ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Иркутский государственный университет путей сообщения»
(ФГБОУ ВО ИРГУПС)

На правах рукописи

Наседкин Павел Николаевич

МОДЕЛИ И АЛГОРИТМИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ПО ПОВЫШЕНИЮ ЭФФЕКТИВНОСТИ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ПРЕДПРИЯТИЯ

Специальность: 2.3.1 – Системный анализ, управление и обработка информации, статистика

Диссертация на соискание ученой степени кандидата технических наук

Научный руководитель:
доктор технических наук,
доцент, Аршинский Леонид Вадимович

Иркутск – 2024

Содержание

Введение

Актуальность. С развитием информационных технологий и внедрением их в деятельность предприятий растёт необходимость совершенствования способов защиты предприятия от различных видов киберугроз, которые становятся все более сложными и разнообразными. С одной стороны происходит увеличение объема и значимости хранимой, передаваемой и обрабатываемой информации, что требует развития и совершенствования средств её защиты, с другой – предприятия функционируют в условиях ограниченных финансовых ресурсов, что усложняет проблему.

Изучение литературы показывает, что большинство исследований в области оценки и управления эффективностью систем защиты информации (СЗИ) посвящены вопросам оценки и управлению рисками информационной безопасности (ИБ). В то же время риск оценивается с использованием экспертных методов, которые характеризуются известным субъективизмом при недостатке статистических данных, когда вероятностный фактор риска рассчитывается исходя из следующего: вероятности реализации угрозы, вероятности использования уязвимости, размера ущерба.

Несмотря на общую результативность научных исследований и выработку стандартов в области управления ИБ, вопросы формализации оценок и измерения различных показателей безопасности всё ещё остаются недостаточно изученной областью знаний. В диссертационном исследовании рассматривается подход, основанный на онтологиях – специальной форме знаниевого моделирования предметной области, позволяющей отразить существующие в ней взаимосвязи. Исследования в области формализации знаний, касающиеся ключевых показателей ИБ, влияющие на свойства эффективности СЗИ описаны как в трудах российских учёных Г.Б. Петухова, Б.Е. Поклонова, Б.В.Черникова, В.И. Якунина и др., так и зарубежных авторов Г. Ковачича, К. Кормоса, Т. Кохонена, К. Пэйна, Ч. Робинсона, В. Рэйфорда, М. Свансона, М. Сэйко и др.

Вопросы онтологического моделирования и применения знаниевых моделей для поддержки принятия управленческих решений отражены как в трудах

зарубежных авторов А. Гомес-Перес, Т.Р. Грубера, О. Корчо, М. Фернандеса-Лопеса и др., так и российских учёных И. Бубакара, М.Б. Будько, Т.А. Гавриловой, В.В. Грибовой, Ю.А. Загорулько, Л.В. Массель., С.В. Смирнова и др.

В контексте повышения эффективности функционирования СЗИ, применение онтологий позволяет достаточно точно определить компоненты и взаимосвязи предметной области и выполняемые ими функции, рассчитать агрегированные показатели соответствия СЗИ заявленным целям. Притом, что в прикладном плане необходимо не просто повысить эффективность СЗИ, а выполнить это с учётом возможных финансовых ограничений. Владельцы информационных активов должны решить задачу каким образом обеспечить максимальную функциональную эффективность СЗИ при ограничении на затраты, либо каким образом минимизировать затраты при ограничении на эффективность СЗИ (под функциональной эффективностью здесь и далее понимаем соответствие системы целям своего функционирования; под оценкой функциональной эффективности – количественную меру такого соответствия).

Все вышеперечисленное обосновывает необходимость использования системного подхода при создании моделей и разработке алгоритмического обеспечения для повышения эффективности СЗИ. Это же определяет актуальность выбранной темы диссертационного исследования, позволяет определить его цель и задачи.

Целью диссертационной работы является повышение функциональной эффективности СЗИ предприятия на уровне программно-технических компонентов за счет разработки и применения моделей и алгоритмического обеспечения поддержки принятия решений с учётом возможных финансовых ограничений.

Для реализации поставленной цели необходимо решить следующие **задачи**:

1. Выполнить системный анализ предметной области, включая методики, методы и подходы, применяемые для оценки эффективности состояния информационной безопасности предприятия.

2. Используя методы системного анализа и онтологического

моделирования, определить основные компоненты (объекты защиты, угрозы, комплексы средств защиты, подсистемы и функции подсистем) программно-технической СЗИ (ПТСЗИ) и их взаимосвязи.

3. Разработать алгоритмическое обеспечение агрегированного оценивания эффективности функционирования ПТСЗИ предприятия.

4. Разработать и программно реализовать задачу оптимизации распределения денежных средств, направляемых на повышение эффективности СЗИ предприятия в контексте функционирования программно-технических компонентов.

5. Разработать программу для реализации процедуры агрегированного оценивания и визуализации результатов оценивания.

Объектом исследования является ПТСЗИ предприятия в процессе его функционирования.

Предметом исследования является алгоритмическое обеспечение и программы, поддерживающие принятие управленческих решений для повышения эффективности СЗИ предприятия в контексте функционирования её программно-технических компонентов с учетом возможных финансовых затрат.

Методы исследования: для решения поставленных задач применены методы системного анализа и семантического моделирования, линейного программирования (симплекс-метод), а также методы для решения базовых задач визуальной аналитики.

Научную новизну диссертации представляют следующие положения, **выносимые на защиту**:

1. Онтологические модели применительно к программно-технической реализации СЗИ и модели определения исходных данных для вычисления показателей эффективности.

2. Методика и алгоритмическое обеспечение агрегированного оценивания ПТСЗИ, использующие трехмерную матрицу защиты, многомерный бинарный массив и модели эффективности, включая визуализацию результатов оценивания.

3. Две задачи линейного программирования (ЛП) об оптимальном распределении денежных средств на совершенствование ПТСЗИ, в первой из которых для заданного бюджетного ограничения максимизируется нижняя граница функциональной эффективности ПТСЗИ и всех её компонентов, а во второй минимизируются суммарные затраты для обеспечения заданного уровня функциональной эффективности ПТСЗИ и всех её компонентов.

Достоверность результатов, выносимых на защиту, подтверждается использованием хорошо зарекомендовавших себя методов онтологического моделирования, линейного программирования, результатами опытной эксплуатации разработанного программного обеспечения.

Соответствие диссертации паспорту научной специальности. Содержание диссертационной работы соответствует паспорту научной специальности 2.3.1 – Системный анализ, управление и обработка информации, статистика: п.5. Разработка специального математического и алгоритмического обеспечения систем анализа, оптимизации, управления, принятия решений, обработки информации и искусственного интеллекта; п.9. Разработка проблемно-ориентированных систем управления, принятия решений и оптимизации технических объектов; п.11. Методы и алгоритмы прогнозирования и оценки эффективности, качества, надежности функционирования сложных систем управления и их элементов.

Теоретическая значимость исследования определяется разработкой методики поддержки принятия решений по повышению эффективности СЗИ в контексте функционирования её программно-технических компонентов на основе: 1) созданных онтологических моделей для определения исходных данных с целью вычисления показателей функциональной эффективности ПТСЗИ предприятия; 2) методики и алгоритмического обеспечения агрегированного оценивания ПТСЗИ, использующих трехмерную матрицу защиты, многомерный бинарный массив и модели эффективности, включая визуализацию результатов оценивания с использованием 6 уровневой цветовой

шкалы; 3) постановки и решения задач ЛП применительно к ПТСЗИ, позволяющих повысить эффективность принятия управленческих решений.

Практическая значимость результатов состоит в том, что разработанная методика доведена до программно-алгоритмической реализации в виде двух программ: программы «Агрегированное оценивание функциональной эффективности» (АОФЭ) и программы «Оптимальное распределение денежных средств» (ОРДС) для принятия решений по повышению функциональной эффективности СЗИ предприятия в контексте функционирования её программно-технических компонентов. Созданные программы апробированы на различных исходных данных, характеризующих состояние СЗИ предприятия в контексте функционирования её программно-технических компонентов. Получен акт о внедрении результатов диссертационной работы в деятельность предприятия ООО «ЯНТА».

Апробация материалов исследования. Основные результаты диссертационного исследования докладывались и обсуждались на следующих научных конференциях: межвузовской научно-практической конференции молодых ученых «Информационные технологии. Актуальные проблемы защиты информации» (г. Иркутск, 2019); межвузовской научно-теоретической конференции в рамках Сибирского форума «Информационная безопасность – 2021» (г. Новосибирск, 2021); VI-ой Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых «Наука и молодежь» (г. Иркутск, 2020); VII-ой Всероссийской научно-практической конференции студентов, аспирантов и молодых учёных «Наука и молодежь» (г. Иркутск, 2021); VIII-ой Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых «Наука и молодежь» (г. Иркутск, 2022); III-ей Всероссийской научно-практической конференции «Информационные Технологии, их приложения и информационное образование» (ИТПИО`22) (г. Гусиноозёрск, 2022); XI-ой Международной научно-практической конференции «Транспортная ин-фраструктура Сибирского региона» (г. Иркутск, 2020); XII-ой Международной научно-практической конференции «Транспортная

инфраструктура Сибирского региона» (г. Иркутск, 2021); I-ой Всероссийской конференции с международным участием «Информационные технологии, их приложения и информационное образование» (ИТПИО'2020) (г. Иркутск, 2020); XXVII-ой Байкальской Всероссийской конференции с международным участием «Информационные и математические технологии в науке и управлении» (г. Иркутск, 2022).

Публикации. По теме диссертационного исследования опубликовано 12 работ. Из них 4 статьи в рецензируемых научных журналах из перечня ВАК по рассматриваемой научной специальности, 2 свидетельства о государственной регистрации программ для ЭВМ и 6 в других изданиях.

Личный вклад автора. Постановка задачи выполнена совместно с руководителем. Результаты, составляющие новизну и выносимые на защиту, получены лично, либо в неделимом соавторстве. Конфликт интересов с соавторами отсутствует.

Объем и структура работы. Диссертация объемом 171 стр., состоит из введения, 4 глав, заключения, списка сокращений, 2 приложений, списка использованных источников из 183 наименований. Основная часть работы изложена на 167 страницах машинописного текста, содержит 10 таблиц и 37 рисунков.

Глава 1. Анализ существующих методик, методов и подходов, применяемых для оценки эффективности систем защиты информации

Современные информационные системы, обеспечивающие критические процессы и данные на предприятиях, становятся всё более уязвимыми для многочисленных угроз, включая кибератаки, утечки данных и иные инциденты информационной безопасности (ИБ). В условиях роста значимости информации, как ключевого актива, оценка и управление эффективностью систем информационной безопасности приобретают фундаментальное значение. В последние годы особое внимание уделяется системному анализу, который позволяет комплексно подходить к оценке состояния и защищенности информационных систем. Системный анализ в области информационной безопасности не только даёт возможность выявлять и оценивать уязвимости в существующих системах, но и определять взаимосвязи между компонентами системы защиты информации (СЗИ), проводить агрегированную оценку их эффективности и надёжности. Такой подход позволяет применять методы интеллектуальной поддержки принятия решений, онтологическое моделирование, а также автоматизированные и экспертные системы для прогнозирования и минимизации рисков [34-39, 58, 101, 111, 114, 117, 130, 131].

Исследования в области решения задач обработки информации в процессах управления включают работы как зарубежных, так и российских авторов. Среди зарубежных ученых, занимающихся этой областью, стоит отметить работы таких специалистов как Р. Акоффа [3,4], Р. Беллмана [118], Р. Бияшева [143, 144], Н. Винера [25], Е. Дейкстры [154], Т. Кохонена [169], Л. Льюинга [90], М.Д. Месаровича [95], С.Л. Оптнера [112] и др. Среди российских исследователей можно отметить работы П.Н. Девянина [41, 42], П.Д. Зегжды [52-56], И.С. Клименко [60-79], А.А. Корниенко [82], С.И. Носкова [110] и других.

Исследования в области формализации знаний, касающиеся ключевых показателей ИБ, влияющие на свойства эффективности СЗИ описаны как в трудах российских учёных Г.Б. Петухова и В.И. Якунина [113], Б.Е. Поклонова и Б.В. Черникова [132], и др., так и зарубежных авторов Г. Ковачича [171], Т. Кохонена [169], К. Кормоса [170], К. Пэйна [176], Ч. Робинсона [178], В. Рэйфорда [182], М. Сэйко [179], М. Свансона [181] и др.

Теоретические основы компьютерной безопасности и защиты сетей были исследованы П.Н. Девяниным [41,42] и Б.Я. Советовым [123, 124]. Значительный вклад в область защиты информации внесли такие авторы как Л.К. Бабенко [10-14], А.А. Малюк [93], А.С., А.А. Шумский [136, 137] и А.А. Шелупанов [134, 136, 137].

За рубежом вопросами онтологического моделирования и применения знаниевых моделей для поддержки принятия управленческих решений занимались такие ученые, как: Абейоми-Алли Абейоми [141], К. Арбанас [172], О. Т. Арогундейд [141], А. Гомес-Перес [157], Т. Р. Грубер [158], Ч. Джунхо [148], О. Корчо [157], С. Мисра [141], Т. Нойбауэр [156], А. М. Шаабан [140], К. Шмиттнер [140], М. Фернандес-Лопес [157], С. Фенц [156], Ч. Чанг [148], М. Чубрило [172].

Среди российских учёных в области онтологического моделирования и применения знаниевых моделей для поддержки принятия управленческих решений необходимо отметить таких учёных, как: И. Бубакара [23], М. Б. Будько [23], М. Ю. Будько [23], Т.А. Гаврилову [29,30], Гаськову [91], А. В. Гирика [23], В.В. Грибову [40], Ю.А. Загорулько [51], А.Г. Масселя [91], Л.В. Массель [92], и С.В. Смирнова [122] и др.

1.1. Принципы системного анализа в задачах информационной безопасности и их значение для оценки зрелости и устойчивости СЗИ

В настоящее время применение системного подхода в ИБ для оценки текущей защищенности и выработки стратегии устойчивого развития и

совершенствования СЗИ можно рассмотреть по следующим группам:

а) Основы системного анализа и их применение в ИБ.

Основные принципы системного анализа были заложены такими исследователями, как Рассел Акофф, который рассматривал системное мышление как основу для повышения управляемости и устойчивости организаций, опираясь на комплексный взгляд на процессы и задачи [3,4]. В контексте информационной безопасности, системный анализ позволяет более четко определять цели и задачи системы, выделять её элементы и границы, а также учитывать их взаимосвязи. Этот подход позволяет рассматривать систему защиты информации как иерархическую структуру, где каждый уровень отвечает за определенные функции, и все элементы системы взаимодействуют друг с другом для достижения общей цели.

Методы системного анализа также позволяют учесть динамические аспекты работы СЗИ. Динамическое программирование, разработанное Ричардом Беллманом, предоставляет теоретическую основу для анализа изменений во времени, которые имеют особое значение для прогнозирования устойчивости системы и адаптации к новым угрозам [20]. Данный подход особенно эффективен для анализа поведения системы в условиях постоянных изменений, таких как развитие кибератак и эволюция угроз.

б) Иерархическая структура и взаимодействие элементов СЗИ.

Одной из важных особенностей системного подхода в ИБ является способность рассматривать систему как иерархически организованную многоуровневую структуру. Эта концепция нашла отражение в трудах Месаровича М.Д., который совместно с коллегами разработал теорию иерархических многоуровневых систем, применимую к сложным информационным системам, таким как системы информационной безопасности [95]. Подход иерархического моделирования позволяет четко распределять роли и ответственность на каждом уровне СЗИ, а также обеспечивает устойчивость за счет четко структурированных каналов взаимодействия между уровнями.

В условиях функционирования СЗИ иерархическая модель помогает

структурировать систему защиты, распределяя функции и обязанности по уровням – от физической защиты и мониторинга событий до аналитики и прогнозирования на уровне управления. Такой подход облегчает задачи управления, упрощает выявление слабых мест и способствует повышению общей устойчивости системы.

в) Нечеткие множества и их применение в оценке ИБ.

Важной составляющей системного анализа является учёт неопределенностей, связанных с изменчивостью угроз и сложностью прогнозирования поведения злоумышленников. В этой области широкое применение нашли теории нечетких множеств Лотфи А. Заде, которые позволяют учитывать неполную и неопределенную информацию о состоянии системы и угрозах [183]. Методология нечетких множеств актуальна для задач ИБ, где вероятностные и детерминированные методы не всегда применимы ввиду сложности и вариативности атак. Применение методов нечеткой логики в ИБ позволяет моделировать ситуации, когда точные данные отсутствуют или их невозможно получить, что особенно важно для оценки зрелости системы защиты.

г) Оценка зрелости и устойчивости СЗИ через системный анализ.

Применение системного анализа для оценки зрелости и устойчивости СЗИ позволяет выявить текущие возможности системы и определить области для улучшения. Один из известных методов оценки зрелости – это рассмотрение СЗИ как динамической и адаптивной структуры, где каждый элемент должен быть проверен на предмет устойчивости и способности к адаптации к новым угрозам [147]. Питер Чекленд отмечал, что системное мышление позволяет глубже понять внутренние процессы и выявить возможности для их оптимизации, что особенно полезно для анализа систем, подверженных постоянным изменениям [147].

Для того чтобы оценить зрелость СЗИ, необходимо анализировать не только её текущую конфигурацию, но и способность к восстановлению по-

сле инцидентов, возможности для масштабирования и интеграции новых защитных мер. На основе системного подхода возможна разработка метрик и показателей, которые помогают оценить уровень зрелости и устойчивости системы в условиях изменяющейся внешней среды и возрастающих киберугроз.

Управление системами информационной безопасности (ИБ) требует комплексного подхода, включающего как технические, так и управленческие меры. Для обеспечения эффективной защиты информации важно выстроить процесс управления ИБ на основе методологий, обеспечивающих структурированный и систематический подход. Одним из таких подходов является использование моделей зрелости, таких как SSE-CMMI [180, 167], NIST [174, 181], CERT и COBIT [146,179].

Системный анализ играет ключевую роль в оценке зрелости СЗИ. Применение системного анализа позволяет структурировать процессы оценки, выделяя ключевые параметры и метрики. Одной из популярных моделей в данной области является модель COBIT 5, которая предоставляет универсальные рекомендации по управлению ИТ и ИБ, ориентированные на бизнес-цели и результаты [151]. COBIT 5 позволяет организовать оценку эффективности управления ИБ с учетом стратегии предприятия, что делает его универсальным инструментом для организаций различного масштаба. Вместе с тем, COBIT for Risk [23] – это сложный и трудоемкий процесс, требующий значительного объема ресурсов для сбора исходных данных. Этот метод отличается высокой ресурсоемкостью, что может стать препятствием для его применения в некоторых организациях. Еще одним недостатком является отсутствие возможности оценивать риски в денежном эквиваленте, что усложняет анализ потенциальных финансовых последствий.

Для управления устойчивостью СЗИ широко применяется CERT Resilience Management Model (CERT-RMM), ориентированная на управление операционной устойчивостью и защитой критических данных и процессов [146]. CERT-RMM позволяет интегрировать процессы управления рисками, обеспечения

непрерывности бизнеса и ИБ, что важно для организации, сталкивающейся с постоянно меняющимися угрозами. Подобные модели помогают руководителям понимать сильные и слабые стороны СЗИ и принимать решения для улучшения процессов защиты и реагирования на инциденты.

Показатели ИБ являются составной частью этих моделей и обычно связаны с областями процессов и оценкой степени и/или уровня их реализации. В современной практике модели оценки зрелости используются в основном для поиска качества процесса управления безопасностью и лучшего понимания ИБ. Модели зрелости также являются руководством для тех элементов управления, которые должны быть внедрены. «Зрелость» находится в определенной связи с риском, поэтому повышение зрелости отражается на профиле риска всей организации, отношении к безопасности и лучшей отдаче от инвестиций в безопасность [179, 181].

Таким образом, оценка зрелости является полезной и важной мерой при оценке соответствующего предприятия, а также при сравнении одного предприятия с другим. Хотя уровень зрелости может быть использован для сравнения с другими предприятиями («Бенчмаркинг»/Контрольные точки; Эталон), это не является его целью. В основном они используются при внешней оценке программы информационной безопасности. Анализируя конкретную модель оценки зрелости, было установлено, что их основой являются критерии безопасности, которые включают различные аспекты управления ИБ/ИТ. Зрелость или способность предприятию управлять своей безопасностью и противостоять угрозам безопасности определяется путем оценки состояния конкретных критериев. В зависимости от структуры критериев и подкритериев, а также их содержания существуют различные модели. С другой стороны, степени интенсивности или шкалы для структуры оценки процесса качества относительно одинаковы [179, 181]. Сравнительный анализ их особенностей приведен в таблице 1.1 [179, 181].

Таблица 1.1 – Сравнительный анализ особенностей моделей оценки зрелости программ ИБ

Модель оценки		Модель зрелости	Фокус модели
NIST CSEAT IT	1	политика	качество документации
	2	процедуры	
	3	внедрённая система	
	4	судебное разбирательство	
	5	интеграция	
Citigroup's Info. Модель оценки информационной безопасности (CITI-ISEM)	1	самодовольство	корпоративные знания и обучение в организации
	2	познание	
	3	интеграция	
	4	Обычная практика	
	5	постоянное совершенствование	
COBIT	1	Первоначальная / специальная	обзор конкретных процедур
	2	Повторяющиеся, но интуитивно понятные	
	3	определённые процессы	
	4	Управляемые и измеряемые	
	5	Оптимизированный	
SSE-CMM	1	неофициальный	инженерно-конструкторская безопасность
	2	планирование и контроль	
	3	четко определенный	
	4	количественный контроль	

Модель оценки		Модель зрелости	Фокус модели
	5	постоянное совершенствование	
CERT/CSO	1	существовать	для оценки качества документации
	2	повторяющийся	
	3	возложенная ответственность	
	4	задокументировано	
	5	пересмотренный и обновленный	

Можно предположить, что оценка зрелости с помощью различных методов на одной и той же выборке даст разные результаты, хотя исследования в этой области неизвестны. Выявление взаимосвязи между конкретными моделями выходит за рамки и цели данной работы, поэтому это может стать темой будущих исследований [179, 181].

Использование статистических методов и анализа данных помогает минимизировать субъективность при оценке рисков и более точно прогнозировать возможные последствия угроз.

Таким образом, системный анализ, включающий принципы и методы, такие как иерархическое моделирование и учет нечетких данных, позволяет формировать комплексное представление о состоянии СЗИ, её слабых местах и путях развития.

1.2. Показатели оценки эффективности функционирования системы защиты информации и их применение

Методологической основой [119] для определения показателей эффективности функционирования систем защиты информации от несанкционированного доступа (НСД) в автоматизированных информационных системах (АИС) при их разработке являются основные

положения теории эффективности и теории систем. В данной работе решаются следующие задачи:

а) Проводится анализ нормативных международных и российских документов по проблемам оценки качества программного обеспечения в составе следующих подзадач [34-36, 120, 121, 164-166]:

1) Изучения и систематизации требований и стандартов, регулирующих качество программного обеспечения и системы защиты информации (временная эффективность, ресурсоёмкость, времяёмкость, функциональность, результативность, производительность, используемость ресурсов, рациональность, доступность, оперативность, уровень автоматизации, эффективность исполнения, эффективность хранения).
2) Сравнительного анализа международных и российских нормативных актов для выявления общих и специфических требований.

б) Проводится анализ научных материалов по оценке качества программного обеспечения в составе следующих подзадач [113, 132, 155]:

1) Исследования современных методик и подходов к оценке качества программного обеспечения в области информационной безопасности.
2) Оценки применимости методик к системам защиты информации от НСД.

в) Проводится исследование свойств эффективности функционирования систем защиты информации от НСД в АИС в составе следующих подзадач [1, 45, 139]:

1) Определения ключевых свойств и характеристик, влияющих на эффективность систем защиты информации.

В [119] представлены атрибуты (показатели) оценки эффективности функционирования системы защиты информации от НСД. Эти показатели подразделяются на две группы: частные (статические) и интегральные (динамические).

Частные показатели не зависят от времени и основаны на экспертных оценках, тогда как интегральные показатели зависят от времени, и их оценка основывается на математическом моделировании. Краткая характеристика показателей, представлена в таблице 1.2.

Таблица 1.2 – Атрибуты (показатели) оценки эффективности функционирования системы защиты информации от НСД

Показатель	Описание	Тип
Надежность системы	Оценка способности системы функционировать без сбоев и отказов в условиях эксплуатации.	Частный
Уровень защиты информации	Степень соответствия системы требованиям нормативных документов по защите информации.	Частный
Скорость реакции на угрозы	Время, необходимое системе для обнаружения и реагирования на угрозу безопасности.	Интегральный
Устойчивость к атакам	Способность системы противостоять различным видам кибератак и их последствиям.	Интегральный
Обновляемость	Способность системы адаптироваться к новым угрозам и обновлять свои компоненты для их предотвращения.	Интегральный
Экономическая эффективность	Соотношение затрат на систему защиты к предотвращенному ущербу от потенциальных угроз.	Интегральный
Пользовательский опыт	Уровень удобства и простоты использования системы для конечных пользователей.	Частный

2) Изучения факторов, влияющих на устойчивость и надежность систем защиты информации (оптимальность программного кода, в динамике, корелляцию ресуросоёмкости СЗИ от НСД от вычислительных ресурсов АИС, моральное старение СЗИ,

изменение программного и технического обеспечения).

г) Проводится аналитическое обобщение существующих недостатков систем защиты информации от НСД в АИС в составе следующих подзадач:

1) Выявления и классификации основных проблем и недостатков текущих систем защиты информации.
2) Анализа причин возникновения недостатков и их влияние на общую эффективность систем защиты.

д) Проводится разработка показателей эффективности функционирования систем защиты информации от НСД в составе следующих подзадач:

1) Определения критериев для оценки частных (статических) и интегральных (динамических) показателей.
2) Создания системы показателей для комплексной оценки эффективности функционирования систем защиты информации.

Иными словами, показана декомпозиция показателей эффективности СЗИ от НСД на три группы, учитывающие влияние: 1. Количества ресурсов АИС на показатели (временная эффективность, ресурсоёмкость, оптимальность программного кода); 2. Количества функций защиты СЗИ на показатель функциональности; 3. Времени эксплуатации СЗИ от НСД на показатели морального старения и изменяемости.

е) Обоснование и разработка критериев оценки эффективности функционирования систем защиты информации от НСД.

1) Разработка методологических основ для создания критериев оценки эффективности.
2) Определения количественных и качественных критериев, обеспечивающих объективную оценку.

ж) Разработка алгоритма интегральной оценки эффективности функционирования систем защиты информации от НСД.

1) Создания алгоритма, позволяющего проводить комплексную оценку эффективности с учетом временных и независимых

факторов.

2) Интеграции разработанных показателей и критериев в алгоритм оценки.

Для решения поставленных задач авторы [119] применяют комплексный подход, который включает три основных метода оценки эффективности функционирования систем защиты информации от несанкционированного доступа (НСД):

– Экспертный метод – базируется на суждениях и оценках экспертов в области информационной безопасности. Этот метод позволяет учитывать субъективные мнения специалистов и использовать их опыт и знания для определения ключевых показателей эффективности.

– Вероятностный метод – основывается на использовании математических моделей и вероятностных оценок для определения эффективности системы защиты. Этот метод учитывает различные сценарии угроз и вероятности их реализации, что позволяет проводить более точные и обоснованные оценки.

– Оценочный метод – включает количественные и качественные показатели, определяемые на основе анализа нормативных документов и научных исследований. Этот метод позволяет использовать объективные данные для оценки эффективности системы защиты информации от НСД.

Наилучшим подходом в [119] признано сочетание всех трех методов, что обеспечивает комплексное и всестороннее оценивание эффективности функционирования систем защиты информации.

По мнению авторов [119] экспертный метод предполагает проведение опросов и интервью с ведущими специалистами в области информационной безопасности для определения важности и веса каждого показателя. Эксперты оценивают, насколько каждый из показателей важен для общей эффективности системы защиты информации.

Вероятностный метод как показывают авторы [119] включает в себя моделирование различных сценариев угроз и оценку вероятности их реализации. На

основе этих данных рассчитывается вероятность успешной защиты системы при различных условиях эксплуатации.

Оценочный метод базируется на анализе нормативных документов (например, ГОСТ-28806-90 [35], требования ФСТЭК России [101, 114, 130, 131]) и научных публикаций. Этот метод позволяет учитывать как количественные, так и качественные аспекты эффективности функционирования систем защиты информации.

Предложенный в [119] комплексный подход к оценке эффективности функционирования систем защиты информации от НСД, сочетающий экспертный, вероятностный и оценочный методы, по мнению авторов обеспечивает всестороннюю и объективную оценку. Разработка частных и интегральных показателей, как следует из [119] позволяет учитывать как временные, так и независимые от времени характеристики системы, что по мнению авторов способствует повышению ее надежности и безопасности в условиях реальной эксплуатации.

Понятие показателя ИБ чаще всего упоминается как инструмент для анализа, оценки, координации и согласования с требованиями безопасности. Внимания заслуживает работа [179], которую разберём подробнее. Так в работе автора Mario-Sajko [179] приведено описание состояния информационной безопасности и метрик, которые используются для ее оценки. В статье рассматриваются различные показатели и индикаторы, применяемые в разных областях информационной безопасности, и обсуждаются методы их мониторинга и измерения. Автор отмечает, что хотя в литературе можно найти примеры таких показателей и конкретные предложения по их сбору и измерению, область измерения информационной безопасности еще недостаточно исследована. Цель статьи – систематизировать существующие наработки в этой области и определить существующий опыт применения метрик безопасности в оценке состояния информационных систем [179].

Sajko, Mario в своей работе «Measuring and Evaluating the Effectiveness of Infor-mation Security» [179] подчеркивается важность применения метрик для управления процессами информационной безопасности. Автор утверждает, что

невозможно управлять процессами, если они не могут быть измерены. Вопрос заключается не в необходимости измерений, а в выборе правильных метрик и методов для достижения поставленных целей. В качестве ориентиров могут служить стандарты, требования регуляторов, законы и примеры лучших практик [150].

Метрики безопасности в статье Sajko, Mario «Measuring and Evaluating the Effectiveness of Infor-mation Security» [179] определяются как система измерений, предназначенная для оценки и мониторинга эффективности мероприятий по информационной безопасности. Они включают в себя такие элементы, как объект измерения, референтные значения, сенсоры, механизмы сравнения, инициаторы действий, значения, способы представления и временное измерение [171, 179].

Метрики могут использоваться для различных целей, таких как документирование состояния безопасности, координация корректирующих действий, измерение результатов программ безопасности, понимание и управление требованиями безопасности, а также оценка результатов контроля безопасности и установление уровня риска [179].

Автор отмечает, что несмотря на существование различных подходов к структурированию метрик безопасности, их применение остается ограниченным. Основные проблемы связаны с отсутствием единой системы метрик, недостаточной стандартизацией и трудностями в интерпретации и оценке результатов измерений [179]. В работе [179] автором рассмотрены:

а) Основные вопросы, на которые отвечают метрики безопасности: что измеряется, почему это измеряется и кто осуществляет измерения. Автором приводятся связи между различными аспектами применения метрик, такими как технические процессы, организационные системы и описание, прогнозирование и сравнение результатов [179, 181, 182]. Таким образом следует, что понятие показатели ИБ представлено как система преобразования и представления, пригодная для составления отчетов руководству. В тоже время, в [128] и «US National Information Systems Security Glossary» [175] рассматриваются

показатели ИБ как инструмент для принятия решений, документирования и подсчета угроз, а также как часть процесса управления рисками безопасности [128, 171, 175].

В данном случае определение показателя ИБ в интерпретации автора [179] предлагается взять из [160], согласно которому: показатель ИБ определяет измерительную систему или стандарт; измерительные шкалы и единицы для контроля эффективности, а измерение – это акт определения количества, размера степени (чего-либо) с помощью стандартной группы мер и измерительных процедур, определяемого показателем ИБ. Автором [179] отмечается, что показатель ИБ в основном используется для: 1) документирования (состояния безопасности) и координации результатов, которые должны быть исправлены [170]; 2) для понимания и управления требованиями безопасности [178]; 3) как инструмент для оценки результатов контроля безопасности [176].

По мнению автора [179] попытки сделать показатель ИБ и способы его применения понятными отражены в результатах исследований, проведенных зарубежными корпорациями и институтами: «Corporate Information Security Working Group» [150], SSE-CMM [167], NIST [181], и авторов Vaughn [182], Lennon [174]. В тоже время, автор акцентирует внимание на то, что институт NIST [174] предлагает базовое разделение показателей ИБ как для государственного и частного сектора (для многочисленных нормативных требований к безопасности общественных организаций). Однако, предпочтение автора [179] вызывает работа [182], как возможно лучшая попытка декомпозиции показателей ИБ, где как он полагает показатели перечислены в соответствии с типами измерений и областями систем безопасности.

б) Пример иерархической структуры метрик безопасности [170], начиная с общих категорий и переходя к более конкретным показателям в соответствии с инструкциями моделей SSE-CMM [167], где выделяют контроль доступа по списку «А» и контроль доступа по списку «Б», каждый из которых включает ряд мер для обеспечения безопасности. Такой подход по мнению автора [179]

позволяет структурировать метрики в соответствии с различными уровнями управления и аспектами безопасности [160]. Необходимо отметить, что в исследовании Хамфриса и Плэйт предлагается система метрик, позволяющая измерять эффективность внедренной системы ISMS. Данный подход включает в себя оценку как технических мер, так и процедурных аспектов безопасности [160].

в) Контроль доступа по списку «А» (внутренние) [179]:

– Отсутствие ложных попыток ввода пароля: система должна предотвращать несанкционированный доступ, блокируя попытки после нескольких неверных паролей.

– Политика паролей: включает требования к сложности, длине и периодичности смены паролей, что усиливает защиту системы.

– Обновления для обнаружения вирусов: регулярные обновления помогают защититься от новых вирусов. Анализ частоты вирусных инфекций позволяет оценить эффективность мер безопасности.

– Меры реагирования на вирусные инциденты: быстрое и эффективное реагирование на вирусные атаки минимизирует ущерб.

– Аудиторские проверки: Регулярные проверки помогают выявлять уязвимости и нарушения безопасности, что позволяет своевременно реагировать на изменения угроз.

г) Контроль доступа по списку «Б» (внешние) [179]:

– Автоматизированная система обнаружения вторжений: обнаруживает попытки несанкционированного доступа и немедленно сигнализирует об этом, позволяя быстро принимать меры.

– Время реакции на вторжение: быстрая реакция на угрозы уменьшает потенциальный ущерб и предотвращает распространение атаки.

– Межсетевые экраны: установка экранов на внешних точках доступа защищает систему от внешних угроз, фильтруя трафик и предотвращая несанкционированное проникновение.

– Успешные проникновения: минимизация случаев успешного проникновения свидетельствует об эффективной защите системы.

– Надежная идентификация и аутентификация (I&A): обеспечивает легитимность внешних пользователей и предотвращает несанкционированный доступ.

– Случаи несанкционированного доступа через защищенные каналы: несмотря на защитные меры, возможно нарушение безопасности, поэтому важно постоянно улучшать системы идентификации и аутентификации.

