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

Кафедра «Прикладная математика и информатика»
(наименование)

09.04.03 Прикладная информатика
(код и наименование направления подготовки)

Управление корпоративными информационными процессами
(направленность (профиль))

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА (МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ)

на тему Разработка дорожной карты развития системы менеджмента информационной безопасности (на примере АО "Вологдаоблэнерго")

Обучающийся К.С. Чернышев
(Инициалы Фамилия) (личная подпись)

Научный руководитель канд. экон. наук, доцент Т.А. Раченко
(ученая степень (при наличии), ученое звание (при наличии), Инициалы Фамилия)

Тольятти 2024

Содержание

Введение

В современном мире, где автоматизация и повсеместное применение информационных технологий (далее - ИТ) является его неотъемлемой частью, важность электрической энергии, которая необходима для их функционирования, переоценить сложно. Практически любое предприятие или организация имеет оборудование, требующее постоянного потребления электроэнергии, при отсутствии которого имеется риск остановки всего производства. Предприятия, занимающиеся выработкой электроэнергии и её транспортировкой, называются предприятиями топливно-энергетического комплекса (далее - ТЭК) и входят в состав критической информационной инфраструктуры (далее - КИИ) государства [40]. Как правило предприятия ТЭК являются предприятиями непрерывного цикла, круглосуточно выполняющими свои функции. Нарушение их работы является серьезной проблемой, которая может привести к негативным социальным и экономическим последствиям. К сожалению, не редкость, когда такие инциденты возникают по причинам нарушения требований информационной безопасности (далее - ИБ).

В текущий момент, вопросы ИБ на предприятиях энергетики, особенно в условиях напряженной геополитической обстановки, привлекают достаточно много внимания и вызывают особую озабоченность как со стороны владельцев, так и со стороны государства. Поэтому их решение имеет высокую актуальность, а в некоторых случаях, критическую необходимость.

Доказательством тому являются следующие нововведения:

– Федеральным законом от 26.05.2021 года № 141-ФЗ Кодекс об административных нарушениях дополнен статьёй: «13.12.1. Нарушение требований в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации»;

– Федеральным законом от 26.07.2017 года № 194-ФЗ внесены изменения в главу 28 Уголовного Кодекса Российской Федерации, предусматривающие наказание за «Неправомерное воздействие и неправомерный доступ к охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуры Российской Федерации»;
– Министерством цифрового развития, связи и массовых коммуникаций РФ запущена программа формирования региональных штабов по кибербезопасности, направленная на систематичное решение актуальных угроз ИБ и разработке мер по усилению защищенности цифровой инфраструктуры регионов [24].

Также в пример можно привести Указ Президента РФ №250 от 01.05.2022 года «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» который содержит требования о возложении на руководителей предприятий КИИ персональной ответственности за обеспечение ИБ, более того необходимости создавать структурные подразделения по защите информации.

Эти требования вполне оправданы, так как одним из основополагающих этапов, в формировании ландшафта ИБ предприятия, является организация структуры управления этим направлением, а в последующем, его постоянным совершенствованием.

Управление ИБ принято называть - системой менеджмента информационной безопасности (далее - СМИБ) [27]. Она включает в себя управление рисками, знаниями, инцидентами, организационно распорядительной документацией (далее - ОРД), персоналом и многими другими аспектами.

Изучением СМИБ и проблемами её реализации занимались многие российские учёные: Дорофеев А.В., Марков А.С., Рытов М.Ю., Минзов А.С. и другие, что является подтверждением актуальности изучения данных вопросов.

Целью данной работы является разработка дорожной карты развития СМИБ предприятия для повышения уровня её состоятельности и, следовательно, эффективности.

Объектом исследования является СМИБ предприятия ТЭК.

Предметом исследования является процесс стратегического планирования развития ИБ.

Гипотеза научного исследования заключается в предположении того, что реализация проектов разработанной дорожной карты позволит оказать положительное влияние на рост состоятельности процессов СМИБ.

Научная новизна заключается в:

- разработке комбинированного метода оценки состоятельности СМИБ с применением модели CMMI;
- разработке метода ранжирования проектов ИБ с доминирующим коэффициентом.

Задачи, поставленные к выполнению, в рамках работы над диссертационным исследованием:

- изучить теоретическую и методическую основу предметной области;
- провести анализ объекта исследования;
- провести оценку состоятельности СМИБ предприятия;
- определить перечень проектов развития СМИБ и первоочерёдность их реализации;
- разработать дорожную карту развития СМИБ.

1 Теоретический раздел

1.1 Законодательные нормы и требования в сфере управления информационной безопасностью

Логично предположить, что развитие или внедрение какого либо процесса, тем более на предприятиях являющихся КИИ, не рационально без предварительной оценки его текущего уровня, а также согласованности таких изменений с отраслевыми и законодательными требованиями, так как эта область напрямую курируется государственными органами. В противном случае ликвидируя одни риски есть высокая вероятность создать другие. Поэтому для понимания вектора развития ИБ и процессов её управления нужно их идентифицировать и изучить соответствующие методические и законодательные требования, а также научные работы в области аналогичных исследований. Полученная информация будет являться теоретической базой данного научного исследования.

В сфере защиты информации и ИТ в целом, за последние 20 лет, было разработано достаточно много документов, описывающих общие требования к организации управления ИБ. Рассмотрим некоторые из них, для начала те, которые позволят нам выделить общий вектор и представление о безопасности информации с точки зрения официальной позиции государственных органов:

Доктрина ИБ РФ (утв. Указом Президента РФ от 5 декабря 2016 г. № 646), Настоящая доктрина представляет собой официальную систему взглядов, направленную на обеспечение безопасности Российской Федерации в области информации [38]. Относительно нашей темы исследования становиться понятно, что ИБ как термин носит официальный характер, а необходимость её обеспечения имеет один из перспективнейших и необходимых направлений защиты не только локальных предприятий, но и государства в целом.

Следующий один из наиболее значимых документов который имеет отношение к защите информации это Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации». «Настоящий Федеральный закон регулирует отношения, возникающие при:

- осуществлении права на поиск, получение, передачу, производство и распространение информации;
- применении ИТ;
- обеспечении защиты информации» [39].

Конечно, правил и методов управления ИБ в данном документе не имеется, но имеются высокоуровневые классификации информации по открытости её оборота и концепции позволяющие в рамках данного закона понимать зону ответственности защиты информации в целом, а при проектировании ОРД, касаемо защиты информации, ссылаться на термины содержащиеся в данном законе.

Говоря о классификации информации ограниченного доступа можно выделить мнение Кикалова М.Ш., Саидова А.Г. в научной статье «Проблемы классификации информации с ограниченным доступом» [15]. в которой авторы уделяют особое внимание правильному классифицированию документов в организации исходя из их разделения на общедоступную, закрытую и информацию обязательную к распространению. Таким образом при управлении документами и рисками, необходимо учитывать данные вопросы. В соответствии с этой классификацией была разработана схема, которая продемонстрирована на рисунке 1.

Рисунок 1 - Классификация информации по открытости

Следующий документ, на который необходимо обратить внимание, называется «Перечень сведений конфиденциального характера» (утвержден Указом Президента РФ от 6 марта 1997 г. N 188) он важен для того, чтобы понимать какие сведения запрещены к свободному обороту и передаче, соответственно их нужно защищать. Для СМИБ, данный документ будет полезен также для классификации информации по признаку открытости её использования. Перечень содержит 7 пунктов, каждый из которых кратко описывает сведения являющиеся конфиденциальными (виды тайн и других данных), за исключением сведений составляющих государственную тайну [37].

Деятельность, связанная с безопасностью, особенно социально значимых объектов и объектов КИИ не обходиться без участия федеральных законов. Об этом пишет Гунченко А.Г. в своей статье «Формирование единого подхода к подготовке специалистов в области правового обеспечения безопасности КИИ» [9]. В частности, о том, что роль организационных мер обеспечения безопасности включает в себя актуальную систему правовых мер.

Очевидно что, одним из основных направлений работ служб ИБ является защита КИИ, соответственно управление безопасностью

направленное на эти цели должно быть построено в соответствии с требованиями Федерального закона от 26.07.2017 г. № 187-ФЗ «О безопасности КИИ РФ» который регулирует выполнение определенных мер и процедур направленных на устойчивое функционирование цифровой инфраструктуры субъектов КИИ. Данным законом необходимо руководствоваться всем операторам связи, предприятиям космической и горнодобывающей отрасли, а также предприятиям ТЭК. Также из него следует уяснить что, регулирующим органом, за выполнением требований защиты информации и обеспечения безопасности КИИ, является Федеральная служба технического и экспортного контроля (далее - ФСТЭК) [40].

Разбор ключевых тезисов и теоретическое применение данного закона описывают Горелик В.Ю. и Безус М.Ю. в своей научной статье «О безопасности КИИ РФ», также в статье сделаны ссылки на основные приказы и методические документы призванные оказать практическую помощь в построении системы защиты информации [5]. Некоторые документы мы разберём подробнее и выясним как они влияют на СМИБ.

Приказ ФСТЭК России от 25 декабря 2017 г. N 239 «Об утверждении Требований по обеспечению безопасности значимых объектов КИИ РФ» гласит: «Обеспечение безопасности в ходе эксплуатации значимого объекта осуществляется субъектом КИИ в соответствии с эксплуатационной документацией и ОРД по безопасности значимого объекта и должно включать реализацию следующих мероприятий:

- планирование мероприятий по обеспечению безопасности значимого объекта;
- анализ угроз безопасности информации в значимом объекте и последствий от их реализации;
- управление (администрирование) подсистемой безопасности значимого объекта;

– управление конфигурацией значимого объекта и его подсистемой безопасности;
– реагирование на компьютерные инциденты в ходе эксплуатации значимого объекта;
– обеспечение действий в нештатных ситуациях в ходе эксплуатации значимого объекта;
– информирование и обучение персонала значимого объекта;
– контроль за обеспечением безопасности значимого объекта» [31].

То есть при наличии объектов КИИ данный приказ накладывает функции управления планированием, операционным управлением, ситуационным управлением, управление знаниями и повышением осведомленности. Поэтому данные требования будут иметь прямую связь с рассматриваемыми в дальнейшем вопросами развития СМИБ, их необходимо учесть.

Такое же влияние оказывает и приказ ФСТЭК №235 от 21.12.2017 г. «Об утверждении Требований к созданию систем безопасности значимых объектов КИИ РФ и обеспечению их функционирования» [32], а также, в случае обработки персональных данных (далее - ПДн) в информационных системах приказ ФСТЭК №21 от 18.02.2013 г. «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности ПДн при их обработке в информационных системах персональных данных (далее - ИСПДн)» [33]. Меры, предусмотренные последним, «принимаются для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, а также от иных неправомерных действий в отношении ПДн» [33], которые являются конфиденциальной информацией, а значит попадают в зону ответственности СМИБ. Поэтому данные аспекты необходимо учитывать.

1.2 Обзор методической базы и научных работ по теме исследования

Рассмотрев законодательную базу и вышерассмотренные научные работы становиться понятно, что управление и организация ИБ включает в себя множество процессов. Соответственно для каждого процесса должны выбираться эффективные методики и инструменты управления, так как они существенно облегчают достижение поставленных целей. Но помимо углубления в составляющие процессов СМИБ, некоторые учёные, например, Коломыц О.Н., в своей научной статье «Методы управления ИБ предприятия» классифицирует и методы менеджмента ИБ [16]. Классификация методов менеджмента ИБ продемонстрирована на рисунке 2.

Рисунок 2 - Классификация методов менеджмента ИБ

Данная классификация наглядно показывает каким аспектам управления необходимо уделять внимание. Более того в настоящей статье отображены взгляды на основные составляющие информации. Описаны взгляды на важность информационной пирамиды менеджмента организации, а также важность в управлении ИБ в частных организациях. Проведён анализ

нормативной и методической базы изучаемой предметной области. Также автором сделан акцент на необходимость участия высшего менеджмента организации в процессах реализации СМИБ.

Наиболее преимущественным процессом СМИБ, по мнению многих авторов научных статей, является управление угрозами и рисками ИБ, которым нужно противостоять. Об этом пишет Дорофеев А.В. в своей статье «Менеджмент информационной безопасности: Управление рисками», автор называет управление рисками ядром СМИБ. В данной статье приведены практические методы описания рисков ИБ на предприятии в виде таблиц с соответствующими критериями их последствий реализации. Данный метод является унифицированным подходом оценки рисков ИБ, но требует разработки собственных критериев оценки риска [12].

Решение по классификации критериев предлагает Кондраков О.В. в своей статье «Методология оценки риска в контексте экономической безопасности топливно-энергетического комплекса», автор выделяет разовые, периодические и постоянные риски с их количественной оценкой [17]. С точки зрения управления рисками, данная работа позволит разработать и внедрить систему мониторинга состояния ТЭК, с целью прогнозирования рисков и неблагоприятных ситуаций.

Также хочется отметить, что в соответствии с ГОСТ Р ИСО/МЭК 17799-2005 «Практические правила управления информационной безопасностью» который содержит рекомендации по управлению ИБ лицами, ответственным за планирование, реализацию или поддержку решений безопасности в организации. Выделены концептуальные этапы по работе с рисками в следующем порядке:

– «оценка рисков: Оценка угроз, их последствий, уязвимости информации и средств ее обработки, а также вероятности их возникновения;

– управление рисками: Процесс выявления, контроля и минимизации или устранения рисков безопасности, оказывающих влияние на информационные системы, в рамках допустимых затрат» [6].

В 2021 году был разработан Методический документ, утвержденный ФСТЭК России 5 февраля 2021 года, под названием "Методика оценки угроз безопасности информации". Этот документ определяет порядок и содержание работ по определению угроз безопасности информации, которые могут возникнуть в информационных системах, автоматизированных системах управления и информационно-телекоммуникационных сетях. Также он может служить полезным руководством для определения угроз безопасности информации в информационных системах ТЭК [22].

В качестве постоянного улучшения процесса риск менеджмента, как основной части СМИБ, Макеев, А. С. в статье «Менеджмент рисков информационной безопасности как непрерывный процесс» берёт за основу цикл Деминга-Шухарта как на непрерывный процесс улучшения и отслеживания качества управления. Автор считает информационные активы наиболее уязвимыми и в тоже время самыми ценными в современных реалиях. Выявление рисков на ранних стадиях позволяет эффективно бороться с ними и выстраивать устойчивую защиту. Рассмотрены и вопросы самого внедрения риск-менеджмента в организации как аспект ИБ [21]. Наглядный пример цикла совершенствования риск менеджмента продемонстрирован на рисунке 3.

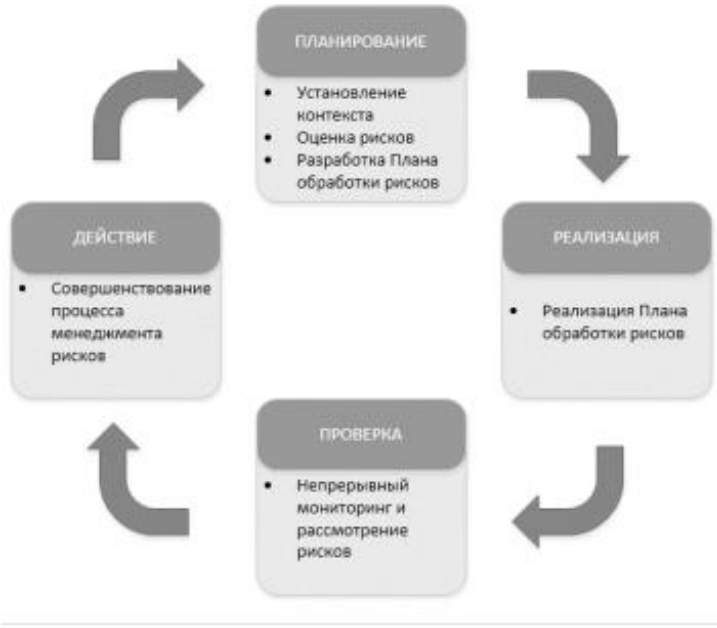


Рисунок 3 - Цикл совершенствования риск-менеджмента

Данный цикл основан на модели PCDA (Plan Check Do Act), он определенно стимулирует к эффективному управлению рисками и применим к нашему объекту исследования т.к. улучшение и постоянная актуализация процессов управления лежит в основе зрелого управления.

Ответы на вопросы о регулярном улучшении процессов управления ИБ и улучшения менеджмента ИБ в организации предлагает ГОСТ Р ИСО/МЭК 27002-2012 «Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности» [7].

Меры, изложенные в данном национальном стандарте, представляют собой полное руководство по общепринятым практикам управления ИБ. Реализация целей управления, а также мер и средств контроля и управления настоящего национального стандарта направлена на удовлетворение требований, определенных оценкой рисков. Настоящий национальный стандарт может служить практическим руководством по разработке систем безопасности организации, для эффективной практики менеджмента безопасности организаций [7].

Также стоит обратить внимание на ГОСТ Р ИСО/МЭК 27003-2012 «Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности [8]. «Руководство по реализации системы менеджмента информационной безопасности» в настоящем стандарте рассматриваются важнейшие аспекты, необходимые для успешной разработки и внедрения СМИБ. В нем описывается процесс определения и разработки СМИБ от запуска до составления планов внедрения. В нем описывается процесс получения одобрения руководством внедрения СМИБ, определяется проект внедрения СМИБ (упоминается в данном международном стандарте как проект СМИБ) и представлены рекомендации по планированию проекта СМИБ, в результате которого получается окончательный план внедрения СМИБ» [8]. Диаграмма фаз проекта внедрения СМИБ продемонстрирована на рисунке 4.

Рисунок 4 - Диаграмма фаз проекта внедрения СМИБ

Исходя из диаграммы, мы видим, что управлению документами и организационным мерам в целом уделяется достаточно много внимания. В подтверждение этому Королев В. Н. в статье «Обеспечение безопасности субъекта критической информационной инфраструктуры» 2021 г.

рассматривает три основных вопроса, которые связаны между собой в рамках обеспечения безопасности субъекта КИИ: какими документами необходимо руководствоваться, как определить, относится ли организация к субъекту КИИ и как обеспечить требуемый уровень защиты критических объектов [18].

В соответствии с международными практиками по ИБ, система документов по ИБ должна быть построена по иерархической схеме с глобальными документами на высшем уровне иерархии и повышением «конкретности» по мере приближения к низкому уровню. Визуально представление иерархии продемонстрировано на рисунке 5.

Рисунок 5 - Иерархия документационного обеспечения СМИБ

К вопросу о том, как управлять составом документов, но не их содержанием предлагает своё решение А.С. Краснов в научной статье «Методика оценки степени выполнения требований по составу организационной распорядительных документов в области информационной безопасности», методика указанная в работе автора направлена на фактическую проверку наличия документов [19]. По итогу расчётов которой мы получим процентное выражение соответствия требования документов,

которые необходимо разработать. Но всё же степень проработанности содержания документов является прямой задачей сотрудников ИБ.

Основываясь на вышерассмотренных научных работах и положениях международных стандартов, как правило, рассматривают следующие четыре основных уровня иерархии, подчиненные общей концепции ИБ:

- документы, содержащие положения корпоративной политики ИБ;
- документы, содержащие положения частных политик ИБ;
- требования ИБ к процедурам;
- свидетельства выполнения деятельности по обеспечению ИБ.

Высокоуровневые документы являются обобщенными и должны изменяться при изменениях стратегического уровня. Подчиненные по иерархии документы корректируются при изменении технологий обеспечения ИБ, внедрении новых продуктов, средств защиты информации.

