatrix} 1 & M1 & M2 & M3 \\ 1/M1 & 1 & M4 & M5 \\ 1/M2 & 1/M4 & 1 & M6 \\ 1/M3 & 1/M5 & 1/M6 & 1 \end{bmatrix}$$

Чтобы нормализовать матрицу необходимо присвоить веса для четырех факторов (W1, W2, W3, W4). После того, как будет определен вес каждого

фактора, будет составлена оценочная матрица для объединения мнений нескольких экспертов. Матрица оценки имеет следующий вид:

$$R_g = \begin{bmatrix} R11 & R21 & R31 & R41 \\ R12 & R22 & R32 & R42 \\ \dots & \dots & \dots & \dots \\ R1j & R2j & R3j & R4j \end{bmatrix}$$

В матрице R_{ij} – это оценка каждого фактора риска, полученная от каждого эксперта, i – представляет из себя четыре фактора риска: Контроль, Активы, Угрозы, Уязвимости. Именно они влияют на финальную оценку рисков информационной системы. А j – номер, присвоенный эксперту. Для количественной оценки факторов риска эксперт может назначить вес от 1 до 5 для каждого R_{ij}, где 1- наименее важное значение, а 5 - чрезвычайно важное значение для критериев верхнего уровня. Если нужна более детальная оценка шкала может быть расширена от 1 до 9. Окончательные риски могут быть представлены следующим образом:

$$R_{final} = W_g * R_g = (W_1, W_2, W_3, W_4) * \begin{bmatrix} R11 & R21 & R31 & R41 \\ R12 & R22 & R32 & R42 \\ \dots & \dots & \dots & \dots \\ R1j & R2j & R3j & R4j \end{bmatrix},$$

Где W_g – это вес каждого из четырех факторов риска, которые были получены из матрицы суждений. R_g представляет из себя матрицу мнений, составленную экспертами. Для подуровней применяется тот же метод, поэтому влияние и вероятность каждого фактора на цель будут очень четко определены, как показано в таблице 4.

Таблица 4. Таблица решений для анализа МАИ

Критерии Первого уровня	Оценка	Критерии Второго Уровня	Оценка
Управление	R1	Профилактический	S1
		Защитный	S2
Активы	R2	Конфиденциальный	S3
		Целостный	S4
		Доступный	S5
Угрозы	R3	Природный	S6

		Человеческий	S7
Уязвимость	R4	Оперативный	S8
		Технический	S9

Таким образом, результатом оценки будет обобщенное суждение всех экспертов относительно каждого фактора влияния. Окончательный риск можно оценить, рассматривая систему снизу-вверх, поэтапно, используя данный метод. После того, как были определены значения факторов риска, можно сравнить их с предыдущими критериями и оценить общий риск. В приложении E2 стандарта In ISO 27005 для данной цели рекомендовано три метода. Первый – составление матрицы с предварительно определенными значениями. Второй – ранжирование угроз по показателям риска. Третий - оценка значения вероятности и возможных последствий рисков. Несмотря на то, что в результате проделанной работы уже имеются абсолютные значения для факторов риска, они не имеют практического значения без привязки к конкретной рабочей среде. Создание матрицы рисков в данном случае было бы более подходящим способом оценки этих факторов.

		1			2			3			4			5			Вероятность угроз
		1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	Удобство изучения
1	1																
	2																
	3																
2	1																
	2																
	3																
3	1																
	2																
	3																
4	1																

	2																
	3																
5	1																
	2																
	3																
Значение активов	Текущий уровень контроля																

Рисунок 7. Общая матрица рисков

На рисунке 7 окончательные риски записаны в форме матрицы с четырьмя факторами риска. Используя данную матрицу, достаточно просто определить уровень риска – необходимо просто посмотреть на положение риска в матрице. На практике случаи могут быть более сложными и их можно проанализировать иначе, метод достаточно гибкий. Матрицу рисков также можно визуализировать в других формах, некоторые расписывают ее по 3 осям или с другими атрибутами, однако принцип остается тем же.

3.4. Оставшиеся проблемы

Предложенная в диссертации методология основывается на стандартах ISO серии 27000. Несмотря на то, что это международные стандарты, принятые повсеместно, некоторые проблемы остаются нерешенными. Появление данных проблем возможно по разным причинам: среда, в которой производится работа, не позволяет осуществить все необходимые процессы; ресурсы организации крайне ограничены; неточное или непонятное описание процессов. Могут возникнуть и другие сложности, например, на каком уровне организация должны идентифицироваться активы? Слишком высокое значение приведет к снижению точности расчетов, а слишком маленькое – к большим временным затратам.

Во время процесса идентификации угроз и уязвимостей мы можем столкнуться с похожими проблемами. Поэтому очень важно принимать их к сведению. Однако создать четкие правила, подходящие для каждого проекта, достаточно сложно. Именно поэтому, если над проектом работает неопытный

человек это станет источником дополнительных проблем и неточностей в вычислениях. Важно понимать, что опыт работы играет большую роль в процессе управления рисками.

4. Разработка программного продукта для помощи в процессе управления рисками информационной безопасности.

На протяжении более чем 50 лет задача обеспечения безопасности была основным стимулом для разработки и внедрения средств осуществления внутреннего контроля за физическими угрозами производственных процессов. И хотя этот стимул сохранился до сих пор и помогает поддерживать процессы в защищенном и рабочем состоянии, перечень потенциальных угроз пополнился киберугрозами. Поэтому сегодня систематический подход к обеспечению кибербезопасности требует разработки единой программы защиты бизнес-процессов и производственных процессов. Создание программы такого рода подразумевает многолетнюю работу, однако на каждом этапе трансформации необходимо преследовать одну и ту же цель, постепенно повышая уровень развития внутренних контрольных процедур для создания безопасной, готовой к работе и защищенной контрольной среды.

4.1. Разработка структуры единой системы управления рисками информационной безопасности

Для повышения уровня безопасности и защиты критически важных объектов энергоснабжения нефтегазодобывающих компаний предлагается применить четырехэтапный процесс организации информационной безопасности, включающий в себя оценку вероятных угроз, разработку политики информационной безопасности и мероприятий для обеспечения ее соблюдения, рекомендованные средства защиты и программные продукты для мониторинга и управления системами информационной безопасности.

Рассмотрим каждый из этапов более подробно:

1. Оценка.

На начальном этапе происходит сбор сведений о текущем уровне зрелости информационной безопасности предприятия. Данные должны включать в себя сведения об осведомленности предприятий о возможных угрозах, идентификацию уязвимых мест и возможных рисков информационной безопасности. Также необходимо провести оценку эффективности текущей системы защиты, применяя методики испытания на проникновение.

2. Разработка политики информационной безопасности и мероприятий для обеспечения ее соблюдения.

После проведения оценки текущей ситуации информационной безопасности предприятия, необходимо разработать единую политику информационной безопасности. В результате будет получен документ, в котором будут обозначены цели и задачи деятельности по обеспечению информационной безопасности, описание объектов защиты, описаны возможные угрозы информационной безопасности, определена организационная основа деятельности по обеспечению информационной безопасности. Также необходимо определить лица, которые будут ответственны за соблюдение положений политики безопасности и обеспечить контроль за соблюдением положений разработанного документа.

3. Рекомендация средств защиты.

С ростом информационных технологий меняется и виды кибератак. Хакеры становятся все более изобретательными, изобретая комибинированные методы и разрабатывая сложный вредоносный код. Учитывая темпы цифровизации нефтегазодобывающей отрасли, важно выбрать наиболее подходящие программные продукты и аппаратные средства для обеспечения максимальной защиты активов от внешнего воздействия.

4. Мониторинг и управление системами информационной безопасности.

Учитывая круглосуточный характер функционирования инфраструктуры в нефтегазодобывающей отрасли, организациям необходимо осуществлять мониторинг и управление системами безопасности, включая круглосуточный мониторинг и управление информационными ресурсами, выполняемые в режиме реального времени в целях предотвращения нарушений нормального хода работы и снижения времени простоя.

Эффективно организованный процесс информационной безопасности требует периодического выполнения оценки уязвимостей систем АСУ ТП и РСУ. Ключевым моментом оценки уровня защиты является испытание на проникновение, проведение которого усложняется непрерывным режимом работы управляющих сетей нефтегазодобывающих объектов. В то же время, круглосуточный характер функционирования таких сетей фактически исключает возможность привлечения обычных компаний-оценщиков информационной безопасности, не обладающих соответствующим опытом проведения испытаний на проникновение в среде АСУ ТП и РСУ.

Такая оценка уровня безопасности и степени риска осложняется тем, что в составе инфраструктуры в целом и в рамках нефтеперерабатывающих заводов в частности реализованы самые разные системы. Взаимосвязанность систем АСУ ТП, РСУ, корпоративных сетей и удаленных специалистов наряду с возрастающей частотой и серьезностью кибератак обусловливает необходимость усиления и обязательного соблюдения мер безопасности на объектах критически важной инфраструктуры – несмотря на отсутствие правил информационной безопасности, предписанных конкретно для данной отрасли.

4.2. Определение приоритетных направлений обеспечения информационной безопасности нефтегазодобывающих предприятий

При разработке программного продукта для помощи в процессе управления рисками информационной безопасности необходимо учитывать специфику нефтегазодобывающей отрасли и, как следствие, определить приоритетные направления для наиболее точных рекомендаций.

Защищенность.

Обеспечивать безопасность системы – значит устранять нарушения и предотвращать взломы путем внедрения эффективных автоматизированных средств контроля и мониторинга. Однако обеспечить одинаковый уровень защищенности всех систем – это очень сложная задача. Очевидно, что важные активы и объекты инфраструктуры, а также соответствующие ICS-системы являются наиболее приоритетными целями. Однако необходимо помнить, что они не представляют собой разрозненные и изолированные компоненты. Это лишь часть масштабных цепочек поставок, и поэтому важно укреплять слабые места в рамках всего процесса. Это может подразумевать работу на многих уровнях и использование самых различных видов контроля: от использования защитных сенсоров на производственных объектах до установки программных брандмауэров. Необходимо разрабатывать системы с таким расчетом, чтобы предприятие, эксплуатирующее тот или иной актив, являлось не единственной организацией, имеющей доступ к соответствующим данным. Сервисные компании, поставщики и производители оборудования также могут получить доступ к операционным данным и данным о работе оборудования в целях повышения качества своих услуг. При отсутствии четкой структуры работы могут создаваться возможности для непредвиденной утечки данных или уязвимости систем, которые могут быть легко использованы в своих целях третьими лицами. При разработке систем осуществления контроля и мониторинга процессов важно обеспечивать четко определенные права доступа к данным и возможность отслеживать нарушение таких прав.

Готовность к угрозам.

Однако просто обеспечивать безопасность недостаточно. Необходимо также подготавливать системы к возможным угрозам или же проводить непрерывный мониторинг, чтобы всегда иметь информацию о том, защищена ли система или же была взломана. Для того, чтобы меры по обеспечению готовности систем к угрозам давали реальные результаты, необходимо с

самого начала понимать, от чего необходимо защититься. Применительно к киберугрозам в нефтегазодобывающем секторе прослеживается четкая закономерность, которая позволяет получить базовое представление о том, какие виды атак могут производиться на ICS-системы нефтегазодобывающих компаний. В то же время это представление должно дополняться пониманием специфики бизнес-рисков конкретной организации, чтобы спрогнозировать возможные происшествия и соответствующим образом спроектировать системы по обнаружению угроз.

Гибкость.

Устойчиво функционирующая организация должна иметь планы и процедуры для обнаружения, сдерживания или нейтрализации последствий кибератак и оперативного восстановления штатного режима работы. Вкратце эти шаги можно обозначить следующим образом: «обнаружить», «среагировать» и «восстановить работу». Набор конкретных мер для обеспечения успеха будет зависеть от вида выявленной угрозы. На всех уровнях цепочки создания стоимости нефтегазодобывающих предприятий, идет ли речь о подготовке устья скважины, переработке, транспортировке или же очистке и поставке продукции, необходимо проводить постоянный мониторинг состояния оборудования, чтобы обнаруживать любые отклонения Разработка единой программы Интегрированный подход к управлению киберрисками / Обеспечение безопасности операционной деятельности в нефтегазодобывающем секторе в его работе в режиме реального времени. Это подразумевает постоянное получение информации о состоянии насосного оборудования, трубопроводной арматуры, компрессоров и технологических узлов, включая данные о темпах добычи и движении жидкостей и газов. Постоянная осведомленность о динамике роста этих показателей позволит быстро принимать меры для устранения угроз окружающей среде и безопасности людей, возникающих при выходе оборудования из-под контроля, вплоть до остановки производственных процессов в случае такой необходимости.

При проведении операций по переработке или очистке нефти и природного газа обнаружить факты незаконного присвоения или изменения служебной коммерческой информации об эксплутационных характеристиках скважин, текущих темпах добычи или использованию активов может оказаться сложной задачей. Поэтому очень важно внедрять средства защиты уже на этапе разработки систем по управлению такими данными. Даже если средства осуществления контроля не сработают и кибератака не будет обнаружена, способность системы обеспечить эффективное реагирование может помочь минимизировать производственные потери, а также финансовый, экологический и репутационный ущерб. На этапах реагирования и восстановления необходимо будет не только принять немедленные меры по коррекции работы пострадавшего оборудования и систем, но и провести тщательный анализ с целью понимания того, где и как произошла атака, какие недостатки системы создали возможность для ее возникновения и что требуется сделать, чтобы смягчить ее последствия и предотвратить риски в дальнейшем.

Важно отметить, что просто разработать планы и регламенты будет недостаточно. По аналогии с учебной пожарной тревогой, необходимо периодически проверять эффективность применения таких планов и регламентов путем моделирования и проигрывания чрезвычайных ситуаций, требующих совместной работы бизнеси технических специалистов

4.3. Разработка программного продукта для помощи в процессе управления рисками информационной безопасности

Так как ситуация информационной безопасности в зависимости от предприятия будет отличаться, было решено составить список вопросов, ответы на которые будут определять, какие программные продукты и методологии будут рекомендованы для каждого конкретного случая. В таблице 5 представлен список вопросов для идентификации текущего положения дел в информационной безопасности данного предприятия.

Таблица 5. Вопросы для анкетирования.

Вопросы	Варианты ответов
1. Бюджет (в рублях)	(целое число)
2. Количество сотрудников	(целое число)
3. Количество скважин	(целое число)
4. Использование протокола передачи данных WITSML	Да /нет
5. Наличие службы информационной безопасности	Да /нет
6. Количество сотрудников службы информационной безопасности	(целое число)
7. Способ аутентификации сотрудников	a) парольная аутентификация b) двухфакторная аутентификация c)биометрическая аутентификация
8. Высокая зависимость от отдельных сотрудников и изолированных процессов	Да/нет
9. В штате имеются сотрудники, работающие удаленно	Да/нет
10. Проводится регулярное обновление программных продуктов информационной безопасности	Да/нет
11. Проводится регулярное техническое обслуживание аппаратных средств	Да/нет
12. Имеется возможность подключения личного usb устройства	Да/нет
13. Проведение инструктажа по информационной безопасности	a) Раз в год b) раз в пол года c) раз в месяц d) разово, при трудоустройстве e) не проводится
14. Наличие программы реагирования на киберинциденты	Да/нет
15. Количество серверов	(целое число)
16. Наличие инфраструктуры открытых ключей	Да/нет
17. Использование шифрования данных	Да/нет
18. Использование ПО для защищенного документооборота	Да/нет
19. Наличие ПО для межсетевого экранирования	Да/нет
20. Использование виртуальных частных сетей	Да/нет
21. Использование аппаратно-программных средств для обнаружения и предотвращения вторжений	Да/нет
22. Использование аппаратно-программных средств для защищенного удаленного доступа	Да/нет
23. Использование программных средств для защиты беспроводных сетей	Да/нет

24. Использование программных продуктов для защиты от НСД	Да/нет
25. Использование программных средств для организации терминального доступа	Да/нет
26. Использование программных средств для защиты виртуальных сред	Да/нет
27. Использование программных средств для организации резервного копирования	Да/нет
28. Использование программно-аппаратных средств для предотвращения утечки данных	Да/нет
29. Использование программных средств для защиты мобильных устройств	Да/нет
30. Использование программных и аппаратных средств для защиты персональных данных	Да/нет
31. Использование программных и аппаратных средств для защиты АСУ ТП	Да/нет
32. Наличие программно-аппаратных средств для автоматизации управления информационной безопасности	Да/нет
33. Наличие программно-аппаратных средств для управления событиями и инцидентами безопасности	Да/нет
34. Использование программных и аппаратных средств для управления доступом и идентификационными данными	Да/нет
35. Использование программных и аппаратных средств для мониторинга и управления инфраструктурой	Да/нет
36. Использование программных и аппаратных средств для организации IP телефонии и видеоконференций	Да/нет
37. Использование систем контроля за подвижными объектами (Глонасс и GPS мониторинг)	Да/нет
38. Использование систем бесперебойного питания и электроснабжения	Да/нет
39. Наличие политики кибербезопасности и соответствующих процедур	Да/нет
40. Архитектура корпоративной сети реализована с сегментацией	Да/нет
41. Система периметрального уличного освещения	Да/нет

42. Наличие системы видеонаблюдения	Да/нет
43. Наличие охранной сигнализации	Да/нет
44. Наличие средств антитеррористической защиты	Да/нет
45. Наличие системы управления доступом в офисные помещения	Да/нет
46. Инциденты кибербезопасности, произошедшие за последний год	○ Кража данных ○ Фишинг ○ Атака вируса-шифровальщика ○ Атака вируса, стирающего данные ○ Инсайдерские угрозы ○ Потеря конфиденциальных данных из-за сотрудника, работающего удалено
47. Количество рабочих станций	(целое число)

Для того, чтобы определить наиболее предпочтительные методы и инструменты идентификации рисков, было принято решение спроектировать второй блок вопросов. Данные для проектирования были взяты из 3 Главы диссертации «Анализ методологий оценки рисков». Результат представлен на рисунках 8 и 9.