На основании изложенного автор [179] делает вывод о том, что контроль доступа по списку «Б» представляет комплексный подход к обеспечению безопасности. Использование автоматизированных систем по мнению автора [179], межсетевых экранов и регулярных проверок помогает достичь высокого уровня защиты от внешних угроз. Однако, как утверждает автор [179] абсолютная безопасность невозможна, поэтому по мнению автора необходимо постоянно анализировать и совершенствовать меры безопасности для адаптации к новым угрозам. Как отмечается автором, хоть в каждом случае область показателей ИБ не завершена и предложенные разделения показателей ИБ не являются универсальными, но это может послужить достойной отправной точкой и попыткой структурирования [179, 182]. Для систематизации показателей ИБ по мнению автора сначала необходимо объяснить основные измерения при их использовании.

д) Показатели безопасности для оценки результатов реализации программ информационной безопасности. В работе автора [179] выделена группа показателей безопасности, связанная с мониторингом реализации целей и задач безопасности, эффективностью и результатами контроля безопасности, степенью реализации программ безопасности, пригодностью проводимых процедур и выявлением возможных улучшений. По мнению автора [179] независимые международные институты, занимающиеся вопросами информационной безопасности, пошли дальше всех в их описании. (ISO, ISACA, ITCGI). Причина того, что об этой теме написано мало, как считает автор [179] заключается в том,

что такие показатели развиваться от случая к случаю и не могут быть просто скопированы из одной среды в другую. Поэтому для задач исследования [179] они обозначаются общим знаменателем – показатели эффективности (ПЭ), среди которых по мнению [179] особо интересными показателями эффективности являются так называемые ключевые показатели целей (КПЦ/ KGI) и ключевые показатели эффективности (КПЭ/ KPI), а также «эталонное» измерение.

Ключевые показатели целей (KGI – Key Goal Indicators) как указывается в [179] используются для измерения целей процесса. Такие показатели говорят руководству, выполнил ли процесс требования бизнеса, которые обычно представлены в виде критериев. Автор утверждает, что они являются мерами того, «ЧТО» должно быть реализовано, и измерительными показателями того, насколько успешно процесс реализует цели.

Ключевые показатели эффективности (KPI – Key Performance Indicators или показатели эффективности) в [179] определены как для достижения целей процесса. Одними из областей мониторинга KPI по мнению автора [179] могут быть:

– принятие программы о повышении уровня знаний в области безопасности;

– необходимые или утвержденные исключения в отношении политики рисков;

– инфицирование злокачественным программным кодом;

– недоступность важных ИТ-услуг;

– время, необходимое для внесения корректировок в программу;

– промежуток времени между увольнением сотрудника и аннулированием его пользовательского аккаунта;

– обнаружил области беспроводного подхода в компании.

В каждом случае, как акцентируется у автора [179], количественные показатели КПЭ(KPI) выстроены заранее и отражают критические факторы успешности. Например, одним из показателей может быть процент потерь из-за инцидентов по отношению к другим потерям или же примеры успешного решения подобных инцидентов [179]. Характеристики безопасности по мнению автора

[179] должны быть переведены на язык, понятный руководству, с помощью КПЭ (KPI). Примеры показателей КПЦ (KGI) и КПЭ (KPI) приведены в таблице 1.3 [179].

В литературных источниках как утверждает автор [179] можно встретить термин ключевые индикаторы риска (КИР/KRI), которые автор допускает, что можно отнести их к КПЭ (KPI) с указанием, что их использование связано исключительно с процессом управления рисками безопасности. КИР (KRI) должны измеряться в контексте КПЭ (KPI), а их отчетность должна быть составной частью процесса управления рисками [179].

Таблица 1.3 – Сравнительный анализ показателей КПЦ (KGI) и КПЭ (KPI)

KGI	KPI
Процент (%) проектов, завершенных в срок	Количество повторных инцидентов
Процент (%) изменений в системе, завершенные в течение требуемого времени	Количество инцидентов, разрешенных с помощью удаленного вмешательства
Количество проектов, в которых запланированные цели не были достигнуты из-за некачественного применения проектных решений	Количество инцидентов, разрешенных после расчетного времени на их устранения
	Среднее время устранения инцидентов по категориям
	Процент (%) количества инцидентов, решенных после первого обращения (в службу Service Desk)

Особым видом измерения эффективности безопасности по мнению автора [179] является измерение «бенчмаркинг» (или «процесс бенчмаркинга» – это процесс сравнения своей деятельности с лучшими компаниями на рынке и в отрасли с последующей реализацией изменений для достижения и сохранения конкурентоспособности.), используемое особенно в стратегическом управлении

бизнесом на предприятии. Такое измерение используется для оценки аспектов бизнес-процессов по отношению к лучшей практике, в основном внутри профессии [179]. Но эталонное измерение может применяться и для измерения внутри более крупной финансово-хозяйственной единицы – это Компании. Бенчмаркинг может быть уникальным процессом, но часто к нему относятся как к непрерывному процессу надлежащего сравнения производительности [179].

В литературе представлены различные подходы к определению областей, которые охватывают показатели информационной безопасности (ИБ). В [179] акцентируется на то, что Jonsson [168] выделяет три основные категории показателей: измерение рисков, оценка характеристик механизмов ИБ для сертификации и мониторинг несанкционированных входов в информационную систему. В другом исследовании [182] показатели ИБ, как приводится в [179], делятся на аспекты технических возможностей, управленческих возможностей и оценки уязвимости.

Стандарт NIST [174] по мнению автора [179] указывает на то, что хотя интерпретация областей, охватывающих показатели ИБ не определена четко, однако предложена структура для программы измерения безопасности. Эта структура включает:

– Показатели для корпоративного мониторинга управления безопасностью, поддерживаемые руководством.

– Показатели для мониторинга успешности внедрения политик и процедур безопасности.

– Количественные показатели для сбора и представления данных.

– Показатели для управления, ориентации на цели, непрерывного мониторинга и улучшения.

Как отмечает автор [179], стандарт ISO 27001 [160, 39] предлагает другой подход, разделяя показатели мониторинга на несколько категорий:

– Результаты управления средствами контроля.

– Процесс оценки и повторной оценки.

– Результаты оперативного контроля.

– Мониторинг результатов физического контроля.

– Результаты технического контроля.

На основании вышеизложенного можно сделать вывод, что показатели ИБ охватывают технический, оперативный и организационный уровни (области) измерения (применения), учитывая также человеческий фактор как отдельную область ответственности за ИБ [179]. Области, применения метрик безопасности, и соответствующие им методы измерения приведены в таблице 1.4.

Из таблицы 1.4 видно, что показатели ИБ для конкретной области измерений определяются её особенностями, а именно: возможностью использования различных комбинаций методов объективной и субъективной оценки, качественных и количественных мер, статических и динамических измерений, прямых и косвенных показателей, абсолютных и относительных величин.

Таблица 1.4 – Области измерений метрик безопасности

Область измерений	Методы измерения	Примеры показателей ИБ
Управленческая	Оценка эффективности процессов	Уровень выполнения задач
Операционная	Мониторинг инциден-тов	Количество инцидентов
Техническая	Тестирование систем безопасности	Уровень уязвимостей
Человеческая	Оценка осведомленно-сти сотрудников	Количество пройденных тре-нингов

С целью подчеркнуть проблему отсутствия стандартизированного разделения метрик, которые вызывают трудности в их использовании, автор в своей работе [179] приводит, как ему кажется наиболее важные метрики для оценки и анализа безопасности:

– Одной из важных категорий метрик по мнению автора [179] являются метрики рисков. Эта подгруппа метрик представляет собой инструмент для

оценки системы безопасности, измеряя степень неопределенности, с которой могут возникнуть последствия для бизнес-организации из-за угроз и слабостей системы безопасности. Эти метрики находятся на грани количественных показателей качества процессов и технических аспектов безопасности.

– Другая группа метрик, которую выделяет автор [179] – это метрики зрелости программы безопасности, развивается как отдельное направление. Как утверждает автор существует несколько моделей оценки зрелости, которые используются на практике как инструменты для ревизии текущего состояния безопасности. На взгляд автора [179] несмотря на то, что метрики оценки зрелости охватывают широкий спектр характеристик безопасности, они больше ориентированы на измерение поддержки со стороны руководства и оценку успешности процессов.

– Метрики производительности, к которым автором [179] отнесены метрики для мониторинга индикаторов рисков, метрики для отслеживания степени внедрения программы безопасности, метрики для мониторинга степени реализации целей безопасности, метрики для «бенчмаркинга» и т.д.

1.3. Оценка рисков, как компонент управления системой информационной безопасности

В условиях нарастающих угроз информационной безопасности важно оценивать и управлять рисками, чтобы минимизировать уязвимости и повысить устойчивость системы защиты информации. Современные методы оценки рисков помогают определить вероятность наступления различных событий, оценить последствия их реализации и выбрать подходящие меры противодействия. Оценка рисков служит основой для выработки стратегий управления ИБ и принятия оперативных решений.

Статья И. Бубакара, М.Б. Будько, М.Ю. Будько и А.В. Гирика, опубликованная в «Трудах ИСП РАН» [23], посвящена разработке онтологического подхода к управлению рисками информационной

безопасности. Основная цель исследования заключается в повышении эффективности системы информационной безопасности через создание онтологической модели, которая способствует улучшению процессов управления рисками. Авторы утверждают, что предложенный ими подход обеспечивает снижение временных затрат на принятие управленческих решений благодаря использованию гибких механизмов поддержки принятия решений. Проведённый сравнительный анализ показывает преимущества предлагаемого подхода перед существующими методами управления рисками. Результаты работы могут служить основой для создания высокоинтеллектуальных систем управления рисками и защиты информации.

Методы оценки рисков делятся на количественные и качественные, каждый из которых имеет свои преимущества и области применения. Количественный подход, описанный в работе Т. Пельтье [177], включает в себя использование числовых показателей и вероятностных расчетов для более точной оценки уровня риска. Этот метод требует сбора статистических данных о прошлых инцидентах и анализа вероятности возникновения конкретных угроз, что позволяет оценить финансовые и другие потери, которые могут быть вызваны угрозами [177].

С другой стороны, качественные методы, такие как матричный анализ, широко применяются при недостатке данных или высокой неопределенности. В таких случаях используется экспертная оценка вероятности и последствий угроз, что помогает в условиях ограниченных ресурсов. Матричные подходы позволяют оценивать риски на основе комбинации категорий вероятности и возможных последствий, обеспечивая относительную простоту и оперативность анализа, как указано в стандарт ISO/IEC 31010:2019 [161].

Одним из методов, объединяющих преимущества количественных и качественных подходов, является метод BowTie [145]. Он применяется для визуализации рисков и построения наглядных диаграмм, где угрозы, меры защиты и возможные последствия отображаются в форме «галстука-бабочки» [145]. BowTie позволяет не только выявить угрозы и уязвимости, но и

разработать меры реагирования, распределяя их по категориям, что упрощает процесс управления рисками и позволяет сосредоточиться на критических участках.

Метод BowTie используется для анализа цепочек причинно-следственных связей между возможными угрозами и их последствиями, помогая выявить слабые звенья в системе защиты. Это особенно важно для оценки рисков в сложных СЗИ, где требуется комплексный подход и многослойная защита от атак.

Оценка рисков является активно используемым компонентом управления системой информационной безопасности (ИБ) с 1974 года (Federal Information Processing Standards (FIPS)), и это практика, которая развивалась с течением времени. Оценка рисков в ИБ является процессом идентификации, анализа и оценки потенциальных угроз, уязвимостей и возможных последствий для информационных ресурсов организации. Она позволяет определить вероятность возникновения угроз и величину потенциального ущерба, а также помогает в выработке эффективных стратегий управления ИБ.

Оценка рисков в ИБ помогает организациям понять, какие угрозы могут повлиять на их информационные активы, и принять соответствующие меры для снижения рисков. Она позволяет организации определить приоритеты в области ИБ, распределить ресурсы для защиты наиболее значимых активов, а также оценить эффективность принимаемых мер.

Оценка рисков в ИБ стала особенно актуальной в современных условиях, когда информационные системы стали все более сложными и подвержены новым видам угроз. Развитие технологий и появление новых угроз, таких как кибератаки, вирусы, хакерские атаки и многие другие, усилили необходимость системного подхода к оценке рисков и принятию соответствующих мер по обеспечению безопасности информационных систем. Таким образом, оценка рисков находит широкое применение в управлении системами ИБ и позволяет организациям эффективно защищать свои информационные активы от потенциальных угроз.

В настоящее время имеется богатый спектр разработанных и предлагаемых алгоритмов, методов и методик для оценки рисков и угроз информационной безопасности [115, 116], которые могут в своей сути применяться дифференцированно в зависимости от размеров предприятия и степени получения оперативности оценочных суждений с применением количественного или качественного подхода. Для полноты понимания данного вопроса рассмотрим наиболее значимые подходы, предлагаемые к оценке рисков со стороны ученых и с использованием разработанных инструментальных программных средств.

В диссертационной работе П.В. Плетнева [116] проведен анализ более 100, опубликованных в научной периодике работ за 2006 по 2010 гг. по вопросам оценки угроз и информационных рисков. Анализ проводился с учетом отраженных в публикациях подходов к оценке угроз ИБ, а именно: сложность вычислений (низкая, средняя, высокая), сложность создания программного обеспечения (низкая, средняя, высокая), типов оценки угроз (статистическая, экспертная), вида итогового результата (количественный метод, качественный метод), связи с существующими стандартами в области ИБ. Автор отметил, что в рассматриваемых публикациях отсутствуют связи с действующими государственными стандартами в области ИБ в РФ и методиками по защите информационно-телекоммуникационных систем (ИТС).

В работе [48] авторами Е.А. Еременко, А.С. Сафроновым предложен подход к анализу риска с точки зрения выборки таких значимых методов из стандарта ISO/IEC 31010 [37, 48], как: «анализ дерева событий» [48]; «матрица последствий и вероятностей» [48]; «марковский анализ» [48]; hazop; метод Дельфи; предварительный анализ опасностей. Процесс оценки риска в разрезе методов в основе своём состоит из: идентификации рисков и анализа риска с учётом последствий, вероятностных характеристик и уровня риска. Оценка риска проводится с учётом качественных критериев («не применимо», «применимо», «строго применимо»). По мнению авторов, для точной оценки риска необходимо комбинированное использование методов оценки рисков ИБ, поскольку с точки

зрения анализа методов оценки необходимо учитывать такие критерии как: шкалы оценивания (количественные и/или качественные), сложность проведения оценки, ресурсы (временные/информационные), возможность оценки в динамике, степень неопределённости). Необходимо отметить, что комбинированное использование методов оценки рисков ИБ ведет к улучшению методов оценки за счет взаимной компенсации их недостатков.

Немаловажное значение в области экспертных оценок имеет так называемый метод Дельфи [96]. Этот метод используется для прогноза оценочных суждений группой независимых экспертов, используя опрос экспертов, не собирая их в одном месте. Метод Дельфи применим на любом этапе СУИБ и жизненного цикла информационных систем.

В задачах ИБ аналитический этап по методу Дельфи включает анализ полученных результатов оценки с итоговыми рекомендациями по вопросу как снизить уровень рисков ИБ. Вместе с тем, отметим, что на достоверность оценок в ходе проведения работ по данному методу влияет рассчитываемый коэффициент конкордации (согласованности) мнений экспертов.

Главная задача, решаемая в ходе исследования по данному методу – это получить объективно-точные результаты. Необходимо отметить, что опросные листы должны включать в себя документы в области ИБ: локально-нормативные документы имеющиеся на объекте исследования; отраслевые нормативно-правовые акты и международные стандарты.

Метод Дельфи прост с точки зрения использования математики может использоваться как самостоятельно, так и в комплексе общего процесса оценки СУИБ предприятия. Основное достоинство методики – это независимость оценки экспертов. Однако этот метод сталкивается с рядом сложностей [96]:

а) *Большое количество участников*. При привлечении большого числа экспертов может возникнуть сложность в координации их работы и обработке полученных данных.

б) *Высокая субъективность оценок.* Мнения экспертов могут сильно различаться, что приводит к чрезмерной субъективности результатов. Это

затрудняет достижение консенсуса и объективного решения проблемы.

Таким образом несмотря на то, что метод Дельфи позволяет учитывать мнения многих специалистов, он требует тщательной организации процесса и учета возможных искажений, связанных с субъективными оценками.

В статье Г.А. Евстафьева [46] рассмотрен подход к управлению рисками ИБ с использованием нечётких когнитивных карт и искусственных нейронных сетей. Чтобы учесть все участвующие элементы в обработке данных в автоматизированной системе, и автоматизировать процесс управления рисками предлагается разделить понятие риска на системозависимый и системонезависимый. В этой связи, автор [46] рекомендуют применять нечеткую логику в математическом анализе для оценки риска, связанного с деятельностью предприятия. Такой подход обеспечит точность и быстроту в классификации активов в зависимости от уровня риска [46]. В процессе построения нечетких когнитивных карт (НКК) исследуемый объект изображается в соответствии с рисунком 1.1 в виде знакового ориентированного графа. Сценарий вероятных атак рассматривается на уровне нижнего графа. Уровни верхнего графа используются для учета влияния внешних уязвимостей на предприятие [46].

В работе [46] граф представлен следующим образом: 1 – это множество вершин графа, которые представляют концепты или понятия; 2 – это множество дуг графа, которые отражают причинно-следственные связи между понятиями (концептами); 3 – это множество обозначающие направление связи (+ для положительной связи, – для отрицательной связи); 4 – это множество весовых коэффициентов, которые выражают степень взаимосвязи между концептами по качественной шкале: сильная, слабая, средняя [40].

Анализ рисков на базе НКК позволяет создать адекватную модель воздействия угроз на защищаемые ресурсы, а также оценить последствия реализации угроз ИБ с учетом дефицита и противоречивости исходной информации [24, 46]. Построенная модель позволяет выбрать эффективные меры защиты от информационных угроз и стратегию управления рисками.

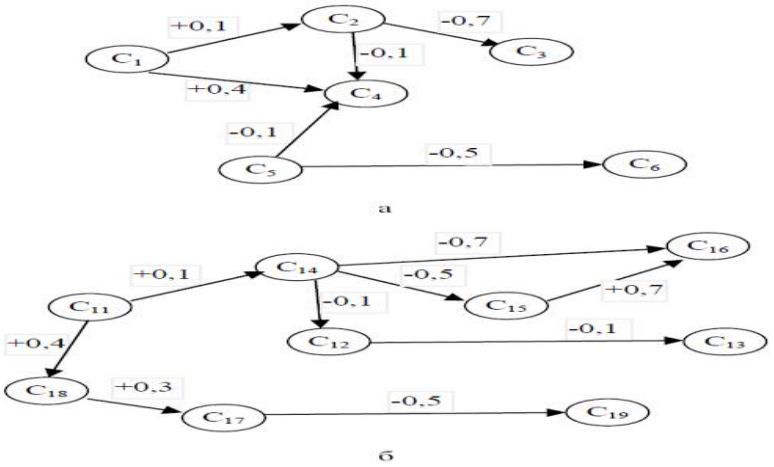


Рисунок 1.1 – Знакового-ориентированный граф: а – граф верхнего уровня, б – граф нижнего уровня

В статье П. В. Плетнева и В. М. Белова «Методика количественного определения рисков ИБ» [115] авторами представлен подход к оцениванию риска в разрезе выбранных актуальных угроз ИБ с учётом вычисления вероятностей реализации угроз; расчета ценности активов в стоимостном выражении; определения коэффициентов организационной и технической незащищённости информации [115]. Необходимо отметить, что рекомендации по оценке риска авторами предлагаются для предприятий малого среднего бизнеса (МСБ). При этом, оценка рисков ИБ применяется в разрезе каждого типа актива. При этом авторы устанавливают ограничение на величину допустимого риска и если его значение превышает указанное значение в 5 %, то необходимо оперативно принимать решение о его снижении.

В статье Е. К. Барановой [16] предлагается два подхода к обоснованию проектирования подсистемы информационной системы (ИС). Первый подход предполагает проверку уровня безопасности ИС на соответствие требований одного из стандартов информационной безопасности. Второй подход предполагает оценку и управление рисками с учетом принципа «разумной достаточности» для обеспечения ИБ. В статье представлена модель на основе графов, в которой отражаются компоненты: объекты защиты, перечень угроз, перечень средств защиты, перечень уязвимостей и барьеров. Компоненты

модели представляются в виде упорядоченных троек. Модель идентифицирует объекты, требующие защиты, оценивает эффективность средств защиты и их вклад в общую безопасность ИБ. Автор предлагает использовать предложенную модель для малых предприятий с полным дублированием для разработки «политики безопасности» или создания КСЗИ.

Современные практические методики также включают CIS RAM (Risk Assessment Method), разработанную Центром интернет-безопасности (CIS). Эта методика ориентирована на предприятия, ищущие методы для оценки рисков и определения защитных мер с учетом отраслевых стандартов и практик [149]. CIS RAM позволяет компаниям выбирать наиболее эффективные способы снижения рисков на основе их бизнес-потребностей и ограничений. Она помогает организациям создавать защитные меры, которые не только соответствуют требованиям безопасности, но и оптимальны с точки зрения затрат.

CIS RAM предлагает пошаговое руководство по оценке рисков, включая определение активов, анализ угроз, оценку уязвимостей и последствий, что позволяет формировать полноценные модели управления рисками в ИБ. Использование CIS RAM также помогает организациям сократить потенциальные убытки, заранее внедряя необходимые меры для минимизации рисков.

В статье «A systematic review of information security risk assessment» авторами Л. Паном и А. Томлинсоном [173] представлен системный обзор более чем 80 научных работ, опубликованных за период с 2004 по 2014 год. В статье акцентируется, что потенциальным направлением исследований могло бы стать сосредоточение внимания на управлении данными в практическом процессе оценки рисков ИБ, а также знание методов для действенного и точного сбора и анализа данных о рисках. Авторы в своей работе выявили проблемы:

– отсутствие обучающих данных или «реальных» данных, что становится актуальной исследовательской проблемой в оценке рисков ИБ;

– проблема в выборе методологии для применения в разных типах организаций.

Необходимо отметить, что применение системного подхода в оценивании и управлении рисков на предприятии позволяет рассмотреть ИБ как неотъемлемую часть всей системы управления организацией. Как отмечает в своей работе Терье Авен [142], системный анализ и методология управления рисками позволяют принимать взвешенные решения, учитывающие вероятность различных сценариев угроз и их влияние на стратегические и операционные цели предприятия [142]. Системный анализ позволяет учитывать сложные взаимосвязи между элементами СЗИ и их роль в общей защите предприятия.

Методики по автоматизированной оценки рисков ИБ можно разделить, как использующие оценку риска с применением качественного (высокий, средний, низкий), количественного и смешенного подхода (количественно-качественный). Выбор методик оценивания должен осуществляться с учетом масштаба и бизнес-процессов предприятия с учетом лучших мировых практик, а также и иметь достаточно детальное описание процессов и требуемых действий.

В статье Е. К. Барановой [17] приведен анализ методик (RiskWatch, CRAMM, ГРИФ, CORAS, MSAT) по оценке рисков и их сравнения. Анализ методик показал, что большинство методик хорошо соответствует критериям по разделам «Риски» и «Процессы» (использование элементов риска). Методики CORAS и CRAMM имеют недостатки по критериям разделов «Мониторинг» и «Управление», а также с многими подразделами «Процессы». Методики MSAT, ГРИФ и RiskWatch предоставляют детальные рекомендации по составлению расписания повторных мероприятий по оценке рисков. Как следует из работы [16] инструмент MSAT («Microsoft Security Assessment Tools») имеет несколько недостатков. Во-первых, отсутствуют готовые рисковые сценарии, что усложняет работу с ним. Процесс управления рисками требует значительных усилий и времени. Кроме того, MSAT недостаточно хорошо адаптирован к особенностям российских компаний, не соответствует требованиям российского законодательства и стандартов. Он также не оценивает эффективность применяемых защитных мер. Методика CORAS рекомендуется к применению на предприятиях среднего масштаба с разовой оценкой уровня риска. Согласно

представленного в [16] CORAS не предусматривает регулярный пересмотр и актуализацию оценок рисков, что может привести к устаревшим данным. Этот инструмент также не позволяет оценить экономическую выгоду от внедрения различных мер безопасности, что затрудняет принятие обоснованных инвестиционных решений. Ещё одной проблемой является отсутствие возможностей для нахождения оптимального баланса между различными стратегиями защиты информации, такими как предотвращение, обнаружение, исправление или восстановление активов. Методика CRAMM рекомендуется по управлению рисками при периодических проверках на техническом уровне. Для использования метода CRAMM, как указывается в работе [16] требуется высокая квалификация аудитора, так как процесс аудита достаточно сложен и требует глубоких знаний. Адаптация этого метода к новым информационным системам также вызывает трудности, поскольку он не всегда легко интегрируется с современными технологиями. Процесс проведения аудита довольно трудоемок, а отчетность сложна для понимания и интерпретации. Одной из проблем является невозможность пользователей модифицировать базу знаний и шаблоны отчетов, что ограничивает гибкость инструмента под конкретные нужды компании. Дополнительно, программное обеспечение доступно только на английском языке, что может создавать барьеры для русскоязычных пользователей. Лицензия на использование CRAMM также весьма дорога. Методика RiskWatch и Microsoft Security Assessment Tool рекомендуется автором для использования на крупных предприятиях на основе регулярных оценок, на которых планируется внедрение системы управления рисками ИБ уровнем не меньше, чем организационный, а также требуется разработка плана мероприятий по их снижению [17, 128]. Однако стоит заметить, что как указано в работе [16] Методика RiskWatch имеет ряд ограничений, а именно: во-первых, она не охватывает организационный и административный уровни обеспечения безопасности, что снижает её эффективность в комплексном подходе к защите информаци [16]. Кроме того, методика не полностью реализует все аспекты защиты информации, упуская важные элементы комплексного подхода. Также

стоит отметить, что используемая в RiskWatch оценка математического ожидания ущерба не всегда точно отражает концепцию риска с системной точки зрения [16].

В статье Л. Ю. Емалетдиновой и И. В. Аникина [47] приведен анализ методологии, методов и частных задач в оценке рисков ИБ по критериям (моделирование объекта защиты; экспертные и/или статистические оценки; учёт различных частных показателей; управление).

В то же время нельзя не отметить, что общей проблемой моделей на основе рисков является известная доля субъективности их вычисления. Это связано с дефицитом необходимой статистики и необходимостью задавать неочевидные показатели.

Таким образом, комплексная оценка рисков и угроз, включающая стандартизированные методы, визуальные модели и практические подходы, помогает предприятиям выстраивать более эффективные системы ИБ, адаптированные к меняющимся условиям внешней среды.

Вместе с тем отметим, ключевую роль в применении в Российской Федерации методики ФСТЭК [100] для определения актуальных угроз, где предлагается использовать качественный подход. Методика предлагает три этапа: 1) этап выявления негативных последствий; 2) этап определения объектов, на которые может быть осуществлено воздействие; 3) этап оценки потенциальной реализации угроз и выявления их актуальности.

С целью создания модели угроз безопасности систем и сетей и последующего обоснования выбора организационно-технических мер по защите информации и выбора средств защиты информации в соответствии с методикой [100] выделяют следующие этапы, влияющие на оценку угроз безопасности информации, а именно: этап создания и этап эксплуатации систем и сетей. В процессе создания систем и сетей необходимо определить сценарии возможных угроз безопасности информации и уровни возможностей нарушителей. Даже один сценарий угрозы достаточен для считать ее актуальной для системы. При эксплуатации систем и сетей эффективность технических мер по защите информации от угроз

определяется через рассмотрение различных сценариев реализации угрозы для каждого нарушителя и его возможностей. В этом процессе используется информация из инвентаризации информационной инфраструктуры, анализа уязвимостей и тестирования с применением автоматизированных инструментов. С выходом методики ФСТЭК были отменены ранее утверждённые ФСТЭК методики [97] и [98]. Достоинство ныне действующей методики ФСТЭК – она доступна в освоении и не требует специальных знаний. Недостатки методики ФСТЭК – это сложность, связанная с проведением оценки актуальности объектов воздействия применительно к конкретной информационной системе, а также сложности, связанной с терминологией, касающейся объектов воздействия, актуализация которых находится в ведении ФСТЭК России. Методика ФСТЭК не применима к оценке угроз безопасности криптографических средств защиты информации.

Методика ФСТЭК [100] применима к оценке антропогенных (действия внешних и/или внутренних нарушителей) угроз безопасности.

Другими не менее значимыми документами в области управления и оценки рисков ИБ являются лучшие практики COSO [153]. В 2017 году вышла COSO 2017 г. «Концептуальные основы управления рисками организации: интеграция со стратегией и управлением деятельностью» [152]. COSO представляет собой набор лучших практик в управлении рисками и не относится по своей сути к разряду стандартов. Стоимость документа варьируется, в зависимости от наличия членства в организации и версии (электронная, бумажная) от 129.99$ до 169.99$. Документ COSO от 2017 в отличие от предыдущей версии 2004 года определяет смещение фокуса с управления рисками различных бизнес-функций на направление проактивного выявления и использования новых возможностей на уровне предприятия. Если COSO от 2004 года использовалась при внедрении интегрированной системы управления рисками, то COSO от 2017 года отражает современный вектор в практике управления рисками.

Ключевые выводы по COSO 2017:

– новая версия COSO ERM устанавливает новые перспективы развития в области управления рисками и их внедрения в процессы стратегического планирования и управления эффективностью предприятия;

– не смотря на изменение базовых аспектов корпоративного управления новая версия COSO остается актуальной и для Российской практики по управлению рисками;

– недостатком COSO, как и прежде остается тот факт, что она не охватывает в полной мере подходы к количественной оценке рисков и альтернативные инструменты визуализации рисков.

Поскольку документ COSO 2017 не доступен для ознакомления по причине вышеизложенного, то приведем оценку угроз согласно COSO 2004. В оценке угроз согласно COSO 2004 используется качественный подход, в основе которого заложены статистические данные и экспертные оценки. Необходимо отметить, что с помощью экспертных оценок рассчитывается ущерб. Ранжирование угроз осуществляется на основе расчетов по всем видам угроз математического ожидания, а также дисперсии. Угрозы определяются на основании анализа наибольшего влияния их параметров на дисперсию.

Достоинства COSO 2004: используются статистические данные и экспертные оценки, а также применяются абсолютные и относительные оценки вероятности угроз ИБ.

Недостатки COSO 2004: число расчетов чрезвычайно велико; если оцениваемый ущерб имеет постоянное значение, то использовать методику COSO [134] нет необходимости.

Кратко отметим стандарт ГОСТ Р ИСО/МЭК 27001-2006 [39]. Стандарт предлагает процессную модель «Планируй-Делай-Проверяй-Действуй». Достоинство стандарта – это контроль системы управления ИБ (СУИБ) на каждом её шаге, в том числе корректировки. Положительные или отрицательные стороны стандарта зависят от выбранного подхода к оценке угроз безопасности информации.

Система оценки рисков является важной составляющей процесса управления

ИБ, так как позволяет прогнозировать возможные угрозы и разрабатывать меры для их предотвращения. Подход, предложенный Хаббардом и Сейерсеном в их книге «How to Measure Anything in Cybersecurity Risk», акцентирует внимание на количественных методах оценки рисков, что позволяет более точно оценивать потенциальные убытки и принимать обоснованные решения на основе данных [159].

Для обеспечения ИБ с точки зрения оценки рисков организаций БС РФ на соответствие требованиям СТО БР ИББС-1.0 применяется методика Банка России [117] которая содержит в себе способы и порядок проведения оценки информационных рисков. Оценка рисков ИБ по данной методике осуществляется экспертами используя качественный подход. По своей сути данный метод носит рекомендательный характер и содержит оценку степени вероятности реализации (СВР) угроз и степени тяжести последствий (СТП) от нарушения ИБ. Выделяют шесть этапов при проведении оценок рисков ИБ: этап сбора информации обо всех информационных активах в разрезе свойств ИБ; этап формирования объектов среды и их сопоставление каждому информационному активу; этап сопоставления источников угроз каждому объекту среды; этап оценки СВР угроз в разрезе потерь свойств ИБ для каждого информационного актива; этап оценки СТП от нарушения ИБ и анализе потерь свойств ИБ для каждого информационного актива; этап подведения итогов по оценке рисков для свойств ИБ для каждого информационного актива с учетом объектов среды и влияния источников угроз ИБ.

Для проведения оценки СВР угроз и СТП ИБ применяются качественные шкалы: минимальная; средняя; высокая; критическая. А суждение «нереализуемая» – применяется дополнительно к перечисленным выше качественным шкалам для СВР угроз.

Перевод в количественный (денежный) формат рисков нарушения ИБ по данной методике необходим для создания резервов на возможные потери от инцидентов ИБ. Для получения количественных оценок СВР угроз и СТП от нарушений ИБ по данной методике прилагаются в табличной форме шкалы

перевода из качественных оценок в количественные.

Расчёт оценки (количественный подход) рисков нарушения ИБ должен проводится с учётом всех свойств информации и при том для каждого информационного актива, т.е. – путем перемножения оценок СВР угроз и СТП от нарушения ИБ. Результирующая оценка риска, влияющая ИБ по всем информационным активам получается, как сумма всех частных оценок рисков в разрезе информационных активов. Принимая во внимание возможные потери за-за инцидентов ИБ согласно методики предлагается осуществлять планирование затрат для формирования резерва. Затраты на резерв рекомендовано формировать исходя из итоговой оценки риска нарушения ИБ, вычисленной по всем информационным активам.

Среди прочего, рассмотрим методику OCTAVE [18]. Суть данной методики построить профиль защиты исходя из перечня мер защиты и структуры (профиля) угроз ИБ, которые влияют на построение профиля защиты. Данный профиль защиты используется для оценки рисков ИБ силами своих сотрудников внутри предприятия и отображается в своей структуре построения, как дерево. Анализ рисков ИБ методики включает восемь процессных шагов: 1) производится оценка риска ИБ и определяется перечень последствий от его реализации в качественном выражении; 2) составляется перечень информационных активов (ИА) с описанием их особенностей, характеристик и стоимости, т.е. их профиля. В связи с чем, устанавливаются требования ИБ к ним и их «границам». Профиль угроз ИБ строится из «дерева вариантов» в котором отражаются следующие компоненты: информационный актив (ИА), тип доступа к ИА; источник угрозы; тип нарушения; результат; описания угрозы ИБ; 3) составляется перечень мест хранения ИА, которые были определены на втором шаге, а также определения уязвимостей для процессов передачи и обработки с целью обеспечения контроля и защиты ИА в направлении ИБ; 4) происходит выявление очевидных угроз ИБ: исходящих от нарушителя, имеющих место быть в сетях передачи данных; возникающих из-за сбоя в работе систем и т.п.; 5) составляется перечень сценариев угроз с использованием дерева решений, где каждая ветвь исследуется

для каждого информационного актива; 6) определение рисков ИБ и как они будут действовать на предприятие или информационный актив. Необходимо отметить, чтобы оценить степень критичности риска его определяют для каждого ИА предприятия; 7) подсчёт относительной оценки возможного ущерба. В связи с чем, это позволяет присвоить приоритеты рискам; 8) предусматривает с учетом приоритета определенных рисков ИБ определение мер безопасности. Согласно проведённого анализа в работе [16] методика OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) обладает несколькими ограничениями. Во-первых, она не предоставляет количественную оценку рисков, что затрудняет точное определение уровня угрозы. Во-вторых, отсутствует доступ к подробным базам знаний, что может ограничить возможности анализа. Наконец, OCTAVE не включает возможность оценки рисков в денежном выражении, что делает сложным сопоставление потенциальных финансовых потерь с уровнем угроз.