Помимо документационного обеспечения, анализа угроз и управления рисками на предприятиях ТЭК не обойтись без управления инцидентами, от которых никто не застрахован. Инцидент – это реализация угрозы. Об основных причинах инцидентов ИБ пишет Куйчогло С. И. в научной статье «Информационная безопасность. Атаки и вирусы в производстве» 2019 г. Автор выделяет основные причины, по которым у предприятий энергетики возникают инциденты ИБ. Самые частые из них это человеческий фактор, кибератаки на инфраструктуру, и низкая осведомленность персонала [20].

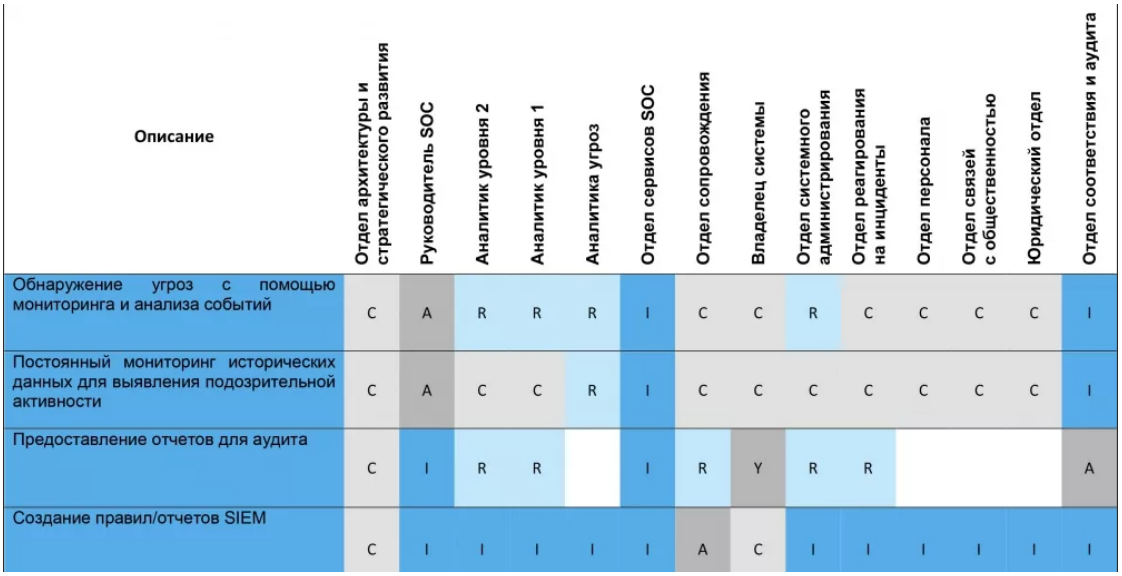
В научной статье С.А. Веревкин, А.В. Кравчук, М.И. Беляков «Методика управления инцидентами информационной безопасности на объектах критической информационной инфраструктуры» Перечислены наиболее известные и широко распространенные векторы атак, а также характеристики наиболее популярных вредоносных программ. На основе задач рассматриваемой методики выделены этапы мониторинга и анализа событий в сети КИИ с помощью баз MITRE и средств DLP, которые помогают управлять инцидентами безопасности в реальном времени по

заданным правилам [3]. Данное решение очень гибко и находит применение во всех отраслях предприятий.

Эффективное управление инцидентами должно включать следующие функции:

- выявление и своевременное реагирования на инциденты ИБ;
- формализация порядка управления инцидентами ИБ;
- разработка критериев отнесения того или иного события к инциденту ИБ;
- разработка порядка классификации инцидентов ИБ;
- распределение ответственности за обеспечение реагирования на инциденты ИБ;
- применение средств, позволяющих осуществлять оценку и мониторинг инцидентов ИБ;
- проведение анализа инцидентов, разработка мероприятий, направленных на предотвращение повторного возникновения подобных инцидентов;
- разработка собственных инструкций реагирования на инциденты ИБ;
- контроль реализации процесса посредством внедрения метрик эффективности и периодического их анализа.

Выполнение каждой функции одного или нескольких процессов управления ИБ, требует определённых ресурсов, не только вычислительных, но и человеческих (трудовых). Распределить зоны ответственности помогает специальная матрица, пример матрицы продемонстрирован на рисунке 6.



Описание	Отдел архитектуры и стратегического развития	Руководитель SOC	Аналитик уровня 2	Аналитик уровня 1	Аналитика угроз	Отдел сервисов SOC	Отдел сопровождения	Владелец системы	Отдел системного администрирования	Отдел реагирования на инциденты	Отдел персонала	Отдел связей с общественностью	Юридический отдел	Отдел соответствия и аудита
Обнаружение угроз с помощью мониторинга и анализа событий	C	A	R	R	R	I	C	C	R	C	C	C	C	I
Постоянный мониторинг исторических данных для выявления подозрительной активности	C	A	C	C	R	I	C	C	C	C	C	C	C	I
Предоставление отчетов для аудита	C	I	R	R		I	R	Y	R	R				A
Создание правил/отчетов SIEM	C	I	I	I	I	I	A	C	I	I	I	I	I	I

Рисунок 6 - Пример заполнения матрицы RACI

«На пересечении задач и исполнителей ставят буквы, которые обозначают роли в процессе и степень ответственности. Из этих букв состоит аббревиатура RACI:

– R (responsible) - исполнитель задачи или подзадачи проекта. Тот, кто самостоятельно выполняет все работы в рамках задачи. Если задача масштабная, у неё может быть несколько исполнителей. Однако эффективнее разбить её на подзадачи и назначить исполнителей для каждой из них.
– A (accountable) - ответственный за всю задачу. Участник с этой ролью несёт ответственность за то, чтобы задачу завершили в срок, но не обязательно выполняет её сам. Часто A-участники назначают задачи и подзадачи R-участникам. Важно, чтобы у одной задачи был только один ответственный. При этом сам ответственный может быть одновременно и исполнителем.
– C (consult) - эксперт, который консультирует команду по вопросам, находящимся в его компетенции. Он не выполняет задачу, но даёт советы и рекомендации, которые помогают выполнить её эффективнее.

– I (informed) - участник проекта, который должен быть в курсе выполнения задачи. Результат задачи или всего проекта влияет на дальнейшую деятельность I-участников, поэтому им важно следить, что происходит» [43].

Применение данного метода распределения ответственности широко используется по всему миру без привязки к видам проектов или отдельной отрасли. Данная матрица легко строится и позволяет наглядно распределить функционал всех участвующих лиц какого-либо процесса или проекта. Таким образом Налбандян Г.Г. и Кушниренко Е.Б. в научной статье «Оптимизация распределения полномочий и ответственности по методике RACI» выделяют построение эффективной матрицы ответственности в шесть этапов от проведения вводной встречи и документирования до последующего контроля её выполнения [26].

Не менее важной задачей после первичного формирования СМИБ является повышение уровня зрелости составных процессов ИБ. Дмитриева М.А. в статье «Применение анализа зрелости информационной безопасности в системе оценки зрелости бизнес-процессов предприятия в целом» выделяет 6 уровней зрелости бизнес-процесса: Нулевой, Начальный, Повторяемый, Определенный, Измеримый, Оптимизируемый. Выводы сделаны на основании изучения существующих стандартов оценки зрелости БП. Так же в статье приведена таблица с их кратким описанием, что позволит нам изучить их более предметно в других научных работах [11].

Голованов В.Б. в статье «Модель зрелости как подход измерения эффективности процессов информационной безопасности» кроме выделения шести уровней зрелости говорит о сочетании различных методов оценки ИБ в зависимости от целей такой оценки. Приводит пример опросного листа для анализа текущего состояния аттестации уровня зрелости процессов ИБ с применением требований к зрелости процессов менеджмента ИБ. За эталонную модель СМИБ берется модель COBIT с оценкой зрелости CMM [4].

В статье «Модели зрелости управления проектами: критический обзор» Николаенко В.С., Мирошниченко Е.А., и Грицаев Р.Т. упоминают модель CMM которая в свою очередь разделялась на три подмодели для организации занимающихся разработкой, предоставлением сервиса и занимающихся закупками и обеспечением. Приводится метод для оценки уровня конкретного процесса по четырем уровням, а также проводится обзор изменений модели новой версии CMMI 2.0 которая по отношению к CMM уже не имеет разделения на подмодели, а становится единой [28]. Представление классической модели CMMI продемонстрировано на рисунке 7.

Рисунок 7 - Модель оценки зрелости CMMI

Алёшин, В.А., Баскаков А.В., Ёрохов Е.И., в статье «Модель зрелости как инструмент управления совершенствованием непрерывности безопасности бизнеса» проводят анализ моделей зрелости применимо к ИБ. Рассмотрены такие модели как O-ISM, EIM MM, методология PRISMA, CCSMM. Анализ данных моделей показал, что единой трактовки понятия зрелости нет. Каждая модель разрабатывается под свои цели и задачи. На основании стандарта ISO 27001:2005 приведена адаптивная модель зрелости в области управления непрерывностью безопасности бизнеса направленная на постоянное улучшение зрелости процессов управления ИБ [13].

В статье «Анализ уровня зрелости бизнес-процессов организаций, функционирующих на медиарынке в России» Еремия Т.В. рассматривает возможность анализа зрелости процессов кибербезопасности по модели CSMM преимуществом методики CSMM является то, что модель состоит из набора различных элементов и учитывает не только метрики, но и технологии, уязвимости, тесты, которые могут быть использованы вместе с метриками для измерения текущего состояния уровня безопасности [14]. Также стоит отметить, что зрелость бизнес-процессов менеджмента ИБ основывается на цикличном улучшении оценки и актуализации современных угроз нулевого дня.

Управление ИБ в целом можно представлять как часть управления ИТ, либо как отдельное направление, что исключило бы конфликты интересов специалистов по безопасности и специалистов эксплуатации или технической поддержки. Лучшие мировые практики по сегментированию данных направлений и управлением информационной инфраструктурой как предоставлением сервиса описано в методологии ITIL.

«ITSM и ITIL — известные методологии для управление ИТ-инфраструктурой. Чтобы лучше разобраться в особенностях систем, принципах и преимуществах их применения, стоит ознакомиться со следующим материалом:

Бизнес-процессы обычно основаны на простом управлении ресурсами, где оборудование определенного типа производит заданное количество продукции за единицу времени. Руководители знают, сколько товара нужно произвести, чтобы получить прибыль. Этот подход не применим к ИТ-инфраструктуре. Например, восстановление работы систем корпоративной почты может занять от пяти минут до нескольких дней. Разница во времени требует анализа большого количества переменных. ITSM помогает ответить на вопросы, связанные с функционированием ИТ-инфраструктуры, и может оптимизировать организационные процессы» [49].

Применение ITSM в ИБ описано в научной статье Сулейкина А.С.

«Применение методологии ITSM в электросетевой компании ПАО «МОЭСК» для процесса управления инцидентами энергосети» в которой применение методологии ITSM как пример, позволяет создать единую точку входа всех инцидентов, случившихся на объектах энергосетей, установить нормативные сроки устранения инцидентов в соответствии с их характеристиками и вывести требуемые атрибуты по каждому вида инцидента за счёт разработки SLA [36].

Теперь нужно отметить, что такое ITIL — «это сборник лучших практик, на которых ориентируется ITSM. В базе ITIL собраны детальные описания опыта ИТ-подразделений и компаний по всему миру. Её разработкой занималось управление правительственной торговли Великобритании, с целью навести порядок в ИТ-государственных учреждений. Подходы, собранные в сборнике, стали применяться в различных сервисных подразделениях. На сегодняшний день ITIL — это непросто библиотека, а полноценная индустрия по обучению и сертификации. ITIL уходит своими корнями в мир ИТ, но его принципы могут быть легко реализованы за его пределами, например, в производственных помещениях или отделах кадров» [49].

Применение ITIL в ИБ описано автором Ashraf Khazale в научной статье «ITIL framework as a standart of information security», согласно которой адаптация «ITIL включает набор методик для работы с ИТ-инфраструктурой (комплекс оборудования, ПО, процедур, коммуникаций, связанных с компьютерной техникой, документирования и навыков, необходимых для поддержки ИТ-обслуживания)» [44].

В целом по методологии ITIL управление ИТ-инфраструктурой принято называть Управлением ИТ-обслуживанием (IT Service Management), в нашем случае это сервис обеспечения ИБ (IS Service Management) которое строится на семи принципах:

– «фокус на ценности — главное в деятельности компании принести пользу клиенту;

– действия по текущей ситуации — перед использованием и интеграцией процессов стоит проверить их общее состояние и продуктивность;
– итеративный прогресс с обратной связью — при совершение каждой итерации необходимо проверять обратную связь;
– сотрудничество и открытость — все задачи компании должны решаться совместно разными подразделениями;
– целостное мышление и слаженная работа — нужно использовать системный подход в решение проблем;
– практичность и простота — использование упрощенных алгоритмов;
– оптимизация и автоматизация — системы должны быть гармоничными и оптимально использовать свои мощности» [49].

Оценку данных решений можно найти в научной статье «К вопросу о внедрении концепции ITSM в Российской отрасли» где автор Е.Г. Сорока считает, что в целом, внедрение ITSM, в отраслях российской промышленности как концепция управления, сложный и трудоемкий труд требующий колоссальных усилий и затрат, особенно в процессе сертификации и подготовки персонала. Однако затраты на внедрение таких инноваций, это инвестиции в будущее [35].

Выводы по разделу

Таким образом по завершению теоретического раздела, можно сделать вывод что ИБ является самодостаточным направлением трудовой деятельности и имеет значительную роль в обеспечении устойчивого функционирования современного предприятия, имеет множество аспектов управления, требующих индивидуального подхода и адаптации с учётом специфики конкретного предприятия и отрасли в целом.

В данный момент ИБ имеет широкий спектр законодательной и методической базы, что говорит о высоком потенциале развития данной области.

В ходе работы проведено изучение научной литературы и источников касаемо этапов внедрения ИБ, методов, инструментов и проблем оценки состоятельности её процессов, рассмотрены модели проведения таковых оценок.

На базе полученной информации, в качестве следующего шага исследования, будет проведен анализ СМИБ АО «Вологдаоблэнерго», включая организационную структуру подразделений ИТ-ИБ и их функции, реализуемые технические и организационные меры ИБ, а также имеющиеся технические средства защиты информации.

2 Аналитический раздел

2.1 Анализ организационной структуры

По результатам изучения теоретической базы исследования становится очевидно, что составление стратегии развития ИБ не рационально без предварительной оценки её состоятельности. Проводить данную оценку предлагается последовательно, с анализа и сбора необходимой информации. Начать следует с анализа организационной структуры и распределения функционала среди работников ответственных за ИБ на предприятии.

В АО «Вологдаоблэнерго» функции управления информационной безопасностью предприятия лежат на заместителе генерального директора по информационным технологиям (далее – ЗГТ по ИТ), также, как и функции управления ИТ. В зону ответственности ЗГТ по ИТ входят следующие вопросы:

- осуществление организационного и технического руководства производственно-технической деятельностью в сфере IT-инфраструктуры;
- осуществление руководства разработкой и внедрением проектов совершенствования управления производством с помощью ИТ;
- организация и контроль по вводу в эксплуатацию программно-аппаратных комплексов для нужд предприятия;
- выработка мер и осуществление бесперебойного функционирования IT-инфраструктуры предприятия;
- обеспечение ИБ предприятия, в том числе выполнение задач по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты;
- обеспечение безопасности КИИ и прочие.

В прямом подчинении у ЗГТ по ИТ находится центр IT-инфраструктур. Организационная структура центра IT-инфраструктур АО «Вологдаоблэнерго» продемонстрирована на рисунке 8.

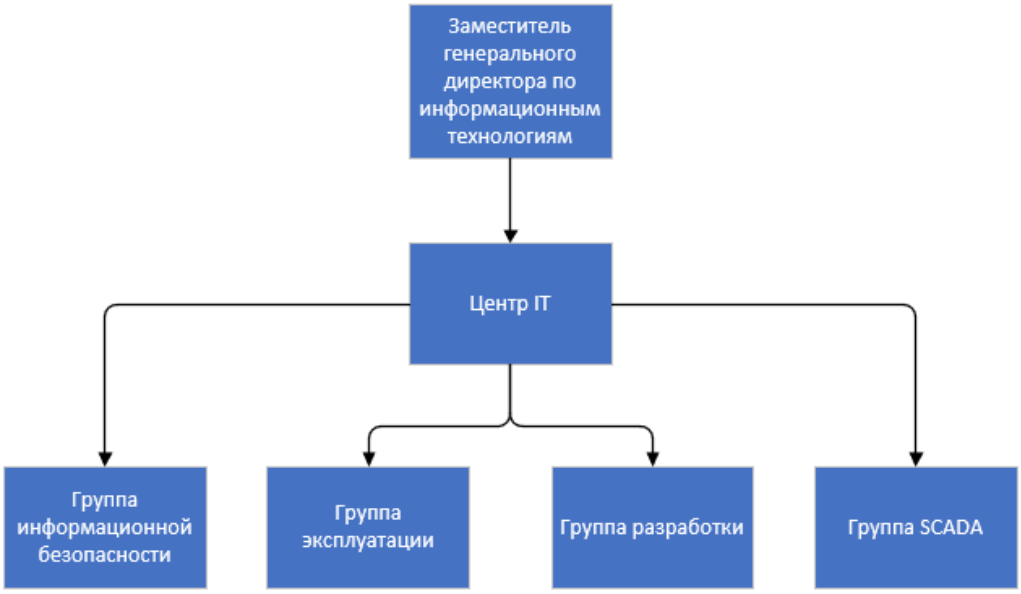


Рисунок 8 – Организационная структура центра IT-инфраструктур АО «Вологдаоблэнерго»

Большинство организационных функции по обеспечению ИБ лежат на группе ИБ, которая была организованна в составе центра только в мае 2023 года и имеет на данный момент двух сотрудников. Организационная структура группы ИБ центра IT-инфраструктур АО «Вологдаоблэнерго» отображена на рисунке 9.

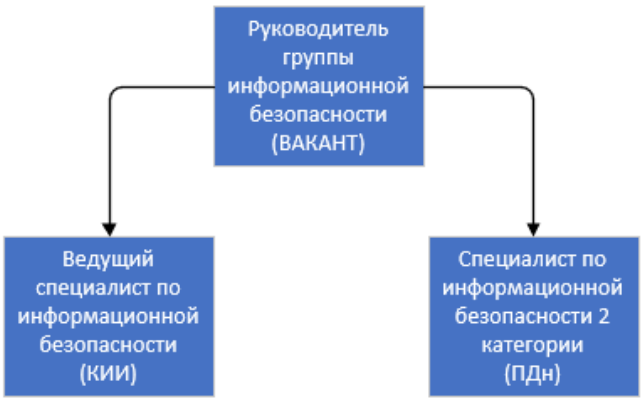


Рисунок 9 – Организационная структура группы информационной безопасности центра IT-инфраструктур АО «Вологдаоблэнерго»

Функции специалистов группы ИБ закреплены в должностных инструкциях. К примеру, некоторые из них:

- разрабатывать ОРД по обеспечению ИБ и защиты ПДн в Обществе;
- разрабатывать и реализовывать организационные меры, обеспечивающие эффективность защиты информации в Обществе;
- проводить контроль (мониторинг) состояния технических систем защиты информации;
- проводить анализ угроз ИБ и предотвращать риски утечек информации, подлежащей защите;
- проводить расследования инцидентов ИБ и выявленных нарушений мер защиты информации.

Предприятия энергетики как правило являются операторами ПДн, обрабатывающих информацию не только о своих работниках, но и о потребителях, подключенных к электросетям. Это накладывает соответствующие обязанности по выполнению широкого спектра мер ИБ ПДн, включая их безопасную обработку, хранение, уничтожение и другие.