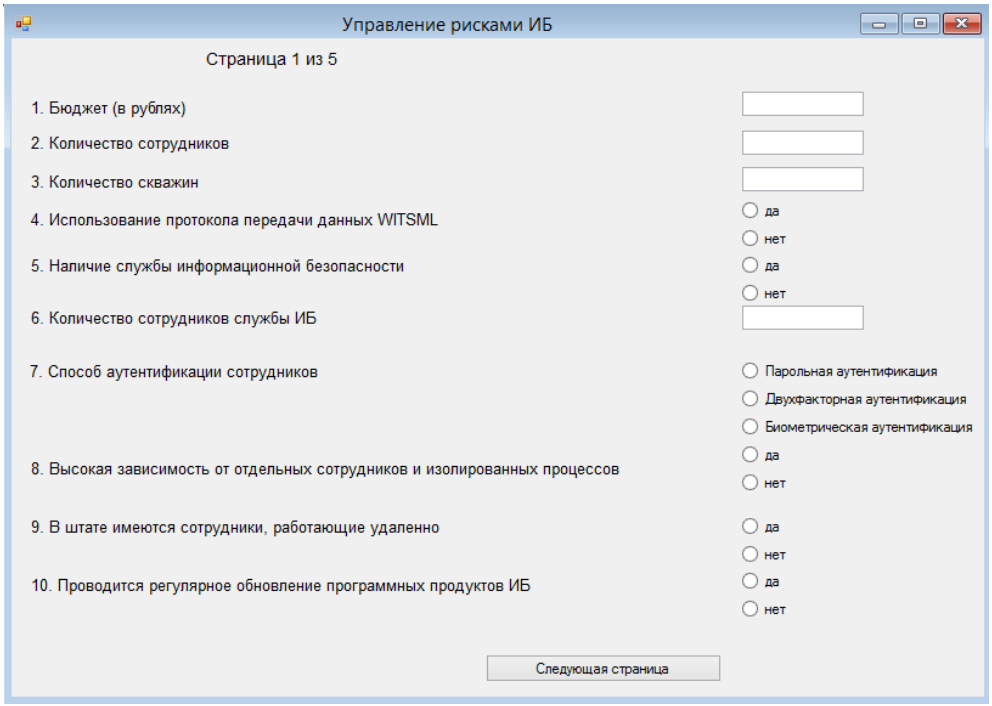

Рисунок 8. Анкета для выявления текущей ситуации информационной безопасности предприятия

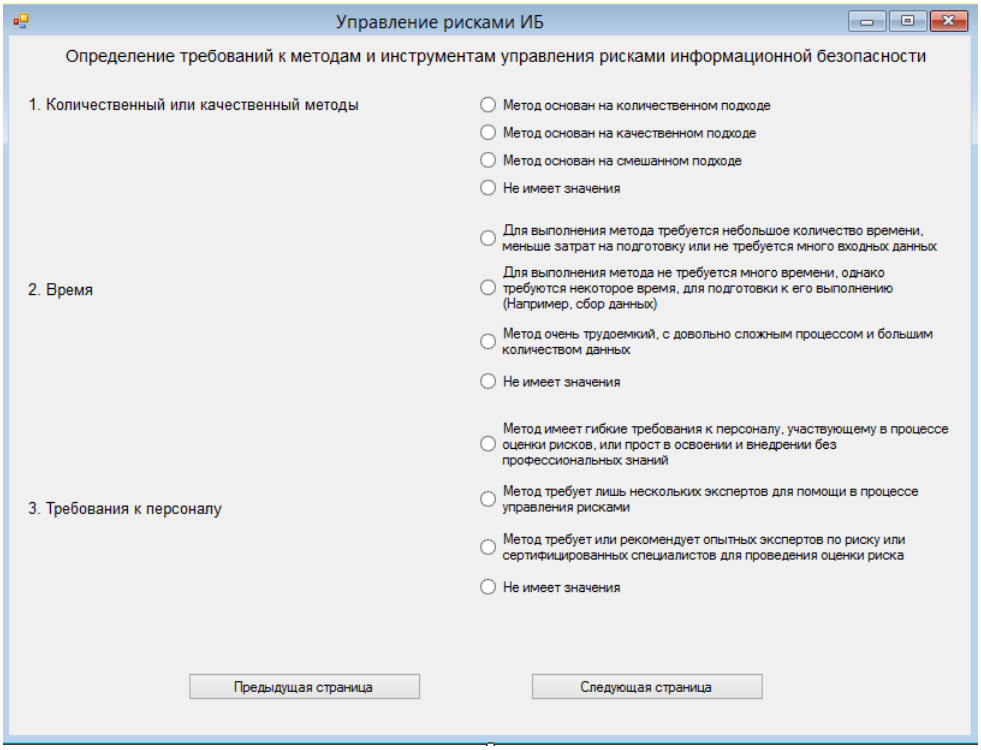

Рисунок 9. Определение требований к методам и инструментам управления рисками информационной безопасности.

Важным моментом является определение бюджета, который предприятие готово потратить на процесс информационной безопасности. Все рекомендованные продукты будут вписываться в рамки казанного в первом вопросе бюджета. При этом, в случае нехватки денежных средств на все рекомендованные продукты, система подбирает рекомендации в порядке приоритета, с учетом специфики нефтегазодобывающей отрасли и особенностями конкретного предприятия.

Для каждого пункта рекомендаций система показывает несколько альтернатив для того, чтобы пользователь имел свободу выбора в случае, если какое из программных продуктов ему не подойдет. Нажав на название программного продукта, пользователь увидит справа краткое описание возможностей и особенностей данного ПО.

Так как системой будет предложено несколько альтернатив, пользователь будет иметь возможность выбрать из них одну или несколько, по своему усмотрению. Для этого необходимо отметить нужные варианты. Внизу программы будет отображен бюджет, который предприятие готово потратить

на информационную безопасность и итоговая сумма, которая складывается из итоговой стоимости выделенных продуктов. В случае, если итоговая стоимость станет выше бюджета, строка будет отображена красным цветом. Результат работы программы показан на рисунках ниже.

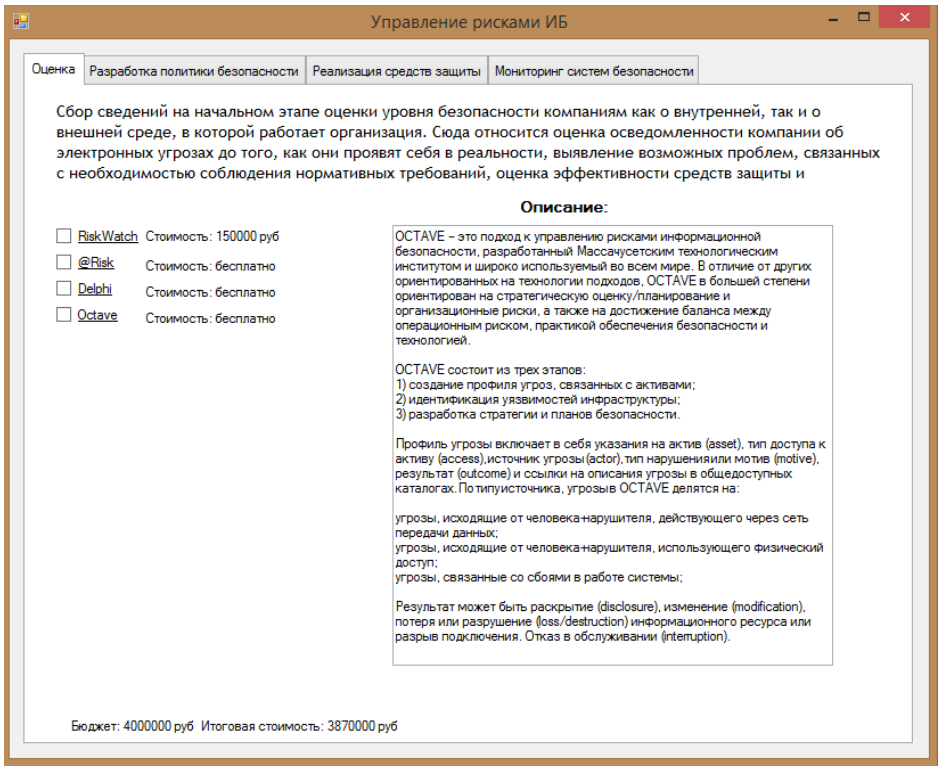

Рисунок 10. Вкладка «Оценка»

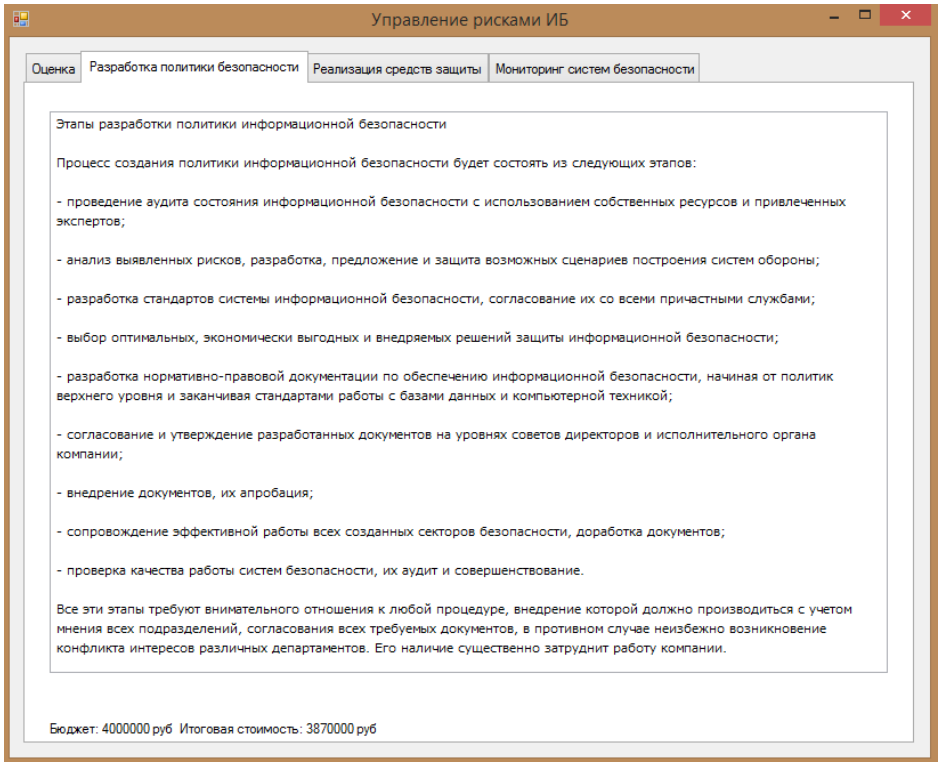

Рисунок 11. Вкладка «Разработка политики безопасности»

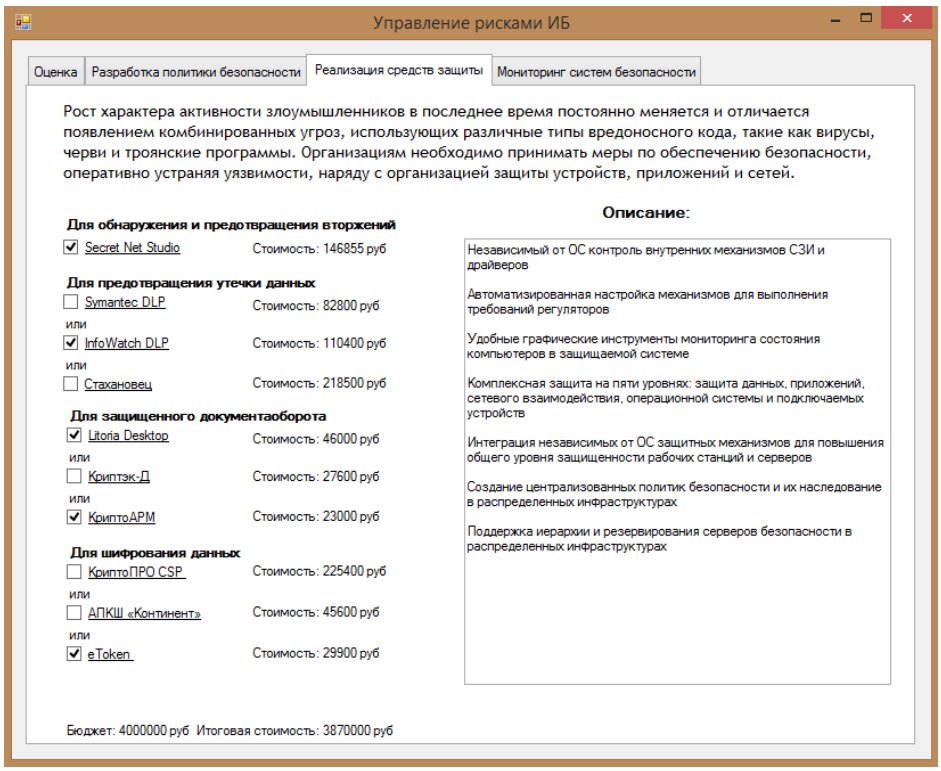

Рисунок 12. Вкладка «Реализация средств защиты»

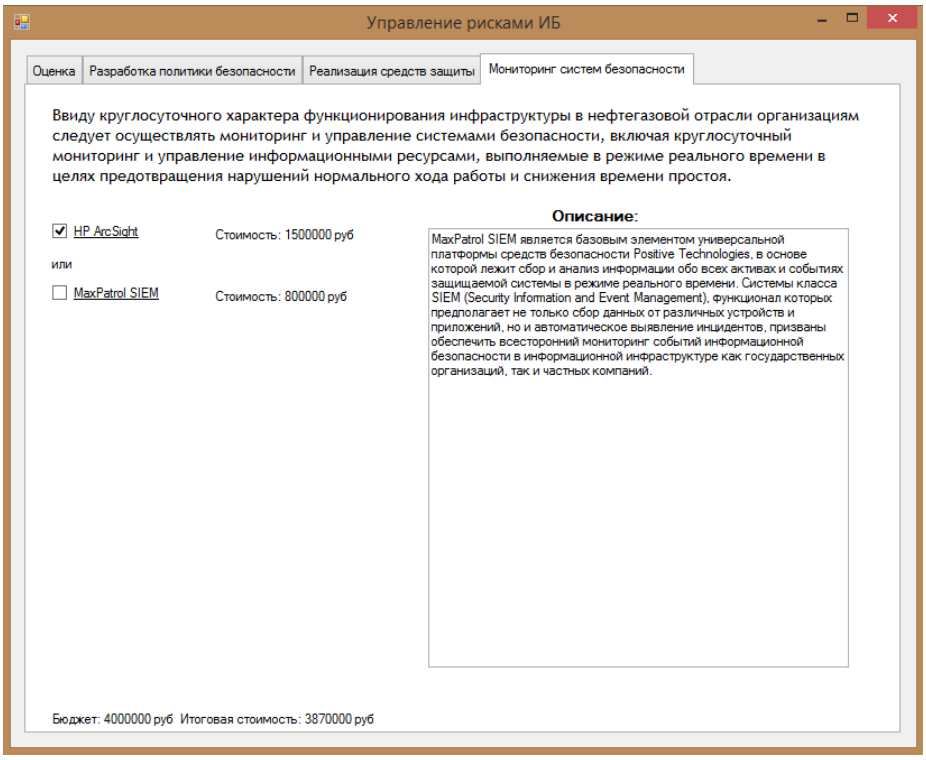

Рисунок 13. Вкладка «Мониторинг систем безопасности»

Применение данного программного продукта поможет предприятию разработать унифицированную программу управления рисками информационной безопасности на предприятии, выявить уязвимые места

текущей системы, эффективно расходовать бюджет, выделенный на информационную безопасность и существенно повысить уровень зрелости системы информационной безопасности предприятия.

5. Финансовый менеджмент, ресурсоэффективность и ресурсосбережение.

5.1. Введение

Для оценки коммерческой привлекательности любого проекта, вне зависимости от того, какой характер он несёт, научный или практический, необходимо определить не только превышение технических параметров над предыдущими разработками, но и дать ответы на такие вопросы – сколько будет стоить проект, каков бюджет данного проекта, будет ли полученный продукт востребован на рынке, сколько потребуется времени для выхода продукта на рынок и т.д. В рамках данной квалификационной работе создается программный продукт, позволяющий пользователям улучшить процесс управления рисками информационной безопасности.

5.2. Оценка коммерческого потенциала и перспективности проведения научных исследований с позиции ресурсоэффективности и ресурсосбережения

5.2.1. Потенциальные потребители продукта исследования

Основными потребителями услуг данного программного продукта являются отечественные и зарубежные компании, занимающиеся нефтедобычей, бурением скважин, разработкой месторождений, а также компании, владеющие буровыми установками. Данные о сегментировании рынка программных продуктов для управления процессом информационной безопасности предоставлены в таблице 6.

Таблица 6. Карта сегментирования рынка продаж услуг программных продуктов для управления процессом информационной безопасности

		Местоположение программных продуктов	
		Зарубежное ПО	Отечественное ПО
Местоположение компании	Зарубежные компании		
	Отечественные компании		

Исходя из данных о сегментировании рынка, можно сделать вывод, что сегмент свободен. Целевым сегментом продажи нашей продукции будут являться отечественные компании, занимающиеся добычей нефти и газа.