В заключении, рассмотрим методику управления рисками ИБ, предложенную компанией Microsoft в 2006 году процесс анализа которой включает четыре этапа: оценки рисков; поддержки принятия решений; реализации контроля; оценки эффективности программы [99].

Методика для каждого из этапов содержит: инструкции; типовые перечни ИА, угроз, уязвимостей; шаблоны документов по управлению рисками ИБ.

Достоинства методики Microsoft [99]: наглядность логики управления рисками ИБ; эффективность управления рисками путём комбинирования качественного и количественного подхода; минимизация трудозатрат и времени на выполнение анализа рисков и их управления; минимизация ошибок; непрерывная актуализация информации о рисках и их управлении; позволяет обосновывать инвестиции для внедрения мероприятий по защите информации; не требует специальных знаний и компетенций исполнителей для анализа и управления рисками.

Недостатки реализации методики Microsoft [99]: требует значительных затрат в связи с высокой трудоемкостью управления рисками ИБ и отсутствием типовых сценариев рисков ИБ.

Методика Microsoft может широко применяться в правительственных, в коммерческих организациях. Методика позволят за некоторое количество итераций осуществить переход от качественной к количественной оценке рисков.

Подводя итог, заметим, однако, что оценки на основе измерения рисков отличаются известной долей субъективности, что не всегда позволяет рассматривать их как единственно возможный подход к оценке защищённости информационных ресурсов.

1.4. Современные подходы к онтологическому моделированию СЗИ

Современные подходы к моделированию СЗИ направлены на повышение точности представления данных, формализацию знаний и оптимизацию процессов управления рисками. Одним из наиболее актуальных инструментов для этого является онтологический подход, который позволяет формализовать знания в ИБ и создать взаимосвязанные модели, способные адаптироваться к изменениям в среде угроз, а именно:

а) Онтологии как метод моделирования СЗИ.

Онтологии играют ключевую роль в построении иерархической и семантически насыщенной модели СЗИ. Определение и структурирование понятий позволяет создать унифицированные термины и взаимоотношения, что упрощает обмен знаниями между системами и специалистами. В этом отношении основополагающей работой является труд Т.Р. Грубера, который предложил подход к созданию переносимых онтологий [158]. Этот подход заложил основы для использования онтологий в ИБ и других областях, требующих формального представления знаний. Эта работа Т.Р. Грубера посвящена подходам к созданию переносимых онтологий, направленных на упрощение обмена знаниями между различными системами искусственного интеллекта (ИИ). Основная цель подхода – разработка общего словаря, который может быть понят и использован различными системами ИИ независимо от их внутренних форматов данных и языков. Введение Ontolingua позволяет преобразовывать определения онтологий,

написанные в стандарте KIF (Knowledge Interchange Format), в формы, которые можно применить в различных системах представления знаний.

Переносимость онтологий является одной из ключевых задач. В разных системах представления знаний участники могут использовать различные языки и подходы. Ontolingua помогает решить эту проблему, обеспечивая перевод на несколько языков, что позволяет обеспечить общий уровень понимания терминов и концепций между агентами.

Значение онтологий для обмена знаниями заключается в их способности формально определять и структурировать данные. Онтологии также способствуют соглашению о содержании знаний, обеспечивая возможность более точного и эффективного взаимодействия между различными системами, даже если у них есть только частичные или несовместимые знания.

Т.Р. Грубер подчеркивает, что онтологические обязательства играют важную роль в процессе взаимодействия агентов, поскольку они фиксируют, каким образом различные системы будут использовать определенные термины. Эти обязательства помогают системам корректно интерпретировать запросы и получать доступ к базам данных, придерживаясь установленной терминологии и аксиом.

Фреймовая онтология в Ontolingua включает детально проработанную аксиоматизацию классов и связей, что позволяет легко интегрировать объектно-ориентированные представления с реляционными подходами.

б) Применение онтологий в управлении и оценке рисков ИБ.

Онтологии позволяют структурировать данные о рисках и угрозах, облегчая разработку методик для их оценки и управления. В частности, модель управления рисками на основе онтологий, предложенная О.Т. Арогундадом и его коллегами, обеспечивает гибкий способ идентификации и анализа рисков в информационных системах [141]. Использование онтологических моделей помогает не только систематизировать данные о рисках, но и обеспечивает более точную адаптацию к новым угрозам, что особенно важно для современных СЗИ. В статье представлена модель управления рисками безопасности, которая поддерживает

полный жизненный цикл защиты информационной системы (ИС). Модель обеспечивает постоянный сбор данных о выявленных угрозах через систему обнаружения вторжений (IDS), их фильтрацию и анализ в реальном времени. Важные заинтересованные стороны, такие как администратор безопасности, менеджеры и сама система управления безопасностью, участвуют в оценке и повторной проверке выбранных контрмер. Используется агент-пробоотборник, который классифицирует угрозы с помощью базы знаний на основе онтологии, а вероятность возникновения угроз рассчитывается с использованием долгосрочной статистики. Для анализа угроз применяется метод рассуждений на основе прецедентов, а повторная оценка контрмер проводится с учетом вероятности успеха текущих угроз. Модель помогает руководству принимать обоснованные решения о мерах безопасности, чтобы оптимизировать инвестиции в защиту ИС. Принцип работы модели, охватывающий этапы «сбор – проверка – анализ – обоснование – переоценка», продемонстрирован на примере системы электронного банкинга.

В работе А.Г. Массель и Д.А. Гаськовой «Онтологический инжиниринг для разработки интеллектуальной системы анализа угроз и оценки рисков кибербезопасности энергетических объектов» [91] представлены результаты использования онтологического инжиниринга для создания интеллектуальной системы анализа угроз и оценки рисков для кибербезопасности энергетических объектов. Были разработаны онтологии для каждой части системы, которые структурируют знания о рисках и угрозах, способных вызвать критические ситуации в энергетике.

Основные элементы онтологий включают понятия, связанные с кибербезопасностью в энергетике, актуальные угрозы, классификацию рисков и сценарии возникновения экстремальных ситуаций. Эта онтологическая модель интегрирует ключевые области знаний: энергетическую безопасность, кибербезопасность, сценарное планирование и управление рисками.

В результате разработанное онтологическое пространство позволяет систематизировать экспертные знания и применять их в интеллектуальной

системе для анализа киберугроз и оценки рисков в энергетическом секторе.

в) Онтологии для соблюдения стандартов ИБ.

Для выполнения требований стандартов ИБ, таких как ISO 27002, также может использоваться онтологический подход. В работе С. Фенца и Т. Нойбауэра [156] предложен способ использования онтологий для автоматизации процесса выбора контролей безопасности в соответствии с требованиями ISO 27002. Подход позволяет системам предприятия адаптироваться к изменениям в стандартах и автоматизировать процесс оценки соответствия, что ведёт к повышению эффективности в оценивании соблюдения нормативных требований безопасности и в принятии решения по выбору мер защиты, тем самым стремясь к минимизации затрат.

Исследование [156] направлено на разработку системы поддержки принятия решений для управления информационной безопасностью (ИБ) и оценки соответствия требованиям стандарта ISO 27002. Методология основывается на принципах проектной науки и использует онтологии для формализации элементов управления ИБ, автоматического определения статуса соответствия, уровня рисков и выявления недостающих контрмер.

Преимущества онтологий заключаются в возможности автоматизировать проверку соответствия и интеграции с программными решениями для управления рисками. Это позволяет упростить процессы инвентаризации и визуализации активов, а также оптимизировать выбор контрмер.

Система построена на базе знаний, включающей стандарты ISO 27002 и принципы управления ИБ, которая позволяет автоматически анализировать активы, риски и меры противодействия. На практике это обеспечивает пользователю рекомендации по снижению рисков и выбору необходимых контрмер. Прототип системы был протестирован в компании среднего размера в Австрии, что показало экономическую эффективность и актуальность подхода. В дальнейшем предполагается расширение методологии для различных стандартов ИБ и отраслей.

Выводы исследования подчеркивают, что система поддержки принятия

решений облегчает выбор контрмер, автоматически создавая оптимальные портфели для снижения рисков и затрат.

г) Онтологическое управление доступом.

В условиях распространения облачных технологий возникает потребность в более гибких и интеллектуальных моделях контроля доступа. В этом контексте онтологический подход также оказывается полезным, позволяя создавать адаптивные модели доступа. Например, Чой и его коллеги разработали модель управления доступом на основе онтологий, которая позволяет управлять политиками безопасности в облачных средах с учетом изменяющихся условий [148]. Эта модель улучшает способность систем безопасности адаптироваться к изменениям в конфигурации и политике доступа, обеспечивая динамичное управление правами пользователей.

д) Онтологические модели для киберфизических систем.

Киберфизические системы требуют особого подхода к моделированию, поскольку они объединяют физические объекты и цифровые компоненты. Онтологическая модель, представленная А.М. Шаабаном и его коллегами, служит основой для инструментов безопасности, ориентированных на критические киберфизические системы [140]. Этот подход позволяет учесть специфику взаимодействия физических объектов и цифровых систем, повышая устойчивость системы к кибератакам и обеспечивая надежность в условиях критически важной инфраструктуры.

Необходимо отметить, что исследованию роли онтологий в обеспечении информационной безопасности посвящена научная работа Крунослава Арбанаса и Мирко Чубрило под названием «Онтология в информационной безопасности» [172]. Основная идея работы авторов заключается в том, что информация становится все более важным активом, требующим надежной защиты, поэтому системы управления информационной безопасностью должны учитывать разные уровни (оперативный, тактический и стратегический).

Основные положения работы:

а) Значение информационной безопасности. Авторы подчеркивают важность

защиты информации с точки зрения поддержания непрерывности бизнес-процессов от различных угроз, таких как перехват, изменение, прекращение передачи, создание ложной информации или уничтожение данных.

б) Роль онтологий. В работе авторов подчёркивается роль онтологий в формализации знания в области информационной безопасности, обеспечивая тем самым точную и структурированную базу данных об угрозах, методах защиты и других аспектах безопасности, что соответственно помогает администраторам лучше управлять системой безопасности.

в) *Классификация онтологий безопасности.* В работе авторов рассматриваются публикации за период с 2004 по 2014 годы в разрезе трёх категорий:

– общие онтологии безопасности,

– специфические онтологии (например, для определенных типов атак),

– теоретические работы.

г) Эволюция информационной безопасности и роль онтологий.

Отмечается рост числа конференций и публикаций по вопросам безопасности, а также то, что онтологические подходы способствуют интеграции знаний и поддержке обмена ими.

д) Организационные аспекты информационной безопасности.

В работе авторов отмечается, что онтологии играют важную роль в управлении знаниями внутри организаций, помогая улучшить коммуникацию и обеспечить лучшее понимание сложных аспектов ИТ-инфраструктуры.

е) Терминологическая проблема.

В работе авторами определяется одна из ключевых проблем в сфере информационной безопасности – это отсутствие четкой терминологической базы, что затрудняет взаимодействие специалистов разных уровней. По мнению авторов онтологии решают эту проблему, предоставляя точные определения терминов и связей между ними.

ж) Компоненты онтологических моделей.

Авторами рассматриваются такие элементы, как понятия, отношения,

аксиомы, свойства и экземпляры, а также таксономии, которые используются для классификации и организации понятий.

з) Обзор существующих работ.

В работе авторов приводится обзор литературы, включая работы авторов, предложивших классификации и систематизации онтологий, а также систематический обзор онтологического подхода в информационной безопасности.

и) Практическое применение онтологий.

Авторы отмечают, что успешная интеграция знаний через общую онтологию требует широкой дискуссии и достижения консенсуса среди экспертов.

Таким образом, авторы акцентируют внимание на важности онтологический подходов в информационной безопасности для повышения эффективности управления ИБ и улучшения взаимодействия между специалистами.

1.5. Финансирование информационной безопасности

Среди работ российских учёных, исследующих вопросы оценки финансовых затрат на построение средств защиты информации с помощью системы поддержки принятия решений, выделяется работа А.П. Жука, Д.Л. Осипова и А.А. Гавришева [50]. В данной работе рассматривается проблема оценки финансовых затрат на создание средств защиты информации с использованием систем поддержки принятия решений. Исследователи отмечают, что существующие системы часто либо не включают подсистемы для расчета таких затрат, либо используют сложные математические методы, что затрудняет их практическое применение. Авторы предлагают новый метод оценки финансовых расходов на разработку средств защиты, включая технические системы охраны, основанный на теории игр. Разработанный метод позволяет учитывать специфику этих систем и минимизировать затраты при заданной стоимости защищаемой информации. На базе данного метода предлагается структура системы поддержки принятия решений, которая способна предоставлять рекомендации лицам, ответственным за принятие управленческих решений.

Использование онтологического подхода в моделировании СЗИ позволяет создать более точные и адаптируемые модели для управления информационной безопасностью и с финансовой точки зрения. Онтологии помогают формализовать и структурировать знания в области ИБ, обеспечивая целостный подход к управлению ИБ и соответствию стандартам.

1.6. Выводы по главе

В первой главе работы выполнен системный анализ предметной области, касающейся оценки эффективности функционирования СЗИ от различных угроз. Исследование включает изучение методов, методик, стандартов и моделей, применяемых для оценки информационных рисков и управления информационной безопасностью (ИБ) на предприятии. Анализ показал, что существующие методики имеют особенность – они ориентированы на оценку рисков с использованием экспертных методов, которые характеризуются известным субъективизмом при недостатке статистических данных. Более того, отсутствует системообразующая модель, способная дать ответ на вопрос, как снизить влияние субъективных факторов на оценку эффективности СЗИ. В ходе анализа были выявлены важные показатели ИБ, применяемые к оценке рисков, зрелости, бенчмаркингу (контрольных точек и эталонов), процессов мониторинга производительности, обеспечению целостного управления кибербезопасностью. Для корректного использования показателей ИБ в контексте повышения эффективности СЗИ и непрерывной ее работы рассмотрен системный подход с использованием онтологического моделирования. Анализ современных подходов к онтологическому моделированию СЗИ показал значимость онтологий как инструмента для унификации терминологии, структурирования данных предметной области, а также интеграции знаний между системами и экспертами. В главе также обоснована роль онтологий в повышении точности анализа, автоматизации управления безопасностью и принятия решений, что способствует снижению затрат и влияния субъективных факторов.

Глава 2. Структурный анализ системы ИБ предприятия

Сегодня ИС играют важную роль в производственной деятельности предприятия, относящихся к объектам критической информационной инфраструктуры. Использование ИС для хранения, обработки и передачи информации приводит к актуальной проблеме защиты этих систем, особенно в свете растущего числа информационных атак, которые причиняют значительные финансовые и материальные убытки. Чтобы эффективно защитить ИС предприятия, необходимо объективно оценить уровень их защищенности и принять соответствующие решения по организации и обеспечению системы информационной безопасности (СИБ) предприятия. Недостаток сегодня известных методик в области оценки уровня защищённости ИС связан с известной долей субъективизма, вызванной возможным дефицитом статистики, необходимой для оценки вероятности соответствующих событий. В связи с чем, существует потребность в разработке системообразующего подхода к анализу предметной области, в качестве которого предлагается онтологическое моделирование. Предполагается, что это также может способствовать снижению вклада субъективных оценок на вычисление эффективности СЗИ и принятие решений по их совершенствованию. В долгосрочной перспективе может потребоваться создание комплексной системы защиты информации (КСЗИ) для минимизации возможных ущербов. В виду того, что КСЗИ являет собой очень сложную структуру, мы будем рассматривать оценку эффективности КСЗИ на примере одной из ее основных составляющих – системы программно-технических средств защиты информации (ПТСЗИ). Для составления базы знаний по КСЗИ проведен анализ открытых источников информации по объектам КИИ [2, 43, 44, 57, 58, 81, 106, 111, 133, 135].

В данной главе будет предложен онтологический подход к агрегированному оцениванию. Онтологический подход здесь основывается на структурировании предметной области с помощью легких онтологий и последующей обработке

числовых показателей, характеризующих связи между концептами предметной области, с целью получения агрегированного итогового показателя.

Анализ процесса управления и оценки ИБ предприятия выявил ключевые технические решения, направленные на минимизацию ущерба, вызванного информационными рисками. В этом контексте предлагается создание СИБ как части КСЗИ. Программно-технические решения играют центральную роль в этой системе, дополняя существующую систему менеджмента ИБ (СМИБ) предприятия. Однако, существует значительная проблема в данной области исследований – сложность, плохая структурированность и трудная формализуемость процесса СМИБ в контексте СИБ. В этой связи онтологические модели призваны помочь экспертам по ИБ и руководству предприятий рассматривать задачу управления ИБ с системной точки зрения и найти отправную точку для принятия управленческих решений. Это включает оценку эффективности программно-технических средств защиты информационной системы предприятия в рамках комплексной оценки состояния системы ИБ.

2.1. Онтологическая модель системы управления информационными потоками на предприятии

Отсутствие объективной информации о находящихся в промышленной эксплуатации на предприятии информационных системах, средствах защиты информации и инженерно-технической защиты, а также о внедряемых решениях различных производителей как в области АСУ ТП, так и в ИТ-инфраструктуре влияет на принятие решения руководством в области обеспечения ИБ. В результате, возникает потребность в актуальной информации об объектах и процессах предприятия, а также их взаимосвязях и влиянии на уровень защищенности предприятия. Для решения этой задачи в рамках диссертационного исследования предлагается использовать такой метод

системного анализа как построение онтологических моделей и использование концепт-карт.

В исследованиях авторов, охватывающих сферу информационной безопасности, были проведены анализ и изучение различных аспектов, включая фактографические системы и кибербезопасность сетей связи транспортных средств [83, 86]. Тем не менее, внимание, уделенное автоматизированным средствам информационной безопасности [53, 54], не всегда сопровождалось достаточным освещением методов системного анализа и системного подхода в данной области.

Однако в одной из исследовательских работ [86], проведенной с применением принципов системного анализа и системного подхода [5, 26, 27, 49], были представлены специфические показатели, связанные с оценкой эффективности инструментов информационной безопасности и фактографических информационных систем. Иные исследования [85, 87, 125, 126] подчеркнули потенциал системного анализа в области информационной безопасности. В исследованиях [19, 84, 88, 102-104, 163] были рассмотрены разнообразные показатели. В частности, стандарт ISO/IEC TR 27016 [163] выступает в качестве ценного инструмента для оценки эффективности средств информационной безопасности, особенно с учетом экономических и стоимостных аспектов.

Современные подходы к формализации систем охватывают разнообразные методы и инструменты [106]. Одним из наиболее тщательно изученных подходов является математическое моделирование, которое позволяет описать количественные взаимосвязи между компонентами системы, ее внешней средой и целями функционирования [106]. Однако такой подход применим только для относительно простых систем или их фрагментов. В более сложных случаях, особенно когда процессы развиваются случайно, эффективным оказывается имитационное моделирование [89, 138] и его подвид – агентное моделирование [21, 59, 127]. Агентное моделирование предполагает имитацию поведения системы путем моделирования поведения ее фрагментов, таких как агенты, и их

взаимодействия, а анализ поведения системы в целом осуществляется на основе модели [106].

В случаях, когда система обладает слабой структурированностью и трудно поддается формализации, что типично для многих управленческих задач, применяется качественное моделирование, основанное на знаниях [22, 92, 122]. Также используется агрегатное моделирование, которое позволяет описать характеристики системы в целом на основе характеристик ее составных частей [7-9].

Одним из интересных подходов в знаниевом моделировании является моделирование с использованием онтологий [92, 122]. Онтологии представляют собой формальные модели, которые описывают понятия и отношения в определенной области знаний, позволяя более точно и систематически представлять знания и взаимосвязи между ними [106].

Каждое из указанных понятий имеет свои уникальные функции, выполняемые в системе управления информационной безопасностью. Взаимосвязь между ними обеспечивает комплексный подход к обеспечению безопасности информационных ресурсов и эффективное функционирование системы ИБ.

Концепты и их взаимосвязи должны учитывать, как объекты защиты – ИС, обрабатывающие конфиденциальную информацию, персональные данные (ИСПДн) и автоматизированные системы управления технологическими процессами (АСУ ТП).

Для обеспечения безопасности информационных систем, особенно в случаях, когда они обрабатывают конфиденциальную информацию с повышенными требованиями к безопасности (ПТБ), необходимо уделять внимание автоматизированным рабочим местам (АРМ) и АСУ ТП. Эти рабочие места, известные как АРМ ПТБ, должны быть оснащены соответствующими мерами защиты, которые гарантируют надежность и конфиденциальность передаваемой информации.

На основании проведенного анализа литературы [31] с учетом стандарта ГОСТ Р ИСО/МЭК 15408-1-2012 [38], в диссертации был разработан состав концептов, описывающих внутренние угрозы информационной безопасности предприятий, и их взаимосвязи, а также определено влияние этих угроз на возможный ущерб предприятия. На основе этого анализа была построена онтологическая модель в соответствии с рисунком 2.1 [31]. Данная модель может быть адаптирована и применена в различных предметных областях исследований, а также в области принятия управленческих решений по вопросам информационной безопасности.

Принимая во внимание работу [31], разработана онтологическая модель, которая представлена на рисунке 2.1. Просматривается влияние на расчет возможного ущерба (оценки суммарных издержек) следующих составляющих характеристик: количество рисков (угроз) для каждого информационного актива в разрезе основных свойств информации (конфиденциальность, целостность, доступность) по каждому информационному активу.

Некоторые методики фокусируются на оценке ущерба, связанного с автоматизированными системами или информационными ресурсами [80]. Они применяются в случаях, когда важно определить потери, связанные с недоступностью или повреждением систем. Однако эти методики не учитывают другие аспекты, такие как правомерность доступа и утечки персональных данных, которые также могут привести к серьезным последствиям для предприятия.

В то же время, некоторые подходы ориентированы на оценку ущерба от реализации угроз, связанных с неправомерным доступом и использованием утечки персональных данных. Эти подходы включают в себя не только материальные потери, но и штрафы за нарушение законодательства и затраты на восстановление информационных ресурсов [129]. Они обеспечивают более полное представление о возможных последствиях, однако также не учитывают все аспекты информационной безопасности.

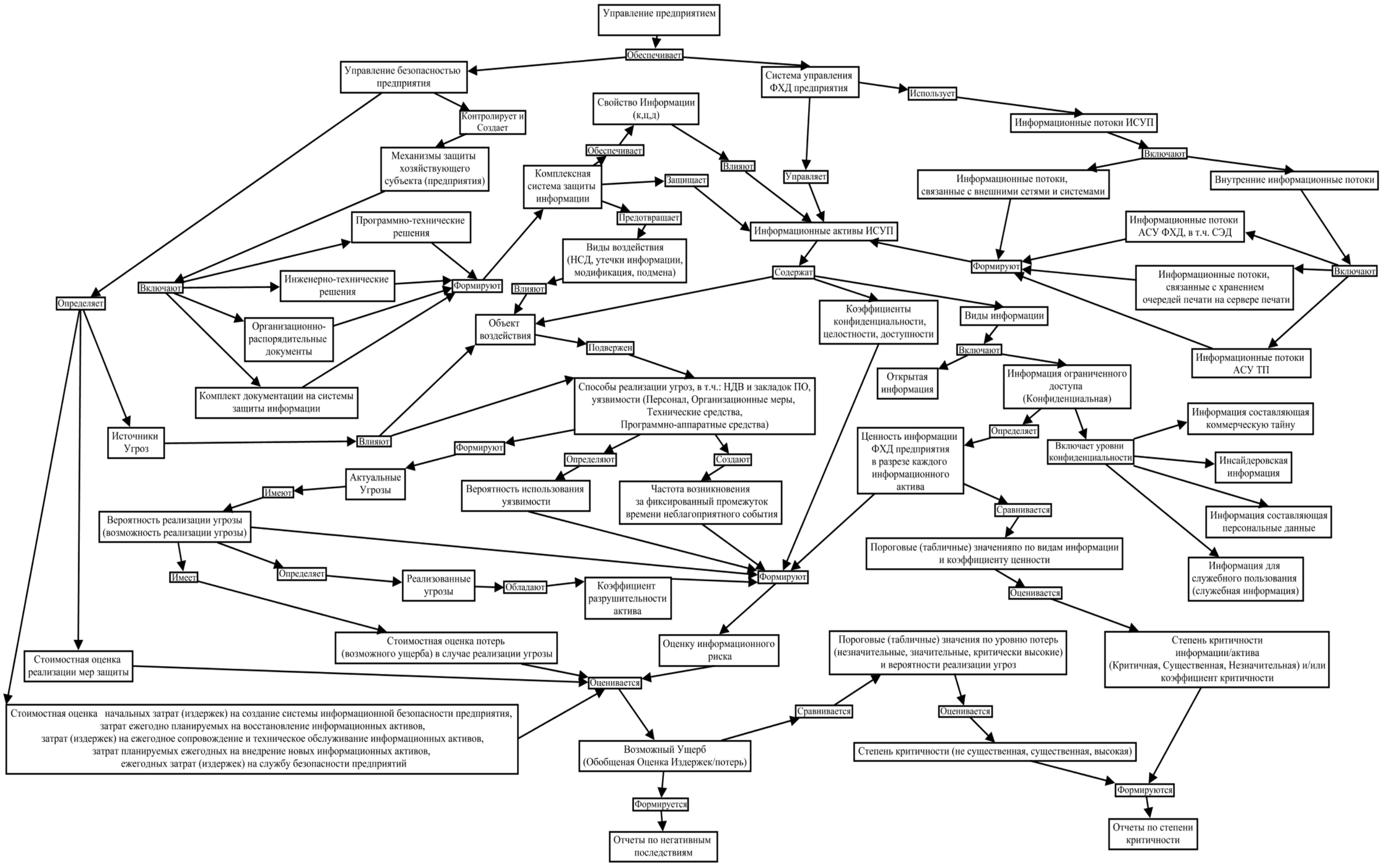


Рисунок 2.1 – Онтологическая модель взаимосвязи основных концептов в процессе управления информационной безопасностью предприятия

В соответствии с рисунком 2.1 отражены концепты и взаимосвязи, которые играют важную роль в определении перечня негативных последствий и оценке степени критичности информации для предприятия. В соответствии с исследованиями [32, 33, 81, 133, 162], степень критичности информации для предприятия определяется на основе следующих факторов:

– ценность информации в целом для предприятия, учитывая ее вид и ограничения доступа. Это позволяет определить, насколько важна информация для предприятия и какие меры необходимо предпринять для ее защиты;

– потенциальный ущерб от утраты информации, связанный с вероятностью реализации угроз. Это позволяет оценить возможные негативные последствия для предприятия.

Определение негативных последствий для предприятия осуществляется путем анализа взаимосвязи концептов, влияющих на определение возможного ущерба. Это позволяет учесть риски информационной безопасности для каждого информационного актива предприятия.

Для более точного определения степени критичности информации для предприятия, необходимо учитывать процедуру оценки рисков и их характеристик, как указано в исследовании [31]. Это помогает предприятию понять масштаб рисков и принять соответствующие меры по обеспечению информационной безопасности.

Стоит отметить, что данная онтологическая модель является важным инструментом для анализа и понимания информационной безопасности предприятия. Она позволяет учесть различные факторы, влияющие на определение перечня негативных последствий и оценку степени критичности информации. Использование такой модели позволяет принимать обоснованные управленческие решения и применять соответствующие меры для обеспечения безопасности предприятия, а именно:

– в направлении идентификации и анализа информации и объектов защиты, а также их ценности для целей и задач деятельности предприятия. Этот этап

позволяет определить, какие данные и ресурсы требуют особой защиты, и насколько важны они для успешной работы предприятия;

– в направлении идентификации угроз безопасности информации, мер обеспечения ИБ, уязвимостей, нарушителей ИБ предприятия, неблагоприятных событий за фиксированный промежуток времени и эффективности применяемых мер защиты;

– в направлении процесса обработки рисков ИБ информации (снижение, сохранение, предотвращение и перенос (страхования)).

Важно отметить, что в данном исследовании предлагается анализировать возможность реализации угроз безопасности в отношении различных информационных активов предприятия. Это позволяет учесть особенности каждого актива и применить соответствующие меры защиты. Таким образом, в результате определения негативных последствий и оценки степени критичности информации для предприятия может быть проведен анализ критичности информации и/или объекта защиты, а также учтены базовые требования к выявлению актуальных угроз безопасности и уязвимостей [31]. Это позволяет предприятию разработать эффективную стратегию по обеспечению информационной безопасности и принять соответствующие меры.

Идентификация информации и объектов защиты, их ценности для целей и задач деятельности, позволяет предприятию определить, какие данные и ресурсы являются наиболее значимыми, требующими особой защиты. Это важно для того, чтобы выделить ресурсы (материальные и/или денежные) и установить соответствующие меры по обеспечению их безопасности.

Таким образом, результаты анализа критичности информации и/или объектов защиты, учета базовых требований и угроз безопасности, являются основой для разработки стратегии обеспечения информационной безопасности предприятия. Это позволяет предпринять соответствующие меры по защите информации и ресурсов, минимизировать негативные последствия ИБ и обеспечить стабильную и безопасную работу предприятия.

2.2. Онтологическое моделирование программно-технической системы защиты информации (ПТСЗИ)

В условиях производственной деятельности предприятия информация рассматривается, как ценный информационный актив. Воздействие на информацию, такое как ее разрушение или хищение, подчеркивает необходимость защиты информации как актуальной задачи в обеспечении безопасности информационных активов, включая автоматизированные управляющие системы технологическим процессом.

2.2.1. Основные задачи разработки легких онтологий ПТСЗИ

При разработке модели прототипа онтологии ПТСЗИ предприятия решаются задачи:

– защита информации и средств её обработки от несанкционированного доступа;

– защита персональных данных в соответствии с законодательством Российской Федерации;

– защита информационных ресурсов от внешних программно-технических воздействий;

– контроль информационных потоков и их содержания;

– защита информации в прикладных информационных системах;

– защита от вредоносного кода.

Разрабатываемая модель имеет целью обеспечить надежную и эффективную защиту информационных активов предприятия и обеспечить соблюдение требований безопасности информации. Методика разработки модели основана на применении онтологического подхода и учете специфики предметной области. Результаты исследования могут быть использованы при создании прототипов и последующей реализации систем защиты информации на других предприятиях.

Защита информации на предприятии должна быть обеспечена на всех этапах обработки и во всех режимах функционирования информационных систем (ИС) и автоматизированных систем управления технологическим процессом (АСУ ТП). Важно учитывать, что на уровне ПТСЗИ необходимо использовать сертифицированные средства защиты информации, рекомендованные регуляторами в области информационной безопасности (ИБ).

При разработке отдельных элементов онтологий и самого прототипа онтологической модели ПТСЗИ, необходимо учитывать, чтобы они не должны препятствовать достижению целей информационных систем на предприятии и их нормальному функционированию. Разработка прототипа онтологической модели системы ПТСЗИ и онтологических моделей ее компонент должна соответствовать техническому заданию на создание ПТСЗИ и отвечать общим требованиям к ПТСЗИ в целом, включая соответствующее техническое задание на создание ПТСЗИ.

Прототип онтологии ПТСЗИ должен быть разработан с учетом онтологических моделей входящих в неё компонент и взаимосвязей между ними для выполнения функций, направленных на выявление, блокирование, минимизацию актуальных угроз и в дальнейшем обеспечить соответствие структуры системы защиты информации на предприятии требованиям законодательных и нормативно-правовых актов по информационной безопасности.

Основные компоненты прототипа онтологии ПТСЗИ — объекты защиты, комплексы средств защиты информации, подсистемы и их функции.

2.2.2 Онтологический подход в моделировании ПТСЗИ

Онтологическая модель ПТСЗИ выполняет ключевую роль в процессе агрегированного оценивания эффективности функционирования данной системы. Определяемые далее в рамках построения онтологической модели концепты

(например, подсистемы защиты, функции контроля доступа, антивирусной защиты и др.) и их взаимосвязи служат основой для выбора показателей оценки. Это позволяет структурировать процесс измерения эффективности на всех уровнях системы, а также минимизировать влияние субъективных факторов за счёт формализации взаимосвязей между компонентами.

Для построения прототипа онтологической модели ПТСЗИ в процессе управления ИБ хозяйствующего субъекта для объектов защиты (системы хранения данных, серверы СрЗИ, активное сетевое оборудование, автоматизированные рабочие места (с повышенными требованиями к безопасности; автоматизированных систем и др.), серверы и др.) определены, как представлено в таблице 2.1, концепты ПТСЗИ предприятия и их основные функции.

Здесь комплексы К1, … К15 являются сложными и могут быть разделены на составляющие, однако в данном контексте они рассматриваются как функциональные элементы [106]. Это: К1 (комплекс встроенных средств защиты серверов и автоматизированных рабочих машин (АРМ) под управлением операционных систем (ОС) семейства Windows); К2 (комплекс антивирусной защиты); К3 (комплекс резервного копирования); К4 (комплекс защиты среды виртуализации); К5 (комплекс сбора, анализа и корреляции событий ИБ); К6 (комплекс встроенных средств АСО); К7 (комплекс резервного копирования конфигурационных файлов АСО); К8 (комплекс межсетевого экранирования); К9 (комплекс обнаружения вторжений); К10 (комплекс встроенных средств защиты систем хранения данных); К11 (комплекс централизованного управления СрЗИ); К12 (комплекс анализа защищенности); К13 (комплекс контроля целостности); К14 (комплекс встроенных средств защиты прикладного программного обеспечения (ППО)); К15 (комплекс контроля использования информационных ресурсов) [106].