Также все предприятия энергетики являются субъектами КИИ, зачастую имеющие в своем пользовании значимые объекты, выражаемые в информационных или автоматизированных системах управления технологическими процессами.

АО «Вологдаоблэнерго» не исключение и является как оператором обработки ПДн, так и субъектом КИИ имеющее в своём составе значимые объекты.

Поэтому в существующей организационной структуре группы ИБ, существует разделение функций и обязанностей по принципу разделения в этих аспектах: один специалист занимается комплексной защитой КИИ, а другой комплексной защитой ПДн. Должность руководителя группы в настоящий момент вакантна.

Из недостатков стоит заметить тот факт, что количество поставленных задач, с учётом масштабов предприятия, количества информационных

систем, не соразмерен количеству персонала, занимающегося ИБ. Поэтому деятельность группы в данный момент направлена на решение оперативных задач без достаточного внимания к стратегическому развитию и совершенствованию рабочего процесса.

2.2 Анализ процессов управления информационной безопасностью

Задачами в рамках управления процессами ИБ должно являться их достаточное организационное и техническое сопровождение. К организационным мерам в первую очередь относится разработка соответствующей документации. Основываясь на положениях мировых стандартов, рассмотренным в теоретическом разделе, разработку полного и логически непротиворечивого комплекта документации по ИБ целесообразно производить согласно следующей классификации документов:

- политики ИБ;
- положения и регламенты;
- инструкции и памятки соблюдения специальных требований;
- обучающие материалы, направленные на повышение осведомленности (буклеты, планы-конспекты инструктажей и прочее).

Однако, мероприятия по защите информации с точки зрения организационных мер не заключаются лишь разработкой документов. Кроме этого, следует также:

- оптимизировать бизнес-процессы;
- классифицировать информацию и обеспечивать соответствующий допуск к ней;
- создавать подразделения и/или назначать лица, ответственные за обеспечение ИБ;
- организовывать информирование и обучение персонала;
- проводить аудиты и инвентаризации технических средств;

– организовывать мероприятия по проверке действий персонала в случае нештатных ситуаций;
– обеспечивать техническую защиту помещений и контролируемых зон, следить за их соответствием нормативно-правовым требованиям;
– принимать меры безопасности, при взаимодействии с контрагентами, предусматривать меры по сохранению конфиденциальности информации и мер ответственности за ее разглашение при обмене ею;
– обеспечивать взаимодействие с государственными органами по вопросам ИБ и защите конфиденциальной информации.

Описание и наличие организационных мер в АО «Вологдаоблэнерго» продемонстрировано в таблице 1.

Таблица 1 – Организационные меры АО «Вологдаоблэнерго»

Организационная мера	Реализация
Политики информационной безопасности	Утверждена Политика информационной безопасности
Управление инцидентами	Только в рамках КИИ – План реагирования на инциденты ИБ в КИИ
Контроль доступа	Утверждены правила пропускного режима через пропускные пункты на территорию, правила доступа к ЛВС не разработаны
Классификация информации	Не реализована
Аудит информационной безопасности	Не реализована, не проводится
Обучение и повышение осведомленности персонала в сфере ИБ	Частично реализована, имеются бюллетени информирования об основных требованиях безопасности, систематичного и комплексного выполнения меры не наблюдается
Соответствие требованиям	Цели соответствия требованиям ИБ лучшим мировым практикам и требованиям регулирующих органов имеются в политике ИБ, по факту нужно проводить аудит выполнения.
Управление резервированием	Не реализовано

К техническим мерам относится использование таких средств защиты информации, как:

- средства защиты от несанкционированного доступа,
- средства доверенной загрузки,
- межсетевые экраны,
- средства антивирусной защиты,
- средства обнаружения вторжений,
- средства контроля и анализ защищённости,
- средства резервного копирования и восстановления данных,
- средства защиты среды виртуализации,
- криптографические средства.

Основными принципами построения защиты с помощью технических средств должны являться:

- архитектурная простота, минимизация компонентов и межсетевых протоколов, исключение избыточных элементов;
- внедрение проверенных программных решений, уже апробированных другими предприятиями, с учетом их преимуществ и недостатков;
- минимальные модификации лицензионных программных продуктов, выполняемые собственными или привлеченными специалистами;
- использование лицензионного ПО, предпочтительно внесенного в государственный реестр программ и баз данных;
- использование аутентичных, надежных и долговечных компонентов, совместимых друг с другом;
- управляемость и простота администрирования системы и программных продуктов, минимизация сторонней технической поддержки;

– протоколирование и документирование всех действий пользователей, связанных с конфиденциальной информацией и несанкционированным доступом;
– эшелонированная защита, предусматривающая несколько рубежей системы защиты для каждого потенциального канала утечки.

Технические меры АО «Вологдаоблэнерго» продемонстрированы в таблице 2.

Таблица 2 – Технические меры АО «Вологдаоблэнерго»

Техническая мера ИБ	Реализация
Защита периметра корпоративной сети предприятия, обнаружение и предотвращение вторжений	Не реализована в полной мере, специализированные СрЗИ отсутствуют
Защита физического периметра контролируемой зоны	PSIM система верхнего уровня – «Интеллект» включающая управление системой контроля и управления доступом, видеонаблюдением. Физическую защиту реализует служба безопасности, а не центр ИТ.
Анализ уязвимостей и инвентаризация технических средств	Не реализована
Средства антивирусной защиты	Сервер управления Kaspersky end-point Security 10, Локальные агенты антивирусной защиты на хостах ЛВС.
Средства предотвращения утечек информации	DLP Infowatch traffic monitor и personal monitoring
Средства контроля за данными	Infowatch Crawler
Средства корреляции инцидентов и оповещение о них (SIEM)	Не реализовано
Комплексное управление неструктурированными данными по всей сети	Не реализовано
Контроль мобильных устройств	Не реализовано
Защита электронной почты	Не реализовано

По итогам проведения анализа процессов управления ИБ АО «Вологдаоблэнерго» можно сделать вывод о том, что уровень организационного и технического сопровождения низкий. Документы,

устанавливающие общекорпоративный порядок управления процедурно-нормативными, распорядительными и информационными документами, не разработаны.

Большинство процедур и задач выполняются инженерами центра IT-инфраструктур, не обладающих необходимым уровнем подготовки в сфере ИБ. Поэтому такие задачи, не рассматриваются ими как приоритетные.

2.3 Анализ применяемых технических средств защиты

2.3.1 Подсистема антивирусной защиты

Подсистема антивирусной защиты (далее - ПАЗ) применяется для обеспечения антивирусной защиты рабочих станций и серверов, в том числе виртуальных, функционирует на базе комплекса Kaspersky Endpoint Security (далее - KES). Для защиты серверов под управлением операционной системы Windows и защиты рабочих станций применяется ПО KES версий 10 и 11. Для серверов под управлением операционной системы семейства Unix данное решение не применяется. Для управления используется ПО Kaspersky Security Center (далее – KSC).

Сводная информация по компонентам подсистемы антивирусной защиты на базе ПО KES приведена в таблице 3.

Таблица 3 – Сводная информация по компонентам подсистемы антивирусной защиты

Название компонента	ПО	Описание сервера	ОС	IP-адрес
Сервер управления KSC beta.elset.oets35.ru	ПО Kaspersky Security Center 11.0.0.1131; ПО Kaspersky Endpoint Security для Windows (11.1.1.126); СУБД MS SQL 2016	Выделенный виртуальный сервер ksc (ksc.bveb.by). Процессор: 2x2vCore Intel Xeon E5-2400 2,40 ГГц. Память: 8ГБ	Windows Server 2008 R2 Standard SP1	192.168.223.11

Количество лицензий антивирусной защиты продемонстрированно в таблице 4.

Таблица 4 – Количество лицензий антивирусной защиты

Наименование лицензии	Ограничение	Активно	Срок окончания подписи
Kaspersky Endpoint Security для бизнеса Стандартный Russian Edition. 500-999 + Node 1 year Renewal license: Kaspersky Security for WS and FS	550	373	25.11.2023
Kaspersky Security Center для бизнеса Стандартный Russian Edition. 500-999 + Node 1 year Renewal license: Security Center	550	373	25.11.2023

Логическая схема ПАЗ на базе решения KES представлена на рисунке 10.

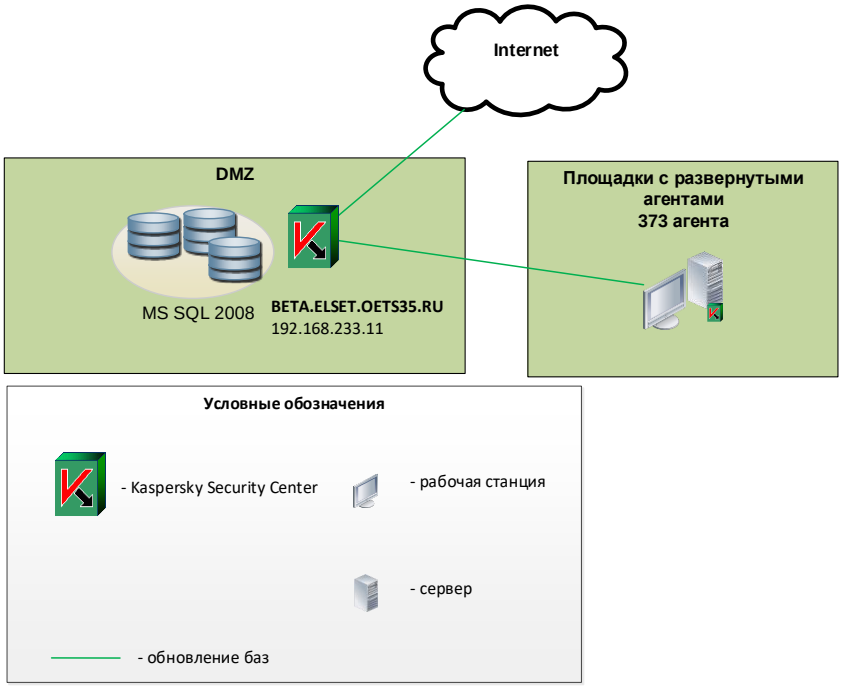


Рисунок 10 – Логическая схема ПАЗ

Для обновления сигнатур безопасности KSC обращается к общедоступным серверам. Обновление осуществляется с помощью задачи на

загрузку обновлений в хранилище KSC с периодичностью 1 раз каждый час для каждой площадки и филиала, последующего распространения на клиентах с периодичностью 1 раз каждый час.

Доступ к серверу управления KSC осуществляется с помощью консоли управления KSC, установленной на рабочей станции администратора и сервере управления KSC. Управление KSC осуществляют инженеры группы эксплуатации центра IT-инфраструктуры.

Из значительных плюсов решения, можно отметить наличие ролевой модели. Осуществляется разграничение доступа в KSC.

Для каждого филиала настроена политика, для центрального офиса расширенная, для филиалов минимальная с учетом ширины каналов.

Резервное копирование не осуществляется. Периодическое восстановление данных из резервной копии не выполняется.

Доля защищаемых устройств, которым по тем или иным причинам присвоен статус «Критический» на момент анализа, не превышает 49 % от общего числа устройств.

Устройства с присвоенным статусом «Критический» имеют ошибки, распределённые следующим образом относительно общего кол-ва установленных агентов (373). Наглядная диаграмма состояния защиты на устройствах сети представлена на рисунке 11.

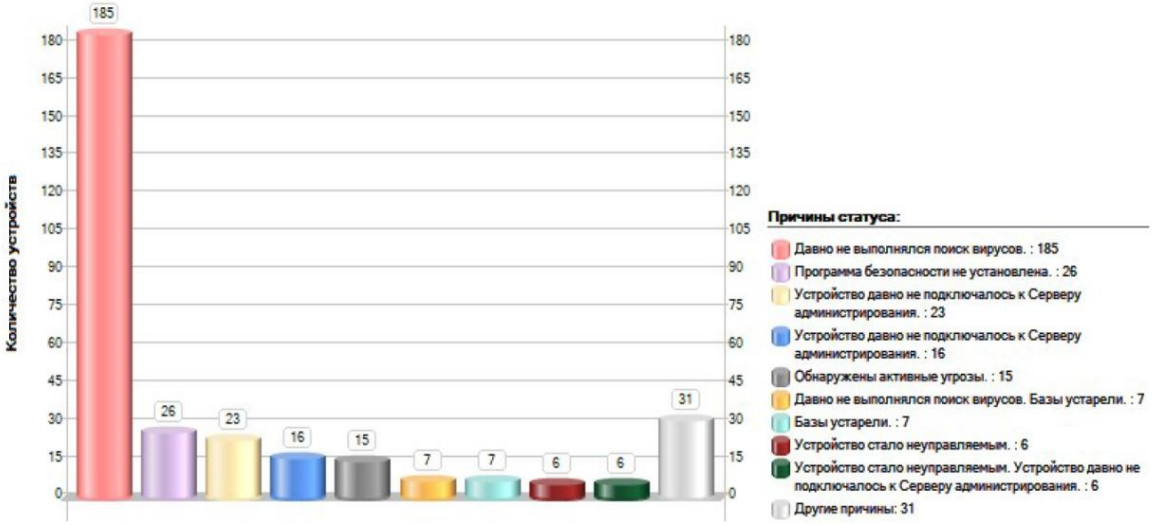


Рисунок 11 – Состояние защиты на устройствах

В целом, в части производительности ПАЗ недостатков не выявлено. В части улучшения сервисов ИБ в рамках ПАЗ рекомендуется:

- передать управление ПАЗ в зону ответственности работников группы ИБ;
- реализовать создание резервных копий ПАЗ с помощью инструментов, встроенных в KSC;
- на периодической основе проводить восстановление ПАЗ из резервной копии в тестовой среде;
- разработать необходимую документацию на систему;
- формализовать процедуры по антивирусной защите.

2.3.2 Подсистема контроля доступа в сеть Интернет

Подсистема контроля доступа в сеть интернет (далее - ПКДСИ) обеспечивает безопасный доступ пользователей к ресурсам сети интернет согласно принятой политике использования интернет-ресурсов, принятой на предприятии. В качестве средства предоставления доступа пользователей к ресурсам сети интернет выступает прокси-сервер Squid версии 3. ПКДСИ

функционирует под управлением операционной системы CentOS 7.6 версии 1810.

Авторизация пользователей для доступа в интернет при подключении пользователей к ПКДСИ осуществляется по протоколу IP рабочих станций пользователей. Пользователи получают настройки для доступа в Интернет через DHCP в виде конфигурационного файла.

Сводная информация по компонентам ПКДСИ представлена в таблице 5.

Таблица 5 – Сводная информация по компонентам ПКДСИ

Название компонента	ПО	Описание сервера	ОС	IP-адрес
Сервер SQUID	ПО	Выделенный физический сервер	ОС FreeBSD clang version 3.4.1	IP: 192.168.223.250 GW: 192.168.223.254 DNS: 192.168.223.1, 192.168.223.2

Конфигурация сервера подсистемы контроля доступа в сеть Интернет представлена в таблице 6.

Таблица 6 – Конфигурация сервера подсистемы контроля доступа в сеть Интернет

Название компонента	Доменное имя	Конфигурация сервера
Сервер SQUID	squid.elset.oets35.ru	Физический сервер: ProLiant DL380 G7, 2xIntel(R) Xeon(R) CPU X5650 @ 2.67GHz, RAM 80GB, HDD

Squid - это мощное и многофункциональное приложение кэширующего прокси-сервера, которое предоставляет широкий спектр сервисов кэширования и прокси для HTTP, FTP и других популярных сетевых протоколов. Одной из ключевых особенностей Squid является его способность осуществлять кэширование результатов DNS-поиска, что

позволяет значительно ускорить процесс получения информации о доменных именах. Кроме того, Squid поддерживает прозрачное кэширование, что означает, что он может работать без необходимости изменения настроек клиентских приложений. Squid также поддерживает широкий набор кэширующих протоколов, таких как ICP (кэширующий интернет-протокол), HTCP (гипертекстовый кэширующий протокол), CARP (протокол кэширования маршрутизации) и WCCP (кэширующий протокол перенаправления контента), что позволяет ему эффективно взаимодействовать с другими сетевыми устройствами и оптимизировать процесс кэширования. Актуальная логическая схема ПКДСИ представлена на рисунке 12.

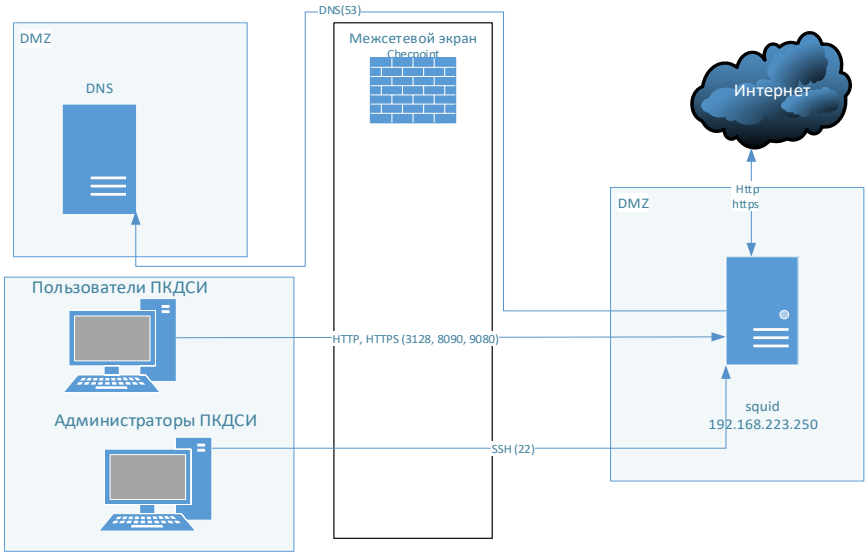


Рисунок 12 – Логическая схема ПКДСИ

Сервер ПКДСИ работает в подсети 192.168.223.0/24 и изолирован в DMZ. Для взаимодействия компонентов ПКДСИ со смежными корпоративными системами, целевыми объектами и рабочими станциями пользователей ПКДСИ на межсетевом экране настроены соответствующие разрешающие правила. Используется три типа аутентификации Basic.

Раскрытие SSL-трафика не настроено.

Для построения отчетов используется приложение Lite Squid 1.8W.

Доступ к Интернету предоставляется пользователю в соответствии со служебной запиской на имя ЗГД по ИТ.

На ПКДСИ документация отсутствует. Резервное копирование выполняется средствами среды виртуализации.

Настройку и обслуживание ПКДСИ осуществляют специалисты группы эксплуатации. По данным, полученным в ходе анализа, персонал имеет достаточную квалификацию.

По информации, полученной в ходе обследования, функционал ПКДСИ требует модернизации. В ПО Squid отсутствует внешний обновляемый категоризатор веб-ресурсов. Нет встроенного антивируса для защиты веб-трафика. Отсутствует защита от целенаправленных атак. Работы по модернизации подсистемы не планируются.

2.3.3 Подсистема защиты от утечек информации

Подсистема защиты от утечек информации (далее – ПЗУИ) предназначена для автоматизации деятельности персонала предприятия, направленной на обеспечение ИБ в части обнаружения и реагирования на события, возникающие в процессе обработки, хранения и перемещения конфиденциальной информации.

ПЗУИ функционирует на базе прикладного ПО «InfoWatch Traffic Monitor Enterprise».

Сводная информация по компонентам подсистемы защиты от утечек информации приведена в таблице 7.