5.2.2. Анализ конкурентных технических решений

Для анализа конкурирующих разработок была составлена оценочная карта для сравнения аналоговых продуктов, произведённых иными компаниями, а именно – ООО “НПФ ИСБ” (k1) и “АСТ” (k2), предоставляющих услуги управления процессом информационной безопасности.

Для того, чтобы проанализировать конкурентные технические решения, необходимо использовать формулу:

$$К = \Sigma Вi * Бi, \quad (1)$$

где К – является ли проект или научное исследование конкурентоспособным;

В i – вес i-го критерия (в долях единицы);

Б i – балл i-го показателя.

$К_{ф1}$ = 0,06*4=0,24. Прочие вычисления выполнены по аналогии.

Таблица 7. Карта оценки конкурентоспособности проекта

Показатели	**Вес критерия**	**Баллы**			**Конкурентоспособность**		
		Бф	$Б_{к1}$	$Б_{к2}$	Кф	$К_{к1}$	$К_{к2}$
1	2	3	4	5	6	7	8
Технические критерии оценки ресурсоэффективности							
1. Удобство в эксплуатации	0,06	4	4	3	0,24	0,24	0,18
2. Надежность	0,1	4	4	3	0,4	0,4	0,3
3. Увеличение производительности труда пользователя	0,12	4	4	2	0,48	0,48	0,24
4. Помехоустойчивость	0,05	3	4	4	0,15	0,2	0,2
5. Качество интерфейса	0,05	4	4	4	0,2	0,2	0,2
6. Легкость использования	0,03	4	3	4	0,12	0,09	0,12
7. Количество ресурсов памяти	0,07	3	4	3	0,21	0,28	0,21
8. Функциональность продукта	0,13	4	3	4	0,52	0,39	0,52
9. Отсутствие потери данных	0,1	3	4	4	0,3	0,4	0,4
Экономические критерии оценки эффективности							
10. Уровень конкурентоспособности продукта	0,08	4	5	4	0,32	0,4	0,32
11. Стоимость	0,05	4	3	2	0,2	0,15	0,1
12. Срок эксплуатации	0,05	4	4	4	0,2	0,2	0,2
13. Поддержка продукта	0,07	3	3	4	0,21	0,21	0,28
14. Способность проникнуть на рынок	0,04	4	3	4	0,16	0,12	0,16
Итого	**1**	**52**	**52**	**49**	**3,71**	**3,76**	**3,43**

Найдем коэффициент конкурентоспособности предприятия

$$k_{кс} = К_{ф} / К_{фко} = (3,71/3,76+3,71/3,43)/2 = 1,03.$$

Так как найденный коэффициент больше 1, то можно с уверенностью считать, что наш проект конкурентоспособен. Такими образом была рассмотрена конкурентоспособность относительно существующих отечественных компаний, предоставляющих услуги управления процессом информационной безопасности

5.2.3. Технология QuaD

В данном разделе мы рассмотрим конкурентоспособность нашего проекта с помощью оценочной карты QuaD.

Таблица 8. Карта оценки конкурентных разработок

Показатели	**Вес кри-терия**	**Баллы**	**Максимальный балл**	**Относительное значение**	**Средневзвешенное значение**
1	2	3	4	5	6
Показатели оценки качества разработки					
1. Удобство в эксплуатации	0,1	30	100	0,3	0,03
2. Надежность	0,1	70	100	0,7	0,07
3. Увеличение производительности труда пользователя	0,1	80	100	0,8	0,08
4. Помехоустойчивость	0,05	70	100	0,7	0,035
5. Качество интерфейса	0,05	85	100	0,85	0,0425
6. Легкость использования	0,1	90	100	0,9	0,09
7. Количество ресурсов памяти	0,05	90	100	0,9	0,045
8. Функциональность продукта	0,1	70	100	0,7	0,07
9. Отсутствие потери данных	0,1	3	4	4	0,3
Показатели оценки коммерческого потенциала разработки					
10. Уровень конкурентоспособности продукта	0,08	4	5	4	0,32
11. Стоимость	0,05	4	3	2	0,2
12. Срок эксплуатации	0,05	4	4	4	0,2
13. Поддержка продукта	0,07	3	3	4	0,21
14. Способность проникнуть на рынок	0,04	4	3	4	0,16
Итого	1	52	52	49	3,71

$$П_{ср}=\sum Bi \cdot Б_i, \quad (2)$$

$П_{ср1}$=0,1*0,3=0,03. Прочие вычисления выполнены по аналогии.

где Пср – средневзвешенное значение оценки качества и перспектив научной разработки;

B_i – вес критерия (в долях единицы);

$Б_i$ – средневзвешенное значение *i*-го показателя.

Значение $П_{ср}$ составило 72,25, что показывает перспективность разработки выше среднего.

5.2.4. SWOT-анализ

Посредством SWOT-анализа выявим внешние и внутренние факторы среды проекта, и выявим степень соответствия сильных и слабых сторон проекта внешним условиям окружающей среды.

Таблица 9. Матрица SWOT

		Сильные стороны	Слабые стороны
		С1. Высокое качество программного продукта. С2. Интуитивно понятный интерфейс. С3. Удобство в использовании. С4. Быстрая установка программного продукта. С5. Экономичность ресурсов памяти.	Сл1. Небольшой функционал. Сл2. Локальное приложение. Сл3. Уступает конкурентам в быстродействии. Сл4. Неполная оптимизация функций. Сл5. Ограниченное количество ресурсов
Возможности	В1. Появление дополнительного спроса на продукт. В2. Удовлетворение новой потребности потребителя. В3. Использование дополнительных ресурсов. В4. Появление дополнительных финансовых ресурсов. В5. Повышение стоимости конкурентных разработок	1. Постоянная оптимизация продукта для более удобного пользования. 2. Добавление новых функций в программный продукт.	1. Улучшение быстродействия программного продукта. 2. Повышение конкурентоспособности.

Угрозы	У1. Отсутствие спроса. У2. Выход продукта – конкурента с полным функционалом. У3. Выход продукта – конкурента с более полной информацией об оборудовании. У4. Проблемы с материально-техническим обеспечением У5. Введение дополнительных государственных требований к сертификации продукции	1. За счет повышения качества продукта увеличить спрос на рынке. 2. Уменьшить использование ресурсов оперативной и локальной памяти.	1. Увеличить функционал продукта. 2. Улучшить оптимизацию и уменьшить затраты ресурсов.

Таблица 10. Интерактивная матрица проекта

	Сильные стороны					
Возможности		С1	С2	С3	С4	С5
	В1	+	+	+	+	+
	В2	-	0	-	-	-
	В3	+	-	+	-	-
	В4	+	+	-	+	+
	В5	+	-	+	-	-

Направления реализации проекта: В1С1С2С3С4С5, В3С1С3, В4С1С2С4С5, В5С1С3.

Таблица 11. Интерактивная матрица проекта

Слабые стороны						
Возможности		Сл1	Сл2	Сл3	Сл4	Сл5
	В1	-	-	-	-	-
	В2	0	-	0	+	-
	В3	-	-	-	-	-
	В4	+	-	+	-	+
	В5	-	-	-	-	-

Направление реализации проекта: В2Сл4, В4Сл1Сл3Сл5.

Таблица 12. Интерактивная матрица проекта

Сильные стороны						
Угрозы		С1	С2	С3	С4	С5
	У1	-	+	-	-	+
	У2	-	+	-	+	+
	У3	+	0	-	-	-
	У4	-	0	-	-	-
	У5	0	-	-	+	+

Направления реализации проекта: У1С2С5, У2С2С4С5, У3С1, У5С4С5.

Таблица 13. Интерактивная матрица проекта

	Слабые стороны					
Угрозы		Сл1	Сл2	Сл3	Сл4	Сл5
	У1	+	-	-	-	-
	У2	-	-	-	-	-
	У3	+	-	-	-	+
	У4	+	+	+	+	+
	У5	-	+	-	+	-

Направления реализации проекта: У1Сл1, У3Сл1Сл5, У4Сл1Сл2Сл3Сл4Сл5, У5Сл2Сл4.

К проблемным зонам относятся отсутствие спроса, выход продукта-конкурента с аналогичным функционалом, выход продукта – конкурента с более полной информацией об оборудовании и введение дополнительных государственных требований к сертификации продукции, однако их можно компенсировать сильными сторонами: высокое качество программного продукта, интуитивно понятный интерфейс, удобство в использовании, быстрая установка программного продукта, экономичность ресурсов памяти.

5.3. Нахождение альтернативных способов проведения научных исследований

Для нахождения возможных альтернативных способов проведения научных исследований воспользуемся морфологическим методом. Для этого построим морфологическую матрицу.

Таблица 14. Морфологическая матрица для веб-интерфейса программного продукта

	1	2	3	4	5
А. Тип клиентского интерфейса	Веб-портал	Веб - страница	Веб-приложение	Стационарное приложение	Нет интерфейса
Б. Тип хранения данных	Сервер хранения	Система хранения	Локальные базы данных		
В. Доступ к данным	В режиме реального времени	По запросу клиента	Нет доступа		
Г. Процесс составления договора	Полностью автоматизированный	Частично автоматизированный	Полностью ручной	Отсутствие договора	
Д. Составление тарифного плана	Индивидуальное для каждого клиента	Общее для всех клиентов			
Е. Расчет стоимости услуги	Индивидуальный для каждого клиента	Строго определенная сумма для всех клиентов			
Ж. Способ оплаты услуги	Банковским переводом	Электронные системы оплаты	Личная оплата в кассу		

С помощью морфологического анализа были выделены следующие преимущественные варианты:

1) А1Б2В1Г2Д1Е1Ж1 – разработка веб-портала для управления информационной безопасностью, с использованием глобальной системы хранения и предоставлением рекомендаций программных продуктов для управления информационной безопасности, а также с обеспечением, частично автоматизированного документооборота, и индивидуальными расчетами тарифных планов и стоимости услуг для каждого клиента, оплачиваемых посредством банковского перевода.

2) А2Б1В2Г1Д2Е2Ж2 – разработка веб-страницы для управления информационной безопасностью, с использованием серверов хранения данных и предоставления доступа к данным по запросу клиента, а также с обеспечением полностью автоматизированного документооборота, общие тарифные планы и стоимости услуг для всех клиентов, и оплата посредством электронных платежных систем.

3) А3Б2В1Г1Д1Е1Ж1 – разработка веб-приложения для управления информационной безопасностью, с использованием глобальной системы хранения и предоставлением доступа клиентам к данным скважин в режиме реального времени, а также с обеспечением, полностью автоматизированным документооборотом, и индивидуальными расчетами тарифных планов и стоимости услуг для каждого клиента, оплачиваемых посредством банковского перевода.

5.4. Планирование управления научно-технического проектом

5.4.1. Этапы планирования работ в рамках научного исследования

Таблица 15 Список этапов, содержание работ и распределение ролей

Этапы	№ раб	Содержание работ	Должность исполнителя
Разработка ТЗ	1	Выбор темы	И1, Руководитель
	2	Составление и утверждение ТЗ	Руководитель
Анализ предметной области	3	Создание календарного плана работ	И1
	4	Выбор и изучение теоретических материалов по теме	И1
	5	Анализ изученного материала	И1, Руководитель
	6	Проработка литературных источников и периодической литературы	И1
	7	Анализ текущего положения дел в области управления рисками информационной безопасности в нефтегазовой отрасли	И1

Основная	8	Подбор и категоризация программных продуктов и методологий для управления рисками информационной безопасности	И1
	9	Проектирование основных функций программного продукта	И1
	10	Разработка программного продукта для управления рисками информационной безопасности	И1
	11	Разработка системы формирования финансовой документации	И1
	12	Тестирование и доработка системы	И1
Заключительная	13	Написание пояснительной записки	И1
	14	Создание и оформление презентации дипломного проекта	И1

Для выполнения научного исследования формируется рабочая группа, в состав которой входят 1 студент-дипломник и один руководитель. Порядок этапов и работ, распределение исполнителей по данным видам работ приведен в таблице.

5.4.2. Расчет трудоемкости исполнения работ

Чтобы определить ожидаемое значение продолжительности работ $t_{ож}$ применяются две оценки: t_{min} и t_{max} (метод двух оценок).

$$t_{ожс} = \frac{3 \cdot t_{\min} + 2 \cdot t_{\max}}{5}, \quad (3)$$

$t_{ожс}$= (3*2+2*3)/5=1,2. Прочие вычисления выполнены по аналогии.

где t_{min} – наименьшая трудоемкость работ, чел/дн.;

t_{max} – наибольшая трудоемкость работ, чел/дн.

После нахождения значения ожидаемой трудоемкости работ, необходимо определить длительность каждой работы в рабочих днях $T_р$, учитывая при этом возможность параллельности работ сразу несколькими исполнителями.

$$T_{рi} = \frac{t_{ожi}}{Ч_i}, \quad (4)$$

$T_{рi}$=1,2/3=0,4. Прочие вычисления выполнены по аналогии.

$T_{рi}$ – длительность одной работы, раб. дн.;

где $t_{ожi}$ – ожидаемая трудоемкость выполнения одной работы, чел.-дн.

$Ч_i$ – количество исполнителей, которые выполняют одну и ту же работу параллельно, чел.

Для удобства построения графика, длительность каждого из этапов работ из рабочих дней следует перевести в календарные дни.

$$T_{кi} = T_{рi} \cdot k_{кал}, \quad (5)$$

$T_{кi}$= 0,4*1,47=0,6. Округляем до 1. Прочие вычисления выполнены по аналогии.

где $T_{кi}$– продолжительность выполнения i-й работы в календарных днях;

$T_{рi}$ – продолжительность выполнения i-й работы в рабочих днях;

k – коэффициент календарности. кал

Коэффициент календарности определяется по следующей формуле:

$$k_{кал} = \frac{T_{кал}}{T_{кал} - T_{вых} - T_{пр}}, \quad (6)$$

$k_{кал}$= 365/(365-105-13)=1,47.

где $T_{кал}$ – количество календарных дней в году;

$T_{вых}$ – количество выходных дней в году;

$T_{пр}$ – количество праздничных дней в году.

Для выполнения перечисленных в таблице 10 работ требуются специалисты: студент и научный руководитель. Результаты расчетов представлены в таблице 16.

Таблица 16. Временные показатели проведения научного исследования

№ Работы	**Трудоёмкость работ**									**Исполнители**			**Длительность работ в рабочих днях** T_{pi}			**Длительность работ в календарных днях** T_{ki}		
	tmin, чел-дни			tmax, чел-дни			$t_{ожi}$, чел-дни											
	Исп.1	Исп.2	Исп.3	Исп.1	Исп.2	Исп.3	Исп.1	Исп.2	Исп.3	Исп.1	Исп.2	Исп.3	Исп.1	Исп.2	Исп.3	Исп.1	Исп.2	Исп.3
Выбор темы	2	2	2	3	3	3	1,2	1,2	1,2	3	3	3	0,4	0,4	0,4	1	1	1
Составление и утверждение ТЗ	4	6	5	7	9	8	5,2	7,2	6,2	1	1	1	5,2	7,2	6,2	8	11	9
Создание календарного плана работ	1	1	1	2	2	2	1,4	1,4	1,4	2	2	2	0,3	0,35	0,35	1	1	1
Выбор и изучение теоретических материалов по теме	10	9	11	14	13	15	11,6	10,6	12,6	2	2	2	2,9	2,65	3,15	4	4	5
Анализ изученного материала	7	8	10	10	11	13	8,2	9,2	11,2	3	3	3	1,6	1,84	2,24	2	3	3

Проработка литературных источников и периодической литературы	3	3	3	6	6	6	4,2	4,2	4,2	2	2	2	1,0	1,05	1,05	2	2	2
Анализ текущего положения дел в области управления рисками информационной безопасности в нефтегазовой отрасли	7	10	8	14	18	13	9,8	13,2	10	1	1	1	2,4	3,3	2,5	4	5	4
Подбор и категоризация программных продуктов и методологий для управления рисками информационной безопасности	20	23	26	30	36	31	24	28,2	28	2	2	2	6	7,05	7	9	10	10
Проектирование основных функций программного продукта	31	31	31	50	50	50	38,6	38,6	38,6	1	1	1	38,6	38,6	38,6	57	57	57

Разработка программного продукта для управления рисками информационной безопасности	31	31	31	50	50	50	38,6	38,6	38,6	1	1	1	38,6	38,6	38,6	57	57	57
Разработка системы формирования финансовой документации	31	31	31	50	50	50	38,6	38,6	38,6	1	1	1	38,6	38,6	38,6	57	57	57
Тестирование и доработка системы	31	31	31	50	50	50	38,6	38,6	38,6	2	2	2	38,6	38,6	38,6	57	57	57
Написание пояснительной записки	8	11	16	14	20	24	10,4	14,6	19,2	2	2	2	2,6	3,65	4,8	4	5	7
Создание и оформление презентации научного исследования	7	10	11	10	14	18	8,2	11,6	13,8	2	2	2	2,05	2,9	3,45	3	4	5
Итого	197	211	221	317	339	340	245,2	262,2	269	-	-	-	180,3	186,3	187	268	276	277

Ккал = 365/ (365-118) = 1, 48,

По данным расчетам программа будет разработана:

- в первом исполнении 268 дней
- во втором исполнении 276 дней
- в третьем исполнении 277 дней

Следовательно, можно сделать вывод, что в первом исполнении работы будет выполнена быстрее.