Таблица 2.1 – Основные концепты ПТСЗИ предприятия и их функции в разрезе объектов защиты

№ п.п.	Объекты защиты	Наименование функции (действия)	Наименование концепта	Наименование функции (действия)	Наименование концепта
1.	Автоматизированное рабочее место с повышенными требованиями к безопасности (АРМ ПТБ), АРМ автоматизированной системы, обрабатывающей конфиденциальную информацию и/или персональные данные (АРМ АС), АРМ автоматизированной системы управления технологическим процессом (АСУ ТП), АСО, Серверы средств защиты информации (СрЗИ), Серверы АС, Серверы АСУ ТП, система хранения данных (СХД)	Контроль и управление доступом к защищаемым информационным ресурсам (А1), контроль и управление доступом к внешним носителям информации и периферийным устройствам (А2)	Подсистема контроля и управления доступом (П1)	Аудит и мониторинг использования информационных ресурсов, контроль доступа, регистрация событий, управление правами, управление установкой обновлений и исправлений сертифицированных версий ОС семейства Windows на серверах и АРМ.	Комплекс встроенных средств защиты серверов и автоматизированных рабочих машин (АРМ) под управлением операционных систем (К1)
				Мониторинг и аудит доступа к информационным ресурсам, настройка ограничений по типам файлов и использованию ресурсов, аудит использования информационных ресурсов.	Комплекс контроля использования информационных ресурсов (К15)
		Контроль и управление доступом к защищаемым информационным ресурсам (А1).		Регистрация событий доступа к средствам управления виртуальной инфраструктурой, ограничение доступа к виртуальным машинам (ВМ), контроль консоли ВМ.	Комплекс защиты среды виртуализации (К4)
				Контроль целостности данных, обеспечение защиты ПО от несанкционированного доступа: 1) контроль и управление доступом к серверам и АРМ; 2) регистрация и учет событий доступа к серверам и АРМ; 3) получение и распространение сертифицированных обновлений ПО производства Microsoft; 4) контроль целостности исполняемых файлов системного ПО.	Комплекс встроенных средств защиты систем хранения данных (К10)
				Обеспечение защиты ПО от несанкционированного доступа: 1) контроль и управление доступом к серверам и АРМ; 2) регистрация и учет событий доступа к серверам и АРМ; 3) получение и распространение сертифицированных обновлений ПО производства Microsoft; 4) контроль целостности исполняемых файлов системного ПО.	Комплекс встроенных средств защиты прикладного программного обеспечения (ППО) – К14

№ п.п.	Объекты защиты	Наименование функции (действия)	Наименование концепта	Наименование функции (действия)	Наименование концепта
		Контроль и управление доступом к защищаемым информационным ресурсам (А1), контроль доступа к активному сетевому оборудованию (АСО) (А3)		Фильтрация сетевого трафика, блокировка несанкционированных соединений.	Комплекс межсетевого экранирования (К8)
		Контроль доступа к активному сетевому оборудованию (АСО) (А3)		Управление активным сетевым оборудованием.	Комплекс встроенных средств активного сетевого оборудования (АСО) – К6
2.	АРМ ПТБ, АРМ АС, АРМ АСУ ТП, АСО, Серверы АС, Серверы АСУ ТП, Серверы СрЗИ, СХД	Регистрация и учет действий пользователей и процессов (Б1), регистрация событий доступа к внешним устройствам и портам ввода-вывода (Б2).	Подсистема регистрации и учета (П2)	Аудит и мониторинг использования информационных ресурсов, контроль доступа, регистрация событий, управление правами, управление установкой обновлений и исправлений сертифицированных версий ОС семейства Windows на серверах и АРМ.	Комплекс встроенных средств защиты серверов и автоматизированных рабочих машин (АРМ) под управлением операционных систем (К1)
				Мониторинг и аудит доступа к информационным ресурсам, настройка ограничений по типам файлов и использованию ресурсов, аудит использования информационных ресурсов.	Комплекс контроля использования информационных ресурсов (К15)
		Регистрация и учет действий пользователей и процессов (Б1)		Защита от вредоносного ПО, проверка файлов и процессов, обновление версий клиентского ПО, сигнатур.	Комплекс антивирусной защиты (К2)
				Регистрация событий доступа к средствам управления виртуальной инфраструктурой, ограничение доступа к виртуальным машинам (ВМ), контроль консоли ВМ.	Комплекс защиты среды виртуализации (К4)

№ п.п.	Объекты защиты	Наименование функции (действия)	Наименование концепта	Наименование функции (действия)	Наименование концепта
				Сбор событий безопасности — сбор и накопление событий безопасности, генерируемых различными элементами системы, такими как серверы, сетевые устройства, средства защиты информации и другие источники. Анализ событий — анализ собранных событий с целью выявления подозрительной или аномальной активности, которая может свидетельствовать о возможной угрозе информационной безопасности. Корреляция событий — сопоставление и объединение отдельных событий в более значимые инциденты, что позволяет лучше понять контекст происходящего и выявить сложные атаки. Обнаружение инцидентов — определение и классификация инцидентов информационной безопасности на основании проанализированных и коррелированных событий. Оповещение и уведомление — генерация предупреждений и уведомлений о выявленных инцидентах для своевременного реагирования и принятия мер по их устранению. Архивирование и хранение — долгосрочное хранение собранных и обработанных событий для дальнейшего анализа и расследования инцидентов. Генерация отчетов — создание отчетов о событиях безопасности и инцидентах для внутреннего использования, отчетности перед регулирующими органами или руководством.	Комплекс сбора, анализа и корреляции событий информационной безопасности (ИБ) – К5
				Управление активным сетевым оборудованием.	Комплекс встроенных средств активного сетевого оборудования (АСО) – К6

№ п.п.	Объекты защиты	Наименование функции (действия)	Наименование концепта	Наименование функции (действия)	Наименование концепта
				Фильтрация сетевого трафика, блокировка несанкционированных соединений.	Комплекс межсетевого экранирования (К8)
				Мониторинг активности, предотвращение атак, сбор, запись и хранение зарегистрированных событий безопасности в течение установленного времени хранения.	Комплекс обнаружения вторжений (К9)
				Контроль целостности данных, обеспечение защиты ПО от несанкционированного доступа: 1) контроль и управление доступом к серверам и АРМ; 2) регистрация и учет событий доступа к серверам и АРМ; 3) получение и распространение сертифицированных обновлений ПО производства Microsoft; 4) контроль целостности исполняемых файлов системного ПО.	Комплекс встроенных средств защиты систем хранения данных (К10)
				Проведение регулярных проверок на наличие уязвимостей в системах, анализ защищенности информационных ресурсов, оценка рисков и разработка рекомендаций по устранению уязвимостей.	Комплекс анализа защищенности (К12)
				Выявление несанкционированных изменений в данных и системах, контроль целостности исполняемых файлов системного ПО, контроль настроек встроенных средств защиты ОС семейства Windows серверов и АРМ на соответствие их сертифицированным конфигурациям.	Комплекс контроля целостности (К13)
				Обеспечение защиты ПО от несанкционированного доступа: 1) контроль и управление доступом к серверам и АРМ; 2) регистрация и учет событий доступа к серверам и АРМ; 3) получение и распространение сертифицированных обновлений ПО производства Microsoft; 4) контроль целостности исполняемых файлов системного ПО.	Комплекс встроенных средств защиты прикладного программного обеспечения (ППО) – К14

№ п.п.	Объекты защиты	Наименование функции (действия)	Наименование концепта	Наименование функции (действия)	Наименование концепта
3.	АРМ ПТБ, АРМ АС, АРМ АСУ ТП, Серверы АС, Серверы АСУ ТП, Серверы СрЗИ	Контроль целостности исполняемых и конфигу-рационных файлов СрЗИ, компонентов ОС и при-кладного ПО (В1), контроль неизменности параметров встроенных СрЗИ и компонентов системного ПО (В2)	Подсистема обеспечения целостности (П3)	Аудит и мониторинг использования информационных ресурсов, контроль доступа, регистрация событий, управление правами, управление установкой обновлений и исправлений сертифицированных версий ОС семейства Windows на серверах и АРМ.	Комплекс встроенных средств защиты серверов и автоматизированных рабочих машин (АРМ) под управлением операционных систем (К1)
				Проведение регулярных проверок на наличие уязвимостей в системах, анализ защищенности информационных ресурсов, оценка рисков и разработка рекомендаций по устранению уязвимостей.	Комплекс анализа защищенности (К12)
				Выявление несанкционированных изменений в данных и системах, контроль целостности исполняемых файлов системного ПО, контроль настроек встроенных средств защиты ОС семейства Windows серверов и АРМ на соответствие их сертифицированным конфигурациям.	Комплекс контроля целостности (К13)
4.	АРМ ПТБ, АРМ АС, АРМ АСУ ТП, Серверы АС, Серверы АСУ ТП, Серверы СрЗИ	Защита файловой системы от вирусов и вредоносных программ (Г1)	Подсистема антивирусной защиты (П4)	Защита от вредоносного ПО, проверка файлов и процессов, обновление версий клиентского ПО, сигнатур.	Комплекс антивирусной защиты (К2)
		Потоковая защита межсетевого трафика от вирусов и вредоносных программ (Г2)		Фильтрация сетевого трафика, блокировка несанкционированных соединений.	Комплекс межсетевого экранирования (К8)
5.	АРМ ПТБ, Серверы АС	Контроль каналов утечек защищаемой информации (Д1)	Подсистема контроля использования ресурсов (П5)	Аудит и мониторинг использования информационных ресурсов, контроль доступа, регистрация событий, управление правами, управление установкой обновлений и исправлений сертифицированных версий ОС семейства Windows на серверах и АРМ.	Комплекс встроенных средств защиты серверов и автоматизированных рабочих машин (АРМ) под управлением

№ п.п.	Объекты защиты	Наименование функции (действия)	Наименование концепта	Наименование функции (действия)	Наименование концепта
					операционных систем (К1)
		Контроль каналов утечек защищаемой информации (Д1), обнаружение несанкционированного хранения конфиденциальной информации (Д2).		Мониторинг и аудит доступа к информационным ресурсам, настройка ограничений по типам файлов и использованию ресурсов, аудит использования информационных ресурсов.	Комплекс контроля использования информационных ресурсов (К15)
6.	Серверы АС, Серверы СрЗИ, СХД	Обеспечение возможности оперативного получения информации о состоянии защищенности (Е1)	Подсистема централизованного управления СрЗИ (П6)	Централизованное управление активным сетевым оборудованием	Комплекс централизованного управления средствами защиты информации (СрЗИ) – К11
		Обеспечение автоматизации рутинных задач (Е2).		Централизованное управление системами хранения данных	
				Управление серверами, предоставление инструментов для администрирования	
7.	АСО, Серверы АС, Серверы АСУ ТП, Серверы СрЗИ	Предоставление в виде отчетов информации об обнаруженных уязвимостях с рекомендациями по их устранению (Ж1).	Подсистема анализа защищенности (П7)	Проведение регулярных проверок на наличие уязвимостей в системах, анализ защищенности информационных ресурсов, оценка рисков и разработка рекомендаций по устранению уязвимостей.	Комплекс анализа защищенности (К12)
		Обеспечение инвентаризации узлов, выявление и идентификация уязвимостей (Ж2).			

№ п.п.	Объекты защиты	Наименование функции (действия)	Наименование концепта	Наименование функции (действия)	Наименование концепта
8.	АРМ ПТБ, АРМ АС, АРМ АСУ ТП, АСО, Серверы АС, Серверы АСУ ТП, Серверы СрЗИ	Межсетевое экранирование ЛВС (З1), обеспечение безопасного функционирования се-тевого оборудования (З3).	Подсистема обеспечения сетевой безопасности (П8)	Фильтрация сетевого трафика, блокировка несанкционированных соединений.	Комплекс межсетевого экранирования (К8)
		Обнаружение вторжений в ЛВС (З2), обеспечение безопасного функционирования сетевого оборудования (З3).		Мониторинг активности, предотвращение атак, сбор, запись и хранение зарегистрированных событий безопасности в течение установленного времени хранения.	Комплекс обнаружения вторжений (К9)
		Обеспечение безопасного функционирования сетевого оборудования (З3).		Управление активным сетевым оборудованием.	Комплекс встроенных средств активного сетевого оборудования (АСО) – К6
				Резервное копирование конфигураций сетевого оборудования, комплекса контроля доступа администратора к АСО и комплекса контроля доступа пользователей к ЛВС, восстановление конфигураций из резервных копий.	Комплекс резервного копирования конфигурационных файлов АСО (К7)
9.	АРМ АСУ ТП, АСО, Серверы АС, Серверы АСУ ТП, Серверы СрЗИ	Резервное копирование конфигурационных фай-лов СрЗИ и восстановление данных из резервных копий в случаях сбоев (И1).	Подсистема обеспечения непрерывности функционирования (П9)	Резервное копирование конфигурационных файлов серверов СрЗИ, ИС, периодическое резервное копирование БД ИС, резервирование "эталонного" образа ОС серверов и АРМ АСУ ТП, периодическое резервное копирование образов системных дисков серверов и АРМ АСУ ТП.	Комплекс резервного копирования (К3)
				Резервное копирование конфигураций сетевого оборудования, комплекса контроля доступа администратора к АСО и комплекса контроля доступа пользователей к ЛВС, восстановление конфигураций из резервных копий.	Комплекс резервного копирования конфигурационных файлов АСО (К7)

Структура комплексной СЗИ (КСЗИ) предприятия представлена в виде онтологии общей схемы в соответствии с рисунком 2.2. В рамках данной структуры ПТСЗИ является частью КСЗИ [106, 107].

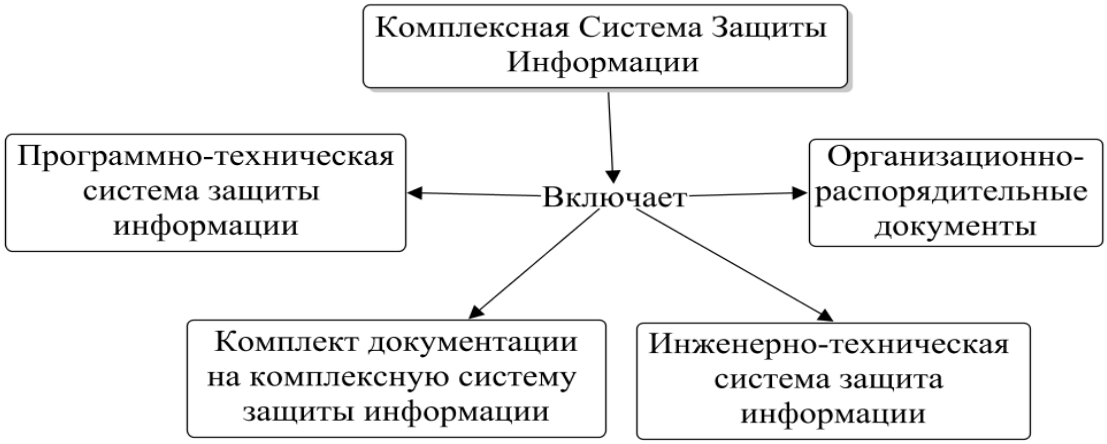


Рисунок 2.2 – Онтология общей структуры КСЗИ предприятия

Принимая во внимание основные функции концептов СЗИ предприятия (табл. 2.1) онтология состава подсистем ПТСЗИ представлена на рисунке 2.3. Представленный в соответствии с рисунком 2.3 состав подсистем ПТСЗИ обеспечивает выполнение ими функций как показано на рисунке 2.4 [106]

Рисунок 2.3 – Онтология состава подсистем ПТСЗИ

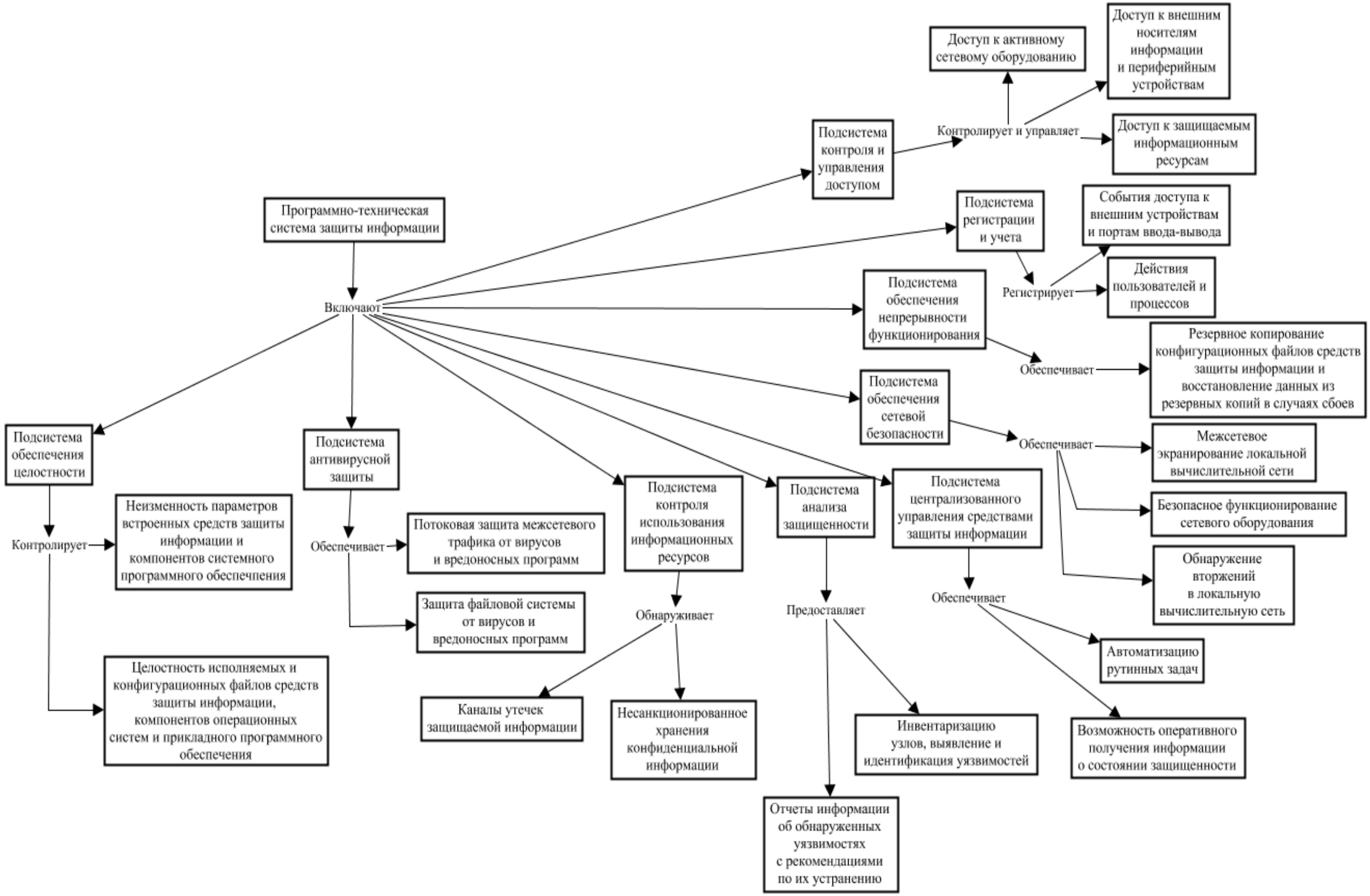


Рисунок 2.4 – Онтология подсистем ПТСЗИ и выполняемых ими функций

Онтология, представленная на рисунке 2.5, описывает подсистему контроля и управления доступом [106, 107].

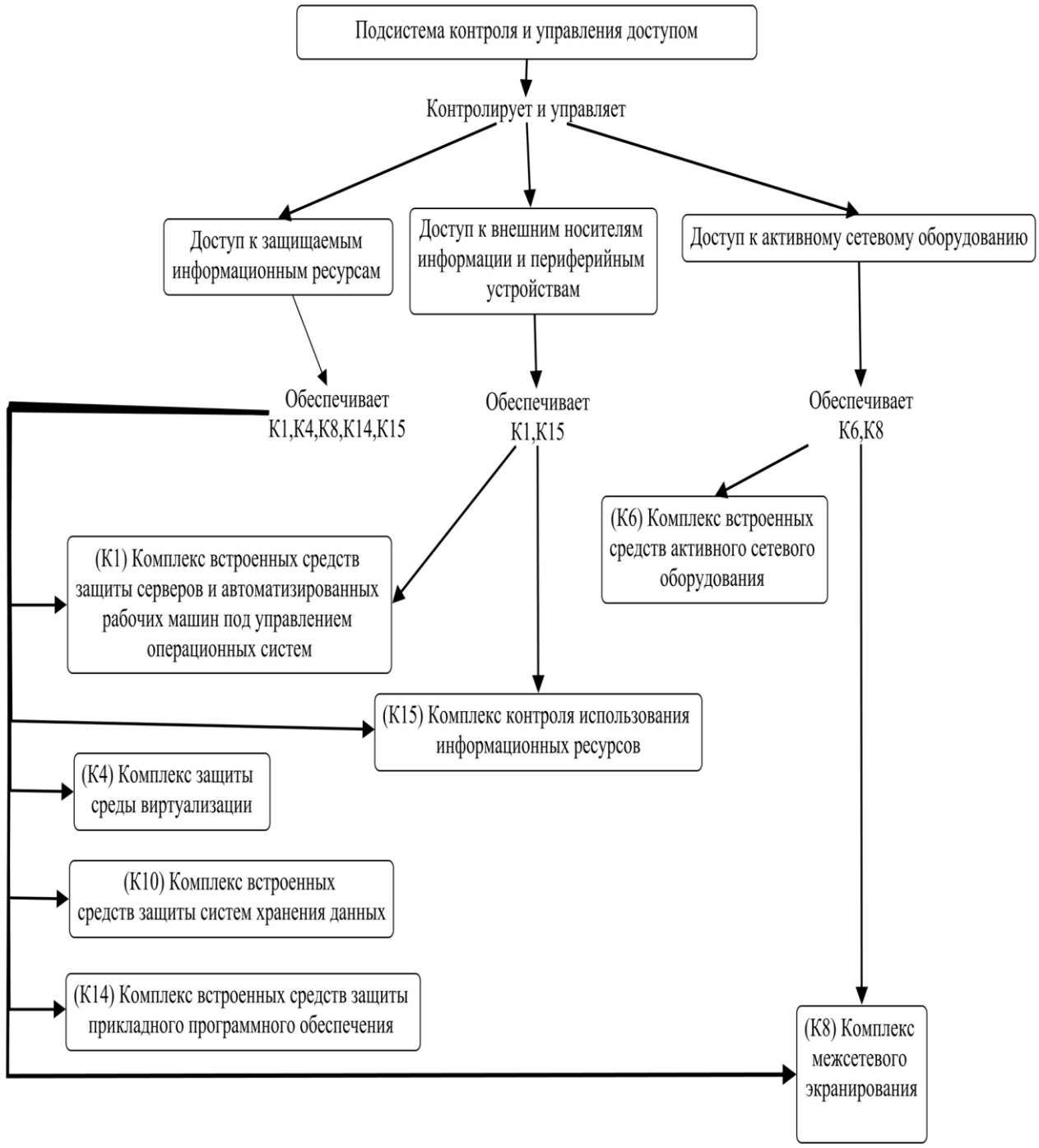


Рисунок 2.5 – Онтология подсистемы контроля и управления доступом комплекса ПТСЗИ

Подсистема контроля и управления доступом выполняет следующие функции [33, 106, 107]: идентификация, аутентификация, создание, активация, модификация, пересмотр (с определенной периодичностью), отключение

(блокирование) и удаление учетных записей, а также обеспечение контроля над действиями пользователей и администраторов при доступе к информационным активам предприятия. В рамках данной подсистемы осуществляется идентификация программ, томов, каталогов и файлов на рабочих местах и серверах.

После этого следует подсистема регистрации и учета, изображенная в соответствии с рисунком 2.6.

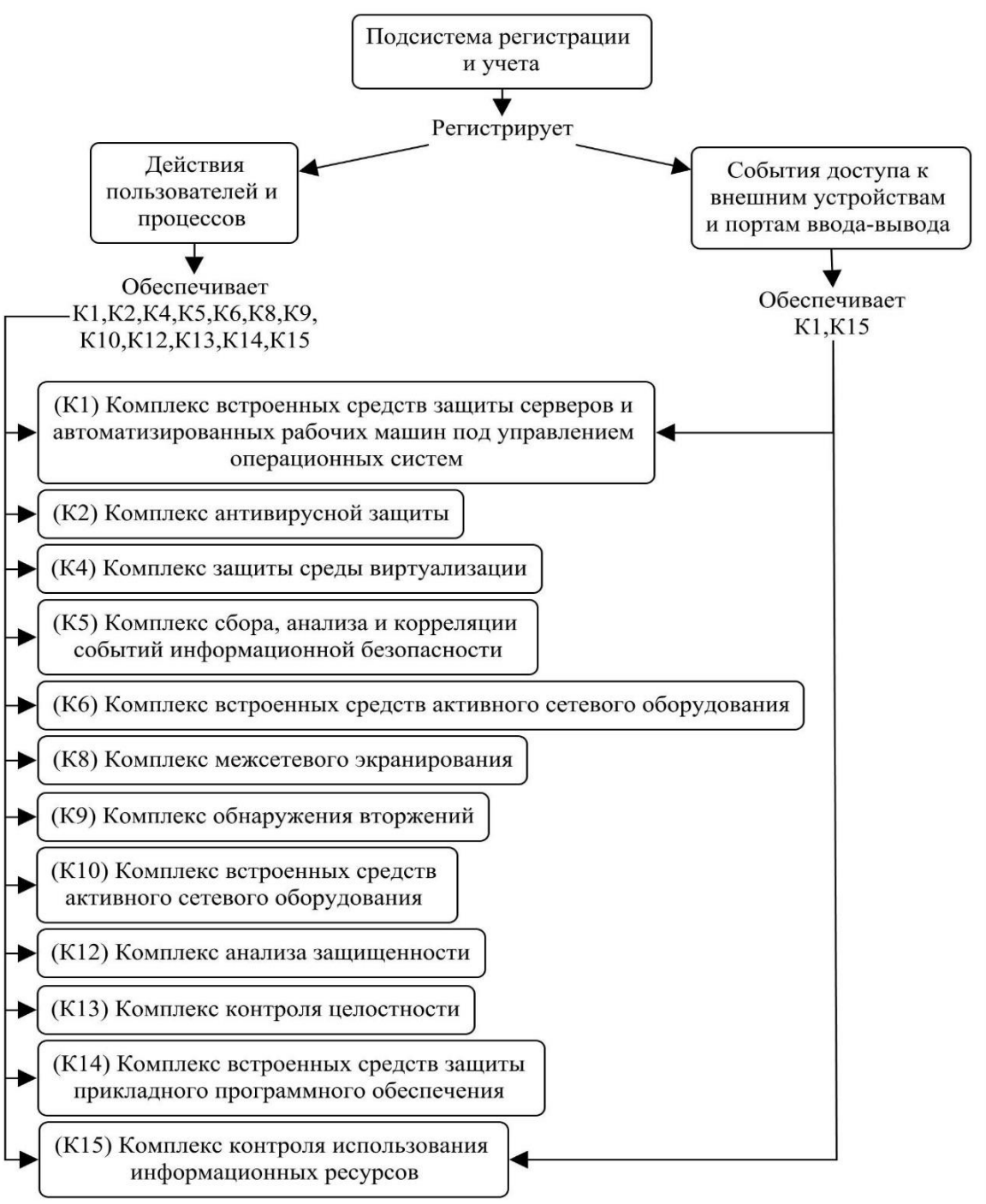


Рисунок 2.6 – Онтология подсистемы регистрации и учёта

В рамках данной подсистемы выполняются следующие функции [106]:

– регистрация входа/выхода субъектов доступа (пользователей и процессов) к защищаемым информационным ресурсам (ИР). Информационный ресурс может включать в себя различные источники информации, используемые для обучения, коммуникации или принятия решений. Примеры информационных ресурсов включают в себя [106]: 1) электронные документы (книги, статьи и другие); 2) электронные базы данных и другие источники электронной информации; 3) веб-сайты; 4) аудио- и видеозаписи, включая подкасты и вебинары. В общем, любой элемент, который может использоваться для сбора или передачи информации, может быть рассматриваем как часть информационного ресурса. Конкретные компоненты, составляющие информационный ресурс, будут зависеть от контекста и целей его использования [96];

– запись и отслеживание запуска и завершения программ и процессов, предназначенных для обработки защищаемых файлов

регистрация попыток доступа пользователей и процессов к защищаемым объектам доступа, таким как файлы и каталоги;

– отслеживание событий печати документов;

– регистрация событий доступа к внешним устройствам, таким как внешние накопители информации, а также к портам ввода-вывода на автоматизированных рабочих машинах;

– запись событий информационной безопасности на активном сетевом оборудовании, включая коммутаторы, маршрутизаторы, и средства защиты информации;

– сбор, запись и хранение зарегистрированных событий безопасности в течение определенного времени. События безопасности могут быть собраны с использованием различных протоколов, таких как Syslog, MS Windows Event log, SSH/Telnet, СУБД с использованием ODBC, SNMP Trap, Checkpoint LEA/OPSEC, NetFlow и другие. При этом необходимо учитывать функциональные возможности источника событий;

– обработка полученных событий безопасности, включая фильтрацию, нормализацию, агрегацию, категоризацию, приоритезацию и корреляцию.

Под корреляцией событий информационной безопасности (ИБ) понимают процесс объединения и анализа множества отдельных событий, собираемых из различных источников в системе, с целью выявления взаимосвязей между ними и определения значимых инцидентов информационной безопасности. Этот процесс помогает превратить большое количество разрозненных данных в осмысленную картину, позволяющую быстро и точно обнаруживать угрозы, и реагировать на них.

Основные аспекты корреляции событий ИБ включают:

– *Сбор данных:* события собираются из различных источников, таких как сетевые устройства, серверы, приложения, системы обнаружения вторжений (IDS), системы предотвращения вторжений (IPS), журналы аудита и другие средства защиты информации.

– *Анализ данных:* анализируется каждое событие отдельно для поиска признаков потенциальных угроз. Это может включать проверку на соответствие правилам безопасности, выявление аномалий и отклонений от нормы.

– *Сопоставление событий:* выполняется сопоставление и объединение нескольких событий, которые могут указывать на одну и ту же активность или атаку. Например, несколько неудачных попыток входа в систему могут указывать на попытку взлома.

– *Определение контекста:* каждое событие рассматривается в контексте других событий и всей системы в целом. Это помогает лучше понимать природу угрозы и её возможные последствия.

– *Поиск паттернов и аномалий:* использование алгоритмов машинного обучения и статистических методов для выявления необычных или подозрительных паттернов поведения, которые могут указывать на кибератаки.

– *Генерация отчетов и уведомлений:* на основе проанализированных данных формируются отчеты и уведомления, которые направляются ответственным лицам для принятия дальнейших мер.

Корреляция событий ИБ является важным инструментом в арсенале специалистов по кибербезопасности, поскольку она позволяет оперативно реагировать на возникающие угрозы.

Правила корреляции могут быть созданы на основе встроенной базы правил или пользовательских правил и могут использовать справочники и данные об активах для более точной корреляции событий. Также возможна многоуровневая корреляция, где результаты одного правила корреляции передаются на вход другому правилу;

– возможность оптимизации правил корреляции с использованием новых данных об активах;

– управление задачами сбора, обработки и корреляции событий, а также управление активами через единую консольный интерфейс.

Подсистема обеспечения целостности, представленная в соответствии с рисунком 2.7, выполняет следующие задачи [106]:

– проверка целостности исполняемых и конфигурационных файлов средств защиты информации (СрЗИ) и операционных систем (ОС);

– контроль целостности программного обеспечения (ППО);

– мониторинг неизменности параметров встроенных средств защиты информации, операционных систем, АРМ и серверов, входящих в состав ИС и АСУ ТП.

Рисунок 2.7 – Онтология подсистемы обеспечения целостности

Подсистема антивирусной защиты представлена в соответствии с рисунком 2.8 [106].

Подсистема антивирусной защиты выполняет следующие функции [106]:

– постоянная защита файловой системы автоматизированных рабочих машин (АРМ) и серверов под управлением различных версий операционных систем (ОС) от вирусов, троянских программ и червей. Защита осуществляется как с использованием баз вирусных описаний, так и с помощью эвристического анализа;

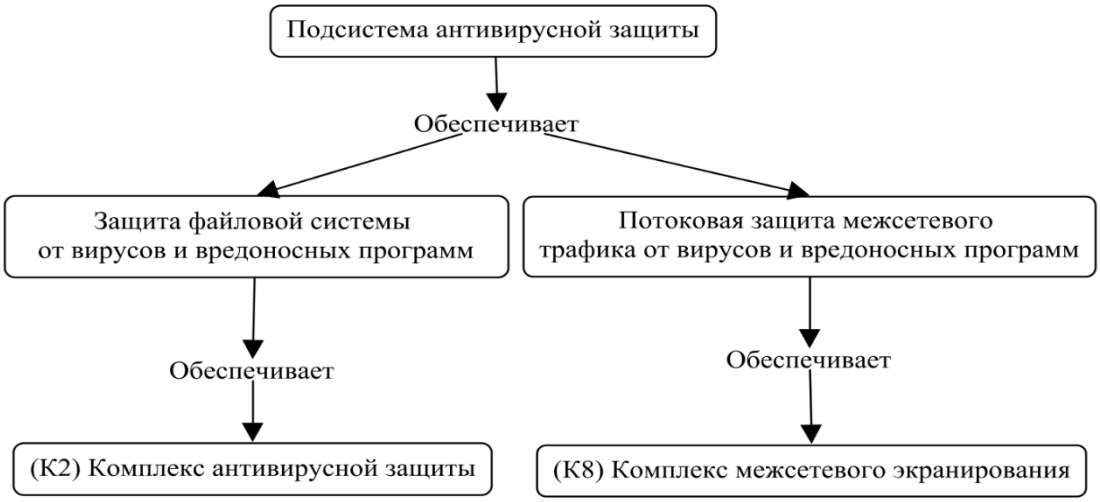


Рисунок 2.8 – Онтология подсистемы антивирусной защиты

– потоковая защита сетевого трафика между сетями от вирусов и вредоносных программ.

В соответствии с рисунком 2.9 изображена подсистема контроля использования информационных ресурсов.

Рисунок 2.9 – Онтология подсистемы контроля использования информационных ресурсов

Несмотря на свою простоту, она выполняет широкий спектр функций [33, 106, 107]:

– обнаружение несанкционированного хранения конфиденциальной информации в информационных ресурсах, таких как файловые серверы, файловые хранилища, автоматизированные рабочие машины пользователей, базы данных;

– контроль утечек защищаемой информации через различные каналы;

– аутентификация пользователей и управление профилями доступа к ресурсам в сети Интернет;

– расшифровка SSL (TLS) трафика с помощью программного компонента на автоматизированной рабочей машине, который действует от имени более крупной системы или приложения, обычно распределенного или децентрализованного;

– контроль отправки информации из системы, когда программный компонент находится за пределами локальной вычислительной сети предприятия;

– анализ и перехват трафика с возможностью блокировки сообщений, отправляемых через корпоративную электронную почту с использованием протокола SMTP. В контексте корпоративной электронной почты это означает мониторинг электронных писем, отправленных и полученных сотрудниками с использованием почтовой системы компании. Для перехвата и анализа трафика могут использоваться различные методы, такие как инструменты сетевого мониторинга, программное обеспечение для перехвата пакетов или специализированные аппаратные устройства. Эти инструменты позволяют перехватывать и анализировать содержимое электронных сообщений, включая адреса отправителя и получателя, тему и текст сообщения. Кроме того, благодаря возможности блокировки сообщений, отправленных через корпоративную электронную почту, система может предотвратить доставку определенных сообщений получателям. Обычно эта функция используется для предотвращения распространения вредоносного контента или конфиденциальной информации за пределы сети

компании. В общем и целом, применение перехвата и анализа трафика, сопровождаемое возможностью блокировки сообщений, отправляемых через корпоративную электронную почту, способно эффективно обеспечить безопасность и неприкосновенность системы электронной переписки организации, а также предотвратить утечку данных и другие инциденты безопасности;

– захват и анализ сообщений, отправляемых через веб-сервисы (веб-почта, социальные сети, файловые ресурсы в Интернете, облачные хранилища и т.д.);

– захват и анализ информации в системах мгновенных сообщений (ICQ, Skype, Jabber, Mail.ru);

– централизованное хранение истории инцидентов, оригинальных писем и перехваченных данных;

– автоматическое разбиение сообщений на составляющие части на этапе их приема с возможностью анализа атрибутов сообщения (заголовки, тело, вложения);

– создание, редактирование и удаление правил фильтрации, анализа и архивирования;

– обнаружение заполненных форм – определение заполненных и незаполненных полей документов с возможностью обнаружения информации, связанной с персональными данными, согласно федеральному закону «О персональных данных» от 27.07.2006 № 152-ФЗ;

– оперативное уведомление ответственных сотрудников о зафиксированных событиях информационной безопасности по электронной почте;

– захват документов, отправляемых на печать (сетевые и локальные принтеры) и другие функции.