Таблица 7 – Сводная информация по компонентам ПЗУИ

Название компонента	ПО	Описание сервера	ОС	IP-адрес
Сервер управления, хранения и анализа (перехват, анализ, хранение, индексация)	ПО «InfoWatch Traffic Monitor» версии 6.10.18	Выделенный виртуальный сервер iwtm.elset.oets35.ru	ОС Red Hat Enterprise Linux Server 6.9 x86 64 bit	192.168.223.225
Сервер управления агентами (InfoWatch Device Monitor, Crawler, InfoWatch Person Monitor)	ПО «InfoWatch Device Monitor» версии 6.10.18, ПО «InfoWatch Crawler Server» версии 1.0, ПО «InfoWatch Crawler Scanner» версии 1.0, ПО «InfoWatch Person Monitor» версии 7.47, ПО СУБД MS SQL Express 2017.	Выделенный виртуальный сервер iwdm.elset.oets35.ru	Windows Server 2016 Standard Edition x64	192.168.223.127
Сервер визуальной аналитики (InfoWatch Vision)	ПО «InfoWatch Vision 2.0.0».	Выделенный виртуальный сервер iwvision.elset.oets35.ru	ОС CentOS 7.6 x86 64-бит	192.168.223.128

Конфигурация серверов подсистемы защиты от утечек информации представлена в таблице 8.

Таблица 8 – Конфигурация серверов ПЗУИ

Название компонента	Доменное имя	Конфигурация сервера
Сервера управления, хранения и анализа (перехват, анализ, хранение, индексация)	iwtm.elset.oets35.ru	Выделенный виртуальный сервер: Процессор: 16vCore 2,6ГГц. Память: 192ГБ. HDD: 600 ГБ HDD SAS 10k;

Продолжение таблицы 8

Сервер управления агентами (InfoWatch Device Monitor, Crawler, InfoWatch Person Monitor)	iwdm.elset.oets35.ru	Выделенный виртуальный сервер: Процессор: 8vCore 2,4ГГц. Память: 16ГБ. HDD: 1 ТБ HDD SAS 10k. Сетевой контроллер 1 Гбит/с
Сервер визуальной аналитики (InfoWatch Vision)	iwvision.elset.oets35.ru	Выделенный виртуальный сервер: Процессор: 16vCore 3,5ГГц. Память: 256ГБ. HDD: 1 ТБ HDD SAS 10k. Сетевой контроллер 1 Гбит/с

Для расширенного контроля пользователей используется модуль ПО «InfoWatch Person Monitor» для 50 пользователей.

Сервер Device Monitor выполняет мониторинг данных на агентах Device Monitor, установленных на АРМ пользователей на площадках АО «Вологодская областная энергетическая компания» в г. Вологда. Общее количество АРМ с установленными агентами Device Monitor около 329 штук.

Контроль приложений и снимков экрана выполняется в режиме «Активных черных списков». Полученные сервером Device Monitor данные передаются на сервер Traffic Monitor для обработки в соответствии с политикой безопасности Компании. Обработанные данные (события, инциденты) помещаются в архив на сервере iwtm.elset.oets35.ru.

Так как серверные компоненты развёрнуты на нелицензированной среде виртуализации Citrix, ограничение на дисковое пространство – 2 ТБ на одну виртуальную машину, в связи с чем хранение событий на сервере Traffic Monitor организовано следующим образом: для событий с нарушениями – в течение двух месяцев, для событий без нарушений и скриншотов – в течение месяца.

Политики теневого копирования трафика на агентах Device Monitor представлены на рисунке 13.

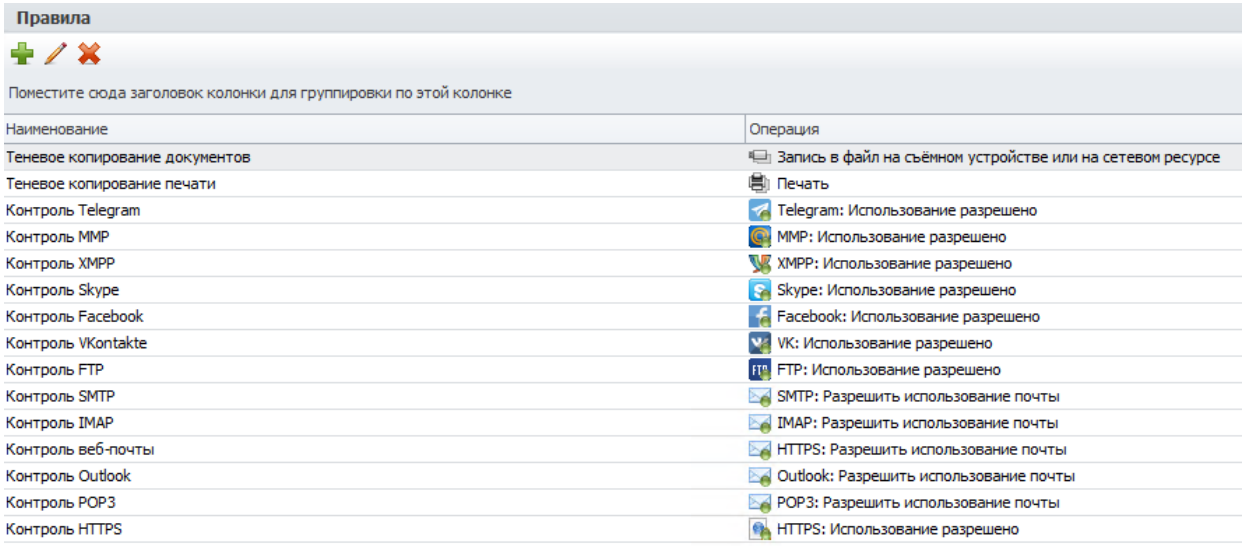


Рисунок 13 – Политика Device Monitor

Главное окно офицера администратора безопасности представляет собой набор виджетов демонстрирующих статистику нарушений за указанный период. Главное окно DLP продемонстрированно на рисунке 14.

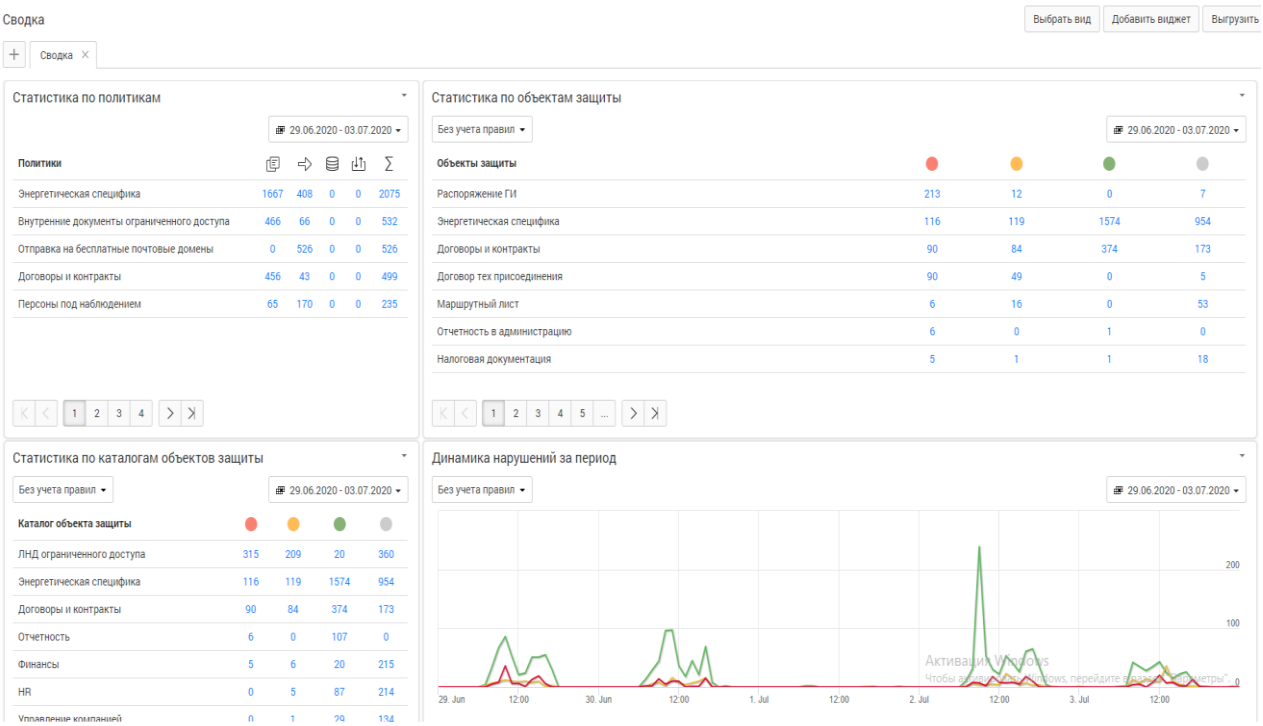


Рисунок 14 – Главное окно DLP

Используемые в ПЗУИ методы аутентификации – LDAP-аутентификация. ПЗУИ интегрирована со службой каталогов Microsoft Active Directory (далее – MS AD) в части разграничения доступа и аутентификации привилегированных пользователей.

Текущая версия агентов, используемых на АРМ пользователей, 6.10.14.349. Уведомления по событиям ИБ не настроены.

Настройка и обслуживание ПЗУИ осуществляется специалистами подрядной организации. В рамках оказываемых услуг подрядной организацией осуществляется анализ инцидентов безопасности, актуализация политик, предоставление еженедельных отчётов о выявленных инцидентах.

Резервное копирование не выполняется.

Мониторинг подсистемы не осуществляется.

В рамках проекта внедрения ПЗУИ были разработаны документы: «Положение о контроле использования технических средств хранения, обработки и передачи информации (мониторинга)» и «Положение о расследовании инцидентов, связанных с утечками информации ограниченного доступа». Документы утверждены ознакамление работников с ними происходит при приеме на работу.

Ошибок в работе InfoWatch Traffic Monitor и Device Monitor на момент проведения анализа не выявлено. Для анализа данных, хранимых на АРМ пользователей, используется модуль Crawler.

Настройку, обслуживание, мониторинг производительности и обновление серверных компонентов выполняет подрядчик в рамках контракта по обслуживанию.

Установку агентов ПЗУИ осуществляет руководитель группы эксплуатации.

2.3.4 Подсистема межсетевого экранирования

Функционал межсетевого экранирования реализован (созданы соответствующие правила доступа и NAT) на маршрутизаторах ВОЭК Cisco 1841 (cherets-gw0), Cisco 2821 (uprav-gw0), Mikrotik hEX lite (cherets-gw1), Mikrotik RB1100AHx2 (uprav-gw1).

Для пользователей доступны два способа взаимодействия с сетью Интернет:

- через прокси, реализованный на базе SQUID;
- доступ в сеть Интернет напрямую. Трафик анализируется средствами маршрутизаторов Cisco 1841 (cherets-gw0), Cisco 2821 (uprav-gw0), Mikrotik hEX lite (cherets-gw1), Mikrotik RB1100AHx2 (uprav-gw1).

Применяемые правила в FILTER на устройствах Mikrotik hEX lite (cherets-gw1) и Mikrotik RB1100AHx2 (uprav-gw1) ограничивают трафик в сеть Интернет в недостаточной мере (применяются ограничения по IP-адресам, портам/протоколам), т.к. основная фильтрация пользовательского трафика выполняется на прокси-сервере на базе SQUID и на указанных устройствах нет результирующего запрещающего правила. Для большинства правил журналирование сессий отключено.

2.3.5 Подсистема удаленного доступа

В состав подсистемы удаленного доступа входят:

- пограничный маршрутизатор Mikrotik RB1100AHx2 (uprav-gw1) ;
- VPN-клиенты на базе средств ОС Windows, подключение выполняется с помощью связки протоколов L2TP и IPsec;
- аутентификация и авторизация осуществляются посредством RADIUS-сервера (NPS-сервер) с пересылкой учетных данных в службу каталогов AD.

Порядок предоставления удаленного доступа не регламентирован.

При подключении к VPN клиенты имеют доступ ко всем внутренним информационным ресурсам (разграничение доступа для VPN-клиентов не осуществляется).

Двухфакторная аутентификация при подключении клиентов к VPN не используется.

Проверка клиентских рабочих станций при подключении к VPN не осуществляется.

2.4 Выявленные недостатки и рекомендации

По результатам проведенного анализа, общий уровень ИБ предприятия был оценен как низкий.

Основные недостатки обусловлены следующими факторами:

– усилия в области ИБ носят несистемный характер, что негативно сказывается на их эффективности. Большинство процессов ИБ не формализованы, что приводит к неуправляемости и неэффективности реализуемых мероприятий по обеспечения ИБ информационной инфраструктуры. Отсутствие согласованной программы обеспечения ИБ, учитывающей особенности инфраструктуры предприятия, не позволяет верно определить основные стратегические цели обеспечения ИБ и задачи для достижения этих целей, согласовать приоритетные методы реализации защитных механизмов, определить необходимый бюджет;

– ощутимая нехватка кадровых ресурсов по направлению ИБ. На текущий момент создана группа ИБ в количестве 2 человек, до 2023 года работал один человек. Некоторые задачи, связанные с обеспечением ИБ, выполнялись и выполняются работниками Центра ИТ-инфраструктуры, что ведет к конфликту интересов и сложности аудита действий администраторов. Также многие функции и задачи ИБ остаются непокрытыми в силу нехватки человеческих ресурсов;

– архитектура ИБ требует качественного обновления и развития. Специфика современных атак в области ИБ, такова, что мотивированный злоумышленник так или иначе и практически гарантированно сможет преодолеть любую защиту сетевого периметра и иные превентивные контроли. В этих реалиях парадигма построения систем защиты должна смещаться с «необходимо не пустить злоумышленника в сеть» на «сетевой периметр и пользовательские учетные записи всегда могут быть скомпрометированы, и защита должна основываться на максимально быстром обнаружении факта проникновения» ;
– ряд необходимых средств защиты отсутствует. В ряде случаев процесс ИБ просто не может функционировать как процесс без использования специального инструментария. Это обусловлено значительными объемами данных, которые необходимо анализировать (например, при мониторинге событий ИБ или анализе трафика на утечки). Отсутствие необходимых средств защиты или использование непригодных приводит к тому, что действия приходится выполнять вручную и с недопустимой периодичностью, что приводит к их неэффективности.

Описанные выше негативные факторы порождают следующие недостатки/проблемы ИБ, выявленные в ходе работ:

– большинство процессов ИБ не реализуются, что приводит к повышенным рискам нарушения ИБ активов предприятия, среди которых: несанкционированный доступ, нарушение функционирования ИТ-сервисов и другие;
– процессы ИБ выполняются неформально или в соответствии со сложившейся «исторической практикой», или какие-либо требования были зафиксированы электронными письмами/памятками;
– работники, ответственные за сопровождение элементов ИТ-инфраструктуры, самостоятельно определяют необходимые

настройки, в результате чего они (настройки) могут отличаться от рекомендованных лучшими практиками по безопасности;

- инвентаризация выданных прав доступа не производится на периодической основе, часть пользователей (в том числе работники сторонних организаций) обладает избыточными правами;
- оценка защищенности ИТ-инфраструктуры посредством специализированных средств не осуществляется;
- безопасность корпоративной сети предприятия обеспечивается недостаточно, что может привести к недоступности ИТ-сервисов для работы пользователей;
- требований регуляторов в области ИБ не выполняются. В частности, требования нормативных актов: Федеральный закон Российской Федерации № 152-ФЗ «О персональных данных» от 27.07.2006 г., Частично Федеральный закон Российской Федерации №187-ФЗ «О безопасности критической информационной инфраструктуры» от 26.07.2017 г.;
- меры, направленные на сохранность имеющихся активов (информации), являются неэффективными в силу того, что в документах предприятия не определено, какая информация является защищаемой.

Выявленные недостатки/идентифицированные факторы могут привести к следующим рискам:

- разглашение/утечка конфиденциальной информации в следствие несанкционированного доступа к системам со стороны внутренних работников или подрядчиков;
- принятие неверных управленческих решений в рамках бизнес-процессов в случае несанкционированного изменения информации, обрабатывающейся в бизнес-системах;

– приостановка бизнес-процессов в случае нарушения доступности бизнес систем в результате инцидента ИБ;
– получение предписаний и штрафов от контролирующих органов.

Выводы по разделу

По результатам анализа следует отметить, что процессы управления ИБ не регламентированы, не прозрачны и не постоянны. Учитывая уровень социальной значимости предприятия и имеющихся активов, вопрос их совершенствования стоит весьма остро. Требуется серьёзное повышение уровня ИБ.

Соответственно в качестве дальнейшей научной деятельности следует взять вектор на разработку необходимых мер по повышению зрелости процессов управления ИБ ориентируясь на процессный подход, основанный на лучших мировых практиках, где каждая управленческая функция также представляет процесс, а процесс управления ИБ в целом является общей суммой всех этих функций. Необходимо выбрать модель оценки процессов, измерить их и разработать меры по достижению целевого уровня, после чего ранжировать их внедрение, так как единоразовое внедрение всех необходимых мер невозможно в силу ресурсоёмкости данного процесса. То есть, по сути, нужно разработать план поэтапного совершенствования СМИБ предприятия, на основе полученных результатов оценки её процессов, реализация которого позволит достигнуть целевого уровня в соответствии с лучшими мировыми практиками.

Это позволит:

– обеспечить выполнение законодательных требований, тем самым сократить потенциальные риски привлечения к ответственности и штрафам;
– повысить потенциал и эффективность управления ИБ, чётко распределить зоны ответственности;

- укрепить имидж предприятия в аспекте технологичности и заботы о безопасности информационных активов (как собственных, так и контрагентов);
- снизить риски финансовых и репутационных потерь;
- обеспечить положительное влияние на достижение стратегических целей;
- обеспечить перспективу для сертификации по стандартам информационной безопасности;
- повысить привлекательность для клиентов с точки зрения надежности как партнера;
- Занять более авторитетную позицию на рынке по влиянию на отрасль в целом, касаемо приемлемости мер информационной безопасности.

3 Практический раздел

3.1 Идентификация показателей эффективности информационной безопасности на основе целей предприятия

Основные бизнес-процессы предприятия в высокой степени зависят от систем, средств и сервисов ИТ, а также от циркулирующей в них информации. «Потеря доступности, целостности и конфиденциальности данных может привести к дезорганизации или снижению деловой активности предприятия, нанесению ему финансового ущерба, возникновению неблагоприятной репутации, причинению ущерба здоровью персонала и появлению других критичных рисков» [1], что в свою очередь влияет на достижение поставленных стратегических целей предприятия.

Стратегическими целями называют - цели компании на три года и более, они могут измеряться в выручке, прибыли или доле рынка (рыночной позиции). Эти цели, как и ценности, всегда являются отражением ожиданий менеджмента от бизнеса в целом, при этом фокус может меняться на разных этапах развития компании.

Типовыми стратегическими целями предприятий, включая АО «Вологдаоблэнерго» являются цели, продемонстрированные на рисунке 15.