5.4.3. Бюджет научно-технического исследования

При распределении бюджета НТИ необходимо обеспечить полное и достоверное отражение всех видов расходов, связанных с его выполнением. В процессе формирования бюджета НТИ используется следующая группировка затрат по статьям:

- материальные затраты НТИ;
- затраты на специальное оборудование;
- основная заработная плата исполнителей темы;
- дополнительная заработная плата исполнителей темы;
- отчисления во внебюджетные фонды (страховые отчисления);
- накладные расходы.

В рамках данной работы были проведены расчеты по следующим затратам: материальные затраты НТИ, основная заработанная плата исполнителей темы, дополнительная заработанная плата исполнителей темы и отчисления во внебюджетные фонды (страховые отчисления).

5.4.3.1. Расчет материальных затрат НТИ

Расчет материальных затрат осуществляется по формуле 7:

$$З_м = (1 + k_т) \cdot \sum_{i=1}^{m} Ц_i \cdot N_{расх i} \quad (7)$$

$З_м$ = 1* 40052*1=40052. Прочие вычисления выполнены по аналогии.

Где m – количество видов материальных ресурсов, потребляемых при выполнении научного исследования;

$N_{расхi}$ – количество материальных ресурсов i-го вида, планируемых к использованию при выполнении научного исследования (шт., кг, м, м^2 и т.д.);

$Ц_i$ – цена приобретения единицы i-го вида потребляемых материальных ресурсов (руб./шт., руб./кг, руб./м, руб./м^2 и т.д.);

k_T – коэффициент, учитывающий транспортно-заготовительные расходы.

Для разработки данного продукта необходимы следующие материальные ресурсы:

- Система хранения данных
- Два сервера

Расчет материальных затрат представлен в таблице 17.

Таблица 17. Материальные затраты

Наименование	**Единица измерения**	**Количество**			**Цена за ед., руб.**			**Затраты на материалы, ($З_м$), руб.**		
		Исп.1	Исп.2	Исп.3	Исп.1	Исп.2	Исп.3	Исп.1	Исп.2	Исп.3
Система хранения данных DEPO Storage 3436	Шт.	1	1	1	40052	40052	40052	40052	40052	40052
Итого								40052	40052	40052

5.4.3.2. Расчет основной заработной платы исполнителей темы

Для расчета основной заработной платы используется формула 8:

$$C_{осн/зп} = \sum_{i=1}^{n} t_i \cdot C_{зп_i} \quad (8)$$

$C_{осн/зп}$ = 7*1530,2=10711,4. Прочие вычисления выполнены по аналогии.

где n – количество работ;

t_i – затраты труда на выполнение i-го вида работ, в днях;

$C_{зпi}$ – средняя заработная плата работника, который выполняет i-ый вид работы, руб/день.

Средняя заработная плата в день рассчитывается по формуле 9:

$$C_{зп_i} = \frac{D \cdot K \cdot M_p}{F_o} \quad (9)$$

$C_{зпi}$ = (10711,4*1,3*11,08)/219= 1530,2. Прочие вычисления выполнены по аналогии.

где D – должностной оклад работника в месяц;

K – районный коэффициент (K=1,3);

M_p – количество месяцев работы без отпуска в течение года;

F_0 – действительный годовой фонд рабочего времени работника, в днях.

При отпуске 28 дня M_p=11,08.

Результаты расчета действительного годового фонда проведены в таблице 18.

Таблица 18. Баланс рабочего времени

Показатели рабочего времени	**Руководитель**	**Студент1**	**Студент2**
Календарное число дней	365	365	365
Количество нерабочих дней - выходные дни - праздничные дни	118	118	118
Потери рабочего времени - отпуск - невыходы по болезни	28	28	28
Действительный годовой фонд рабочего времени	219	219	219

Расчет затрат на основную заработную плату приведен в таблице 19. При этом затраты на оплату труда студента-дипломника определяются как оклад студента 1 (D = 6976,22), а оклад руководителя проекта составляет 23264,86. Коэффициент К - районный коэффициент равен 1,3, а $М_р$ равно 11,08.

Таблица 19. Затраты на основную заработную плату

Исполнители	**Среднедневная заработная плата $С_{зп}$ (руб.)**			**Трудоемкость (t_i), чел-дни**			**Затраты на основную зарплату (руб.)**		
	Исп. 1	**Исп. 2**	**Исп. 3**	**Исп. 1**	**Исп. 2**	**Исп. 3**	**Исп. 1**	**Исп. 2**	**Исп. 3**
Руководитель	1530,2			7	9	8	10711,4	13771,8	12241,6
Студент 1	458,8			43	44	45	19728,4	20187,2	20646
Итого							30439,8	33959	32887,6

5.4.3.3. Дополнительная заработная плата

Дополнительная заработная плата включает заработную плату за не отработанное рабочее время, но гарантированную действующим законодательством.

Расчет дополнительной заработной платы ведется по формуле 10:

$$З_{доп} = k_{доп} \cdot З_{осн} \quad (10)$$

$З_{доп}$=0,12*10711,4=1285,4. Прочие вычисления выполнены по аналогии.

где $k_{доп}$ – коэффициент дополнительной заработной платы (на стадии проектирования принимается равным 0,12 – 0,15). $k_{доп}$ равен 0,12. Результаты по расчетам дополнительной заработной платы сведены в таблицу 20.

Таблица 20. Затраты на дополнительную заработную плату

Исполнители	**Основная зарплата(руб.)**			**Коэффициент дополнительной заработной платы ($k_{доп}$)**	**Дополнительная зарплата(руб.)**		
	Исп.1	**Исп.2**	**Исп.3**		**Исп.1**	**Исп.2**	**Исп.3**
Руководитель	10711,4	13771,8	12241,6	0,12	1285,4	1652,6	1469
Студент 1	19728,4	20187,2	20646	-	2367,4	2422,5	2477,5
Итого					3652,8	4075,1	3946,5

5.4.3.4. Отчисления во внебюджетные фонды (страховые отчисления)

Величина отчислений во внебюджетные фонды определяется исходя из формулы 11:

$$З_{внеб} = k_{внеб} \cdot (З_{осн} + З_{доп}), \quad (11)$$

$З_{внеб}$ = 27,1*(10711,4+1285,4)= 15227,06**.** Прочие вычисления выполнены по аналогии.

где $k_{внеб}$ – коэффициент отчислений на уплату во внебюджетные фонды (пенсионный фонд, фонд обязательного медицинского страхования и пр.). На 2014 г. В соответствии с Федеральным законом от 24.07.2009 №212-ФЗ, установлен размер страховых взносов равный 30%. На основании пункта 1 ст.58 закона №212-ФЗ для учреждений, осуществляющих образовательную и научную деятельность с 2014 году введена пониженная ставка – 27,1%.

Отчисления во внебюджетные фонды представлены в таблице 21.

Таблица 21. Отчисления во внебюджетные фонды

Исполнитель	**Основная заработная плата, руб.**			**Дополнительная заработная плата, руб.**		
	Исп.1	**Исп.2**	**Исп.3**	**Исп.1**	**Исп.2**	**Исп.3**
Руководитель проекта	10711,4	13771,8	12241,6	1285,4	1652,6	1469
Студент 1	-	-	-	-	-	-
Коэффициент отчислений во внебюджетные фонды	27,1%					
Итого						
Исполнение 1	**15227,06**					
Исполнение 2	**16434,47**					
Исполнение 3	**16248,51**					

5.4.3.5. Формирование бюджета затрат научно-исследовательского проекта

Рассчитанная величина затрат научно-исследовательской работы (темы) является основой для формирования бюджета затрат проекта, который при формировании договора с заказчиком защищается научной организацией

в качестве нижнего предела затрат на разработку научно-технической продукции. Определение бюджета затрат на научно-исследовательский проект по каждому варианту исполнения приведен в таблице 22.

Таблица 22. Расчет бюджета затрат НТИ

Наименование статьи	**Сумма, руб.**		
	Исп.1	**Исп.2**	**Исп.3**
1. Материальные затраты НТИ	40052	40052	40052
2. Амортизационные отчисления	1112.56	1112.56	1112.56
3. Затраты по основной заработной плате исполнителей темы	30439,8	33959	32887,6
4. Затраты по дополнительной заработной плате исполнителей темы	3652,8	4075,1	3946,5
5. Отчисления во внебюджетные фонды	16434,47	16434,47	16248,51
6. Бюджет затрат НТИ	**90579,07**	**94520,57**	**93134,61**

Вывод: Основываясь на данных, полученных в пунктах 5.4.1 – 5.4.3, был рассчитан бюджет затрат научно-исследовательской работы для трех исполнителей. Наиболее низким по себестоимости оказался проект первого исполнителя, затраты на его полную реализацию составляют **90579,07 рублей**.

5.5. Определение ресурсной (ресурсосберегающей), финансовой, бюджетной, социальной и экономической эффективности исследования.

Эффективность научного ресурсосберегающего проекта включает в себя социальную эффективность, экономическую и бюджетную эффективность. Показатели общественной эффективности учитывают социально-экономические последствия осуществления инвестиционного

проекта как для общества в целом, в том числе непосредственные результаты и затраты проекта, так и затраты, и результаты в смежных секторах экономики, экологические, социальные и иные внеэкономические эффекты.

Показатели экономической эффективности проекта учитывают финансовые последствия его осуществления для предприятия, реализующего данный проект. В этом случае показатели эффективности проекта в целом характеризуют с экономической точки зрения технические, технологические и организационные проектные решения.

Бюджетная эффективность характеризуется участием государства в проекте с точки зрения расходов и доходов бюджетов всех уровней.

5.5.1 Динамические методы экономической оценки инвестиций.

Динамические методы оценки инвестиций базируются на применении показателей:

- чистая текущая стоимость (NPV);
- срок окупаемости (PP);
- внутренняя ставка доходности (IRR);
- индекс доходности (PI).

Все перечисленные показатели основываются на сопоставлении чистых денежных поступлений от операционной и инвестиционной деятельности, и их приведении к определенному моменту времени. Теоретически чистые денежные поступления можно приводить к любому моменту времени (к будущему либо текущему периоду). Но для практических целей оценку инвестиции удобнее осуществлять на момент принятия решений об инвестировании средств.

5.5.2 Чистая текущая стоимость (NPV).

Данный метод основан на сопоставлении дисконтированных чистых денежных поступлений от операционной и инвестиционной деятельности.

Если инвестиции носят разовый характер, то NPV определяется по формуле

$$\boldsymbol{NPV = \sum_{t=1}^{n} \frac{ЧДП_{ОП_t}}{(1+i)^t} - I_0},$$

где $ЧПД_{ОП_t}$ – чистые денежные поступления от операционной деятельности;

I_0 – разовые инвестиции, осуществляемые в нулевом году;

t – номер шага расчета (t =0, 1, 2…n);

n – горизонт расчета;

i – ставка дисконтирования (желаемый уровень доходности инвестируемых средств).

Чистая текущая стоимость является абсолютным показателем. Условием экономичности инвестиционного проекта по данному показателю является выполнение следующего неравенства: NPV >0.

Чем больше NPV, тем больше влияние инвестиционного проекта на экономический потенциал предприятия, реализующего данный проект, и на экономическую ценность этого предприятия. Таким образом, инвестиционный проект считается выгодным, если NPV является положительной.

Таблица 23. Расчет текущей стоимости по проекту в целом

№	Наименование показателей	Шаг расчета				
		0	1	2	3	4
1.	Выручка от реализации, тыс.руб	0	1271112	1271112	1271112	1271112
2.	Итого приток	0	1271112	1271112	1271112	1271112
3.	Инвестиционные издержки, тыс.руб.	338963,48	288963,48	288963,48	238963,48	188963,48
4.	Операционные затраты, тыс. руб С+Ам+ФОТ	0	70476,4	70476,4	70476,4	70476,4

5.	Налоги Выр-опер=донал.приб*20 %	0	240127,12	240127,12	240127,12	240127,12
6.	Итого отток Опер.затр+налоги	0	310603,52	310603,52	310603,52	310603,52
7.	Чистый денежный поток ЧДП=п1-п3	-338963,48	982148,52	982148,52	1032148,5	1082148,5
8.	Коэффициент дисконтирования (приведения при i =0,20)	1	0,833	0,694	0,578	0,482
9.	Дисконтированный чистый денежный поток (с7*с8)	-338963,48	818129,72	681611,07	596581,85	521595,59
10.	То же нарастающим итогом	-338963,48	479166,24	1160777,3	1757359,2	2278954,8

Таким образом, чистая текущая стоимость по проекту в целом составляет 2278954,8 д. ед., что позволяет судить о его эффективности.

5.5.3 Дисконтированный срок окупаемости.

Как отмечалось ранее, одним из недостатков показателя простого срока окупаемости является игнорирование в процессе его расчета разной ценности денег во времени. Этот недостаток устраняется путем определения дисконтированного срока окупаемости.

Рассчитывается данный показатель примерно по той же методике, что и простой срок окупаемости, с той лишь разницей, что последний не учитывает фактор времени.

Наиболее приемлемым методом установления дисконтированного срока окупаемости является расчет кумулятивного (нарастающим итогом) денежного потока.

Таблица 24. Дисконтированный срок окупаемости

№	Наименование показателя	Шаг расчета				
		0	1	2	3	4
1.	Дисконтированный чистый денежный поток (i =0,20)	-338963,48	818129,72	681611,07	596581,85	521595,6
2.	То же нарастающим итогом	-338963,48	479166,24	1160777,3	1757359,2	2278954,8
3.	Дисконтированный срок окупаемости	$PP_{дск}$=1+479166,24/681611,07=1,7месяца				

5.5.4 Внутренняя ставка доходности (IRR)

Для установления показателя чистой текущей стоимости (NPV) необходимо располагать информацией о ставке дисконтирования, определение которой является проблемой, поскольку зависит от оценки экспертов. Поэтому, чтобы уменьшить субъективизм в оценке эффективности инвестиций на практике широкое распространение получил метод, основанный на расчете внутренней ставки доходности (IRR).

Между чистой текущей стоимостью (NPV) и ставкой дисконтирования (i) существует обратная зависимость. Эта зависимость следует из таблицы 21 и графика,

Таблица 25. Зависимость NPV от ставки дисконтирования

№ п/п	Наименование показателя	0	1	2	3	4	NPV
1	Чистые денежные потоки	-268420	211660	211660	211660	211660	

2	коэффициент дисконтирования						
	i=0,1	1	0,909	0,826	0,751	0,683	
	i=0,2	1	0,833	0,694	0,578	0,482	
	i=0,4	1	0,714	0,51	0,364	0,26	
	i=0,5	1	0,667	0,444	0,295	0,198	
	i=0,6	1	0,625	0,390	0,244	0,095	
	i=0,7	1	0,588	0,335	0,203	0,070	
3	Дисконтированный денежный поток						
	i=0,1	-268420	192398,9	174831,2	158956,7	144563, 8	402330
	i=0,2	-268420	176312,8	146892	122339,5	102020, 1	279144,4
	i=0,4	-268420	151125,2	107946,6	77044,24	55031,6	122727,6
	i=0,5	-268420	141177,2	93977,04	62439,7	41908,6 8	71082,6
	i=0,6	-268420	132287,5	82547,4	51645,04	20107,7	18167,6
	i=0,7	-268420	124456,1	70906,1	42966,98	14816,2	-15274,6

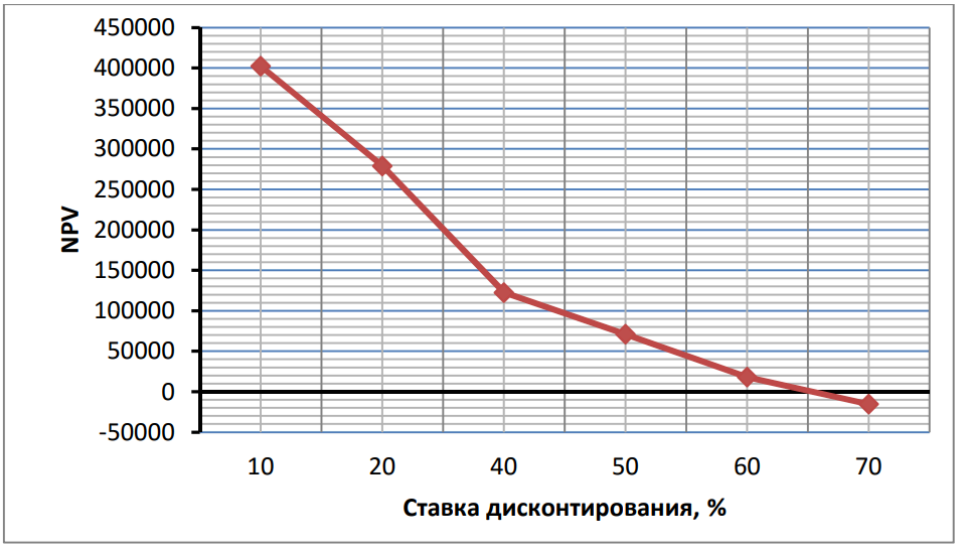

Рисунок 14. Зависимость NPV от ставки дисконтирования

Из таблицы и графика следует, что по мере роста ставки дисконтирования чистая текущая стоимость уменьшается, становясь отрицательной. Значение ставки, при которой NPV обращается в нуль, носит название «внутренней ставки доходности» или «внутренней нормы прибыли». Из графика получаем, что IRR составляет 0,65.

5.5.5 Индекс доходности (рентабельности) инвестиций (PI)

Индекс доходности показывает, сколько приходится дисконтированных денежных поступлений на рубль инвестиций.

Расчет этого показателя осуществляется по формуле

$$PI = \sum_{t=1}^{n} \frac{\text{ЧПД}_t}{(1+i)^t} / I_0,$$

где I0 – первоначальные инвестиции.

$$PI = \frac{742160 + 674390 + 613160 + 557640}{269220} = 9{,}6$$

PI=9.6>1, следовательно проект эффективен при i=0,1; NPV=268415.