В соответствии с рисунком 2.10 представлена подсистема централизованного управления СрЗИ.

– С помощью подсистемы централизованного управления СрЗИ, можно осуществлять следующие функции [96]:
– получение оперативной информации о состоянии безопасности ИС и АСУ ТП;

– оперативное реагирование на инциденты ИБ;

– предоставление администраторам инструментов для осуществления контрольных функций;

– управление обеспечением ИБ и автоматизацией рутинных задач.

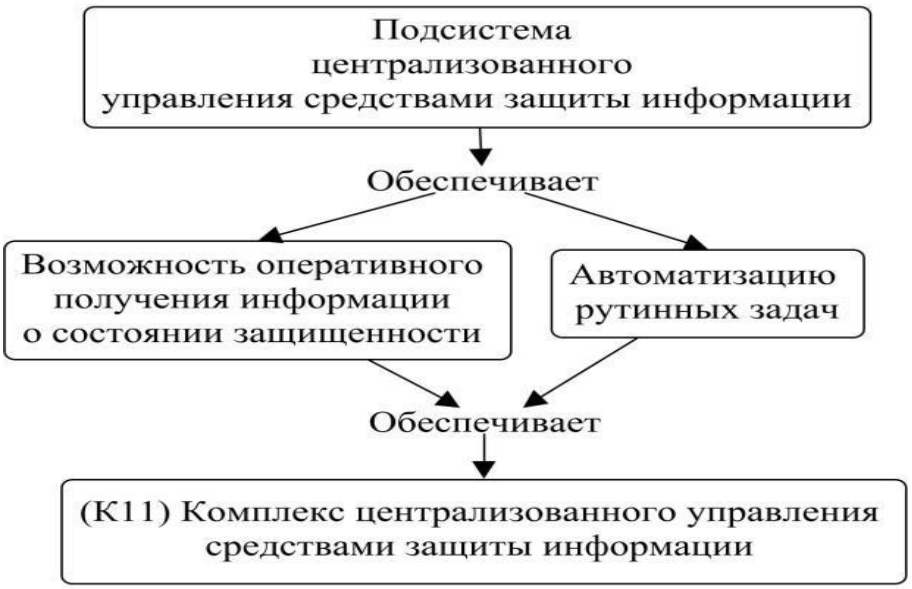


Рисунок 2.10 – Онтология подсистемы централизованного управления СрЗИ

Подсистема анализа защищенности, представленная в соответствии с рисунком 2.11, имеет схожую топологию и структуру [106].

Рисунок 2.11 – Онтология подсистемы анализа защищённости

Функции подсистемы анализа защищенности включают [106]:

– обнаружение и учет защищаемых ресурсов;

– анализ защищенности компонентов локальной вычислительной сети (ЛВС) предприятия, таких как: 1) операционные системы серверов ИС; 2) системы АСУ ТП; 3) СрЗИ; 4) автоматизированные системы обработки (АСО) и сетевые сервисы серверов ИС; 5) прикладное программное обеспечение (ППО);

– анализ защищенности информационных систем предприятия;

– сканирование узлов ЛВС и принятие решений о соответствии или несоответствии узлов ИС и информационных систем в целом установленным на предприятии техническим стандартам;

– регулярное централизованное обновление компонентов подсистемы;

– централизованное управление компонентами подсистемы и управление доступом пользователей к функциям подсистемы;

– генерация отчетов о результатах сканирования и доставка отчетов уполномоченным сотрудникам предприятия.

Двумя последними подсистемами комплекса по обеспечению технической защиты информации являются подсистема сетевой безопасности в соответствии с рисунком 2.12 и подсистема обеспечения непрерывности функционирования в соответствии с рисунком 2.13 [106].

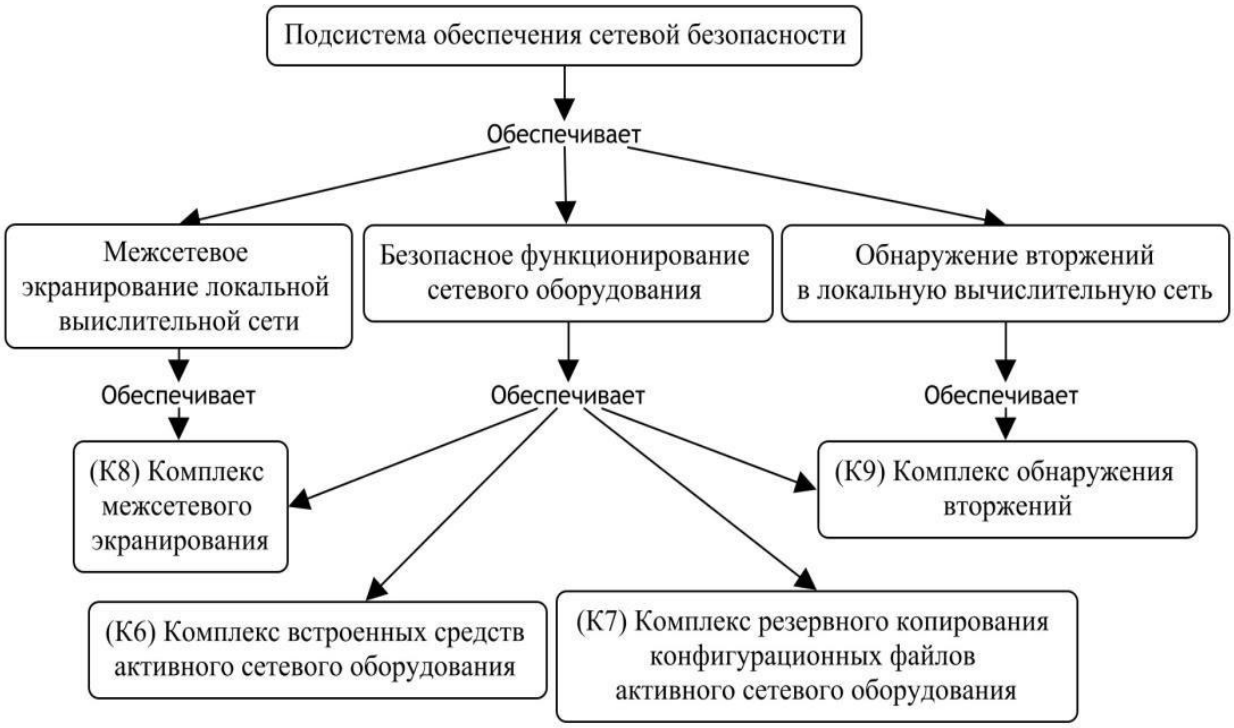


Рисунок 2.12 – Онтология подсистемы обеспечения сетевой безопасности

Первая из них, представленная в соответствии с рисунком 2.12, осуществляет следующие функции [106]:

– межсетевое экранирование и сегментирование ЛВС предприятия;

– обнаружение вторжений;

– централизованное управление подсистемой;

– интеграция с периметральной системой защиты информации предприятия.

Вторая подсистема, представленная в соответствии с рисунком 2.13 выполняет следующие задачи [106]:

– резервное копирование конфигурационных файлов СрЗИ и АСО и восстановление данных из резервных копий в случае сбоев;

– хранение резервных копий;

– восстановление данных из резервных копий;

– реализация отказоустойчивой конфигурации межсетевого экрана (МЭ) и АСО.

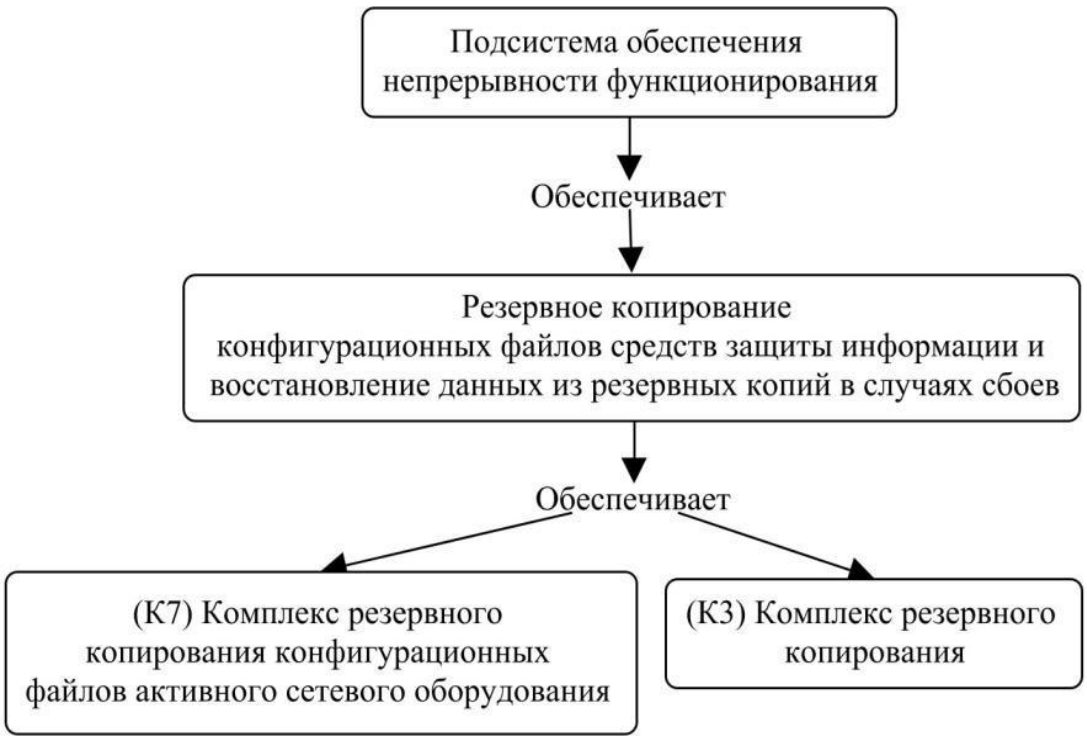


Рисунок 2.13 – Онтология подсистемы обеспечения непрерывности функционирования

2.3. Выводы по главе

Во второй главе, с учётом проведённого системного анализа, разработана система онтологий, которая положена в основу вычислительного алгоритма для оценки эффективности ПТСЗИ на предприятиях с различным уровнем зрелости в области ИБ. Предложенная система формирует базу знаний предметной области, описывающую компоненты, входящие в ПТСЗИ и связи между ними. Онтологические модели играют ключевую роль в процессе агрегированного оценивания эффективности функционирования СЗИ. Определённые в рамках моделей концепты (например, подсистемы защиты, функции контроля доступа, антивирусной защиты и др.) и их взаимосвязи служат основой для выбора показателей оценки. Это позволяет структурировать процесс измерения эффективности на всех уровнях системы, а также минимизировать влияние субъективных факторов за счёт формализации межкомпонентных связей. В рамках анализа выделены девять ключевых подсистем, каждая из которых интегрируется в общую архитектуру защиты.

Для построения системы онтологий ПТСЗИ использовались методы онтологического моделирования, что позволило детализировать функции, выполняемые на уровне каждой подсистемы. Это дало возможность структурировать комплексы средств защиты информации (СрЗИ) в рамках ПТСЗИ, такие как: К1 (комплекс встроенных средств защиты серверов и автоматизированных рабочих машин (АРМ) под управлением операционных систем (ОС) семейства Windows); К2 (комплекс антивирусной защиты); К3 (комплекс резервного копирования); К4 (комплекс защиты среды виртуализации); К5 (комплекс сбора, анализа и корреляции событий ИБ); К6 (комплекс встроенных средств АСО); К7 (комплекс резервного копирования конфигурационных файлов АСО); К8 (комплекс межсетевого экранирования); К9 (комплекс обнаружения вторжений); К10 (комплекс встроенных средств защиты систем хранения данных); К11 (комплекс централизованного управления СрЗИ); К12 (комплекс анализа защищенности); К13 (комплекс контроля целостности); К14 (комплекс встроенных средств

защиты прикладного программного обеспечения (ППО)); К15 (комплекс контроля использования информационных ресурсов).

Комплексы СрЗИ К1 … К15, несмотря на их внутреннюю сложность, рассматриваются в данном исследовании как функциональные элементы системы. Системный подход позволяет оценивать их не по отдельности, а как взаимосвязанные компоненты, что обеспечивает всесторонний анализ и управление защитными мерами. Разработанные онтологические модели ПТСЗИ не только формализуют знания о компонентах системы, но и служат методологической основой для разработки методики и алгоритмического обеспечения агрегированного оценивания её функциональной эффективности. Модели позволяют выделить ключевые показатели эффективности, структурировать их по уровням и обеспечить логическую взаимосвязь между компонентами системы. Это повышает объективность результатов и точность оценки.

Полученные результаты могут быть адаптированы для предприятий в различных секторах экономики, когда требуется создать комплексную систему защиты информационных активов, провести минимизацию вероятностей киберугроз, а также сократить время реагирования на инциденты информационной безопасности.

3. Методика агрегированного оценивания эффективности функционирования ПТСЗИ предприятия

Растущая зависимость от программных и аппаратных решений сделала измерение уровня их безопасности важнейшим аспектом современных технологий. Обеспечение безопасности программных и аппаратных решений напрямую влияет на конфиденциальность, целостность и доступность информации в процессе обработки и хранении которой они участвуют или могут быть задействованы. Совокупность программных и аппаратных решений в процессе их применения на предприятии составляют систему решений ИТ-инфраструктуры. В результате, научное сообщество активно занимается разработкой и поиском подходов к оценке ИБ этих систем. Оценка уровня безопасности информационной инфраструктуры предприятия имеет огромное значение в современной быстро меняющейся и технологически развитой бизнес-среде. С ростом использования программного обеспечения и технологий в повседневной деятельности очень важно обеспечить безопасность этих систем и их защиту от потенциальных угроз [105].

Целью настоящей главы является разработка комплексного подхода к оценке эффективности функционирования ПТСЗИ, которая будет учитывать компоненты системы ПТСЗИ.

Разработанная в главе 2 онтологическая модель системы ПТСЗИ сыграла ключевую роль в формировании методики агрегированной оценки эффективности её функционирования. Она обеспечивает систематизацию компонент (например, подсистемы защиты и их функции, комплексы средств защиты информации и др.) в контексте объектов защиты и угроз, что позволяет применить системный подход к построению кубической матрицы «Угрозы – Активы – Комплексы средств защиты информации» и связанных двумерных матриц. Это сделало процесс оценки более прозрачным и объективным [105]. Кроме того, методика позволяет вычислить доли угроз по объектам защиты, в противодействии которым задействованы комплексы СрЗИ.

В основу методики положен подход связанный с анализом состояния трёхмерной кубической матрицы «Угрозы» × «Активы (Объекты воздействия)» × «Комплексы средств защиты информации» («матрица защиты») взаимосвязи и оценки по которой формируются на основе полученных онтологий и связанных с ними двумерных матриц: а) Эталонные значения «Объекты защиты в контексте подсистем»; б) «Угрозы» × «Комплексы средств защиты информации»; в) «Активы (Объекты воздействия)» × «Комплексы средств защиты информации»; д) Матрица «Оценка аудитора».

3.1. Оценка общей эффективности функционирования ПТСЗИ

В данном разделе представлена методика оценки эффективности функционирования системы ПТСЗИ и разработана оптимизационная модель обеспечения заданного уровня информационной безопасности предприятия [105, 109]. Эта модель охватывает систему ПТСЗИ и направлена на решение задач оптимизации эффективности как самой системы ПТСЗИ, так и всех её компонентов при ограниченных финансовых ресурсах. Методика предусматривает оценку доли угроз, нарушающих требования к защищённости информации (конфиденциальность, целостность, доступность) по объектам защиты или воздействия системы ПТСЗИ. Для оценки общей эффективности функционирования системы ПТСЗИ предложены следующие шаги.

Шаг 1. Используя данные с сайта ФСТЭК России (https://bdu.fstec.ru/files/documents/thrlist.xlsx) [10] формируется список объектов воздействия (защиты) в привязке к угрозам ИБ, содержащий n_o элементов. Среди них базы данных, прикладное программное обеспечение, каналы связи, мобильные устройства и т.д. [102, 105].

Шаг 2. В процессе формирования векторов и множеств использованы результаты онтологического моделирования из главы 2. Определённые в онтологической модели подсистемы, их функции и взаимосвязи между компонентами ПТСЗИ составляют основу структурирования данных, что

обеспечивает единообразие при заполнении массивов. Например, концепты подсистем и их функций, описанные в онтологиях, стали основой для разбиения данных на множества, представленные в таблице 3.1. На основании онтологических моделей и компонент системы ПТСЗИ, которые представлены во второй главе диссертационного исследования, формируются: 1) вектор $V=(3,2,2,2,2,2,2,3,1)$ [33, 106, 107, 113], состоящий из v_i элементов, каждый из которых показывает какое количество функций входит в i-ю подсистему; 2) множества M_i^j [105], содержащие как показано в таблице 3.1 номера комплексов, входящих в j-ю функцию i-й подсистемы.

Шаг 3. Формируется бинарный четырехмерный массив D, состоящий из элементов δ_{ijkp}, где i – номер подсистемы ($i=\overline{1,9}$), j – номер функции ($j=\overline{1,v_i}$), k – элементы множества M_i^j, p – номер объекта защиты ($p=\overline{1,n_0}$). Элементы массива D задаются по правилу [105]:

$$\delta_{ijkp}=\begin{cases}1, \text{ если при реализации } j-\text{й функции } i\text{-й подсистемы}\\ k\text{-й комплекс задействован для защиты } p\text{-го объекта;}\\ 0, \text{ в противном случае.}\end{cases}$$

Таблица 3.1 – Комплексы СрЗИ в разрезе подсистем и выполняемых ими функций

Подсистемы	Функции подсистем	Множество M_i^j	Комплексы
Подсистема контроля и управления доступом (П1)	Контроль и управление доступом к защищаемым информационным ресурсам (А1)	M_1^1	К1, К4, К8, К10, К14, К15
	Контроль и управление доступом к внешним носителям информации и периферийным устройствам (А2)	M_1^2	К1, К15
	Контроль доступа к активному сетевому оборудованию (АСО) (А3)	M_1^3	К6, К8
Подсистема регистрации и учета (П2)	Регистрация и учет действий пользователей и процессов (Б1)	M_2^1	К1, К2, К4, К5, К6, К8, К9, К10,

Подсистемы	Функции подсистем	Множество M_i^j	Комплексы
			К12, К13, К14, К15
	Регистрация событий доступа к внешним устройствам и портам ввода-вывода (Б2)	M_2^2	К1, К15
Подсистема обеспечения целостности (П3)	Контроль целостности исполняемых и конфигурационных файлов СрЗИ, компонентов ОС и прикладного ПО (В1)-	M_3^1	К1, К12, К13
	Контроль неизменности параметров встроенных СрЗИ и компонентов системного ПО (В2)-	M_3^2	
Подсистема антивирусной защиты (П4)	Защита файловой системы от вирусов и вредоносных программ (Г1)	M_4^1	К2
	Потоковая защита межсетевого трафика от вирусов и вредоносных программ (Г2)	M_4^2	К8
Подсистема контроля использования информационных ресурсов (П5)	Контроль каналов утечек защищаемой информации (Д1)	M_5^1	К1, К15
	Обнаружение несанкционированного хранения конфиденциальной информации (Д2)	M_5^2	К15
Подсистема централизованного управления СрЗИ (П6)	Обеспечение возможности оперативного получения информации о состоянии защищенности (Е1)	M_6^1	К11
	Обеспечение автоматизации рутинных задач (Е2)	M_6^2	
Подсистема анализа защищенности (П7)	Предоставление в виде отчетов информации об обнаруженных уязвимостях с рекомендациями по их устранению (Ж1)	M_7^1	К12
	Обеспечение инвентаризации узлов, выявление и идентификация уязвимостей (Ж2)	M_7^2	

Подсистемы	Функции подсистем	Множество M_i^j	Комплексы
Подсистема обеспечения сетевой безопасности (П8)	Межсетевое экранирование ЛВС (З1)	M_8^1	К8
	Обнаружение вторжений в ЛВС (З2)	M_8^2	К9
	Обеспечение безопасного функционирования сетевого оборудования (З3)	M_8^3	К6, К7, К8, К9
Подсистема обеспечения непрерывности и функционирования (П9)	Резервное копирование конфигурационных файлов СрЗИ и восстановление данных из резервных копий в случаях сбоев (И1)	M_9^1	К3, К7

Для удобства заполнения бинарного массива D можно воспользоваться формой, представленной в таблице 3.2.

Информация, которая будет внесена в массив D по предприятию в дальнейшем будет считаться как исходная информация для расчетов в оценке функциональной эффективности системы ПТСЗИ КСЗИ и оценке его общего уровня защищённости [105].

Таблица 3.2 – Форма для заполнения бинарного массива

Наименование подсистемы, условное обозначение	Наименование функции, условное обозначение	Наименование комплекса системы ПТСЗИ КСЗИ, условное обозначение	Объект защиты, условное обозначение			
			1	2	...	n_o
1	1	1	1	1	...	0
1	2	6	0	1	...	1
2	1	8	1	1	...	0

Шаг 4. С использованием бинарного массива D для каждого комплекса одного типа, реализующего j-ю функцию i-й подсистемы, вычисляется доля N_{ijk}^1 его связей с выбранными для оценки объектами защиты к общему числу

связей всех комплексов разного типа по j-й функции i-й подсистемы по выбранным объектам защиты по формуле [105]

$$N_{ijk}^{1}=\begin{cases}\dfrac{\sum\limits_{p=1}^{n_o}\delta_{ijkp}}{\sum\limits_{s\in M_i^j}\sum\limits_{p=1}^{n_o}\delta_{ijsp}}, \text{ если } \sum\limits_{s\in M_i^j}\sum\limits_{p=1}^{n_o}\delta_{ijsp}\neq 0, \\ 0, \text{ если } \sum\limits_{s\in M_i^j}\sum\limits_{p=1}^{n_o}\delta_{ijsp}=0,\end{cases} \quad i=\overline{1,9},\ j=\overline{1,v_i},k\in M_i^j \quad (3.1)$$

Затем для каждой j-ой функции, входящей в i-ю подсистему, реализуемой комплексами разного типа вычисляется доля N_{ij}^{2} общего числа связей всех её комплексов с выбранными для оценки объектами защиты к общему числу связей всех комплексов разного типа i-й подсистемы по выбранным объектам защиты по формуле [105]

$$N_{ij}^{2}=\begin{cases}\dfrac{\sum\limits_{s\in M_i^j}\sum\limits_{p=1}^{n_o}\delta_{ijsp}}{\sum\limits_{t=1}^{v_i}\sum\limits_{s\in M_i^j}\sum\limits_{p=1}^{n_o}\delta_{itsp}}, \text{ если } \sum\limits_{t=1}^{v_i}\sum\limits_{s\in M_i^j}\sum\limits_{p=1}^{n_o}\delta_{itsp}\neq 0, \\ 0, \text{ если } \sum\limits_{t=1}^{v_i}\sum\limits_{s\in M_i^j}\sum\limits_{p=1}^{n_o}\delta_{itsp}=0,\end{cases} \quad i=\overline{1,9},\ j=\overline{1,v_i}. \quad (3.2)$$

После чего для каждой подсистемы вычисляется доля N_i^3 общего числа связей всех её комплексов разного типа i-ой подсистемы с выбранными объектами защиты к общему числу связей всех комплексов разного типа всех подсистем уровня системы ПТСЗИ по выбранным объектам защиты по формуле [105]

$$N_i^3 = \begin{cases} \dfrac{\sum\limits_{t=1}^{v_i} \sum\limits_{s \in M_i^j} \sum\limits_{p=1}^{n_o} \delta_{itsp}}{\sum\limits_{s=1}^{9} \sum\limits_{j=1}^{v_i} \sum\limits_{k \in M_i^j} \sum\limits_{p=1}^{n_o} \delta_{sjkp}}, \text{ если } \sum\limits_{s=1}^{9} \sum\limits_{j=1}^{v_i} \sum\limits_{k \in M_i^j} \sum\limits_{p=1}^{n_o} \delta_{sjkp} \neq 0, \\ 0, \text{ если } \sum\limits_{s=1}^{9} \sum\limits_{j=1}^{v_i} \sum\limits_{k \in M_i^j} \sum\limits_{p=1}^{n_o} \delta_{sjkp} = 0, \end{cases} \quad i = \overline{1,9}. \qquad (3.3)$$

Шаг 5. Вычисляется эффективность каждого уровня j-ой функции i-й подсистемы по формулам

$$Э_{ij} = \sum_{k \in M_i^j} N_{ijk}^1 \cdot d_{ijk}, \quad i = \overline{1,9}, \; j = \overline{1,v_i}, \qquad (3.4)$$

где d_{ijk} – оценки аудиторов по шкале от 0 до 1. Оценка «1» означает, что k – й комплекс полностью задействован в обеспечении j-ой функции i-й подсистемы, и удовлетворяет требованиям регуляторов по ИБ. Оценка «0» означает, что k – й комплекс не участвует в обеспечении j-ой функции i-й подсистемы, либо не удовлетворяет требованиям регуляторов по ИБ. Промежуточные значения отражают частичную функциональность комплекса. При этом отметим, что на оценку аудиторов могут влиять следующие факторы: уровень компетенции экспертов в области ИБ и результаты вычислений уязвимостей по интерактивному калькулятору, размещенному на сайте ФСТЭК (https://bdu.fstec.ru/calc31).

Затем определяется эффективность каждого уровня подсистемы по формуле

$$Э_i = \sum_{j=1}^{v_i} N_{ij}^2 \cdot Э_{ij}, \quad i = \overline{1,9}. \qquad (3.5)$$

После чего проводится вычисление оценки функциональной эффективности системы ПТСЗИ по формуле

$$Э = \sum_{i=1}^{9} N_i^3 \cdot Э_i. \qquad (3.6)$$

Оценка функциональной эффективности системы ПТСЗИ принимает значения в интервале от 0 до 1. Оценка «1» означает, что все компоненты системы

ПТСЗИ задействованы в полном объёме в реализации процессов обеспечения защиты информации и эксплуатации технологий безопасности информации, а «0» или любое число меньшее единицы – что система ПТСЗИ соответственно либо полностью или частично не функционирует, либо не соответствует требованиям регуляторов по ИБ.

В силу того, что на поддержание и модернизацию своей системы безопасности у предприятия присутствует так называемое бюджетное ограничение, то возникает задача максимизации уровня информационной защищенности предприятия при ограниченных финансовых ресурсах.

Предположим, что если оценка аудитора d_{ijk} меньше 1, то для того, чтобы обеспечить в будущем полную функциональность данного комплекса нужно затратить $c_{ijk}^{дост}$ условных денежных единиц. Эти затраты могут назначить работники соответствующих финансовых отделов предприятия на основе рекомендаций аудиторов. Таким образом, если затратить $\sum_{i=1}^{9}\sum_{j=1}^{v_i}\sum_{k\in M_i^j} c_{ijk}^{дост}$ условных денежных единиц, то показатель $Э$ будет равен 1, т.е. обеспечится полная защищенность ПТСЗИ. Однако на повышение уровня ИБ есть ограниченная сумма денег – W условных денежных единиц, причем, $W < \sum_{i=1}^{9}\sum_{j=1}^{v_i}\sum_{k\in M_i^j} c_{ijk}^{дост}$. В таком случае обеспечить полную защищенность не получится, но хотелось бы распределить имеющиеся финансы так, чтобы она была максимальна. Обозначим d_{ijk}^{*} – ожидаемые оценки аудиторов после будущей модернизации КСЗИ, а c_{ijk} – затраты, обеспечивающие соответствующие ожидаемые оценки d_{ijk}^{*} аудиторов после будущей модернизации ПТСЗИ.

Будем считать, что затраты и ожидаемые оценки связаны линейными функциональными зависимостями:

$$c_{ijk} = b_{ijk}^{0} + b_{ijk}^{1}\cdot d_{ijk}^{*},\ i=\overline{1,9},\ j=\overline{1,v_i},\ k\in M_i^j, \qquad (3.7)$$

где b_{ijk}^0, b_{ijk}^1, $i=\overline{1,9}$, $j=\overline{1,v_i}$, $k\in M_i^j$ – неизвестные параметры.

Отметим, что в работах [58, 94] аналогичным образом вводятся линейные зависимости рисков отказа работоспособности системы от затрат.

Допустим, что деньги не будут вкладываться, тогда ожидаемая оценка не изменится, т.е. если $c_{ijk}=0$, то $d_{ijk}^*=d_{ijk}$. А если на модернизацию будет затрачена достаточная сумма денежных средств, то это обеспечит полную функциональность данного комплекса, т. е. если $c_{ijk}=c_{ijk}^{дост}$, то $d_{ijk}^*=1$. Используя эту информацию, нетрудно найти неизвестные параметры зависимостей (3.7):

$$b_{ijk}^1=\frac{c_{ijk}^{дост}}{1-d_{ijk}},\ i=\overline{1,9},\ j=\overline{1,v_i},\ k\in M_i^j,$$

$$b_{ijk}^0=\frac{-c_{ijk}^{дост}\cdot d_{ijk}}{1-d_{ijk}},\ i=\overline{1,9},\ j=\overline{1,v_i},\ k\in M_i^j.$$

Если в системе есть хоть одно слабое звено, то злоумышленник может использовать его для получения доступа к конфиденциальной информации или проведения кибератаки на предприятие. На основании изложенного, модель информационной безопасности предприятия будет формализована в виде следующих двух задач линейного программирования (ЛП) [109]:

Задача 1 (о максимизации нижней границы функциональной эффективности ПТСЗИ и всех её компонентов для заданного бюджетного ограничения W).

$$\min\left\{Э_{ij}^*, Э_k^*, Э^*\right\}\to\max, \tag{3.8}$$

где $i=\overline{1,9}$, $j=\overline{1,v_i}$, $k=\overline{1,9}$

и с линейными ограничениями

$$Э_{ij}^*=\sum_{k\in M_i^j}N_{ijk}^1\cdot d_{ijk}^*,\quad i=\overline{1,9},\ j=\overline{1,v_i}, \tag{3.9}$$

$$Э_i^* = \sum_{j=1}^{v_i} N_{ij}^2 \cdot Э_{ij}^*, \qquad i = \overline{1,9}. \tag{3.10}$$

$$Э^* = \sum_{i=1}^{9} N_i^3 \cdot Э_i^*. \tag{3.11}$$

$$c_{ijk} = \frac{-c_{ijk}^{дост} \cdot d_{ijk}}{1-d_{ijk}} + \frac{c_{ijk}^{дост}}{1-d_{ijk}} \cdot d_{ijk}^*, \quad i = \overline{1,9}, \ j = \overline{1,v_i}, \ k \in M_i^j, \tag{3.12}$$

$$d_{ijk} \le d_{ijk}^* \le 1, \qquad i = \overline{1,9}, \ j = \overline{1,v_i}, \ k \in M_i^j, \tag{3.13}$$

$$\sum_{i=1}^{9} \sum_{j=1}^{v_i} \sum_{k \in M_i^j} c_{ijk} \le W, \tag{3.14}$$

$$d_{ijk}^* \ge 0, \ c_{ijk} \ge 0, \ i = \overline{1,9}, \qquad j = \overline{1,v_i}, \ k \in M_i^j, \tag{3.15}$$

где c_{ijk} – затраты, обеспечивающие соответствующие ожидаемые оценки d_{ijk}^* аудиторов после будущей модернизации ПТСЗИ; $c_{ijk}^{дост}$ – затраты, достаточные для обеспечения текущего режима полного функционирования комплекса, при котором все его компоненты используются и работают без нарушений; $Э_{ij}^*$, $Э_i^*$, $Э^*$ – ожидаемые оценки функциональной эффективности.

Для (3.8) используя известный приём [110], введена нижняя граница ожидаемой функциональной эффективности всех компонентов ПТСЗИ, и она максимизируется целевой функцией

$$r \to \max, \tag{3.16}$$

с линейными ограничениями (3.9) – (3.15) и

$$Э_{ij}^* \ge r, \ i = \overline{1,9}, \ j = \overline{1,v_i}, \qquad Э_i^* \ge r, \ i = \overline{1,9}, \qquad Э^* \ge r, \tag{3.17}$$

где r – неотрицательная переменная, играющая роль нижней границы ожидаемой функциональной эффективности всех компонентов ПТСЗИ.

Задача ЛП с целевой функцией (3.16), линейными ограничениями (3.9-3.14), (3.17) и условиями неотрицательности переменных (3.15), эквивалентна задаче (3.8), (3.9-3.15). Решение задачи (3.9) – (3.17) даёт ответ на вопрос, как

распределить имеющуюся сумму W, чтобы максимизировать функциональную эффективность ПТСЗИ и всех её компонентов.

Задача 2 (о минимизации суммарных затрат для обеспечения заданного уровня $U \in [0,1]$ функциональной эффективности ПТСЗИ и всех её компонентов).

Сформулирована задача ЛП с целевой функцией

$$\sum_{i=1}^{9} \sum_{j=1}^{v_i} \sum_{k \in M_{ij}} c_{ijk} \to \min, \tag{3.18}$$

с линейными ограничениями (3.9) – (3.13), (3.15) и

$$Э_{ij}^{*} \geq U,\ i = \overline{1,9},\ j = \overline{1,v_i}, \qquad Э_{i}^{*} \geq U,\ i = \overline{1,9}, \qquad Э^{*} \geq U. \tag{3.19}$$

Решение задачи ЛП (3.9) – (3.13), (3.15), (3.18), (3.19) даёт ответ на вопрос, какие минимальные затраты необходимы и как их распределить, чтобы обеспечить заданный уровень функциональной эффективности U для ПТСЗИ и всех её компонентов.

3.2. Оценка доли угроз, нарушающих свойства информации по объектам защиты ПТСЗИ

Результаты [105] рассмотренной методики представляют практический интерес с точки зрения определения доли угроз в разрезе свойств информации (конфиденциальность, целостность, доступность) по объектам защиты, в обеспечении безопасности которых задействованы комплексы СрЗИ. Для оценки доли угроз предлагаются следующие шаги.