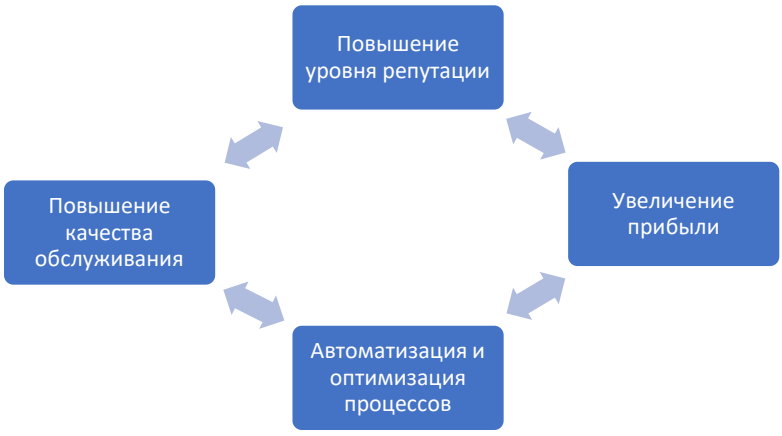


Рисунок 15 – Связь стратегических целей АО «Вологдаоблэнерго»

Для достижения поставленных стратегических целей в АО «Вологдаоблэнерго» имеются процессные модели:

– процессы верхнего уровня,

– поддерживающие процессы.

Процессы верхнего уровня продемонстрированы на рисунке 16.

Рисунок 16 – Модель процессов верхнего уровня

Основной целью процесса «Управление реализацией услуг по транспорту э/э и мощности» – является распределение и снабжение электрической энергией потребителей в рамках договорных условий.

Основной целью процесса «Эксплуатация производственного актива» – является обеспечение надежной подачи потребителям требуемого количества качественной электроэнергии при наименьших удельных затратах материальных, трудовых и денежных ресурсов.

В дополнении к основным процессам в АО «Вологдаоблэнерго» имеются поддерживающие, обеспечивающие поддержку выполнения

основных стратегических задач. Модель поддерживающих процессов представлена на рисунке 17.

Рисунок 17 – Модель поддерживающих процессов

В качестве поддерживающего процесса выступает и управление ИТ, в нашем случае совместно с ИБ. Учитывая рост автоматизации процессов роль ИБ в них крайне важна. Оценить вклад ИБ в достижение развития бизнеса помогут правильно сформированные показатели её эффективности.

Показатели эффективности следует использовать для описания влияния реализации управления СМИБ на цели ИБ организации, которые достигаются путём реализации основных бизнес-процессов. Эти показатели нужно использовать для определения того, работают ли процессы СМИБ и меры обеспечения ИБ так, как задумано, и достигают ли они желаемых результатов.

Рост показателей эффективности достигается путём сбора информации о процессах ИБ, её анализа и сопоставлению качественным или количественным показателям, которые отражает ту или иную характеристику (метрики).

Формированию метрик способствуют следующие факторы:

– влияние на ключевые бизнес-процессы предприятия,

– влияние на качество оказываемых услуг,

– влияние на прибыль,

– влияние на цели предприятия.

Пример показателей эффективности СМИБ АО «Вологдаоблэнерго» и метрики для измерения показателей, приведены в таблице 9.

Таблица 9 – Показатели эффективности СМИБ и их метрики

Показатели эффективности	Метрики
Отсутствие потерь защищаемых активов	1. Количество утраченной защищаемой информации 2. Количество штрафов и предписаний в части ИБ от регулирующих органов 3. Количество инцидентов успешного несанкционированного воздействия на защищаемые ресурсы со стороны злоумышленника
Положительное влияние на стратегические цели	1. Уровень интеграции в ключевые бизнес-процессы 2. Уровень зависимости результатов деятельности бизнеса от информационной безопасности 3. Уровень защищенности автоматизированных систем управления
Положительные заключения независимых аудитов и тестирования на проникновение	1. Количество проведенных проверок 2. Количество полученных рекомендаций и замечаний
Финансовая оправданность	1. Размер затрат на информационную безопасность 2. Финансовый эквивалент стоимости защищаемой информации
Надёжная работа информационных сервисов	1. Количество аварий и отказов в обслуживании 2. Удовлетворенность пользователей

В целом для различных организаций показатели эффективности могут дополнятся или иметь другой вид с учётом специфичности деятельности и направленности организации.

3.2 Моделирование процесса оценки состоятельности

Моделирование позволит наглядно продемонстрировать основную концепцию проведения оценки СМИБ и её участников. Данный процесс является декомпозицией более масштабного процесса развития СМИБ в целом (приложение А). Для более информативного представления процесса оценки зрелости СМИБ предприятия была разработана диаграмма вариантов использования (рисунок 18).

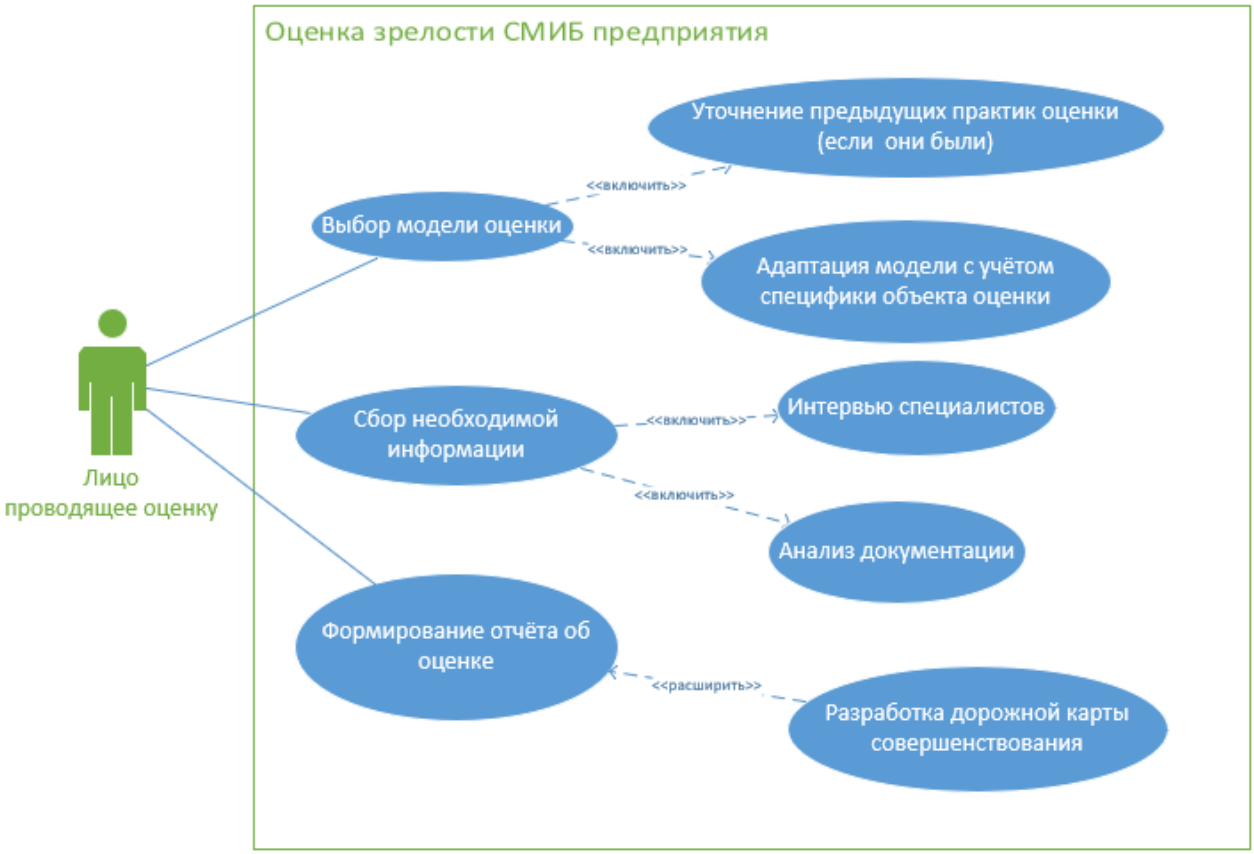


Рисунок 18 - Диаграмма вариантов использования процесса оценки зрелости процессов СМИБ предприятия

На данной диаграмме имеется один актор – «Лицо проводящее оценку», т.к. в качестве ЛПО может выступать как руководитель направления ИБ-ИТ предприятия, так и его специалисты, также в роли ЛПО могут быть независимые эксперты сторонних организаций, к примеру

сертифицированные аудиторы или эксперты компаний интеграторов ИТ-ИБ решений. Но при этом концепция вариантов использования не изменится, поэтому добавление других акторов будет избыточным, потому что между ними всё равно будет организованна связь обобщения к лицу, проводящему оценку, без наличия индивидуальных вариантов использования.

Также следует заметить, что диаграмма выполнена с учётом принципа читабельности и информативности, которые достигаются путём лаконичности изложения. Поэтому на диаграмме не отображен перечень документов к варианту «Анализ документации» или количество и должность специалистов к варианту «Интервью специалистов».

Примерный список документации для анализа СМИБ будет следующим:

- технические задания на создание систем обеспечения безопасности (КИИ, ИСПДн),
- технические задания на внедрение технических средств ИБ (межсетевые экраны, системы управления неструктурированными данными, DLP системы, антивирусные комплексы, защита электронной почты и т.д.),
- регламенты описывающие процессы ИБ,
- инструкции пользователям и администраторам,
- должностные инструкции,
- политики и положения,
- приказы и распоряжения.

Примерный список специалистов, с которыми необходимо провести интервью, будет следующим:

- руководители ИТ-ИБ,
- специалисты ИТ-ИБ,
- администраторы ИТ-ИБ,

– специалисты, отвечающие за функционирование КИИ (администраторы КИИ, руководители SCADA, инженеры АСУТП),
– специалисты, эксплуатирующие КИИ (диспетчеры, техники, инженеры и т.п.).

В случае проведения независимой оценки третьими лицами, высока вероятность того что проводимые работы по оценке будут требовать значительных финансовых вложений от заказчика, поэтому разработка дорожной карты развития имеет связь «расширить» и доступна как опция к результатам оценки текущего уровня и будет из себя представлять поэтапный план совершенствования СМИБ до целевого уровня.

Источниками информации, в рамках проведения оценки, являлись:

– результаты интервью со специалистами ИТ и ИБ предприятия,
– документация, регламентирующая процессы,
– результаты наблюдения за выполнением отдельных процессов,
– результаты анализа конфигураций,
– результаты опроса пользователей,
– свидетельства выполнения процессов (заявки, акты, переписка в электронной почте и т.д.).

3.3 Проведение оценки состоятельности и расчётов

При проведении оценки СМИБ применялся метод комбинированной оценки, где количественные показатели будут демонстрировать общий уровень выполнения мер по ИБ, а качественные показатели демонстрировать состоятельность их реализации.

Перечень мер ИБ, подлежащих оценке, взят из ГОСТ Р ИСО/МЭК 27001-2021 «Системы менеджмента информационной безопасности. Требования». Данный документ полностью идентичен международному стандарту ISO/IEC 27001:2013 «Information technology — Security techniques — Information security management systems — Requirements», IDT) и является

частью серии стандартов ISO/IEC 27000, которая широко используется специалистами по ИБ как в России, так и за рубежом.

Серия ISO/IEC 27000 представляет собой модель для налаживания и функционирования СМИБ, включающую в себя лучшие мировые практики, по которым эксперты достигли согласия на основании международного опыта, накопленного в этой области. При использовании семейства данных стандартов организации могут реализовывать и совершенствовать систему управления защитой информации и подготовиться к независимой сертификации их СМИБ, успешное прохождение которой окажет положительное влияние на репутацию организации в плане её надежности и технологичности.

Проведению оценки должен предшествовать процесс выбора и адаптации модели оценки под отраслевую специфику – в нашем случае ТЭК, поэтому необходимо добавить дополнительные требования по защите АСУ ТП и КИИ. Как вариант дополнительные требования можно взять из ГОСТ Р ИСО/МЭК 27019-2021 «Меры обеспечения информационной безопасности в энергетике (неатомной)».

Иерархия мер, описанных в выбранном нами стандарте, представляет собой строго подчиненную структуру, состоящую из четырнадцати «доменов» на самом верхнем уровне и самих «мер» на самом нижнем уровне. Иерархия домена продемонстрирована на рисунке 19.

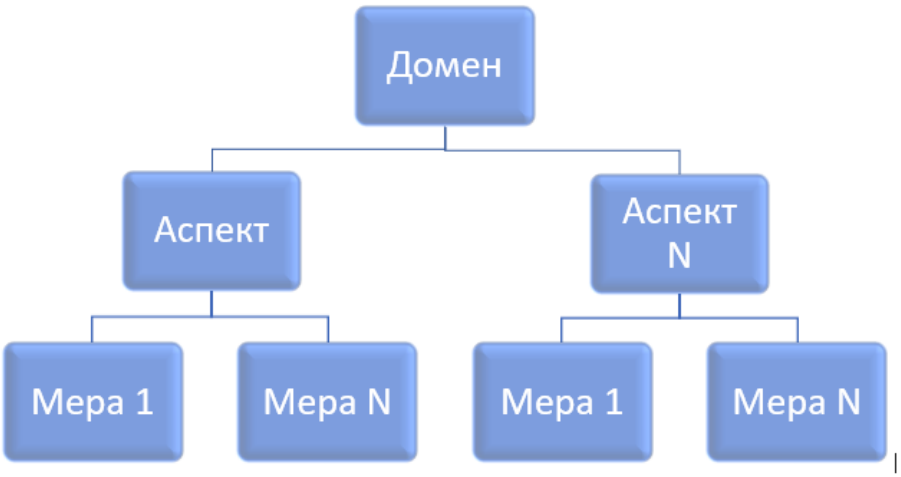


Рисунок 19 – Иерархия домена

Перечень доменов и их аспектов, подлежащие оценке, продемонстрированы в таблице 10.

Таблица 10 – Домены и аспекты, подлежащие оценке

Домен	Аспект
Политики информационной безопасности	5.1 Руководящие указания в части информационной безопасности
Организация деятельности по информационной безопасности	6.1 Внутренняя организация деятельности по ИБ
	6.2 Мобильные устройства и дистанционная работа
Безопасность, связанная с персоналом	7.1 При приёме на работу
	7.2 Во время работы
	7.3 Увольнение и смена места работы
Менеджмент активов	8.1 Ответственность за активы
	8.2 Категорирование информации
	8.3 Обращение с носителями информации
Управление доступом	9.1 Требования бизнеса по управлению доступом
	9.2 Процесс управления доступом пользователей
	9.3 Ответственность пользователей
	9.4 Управление доступом к системам и приложениям
Криптография	10.1 Криптографическая защита информации

Продолжение таблицы 10

Физическая безопасность и защита от воздействия окружающей среды	11.1 Зоны безопасности
	11.2 Оборудование
Безопасность при эксплуатации	12.1 Эксплуатационные процедуры и обязанности
	12.2 Защита от вредоносных программ
	12.3 Резервное копирование
	12.4 Регистрация и мониторинг
	12.5 Контроль программного обеспечения, находящегося в эксплуатации
	12.6 Менеджмент технических уязвимостей
	12.7 Особенности аудита информационных систем
Безопасность системы связи	13.1 Менеджмент безопасности сетей
	13.2 Передача информации
Приобретение, разработка и поддержка систем	14.1 Требования к безопасности информационных систем
	14.2 Безопасность в процессах разработки и поддержки
	14.3 Тестовые данные
Взаимоотношения с поставщиками	15.1 Информационная безопасность во взаимоотношениях с поставщиками
	15.2 Управление услугами, предоставляемыми поставщиком
Менеджмент инцидентов информационной безопасности	16.1 Менеджмент инцидентов информационной безопасности и улучшений
Аспекты информационной безопасности в рамках менеджмента непрерывности деятельности организации	17.1 Непрерывность информационной безопасности
	17.2 Резервирование оборудования
Соответствие	18.1 Соответствие правовым и договорным требованиям
	18.2 Проверки информационной безопасности

Наименования и описание самих мер в таблице 2 не продемонстрированы в силу нецелесообразности, из-за большого объёма информации.

Получение количественной оценки домена будет формироваться из среднего значения суммы коэффициентов выполнения его мер с

последующим преобразованием в процентный эквивалент, где 100% максимальное и 0% минимальное значение соответственно. Система количественной оценки продемонстрирована в таблице 11.

Таблица 11 – Система количественной оценки

Статус выполнения меры	Вес коэффициента
Не выполняется	0
Выполняется частично	0.5
Выполняется	1

При необходимости получить только количественные показатели можно воспользоваться следующей формулой:

$$K_d = \left(\frac{\sum_{i=0}^{n} x_i}{n}\right) \times 100, \#(1)$$

где, d – порядковый номер домена

i – порядковый номер меры домена

x – вес коэффициента количественной оценки

n – количество мер домена

Критерии качества для проведения оценки описаны в так называемой модели «зрелости» CMMI. Данная модель имеет пять уровней зрелости и представляет собой бизнес-инструмент для измерения состоятельности процесса (в нашем случае домена) на основе определенного набора критериев. Использование модели зрелости как инструмента удобно тем, что промежуточные и итоговые результаты развития ИБ могут быть легко измерены и сравнены с определенным целевым уровнем. Основными достоинствами модели CMMI являются ее простота и универсальность, в отличие от остальных моделей, имеющих либо более абстрактные критерии

оценки, либо больше подходящие под оценку ИТ менеджмента и разработки, или направленные на оценку конкретных технологий (SOC, IdM и др.) [29].

Дополнительным достоинством CMMI является соответствие целей её разработки целям большинства организаций, которые заключаются в следующем:

- производите качественные продукты или услуги – «концепция улучшения процесса в моделях CMMI развилась из парадигмы качества Деминга, Джурана и Кросби: качественные продукты являются результатом качественных процессов. CMMI уделяет большое внимание деятельности, связанной с качеством, включая управление требованиями, обеспечение качества, верификацию и валидацию» [47].
- создание ценности для акционеров – «зрелые организации с большей вероятностью составят более точные оценки затрат и доходов, чем организации с меньшей зрелостью, а затем будут работать в соответствии с этими оценками. CMMI поддерживает качественные продукты, предсказуемые графики и эффективные измерения, чтобы помочь руководству составлять точные и обоснованные прогнозы. Такая зрелость процесса может защитить от проблем с производительностью проекта, которые могут снизить ценность организации в глазах инвесторов» [47].
- повышение удовлетворенности клиентов – «достижение целевых показателей по затратам и графику с помощью высококачественных продуктов, которые проверены на соответствие потребностям клиентов, является хорошей формулой удовлетворенности клиентов. CMMI учитывает все эти компоненты, уделяя особое внимание планированию, мониторингу и измерениям, а также улучшенной предсказуемости, обеспечиваемой более эффективными процессами» [47].

– увеличить долю рынка – «доля рынка зависит от многих факторов, включая качество продуктов и услуг, идентификацию названия, цены и имидж. Заказчикам нравится иметь дело с поставщиками, которые имеют репутацию тех, кто выполняет свои обязательства» [47].
– получить признание в отрасли за выдающиеся достижения – «лучший способ создать репутацию выдающегося специалиста — это постоянно хорошо выполнять проекты, предоставляя качественные продукты и услуги в рамках параметров затрат и графика. Наличие процессов, соответствующих требованиям CMMI, может улучшить эту репутацию» [47].

Система качественной оценки домена по модели CMMI продемонстрирована в таблице 12.