Вывод раздела «Финансовый менеджмент, ресурсоэффективность и ресурсосбережение.

С каждым годом требования к информационной безопасности в отрасли нефтедобычи все больше повышаются. Постоянное развитие и совершенствованин технологий неизбежно влечет за собой увеличение количества киберпреступлений. Угрозы информационной безопасности нефтегазовой отрасли могут повлечь за собой потери, исчисляемые в огромных суммах. При этом важно понимать, что кибератаки могут спровоцировать аварии во время процесса добычи нефти и газа, что может привести к угрозе жизни и здоровья рабочих, а также значительному ущербу экологии. Все это способствует поиску решений, помогающих выбору максимально эффективных средств защиты и управления информационной безопасности. В идеальном варианте необходимо заранее предотвращать все угрозы информационной безопасности предприятия. Однако на практике информационная безопасность нефтегазовой отрасли развита не столь хорошо, как хотелось бы – у многих предприятий отсутствует четкая система управления рисками информационной безопасности, нет программы реагирования на киберинциденты и довольно малое число предприятий занимаются оценкой возможных угроз информационной безопасности.

Именно для этой цели создается программный продукт, позволяющий разработать стратегию управления рисками информационной безопасности нефтегазовых предприятий. Данный продукт учитывает специфику отрасли и помогает пользователю разработать план дальнейшего развития ИБ, подобрать необходимое для этого программное обеспечение и аппаратные комплексы, не заходя за рамки бюджета предприятия.

На данный момент аналогов данному программному обеспечению нет. Функционал разработанного продукта на данный момент предоставляется в виде услуг некоторых компаний, в которых эксперты анализируют

предприятие и разрабатывают план рекомендаций. Однако данные услуги стоят дороже разработки ПО, плюс ко всему, присутствует момент субъективности принятых решений, а также ограниченного числа знаний экспертов. Тогда как база знаний постоянно будет пополняться актуальными средствами управления информационной безопасностью и защиты данных.

Таким образом, данное ПО будет высоко востребовано на отечественном рынке нефтегазовой отрасли, затраты на его полную реализацию будут покрыты.

6. Социальная ответственность

Введение

Выпускная квалификационная работа по разработке системы управления рисками информационной безопасности нефтегазодобывающих предприятий выполнялась на кафедре Оптимизации систем управления в одном из кабинетов Кибернетического центра Томского Политехнического Университета. Рабочее место представляет собой компьютерный класс. В данном разделе изложены вопросы охраны труда и техники безопасности, связанные с работой в помещении, содержащем компьютерную технику.

6.1 Правовые и организационные вопросы обеспечения безопасности

Охрана труда и техника безопасности это – система сохранения жизни и здоровья работников в процессе трудовой деятельности, включающая в себя правовые, социально-экономические, организационно-технические, санитарно-гигиенические, лечебно-профилактические, реабилитационные и иные мероприятия (статья № 1 Федерального закона «Об основах охраны труда в Российской Федерации», 17.07.1999 г. №181-ФЗ [13]), образующие механизм реализации конституционного права граждан на труд (ст. 37 Конституции РФ [14]) в условиях, отвечающих требованиям безопасности и гигиены.

Статья 37 Конституции Российской Федерации гарантирует свободу труда, а также право на труд, в условиях, отвечающих требованиям безопасности и гигиены.

В статье 212 Трудового Кодекса РФ [15] предусмотрено, что на работодателя возлагаются обязанности по обеспечению безопасных условий и охраны труда.

Для работодателя существует два варианта поведения, касающихся выполнения своих обязательств по охране труда на рабочих местах с персональным компьютером.

1. обеспечить такие условия труда, при которых на работников исключено (или не превышает установленных нормативов) воздействие

вредных факторов, а также подтвердить это с помощью сертификации рабочих мест;

2. в случае наличия вредных факторов снабдить работников средствами индивидуальной защиты и произвести материальную компенсацию воздействия вредных факторов, выявленных в результате сертификации рабочего места.

Описанные выше требования СанПиН распространяются на персональные компьютеры, периферийные устройства (клавиатуры, принтеры, модемы, блоки бесперебойного питания и т.д.), а также на видеодисплейные терминалы всех типов.

Федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере труда, является Федеральная служба по труду и занятости Министерства здравоохранения и социального развития Правительства Российской Федерации.

Основными задачами трудового законодательства являются создание необходимых правовых условий для достижения оптимального согласования интересов сторон трудовых отношений, интересов государства, а также правовое регулирование трудовых отношений и иных непосредственно связанных с ними отношений.

Помимо обеспечения безопасных условий труда гражданина, законодательство налагает ответственность на каждого за состояние окружающей природной среды. Так Конституция Российской Федерации статьей 58 обязывает каждого «сохранять природу и окружающую среду, бережно относиться к природным богатствам».

6.1.1. Эргономика рабочего места

Для выполнения данной работы было необходимо: помещение, компьютерный стол, кресла, компьютеры, выход в интернет. В процессе работы принимали участие студент и руководитель проекта.

Требования к организации рабочих мест пользователя:

1. конструкция рабочей мебели (подставка для ног, кресло, рабочий стол) должна обеспечивать возможность индивидуальной регулировки соответственно росту пользователя и создавать удобную позу для работы. Вокруг ПК должно быть обеспечено свободное пространство не менее 60-120см;

2. рабочее место должно быть организовано с учетом эргономических требований согласно ГОСТ 12.2.032-78 [1] «ССБТ. Рабочее место при выполнении работ сидя. Общие эргономические требования» и ГОСТ 12.2.061-81 [2] «ССБТ. Оборудование производственное. Общие требования безопасности к рабочим местам»;

3. на уровне экрана должен быть установлен оригинал-держатель;

Рациональная организация труда в течение смены, в соответствии с государственными стандартами и правовыми нормами обеспечения безопасности, предусматривает:

1. длительность рабочей смены не более 8 часов;
2. обеденный перерыв не менее 40 минут;
3. установление двух регламентируемых перерывов (не менее 20 минут после 1-2 часов работы, не менее 30 минут после 2 часов работы).

При приеме на работу обязателен предварительный медицинский осмотр, а также периодические медицинские осмотры в течение нескольких лет.

Перед приемом на работу каждому сотруднику необходимо пройти инструктаж по технике безопасности, и после необходимо пройти инструктаж по охране труда и электробезопасности.

6.1.2 Организационные мероприятия обеспечения безопасности

В соответствии с государственными стандартами и правовыми нормами обеспечения безопасности предусмотрена рациональная организация труда в течение смены, которая предусматривает:

- длительность рабочей смены не более 8 часов;

– установление двух регламентируемых перерывов (не менее 20 минут после 1-2 часов работы, не менее 30 минут после 2 часов работы);
– обеденный перерыв не менее 40 минут.

Обязательно предусмотрен предварительный медосмотр при приеме на работу и периодические медосмотры.

Каждый сотрудник обязан пройти инструктаж по технике безопасности перед приемом на работу и в дальнейшем, должен быть пройден инструктаж по электробезопасности и охране труда. Предприятие обеспечивает рабочий персонал всеми необходимыми средствами индивидуальной защиты.

Оплата труда, социальные пособия, дополнительные выплаты устанавливаются в соответствии со степенью вредности и опасности выполняемых обязанностей.

Согласно требованиям СанПиН 2.2.2/2.4.1340–03 [10], расстояние между рабочими столами с видеомониторами, равно 2 м, а расстояние между боковыми поверхностями видеомониторов примерно 1,2 м. Площадь на одно рабочее место пользователей персонального компьютера с монитором на базе плоских дискретных экранов (жидкокристаллические, плазменные) - 4,5 м^2.

6.2. Производственная безопасность

Во время разработки системы управления рисками информационной безопасности нефтегазодобывающих предприятий возможно наличие следующих вредных и опасных факторов (таблица 26).

Таблица 26. Опасные и вредные факторы при разработке системы управления рисками информационной безопасности нефтегазодобывающих предприятий.

Факторы (ГОСТ 12.0.003-2015)	Этапы работ			Нормативные документы
	Разработка	Изготовление	Эксплуатация	
1. Недостаточная освещенность рабочей зоны	+	+	+	1. СанПиН 2.2.2/2.4.1340-03 2. СНиП 23-05-95

и отсутствие или недостаток естественного света				3. СанПиН 2.2.1/2.1.1.1278–03
2. Отклонение показателей микроклимата	+	+	+	1. СанПиН 2.2.4.548
3. Превышение уровня шума	+	+	+	1. СанПиН 2.2.2/2.4.1340-03 2. ГОСТ 12.1.003-2014 ССБТ
4. Повышенный уровень электромагнитных излучений	+	-	+	1. СанПиН 2.2.2/2.4.1340-03 2. СанПиН 2.2.2.542-96
5.Повышенное значение напряжения в электрической цепи, замыкание которой может произойти через тело человека	+	+	+	1. ГОСТ 12.1.019-2017

6.2.1. Недостаточная освещенность рабочей зоны и отсутствие или недостаток естественного света

Освещение в недостаточной степени может привести к напряжению зрения, ослаблению внимания и наступлению преждевременной утомленности. Ослепление, резь в глазах и раздражение могут быть вызваны чрезмерно ярким освещением. Неверное направление света на месте труда может создать резкие тени или блики, а также дезориентировать работающего. Перечисленные причины могут привести к профзаболеваниям.

В аудитории № 204 кибернетического центра, где осуществлялось выполнение работы, применяется искусственное освещение, в качестве

источников которого используются люминесцентные лампы типа ЛД-20. Коэффициент пульсации ($К_п$ – колебания светового потока, падающего на единицу поверхности во времени) в аудитории составляет около 40%. Согласно требованиям, СанПиН 2.2.2/2.4.1340-03 [10], в помещениях, оборудованных компьютерами не коэффициент пульсации, должен быть не более 5%.

Поэтому в рамках данной работы проводится расчет искусственного освещения для светодиодных светильников взамен установленным люминесцентным.

Площадь помещения составляет 56м^2 (при длине 8 м и ширине 7 м). Светильников в аудитории размещены в четыре ряда, по шесть в каждом ряду. Каждый светильник позволяет установить четыре светодиодных лампы типа ССОН СД В-О-01-110-30-001-IP20-УХЛ4 (мощность 30 Вт, световой поток 2000 лм). Общее количество ламп в помещении составит 75.

Светильники размещены таким образом, чтобы равномерно освещать помещение и рабочие места (рисунок 15).

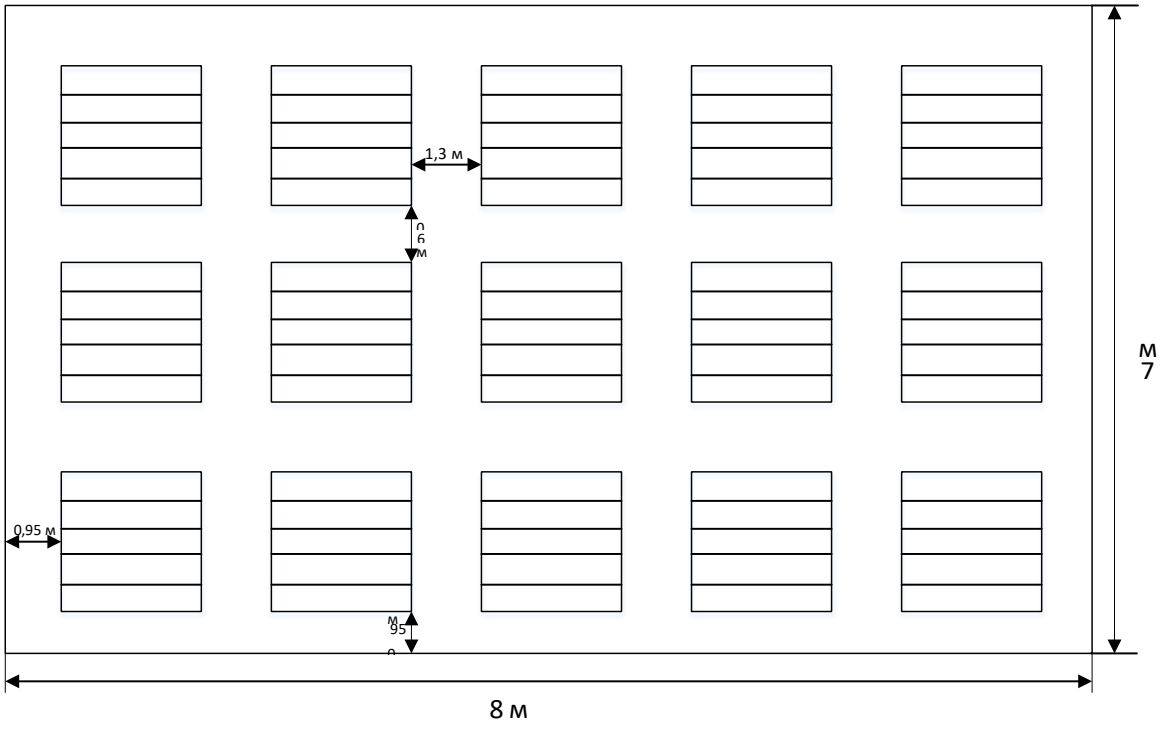

Рисунок 15. Схема размещения светодиодных светильников

Согласно справочной информации, коэффициент естественного освещения (КЕО) должен быть не ниже 3% при выполнении работы с высокой зрительной точностью при наименьшем размере объекта различения 0,3 – 0,5 мм, и не менее 2,4% при выполнении зрительной работы средней точности (наименьший размер объекта различения 0,5…1,0 мм).

Установлено, что для помещений, в которых установлены компьютеры, требуется освещенность не менее 300 лк при выполнении зрительной работы высокой точности и не менее 200 лк, при выполнении работы средней точности.

Для проведения расчетов выбран метод коэффициента использования светового потока.

Требуемая освещенность рассчитывается по следующей формуле:

$$E = \frac{F \cdot N \cdot \eta}{S \cdot z \cdot k} \quad (1)$$

Где:

$E_н$– нормированная минимальная освещенность, лк;

F = 2000 лм – световой поток для ССОН СД В-О-01-110-30-001-IP20-УХЛ4;

S – площадь помещения, $м^2$;

z – коэффициент неравномерности освещения (для светодиодных светильников z = 1);

$k_з$ – коэффициент запаса, зависящий от вида технологического процесса и типа применяемых источников света (k = 1,5 по СНиП 23-05-95 [12], так как используемое помещение относится к помещениям с малым выделением пыли); N – количество ламп в помещении; η – коэффициент использования светового потока.

По СНиП 23-05-95[12] определяются разряды зрительных работ. Работа за ПЭВМ относится к зрительным работам высокой точности для любого типа помещений (III разряд).

Коэффициент использования светового потока выбираем в зависимости от типа светильников, размеров помещения, определяемых индексом помещения, коэффициентов отражения стен и потолка помещения. Коэффициент отражения побеленного потолка $\rho_п$ = 70%; коэффициент отражения от стен, окрашенных в светлую окраску (белый цвет)$\rho_{ст}$ = 50 %;

Расчет индекса помещения произведем по формуле

$$i = \frac{l \cdot d}{h \cdot (l + d)}, \quad (2)$$

Где:

h – высота подвеса светильников, м (h = 4 м);

l – длина помещения, м (l=8м);

d – ширина помещения, м (d =7м).

Тогда индекс помещения равен i = 1. Согласно табличным данным, находим коэффициент использования светового потока при коэффициентах отражения потолка $\alpha_п$=0,7 и стен $\alpha_с$ =0,5, η = 0,3, который показывает какая часть светового потока ламп попадает на рабочую поверхность.

Проведем расчет освещенности: теперь определяем нормированную освещенность:

$E_н$ = (2000*75*0,3) / (56*1,5*1) = 535 лк.

В результате нормированная минимальная освещенность составила 535 лк, что удовлетворяет санитарным нормам для помещения, где выполнялась ВКР.

Чтобы поддерживать освещение в помещении по всем соответствующим нормам, необходимо хотя бы два раза в год стекла и светильники, а также по мере необходимости заменять перегоревшие лампы. В утреннее и вечернее время вводится общее искусственное освещение.

6.2.2. Отклонение показателей микроклимата

Компьютеры могут привести к повышению температуры и снижению относительной влажности в помещении. В таких помещениях должны соблюдаться определенные параметры микроклимата. В санитарных нормах

- СанПиН 2.2.4.548 [5] установлены величины параметров микроклимата, создающие комфортные условия. Отклонения параметров микроклимата от установленных норм способствуют в первую очередь нарушению физиологической функции человека сохранять тепловой баланс организма, что может повлиять на состояние здоровья и общую производительность труда. В обычных климатических условиях теплоотдача осуществляется в основном за счет излучения (примерно 45 % всей удаляемой организмом теплоты), конвекции (30 %) и испарения (25 %).

Аудитория №204 кибернетического центра оснащена компьютерами в количестве 10 штук, которые являются источниками тепла и могут вызвать существенное повышение температуры и уменьшение относительной влажности в помещении.

Нормы на параметры микроклимата в помещении зависят от времени года, характера трудового процесса и характера помещения.

Работа оператора ЭВМ относится к категории работ Iа, в которую входят работы с интенсивностью энергозатрат до 139Вт, производимые сидя и сопровождающиеся незначительным физическим напряжением. Оптимальные параметры микроклимата для этой категории работ представлены в таблице 27.