Шаг 1. Используя данные с сайта ФСТЭК России (https://bdu.fstec.ru/files/documents/thrlist.xlsx) [10] и исходные данные таблицы 3.2 формируется двумерные бинарные массивы D_1 (для всех угроз), K (угроз конфиденциальности), Z (угроз целостности) и D (угроз доступности) элементами которых соответственно являются: δ^{*}_{jn}, δ^{**}_{jnk}, δ^{***}_{jnz} и δ^{****}_{jnd}, где

n – комплексы ($n=\overline{1,15}$), которые могут быть задействованы для противодействия j-ой угрозе ($j=\overline{1,222}$) в разрезе: k - конфиденциальности ($k=\overline{1,146}$); z -целостности ($z=\overline{1,137}$); d -доступности ($d=\overline{1,155}$) по объектам защиты [105, 109]

$$\delta^{*}_{jn}=\begin{cases}1, \text{ если } n\text{-й комплекс связан с } j\text{-й угрозой;}\\ 0, \text{ в противном случае.}\end{cases}$$

$$\delta^{**}_{jnk}=\begin{cases}1, \text{ если } n\text{-й комплекс связан } k\text{-й угрозой нарушения}\\ \text{свойства конфиденциальности}\\ \text{из общего диапазона всех } j\text{-х угроз;}\\ 0, \text{ в противном случае.}\end{cases}$$

$$\delta^{***}_{jnz}=\begin{cases}1, \text{ если } n\text{-й комплекс связан с } z\text{-ой угрозой нарушения}\\ \text{свойства целостности из общего диапазона всех } j\text{-х угроз;}\\ 0, \text{ в противном случае.}\end{cases}$$

$$\delta^{****}_{jnd}=\begin{cases}1, \text{ если } n\text{-й комплекс связан с угрозой } d\\ \text{нарушения свойства доступности из общего диапазона}\\ \text{всех } j\text{-х угроз;}\\ 0, \text{ в противном случае.}\end{cases}$$

Бинарные массивы D_1 (для всех угроз), K (угроз конфиденциальности), Z (угроз целостности) и D (угроз доступности) заполняются по форме представленной в таблице 3.3.

Таблица 3.3 – Форма для заполнения бинарного массива D_1

Наименование угрозы безопасности информации (УБИ)	Наименование комплекса СрЗИ системы ПТСЗИ, условное обозначение							Количественная оценка нарушения свойств информации в разрезе УБИ (с сайта ФСТЭК России)		
	К1	К2	К3	…	К13	К14	К15	нарушение конфиденциальности	нарушение целостности	нарушение доступности
УБИ 1								1	1	1
…	1	1	0	1	1	0	1	1	0	0
УБИ № N	0	1	1	1	0	1	1	1	1	0

Информация, которая формирует массивы по предприятию в дальнейшем будет считаться как исходная информация для определения доли угроз в разрезе

свойств информации (конфиденциальность, целостность, доступность) по объектам защиты в обеспечении безопасности которых задействованы комплексы СрЗИ [105, 109].

Шаг 2. С использованием бинарного массива D_1 для каждого комплекса, связанного с $j-$й угрозой вычисляется доля всех угроз, в противодействие которым задействованы n - ые комплексы, участвующего в защите информации [105, 109]

$$N_n^1 = \frac{1}{222}\sum_{j=1}^{222}\delta^*_{jn}, \qquad n=\overline{1,15}. \tag{3.18}$$

Шаг 3. Вычисляется доля угроз, связанных с нарушением свойства информации (конфиденциальность), в противодействие которым задействован n -й комплекс по выбранным для оценки объектам защиты [105, 109]

$$N_{jn}^2 = \frac{1}{146}\sum_{k=1}^{146}\delta^{**}_{jnk},\ j=\overline{1,222},\ n=\overline{1,15}. \tag{3.19}$$

Шаг 4. Вычисляется доля угроз, связанных с нарушением свойства информации (целостность), в противодействие которым задействован n -й комплекс по выбранным для оценки объектам защиты [105, 109]

$$N_{jn}^3 = \frac{1}{137}\sum_{z=1}^{137}\delta^{***}_{jnz},\ j=\overline{1,222},\ n=\overline{1,15}. \tag{3.20}$$

Шаг 5. Вычисляется доля угроз, связанных с нарушением свойства информации (доступность), в противодействие которым задействован n -й комплекс по выбранным для оценки объектам защиты [105, 109]

$$N_{jn}^4 = \frac{1}{155}\sum_{d=1}^{155}\delta^{****}_{jnd},\ j=\overline{1,222},\ n=\overline{1,15}. \tag{3.21}$$

Необходимо отметить, что с учётом оценок (весовых коэффициентов $A_n \in [0;1]$, где $n=\overline{1,15}$) аудитора в разрезе выполняемых функций по каждому задействованному n - му комплексу результаты, полученные по формулам с 3.18 по 3.21 будут представлены:

– для всех угроз

$$N_n^{1*} = N_n^1 \times A_n,\ N_n^1 = \frac{1}{222}\sum_{j=1}^{222}\delta^*_{jn},\ j=\overline{1,222},\ n=\overline{1,15}, \quad (3.22)$$

– для угроз, связанных с нарушением свойства конфиденциальности

$$N_{jn}^{2*} = N_{jn}^2 \times A_n,\ N_{jn}^2 = \frac{1}{146}\sum_{k=1}^{146}\delta^{**}_{jnk},\ j=\overline{1,222},\ n=\overline{1,15}, \quad (3.23)$$

– для угроз, связанных с нарушением свойства целостности

$$N_{jn}^{3*} = N_{jn}^3 \times A_n,\ N_{jn}^3 = \frac{1}{137}\sum_{z=1}^{137}\delta^{***}_{jnz},\ j=\overline{1,222},\ n=\overline{1,15}, \quad (3.24)$$

– для угроз, связанных с нарушением свойства доступности

$$N_{jn}^{4*} = N_{jn}^4 \times A_n,\ N_{jn}^4 = \frac{1}{155}\sum_{d=1}^{155}\delta^{****}_{jnd},\ j=\overline{1,222},\ n=\overline{1,15}, \quad (3.25)$$

Результаты расчётов, полученные по формулам с 3.22 по 3.25, могут быть использоваться как исходная информация для дальнейших исследований в области системного анализа в рассматриваемой предметной области. В данной диссертационной работе этот вопрос далее не исследуется.

3.3. Выводы по главе

В третьей главе разработана методика и алгоритмическое обеспечение агрегированного оценивания ПТСЗИ. Созданная во второй главе онтологическая модель обеспечила систематизацию объектов защиты, угроз и функций подсистем, что позволило построить кубическую матрицу «Угрозы – Активы – Комплексы средств защиты информации» и связанных с нею двумерные матрицы. Это сделало процесс оценки более объективным. В рамках данного подхода предложена модель повышения ИБ предприятия, охватывающая ПТСЗИ, и сформулированы две задачи ЛП об оптимальном распределении денежных средств: 1) задача о максимизации нижней границы функциональной эффективности ПТСЗИ и всех её компонентов для заданного бюджетного ограничения W; 2) задача минимизации суммарных затрат для обеспечения

заданного уровня функциональной эффективности ПТСЗИ и всех её компонентов.

Методика предусматривает использование системного подхода для оценки влияния киберугроз на конфиденциальность, целостность и доступность информации, учитывая особенности защищаемых объектов и функций ПТСЗИ. Такой подход позволяет детально анализировать и повышать эффективность защитных мер, обеспечивая их более рациональное распределение и управление в условиях ограниченных ресурсов.

4. Программная реализация методики оценки эффективности функционирования ПТСЗИ

В рамках настоящей главы с учётом онтологической модели системы ПТСЗИ, представленной в главе 2, и разработанной методики, представленной в главе 3, решаются задачи по разработке программного обеспечения для реализации процедуры агрегированного оценивания и оптимизации распределения денежных средств, направляемых на повышение эффективности СЗИ предприятия в контексте функционирования программно-технических компонент . Задача реализации процедуры агрегированного оценивания в рамках настоящей главы реализуется автором в виде комплекса «Агрегированное оценивание функциональной эффективности» (АОФЭ). В тоже время, вторая задача решается через создание программы оптимального распределения денежных средств (далее – ОРДС).

В основе решения вышеперечисленных задач лежит отнологическая модель ПТСЗИ, которая обеспечила систематизацию и структурирование данных о компонентах системы, что стало основой для создания алгоритмов и матриц, используемых в программной реализации. Применение онтологической модели позволило снизить влияние субъективных факторов и автоматизировать автору процесс обработки данных.

Пользователями комплекса «АОФЭ» и программы «ОРДС» могут быть как специалисты в области анализа данных, так и исследователи, ориентированные на решение прикладных задач.

4.1. Описание программной реализации методики оценки эффективности функционирования ПТСЗИ

С помощью программы «АОФЭ» на предприятии ООО «ЯНТА» были получены не только оценки эффективности функционирования системы ПТСЗИ и её подсистем, но и доли угроз безопасности информации,

покрываемых комплексами СрЗИ в разрезе свойств информации (конфиденциальность, целостность, доступность). Блок-схема алгоритма программы представлена в соответствие с рисунком 4.1.

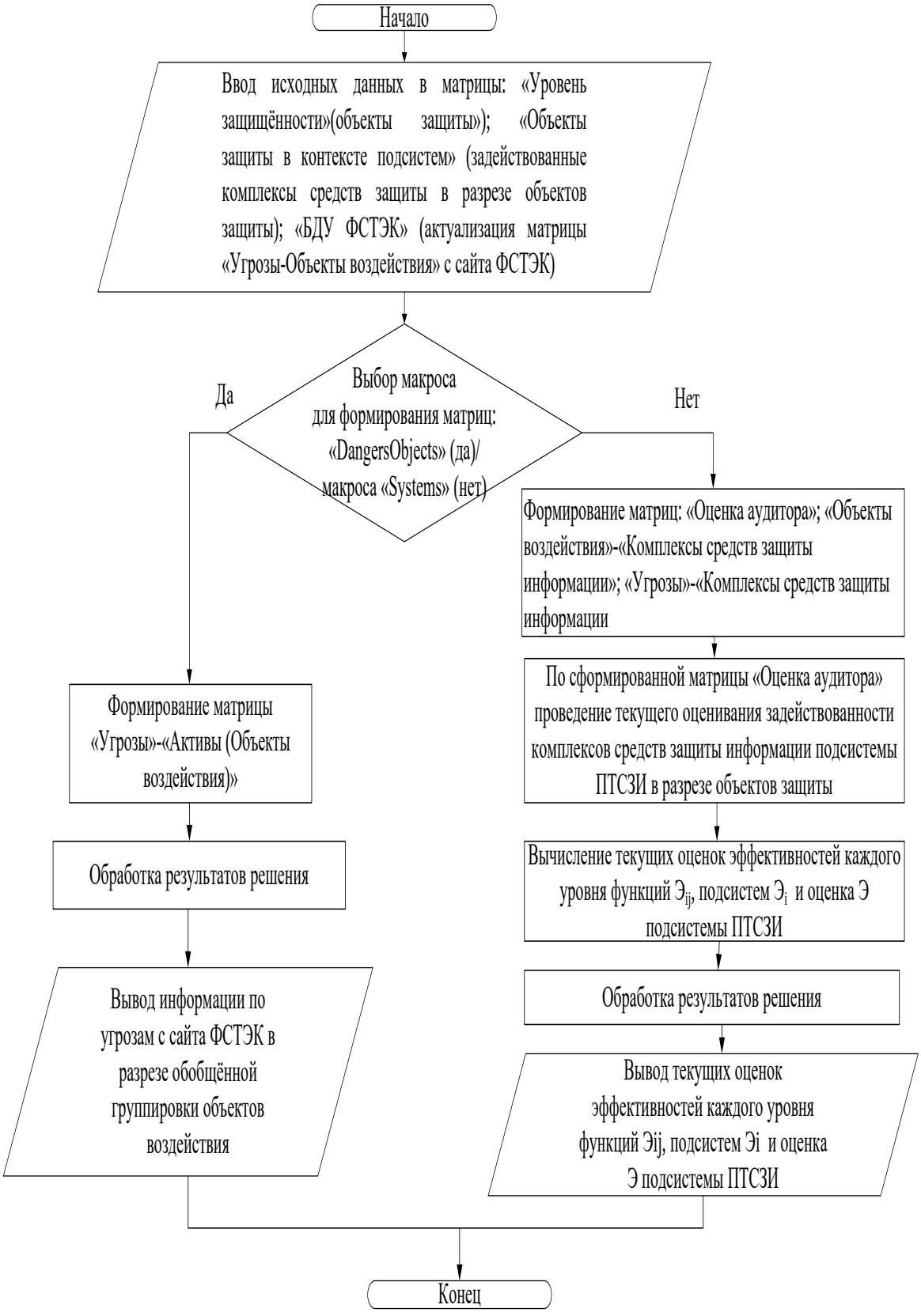


Рисунок 4.1 – Блок-схема алгоритма программы АОФЭ

Основные возможности программы комплекса «АОФЭ»: 1) позволяет создать эталонную матрицу объектов воздействия в разрезе угроз безопасности информации и взаимосвязей компонент (угрозы, объекты воздействия, комплексы СрЗИ); 2) позволяет производить расчет и в наглядном виде отобразить все задействованные компоненты в матричной форме.

Формирование матриц, используемых в комплексе «АОФЭ», основано на концептах и взаимосвязях, определённых в онтологической модели системы ПТСЗИ (глава 2). Например, матрицы «Угрозы – Комплексы средств защиты информации» и «Угрозы – Активы (Объекты воздействия)» структурированы в соответствии с онтологическими взаимосвязями между компонентами системы. Это позволило в рамках рассматриваемой главы автоматизировать создание этих матриц с помощью макросов «DangersObjects» и «Systems», обеспечив согласованность данных и корректность расчётов.

Комплекс «АОФЭ» реализован средством Visual Basic for Application Excel и представляет собой книгу в составе интегрированных в неё макросов («DangersObjects», «Systems») и набора листов (набора матриц) согласно таблицы 4.1.

Таблица 4.1 – Состав комплекса «АОФЭ»

Компоненты	Описание	Примечание
Уровень защищённости	1. Выбор объектов воздействия; Визуализация результатов работы «АОФЭ»: оценка эффективности системы ПТСЗИ и её подсистем; долей угроз по свойствам информации.	Рисунок 4.6, Рисунок 4.7, Рисунок 4.8, Рисунок 4.9, Рисунок 4.10
Оценка аудитора	1. Формруется с помощью макроса «Systems» на основе исходных данных матрицы	Рисунок 4.11, задействован макрос «Systems»

Компоненты	Описание	Примечание
	«Объекты защиты в контексте подсистем»; Внесение аудиторских оценок.	
«БДУ ФСТЭК»	Формируется лист «АОФЭ» на основе: https://bdu.fstec.ru/files/documents/thrlist.xlsx	Рисунок 4.12
«Активы (Объекты воздействия)» × «Комплексы средств защиты информации»	1. Формруется с помощью макроса «Systems» на основе исходных данных матрицы «Объекты защиты в контексте подсистем»; Задействован в формировании матрицы «Угрозы» × «Комплексы средств защиты информации» с помощью макроса «Systems» и «БДУ ФСТЭК».	Рисунок 4.13 по рисунок 4.17, задействован макрос «Systems»
«Угрозы» × «Комплексы средств защиты информации»	1. Формруется с помощью макроса «Systems» на основе матрицы «Активы (Объекты воздействия)» × «Комплексы средств защиты информации»; Для визуализации результатов связанных с вычислением долей угроз по свойствам информации.	Рисунок 4.11, задействован макрос «Systems»

Компоненты	Описание	Примечание
«Угрозы» × «Активы (Объекты воздействия)»	Формируется на основе БДУ ФСТЭК с помощью исполняемого программного кода «DangersObjects» с учётом выбранной группы (58 объектов защиты). Данный лист формируется с целью информативности сопоставления сущностей «Угрозы» и «Объекты».	Рисунок 4.18, задействован макрос «DangersObjects»
«Объекты защиты в контексте подсистем»	1. Ввода исходных данных по объектам защиты с листа «Уровень защищённости» в части задействованности комплексов СрЗИ; Визуализация результатов по вычислению долей задействованности комплексов защиты в разрезе подсистем и выполняемых ими функций.	Рисунок 4.19 и рисунок 4.20

Для наглядного представления матрицы «Угрозы» × «Активы (Объекты воздействия)» (таблица 4.1) реализован программный код «DangersObjects», который представлен в соответствии с рисунком 4.2.

Блок-схема программного кода «Systems» представлена в соответствии с рисунком 4.3 и в соответствии с рисунком 4.4. Алгоритм программного кода «Systems» предусматривает обновление значений программного обеспечения «АОФЭ» по вкладкам-листам, приведённым в таблице 4.1.

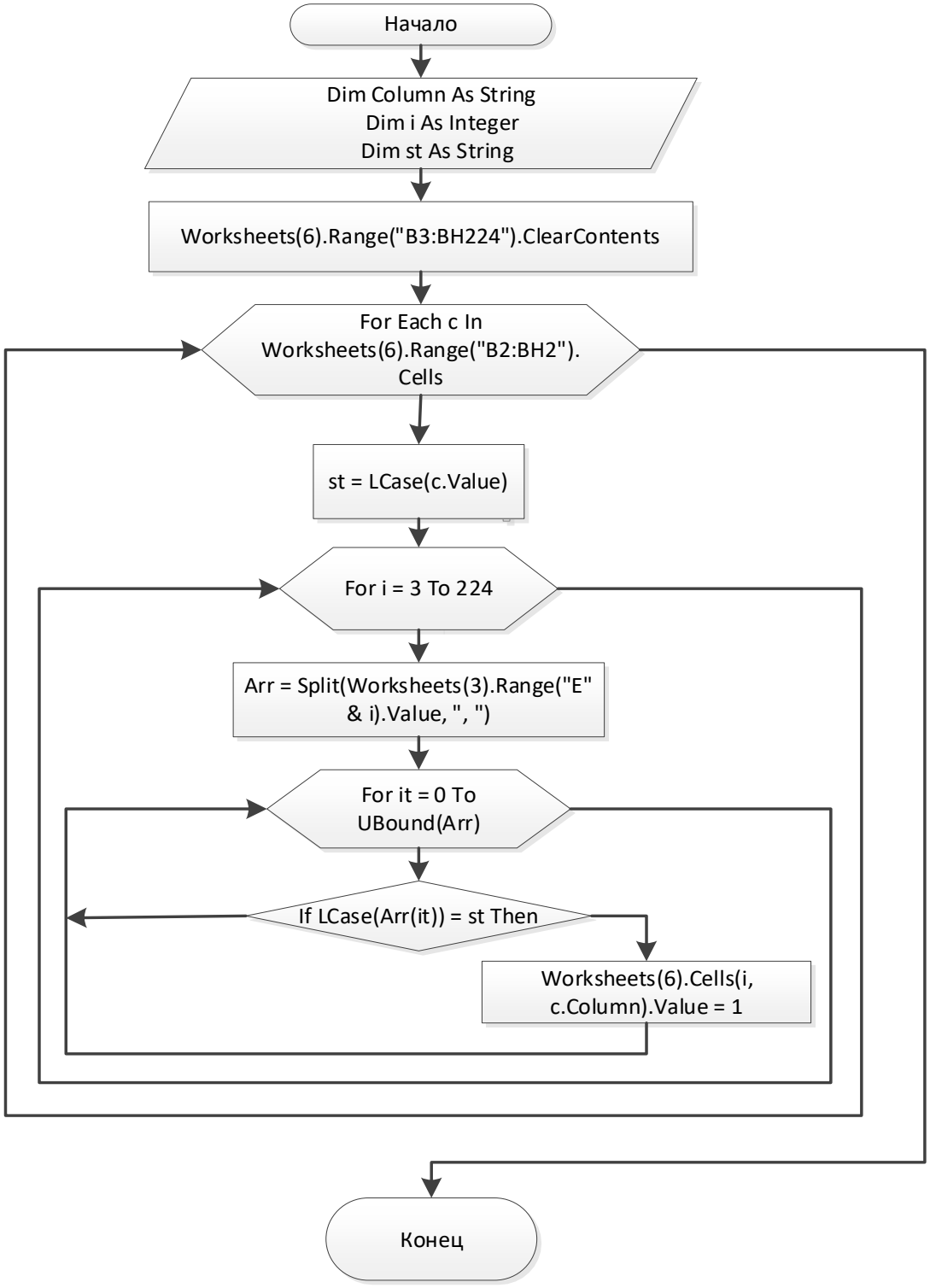


Рисунок 4.2 – Блок-схема программного кода «DangersObjects» VBA Excel для создания матрицы связки «Угрозы-Объекты» программной реализации АОФЭ

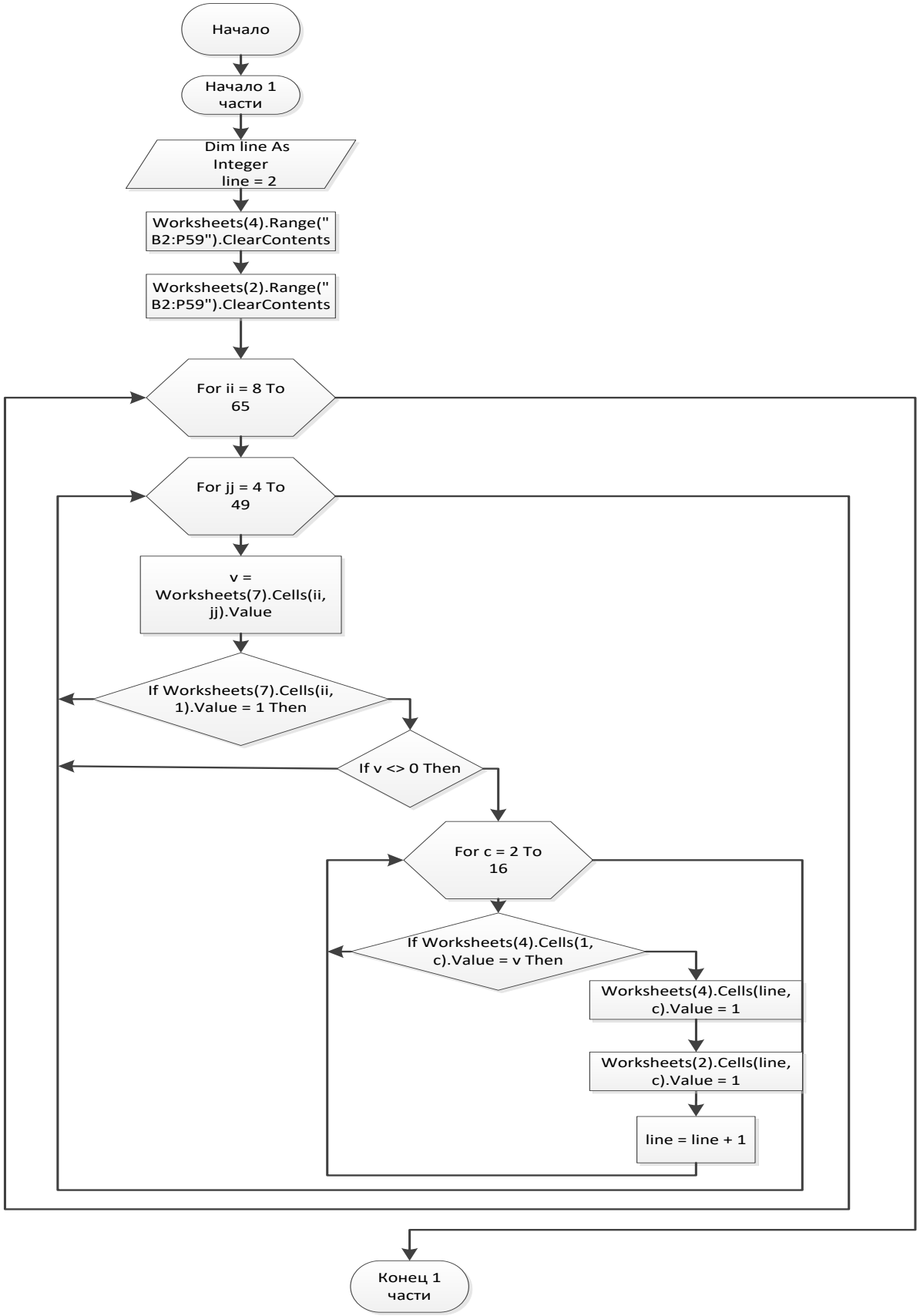


Рисунок 4.3 – Блок-схема программного кода «Systems» VBA Excel для создания матрицы связки «Объекты воздействия – Комплексы» и «Оценка аудитора» программной реализации АОФЭ

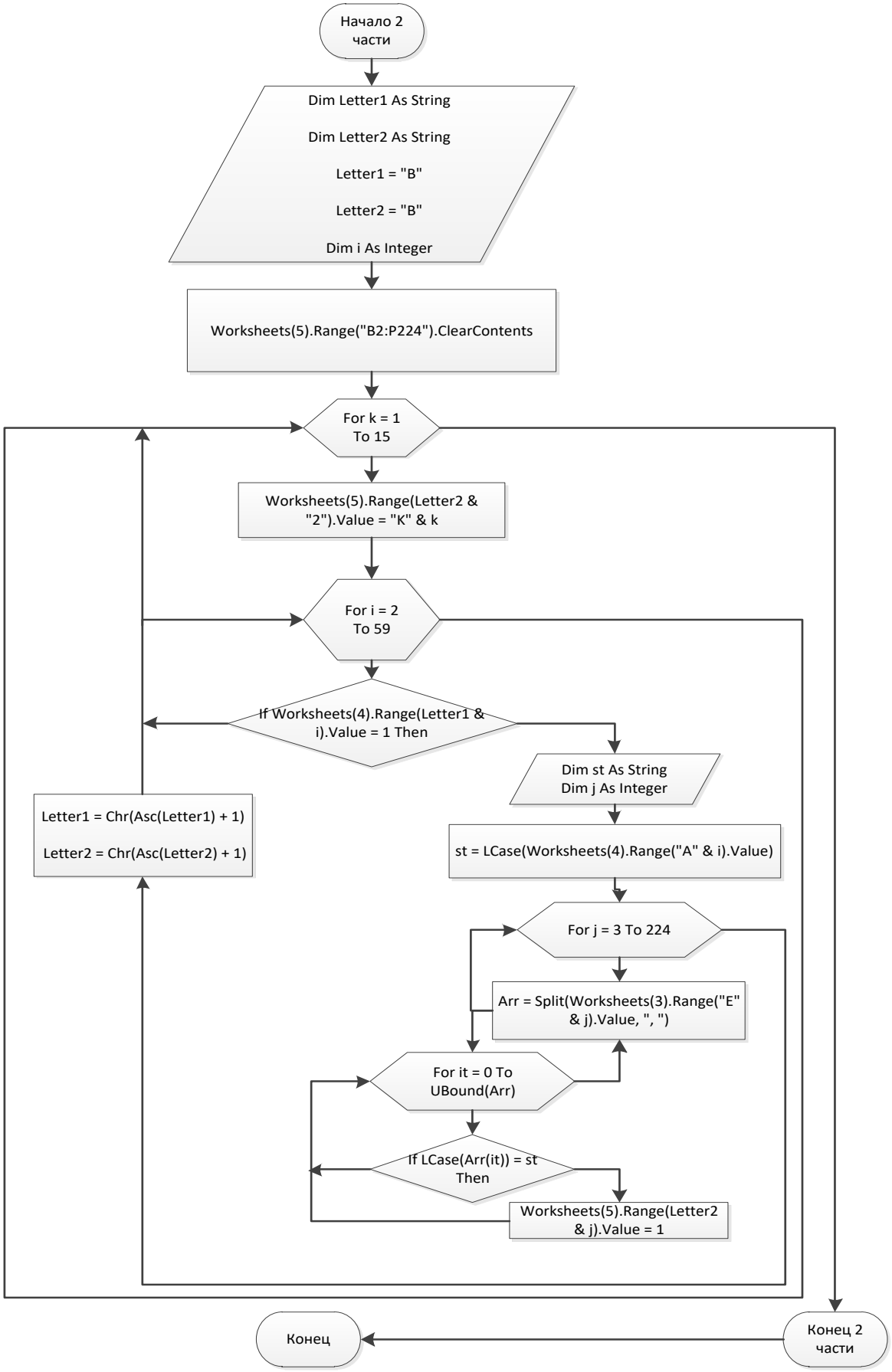


Рисунок 4.4 – Блок-схема программного кода «Systems» VBA Excel для создания матрицы связки «Угрозы – Комплексы»

Созданный средствами VBA MS Office Excel программный код «Systems» в соответствии с рисунком 4.3 и рисунком 4.4 выполняет операции по созданию динамических связей («Объекты – Комплексы»; «Угрозы – Комплексы»; «Оценка аудитора») на разных листах рабочей книги Excel.

Представим описание алгоритма работы программного кода «Systems» (Рисунок 4.5):

– очищается содержимое диапазона ячеек «B2:P59» в рабочем листе № 4 (Объекты – Комплексы) и диапазона ячеек «B2:P59» в рабочем листе № 2 (Оценка аудитора);

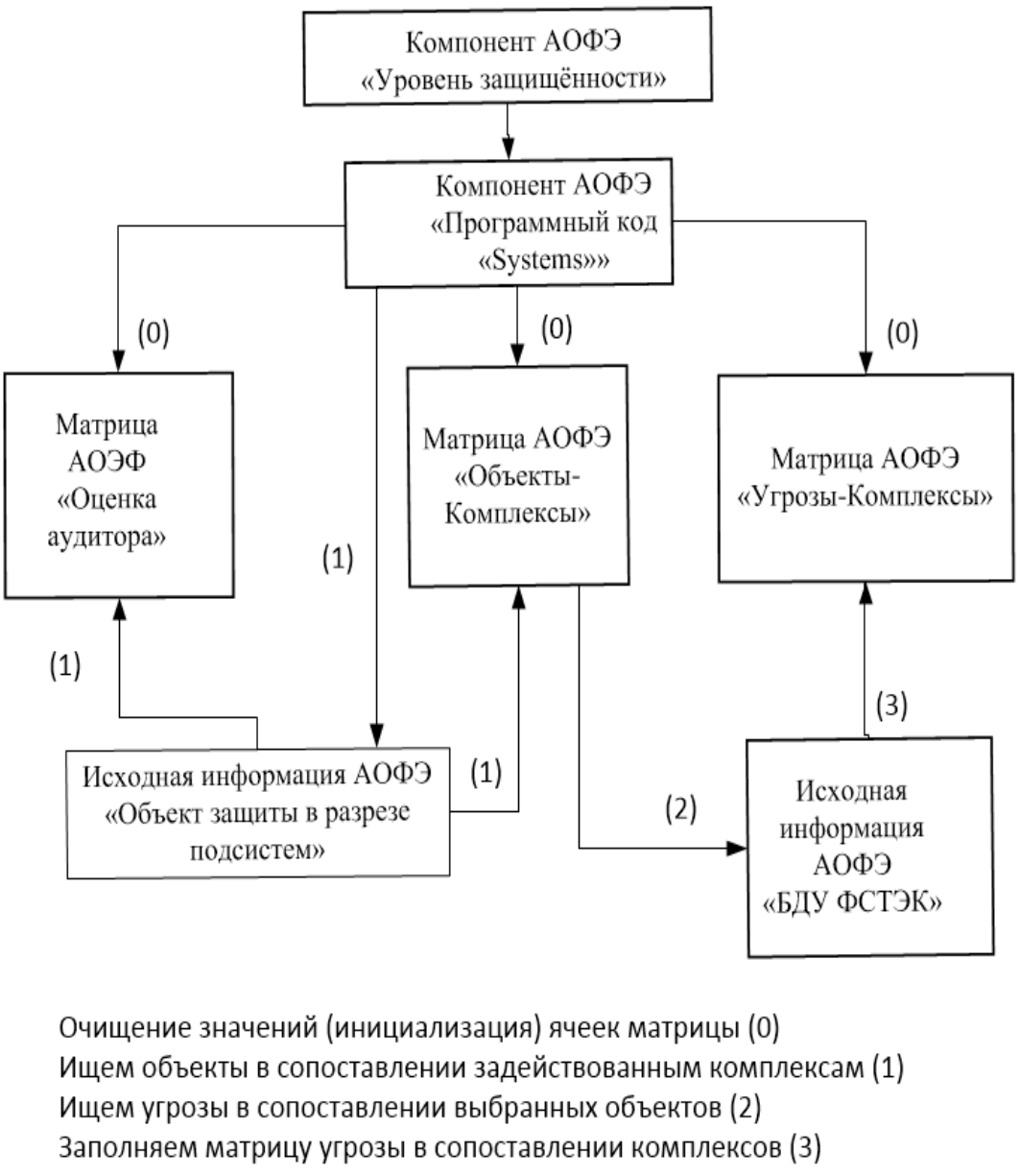


Рисунок 4.5 – Программная реализация программного кода «Systems»

– запускается цикл по формированию матриц № 4 и № 2. В связи с чем, осуществляется анализ ячеек в диапазоне «D4:AX65» в рабочем листе №7 (Объект воздействия в разрезе подсистем) на предмет поиска ячеек с ненулевым значением. Если текущая ячейка имеет значение, отличное от нуля, и соответствующая ячейка в столбце «А» равна «1», то код ищет первое вхождение этого значения в диапазоне столбцов «B1:P1» в рабочем листе № 4 (Объекты – Комплексы). Если значение найдено в рабочем листе № 4, код вводит «1» в соответствующую ячейку в диапазоне «B2:P59» в рабочем листе № 4, а также вводит «1» в соответствующую ячейку в диапазоне «B2:P59» в рабочем листе №2 (Оценка аудитора). Затем код производит переход к следующей ячейке в диапазоне «D4:AX65» на рабочем листе № 7. По завершению цикла формирования матриц № 4 и № 2 осуществляется переход на следующую позицию выполнения кода;

– производится очистка и заполнение содержимого диапазона «B2:P224» в рабочем листе № 5 (Угрозы – Комплексы). Программный код перебирает все столбцы от «B» до «P» в рабочем листе № 5 (Угрозы – Комплексы) и выполняет следующие операции: 1) код выбирает столбец «B2» рабочего листа № 5 (Угрозы – Комплексы); 2) код перебирает все строки от 2 до 59 в рабочем листе № 4 (Объекты – Комплексы). Если текущая ячейка рабочего листа № 4 имеет значение «1», код извлекает значение в столбце «А» для этой строки, преобразует его в строчный регистр и сохраняет в переменной; 3) код перебирает все строки от 3 до 224 в рабочем листе № 3 (БДУ ФСТЭК), и ищет значение в нижнем регистре, сохраненное на предыдущем этапе, в значениях, разделенных запятыми, в столбце «Е» для каждой строки. Если строчное значение найдено в любом из значений, разделенных запятыми, код вводит «1» в соответствующую ячейку рабочего листа № 5 (Угрозы – Комплексы) и переходит к следующей строке рабочего листа № 4 Объекты – Комплексы). После завершения цикла подпрограмма завершается.

На рисунке 4.6 по рисунок 4.10 представлены фрагменты таблиц «Объекты воздействия (защиты)», где осуществляется выбор объектов воздействия и визуализация результатов работы «АОФЭ».