Таблица 12 – Система качественной оценки домена по модели CMMI

Уровень зрелости	Критерии	Вес коэффициента
Отсутствует (Non-existent)	Полное отсутствие каких-либо доказательств существования процесса	0
Начальный (Initial)	Предприятие понимает наличие проблем и необходимость их решения. Какой-либо организованный подход к управлению отсутствует. Процесс ИБ выполняется на нерегулярной основе.	0.2
Повторяемый (Repeatable)	Отсутствует доступ к стандартным процедурам и формальное обучение, ответственность за выполнение задачи лежит на конкретном человеке. В результате степень доверия к профессиональным качествам конкретного человека высока и соответственно велико влияние человеческого фактора.	0.4
Определенный (Defined)	Процедуры, связанные с процессом, документированы или документированы частично, планируются и доведены до сведения работников. Решение о выполнении или невыполнении конкретной процедуры работник может принять самостоятельно, и при этом есть небольшая вероятность того, что невыполнение требований процедуры будет обнаружено. Сами процедуры несложные и являются лишь описанием практически выполняемых действий.	0.6

Продолжение таблицы 12

Управляемый (Controlled)	Имеется возможность осуществлять мониторинг и измерение соответствия фактической реализации процесса разработанным процедурам и принимать те или иные действия в случае несоответствия. Автоматизированные средства используются ограниченно или фрагментарно. Процесс ИБ не только управляется, но и контролируется.	0.8
Оптимизированный (Optimized)	Процесс отработан до уровня лучших практик путем постоянного длительного совершенствования и сравнения с показателями других предприятий. Широко используется автоматизация рабочих процессов. Процесс ИБ измеряется и постоянно совершенствуется.	1

Применение коэффициента качества следует применять к домену в целом с учётом выполняемости его мер, это позволит оценивать именно домен как процесс, а не качество конкретных мер по отдельности. По сути, один из показателей (качества или количества), при вычислении комбинированного показателя, будет являться корректирующим, что позволит получить более объективные результаты оценки.

Формула вычислений комбинированного показателя, с применением количественных и качественных коэффициентов, имеет следующий вид:

$$K_d = \frac{1}{2}\left(\left(\frac{1}{n}\sum_{i=1}^{n} x_i\right) + y_k\right) \times 100, \#(2)$$

где, d – порядковый номер домена

i – порядковый номер меры домена

x – вес коэффициента количественной оценки

y – вес коэффициента качественной оценки

n – количество мер домена

Для перевода комбинированной оценки в эквивалент уровня «зрелости», с учётом шага коэффициента, была разработана система соответствия комбинированной оценки уровням CMMI (таблица 13):

Таблица 13 – Система соответствия комбинированной оценки уровням CMMI

Уровень зрелости CMMI	Диапазон значений комбинированной оценки в процентах
Отсутствует (Non-existent)	0
Начальный (Initial)	1 - 25
Повторяемый (Repeatable)	26 - 50
Определенный (Defined)	51 - 75
Управляемый (Controlled)	76 - 99
Оптимизированный (Optimized)	100

Стоит заметить, что важной задачей является повышение уровня зрелости процессов ИБ до уровня зрелости не ниже четвертого (Controlled). Уровень зрелости процессов ИБ не ниже четвертого является целевым исходя из соображений принципиальной достижимости и так как СМИБ является частью общего процесса управления и зависит от уровня зрелости управления процессов предприятия в целом.

Выбор коэффициентов, проводился с учётом сведений, полученных в результате сбора информации предшествующих проведению вычислений, а также с учётом экспертного мнения лица, проводившего оценку.

Для наглядного примера проведенных расчётов предлагается использовать первый домен в иерархии (рисунок 20).

A.5 Политики информационной безопасности		
A.5.1 Руководящие указания в части информационной безопасности Цель: обеспечить управление и поддержку высшим руководством информационной безопасности в соответствии с требованиями бизнеса, соответствующих законов и нормативных актов		
A.5.1.1	Политики информационной безопасности	*Мера обеспечения информационной безопасности* Совокупность политик информационной безопасности должна быть определена, утверждена руководством, опубликована и доведена до сведения всех работников организации и соответствующих внешних сторон
A.5.1.2	Пересмотр политик информационной безопасности	*Мера обеспечения информационной безопасности* Политики информационной безопасности должны пересматриваться через запланированные интервалы времени или в случае происходящих существенных изменений для обеспечения уверенности в сохранении их приемлемости, адекватности и результативности

Рисунок 20 – Первый домен - «Политики информационной безопасности»

Данный домен имеет один аспект и две меры. Используя информацию, полученную в ходе предварительного обследования, проводим соответствующие расчёты:

$$\frac{1}{2}\left(\frac{0.5+0.5}{2}+0.4\right)\times 100 = 45, \#(3)$$

В соответствии с таблицей 5, полученное значение домена «Политики информационной безопасности» соответствует уровню зрелости «Начальный». Данный уровень характеризуется как низкий, потенциал его совершенствования довольно высок.

После проведения всех необходимых расчётов по каждому из доменов, мы получили результаты, продемонстрированные в таблице 14.

Таблица 14 – Результаты качественной оценки СМИБ

Домен	Уровень зрелости
Политики информационной безопасности	Повторяемый
Организация деятельности по информационной безопасности	Начальный
Безопасность, связанная с персоналом	Повторяемый
Менеджмент активов	Начальный
Управление доступом	Повторяемый
Криптография	Повторяемый

Продолжение таблицы 14

Физическая безопасность и защита от воздействия окружающей среды	Повторяемый
Безопасность при эксплуатации	Начальный
Безопасность системы связи	Начальный
Приобретение, разработка и поддержка систем	Начальный
Взаимоотношения с поставщиками	Начальный
Менеджмент инцидентов информационной безопасности	Повторяемый
Аспекты информационной безопасности в рамках менеджмента непрерывности деятельности организации	Начальный
Соответствие	Отсутствует

По результатам оценки, процессы СМИБ АО «Вологдаоблэнерго», находятся в диапазоне от 0 до 2. Визуальное представление итогов оценки отображено на рисунке 21.

Рисунок 21 – Итоги оценки СМИБ АО «Вологдаоблэнерго»

Если говорить о среднем значении по всем доменам, т.е. о СМИБ в целом, то в нашем случае сумма всех полученных значений (по цифре уровня) равна девятнадцати, что является 26% от максимально-возможной оценки равной семидесяти, что соответствует повторяемому (низкому) уровню СМИБ.

3.4 Формирование показателей целевого уровня на основе полученных данных

Целевой уровень СМИБ определяется рядом факторов, ключевыми из которых являются:

- цели и требования бизнеса;
- тенденции и планы развития IT-инфраструктуры;
- требования нормативно-правовых актов, нормативно методических документов, руководящих документов РФ в области защиты информации.

Целевой уровень СМИБ предполагает создание единого пространства процессов ИБ и повышение их зрелости. Необходимо, чтобы процессы ИБ выполнялись слаженно, без сбоев и критически не зависели от отдельного человека. Важно, чтобы специалисты по ИБ и IT использовали максимально стандартизированные и унифицированные подходы и методы в рамках своей операционной деятельности. Во-первых, это позволит оптимизировать трудозатраты работников, во-вторых, позволит создать фундамент прозрачной и бесперебойной деятельности по ИБ, устойчивой к увольнениям отдельных работников.

Под целевым уровнем СМИБ понимается четвертый уровень зрелости в соответствии с Capability Maturity Model Integration [45]. Данный уровень является целевым исходя из следующих соображений:

- он соответствует выполнению требований ISO/IEC 27001:2013 «Information technology. Security techniques. Information security

managements systems. Requirements» (одной из признанных лучших практик по управлению по ИБ);

- формулировка целевого уровня подобным образом принципиально достижима;
- формулировка целевого уровня подобным образом удобна тем, что промежуточные и итоговые результаты дорожной карты можно измерить (путем оценки зрелости процессов ИБ) и сравнить с целевым уровнем.

Также необходимо создать защищенную от внешних и внутренних злоумышленников корпоративную сеть передачи данных, включая не только сегменты, в которых размещены корпоративные IT-сервисы. Эта задача также включает в себя безопасную настройку элементов IT-инфраструктуры, устранение программно-технических уязвимостей, строгую сегментацию сетей, внедрение дополнительных средств защиты информации и прочие мероприятия технического характера.

Комплексная модель обеспечения ИБ предполагает наличие унифицированных подходов с заранее определенным, ожидаемым уровнем выполнения и прогнозируемым результатом. Переход на данную модель позволит специалистам разных подразделений «говорить на одном языке» и слаженно выполнять общую задачу. Другим позитивным эффектом является повышение доверия к ИБ: результат функционирования процессов ИБ становится понятным и предсказуемым для потребителей ИБ-сервисов (IT-службы, высшее руководство, бизнес-подразделения и т.д.). Основой для реализации модели является разработка карты процессов, масштабирование реализованных подсистем ИБ, и привлечение внешних специалистов ИБ к реализации отдельных функций ИБ (в случае если данная функция не может быть выполнена собственными силами).

К моменту завершения реализации мероприятий должны быть достигнуты качественные показатели эффективности функционирования процессов ИБ, при которых:

– процессы ИБ применяются на постоянной основе в соответствии с подходами, описанными и закрепленными на предприятии;
– обеспечено необходимое кадровое обеспечение ИБ;
– технологическое обеспечение ИБ, направленное на автоматизацию процессов ИБ и контроля состояния безопасности, используется надлежащим образом, предоставляя возможность отслеживать показатели эффективности;
– проводится постоянная оценка эффективности процессов и персонала ИБ.

3.5 Разработка перечня проектов и их ранжирование

Управление ИБ, как и любой другой процесс, для своего полноценного функционирования, требует достаточных ресурсов: трудовых, временных, финансовых и т.д. К сожалению, для большинства предприятий (АО «Вологдаоблэнерго» в том числе), периодическая или постоянная нехватка таких ресурсов больше является закономерностью чем исключением. Поэтому анализ угроз ИБ и разработка мер по их противодействию являются лишь одними из первых этапов на пути построения эффективной СМИБ, следующим этапом является определение первоочерёдности их реализации, этот процесс называется ранжированием проектов.

На первый взгляд можно предположить, что термин ранжирование аналогичен термину – сортировка, но это не совсем так. Сортировка представляет собой процедуру перестановки элементов массива или перечня в определенном порядке по заданному условию, в то время как ранжирование - процесс упорядочивания объектов с учетом определенных критериев.

Особую актуальность ранжирование может иметь при достаточно объёмном перечне проектов, который может быть сформирован, по итогам проведенного аудита ИБ или оценки состоятельности СМИБ предприятия с

использованием моделей зрелости процессов [41]. Тогда количество проектов необходимых для достижения целевого уровня состоятельности СМИБ предприятия может составлять несколько десятков.

Следует заметить что ранжирование проектов используется в случае, когда проекты не являются альтернативными, то есть, возможно принятие всех или нескольких проектов, но предприятие не может реализовать их одновременно, поэтому очередной проект может быть реализован по мере появления такой возможности без радикального исключения его из списка [34].

В целом ранжирование проектов можно описать как процесс, выражаемый в виде последовательности, продемонстрированной на рисунке 22.

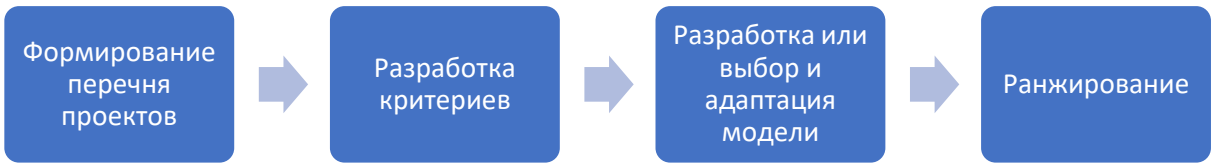


Рисунок 22 – Процесс ранжирования проектов

Так как универсальных инструментов (моделей) для ранжирования проектов, пригодных для использования во всех конкретных ситуациях, не существует, соответствующие критерии ранжирования, как и сама модель, разрабатывается или адаптируется для каждого случая в зависимости от специфики предметной области и поставленных задач.

При проведении ранжирования, важно уделить внимание именно разработке критериев, от их адекватности зависит успешность проводимой оценки. Следовательно, ключ к успешному применению моделей ранжирования состоит в составлении надлежащего списка критериев оценки,

который будет отражать цели реализации проектов к интересам предприятия [23].

Вторым фактором при разработке критериев является их количество. При большом количестве критериев, модель становится громоздкой, а время необходимое для проведения расчётов, с каждым добавленным критерием, растёт по экспоненте. Вырастет и сложность адаптации модели при необходимости её использования в похожих областях. Также недостатком будет являться логическая пересекаемость тех или иных критериев, тем самым результаты некоторых критериев могут противоречить друг другу.

Для проведения ранжирования сформируем перечень проектов (таблица 15).

Таблица 15 – Список проектов

Программа	Проекты
Процессы управления ИБ	ПУ1. Разработка каталога процессов ИБ
	ПУ2. Разработка документации, регламентирующей основные процессы ИБ
Кадровое обеспечение ИБ	КО1. Расширение штата ИБ
	КО2. Закрепление зон ответственности, разработка должностных инструкций
Осведомленность персонала	ПО1. Разработка обучающих материалов по вопросам ИБ
	ПО2. Повышение квалификации ИБ специалистов
Управление IT-активами	УА1. Инвентаризация, классификация и маркировка информационных активов
Соответствие внешним требованиям	СТ1. Обследование и категорирование объектов КИИ
	СТ2. Организация и обеспечение безопасности обработки ПДн
Безопасность сети	БС1. Проектирование модернизации сетевой инфраструктуры и системы межсетевого экранирования
	БС2. Модернизация сетевого оборудования
	БС3. Внедрение системы межсетевого экранирования

Продолжение таблицы 15

Безопасность инфраструктуры удаленного доступа	БИУД1. Проектирование подсистемы защиты удаленного доступа
	БИУД2. Внедрение подсистемы защиты удаленного доступа
Безопасность электронной почты	БЭП1. Проектирование системы защиты электронной почты
	БЭП2. Внедрение подсистемы защиты электронной почты
Управление инцидентами ИБ	УИ1. Проектирование системы корреляции событий ИБ (SIEM)
	УИ2. Внедрение системы корреляции событий ИБ (SIEM)
Управление доступом к IT-сервисам	УД1. Устранение выявленных недостатков
	УД2. Разработка ролевых моделей для IT-сервисов
	УД3. Проектирование системы мульти-факторной аутентификации
	УД4. Внедрение системы мульти-факторной аутентификации
Безопасность IT-инфраструктуры	БИТ1. Устранение выявленных недостатков
	БИТ2. Обновление системного ПО на серверах и АРМ
	БИТ3. Разработка стандартов настроек безопасности элементов IT-инфраструктуры
	БИТ4. Модернизация подсистемы антивирусной защиты
	БИТ5. Проектирование подсистемы анализа защищенности IT-инфраструктуры
	БИТ6. Внедрение подсистемы анализа защищенности IT-инфраструктуры
	БИТ7. Практическое тестирование защищенности IT-инфраструктуры

После формирования перечня необходимо определить критерии. Система критериев для ранжирования проектов ИБ предприятия представлена в таблице 16.

Таблица 16 – Система критериев для ранжирования

Критерий	Качественное описание критерия	Коэффициент	Доминирующий коэффициент
Прогнозный срок реализации	свыше 12 месяцев	1	0.2
	до 12 месяцев	2	
	до 6 месяцев	3	
Ресурсоёмкость (финансы, люди)	Проект технически сложный и требует значительного количества ресурсов с полной реализацией подрядчиком	1	0.3
	Проект требует инвестиций и частичного привлечения подрядчика	2	
	Проект не требует дополнительных ресурсов, реализация достижима собственными силами	3	
Влияние	Имеется влияние на вспомогательные бизнес-процессы	1	0.5
	Имеется влияние на критичные бизнес-процессы	2	
	Имеется влияние на все бизнес-процессы	3	

Для нормирования полученных значений для проектов используются доминирующие коэффициенты a, b, c, присвоенные каждому критерию. Значения доминирующих коэффициентов назначаются экспертно и отражают важность того или иного критерия в системе общей оценки. В данном случае доминирующий коэффициент критерия влияния является самым высоким т.к. от него зависит формирование активов предприятия и достижения им стратегических целей, критичными процессами являются такие как «Передача электрической энергии потребителям», «Функционирование систем газового оборудования котельных», «Функции диспетчеризации SCADA системы». При этом сумма всех доминирующих коэффициентов равна 1.

Стоит заметить, что если имеются факторы ограничения реализации проекта имеющий более повышенный приоритет, такие как срочность исполнения (к примеру для устранения замечаний по выданному

предписанию от регулирующих органов исполнительной власти) или фактор влияния на конкретную информационную систему предприятия, то лицо принимающее решении о назначении веса доминирующего коэффициента может комбинировать их по своему усмотрению.

Таким образом для подсчета итогового балла конкретного проекта используется следующая формула:

$$P_n = Aa + Bb + Cc, \#(4)$$

где, P – показатель приоритета проекта

n – наименование проекта

A – Коэффициент критерия срочности проекта

B – Коэффициент критерия ресурсоёмкости проекта

C – Коэффициент критерия влияния проекта

a – Доминирующий коэффициент срочности проекта

b – Доминирующий коэффициент ресурсоёмкости проекта

c – Доминирующий коэффициент влияния проекта

В случае, если проект оказывает максимальное влияние при минимальной ресурсоёмкости и сроках реализации, данному проекту автоматически присваивается наивысшее значение (Высокий), в противном случае присваивается уровень приоритета (Низкий) или (Средний). Критерии отнесения итогового балла с значением приоритета отражены в таблице 17.

Таблица 17 – Качественная оценка приоритета

Диапазон значений	Приоритет проекта
$2.5 \leq P \leq 3$	Высокий
$2 \leq P \leq 2.4$	Средний
$0 \leq P \leq 1.9$	Низкий

Результаты ранжирования проектов приведены в таблице 18.

Таблица 18 – Пример результатов ранжирования

Наименование проекта	Балл	Качественная оценка приоритета	Ранг при реализации
ПУ1	2.2	Средний	9
ПУ2	2.2	Средний	9
КО1	1.7	Низкий	12
КО2	1.7	Низкий	12
ПО1	1.7	Низкий	12
ПО2	1.7	Низкий	12
УА1	2.1	Средний	10
СТ1	2.8	Высокий	3
СТ2	2.8	Высокий	3
БС1	3	Высокий	1
БС2	2.6	Высокий	5
БС3	3	Высокий	1
БИУД1	2	Средний	11
БИУД2	2	Средний	11
БЭП1	2.9	Высокий	2
БЭП2	2.9	Высокий	2
УИ1	2.2	Низкий	9
УИ2	2.2	Низкий	9
УД1	2.5	Высокий	6
УД2	2.5	Высокий	6
УД3	2.3	Средний	8
УД4	2.3	Средний	8
БИТ1	3	Высокий	1
БИТ2	3	Высокий	1
БИТ3	2.7	Высокий	4
БИТ4	2.5	Высокий	6
БИТ5	2.4	Средний	7
БИТ6	2.4	Средний	7
БИТ7	1.7	Низкий	12

В результате реализации данных проектов ожидается значительное снижение вероятности несанкционированного доступа к конфиденциальной информации, повышение уровня защищенности информационных систем от внешних и внутренних угроз, а также обеспечение непрерывного функционирования информационных ресурсов в соответствии с требованиями ИБ.

3.6 Проектирование дорожной карты на основе полученных данных

Дорожная карта (англ. roadmap) является одним из основных инструментов долгосрочного планирования [2] развития направления обеспечения ИБ, позволяющим создать комплексную систему мероприятий (как технических, так и организационных), обеспечивающих надлежащий уровень защиты информационных активов предприятия.

Дорожная карта определяет долгосрочные целевые программы и проекты по ИБ формируя стратегию развития СМИБ в целом. В среднем срок прогноза и планирования мероприятий при картировании составляет перспективу от 2 до 10 лет [30]. Основным отличием от плана-проекта, является то, что дорожная карта даёт информативный вектор развития и не содержит чёткого описания как именно должен быть реализован тот или иной проект, но включает последовательность реализации этапов с привязкой к временным ориентирам.