Таблица 27. Параметры микроклимата для помещений, где установлены компьютеры

Период	Параметр микроклимата	Величина
Холодный	Температура воздуха в помещении, °С	22…24
	Температура поверхностей, °С	21-25
	Относительная влажность, %	44…60
	Скорость движения воздуха, м/с	До 0,1
Теплый	Температура воздуха в помещении, °С	23…25
	Температура поверхностей, °С	22-26
	Относительная влажность, %	40…60
	Скорость движения воздуха, м/с	0,1…0,2

Обеспечить комфортные условия труда можно как за счет организационных методов (рациональная организация проведения работ в зависимости от времени года и суток, чередование труда и отдыха), так и за счет внедрения технических средств (вентиляция, кондиционирование воздуха, отопительная система). Поэтому в работе проведен расчет потребного воздухообмена в аудитории.

Расчет потребного воздухообмена (L $м^3$ /ч), определяется по формуле:

$$L = \frac{G \cdot 1000}{x_в - x_н}, \quad (3)$$

где:

L, $м^3$/ч – потребный воздухообмен;

G, г/ч – количество вредных веществ, выделяющихся в воздух;

$x_в$, мг/м3 – предельно допустимая концентрация вредности в воздухе рабочей зоны помещения;

$x_н$, мг/$м^3$ – максимально возможная концентрация той же вредности в воздухе населенных мест.

По справочным данным, определяем количество углекислого газа, выделяемое одним человеком. Если в помещении работают 10 человек, g = 23 л/ч, допустимую концентрацию CO_2, $X_в$ = 1 л/$м^3$. Содержание CO_2 в наружном воздухе для больших городов принимаем: $X_н$ = 0,5 л/м3, то потребный воздухообмен составит:

$$L = 23*4 / (1 – 0.5) = 184 м^3/ч.$$

Следовательно, потребный воздухообмен для 204 кибернетического центра общей площадью рабочего помещения 56 $м^2$ и объемом 224 $м^3$, где на каждого работающего приходится в среднем 5,6 $м^2$ общей площади и 22,4 $м^3$ объема, составляет 184 $м^3$/ч. Соответствует принятым нормам.

6.2.3. Превышение уровня шума

Согласно СанПиН 2.2.2/2.4.1340-03[10] в производственных помещениях с использованием ПЭВМ уровни шума на рабочих местах не должны превышать предельно допустимых значений.

Работающие в условиях длительного шумового воздействия испытывают раздражительность, головные боли, головокружение, снижение памяти, повышенную утомляемость, понижение аппетита, боли в ушах и т. д. Все это снижает работоспособность человека и его производительность, качество и безопасность труда.

В аудитории №204 кибернетического центра источниками шума служат винчестеры в системном блоке, вентиляторы, кулеры охлаждения процессора ПК, мониторы, клавиатуры. Согласно установленным нормам, уровень шума на рабочем месте операторов ЭВМ не должен превышать 80 дБ. В таблице 28 приведены уровни шума из различных источников.

Таблица 28. Уровень звукового давления различных источников

Источник шума	Уровень шума, дБ
Жесткий диск	40
Вентилятор	45
Монитор	17
Клавиатура	10
Принтер	45
Сканер	42

Уровень шума, возникающий от нескольких некогерентных источников, работающих одновременно подсчитывается на основании принципа энергетического суммирования излучений отдельных источников.

$$L_{\Sigma}=10\lg\sum_{i=1}^{i=n}10^{0.1L_i} \qquad (4)$$

где Li – уровень звукового давления i – го источника шума

n = количество источников шума.

Подставив в формулу значения уровня звукового давления для каждого оборудования, получим:

$$L_{\Sigma}=10*\log(10^{4}+10^{4.5}+10^{1.7}+10^{1})=\ 46{,}2\ \text{дБ}$$

Полученное значение не превышает допустимую норму, поэтому использование специальных средств защиты не требуется. В случае превышения допустимой нормы для снижения уровня шума стены и потолок помещений, где установлены компьютеры, могут быть оснащены звукопоглощающими материалами.

Для снижения шумового загрязнения в изучаемом помещении могут быть приняты следующие меры:

1. Вентиляторы процессора. Замена кулера процессора на другой – с более тихим вращением лопастей и большей поверхностью теплоотвода, что сделает кулер практически неслышным.

2. Изолирующая оболочка. Заключить жесткий диск в изолирующую оболочку, что снизит уровень издаваемого звука.

3. Прокладки и изолирующие монтажные шайбы. Могут значительно уменьшить создаваемую ПЭВМ вибрацию

4. Звукопоглощающий корпус. При самостоятельной сборке, возможно, имеет смысл приобрести корпус с тихими вентиляторами охлаждения как самого корпуса, так и блока питания, а также с расширенными вентиляционными отверстиями.

5. Звукоизолирующая прокладка для корпуса. Установка внутрь корпуса прокладки из звукопоглощающей пены, заглушает большую часть звуков, создаваемых компонентами ПК.

6. Блок питания. Нередко самым шумным компонентом ПК является блок питания. В таких случаях его замена на более тихий значительно снизит общий уровень шума.

7. Охлаждение корпуса. Используя вентиляторы для охлаждения корпуса для уменьшения уровня звука следует выбирать имеющие специальную конструкцию и термостатический контроль. Либо заменить на водяное охлаждение с минимальным уровнем шума.

6.2.4. Повышенный уровень электромагнитных излучений

В соответствии с СанПиНом 2.2.2/2.4.1340-03 [10] помещения, где размещаются рабочие места с ПЭВМ, должны быть оборудованы защитным заземлением (занулением) в соответствии с техническими требованиями по эксплуатации электроустановок и вычислительной техники. Рабочие места с ПЭВМ не следует размещать вблизи силовых кабелей и вводов, высоковольтных трансформаторов, технологического оборудования, создающего помехи в работе ПЭВМ.

Максимальный уровень рентгеновского излучения на рабочем месте оператора компьютера обычно не превышает 10 мкбэр/ч, а интенсивность ультрафиолетового и инфракрасного излучений от экрана монитора лежит в пределах 10…100 мВт/м^2.

Для снижения воздействия этих видов излучения рекомендуется применять мониторы с пониженным уровнем излучения (MPR-II, TCO-92, TCO-99), устанавливать защитные экраны, а также соблюдать регламентированные режимы труда и отдыха. В таблице 29 представлены Допустимые значения параметров неионизирующих электромагнитных излучений в соответствии с СанПиНом 2.2.2.542-96.

Таблица 29. Допустимые значения параметров неионизирующих электромагнитных излучений.

Наименование параметра	Допустимые значения
Напряженность электрической составляющей электромагнитного поля на расстоянии 50см от поверхности видеомонитора	10 В/м
Напряженность магнитной составляющей электромагнитного поля на расстоянии 50см от поверхности видеомонитора	0,3А/м
Напряженность электростатического поля не должна превышать: для взрослых пользователей	20 кВ/м

Выполнение выпускной квалификационной работы проводилось на современном компьютере, монитор которого удовлетворяет нормативным требованиям по напряженности электромагнитного поля и другим показателям.

6.2.5. Повышенное значение напряжения в электрической цепи, замыкание которой может произойти через тело человека

Электробезопасность согласно ГОСТ 12.1.019-2017 [8] является системой организационных и технических мероприятий и средств, обеспечивающих защиту людей и животных от вредного и опасного воздействия электрического тока, электрической дуги, электромагнитного поля и статического электричества.

Электропитание аудитории № 204 кибернетического центра ТПУ осуществляется от силового распределительного щита однофазного переменного тока с действующим значением напряжения 220В. Таким образом, в соответствии с правилами устройства электроустановок все электроприборы, используемые в аудитории, относятся к низковольтным с напряжением питания до 1000 В. В помещении большая часть электрической проводки является скрытой. Поражение электрическим током возможно только контакте человека с неизолированным проводником.

Следует отметить, что кабель имеет двойную изоляцию, что существенно снижает риск поражения. Однако не следует исключать также опасность поражения и от токоведущих частей компьютера в случае их пробоя и нарушении изоляции.

Для обеспечения электробезопасности в аудитории должны быть проведены следующие мероприятия:

1. для защиты от токов короткого замыкание необходимо предусмотреть наличие быстродействующих устройств защиты; электрическая сеть должна иметь защиту от токов короткого замыкания, обеспечивающую по возможности наименьшее время отключения и

требования селективности; в качестве аппаратов защиты должны применяться автоматические выключатели или предохранители;

2. для защиты от напряжения прикосновения все токоведущие части должны быть изолированы; запрещается использовать кабели и провода с поврежденной или потерявшей защитные свойства изоляцией; неизолированные токоведущие части должны быть оборудованы защитными ограждениями или расположены в недоступном для прикосновения месте; запрещается пользоваться поврежденными розетками, распределительными коробками, рубильниками и другими электроустановочными приборами; устройство и эксплуатация временных электросетей не допускается;

3. для защиты от поражения электрическим током путем возникновения потенциала на проводящих корпусах электроприборов необходимо наличие защитного заземления; зануление, согласно ПУЭ сопротивление заземляющего устройства в любое время года должно быть не более 4 Ом, при этом сечение заземляющей жилы должно быть не менее 4 мм^2 для медных проводников, не менее 6 мм^2 – для алюминиевых и не менее 20 мм^2 – для стальных.

Для предотвращения электротравматизма большое значение имеет правильная организация обслуживания аудитории, проведение ремонтных, монтажных и профилактических работ.

Ремонт, разборку и сборку, наладку электротехнологического оборудования может выполнять только подготовленный персонал, имеющий необходимую для данных работ группу допуска по электробезопасности.

6.3. Экологическая безопасность

В настоящее время проблема экологической безопасности является приоритетной. Это стало поводом для принятия жестких законов, ограничивающих обычную утилизацию компьютерной техники. В большей мере это обусловливается тем, что в производстве такой техники используется множество различных материалов, которые способны нанести непоправимый вред окружающей среде и, соответственно, здоровью человека. Утилизация

компьютерного оборудования является достаточно сложной. Непосредственная переработка большей части компонентов включает в себя их сортировку, последующую гомогенизацию и отправку для повторного использования, т.е. с предварительным помолом или переплавкой. В соответствии с СанПиНом 2.1.7.1322-03 [11] персональные компьютеры в случае выхода из строя списываются, затем отправляются на специальный склад, где соответствующий персонал при необходимости принимает меры по утилизации аппаратного обеспечения и периферии, которое было списано.

Согласно ГОСТ Р 51768-2001 [4] утилизация люминесцентных ламп предполагает то, что эти использованные лампы передаются предприятиям по их переработке, где с помощью специализированного оборудования вредные лампы перерабатываются в безвредное сырье – сорбент. Люминесцентные лампы представляют собой «чрезвычайно опасные» виды отходов. Все люминесцентные лампы содержат от 3 до 5 мг ртути. Лампы должны утилизироваться коммунальными службами, занимающимися вывозом специальных отходов. Транспортировка ламп на полигоны складирования должна выполняться организациями, которые специализируются на утилизации опасных отходов.

6.4. Безопасность в чрезвычайных ситуациях

Наиболее вероятная чрезвычайная ситуация, которая может возникнуть при работе с ПЭВМ – пожар, так как в современных ЭВМ очень высокая плотность размещения элементов электронных схем. В непосредственной близости друг от друга располагаются соединительные провода и кабели, при протекании по ним электрического тока выделяется значительное количество теплоты, при этом возможно оплавление изоляции и возникновение возгорания.

Регулирование пожаробезопасности производится СНиП 21-01-97 [7].

Возможные виды источников воспламенения:

- искра при разряде статического электричества;
- искры от электрооборудования;
- искры от удара и трения;
- открытое пламя.

Согласно ГОСТ 12.1.004-91 [9] «Система стандартов безопасности труда (ССБТ). Пожарная безопасность. Общие требования», пожарная безопасность должна обеспечиваться системами предотвращения пожара и противопожарной защиты, в том числе организационно-техническими мероприятиями.

Рабочее помещение, в котором производится выполнение магистерской диссертации, относится к категории В по пожарной и взрывной опасности.

Следующие мероприятия относятся к противопожарным мероприятиям в помещении:

1) Оборудование помещения средствами пожаротушения (ящики с песком, огнетушители, стенд с противопожарным инвентарем), средствами связи. В помещении должна быть исправная электрическая проводка электрооборудования и осветительных приборов.

2) Инструктаж, чтобы каждый работник знал место нахождения средств пожаротушения и связи, умел пользоваться средствами пожаротушения, а также помнил номера телефонов для сообщения об экстренном случае.

Помещение обеспечено средствами пожаротушения:

- углекислотный огнетушитель ОУ-5 – 1 шт.;
- пенный огнетушитель ОП-10 – 1 шт.

Помещение и этаж оборудованы следующими средствами оповещения:

- пассивными датчиками задымленности;
- звуковой индикацией в виде громкоговорителя;
- световой индикацией в коридорах этажа.

Во избежание возникновения пожара необходимо проводить следующие профилактические работы, которые направлены на устранение возможных источников возникновения пожара:

- отключение оборудования при покидании рабочего места;
- проведение инструктажа работников о пожаробезопасности;
- периодическая проверка проводки.

Выводы раздела «Социальная ответственность»

В данном разделе ВКР были рассмотрены вредные и опасные факторов на рабочем месте оператора ЭВМ в аудитории № 204 кибернетического центра Томского политехнического университета. Рассмотрены требования по технике безопасности, электробезопасности, пожаробезопасности, проведены расчеты требуемой освещенности и воздухообмена рассматриваемого помещения.

Также были выявлены возможные чрезвычайные ситуации и приведен план действий для наиболее вероятной ЧС в данном помещении – возникновение пожара.

В рамках настоящего раздела также изучены правовые основы безопасности труда.

Заключение

При проведении операций по переработке или очистке нефти и природного газа обнаружить факты незаконного присвоения или изменения служебной коммерческой информации об эксплутационных характеристиках скважин, текущих темпах добычи или использованию активов может оказаться сложной задачей. Поэтому очень важно внедрять средства защиты уже на этапе разработки систем по управлению такими данными. Даже если средства осуществления контроля не сработают и кибератака не будет обнаружена, способность системы обеспечить эффективное реагирование может помочь минимизировать производственные потери, а также финансовый, экологический и репутационный ущерб.

На этапах реагирования и восстановления необходимо будет не только принять немедленные меры по коррекции работы пострадавшего оборудования и систем, но и провести тщательный анализ с целью понимания того, где и как произошла атака, какие недостатки системы создали возможность для ее возникновения и что требуется сделать, чтобы смягчить ее последствия и предотвратить риски в дальнейшем. Важно отметить, что просто разработать планы и регламенты будет недостаточно. По аналогии с учебной пожарной тревогой, необходимо периодически проверять эффективность применения таких планов и регламентов путем моделирования и проигрывания чрезвычайных ситуаций, требующих совместной работы бизнес- и технических специалистов.

По результатам исследований были написаны следующие статьи:

1. Прохоренко А.С. Наиболее вероятные риски информационной безопасности в 2019 году / А.С. Прохоренко ; науч. рук. В.Г. Ротарь // Синтез науки и общества в решении глобальных проблем современности : сборник статей Международной научно-практической конференции, 11 марта 2019 г., г. Казань : Изд-во МЦИИ OMEGA SCIENCE, 2019. – [с. 32-35].
2. Прохоренко А.С. Угрозы информационной безопасности нефтегазовых компаний / А.С. Прохоренко ; науч. рук. В.Г. Ротарь // Синтез науки и

общества в решении глобальных проблем современности : сборник статей Международной научно-практической конференции, 11 марта 2019 г., г. Казань : Изд-во МЦИИ OMEGA SCIENCE, 2019. – [с. 35-39].

Список использованных источников

1. Ellen Zhang. Cybersecurity Risks 2019: Top Online Security Risks for Healthcare, SMBs & More [Электронный ресурс]. – Режим доступа: https://digitalguardian.com/blog/cybersecurity-risks-2019, свободный. – (дата обращения 27.02.2019).
2. Иванов О. Самые значимые атаки программ-вымогателей в 2017-2018 годах [Электронный ресурс]. – Режим доступа: https://www.anti-malware.ru/analytics/Threats_Analysis/ransomware-strikes-in-2017-and-2018, свободный. – (дата обращения 27.02.2019).
3. Nate Lord. Social Engineering Attacks: Common Techniques & How to Prevent an Attack [Электронный ресурс]. – Режим доступа: https://digitalguardian.com/blog/social-engineering-attacks-common-techniques-how-prevent-attack, свободный. – (дата обращения 27.02.2019).
4. Imation corp. Remote working puts business data at risk, with over a third of office workers having lost devices in a public place [Электронный ресурс]. – Режим доступа: http://www.ironkey.com/en-US/about-ironkey/press-releases/Imation-Survey-2014-11-05.pdf, свободный. – (дата обращения 27.02.2019).
5. Deepak Dutt. 2018: the year of the AI-powered cyberattack [Электронный ресурс]. – Режим доступа: https://www.csoonline.com/article/3246196/2018-the-year-of-the-ai-powered-cyberattack.html, свободный. – (дата обращения 27.02.2019).
6. Alastair Stevenson. Anonymous OpPetrol hacking campaign targets oil and gas sectors [Электронный ресурс]. – Режим доступа: https://www.v3.co.uk/v3-uk/news/2276288/oil-and-gas-sector-warned-of-anonymous-oppetrol-hacking-campaign, свободный. – (дата обращения 06.03.2019).
7. FireEye. Cyber threats to the Nordic region [Электронный ресурс]. – Режим доступа: https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-nordic-threat-landscape.pdf, свободный. – (дата обращения 06.03.2019).
8. US Department of Homeland Security. NCCIC/ICS-CER – 2015 year in review. [Электронный ресурс]. – Режим доступа: https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2015_Final_S508C.pdf.pdf, свободный. – (дата обращения 06.03.2019).
9. Jim Finkle. Shamoon virus returns in new Saudi attacks after 4-year hiatus. [Электронный ресурс]. – Режим доступа: www.reuters.com/article/cyber-saudi-shamoon-idUSL1N1DW05H, свободный. – (дата обращения 06.03.2019).