Обновить значения

/Обновляет информацию в таблицах:
1 Объекты-комплексы
2 Оценка аудитора
3 Угрозы-комплексы
И долю угроз, покрываемых комплексов

№ п.п.	Объекты воздействия (защиты)	Выбор объекта защиты по предприятию (шкала [0;1])	Задействовано комплексов	Эталон
1	база данных	1	7	15
2	виртуальная машина	1	5	15
3	Виртуальные накопители	0	0	0
4	виртуальные устройства	0	0	0
5	Вычислительный узел суперкомпьютера	0	0	0
6	гипервизор	1	5	15
7	грид-система	0	0	0
8	Данные об учетных записях	1	7	15
9	(Технические средства или программно-	0	0	0
10	Защищаемая информация	1	7	15
11	Защищаемая информация, хранящаяся на компьютере во временных файлах	0	0	0
12	информационная система	1	6	15
13	облако	0	0	0
14	Инфраструктура информационных систем	0	0	0
15	Канал связи	1	2	15
16	обработки данных	0	0	0
17	инфраструктуры	1	7	15
18	консоль управления гипервизором	0	0	0
19	инфраструктурой	0	0	0
20	Машинный носитель информации	1	5	15
21	метаданные	1	6	15
22	или программно-аппаратные средства	0	0	0
23	микропрограммное обеспечение	0	0	0
24	микропрограммное обеспечение BIOS/UEFI	0	0	0
25	Мобильные устройства	0	0	0
26	модели машинного обучения	0	0	0
27	облачная инфраструктура	0	0	0
28	Облачная инфраструктура, созданная с использованием технологий виртуализации	0	0	0
29	облачная система	0	0	0
30	облачный сервер	0	0	0
31	образ виртуальной машины	0	0	0
32	обучающие данные машинного обучения	0	0	0
33	программируемые логические контроллеры	0	0	0
34	и хранения информации	0	0	0
35	программно-аппаратные средства со встроенными функциями защиты	1	7	15
36	Программное обеспечение автоматизированной системы управления	0	0	0
37	Программные средства	1	7	15
38	машинное обучение	0	0	0
39	технологии искусственного интеллекта	0	0	0
40	распределённые системы контроля	0	0	0
41	реестр	0	0	0
42	Ресурсные центры грид-системы	0	0	0
43	сервер	1	6	15
44	сетевой трафик	1	3	15
45	сетевой узел	1	7	15
46	больших данных	1	7	15
47	операционную систему компьютера	1	6	15
48	Система хранения данных суперкомпьютера	0	0	0
49	Средство защиты информации	1	7	15
50	Телекоммуникационное оборудование	0	0	0
51	телекоммуникационное устройство	0	0	0
52	аппаратные средства	0	0	0
53	точка беспроводного доступа	1	6	15
54	узлы грид-системы	0	0	0
55	узлы хранилища больших данных	1	7	15
56	программные средства контроля	0	0	0
57	Файлы и каталоги	1	7	15
58	Хранилище больших данных	1	7	15
			134	330

Рисунок 4.6 –Фрагмент таблицы «Объекты воздействия (защиты)»

G24 | база данных

Доля угроз, связанная с нарушением свойства информации (конфиденциальность), усл. ед.	Доля угроз, связанная с нарушением свойства информации (целостность), усл. ед.	Доля угроз, связанная с нарушением свойства информации (доступность), усл. ед.	Доля всех угроз, связанная с нарушением всех свойств информации
0,822	0,766	0,768	0,779
0,836	0,774	0,781	0,797
0,822	0,766	0,768	0,779
0,000	0,000	0,000	0,000
0,000	0,000	0,000	0,000
0,767	0,686	0,671	0,712
0,000	0,000	0,000	0,000
0,836	0,774	0,781	0,797
0,000	0,000	0,000	0,000
0,795	0,737	0,735	0,757
0,000	0,000	0,000	0,000
0,000	0,000	0,000	0,000
0,000	0,000	0,000	0,000
0,808	0,752	0,748	0,761
0,000	0,000	0,000	0,000

Результат оценки комплексов, реализующих свои функции по объектам защиты (шкала оценки от 0 до 1)	
К1	1,000
К2	1,000
К3	1,000
К4	0,000
К5	0,000
К6	1,000
К7	0,000
К8	1,000
К9	0,000
К10	1,000
К11	0,000
К12	0,000
К13	0,000
К14	1,000
К15	0,000

"Тепловая карта" критериев оценивания	
1	отлично
0,8	хорошо
0,6	средне
0,4	удовлетворительно
0,2	плохо
0	не работает

Оценка функциональной эффективности подсистемы ПТР КСЗИ

0,630

Наименование комплексов и их условное обозначение
К1 Комплекс встроенных средств защиты серверов и автоматизированных рабочих ма-шин (АРМ) под управлением операционных систем (ОС) семейства Windows
К2 Комплекс антивирусной защиты
К3 Комплекс резервного копирования
К4 Комплекс защиты среды виртуализации
К5 Комплекс сбора, анализа и корреляции событий ИБ
К6 Комплекс встроенных средств АСО
К7 Комплекс резервного копирования конфигурационных файлов АСО
К8 Комплекс межсетевого экранирования
К9 Комплекс обнаружения вторжений
К10 Комплекс встроенных средств защиты систем хранения данных
К11 Комплекс централизованного управления СрЗИ
К12 Комплекс анализа защищенности
К13 Комплекс контроля целостности
К14 Комплекс встроенных средств защиты прикладного программного обеспечения (ППО)
К15 Комплекс контроля использования информационных ресурсов

№ п.п.	Объекты воздействия (защиты)	Выбор объекта защиты по предприятию (шкала [0;1])	Задействовано комплексов
1	база данных	1	7
2	виртуальная машина	1	5
3	Виртуальные накопители	0	0
4	виртуальные устройства	0	0
5	Вычислительный узел суперкомпьютера	0	0
6	гипервизор	1	5
7	грид-система	0	0
8	Данные об учетных записях	1	7
9	устройства (Технические средства или	0	0
10	Защищаемая информация	1	7
11	Защищаемая информация, хранящаяся на компьютере во временных файлах	0	0
12	информационная система	1	6
13	иммигрированная в облако	0	0
14	Инфраструктура информационных систем	0	0
15	Канал связи	1	2
16	обработки данных	0	0

Оценка эффективности каждого уровня i-ой подсистемы уровня ПТР КСЗИ, усл. ед.						Оценка комплекс числу св разного т подсис объект
Подсистема контроля и управления доступом (П1)	0,735	А1	0,67	К1	1,0	
				К4	0,0	
				К8	1,0	
				К10	1,0	
				К14	1,0	
				К15	0,0	
		А2	0,50	К1	1,0	
				К15	0,0	
		А3	1,00	К6	1,0	
				К8	1,0	
Подсистема регистрации и учета (П2)	0,500	Б1	0,50	К1	1,0	
				К2	1,0	
				К4	0,0	
				К5	0,0	
				К6	1,0	
				К8	1,0	
				К9	0,0	
				К10	1,0	
				К12	0,0	
				К13	0,0	
				К14	1,0	
				К15	0,0	
		Б2	0,50	К1	1,0	
				К15	0,0	
Подсистема обеспечения целостности (П3)	0,333	В1	0,33	К1	1,0	
				К12	0,0	
				К13	0,0	
		В2	0,33	К1	1,0	
				К12	0,0	
				К13	0,0	
Подсистема антивирусной защиты (П4)	1,000	Г1	1,00	К2	1,0	
		Г2	1,00	К8	1,0	
Подсистема контроля		Д1	0,50	К1	1,0	

Уровень защищённости | Оценка аудитора | БДУ ФСТЭК | Объекты-комплексы | Угрозы-комплексы | Угрозы-объекты

Готово | Специальные возможности: проверьте рекомендации | 80 %

Рисунок 4.7 – Фрагмент листа «Уровень защищённости»

Оценка эффективности каждого уровня i-ой подсистемы уровня ПТР КСЗИ, усл. ед.						комплекса одного типа к общему числу связей всех комплексов разного типа по j-й функции i-й подсистемы по выбранным объектам защиты, усл. ед.	Оценка, касающаяся убыли эффективности подсистемы ПТР КСЗИ, усл. ед.	Оценка, касающаяся убыли эффективности каждого уровня j-ой функции i-й подсистемы ПТР, усл. ед.	Задействованы комплексы по j-ой функции i-й подсистемы уровня ПТР КСЗИ	(комплексы по j-ой функции i-й подсистемы уровня ПТР КСЗИ)	Наименование и условное обозначение j-ой функции i-й подсистемы уровня ПТР КСЗИ
Подсистема контроля и управления доступом (П1)	0,735	А1	0,67	К1	1,0	0,25	0,265	0,33	4,00	6,00	А1- контроль и управление доступом к защищаемым информационным ресурсам
				К4	0,0	0,00					
				К8	1,0	0,29					
				К10	1,0	0,22					
				К14	1,0	0,25					
				К15	0,0	0,00					
		А2	0,50	К1	1,0	1,00		0,50	1,00	2,00	А2- контроль и управление доступом к внешним носителям информации и периферийным устройствам
				К15	0,0	0,00					
		А3	1,00	К6	1,0	0,39		0,00	2,00	2,00	А3- контроль доступа к АСО
				К8	1,0	0,61					
Подсистема регистрации и учета (П2)	0,500	Б1	0,50	К1	1,0	0,17	0,500	0,50	6,00	12,00	Б1- регистрация и учет действий пользователей и процессов
				К2	1,0	0,19					
				К4	0,0	0,00					
				К5	0,0	0,00					
				К6	1,0	0,12					
				К8	1,0	0,19					
				К9	0,0	0,00					
				К10	1,0	0,15					
				К12	0,0	0,00					
				К13	0,0	0,00					
				К14	1,0	0,17					
				К15	0,0	0,00					
		Б2	0,50	К1	1,0	1,00		0,50	1,00	2,00	Б2- регистрация событий доступа к внешним устройствам и портам ввода-вывода
				К15	0,0	0,00					
Подсистема обеспечения целостности (П3)	0,333	В1	0,33	К1	1,0	1,00	0,667	0,67	1,00	3,00	В1- контроль целостности исполняемых и конфигурационных файлов СрЗИ, компонентов ОС и прикладного ПО
				К12	0,0	0,00					
				К13	0,0	0,00					
		В2	0,33	К1	1,0	1,00		0,67	1,00	3,00	В2- контроль неизменности параметров встроенных СрЗИ и компонентов системного ПО
				К12	0,0	0,00					
				К13	0,0	0,00					
Подсистема антивирусной защиты (П4)	1,000	Г1	1,00	К2	1,0	1,00	0,000	0,00	1,00	1,00	Г1- защита файловой системы от вирусов и вредоносных программ
		Г2	1,00	К8	1,0	1,00		0,00	1,00	1,00	Г2- потоковая защита межсетевого трафика от вирусов и вредоносных программ
Подсистема контроля использования информационных ресурсов (П5)	0,500	Д1	0,50	К1	1,0	1,00	0,500	0,50	1,00	2,00	Д1- контроль каналов утечек защищаемой информации
				К15	0,0	0,00					
		Д2	Не применимо	К15	0,0	Не применимо		1,00	0,00	1,00	Д2- обнаружение несанкционированного хранения конфиденциальной информации
Подсистема централизованного управления СрЗИ (П6)	0,000	Е1	Не применимо	К11	0,0	Не применимо	1,000	1,00	0,00	1,00	Е1- обеспечение возможности оперативного получения информации о состоянии защищенности
		Е2	Не применимо	К11	0,0	Не применимо		1,00	0,00	1,00	Е2- обеспечение автоматизации рутинных задач
Подсистема анализа защищенности (П7)	0,000	Ж1	Не применимо	К12	0,0	Не применимо	1,000	1,00	0,00	1,00	Ж1- предоставление в виде отчетов информации об обнаруженных уязвимостях с рекомендациями по их устранению
		Ж2	Не применимо	К12	0,0	Не применимо		1,00	0,00	1,00	Ж2- обеспечение инвентаризации узлов, выявление и идентификация уязвимостей
Подсистема обеспечения сетевой безопасности (П8)	0,690	З1	1,00	К8	1,0	1,00	0,310	0,00	1,00	1,00	З1- межсетевое экранирование ЛВС
		З2	Не применимо	К9	0,0	Не применимо		1,00	0,00	1,00	З2- обнаружение вторжений в ЛВС
		З3	0,50	К6	1,0	0,39		0,50	2,00	4,00	З3- обеспечение безопасного функционирования сетевого оборудования
				К7	0,0	0,00					
				К8	1,0	0,61					
				К9	0,0	0,00					
Подсистема обеспечения непрерывности функционирования (П9)	0,500	И	0,50	К3	1,0	1,00	0,500	0,50	1,00	2,00	И- резервное копирование конфигурационных файлов СрЗИ и восстановление данных из резервных копий в случаях сбоев
				К7	0,0	0,00					

Рисунок 4.8 – Фрагмент таблицы «Оценка текущей функциональной эффективности подсистем ПТСЗИ»

Доля угроз, связанная с нарушением свойства информации (конфиденциальность), усл. ед.	Доля угроз, связанная с нарушением свойства информации (целостность), усл. ед.	Доля угроз, связанная с нарушением свойства информации (доступность), усл. ед.	Доля всех угроз, связанная с нарушением всех свойств информации
0,822	0,766	0,768	0,779
0,836	0,774	0,781	0,797
0,822	0,766	0,768	0,779
0,000	0,000	0,000	0,000
0,000	0,000	0,000	0,000
0,767	0,686	0,671	0,712
0,000	0,000	0,000	0,000
0,836	0,774	0,781	0,797
0,000	0,000	0,000	0,000
0,795	0,737	0,735	0,757
0,000	0,000	0,000	0,000
0,000	0,000	0,000	0,000
0,000	0,000	0,000	0,000
0,808	0,752	0,748	0,761
0,000	0,000	0,000	0,000

Результат оценки комплексов, реализующих свои функции по объектам защиты (шкала оценки от 0 до 1)	
К1	1,000
К2	1,000
К3	1,000
К4	0,000
К5	0,000
К6	1,000
К7	0,000
К8	1,000
К9	0,000
К10	1,000
К11	0,000
К12	0,000
К13	0,000
К14	1,000
К15	0,000

"Тепловая карта" критериев оценивания	
1	отлично
0,8	хорошо
0,6	средне
0,4	удовлетворительно
0,2	плохо
0	не работает

Оценка функциональной эффективности подсистемы ПТР КСЗИ
0,630

Результат оценки комплексов, реализующих свои функции по объектам защиты (шкала оценки от 0 до 1)	
К1	1,000
К2	1,000
К3	1,000
К4	0,000
К5	0,000
К6	1,000
К7	0,000
К8	1,000
К9	0,000
К10	1,000
К11	0,000
К12	0,000
К13	0,000
К14	1,000
К15	0,000

"Тепловая карта" критериев оценивания	
1	отлично
0,8	хорошо
0,6	средне
0,4	удовлетворительно
0,2	плохо
0	не работает

Оценка функциональной эффективности подсистемы ПТР КСЗИ
0,630

Рисунок 4.9 – Фрагмент таблиц Итоговая оценка функциональной эффективности системы ПТСЗИ листа «Уровень защищённости»

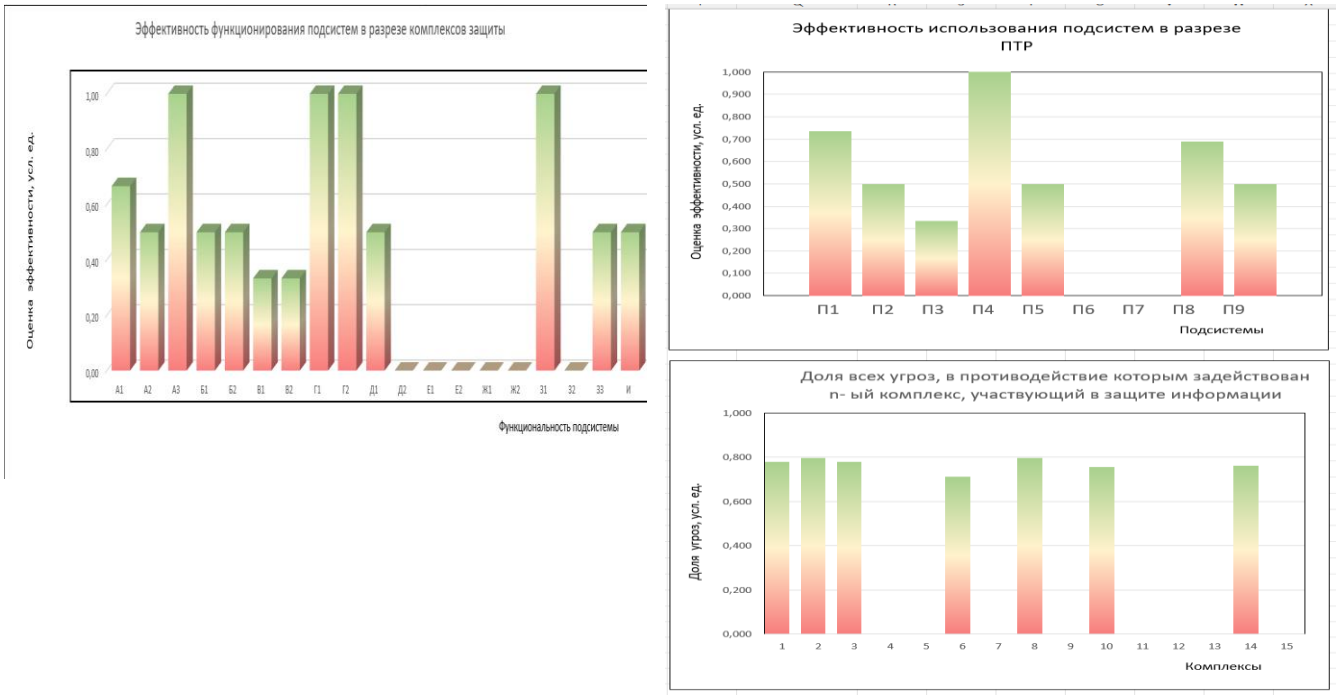


Рисунок 4.10 – Фрагмент динамических гистограмм листа «Уровень защищённости»

На рисунке 4.11 представлены матрицы «Оценка аудитора» и «Объекты – Комплексы», которые формируются с помощью макроса «Systems» на основе исходных данных матрицы «Объекты защиты в контексте подсистем».

Наименование комплекса уровня ПТР / Объекты защиты БДУ ФСТЭК	К1	К2	К3	К4	К5	К6	К7	К8	К9	К10	К11	К12	К13	К14	К15
база данных	1	1	1			1		1		1				1	
виртуальная машина	1	1	1					1						1	
Виртуальные накопители															
виртуальные устройства															
Вычислительный узел суперкомпьютера															
гипервизор	1	1	1					1						1	
грид-система															
Данные об учетных записях	1	1	1			1		1		1				1	
Данные пользователя мобильного устройства (Технические средства или программно-аппаратные средства)															
Защищаемая информация	1	1	1			1		1		1				1	
Защищаемая информация, хранящаяся на компьютере во временных файлах															
информационная система	1	1	1					1		1				1	
информационная система, иммигрированная в облако															
Инфраструктура информационных систем															
Канал связи		1						1							
Климатическое оборудование центра обработки данных															
ключевая система информационной инфраструктуры	1	1	1			1		1		1				1	
консоль управления гипервизором															
консоль управления облачной инфраструктурой															
Машинный носитель информации	1	1	1					1		1					
метаданные	1	1	1					1		1				1	
Микропрограммное и Технические средства или программно-аппаратные средства BIOS/UEFI															
микропрограммное обеспечение															
микропрограммное обеспечение BIOS/UEFI															
Мобильные устройства															
модели машинного обучения															
облачная инфраструктура															
Облачная инфраструктура, созданная с использованием технологий виртуализации															
облачная система															
облачный сервер															
образ виртуальной машины															
обучающие данные машинного обучения															
программируемые логические контроллеры															
Программно-аппаратные средства обработки и хранения информации															
программно-аппаратные средства со встроенными функциями защиты	1	1	1			1		1		1				1	
Программное обеспечение автоматизированной системы управления технологическими															
Программные средства	1	1	1			1		1		1				1	
Программные средства, использующие машинное обучение															
Программные средства, реализующие технологии искусственного интеллекта															
распределённые системы контроля															
реестр															
Ресурсные центры грид-системы															
сервер	1	1	1					1		1				1	
сетевой трафик		1				1		1							
сетевой узел	1	1	1			1		1		1				1	
система разграничения доступа хранилища больших данных	1	1	1			1		1		1				1	
Система управления доступом встроенная в операционную систему компьютера	1	1	1					1		1				1	
Система хранения данных суперкомпьютера															
Средство защиты информации	1	1	1			1		1		1				1	
Телекоммуникационное оборудование															
телекоммуникационное устройство															
Технические средства или программно-аппаратные средства															
точка беспроводного доступа	1	1	1			1		1						1	
узлы грид-системы															
узлы хранилища больших данных	1	1	1			1		1		1				1	
управленческие системы и другие программные средства контроля															
Файлы и каталоги	1	1	1			1		1		1				1	
Хранилище больших данных	1	1	1			1		1		1				1	

Рисунок 4.11 – Матрица «Оценка аудитора» и «Объекты – Комплексы», формируемые программным кодом «Systems»

На рисунке 4.12 представлен фрагмет листа «АОФЭ» на основе данных с сайта ФСТЭК России (https://bdu.fstec.ru/files/documents/thrlist.xlsx)

B186 | Угроза агрегирования данных, обрабатываемых с помощью мобильного устройства

	Общая информация					Последствия			Дополнительно	
	Идентиф	Наименование УБИ	Описание	Источник угрозы (характеристика и потенциал нарушителя)	Объект воздействия	Нарушение конфиденциальности	Нарушение целостности	Нарушение доступности	Дата включения угрозы в БнД УБИ	Дата последнего изменения данных
186	184	Угроза агрегирования данных, обрабатываемых с помощью мобильного устройства	Угроза заключается в возможности осуществления нарушителем сбора и анализа информации, обрабатываемой с помощью мобильного устройства, за счёт использования специального программного обеспечения, встраиваемого пользователем в системное программное обеспечение мобильного устройства, а также встраиваемого в мобильные программы под видом программной платформы для их разработки другими компаниями. Данная угроза обусловлена наличием в мобильном устройстве множества каналов передачи данных, а также сложностью контроля потоков информации в таком устройстве. Реализация данной угрозы возможна при условии использования мобильных устройств пользователями. В качестве собираемой информации могут выступать: персональные данные пользователя и контактирующих с ним лиц (пол, возраст, религиозные и политические взгляды и др.); информация ограниченного доступа (история браузера, список контактов пользователя, история звонков и др.); данные об окружающей среде (текущее местоположение мобильного устройства, маршруты движения, наличие беспроводных сетей в радиусе доступа); видеоданные, снимаемые видеокамерами мобильного устройства; аудиоданные, снимаемые микрофоном устройства	Внутренний нарушитель со средним потенциалом	Мобильные устройства	1	0	0	23.06.2016	11.02.2019
	185	Угроза несанкционированного изменения параметров настройки средств защиты информации	Угроза заключается в возможности осуществления нарушителем несанкционированного изменения параметров настройки Средство защиты информации. Данная угроза обусловлена слабостями мер разграничения доступа к конфигурационным файлам Средство защиты информации. Реализация данной угрозы возможна при условии получения нарушителем прав доступа к программному интерфейсу управления средством защиты информации, а также при наличии у нарушителя сведений о структуре и формате файлов конфигурации Средство защиты информации	Внешний нарушитель с низким потенциалом; Внутренний нарушитель с низким потенциалом	Средство защиты информации	1	1	1	23.06.2016	11.02.2019

Уровень защищённости | Оценка аудитора | БДУ ФСТЭК | Объекты-комплексы | Угрозы-комплексы | Угрозы-объекты

Готово | Фильтр: отбор | Специальные возможности: проверьте рекомендации | 100 %

Рисунок 4.12 – Фрагмент массива (угрозы безопасности, источники угроз, объекты воздействия в разрезе свойств информации) с сайта ФСТЭК

На рисунке 4.13 по рисунок 4.17 представлен фрагмент матрицы «Угрозы» × «Комплексы средств защиты информации», которая формируется с помощью макроса «Systems» на основе исходных данных матрицы «Объекты защиты в контексте подсистем» сведений с сайта ФСТЭК России.

Наименование комплекса уровня ПТР / УБИ	Наименование комплекса уровня ПТР КСЗИ, условное обозначение														Последствия от нарушения УБИ в разрезе свойств информации		
Наименование угрозы безопасности информации (УБИ)	К1	К2	К3	К4	К5	К6	К7	К8	К9	К10	К11	К12	К13	К14	К15	Нарушение конфиденциальности	Нарушение целостности	Нарушение доступности
Угроза автоматического распространения вредоносного кода в грид-системе																1	1	1
Угроза агрегирования данных, передаваемых в грид-системе		1				1		1								1	0	0
Угроза использования слабостей криптографических алгоритмов и уязвимостей в программном обеспечении их реализации	1	1	1			1		1		1				1		1	1	0
Угроза аппаратного сброса пароля BIOS																0	1	0
Угроза внедрения вредоносного кода в BIOS																1	1	1
Угроза внедрения кода или данных	1	1	1			1		1		1				1		1	1	1
Угроза воздействия на программы с высокими привилегиями	1	1	1			1		1		1				1		1	1	0
Угроза восстановления и/или повторного использования аутентификационной информации	1	1	1			1		1		1				1		1	0	0
Угроза восстановления предыдущей уязвимой версии BIOS																1	1	1
Угроза выхода процесса за пределы виртуальной машины	1	1	1			1		1		1				1		1	1	1
Угроза деавторизации санкционированного клиента беспроводной сети	1	1	1			1		1		1				1		0	0	1
Угроза деструктивного изменения конфигурации/среды окружения программ	1	1	1			1		1		1				1		1	1	1
Угроза деструктивного использования декларированного функционала BIOS																0	1	0
Угроза длительного удержания вычислительных ресурсов пользователями	1	1	1			1		1		1				1		0	0	1
Угроза доступа к защищаемым файлам с использованием обходного пути	1	1	1			1		1		1				1		1	0	0
Угроза доступа к локальным файлам сервера при помощи URL	1	1	1			1		1		1				1		1	0	0
Угроза доступа/перехвата/изменения HTTP cookies	1	1	1			1		1		1				1		1	0	1
Угроза загрузки нештатной операционной системы																1	1	1
Угроза заражения DNS-кеша	1	1	1			1		1		1				1		1	0	0
Угроза злоупотребления возможностями, предоставленными потребителям облачных услуг	1	1	1					1						1		1	1	1
Угроза злоупотребления доверием потребителей облачных услуг																1	1	0
Угроза избыточного выделения оперативной памяти	1	1	1			1		1		1				1		0	0	1
Угроза изменения компонентов информационной (автоматизированной) системы	1	1	1			1		1		1				1		1	1	1
Угроза изменения режимов работы аппаратных элементов компьютера																0	1	1
Угроза изменения системных и глобальных переменных	1	1	1			1		1		1				1		1	1	1
Угроза искажения XML-схемы	1	1	1			1		1		1				1		0	1	1
Угроза искажения вводимой и выводимой на периферийные устройства информации	1	1	1			1		1		1				1		0	1	0
Угроза использования альтернативных путей доступа к ресурсам	1	1	1			1		1		1				1		1	0	0
Угроза использования вычислительных ресурсов суперкомпьютера «паразитными»																0	0	1
Угроза использования информации идентификации/аутентификации, заданной по	1	1	1			1		1		1				1		1	1	1
Угроза использования механизмов авторизации для повышения привилегий	1	1	1			1		1		1				1		1	0	0
Угроза использования поддельных цифровых подписей BIOS																0	1	0
Угроза использования слабостей кодирования входных данных	1	1	1			1		1		1				1		0	1	1
Угроза использования слабостей протоколов сетевого/локального обмена данными	1	1	1			1		1		1				1		1	1	1
Угроза использования слабых криптографических алгоритмов BIOS																1	1	1
Угроза исследования механизмов работы программы	1	1	1			1		1		1				1		1	0	1
Угроза исследования приложения через отчёты об ошибках	1	1	1			1		1		1				1		1	0	0
Угроза исчерпания вычислительных ресурсов хранилища больших данных	1	1	1					1		1				1		0	0	1
Угроза исчерпания запаса ключей, необходимых для обновления BIOS																0	1	0
Угроза конфликта юрисдикций различных стран																0	0	1
Угроза межсайтового скриптинга	1	1	1			1		1		1				1		1	1	1
Угроза межсайтовой подделки запроса	1	1	1			1		1		1				1		1	1	1
Угроза нарушения доступности облачного сервера																0	0	1
Угроза нарушения изоляции пользовательских данных внутри виртуальной машины	1	1	1					1						1		1	1	1
Угроза нарушения изоляции среды исполнения BIOS																1	1	1
Угроза нарушения процедуры аутентификации субъектов виртуального информационного	1	1	1			1		1		1				1		1	0	1
Угроза нарушения работоспособности грид-системы при нетипичной сетевой нагрузке		1				1		1								0	0	1
Угроза нарушения технологии обработки информации путём несанкционированного	1	1	1			1		1		1				1		1	1	1
Угроза нарушения целостности данных кеша	1	1	1			1		1		1				1		0	1	1
Угроза неверного определения формата входных данных, поступающих в хранилище	1	1	1			1		1		1				1		0	1	0
Угроза невозможности восстановления сессии работы на ПЭВМ при выводе из	1	1	1			1		1		1				1		0	1	1
Угроза невозможности миграции образов виртуальных машин из-за несовместимости	1	1	1			1		1		1				1		0	1	1
Угроза невозможности управления правами пользователей BIOS																1	1	1
Угроза недобросовестного исполнения обязательств поставщиками облачных услуг	1	1	1			1		1		1				1		1	1	1
Угроза незащищённого администрирования облачных услуг	1	1	1			1		1		1				1		1	1	1
Угроза некачественного переноса инфраструктуры в облако	1	1	1					1		1				1		1	1	1
Угроза неконтролируемого копирования данных внутри хранилища больших данных	1	1	1			1		1		1				1		1	0	0
Угроза неконтролируемого роста числа виртуальных машин																0	0	1
Угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов	1	1	1					1		1				1		0	0	1
Угроза неконтролируемого уничтожения информации хранилищем больших данных	1	1	1			1		1		1				1		0	1	1
Угроза некорректного задания структуры данных транзакции	1	1	1			1		1		1				1		0	1	1
Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера	1	1	1			1		1		1				1		1	0	0
Угроза некорректного использования функционала программного и аппаратного	1	1	1			1		1		1				1		1	1	1
Угроза некорректной реализации политики лицензирования в облаке	1	1	1			1		1		1				1		0	0	1
Угроза неопределённости в распределении ответственности между ролями в облаке	1	1	1			1		1		1				1		1	1	1
Угроза неопределённости ответственности за обеспечение безопасности облака																1	1	1

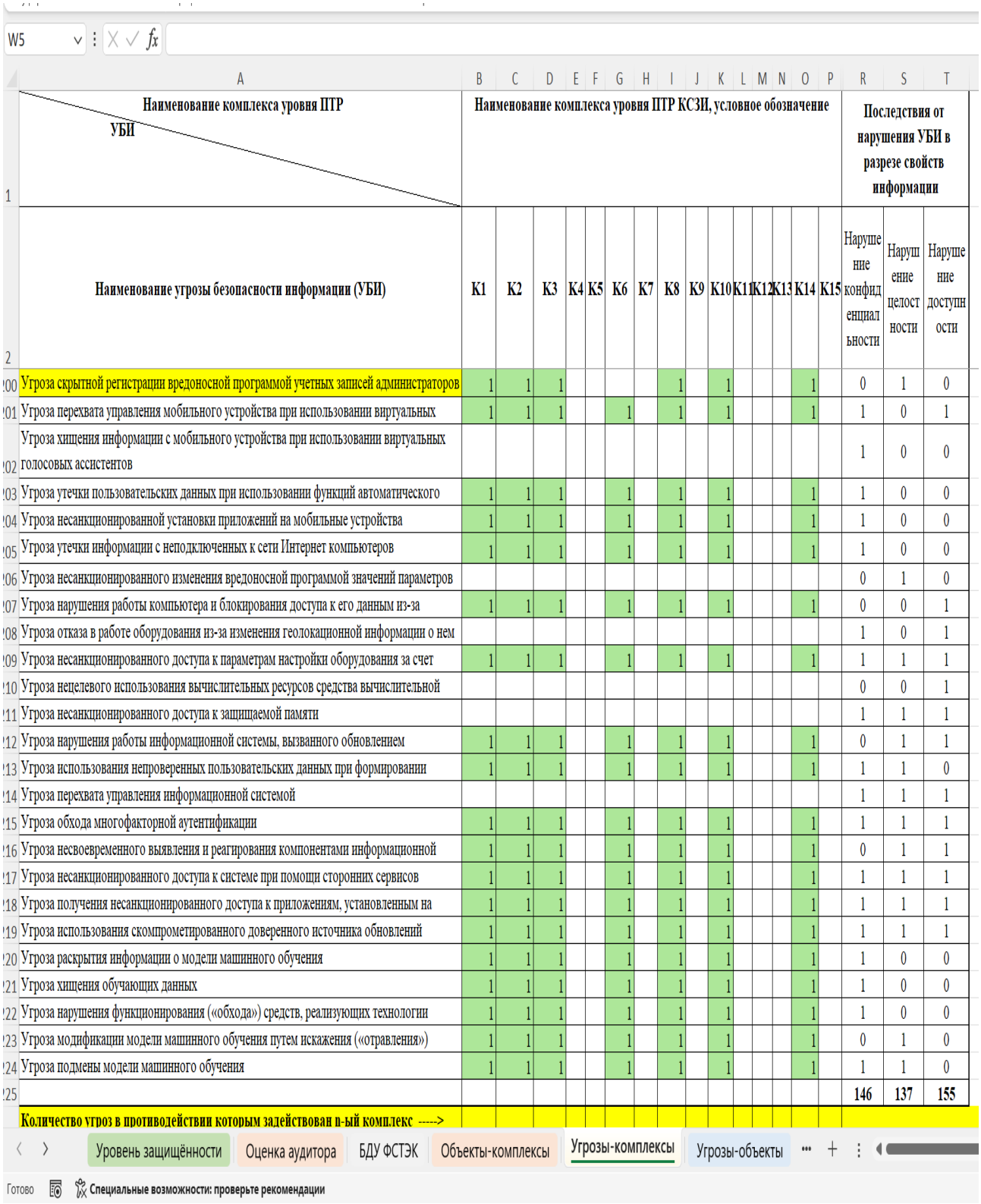
Рисунок 4.13 – Матрица «Угрозы безопасности информации – Комплексы», формируемые программным кодом «Systems»