Целью дорожной карты, в нашем случае, является повышение уровня защищенности информационных активов и снижение операционных рисков предприятия за счет снижения рисков ИБ.

Реализация дорожной карты предполагает следующие выгоды:

- снижение рисков ИБ;
- систематизация и формализация процессов обеспечения и управления ИБ;
- повышение текущего уровня защищенности IT-сервисов и бизнес систем;
- выполнение требований внешних регуляторов в области ИБ.

Структурно дорожная карта состоит из программ, включающих в себя набор проектов, выполнение которых направлено на достижение желаемого (целевого) уровня ИБ. Каждый проект привязан к одной программе в области ИБ, однако может оказывать влияние на реализацию других программ.

Важными характеристиками дорожной карты являются динамичность и гибкость. В силу того, что функция ИБ является вспомогательной (поддерживающей), сама ИБ крайне сильно зависит от общей структуры бизнеса и IT-инфраструктуры. В таких условиях дорожная карта должна быть принципиально изменяема в случае влияния внешних, по отношению к ИБ, факторов.

Декомпозиция целей ИБ в программы по ИБ, а программ по ИБ в конечные проекты позволяет достичь необходимой гибкости. В конце каждого этапа должна производиться оценка выполнения проектов, при необходимости должны быть внесены коррективы в перечень проектов последующих этапов [10]. Структура дорожной карты развития СМИБ АО «Вологдаоблэнерго» приведена на рисунке 23.

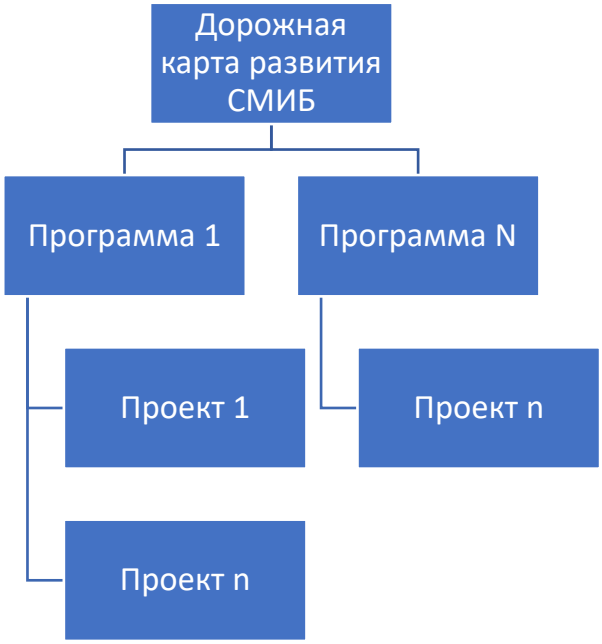


Рисунок 23 - Структура дорожной карты развития СМИБ АО «Вологдаоблэнерго»

Структура дорожной карты должна быть тесно связана с целями развития технологий на предприятии, чтобы обеспечить достижение

ожидаемых результатов. Рассмотрим типовую форму дорожной карты, представленную на рисунке 24.

Рисунок 24 – Типовая форма дорожной карты предприятия

Как видим, дорожная карта, в общем виде, имеет временные промежутки по годам и основную область, где указывают технологию, продукт или рынок, в нашем случае проекты. Возможно указание взаимосвязей между используемыми технологиями и продуктами.

Визуальное представление дорожной карты выполнялось в программе MS PowerPoint 2019, результат разработки дорожной карты представлен в приложении Б.

В заключении можно сказать, что СМИБ предприятия как правило является обеспечивающим (вспомогательным) процессом для бизнеса и не является процессом прямо формирующим его активы но при этом она может и должна вносить существенный вклад в достижение его целей [25] поэтому ранжирование проектов имеет весомое значение с точки зрения менеджмента.

3.7 Апробация результатов исследования

Для оценки эффективности реализации дорожной карты развития СМИБ предприятия проведем расчёт повышения состоятельности доменов, на которые повлияет и окажет влияние программа проектов «Соответствие внешним требованиям», при её реализации (рисунок 25). Данная программа имеет высокий приоритет по результатам ранжирования и является первоочередной.

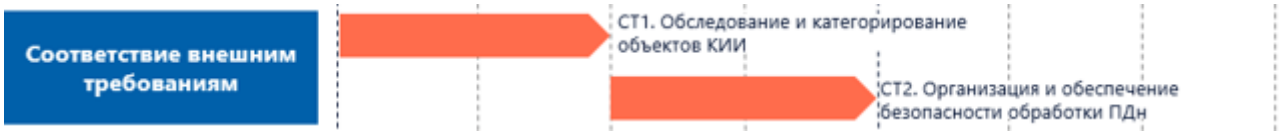


Рисунок 25 – Программа «Соответствие внешним требованиям» в дорожной карте развития СМИБ АО «Вологдаоблэнерго».

Данная программа имеет высокий приоритет по результатам ранжирования и является первоочередной.

При реализации проекта СТ1 будут выполнены такие этапы как:

а) Определение перечня объектов КИИ;

б) Моделирование угроз безопасности объектов КИИ;

в) Определение категорий значимости объектов КИИ на основании показателей критериев значимости объектов КИИ и их значений, предусмотренных перечнем показателей критериев значимости объектов КИИ Российской Федерации и их значений, утвержденным постановлением Правительства Российской Федерации от 8 февраля 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений»;

г) Присвоение каждому из объектов КИИ одной из категорий значимости либо принятие решения об отсутствии необходимости присвоения им одной из категорий значимости;

д) Подготовка проектов актов по результатам категорирования.

е) Заполнение форм категорирования для каждого объекта КИИ в соответствии с приказом ФСТЭК России № 236 от 21.12.2017 «Об утверждении формы направления сведений о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий»;

ж) Устранение полученных замечаний от ФСТЭК России после отправки результатов категорирования объектов в ФСТЭК России;

и) Разработка документации, необходимой для выполнения требований законодательства, в том числе:

1) Политика управления доступом в ОКИИ
2) Регламент управления доступом в ОКИИ
3) Положение по защите ОКИИ (включающее раздел по аудиту безопасности (внутренние проверки), планирование мероприятий по обеспечению защиты информации, обеспечению сетевой безопасности);
4) Регламент проведения внутренних проверок ИБ;
5) Регламент защиты машинных носителей информации и правил их использования;
6) Политика антивирусной защиты;
7) Политика резервного копирования;
8) Регламент управления инцидентами ИБ;
9) Регламент управления обновлениями и уязвимостями;
10) Регламент управления Изменениями в ОКИИ;
11) Политика осведомленности и обучения персонала в области ИБ;
12) Политика обеспечения действий в нештатных ситуациях.

При реализации проекта СТ2 будут выполнены такие этапы как:

а) Сбор информации об информационных системах обработки ПДн, ключевых процессах обработки ПДн (процедурах учета, хранения, передачи, уничтожения ПДн), о ключевых подразделениях, допущенных до обработки ПДн, о документах, регламентирующих технологические процессы обработки ПДн.

б) Проведение анализа текущего состояния порядка обработки ПДн, сформировать организационные и технические рекомендаций по обеспечению безопасности ПДн в системе защиты ПДн.

в) Разработка необходимой документации:

1) Политика в отношении обработки ПДн клиентов;
2) Положение об обработке ПДн клиентов;
3) Порядок работы с обращениями субъектов ПДн;
4) Порядок взаимодействия с уполномоченным органом по защите прав субъектов ПДн;
5) Типовая форма поручения оператором ПДн обработки ПДн третьим лицам;
6) Форма согласия субъекта на обработку ПДн и дополнение в договоры с клиентами о согласии на обработку ПДн;
7) Типовые формы уведомления субъектов ПДн;
8) Форма Акта об уничтожении ПДн;
9) Форма перечня должностей, допущенных к обработке ПДн;
10) Положение о порядке проведения внутренних проверок состояния защиты ПДн и т.п.

Реализация данных мероприятий позволит существенно повлиять на следующие домены:

- политики информационной безопасности,
- соответствие,
- безопасность при эксплуатации,
- безопасность, связанная с персоналом и другие.

Для наглядного примера расчётов предлагается использовать первый домен, на который будет оказано влияние (рисунок 26).

A.5 Политики информационной безопасности		
A.5.1 Руководящие указания в части информационной безопасности Цель: обеспечить управление и поддержку высшим руководством информационной безопасности в соответствии с требованиями бизнеса, соответствующих законов и нормативных актов		
A.5.1.1	Политики информационной безопасности	*Мера обеспечения информационной безопасности* Совокупность политик информационной безопасности должна быть определена, утверждена руководством, опубликована и доведена до сведения всех работников организации и соответствующих внешних сторон
A.5.1.2	Пересмотр политик информационной безопасности	*Мера обеспечения информационной безопасности* Политики информационной безопасности должны пересматриваться через запланированные интервалы времени или в случае происходящих существенных изменений для обеспечения уверенности в сохранении их приемлемости, адекватности и результативности

Рисунок 26 – Первый домен ISO 27001/2021 «Политики информационной безопасности».

Как видно из критериев полного выполнения меры, реализация выбранных проектов им отвечает в полном объёме. Поэтому в соответствии с разработанной системой количественной оценки оба аспекта имеют коэффициент 1.

Уровень качества для данного домена, с учётом стопроцентного выполнения мер и характерного соответствия управляемому уровню, по системе качественной оценки домена по модели CMMI, имеет вес коэффициента в 0.8.

Проводим расчёты с использованием формулы расчёта комбинированного показателя:

$$\frac{1}{2}\left(\frac{1+1}{2}+0.8\right)\times 100 = 90, \#(5)$$

В соответствии с системой соответствия комбинированной оценки уровням CMMI разработанной в НИР2, полученное значение домена

«Политики информационной безопасности» после реализации проектов СТ1 и СТ2 будет соответствовать уровню зрелости «Управляемый (Controlled)». Данный уровень характеризуется как целевой, по причине принципиальной достижимости.

В этом случае, по сравнению с предыдущими расчётами, повышение состоятельности домена будет составлять 100%. Положительные изменения, с учётом разработки документов и иных организационных мер, предусмотренных программой, будут касаться и остальных доменов. Прогнозные показатели доменов СМИБ АО «Вологдаоблэнерго» после реализации программы «Соответствие внешним требованиям» продемонстрированы на рисунке 27.

Рисунок 27 – Прогнозные показатели доменов СМИБ АО «Вологдаоблэнерго» после реализации программы «Соответствие внешним требованиям».

После проведения аналогичных расчётов по каждому из доменов, на которые будет оказано влияние, были получены результаты, продемонстрированные в таблице 19.

Таблица 19 – Показатели прогнозного роста состоятельности доменов

Домен	Предыдущий уровень	Прогнозируемый уровень	Рост состоятельности домена относительно текущего показателя в процентах
Политики информационной безопасности	Повторяемый	Управляемый	100
Соответствие	Отсутствует	Начальный	100
Безопасность при эксплуатации	Начальный	Повторяемый	100
Безопасность, связанная с персоналом	Повторяемый	Повторяемый	50

Таким образом по результатам эксперимента можно сделать вывод о том, что представленные методы и модели могут способствовать повышению качества планирования и реализации проектов, направленных на развитие СМИБ предприятия.

Также в качестве апробации результатов исследования, кроме представленного метода, можно считать публикации научных статей в научных журналах [41, 42].

Выводы по разделу

Таким образом, подводя итоги раздела можно выделить, с точки зрения практической значимости, следующие результаты исследования:

Высокая актуальность. Актуальность связанна с нововведениями нормативной базы в сфере ИБ в России, вопросами импортозамещения и напряженной геополитической обстановки. Соответственно спрос на ИБ в целом, требует стремительного развития этого рынка для полноценного удовлетворения требований защищенности активов заказчиков [46]. Разработанные методы и модели направлены на улучшение качества организации СМИБ, а значит позволят сократить риски ИБ и влиять на достижение целей предприятий.

Гибкость. Заключается в возможности использования результатов широкому кругу организаций и специалистов. Универсальность и относительно низкая сложность адаптации разработанных методов и моделей может вызвать заинтересованность научного сообщества и соответствующих специалистов к их применению [48].

Информативность. Полученные результаты исследований позволяют выявить слабые и сильные стороны СМИБ предприятия, и продемонстрировать их бизнесу на понятном для него языке. Соответственно наиболее эффективно планировать меры по совершенствованию процессов и повышению качества СМИБ в целом [50].

Прикладной характер. Исследования имеют практическую значимость в виде прикладного характера непосредственно для объекта исследования. Готовые результаты позволяют провести реализацию улучшения СМИБ предприятия ориентируясь на лучшие мировые практики и ведомственные требования.

Заключение

В заключении можно сделать вывод, что стратегическое планирование развития ИБ на предприятии позволяет определить долгосрочные цели и задачи, а также разработать план действий для их достижения. Поэтому формирование дорожных карт играет важную роль в процессе стратегического планирования, но требует достаточного количества времени на предварительную подготовку. Также следует заметить, что картирование требует выделения большого количества человеческих ресурсов, а именно участия: инженеров, маркетологов, экономистов, бизнес-аналитиков и других специалистов. Однако, в перспективе, разработанная дорожная карта развития будет являться эффективным инструментом на пути к развитию СМИБ.

Для развития СМИБ предприятия необходимо проводить регулярный анализ текущей ситуации, своевременно выявлять уязвимости и риски, а также определять необходимые меры для их устранения. Кроме того, необходимо своевременно и точно расставлять приоритеты, для эффективной реализации проектов в этой области.

Важным аспектом развития СМИБ является адаптация к изменяющимся условиям внешней среды, таким как изменения в законодательстве, рыночные тренды и конкурентная среда. Для этого необходимо проводить регулярный мониторинг и анализ эффективности принятых мер, а также учитывать новые технологии и методы защиты информации.

Таким образом, в рамках исследования были выполнены следующие задачи:

- проведен анализ научной литературы и источников по теме аналогичных исследований;
- проведен анализ законодательной и методической базы изучаемой предметной области;

- проведен анализ объекта исследования в рамках изучаемой предметной области;
- идентифицированы показатели эффективности СМИБ предприятия;
- проведена оценка состоятельности СМИБ и выявлен потенциал развития её процессов;
- с учетом выявленных недостатков существующей СМИБ предприятия сформирован перечень проектов, направленных на развитие системы менеджмента информационной безопасности предприятия;
- разработана дорожная карта развития СМИБ с перспективой до 2027 года;
- проведена апробация разработанных и адаптированных методов и моделей;

Гипотеза исследования подтверждена, реализация проектов разработанной дорожной карты действительно способна оказать положительное влияние на рост состоятельности процессов СМИБ в разных временных перспективах, что в свою очередь повышает эффективность её управления.

Список используемых источников

1. Бизнес-процесс «Обеспечение информационной безопасности организации» : учебное пособие / В. Ю. Дронов, Г. А. Дронова. – Новосибирск : Изд-воНГТУ, 2021. – 76 с.
2. Варзунов А. В., Торосян Е. К., Сажнева Л. П., Анализ и управление бизнес-процессами // Учебное пособие. — СПб: Университет ИТМО, 2016.
3. Веревкин Сергей Александрович, Кравчук Алексей Владимирович, Беляков Максим Игоревич МЕТОДИКА УПРАВЛЕНИЯ ИНЦИДЕНТАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОБЪЕКТАХ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ // Известия ТулГУ. Технические науки. 2022. №8. URL: https://cyberleninka.ru/article/n/metodika-upravleniya-intsidentami-informatsionnoy-bezopasnosti-na-obektah-kriticheskoy-informatsionnoy-infrastruktury
4. Голованов В. Б. Модель зрелости как подход измерения эффективности процессов информационной безопасности // НиКа. 2006. №. URL: https://cyberleninka.ru/article/n/model-zrelosti-kak-podhod-izmereniya-effektivnosti-protsessov-informatsionnoy-bezopasnosti (дата обращения: 05.03.2024).
5. Горелик Владимир Юдаевич, Безус Михаил Юрьевич О безопасности критической информационной инфраструктуры Российской Федерации // StudNet. 2020. №9. URL: https://cyberleninka.ru/article/n/o-bezopasnosti-kriticheskoy-informatsionnoy-infrastruktury-rossiyskoy-federatsii (дата обращения: 05.03.2024).
6. ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью // Интернет и право URL: https://internet-law.ru/gosts/gost/2262/

7. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности // Интернет и право URL: https://internet-law.ru/gosts/gost/54705

8. ГОСТ Р ИСО/МЭК 27003-2012 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности // Интернет и право URL: https://internet-law.ru/gosts/gost/54546/

9. Гунченко Александр Григорьевич ФОРМИРОВАНИЕ ЕДИНОГО ПОДХОДА К ПОДГОТОВКЕ СПЕЦИАЛИСТОВ В ОБЛАСТИ ПРАВОВОГО ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КРИТИЧЕСКИ ВАЖНОЙ ИНФРАСТРУКТУРЫ // Международное сотрудничество евразийских государств: политика, экономика, право. 2022. №2. URL: https://cyberleninka.ru/article/n/formirovanie-edinogo-podhoda-k-podgotovke-spetsialistov-v-oblasti-pravovogo-obespecheniya-bezopasnosti-kriticheski-vazhnoy

10. Демидов А.В. Корпоративная дорожная карта как инструмент управления организацией в период кризиса // Управление социальными изменениями в нестабильных условиях. Материалы Всероссийской научной конференции. Московский государственный университет им. М.В. Ломоносова. 24 мая 2016 г. М.: ООО «МАКС Пресс», 2016. С. 310-312.

11. Дмитриева Марьям Александровна Применение анализа зрелости информационной безопасности в системе оценки зрелости бизнес-процессов предприятия в целом // Информационная безопасность регионов. 2015. №3 (20). URL: https://cyberleninka.ru/article/n/primenenie-analiza-zrelosti-informatsionnoy-bezopasnosti-v-sisteme-otsenki-zrelosti-biznes-protsessov-predpriyatiya-v-tselom (дата обращения: 05.03.2024).

12. Дорофеев Александр Владимирович Менеджмент информационной безопасности: управление рисками // Вопросы кибербезопасности. 2014. №2 (3). URL:

https://cyberleninka.ru/article/n/menedzhment-informatsionnoy-bezopasnosti-upravlenie-riskami (дата обращения: 05.03.2024).

13. Доррер Михаил Георгиевич Модель управления совершенствованием бизнес-процессов на базе оценки уровней зрелости // ИТНОУ: информационные технологии в науке, образовании и управлении. 2018. №3 (7). URL: https://cyberleninka.ru/article/n/model-upravleniya-sovershenstvovaniem-biznes-protsessov-na-baze-otsenki-urovney-zrelosti

14. Еремия, Т. В. Анализ уровня зрелости бизнес-процессов организаций, функционирующих на медиарынке в России / Т. В. Еремия, А. О. Кузаков. — Текст : непосредственный // Молодой ученый. — 2021. — № 16 (358). — С. 211-214. — URL: https://moluch.ru/archive/358/80172/

15. Кикалов Магомед Шимилович, Саидов Абдулмуталиб Гасанович ПРОБЛЕМЫ КЛАССИФИКАЦИИ ИНФОРМАЦИИ С ОГРАНИЧЕННЫМ ДОСТУПОМ // Достижения науки и образования. 2021. №7 (79). URL: https://cyberleninka.ru/article/n/problemy-klassifikatsii-informatsii-s-ogranichennym-dostupom

16. Коломыц Оксана Николаевна, Геворкова Маргарита Сергеевна, Павлова Анна Сергеевна МЕТОДЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ПРЕДПРИЯТИЯ // Инновационная экономика: перспективы развития и совершенствования. 2020. №6 (48). URL: https://cyberleninka.ru/article/n/metody-upravleniya-informatsionnoy-bezopasnostyu-predpriyatiya (дата обращения: 05.03.2024).