10. McAfee. Global energy cyberattacks: Night Dragon. [Электронный ресурс]. – Режим доступа: www.mcafee.com/hk/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf, свободный. – (дата обращения 06.03.2019).

11. Tim Heidar. Digital trenches: On the front lines of the cyber war. [Электронный ресурс]. – Режим доступа: www.fox-it.com/en/about-fox-it/corporate/news/65-oil-gas-companies-unprepared-major-cyberattack/, свободный. – (дата обращения 06.03.2019).

12. Яковис Л. М. От единого информационного пространства к единому пространству управления производством // Автоматизация в промышленности, 2013. с. 20-26. Режим доступа: https://elibrary.ru/item.asp?id=18419873. Дата обращения: 01.03.2019;

13. Ефремов А. А. Единые цифровые пространства: в поиске баланса между интеграцией и суверенностью // Информационное право №3, 2016. с. 36- 39. Режим доступа: https://elibrary.ru/item.asp?id=27036305. Дата обращения: 01.03.2018;

14. Бова В. В. Концептуальная модель представления знаний при построении интеллектуальных информационных систем // Известия ЮФУ. Технические науки №7, 2014. с. 109-117. Режим доступа: https://elibrary.ru/item.asp?id=21782588. Дата обращения: 01.03.2018;

15. Common Information Model. Официальный сайт Distributed management task force. Режим доступа: http://www.dmtf.org/standards/cim. Дата обращения: 01.03.2018;

16. Zhang Hong, Liu Dong, Lu Yiming Ontology-based automatic mapping technology for heterogeneous common information model // China International Conference on Electricity Distribution (CICED) 10-13 Aug. p. 1-5. Режим доступа: http://ieeexplore.ieee.org/document/7576371/. Дата обращения: 01.03.2018;

17. Gelli Ravikumar, Shrikrishna A. Khaparde. A Common Information Model Oriented Graph Database Framework for Power Systems // IEEE Transactions on Power Systems Volume: 32, Issue: 4, July 2017. p. 2560 - 2569. Режим доступа: http://ieeexplore.ieee.org/document/7752988/. Дата обращения: 01.03.2018;

18. Jens Pottebaum, Christina Schäfer, Maike Kuhnert Common information space for collaborative emergency management // IEEE Symposium on Technologies for Homeland Security (HST) 10-11 May 2016. p. 1-6. Режим доступа: http://ieeexplore.ieee.org/document/7568904/. Дата обращения: 01.03.2018;

19. Hang Qin, Zhu Han. Stochastic Resource Allocation for Well Control With Digital Oil Field Infrastructure // IEEE Systems Journal, October 2016 (Volume: PP, Issue: 99). p. 1-12. Режим доступа: http://ieeexplore.ieee.org/document/7605471/. Дата обращения: 01.03.2018;

20. Прохоренко А.С. Наиболее вероятные риски информационной безопасности в 2019 году / А.С. Прохоренко ; науч. рук. В.Г. Ротарь // Синтез науки и общества в решении

глобальных проблем современности : сборник статей Международной научно-практической конференции, 11 марта 2019 г., г. Казань : Изд-во МЦИИ OMEGA SCIENCE, 2019. – [с. 32-35].

21. Прохоренко А.С. Угрозы информационной безопасности нефтегазовых компаний / А.С. Прохоренко ; науч. рук. В.Г. Ротарь // Синтез науки и общества в решении глобальных проблем современности : сборник статей Международной научно-практической конференции, 11 марта 2019 г., г. Казань : Изд-во МЦИИ OMEGA SCIENCE, 2019. – [с. 35-39].

22. ГОСТ 12.2.032-78. СБТ. Рабочее место при выполнении работ сидя. Общие эргономические требования

23. ГОСТ 12.2.061-81 ССБТ. Оборудование производственное. Общие требования безопасности к рабочим местам

24. ГОСТ 12.1.003-2014 ССБТ. Шум. Общие требования безопасности

25. ГОСТ Р 51768-2001. Ресурсосбережение. Обращение с отходами. Методика определения ртути в ртутьсодержащих отходах. Общие требования.

26. СанПиН 2.2.4.548–96. Гигиенические требования к микроклимату производственных помещений.

27. СанПиН 2.2.1/2.1.1.1278–03. Гигиенические требования к естественному, искусственному и совмещённому освещению жилых и общественных зданий.

28. СНиП 21-01-97 Пожарная безопасность зданий и сооружений

29. ГОСТ 12.1.019-2017 ССБТ. Электробезопасность. Общие требования и номенклатура видов защиты

30. ГОСТ 12.1.004-91 ССБТ. Пожарная безопасность. Общие требования

31. СанПиН 2.2.2/2.4.1340–03. Санитарно-эпидемиологические правила и нормативы Гигиенические требования к персональным электронно-вычислительным машинам и организации работы.

32. СанПиН 2.1.7.1322-03. Гигиенические требования к размещению и обезвреживанию отходов производства и потребления.

33. СанПиН 52.13330.2016 Естественное и искусственное освещение. Актуализированная редакция СНиП 23-05-95*

34. Федеральный закон «Об основах охраны труда в Российской Федерации» от 17.07.1999 №181-ФЗ

35. Конституция Российской Федерации: офиц. текст. – М.: ЭКСМО, 2012. – 36 с.

36. Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ (ред. от 01.04.2019) // Собрание законодательства Российской Федерации. - 07.01.2002. - N 1 (Ч. 1). - Ст. 3.

37. Ссылка на интернет ресурс [https://studbooks.net/2278735/informatika/komfortnyy_uroven_shuma]

38. Панин В.Ф., Сечин А.И., Федосова В.Д. Экология для инженера // под ред. проф. В.Ф. Панина. – М.: Изд. Дом «Ноосфера», 2000. – 284 с.

39. Авраамов, Ю. С. Защита человека от электромагнитных воздействий / Ю. С. Авраамов, Н. Н. Грачев, А. Д. Шляпин. — Москва: Изд-во МГИУ, 2002. — 232 с.: ил. — Это важно знать!. — Библиогр.: с. 227-231.

40. Романенко С.В. Методические указания по разработке раздела «Социальная ответственность» выпускной квалификационной работы магистра, специалиста и бакалавра всех направлений (специальностей) и форм обучения ТПУ/Сост. С.В. Романенко, Ю.В. Анищенко – Томск: Изд-во Томского политехнического университета, 2016. – 11 с.

Приложение А
(справочное)

Раздел:

Chapter 3. Development of methodology

Студент:

Группа	ФИО	Подпись	Дата
8КМ71	Прохоренко Ангелина Сергеевна		

Руководитель ВКР:

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Доцент ОИТ ИШИТР	Ротарь Виктор Григорьевич	к.т.н.		

Консультант – лингвист отделения иностранных языков ШБИП:

Должность	ФИО	Ученая степень, звание	Подпись	Дата
Доцент	Диденко Анастасия Владимировна	к.ф.н.		

3. Development of methodology

This chapter analyses the result obtained in chapter 2, and compares different RA (risk assessment) methodologies. It gives a decision framework to help users select the proper RA method according to their requirements.

3.1. Comparison of methods

We need to categorize the methods to clarify the situation and show the pros and cons of different methods. As stated before, the methods can be categorized into three types: qualitative, combined and quantitative method.

For each of the studied methods, a summary is made in the table below. It shows the characteristics as well as advantages and disadvantages of each method:

Table 3. Analysis of risk management methods and tools.

Qualitative methods			
Method	Characteristics	Advantages	Disadvantages
Hazop	Checking the reliability and availability of protective measures provided in certain nodes	Capturing possible human errors for safety and operational aspects.	Focus on single events not all opportunities, time consuming and expensive
Delphi	Experts based assessment systems	Ensuring anonymity. Independence. Objective decision.	Process complexity. Time consuming.
OCTAVE	Strategic assessment and organizational risks, assessment based on single assets	Only internal staff needed in the assessment, low cost, simple to use	Only ranking of risks, indicating no relationship between different risks, not very accurate without mathematic approval
CORAS	Feature based on UML and brain-storm method	Only internal staff needed in the assessment, low cost, simple to use	Only ranking of risks, indicating no relationship between different risks, not very accurate without mathematic approval
ETA	Using initial events to find out the cause of different routes	Able to find out different consequences of the failures and their probabilities	Inability to analyse the parallel causes of consequences. Not suitable for detailed analysis.
CCA	Cause and effect analysis	Very flexible. Able to cover most possibilities. Easy to clearly document the cause-consequence relations.	Difficulty understanding graphs
Quantitative methods			
Method	Characteristics	Advantages	Disadvantages

CORA	Based on estimating the unit losses plus expected annual losses.	Minimal preparation and information.	Requiring external experts.
FTA	Allowing identifying and analyzing the conditions and factors that cause or contribute to the implementation of a particular dangerous event.	Able to find out all possible causes of incidents and the ranking of different risks.	Difficult to understand with complicated logic relations and the need to know probability of bottom events.
Combined methods			
PRA	Understanding the strengths and weaknesses of design and operation of information systems.	Identifying event risks and causes with their consequences and probabilities.	Need for integrity and accuracy of all collected data.
AHP	Making a hierarchy of the system and quantifies the analysis.	Clear structure for good decision making.	Time consuming with complicated mathematical calculations.
FMECA	Consideration of the failure mode for every component identifying their relative importance.	Improving reliability and quality.	Time consuming and costly.

3.2. Development of a strategy for selecting the appropriate method and tool

This thesis has selected several criteria commonly shared in different methods. They are comparable elements that show preference according to the user's objective and purpose. The criteria are divided into two different sections, cost/effect and environment criteria.

Table 4. Represents the cost/effect criteria

Cost/effect criteria	Value description	Value
1. Quantitative or Qualitative	if the method is based on quantitative or combined methods	2
	the method is based on a qualitative approach	1
2. Time	if the method is less time consuming with less data preparation	3
	if the method is not time consuming with some data needed without too much processing to prepare and collect	2
	if the method is very time consuming with a complicated process and involving a large data/preparation	1
3. Human factors	if the method has flexible requirements for staff that are involved in the risk assessment process while easy to learn and implement without professional knowledge	3
	if the method requires few experts to help with the RA process	2
	If the method requires or recommends experienced risk experts or certified professionals to conduct the risk assessment	1
4. Usability	if the method is simple in the assessment process, with no need for strict proof of the steps involved while easy to maintain with no extra training needed to conduct the assessment	3
	if the method needs certain proof in the assessment process with the support of simple mathematical calculations and some extra professional knowledge	2
	if the method requires complicated mathematical formulas or proving a complex process	1

Tables 5 and 6 represent the results of evaluating the methods for each of the listed criteria. Table 5 represents the evaluation of software products based on cost and effectiveness criteria.

Table 5. Evaluation of methods based on cost and effectiveness criteria.

	Quantitative or Qualitative	Time	Human factors	Usability
OCTAVE	1	1	3	3
CORAS	1	2	3	3
CORA	1	3	1	3
COBRA	2	3	3	1
RISK Watch	2	3	3	3
FRAP	1	3	2	3
COSO ERM	2	1	2	3
@Risk	2	2	3	3

Table 6. Evaluation of methods based on cost and effectiveness criteria.

	Quantitative or Qualitative	Time	Human factors	Usability
FTA	2	2	2	1
ETA	2	2	3	2
Delphi	1	1	2	3
AHP	2	2	1	2
FMECA	2	2	2	2

3.3. Environmental criteria

The scope of risk assessment activities depends on the purpose and the capability of organization. A risk assessment method could only be focused on information security risks or cover a greater range of areas. Choosing the risk assessment method with the appropriate scope could lead to a more accurate result. The criteria can be categorized into two different types: narrow scope or broad scope.

We can define the flexibility of risk assessment activities into two types: process flexibility and time flexibility. For process flexibility, some methods are designed to assess the risk of a single process in risk assessment project, while others are capable of analyzing more complicated system risks. We consider if the method could assess in complex environment, it is a flexible method. For time flexibility, if the method could conduct the risk assessment just once and then starting from the beginning, it is not a flexible method. Thus, in the criteria we categorize the methods to be flexible and non-flexible.

Some users might have requests for support from certain risk assessment standards documents. This is due to risk assessment project purpose and requirement, usage environment or legal issues, regard to the existing difference between different nations law systems and interests.

Some methodologies might require a certain amount of usage fees, depending on the developer. The aspect listed here depends on the budget of the risk assessment project, and what level of support the user wants to get. The price criterion categorizes the methodologies into free and cost methods. So, tables 7 and 8 represent the results of evaluating the methods for each of the listed criteria.

Table 7. Evaluation of software products based on environmental criteria

	Scope	Flexibility	Standards Compliance	Purchase price
OCTAVE	Narrow	Flexible	N/A	Free
CORAS	Narrow	Flexible	ISO 31000, ISO 27000	Free

	Scope	Flexibility	Standards Compliance	Purchase price
CORA	Broad	Not flexible	N/A	Cost $7,000 to $85,000
COBRA	Broad	Flexible	ISO 27000	Cost $895 to $1,995
RISK Watch	Broad	Flexible	ISO 31000, ISO 27000 and other standards	$150,000
FRAP	Narrow	Not flexible	ISO 27000	Free
COSO ERM	Broad	Not flexible	2010.A1, 2020.A1, 2210.A1	$45,000
@Risk	Broad	Flexible	N/A	Free, but extra costs for software support

Table 8. Decision table for RA methods based on environmental criteria

	Scope	**Flexibility**	**Standards Compliance**	**Purchase price**
FTA	Broad	Flexible	BS7799/ISO27K	Free
ETA	Broad	Flexible	IEC 61025	Free
Delphi	Broad	Not flexible	N/A	Free
AHP	Broad	Flexible	BS7799/ISO27K	Free
FMECA	Broad	Not flexible	N/A	Free

To evaluate the methodologies, we first need to assign a weight to each row (Wscope, Wflexibility, Wstandards, Wprice). Depending on the requirements for different risk assessment projects, the user needs to prioritize these environment

criteria, and assign a percentage weight to each criterion. After the relative importance of each environment criteria is set, users are able to pick the right method, according to their criteria list.

For the each method, we have

SumE = Wscope* Sscope + Wflexibility* Sflexibility + Wstandards* Sstandards + Wprice* Sprice,

where W is the weight for each criterion and S is the score for each criterion.

After summing up the environmental criteria, the user needs to assess the usability of the cost/effect criteria of each methodology. To find the best result, the user needs to evaluate the relative importance of the four cost/effect criteria, and assign a percentage weight to them. The assigned weight to each cost/effect criterion is Wmethods, Wtime, Whuman, Wusability, respectively. This depends on the projects specific needs and the user's strategy. Then the total weight for each method could be calculated as:

SumC/E = Wmethods* Smethods + Wtime* Stime + Whuman* Shuman + Wusability* Susability

With this equation the user can choose and identify the most efficient method for their individual risk assessment project.

3.4. Self-developed methodology

After selecting the right RA method for a project, the project team should be able to start with a risk assessment process. In reality, as we have observed before, no single method is perfect, and it might be hard to find a perfect method for the risk assessment. Therefore, we need to tailor it or combine different methods to find the best solution. Nowadays, AI theory / machine learning / neural networks and fuzzy method are more involved in the RA process, and hybrid methods are more commonly used in practice. There is a number of hybrid methods with various purpose and different emphasis. Some of the typical ones are introduced in chapter 5. This hybrid mode framework is able to provide a standard procedure to assess the organizations risk that is compatible with generally accepted security standards.

3.5. Method foundation

3.5.1. The concept of RAF

A Risk Assessment Framework (RAF) is a strategy to share and review the information flow regarding organizational risks. A good RAF should be easy for both professional and unprofessional staff to understand. It not only focus on a single asset or system, but target the whole organization. The related environmental elements that are related to the organizations operation should be considered, e.g. the organizations goal, structure, documentation, etc. A good RAF can enable the organization to discover the potential risks, the relative level of risks, and help the organization to deal with the potential threats, making strategic development and financial plans, as well as cultivate a sustainable business culture. The existing RAFs that are widely used in the industry are ISO 27000, NIST, OCTAVE, etc., and an organization can apply them directly or modify them to create a new framework for their specific requirement.

3.5.2. Integration with 27000 standards family

The self-developed RA method presented in the following graph integrated with ISO 27000 standards family, but also borrows some ideas from ISO 31000 and NIST 800-30. The ISO 27000 standards family follows the ISMS PDCA model with continuous improvement ability.

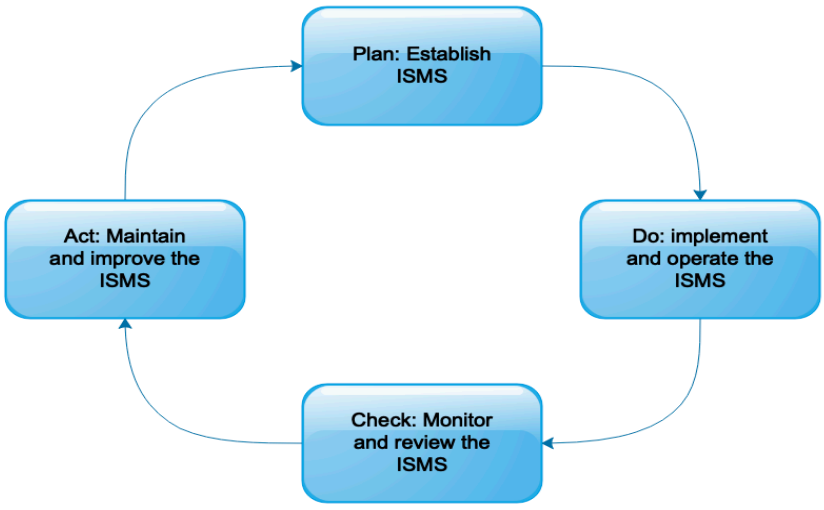

Figure 8. ISMS PDCA model defined in ISO 27000

As showed in Figure 8, ISMS continuously improves the RA performance and maintains the safety of the system. In the Planning phase, organizations identify assets and security requirements, assess information security risks and select risk controls. In the Do phase, the organization implements and operates the security policy defined the last stage, in order to control unacceptable risks. In the Check phase, the organization assesses the effectiveness of the implementation, and reviews the performance. In the Act phase, the organization takes corrective actions and preventive measures to improve performance.