17. Кондраков О.В., Лапшин В.Ю. Методология оценки риска в контексте экономической безопасности топливно-энергетического комплекса // Российское предпринимательство. – 2014. – Том 15. – № 6. URL: https:// https://1economic.ru/lib/8518.

18. Королев, В. Н. Обеспечение безопасности субъекта критической информационной инфраструктуры / В. Н. Королев. — Текст : непосредственный // Молодой ученый. — 2021. — № 20 (362). — С. 31-33. — URL: https://moluch.ru/archive/362/80964/

19. Краснов Алекс Сергеевич Методика оценки степени выполнения требований по составу организационно-распорядительных документов в области информационной безопасности // Вестник российских университетов. Математика. 2014. №6. URL: https://cyberleninka.ru/article/n/metodika-otsenki-stepeni-vypolneniya-trebovaniy-po-sostavu-organizatsionno-rasporyaditelnyh-dokumentov-v-oblasti-informatsionnoy

20. Куйчогло, С. И. Информационная безопасность. Атаки и вирусы в производстве / С. И. Куйчогло. — Текст : непосредственный // Молодой ученый. — 2019. — № 45 (283). — С. 6-9. — URL: https://moluch.ru/archive/283/63797/

21. Макеев, А. С. Менеджмент рисков информационной безопасности как непрерывный процесс / А. С. Макеев. — Текст : непосредственный // Молодой ученый. — 2016. — № 10 (114). — С. 62-66. — URL: https://moluch.ru/archive/114/29934/ (дата обращения: 05.03.2024).

22. МЕТОДИЧЕСКИЙ ДОКУМЕНТ МЕТОДИКА ОЦЕНКИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ // ФСТЭК России URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g

23. Милошевич Д. Набор инструментов для управления проектами / Драган З. Милошевич; Пер. с англ. Мамонтова Е.В.; Под ред. Неизвестного С.И. — М.: Компания АйТи; ДМК Пресс, 2008.

24. Минцифры сообщило, что практически все регионы РФ уже создали штабы по кибербезопасности // Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации URL: https://digital.gov.ru/ru/events/41613/

25. Молчанов С.В. ОСОБЕННОСТИ ВНЕДРЕНИЯ МЕТОДА ДОРОЖНОГО КАРТИРОВАНИЯ ПРИ ОСУЩЕСТВЛЕНИИ ФИНАНСОВОГО КОНТРОЛЯ НА ПРЕДПРИЯТИИ // Фундаментальные

исследования. – 2018. – № 6. – С. 166-171; URL: https://fundamental-research.ru/ru/article/view?id=42186 (дата обращения: 09.11.2023).

26. Налбандян Г.Г., Кушниренко Е.Б. Оптимизация распределения полномочий и ответственности по методике RACI // Стратегии бизнеса. 2014. №4 (6). URL: https://cyberleninka.ru/article/n/optimizatsiya-raspredeleniya-polnomochiy-i-otvetstvennosti-po-metodike-raci (дата обращения: 05.03.2024).

27. Национальный стандарт ГОСТ Р ИСО/МЭК 27000-2012 «Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология» URL: https://docs.cntd.ru/document/1200102762

28. Николаенко Валентин Сергеевич, Мирошниченко Евгений Александрович, Грицаев Руслан Талгатович Модели зрелости управления проектами: критический обзор // Государственное управление. Электронный вестник. 2019. №73. URL: https://cyberleninka.ru/article/n/modeli-zrelosti-upravleniya-proektami-kriticheskiy-obzor (дата обращения: 05.03.2024).

29. Николаенко Валентин Сергеевич, Мирошниченко Евгений Александрович, Грицаев Руслан Талгатович Модели зрелости управления проектами: критический обзор // Государственное управление. Электронный вестник. 2019. №73. URL: https://cyberleninka.ru/article/n/modeli-zrelosti-upravleniya-proektami-kriticheskiy-obzor

30. Павлов А.Ю. Дорожная карта: основные понятия и особенности построения для высокотехнологичных предприятий // Экономика: вчера, сегодня, завтра. 2016. Том 6. № 12А. С. 130-142.

31. Приказ ФСТЭК России от 25 декабря 2017 г. N 239 // ФСТЭК России URL: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239

32. Приказ ФСТЭК России от 25 декабря 2017 г. N 239 // ФСТЭК России URL: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-21-dekabrya-2017-g-n-235

33. Приказ ФСТЭК России от 25 декабря 2017 г. N 239 // ФСТЭК России URL: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21

34. Соловьева И.А., Гальтяев А.В. Разработка многокритериальной модели отбора и ранжирования проектов при формировании инвестиционной программы компании // Интернет-журнал «НАУКОВЕДЕНИЕ» Том 9, №1 (2017) http://naukovedenie.ru/PDF/44EVN117.pdf (доступ свободный).

35. Сорока Елена Георгиевна К вопросу о внедрении концепции ITIL/ITSM в Российской it- отрасли // Вестник СИБИТа. 2014. №4 (12). URL: https://cyberleninka.ru/article/n/k-voprosu-o-vnedrenii-kontseptsii-itil-itsm-v-rossiyskoy-it-otrasli

36. Сулейкин Александр Сергеевич Применение методологии ITSM в электросетевой компании ПАО «МОЭСК» для процесса управления инцидентами энергосети // Economics. 2015. №8 (9). URL: https://cyberleninka.ru/article/n/primenenie-metodologii-itsm-v-elektrosetevoy-kompanii-pao-moesk-dlya-protsessa-upravleniya-intsidentami-energoseti

37. Указ Президента РФ от 06.03.1997 N 188 (ред. от 13.07.2015) "Об утверждении Перечня сведений конфиденциального характера" // КонсультантПлюс URL: https://www.consultant.ru/document/cons_doc_LAW_13532/0179b6b5a612a4e6b17de579e3589aa0526bfe79/

38. Указ Президента РФ от 5 декабря 2016 г. N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации" // Информационно правовой портал ГАРАНТ.РУ URL: https://base.garant.ru/71556224/

39. Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ // КонсультантПлюс URL: https://www.consultant.ru/document/cons_doc_LAW_61798/

40. Федеральный закон от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // Консультант плюс URL: https://www.consultant.ru/document/cons_doc_LAW_220885/

41. Чернышев, К. С. Комбинированный метод оценки зрелости системы менеджмента информационной безопасности с применением модели CMMI / К. С. Чернышев. — Текст : непосредственный // Молодой ученый. — 2023. — № 36 (483). — С. 24-28. — URL: https://moluch.ru/archive/483/105848/

42. Чернышев, К. С. Ранжирование проектов информационной безопасности / К. С. Чернышев. — Текст : непосредственный // Молодой ученый. — 2023. — № 44 (491). — С. 30-34. — URL: https://moluch.ru/archive/491/107204

43. Что такое матрица RACI и как она помогает выполнить проект в срок, не растеряв задачи // SkillBox media URL: https://skillbox.ru/media/management/chto-takoe-matritsa-raci-i-kak-ona-pomogaet-vypolnit-proekt-v-srok-ne-rasteryav-zadachi/

44. Ashraf Khaza'Aleh Itil framework as a standard of information security // Символ науки. 2016. №3-3. URL: https://cyberleninka.ru/article/n/itil-framework-as-a-standard-of-information-security (дата обращения: 05.03.2024).

45. Building a Maturity Model for COBIT 2019 Based on CMMI // ISACA URL: https://www.isaca.org/resources/isaca-journal/issues/2021/volume-6/building-a-maturity-model-for-cobit-2019-based-on-cmmi

46. Capability Maturity Model® Integration (CMMI®) Overview // elsmar.com URL: https://elsmar.com/pdf_files/cmmi-overview05.pdf

47. CMMI - Quick Guide: [сайт]. – 2018 - URL: https://www.tutorialspoint.com/cmmi/cmmi_quick_guide.htm

48. Guide To CMMI // Business Transformation Institute URL: https://www.biztransform.net/guide-to-cmmi/

49. ITIL и ITSM: определение методологий, сравнение, преимущества и недостатки // Smart Service URL: https://mysmartservice.com/blog/itil-i-itsm

50. Kevin Scott Capability Maturity Model Integration (Cmmi) for Small Organizations. - 2010: Regis University, 92 с.

Приложение А

Концептуальная модель процесса развития системы менеджмента информационной безопасности предприятия

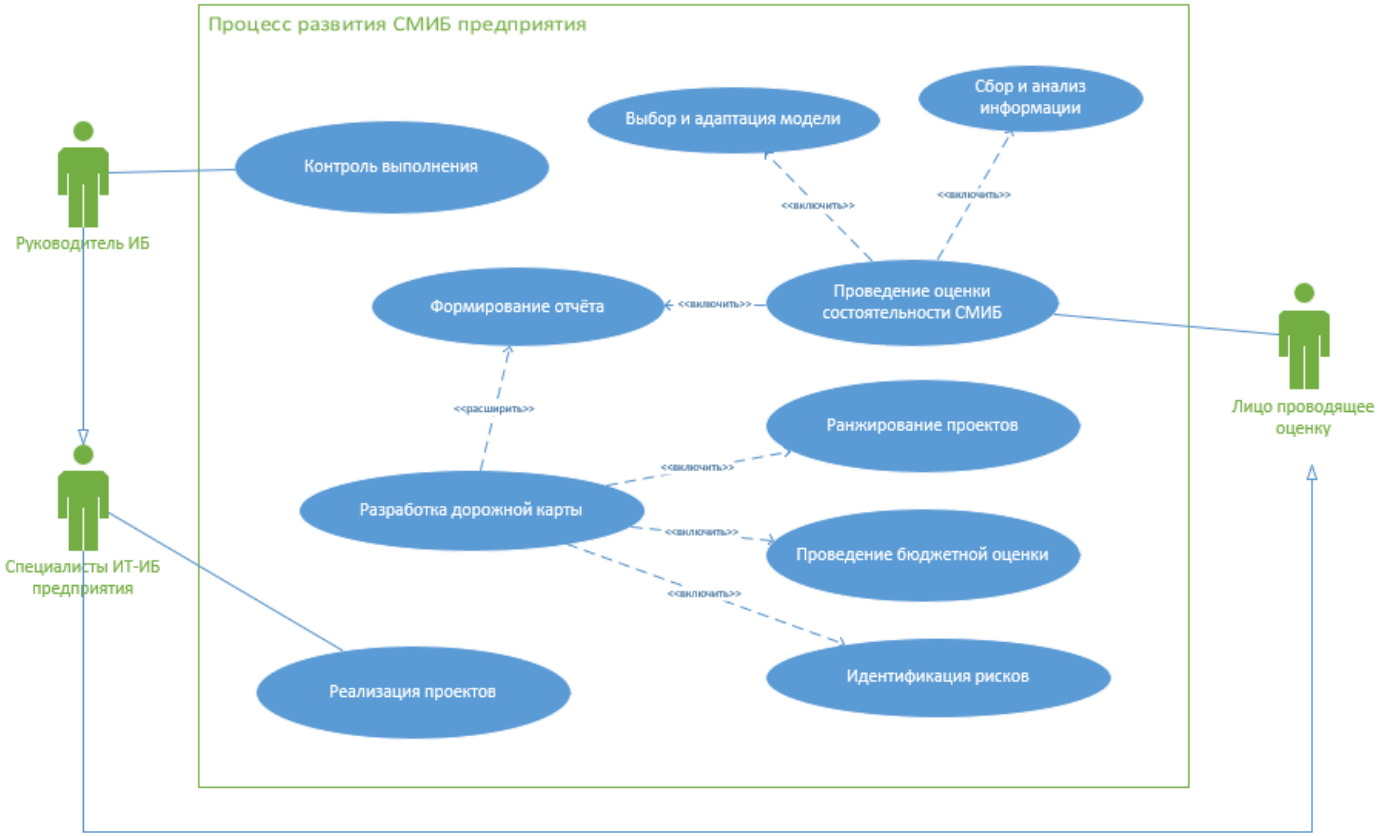


Рисунок А.1 - Диаграмма вариантов использования процесса развития СМИБ предприятия

Приложение Б

Дорожная карта развития

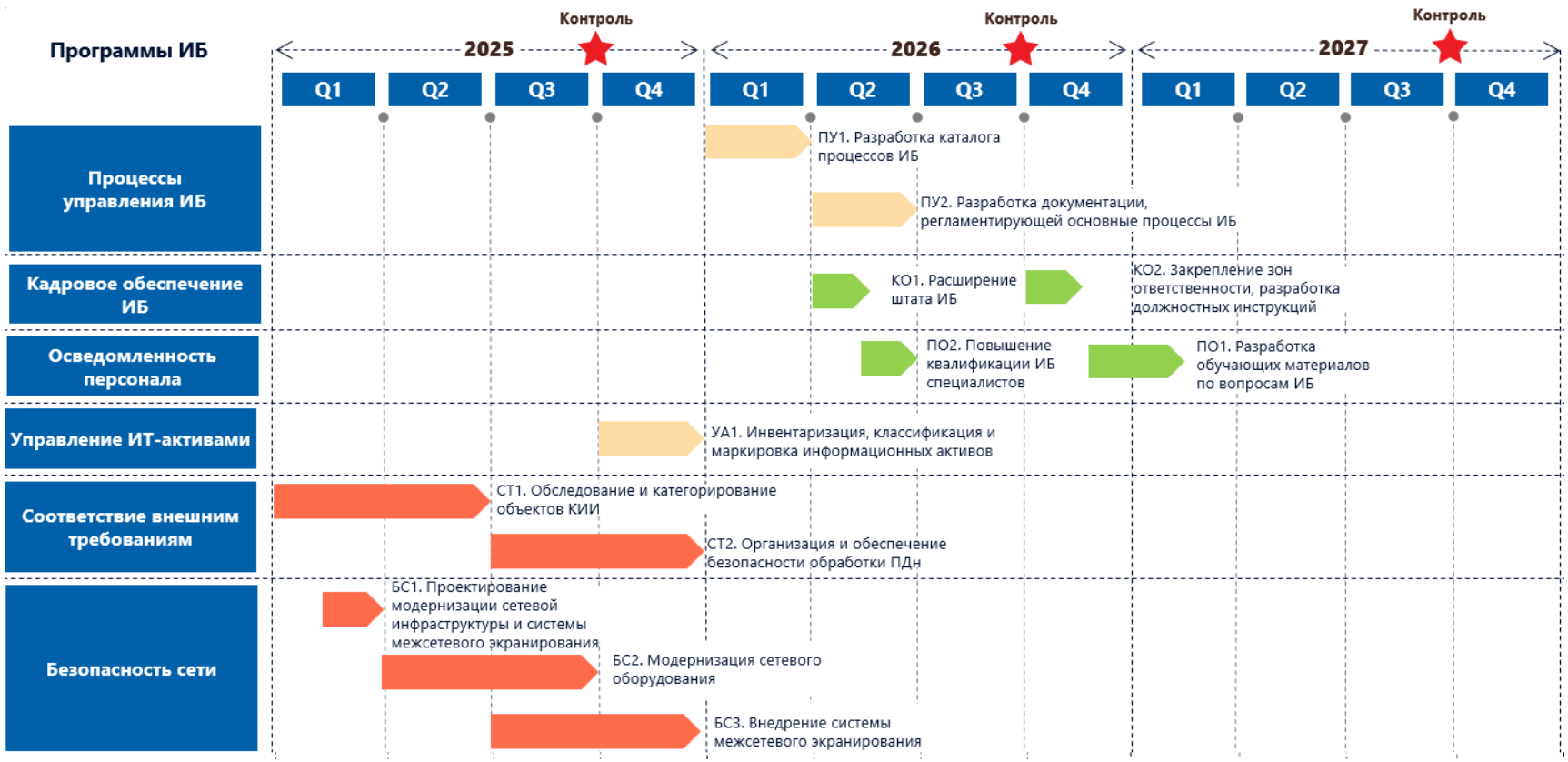


Рисунок Б.1 - Дорожная карта развития (первая часть)

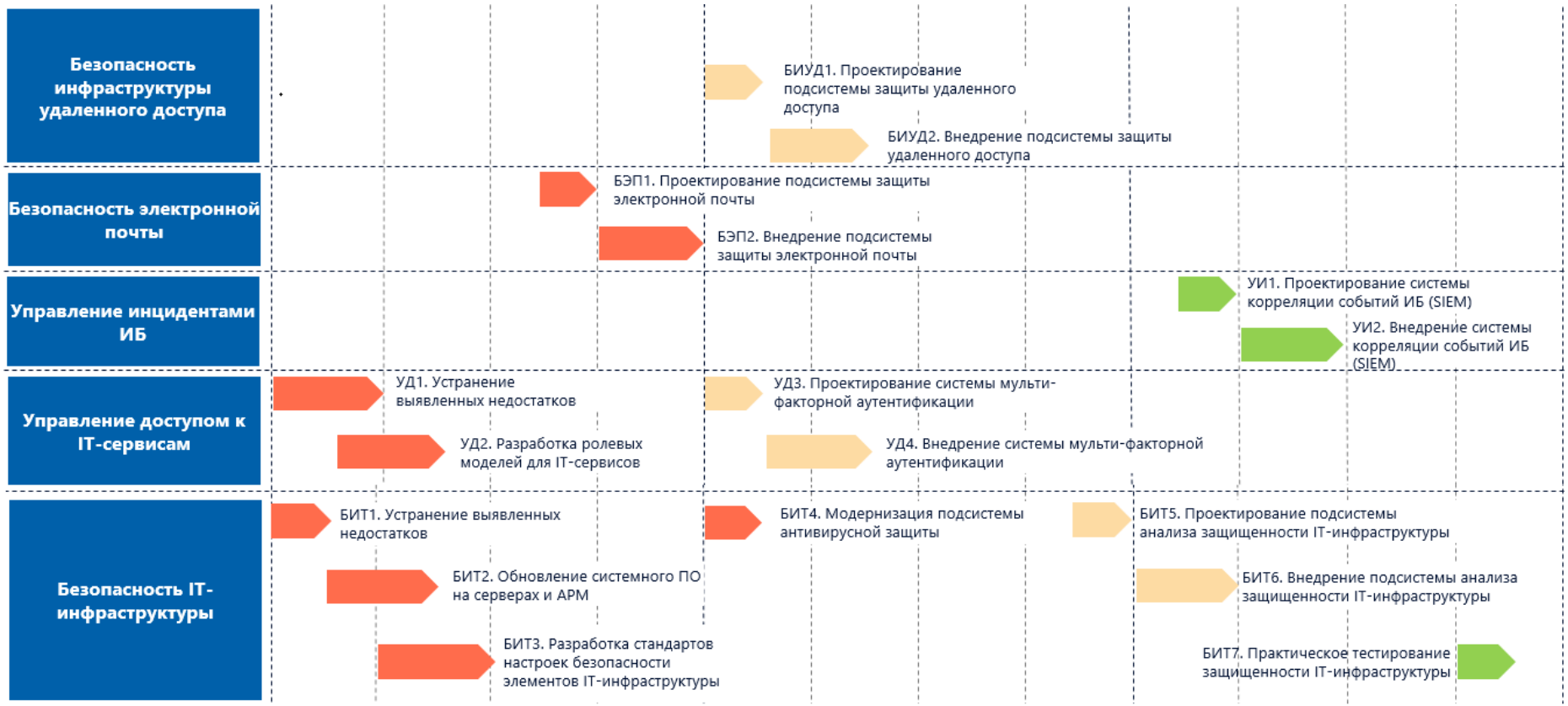


Рисунок Б.2 - Дорожная карта развития (вторая часть)