3.5.3. Key Problems to solve

The main tasks of risk assessment are to assess all kinds of risk that an organization may encounter, assess the probability and impact of risk, determine the gravity of each risk for organization, choose the risk mitigation measures and corresponding reactions. There are several key questions to be considered:

1. What are the key assets that need to be protected? What is their direct use value and indirect use value?

2. What are the potential threats that these assets face? What is the source of the threats? What are the probabilities that these threats are actually occurring?

3. What are the vulnerabilities in the assets that could be used by the threats? And how easily can this happen?

4. Once the threat happens, what loss or negative effects may the organization face?

5. What security measures should the organization take to control and mitigate the risk to an accepted level?

3.6. The structure of the self-developed methodology

The method developed following the instructions of the ISO 27000 standards family, and the key definitions are derived from the standards documents. In the following part a detailed process and a model are proposed.

The purpose of this model is to target all kinds of information related risks in the organization, so the ERM concept is introduced, as the ERM Framework develops a portfolio view from three different levels: Entity level, Business level,

Operational level. According to COSO ERM model, for each level we consider eight risk components, which follow the PDCA model of the ISO standards as well. ISO 27005 instruction also state that, "Risk assessment is often conducted in two (or more) iterations". First, a high-level assessment is carried out to identify potentially high risks that warrant further assessment. The next iteration can involve further in-depth consideration of potentially high risks revealed in the initial iteration. When this provides insufficient information to assess the risk then further detailed analyses are conducted, probably on parts of the total scope, and possibly using a different method.

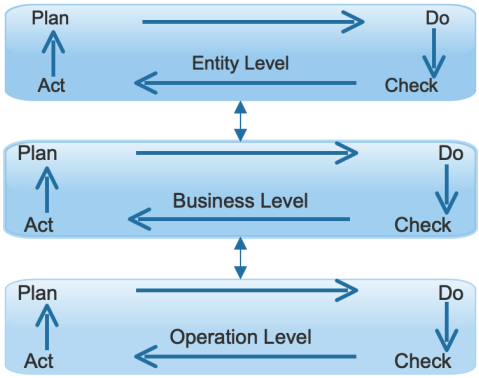

Figure 9. Data flow between different levels of IT systems in risk assessment activity

The data flow in between identifies information and guidance from the upper level to lower level and the feedback information for continuous improvement from lower level to upper level.

3.7. Method implementation

After the structure of the risk assessment method has been decided, we come to the implementation part. This method follows the ISO 27005 instructions in all three levels of organization of conducting risk assessment. The thesis is used the operational level as an example to illustrate the implementation of the risk assessment process. The main process for risk assessment according to ISO 27005 are: risk identification, risk analysis, risk evaluation and risk treatment. In risk identification, we need to identify assets, threats, existing controls, vulnerabilities and consequences. In risk analysis, we decide the methodology to measure risks,

qualitative or quantitative. Then we assess the consequence and likelihood of the incident, and decide the level of risks. In risk evaluation, a fuzzy theory is applied to combine different experts opinions, comparisons is conducted between the estimated risks criteria and related factors are considered for the evaluation. Risk treatment is the final step including risk modification, retention, avoidance and sharing.

3.8.1. Preparatory stage

In this stage, the organization should define the goal of the risk assessment. It should meet the requirements of confidentiality, integrity and availability of the object and support the business strategy at a higher level. Then the organization needs to:

- Define the scope of the risk assessment;
- Develop criteria for the information systems risk assessment;
- Select an appropriate framework and standard for risk assessment, for this part we are using COSO ERM, AHP, a fuzzy theory and mainly based on the ISO 27000 standards;
- Maintain or build sufficient communication channels between the upper level of the management board with the lower level of technical teams. Thus, the team can have full support and enough information to carry out the risk assessment.

Human factor is also an important issue. Establishing a competent team is vital to the success of the RA process. The team is usually led by the head of project, who has sufficient knowledge in the risk assessment area and has excellent coordination skills. The team also involved people with related technical background for risk assessing. It might be good to have an official person certified for certain RA standards and tools according to the risk assessment requirement. External consultants can be helpful when necessary.

To decide if external consultants are needed or not, and how many of them are needed, an evaluation form can be used from to judge which type of approach the risk assessment project belongs to, in-sourcing, partial outsourcing or full outsourcing. In-sourcing RA approach is not involving any external consultant, full outsourcing RA approach need enough external consultants to take over the whole

project, while partial outsourcing RA approach need some external consultants depending on the project requirement. Sometimes more than one expert is involved in the team, and they give different opinions for the risk assessment. In this case a fuzzy theory can be applied to achieve a balanced result discussed in section 6.3.3.

3.8.2. Risk identification

Risk identification is to identify the information systems assets, threats and vulnerabilities. Risk identification is in charge of collecting data for the later risk analysis. An example of identification and evaluation of assets and impact assessment is provided In the ISO 27005 document, in the Annex B. For the assets identification data collection, an expert's opinion is highly valued. In orыder to get more accurate results, the Delphi method can be used. In other cases some general survey methodologies might be applied, such as questionnaires, interviews with staff and users, physical inspection or document analysis. The following part represents the risk identification process:

a. Analyzing system components: This step is to analyze information systems (on operational level here) and different subsystems, within the RA scope as defined previously and according to the organization structure and business process. It would be clearer to have a system topology map. A network topology system is a good example. In order to cover all the risks for a complete information system, we not only should consider the network components, but also software, environment and so on. A clear system structure and on identified protection requirement level for the different parts make the assets and control identification process easy.

b. Identifying assets: Based on an analysis of the system, an assets catalog can be collected. Then we assign values to assets, based on the three attributes: confidentiality, integrity, availability. There are qualitative or quantitative ways to do this. In ISO 27005 Annex B2, there is an example that shows how this could be done.

c. Identifying threats: In ISO 27005 Annex B3, there are some typical threats to information systems that are listed with sources and consequences. It is helpful to refer to this and other professional libraries/databases, to compare with the identified

assets. Some general survey methods stated in the beginning of chapter 6.3.2 can also be used. An assets-threats table can be drawn in this step. Then we assign the likelihood level to each threat, based on an expert's experience or some statistical data from previous activities.

d. Identifying vulnerabilities: Vulnerability identification is done based on the definition introduced at 3.1.3. Since vulnerability is not affected if the threat does not happen, we can have this step after identification of threats. Beside the normal survey methods mentioned in the beginning of this chapter, some technical methods such as automated vulnerability scanning tools, security testing and evaluation, penetration testing, code review can be used. An impact value is assigned to the vulnerable part depending on how serious the consequence is. After this step, we can have a table of the relation between assets, threats and vulnerabilities.

e. Identifying existing controls: According to ISO 27005, existing risk controls can be identified from documentation of controls and risk treatment implementation plans. There are two types of risk controls: 1) prevention for potential threats that have not happened yet, and 2) protection for already existing vulnerabilities. It is not easy to assign a value to this part, but a list of existing controls and usages status is achieved, and it helps better assess the likelihood and impact when a threat actually takes advantage of a vulnerability. Figure 10 shows the structure of all the elements that are needed to be identified for risk assessment in the information system. After the identification, we should be ready for the next step, the analysis and evaluation part.

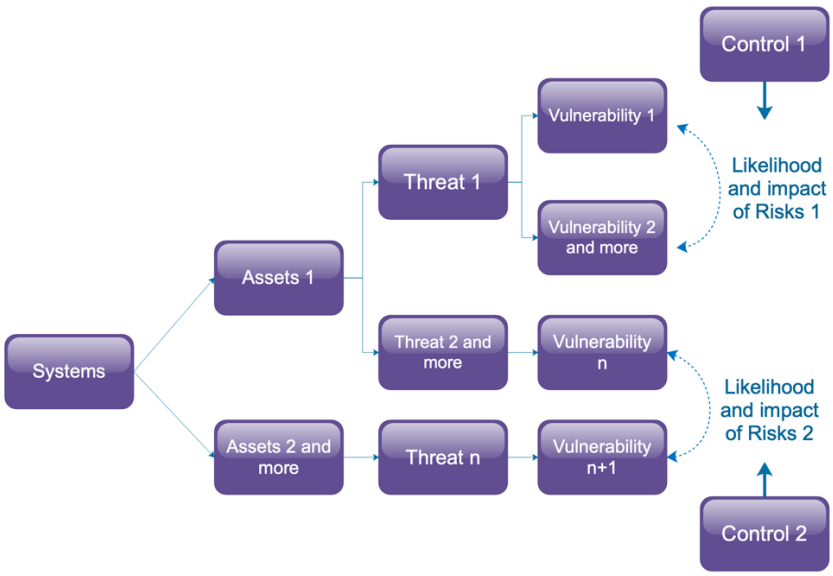

Figure 10. Relations of different criteria of risk assessment

3.8.1. Risk analysis and evaluation

From previous step, we can have a clear map of the risk influence factors of the information system. Now we evaluate each of the influence factors individually and comprehensively. This means for different valued influence factors, we need to standardize the figures for comparison and consideration in order to come to a balanced conclusion. There are quantitative and qualitative methods to assess previous influence factors. In this section, we are using a fuzzy theory.

First, we assign a single value to each influence factors in the RA process and then give a comprehensive assessment of the whole risk. This is a typical approach when dealing with qualitative data that varies in a certain range. By analyzing the collected data, we can have a quantitative description of the final judgment. The detailed process is show in the following paragraphs. For risk assessment with many people involved, a fuzzy theory is a mathematical way that can significantly unite various opinions with weights on basic requirement on the target and get the best result in theory with little objective interference. There are other approaches to deal with quantitative values that this thesis does not cover.

In the structure each influence factor that belongs to the same layer has a different influence on the upper layer, so it is important to identify their weight as

well. To identify the weight of each influence factor, the AHP method is applied. It can show the relative importance of bottom factors to the total goal, by constructing an evaluation matrix and comparing factors with each other. Thus, it helps us to solve complex relations of influence factors and multi-level structured problems.

AHP is a typical subjective weighting method that heavily depends on the decision makers experience and judgment. Similar to the Delphi method that combines experts opinions in evaluation of the weight. There are also objective weighting methods such as the entropy method, which is usually more accurate and flexible, but also more time consuming. The AHP structure regarding the information systems shown in Figure 1.

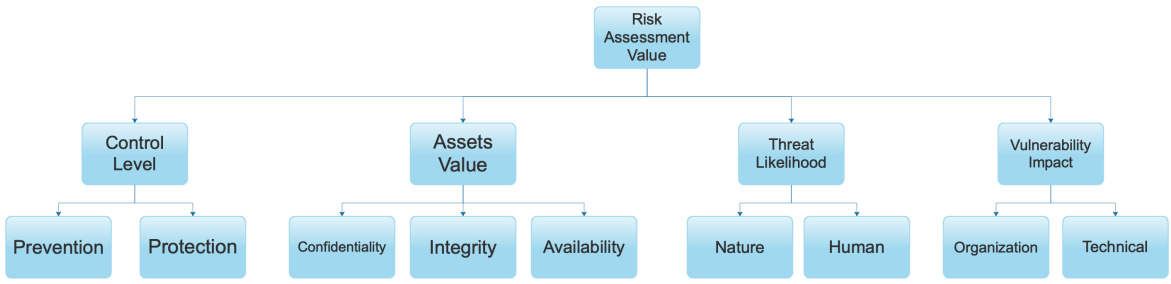

Figure 11. AHP structure of risk assessment

The first three AHP layers are defined: the top layer is the goal layer, the criterion layer, and the alternatives layer. Secondly, a pair-wise comparison is conducted to calculate the weight of each influence factor to their upper level criteria. For the criteria that have been identified, we take the criterion layer as an example, a judgment matrix can be derived from the experts estimation. Following the proportion criteria theory, a nine-level comparison table is derived.

Table 9. Comparison table

Score (M)	Meaning
1	Two factors are equally important
3	One is moderately more important than another
5	One is considerably more important than another

7	One is very strong and more important than another
9	One is extremely strong and more important than another
2, 4, 6, 8	Median value is supplemented by previous judgment
1, 1/2, 1/3, ... 1/9	The value is reversed compared to the previous judgment

Table 10. Judgment matrix

	Control	Assets	Threat	Vulnerability
Control	1	M_1	M_2	M_3
Assets	$1/M_1$	1	M_4	M_5
Threat	$1/M_2$	$1/M_4$	1	M_6
Vulnerability	$1/M_3$	$1/M_5$	$1/M_6$	1

In the judgment matrix, M1 represents the importance level of the Control factor, in analogy with the Assets factor in the RA process consideration. And 1/M1 represents the reverse relations. The rest of parameters are listed in the same way. Then we have the calculation matrix:

$$W = \begin{bmatrix} 1 & M1 & M2 & M3 \\ 1/M1 & 1 & M4 & M5 \\ 1/M2 & 1/M4 & 1 & M6 \\ 1/M3 & 1/M5 & 1/M6 & 1 \end{bmatrix}$$

To normalize the matrix, we can get the weight set for these four factors (W1, W2, W3, W4). With each factors weight being decided, an evaluation matrix is made to combine different experts judgments together. An evaluation matrix is shown below:

$$R_g = \begin{bmatrix} R11 & R21 & R31 & R41 \\ R12 & R22 & R32 & R42 \\ \dots & \dots & \dots & \dots \\ R1j & R2j & R3j & R4j \end{bmatrix}$$

In the matrix, here R_{ij} is the evaluation of each risk factor that has been assessed by each expert, where i represents four risk factors in our case: Control, Assets, Threats, Vulnerability, that influences the final information systems risks. And j represents the experts series number. To quantify the risk factors the expert could assign scales, 1 – 5 to each R_{ij}, where 1 indicates the least important and 5 indicates extremely important to the upper level criteria. If more detailed evaluation is needed, we can have a 1 – 9 scaled systems as well. The final risk presents as:

$$R_{final} = W_g * R_g = (W_1, W_2, W_3, W_4) * \begin{bmatrix} R11 & R21 & R31 & R41 \\ R12 & R22 & R32 & R42 \\ \dots & \dots & \dots & \dots \\ R1j & R2j & R3j & R4j \end{bmatrix},$$

where W_g represents the weight of the four risk factors, as achieved in the judgment matrix, and R_g represents the opinion matrix assessed by the experts. For the sub-layers, the same method applies so the impact and likelihood of each influence factor to the goal would be very clearly identified, as showed in Table 11.

Table 11. Decision table for AHP analysis.

First Layer Criteria	Evaluation	Second Layer Criteria	Evaluation
Control	R1	Prevention	S1
		Protection	S2
Assets	R2	Confidentiality	S3
		Integrity	S4
		Availability	S5
Threats	R3	Nature	S6
		Human	S7
Vulnerability	R4	Operational	S8
		Technical	S9

So, the result is the comprehensive judgment from various experts regarding each influence factor. With this method the final risk can be assessed from bottom up, layer by layer. With the risk factors values identity, we can compare them with the previous criteria and finally decide the overall risk. In ISO 27005 Annex E2, three methods are recommended to do this. There are: 1) a matrix with predefined values, 2) ranking of threats by measures of risk, and 3) assessing a value for the likelihood and the possible consequences of risks. Since we already have the absolute values of the risk factors, but where these values lack the practical meanings without analyzing in specific environments. Here the risk matrix would be the proper way to deal with these factors.

		1			2			3			4			5			Likelihood of threats
		1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	Ease of Exploration
1	1																
	2																
	3																
2	1																
	2																
	3																
3	1																
	2																
	3																
4	1																

	2															
	3															
5	1															
	2															
	3															
Assets Value	Existing Control Level															

Figure 12. Overall risk matrix

In Figure 12, an achieved final risk assessment result is mapped into the risk matrix, with its four risk factors. With the help of risk matrix, the user can easily decide the risk level by checking where the result is located in the matrix.

For this AHP example structure, the practical cases might be more complicated or analyzed in a different way, the reader can use the method flexibly. The risk matrix might also exist in other forms, some people developed it in 3 axes, or with different attributes, but the same principle applies.

3.9. Remaining Problems

The proposed methodology in the thesis basically follows ISO 27000 guidance. Even though this standard is internationally recognized and widely used now, there are still some inevitable problems that remain. This is for various reasons, such as insufficient environment to carry out all the processes, limitless of organizational structure and resources. Obscure description of the process in the method/standard can also cause trouble, though this might depend on the situation. For example, on what level should the organization identify assets? Too large would lead to less accuracy, too small would be time-consuming.

Identification of threats and vulnerabilities would also give similar problems. The same threats can affect different assets, but depending on existing vulnerabilities and which controls that are in place, the impact might vary. So, in general, it is very

important to consider these issues. It is difficult to put this into rules. Thus, it might affect the result or cause extra trouble for an inexperienced evaluator. Experience would definitely be of value in such a situation.