Наименование комплекса уровня ПТР / УБИ	Наименование комплекса уровня ПТР КСЗИ, условное обозначение															Последствия от нарушения УБИ в разрезе свойств информации		
Наименование угрозы безопасности информации (УБИ)	К1	К2	К3	К4	К5	К6	К7	К8	К9	К10	К11	К12	К13	К14	К15	Нарушение конфиденциальности	Нарушение целостности	Нарушение доступности
Угроза неопределённости ответственности за обеспечение безопасности облака																1	1	1
Угроза неправомерного ознакомления с защищаемой информацией	1	1	1			1		1		1				1		1	0	0
Угроза неправомерного/некорректного использования интерфейса взаимодействия с	1	1	1			1		1		1				1		1	1	1
Угроза неправомерных действий в каналах связи		1				1		1								1	1	0
Угроза непрерывной модернизации облачной инфраструктуры																0	1	1
Угроза несанкционированного восстановления удалённой защищаемой информации	1	1	1					1		1						1	0	0
Угроза несанкционированного выключения или обхода механизма защиты от записи в																1	1	1
Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и	1	1	1			1		1		1				1		1	1	1
Угроза несанкционированного доступа к аутентификационной информации	1	1	1			1		1		1				1		1	0	0
Угроза несанкционированного доступа к виртуальным каналам передачи	1	1	1			1		1		1				1		1	0	0
Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или)	1	1	1					1						1		0	0	1
Угроза несанкционированного доступа к данным за пределами зарезервированного	1	1	1					1		1				1		0	1	1
Угроза несанкционированного доступа к защищаемым виртуальным машинам из	1	1	1					1						1		1	1	1
Угроза несанкционированного доступа к защищаемым виртуальным машинам со стороны	1	1	1					1						1		1	1	1
Угроза несанкционированного доступа к защищаемым виртуальным устройствам из																1	1	1
Угроза несанкционированного доступа к локальному компьютеру через клиента грид-																1	1	1
Угроза несанкционированного доступа к сегментам вычислительного поля																1	1	0
Угроза несанкционированного доступа к системе по беспроводным каналам	1	1	1			1		1		1				1		1	1	1
Угроза несанкционированного доступа к системе хранения данных из виртуальной и (или)																1	1	1
Угроза несанкционированного доступа к хранимой в виртуальном пространстве	1	1	1			1		1		1				1		1	0	0
Угроза несанкционированного изменения аутентификационной информации	1	1	1			1		1		1				1		0	1	1
Угроза несанкционированного использования привилегированных функций BIOS																1	1	1
Угроза несанкционированного копирования защищаемой информации	1	1	1			1		1		1				1		1	0	0
Угроза несанкционированного редактирования реестра	1	1	1			1		1		1				1		1	1	1
Угроза несанкционированного создания учётной записи пользователя	1	1	1			1		1		1				1		1	1	1
Угроза несанкционированного удаления защищаемой информации	1	1	1			1		1		1				1		0	0	1
Угроза несанкционированного удалённого внеполосного доступа к аппаратным средствам	1	1	1					1		1				1		1	1	1
Угроза несанкционированного управления буфером	1	1	1			1		1		1				1		1	1	1
Угроза несанкционированного управления синхронизацией и состоянием	1	1	1			1		1		1				1		0	1	1
Угроза несанкционированного управления указателями	1	1	1			1		1		1				1		1	1	1
Угроза несогласованности политик безопасности элементов облачной инфраструктуры	1	1	1			1		1		1				1		1	1	1
Угроза несогласованности правил доступа к большим данным	1	1	1			1		1		1				1		1	0	1
Угроза обнаружения открытых портов и идентификации привязанных к ним сетевых служб	1	1	1			1		1		1				1		1	0	0
Угроза обнаружения хостов	1	1	1			1		1		1				1		1	0	0
Угроза обхода некорректно настроенных механизмов аутентификации	1	1	1			1		1		1				1		1	1	1
Угроза общедоступности облачной инфраструктуры	1	1	1			1		1		1				1		1	1	1
Угроза опосредованного управления группой программ через совместно используемые	1	1	1			1		1		1				1		0	1	1
Угроза определения типов объектов защиты	1	1	1			1		1		1				1		1	0	0
Угроза определения топологии вычислительной сети	1	1	1			1		1		1				1		1	0	0
Угроза отказа в загрузке входных данных неизвестного формата хранилищем больших	1	1	1			1		1		1				1		0	1	1
Угроза отказа в обслуживании системой хранения данных суперкомпьютера																0	0	1
Угроза отключения контрольных датчиков	1	1	1			1		1		1				1		0	1	1
Угроза ошибки обновления гипервизора	1	1	1			1		1		1				1		1	1	1
Угроза перебора всех настроек и параметров приложения	1	1	1			1		1		1				1		0	1	1
Угроза перегрузки грид-системы вычислительными заданиями																0	0	1
Угроза передачи данных по скрытым каналам	1	1	1			1		1		1				1		1	0	0
Угроза передачи запрещённых команд на оборудование с числовым программным	1	1	1			1		1		1				1		0	1	0
Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной	1	1	1			1		1		1				1		0	1	1
Угроза переполнения целочисленных переменных	1	1	1			1		1		1				1		1	1	1
Угроза перехвата вводимой и выводимой на периферийные устройства информации	1	1	1			1		1		1				1		1	0	0
Угроза перехвата данных, передаваемых по вычислительной сети	1	1	1			1		1		1				1		1	0	0
Угроза перехвата привилегированного потока	1	1	1			1		1		1				1		1	1	1
Угроза перехвата привилегированного процесса	1	1	1			1		1		1				1		1	1	1
Угроза перехвата управления гипервизором	1	1	1			1		1		1				1		1	1	1
Угроза перехвата управления средой виртуализации	1	1	1			1		1		1				1		1	1	1
Угроза повреждения системного реестра	1	1	1			1		1		1				1		0	1	1
Угроза повышения привилегий	1	1	1			1		1		1				1		1	1	1
Угроза подбора пароля BIOS																1	0	1
Угроза подделки записей журнала регистрации событий	1	1	1			1		1		1				1		0	1	0
Угроза подключения к беспроводной сети в обход процедуры аутентификации	1	1	1			1		1		1				1		1	1	1
Угроза подмены беспроводного клиента или точки доступа	1	1	1			1		1		1				1		1	0	1
Угроза подмены действия пользователя путём обмана	1	1	1			1		1		1				1		1	1	1
Угроза подмены доверенного пользователя	1	1	1			1		1		1				1		1	0	0

Рисунок 4.14 – Матрица «Угрозы безопасности информации – Комплексы», формируемые программным кодом «Systems»

Наименование комплекса уровня ПТР / УБИ	Наименование комплекса уровня ПТР КСЗИ, условное обозначение															Последствия от нарушения УБИ в разрезе свойств информации		
Наименование угрозы безопасности информации (УБИ)	К1	К2	К3	К4	К5	К6	К7	К8	К9	К10	К11	К12	К13	К14	К15	Нарушение конфиденциальности	Нарушение целостности	Нарушение доступности
Угроза подмены резервной копии программного обеспечения BIOS																0	1	0
Угроза подмены содержимого сетевых ресурсов	1	1	1			1		1		1				1		1	0	0
Угроза подмены субъекта сетевого доступа	1	1	1			1		1		1				1		1	1	0
Угроза получения предварительной информации об объекте защиты	1	1	1			1		1		1				1		1	0	0
Угроза получения сведений о владельце беспроводного устройства	1	1	1			1		1		1				1		1	0	0
Угроза потери доверия к поставщику облачных услуг	1	1	1			1		1		1				1		1	1	1
Угроза потери и утечки данных, обрабатываемых в облаке	1	1	1			1		1		1				1		1	1	1
Угроза потери информации вследствие несогласованности работы узлов хранилища	1	1	1			1		1		1				1		0	1	1
Угроза потери управления облачными ресурсами	1	1	1			1		1		1				1		1	1	1
Угроза потери управления собственной инфраструктурой при переносе её в облако	1	1	1			1		1		1				1		1	1	1
Угроза преодоления физической защиты	1	1	1					1		1				1		1	1	1
Угроза приведения системы в состояние «отказ в обслуживании»	1	1	1			1		1		1				1		0	0	1
Угроза привязки к поставщику облачных услуг	1	1	1			1		1		1				1		0	0	1
Угроза приостановки оказания облачных услуг вследствие технических сбоев	1	1	1			1		1		1				1		0	0	1
Угроза программного выведения из строя средств хранения, обработки и (или)	1	1	1					1		1						0	1	1
Угроза программного сброса пароля BIOS	1	1	1			1		1		1				1		1	1	0
Угроза пропуска проверки целостности программного обеспечения	1	1	1			1		1		1				1		0	1	1
Угроза прямого обращения к памяти вычислительного поля суперкомпьютера	1	1	1			1		1		1				1		1	0	0
Угроза распространения несанкционированно повышенных прав на всю грид-систему	1	1	1			1		1		1				1		1	1	0
Угроза сбоя автоматического управления системой разграничения доступа хранилища	1	1	1			1		1		1				1		1	0	1
Угроза сбоя обработки специальным образом изменённых файлов	1	1	1			1		1		1				1		1	1	1
Угроза сбоя процесса обновления BIOS		1						1								0	0	1
Угроза сканирования веб-сервисов, разработанных на основе языка описания WSDL	1	1	1			1		1		1				1		1	0	0
Угроза удаления аутентификационной информации	1	1	1			1		1		1				1		1	1	1
Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи	1	1	1			1		1		1				1		0	0	1
Угроза установки уязвимых версий обновления программного обеспечения BIOS																1	1	1
Угроза утраты вычислительных ресурсов	1	1	1			1		1		1				1		0	0	1
Угроза утраты носителей информации	1	1	1					1		1						1	0	1
Угроза физического выведения из строя средств хранения, обработки и (или)	1	1	1					1		1				1		0	1	1
Угроза форматирования носителей информации	1	1	1					1		1						0	1	1
Угроза «форсированного веб-браузинга»	1	1	1			1		1		1				1		1	0	0
Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации	1	1	1					1		1				1		1	0	1
Угроза чрезмерного использования вычислительных ресурсов суперкомпьютера в ходе																0	0	1
Угроза эксплуатации цифровой подписи программного кода	1	1	1			1		1		1				1		1	1	1
Угроза перехвата исключения/сигнала из привилегированного блока функций	1	1	1			1		1		1				1		1	1	1
Угроза распространения состояния «отказ в обслуживании» в облачной инфраструктуре																1	1	1
Угроза включения в проект не достоверно испытанных компонентов	1	1	1			1		1		1				1		1	1	1
Угроза внедрения системной избыточности	1	1	1			1		1		1				1		0	0	1
Угроза заражения компьютера при посещении неблагонадёжных сайтов	1	1	1			1		1		1				1		1	1	1
Угроза «кражи» учётной записи доступа к сетевым сервисам	1	1	1			1		1		1				1		1	0	1
Угроза наличия механизмов разработчика	1	1	1			1		1		1				1		1	1	1
Угроза неправомерного шифрования информации	1	1	1			1		1		1				1		0	0	1
Угроза скрытного включения вычислительного устройства в состав бот-сети	1	1	1			1		1		1				1		0	0	1
Угроза распространения «почтовых червей»	1	1	1			1		1		1				1		1	1	1
Угроза «спама» веб-сервера	1	1	1			1		1		1				1		0	0	1
Угроза «фарминга»	1	1	1			1		1		1				1		1	0	0
Угроза «фишинга»	1	1	1			1		1		1				1		1	0	0
Угроза нарушения технологического/производственного процесса из-за временны́х	1	1	1			1		1		1				1		0	0	1
Угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью	1	1	1			1		1		1				1		0	1	1
Угроза несанкционированного использования системных и сетевых утилит	1	1	1			1		1		1				1		1	1	1
Угроза несанкционированной модификации защищаемой информации	1	1	1			1		1		1				1		0	1	0
Угроза отказа подсистемы обеспечения температурного режима																0	0	1
Угроза перехвата одноразовых паролей в режиме реального времени	1	1	1			1		1		1				1		0	1	0
Угроза физического устаревания аппаратных компонентов																0	0	1
Угроза перехвата управления автоматизированной системой управления технологическими																0	1	1
Угроза агрегирования данных, обрабатываемых с помощью мобильного устройства																1	0	0
Угроза несанкционированного изменения параметров настройки средств защиты	1	1	1			1		1		1				1		1	1	1
Угроза внедрения вредоносного кода через рекламу, сервисы и контент	1	1	1			1		1		1				1		0	1	1
Угроза несанкционированного воздействия на средство защиты информации	1	1	1			1		1		1				1		1	1	1
Угроза подмены программного обеспечения	1	1	1			1		1		1				1		1	1	1
Угроза маскирования действий вредоносного кода	1	1	1			1		1		1				1		0	1	1
Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети Интернет	1	1	1			1		1		1				1		1	1	1
Угроза внедрения вредоносного кода в дистрибутив программного обеспечения	1	1	1			1		1		1				1		1	1	1
Угроза использования уязвимых версий программного обеспечения	1	1	1			1		1		1				1		1	1	1
Угроза утечки информации за счет применения вредоносным программным обеспечением	1	1	1			1		1		1				1		1	0	0
Угроза несанкционированного использования привилегированных функций мобильного																1	1	1
Угроза удаленного запуска вредоносного кода в обход механизмов защиты операционной																0	1	0
Угроза контроля вредоносной программой списка приложений, запущенных на мобильном устройстве																0	1	1
Угроза хищения аутентификационной информации из временных файлов cookie	1	1	1			1		1		1				1		1	0	0
Угроза скрытной регистрации вредоносной программой учетных записей администраторов	1	1	1					1		1				1		0	1	0

Рисунок 4.15 – Матрица «Угрозы безопасности информации – Комплексы», формируемые программным кодом «Systems»



Наименование комплекса уровня ПТР / УБИ	Наименование комплекса уровня ПТР КСЗИ, условное обозначение														Последствия от нарушения УБИ в разрезе свойств информации		
Наименование угрозы безопасности информации (УБИ)	К1	К2	К3	К4	К5	К6	К7	К8	К9	К10	К11	К12	К13	К14	К15	Нарушение конфиденциальности	Нарушение целостности	Нарушение доступности
Угроза скрытной регистрации вредоносной программой учетных записей администраторов	1	1	1					1		1				1		0	1	0
Угроза перехвата управления мобильного устройства при использовании виртуальных	1	1	1			1		1		1				1		1	0	1
Угроза хищения информации с мобильного устройства при использовании виртуальных голосовых ассистентов																1	0	0
Угроза утечки пользовательских данных при использовании функций автоматического	1	1	1			1		1		1				1		1	0	0
Угроза несанкционированной установки приложений на мобильные устройства	1	1	1			1		1		1				1		1	0	0
Угроза утечки информации с неподключенных к сети Интернет компьютеров	1	1	1			1		1		1				1		1	0	0
Угроза несанкционированного изменения вредоносной программой значений параметров																0	1	0
Угроза нарушения работы компьютера и блокирования доступа к его данным из-за	1	1	1			1		1		1				1		0	0	1
Угроза отказа в работе оборудования из-за изменения геолокационной информации о нем																1	0	1
Угроза несанкционированного доступа к параметрам настройки оборудования за счет	1	1	1			1		1		1				1		1	1	1
Угроза нецелевого использования вычислительных ресурсов средства вычислительной																0	0	1
Угроза несанкционированного доступа к защищаемой памяти																1	1	1
Угроза нарушения работы информационной системы, вызванного обновлением	1	1	1			1		1		1				1		0	1	1
Угроза использования непроверенных пользовательских данных при формировании	1	1	1			1		1		1				1		1	1	0
Угроза перехвата управления информационной системой																1	1	1
Угроза обхода многофакторной аутентификации	1	1	1			1		1		1				1		1	1	1
Угроза несвоевременного выявления и реагирования компонентами информационной	1	1	1			1		1		1				1		0	1	1
Угроза несанкционированного доступа к системе при помощи сторонних сервисов	1	1	1			1		1		1				1		1	1	1
Угроза получения несанкционированного доступа к приложениям, установленным на	1	1	1			1		1		1				1		1	1	1
Угроза использования скомпрометированного доверенного источника обновлений	1	1	1			1		1		1				1		1	1	1
Угроза раскрытия информации о модели машинного обучения	1	1	1			1		1		1				1		1	0	0
Угроза хищения обучающих данных	1	1	1			1		1		1				1		1	0	0
Угроза нарушения функционирования («обхода») средств, реализующих технологии	1	1	1			1		1		1				1		1	0	0
Угроза модификации модели машинного обучения путем искажения («отравления»)	1	1	1			1		1		1				1		0	1	0
Угроза подмены модели машинного обучения	1	1	1			1		1		1				1		1	1	0
																146	137	155
Количество угроз в противодействии которым задействован n-ый комплекс ----->																		

Уровень защищённости | Оценка аудитора | БДУ ФСТЭК | Объекты-комплексы | Угрозы-комплексы | Угрозы-объекты

Готово | Специальные возможности: проверьте рекомендации

Рисунок 4.16 – Матрица «Угрозы безопасности информации – Комплексы», формируемые программным кодом «Systems»

Наименование комплекса уровня ПТР / УБИ	Наименование комплекса уровня ПТР КСЗИ, условное обозначение														Последствия от нарушения УБИ в разрезе свойств информации		
Наименование угрозы безопасности информации (УБИ)	K1	K2	K3	K4	K5	K6	K7	K8	K9	K10	K11	K12	K13	K14	K15	Нарушение конфиденциальности	Нарушение целостности	Нарушение доступности
Угроза подмены модели машинного обучения	1	1	1			1		1		1				1		1	1	0
																146	**137**	**155**
Количество угроз в противодействии которым задействован n-ый комплекс ----->	173	177	173	0	0	158	0	177	0	168	0	0	0	169	0			
Доля всех угроз, в противодействие которым задействован n- ый комплекс, участвующий в защите информации (формула 3.9)---------->	0,779	0,797	0,78	0	0	0,71	0	0,8	0	0,8	0	0	0	0,8	0			
Количество угроз, связанных с нарушением свойства конфиденциальности из общего диапазона j-ых угроз ФСТЭК, в противодействии которым задействован n-ый комплекс по объектам защиты ---------->	120	122	120	0	0	112	0	122	0	116	0	0	0	118	0			
Доля угроз, связанных с нарушением свойства информации (конфиденциальность), в противодействие которым задействован n- ый комплекс по выбранным для оценки объектам защиты (формула 3.10)---------->	0,822	0,836	0,82	0	0	0,77	0	0,84	0	0,8	0	0	0	0,8	0			
Количество угроз, связанных с нарушением свойства информации (целостность) из общего диапазона j-ых угроз ФСТЭК, в противодействии которым задействован n-ый комплекс по объектам защиты ---------->	105	106	105	0	0	94	0	106	0	101	0	0	0	103	0			
Доля угроз, связанных с нарушением свойства информации (целостность), в противодействие которым задействован n-ый комплекс по выбранным для оценки объектам защиты (формула 3.11) ---------->	0,766	0,774	0,77	0	0	0,69	0	0,77	0	0,7	0	0	0	0,8	0			
Количество угроз, связанных с нарушением свойства информации (доступность) из общего диапазона j-ых угроз ФСТЭК, в противодействии которым задействован n-ый комплекс по объектам защиты ---------->	119	121	119	0	0	104	0	121	0	114	0	0	0	116	0			
Доля угроз, связанных с нарушением свойства информации (доступность), в противодействие которым задействован n-ый комплекс по выбранным для оценки объектам защиты (формула 3.12)---------->	0,768	0,781	0,77	0	0	0,67	0	0,78	0	0,7	0	0	0	0,7	0			

Уровень защищённости | Оценка аудитора | БДУ ФСТЭК | Объекты-комплексы | Угрозы-комплексы | Угрозы-объекты

Готово | Специальные возможности: проверьте рекомендации

Рисунок 4.17 – Оценка доли угроз, нарушающих свойства информации

На рисунке 4.18 представлен фрагмент матрицы «Угрозы» × «Активы (Объекты воздействия)», которая формируется с помощью исполняемого программного кода «DangersObjects» с учётом выбранной группы (58 объектов защиты).

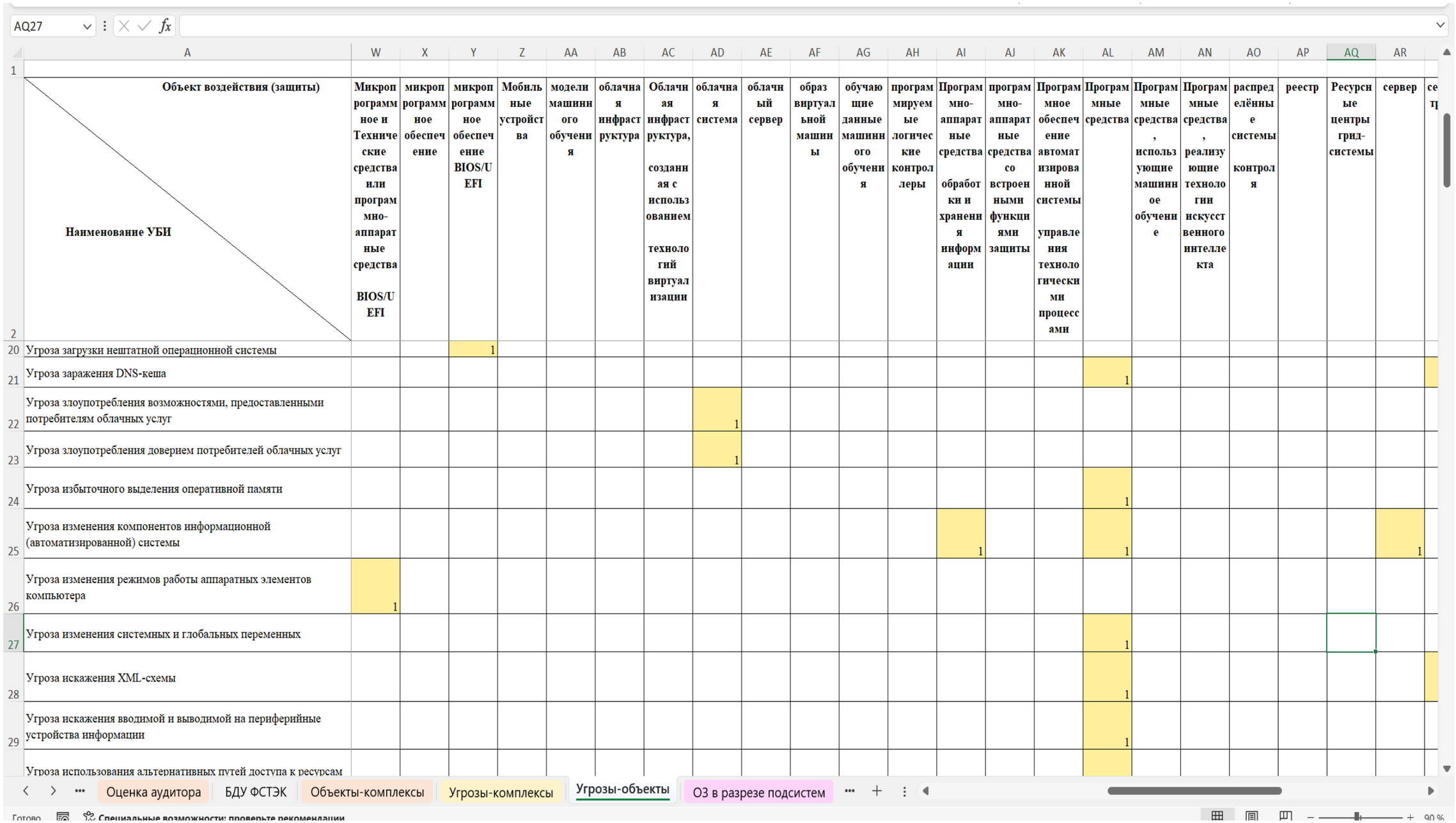


Рисунок 4.18 – Фрагмент матрицы «Угрозы-Объекты» по объектам воздействия

На рисунке 4.19 и рисунке 4.21 представлены фрагменты матрицы «Объекты защиты в контексте подсистем», который формируется как эталонная таблица исходных сведений по ПТСЗИ.

		Наименование подсистем	Подсистема контроля и управления доступом (П1)										Подсистема регистрации и учета (П2)												
		Условное обозначение подсистем	П1										П2												
	№ п.п.	Наименование j-ой функции подсистемы, условное обозначение	А1						А2		А3		Б1											Б2	
Для выбора ОЗ аудитором		Наименование j-ой функции подсистемы КСЗИ	- контроль и управление доступом к защищаемым информационным ресурсам						- контроль и управление доступом к внешним носителям информации и периферийным устройствам		- контроль доступа к АСО		- регистрация и учет действий пользователей и процессов											- регистрация событий доступа к внешним устройствам и портам ввода-вывода	
		Наименование комплекса уровня ПТР КСЗИ, условное обозначение	К4	К8	К10	К14	К15	К1	К1	К15	К6	К8	К1	К2	К4	К5	К6	К8	К9	К10	К12	К13	К14	К15	К1	К15
		Объекты защиты БДУ ФСТЭК																								
1	1	база данных	0	К8	К10	К14	0	**К1**	**0**	0	К6	К8	**К1**	К2	0	0	К6	К8	0	К10	0	0	К14	0	**К1**	0
1	2	виртуальная машина	0	К8	0	К14	0	**К1**	**0**	0	0	К8	**К1**	К2	0	0	0	К8	0	0	0	0	К14	0	**К1**	0
1	6	гипервизор	0	К8	0	К14	0	**К1**	**К1**	0	0	К8	**К1**	К2	0	0	0	К8	0	0	0	0	К14	0	**К1**	0
1	8	Данные об учетных записях	0	К8	К10	К14	0	**К1**	**К1**	0	К6	К8	**К1**	К2	0	0	К6	К8	0	К10	0	0	К14	0	**К1**	0
1	10	Защищаемая информация	0	К8	К10	К14	0	**К1**	**К1**	0	К6	К8	**К1**	К2	0	0	К6	К8	0	К10	0	0	К14	0	**К1**	0
1	12	информационная система	0	К8	К10	К14	0	**К1**	**К1**	0	0	К8	**К1**	К2	0	0	0	К8	0	К10	0	0	К14	0	**К1**	0
1	15	Канал связи	0	К8	0	0	0	0	0	0	0	К8	0	К2	0	0	0	К8	0	0	0	0	0	0	0	0
1	17	ключевая система информационной инфраструктуры	0	К8	К10	К14	0	**К1**	**К1**	0	К6	К8	**К1**	К2	0	0	К6	К8	0	К10	0	0	К14	0	**К1**	0
1	20	Машинный носитель информации	0	К8	К10	0	0	**К1**	**К1**	0	0	К8	**К1**	К2	0	0	0	К8	0	К10	0	0	0	0	**К1**	0
1	21	метаданные	0	К8	К10	К14	0	**К1**	**К1**	0	0	К8	**К1**	К2	0	0	0	К8	0	К10	0	0	К14	0	**К1**	0
1	35	программно-аппаратные средства со встроенными функциями защиты	0	К8	К10	К14	0	**К1**	**К1**	0	К6	К8	**К1**	К2	0	0	К6	К8	0	К10	0	0	К14	0	**К1**	0
1	37	Программные средства	0	К8	К10	К14	0	**К1**	**К1**	0	К6	К8	**К1**	К2	0	0	К6	К8	0	К10	0	0	К14	0	**К1**	0
1	43	сервер	0	К8	К10	К14	0	**К1**	**К1**	0	0	К8	**К1**	К2	0	0	0	К8	0	К10	0	0	К14	0	**К1**	0
1	44	сетевой трафик	0	К8	0	0	0	0	0	0	К6	К8	0	К2	0	0	К6	К8	0	0	0	0	0	0	0	0
1	45	сетевой узел	0	К8	К10	К14	0	**К1**	**К1**	0	К6	К8	**К1**	К2	0	0	К6	К8	0	К10	0	0	К14	0	**К1**	0
1	46	система разграничения доступа хранилища больших данных	0	К8	К10	К14	0	**К1**	**К1**	0	К6	К8	**К1**	К2	0	0	К6	К8	0	К10	0	0	К14	0	**К1**	0
1	47	Система управления доступом встроенная в операционную систему компьютера	0	К8	К10	К14	0	**К1**	**К1**	0	0	К8	**К1**	К2	0	0	0	К8	0	К10	0	0	К14	0	**К1**	0
1	49	Средство защиты информации	0	К8	К10	К14	0	**К1**	**К1**	0	К6	К8	**К1**	К2	0	0	К6	К8	0	К10	0	0	К14	0	**К1**	0
1	53	точка беспроводного доступа	0	К8	0	К14	0	**0**	**К1**	0	К6	К8	**0**	К2	0	0	К6	К8	0	0	0	0	К14	0	**0**	0
1	55	узлы хранилища больших данных	0	К8	К10	К14	0	**К1**	**К1**	0	К6	К8	**К1**	К2	0	0	К6	К8	0	К10	0	0	К14	0	**К1**	0
1	57	Файлы и каталоги	0	К8	К10	К14	0	**К1**	**К1**	0	К6	К8	**К1**	К2	0	0	К6	К8	0	К10	0	0	К14	0	**К1**	0
1	58	Хранилище больших данных	0	К8	К10	К14	0	**К1**	**К1**	0	К6	К8	**К1**	К2	0	0	К6	К8	0	К10	0	0	К14	0	**К1**	0
			0	22	17	19	0	19	18	0	14	22	19	22	0	0	14	22	0	17	0	0	19	0	19	0
		Количество комплексов разного типа, реализующих j-ю функцию i-й подсистемы по выбранным объектам защиты ------>						77		18		36												113		19
		Доля участия каждого комплекса одного типа к общему числу связей всех комплексов разного типа по j-й функции i-й подсистемы по выбранным объектам защиты (формула 3.1)--------->	0,00	0,29	0,22	0,25	0,00	0,25	1,00	0,00	0,39	0,61	0,17	0,19	0,00	0,00	0,12	0,19	0,00	0,15	0,00	0,00	0,17	0,00	1,00	0,00
		Общее количество задействованных всех связей по всем комплексам разного типа i-й подсистемы по выбранным объектам защиты ------>								131																132
		Доля общего числа связей всех комплексов разного типа j-ой функции i-ой подсистемы по выбранным объектам защиты к общему числу связей всех комплексов разного типа i-й подсистемы по выбранным объектам защиты (формула 3.2) ------>						0,588		0,137		0,275												0,856		0,144
		Доля общего числа связей всех её комплексов разного типа -ой подсистемы с выбранными объектами защиты к общему числу связей всех комплексов разного типа всех подсистем уровня ПТР по выбранным объектам защиты (формула 3.3) ------>								0,296																0,299

Рисунок 4.19 – Фрагмент формы заполнения массива «Объектам воздействия (защиты) в разрезе подсистем П1 – П2 ПТСЗИ» (начало формы)

		Наименование подсистем	Подсистема обеспечения целостности (П3)						Подсистема антивирусной защиты (П4)		Подсистема контроля использования информационных ресурсов			Подсистема централизованного управления СрЗИ (П6)		Подсистема анализа защищенности (П7)	
		Условное обозначение подсистем	П3						П4		П5			П6		П7	
	№ п.п.	Наименование j-ой функции подсистемы, условное обозначение	В1			В2			Г1	Г2	Д1		Д2	Е1	Е2	Ж1	Ж2
Для выбора ОЗ аудитором		Наименование j-ой функции подсистемы КСЗИ	- контроль целостности исполняемых и конфигурационных файлов СрЗИ, компонентов ОС и прикладного ПО			- контроль неизменности параметров встроенных СрЗИ и компонентов системного ПО			- защита файловой системы от вирусов и вредоносных программ	- потоковая защита межсетевого трафика от вирусов и вредоносных программ	- контроль каналов утечек защищаемой информации		- обнаружение несанкционированного хранения конфиденциальной информации	- обеспечение возможности оперативного получения информации о состоянии защищенности	- обеспечение автоматизации рутинных задач	- предоставление в виде отчетов информации об обнаруженных уязвимостях с рекомендациями по их устранению	- обеспечение инвентаризации и узлов, выявление и идентификация уязвимостей
		Наименование комплекса уровня ПТР КСЗИ, условное обозначение	К1	К12	К13	К12	К13	К1	К2	К8	К1	К15	К15	К11	К11	К12	К12
		Объекты защиты БДУ ФСТЭК															
1	1	база данных	К1	0	0	0	0	К1	К2	К8	К1	0	0	0	0	0	0
1	2	виртуальная машина	К1	0	0	0	0	К1	К2	К8	К1	0	0	0	0	0	0
1	6	гипервизор	К1	0	0	0	0	К1	К2	К8	К1	0	0	0	0	0	0
1	8	Данные об учетных записях	К1	0	0	0	0	К1	К2	К8	К1	0	0	0	0	0	0
1	10	Защищаемая информация	К1	0	0	0	0	К1	К2	К8	К1	0	0	0	0	0	0
1	12	информационная система	К1	0	0	0	0	К1	К2	К8	К1	0	0	0	0	0	0
1	15	Канал связи	0	0	0	0	0	0	К2	К8	0	0	0	0	0	0	0
1	17	ключевая система информационной инфраструктуры	К1	0	0	0	0	К1	К2	К8	К1	0	0	0	0	0	0
1	20	Машинный носитель информации	К1	0	0	0	0	К1	К2	К8	К1	0	0	0	0	0	0
1	21	метаданные	К1	0	0	0	0	К1	К2	К8	К1	0	0	0	0	0	0
1	35	программно-аппаратные средства со встроенными функциями защиты	К1	0	0	0	0	К1	К2	К8	К1	0	0	0	0	0	0
1	37	Программные средства	К1	0	0	0	0	К1	К2	К8	К1	0	0	0	0	0	0
1	43	сервер	К1	0	0	0	0	К1	К2	К8	К1	0	0	0	0	0	0
1	44	сетевой трафик	0	0	0	0	0	0	К2	К8	0	0	0	0	0	0	0
1	45	сетевой узел	К1	0	0	0	0	К1	К2	К8	К1	0	0	0	0	0	0
1	46	система разграничения доступа хранилища больших данных	К1	0	0	0	0	К1	К2	К8	К1	0	0	0	0	0	0
1	47	Система управления доступом встроенная в операционную систему компьютера	К1	0	0	0	0	К1	К2	К8	К1	0	0	0	0	0	0
1	49	Средство защиты информации	К1	0	0	0	0	К1	К2	К8	К1	0	0	0	0	0	0
1	53	точка беспроводного доступа	0	0	0	0	0	0	К2	К8	0	0	0	0	0	0	0
1	55	узлы хранилища больших данных	К1	0	0	0	0	К1	К2	К8	К1	0	0	0	0	0	0
1	57	Файлы и каталоги	К1	0	0	0	0	К1	К2	К8	К1	0	0	0	0	0	0
1	58	Хранилище больших данных	К1	0	0	0	0	К1	К2	К8	К1	0	0	0	0	0	0
			19	0	0	0	0	19	22	22	19	0	0	0	0	0	0
		Количество комплексов разного типа, реализующих j-ю функцию i-й подсистемы по выбранным объектам защиты ------>			19			19	22	22		19	0	0	0	0	0
		Доля участия каждого комплекса одного типа к общему числу связей всех комплексов разного типа по j-й функции i-й подсистемы по выбранным объектам защиты (формула 3.1)-------->	1,00	0,00	0,00	0,00	0,00	1,00	1,00	1,00	1,00	0,00	#ДЕЛ/0!	#ДЕЛ/0!	#ДЕЛ/0!	#ДЕЛ/0!	#ДЕЛ/0!
		Общее количество задействованных всех связей по всем комплексам разного типа i-й подсистемы по выбранным объектам защиты ------>						38		44			19		0		0
		Доля общего числа связей всех комплексов разного типа j-ой функции i-ой подсистемы по выбранным объектам защиты к общему числу связей всех комплексов разного типа i-й подсистемы по выбранным объектам защиты (формула 3.2) ------>			0,500			0,500	0,500	0,500		1,000	0,000	#ДЕЛ/0!	#ДЕЛ/0!	#ДЕЛ/0!	#ДЕЛ/0!
		Доля общего числа связей всех её комплексов разного типа -ой подсистемы с выбранными объектами защиты к общему числу связей всех комплексов разного типа всех подсистем уровня ПТР по выбранным объектам защиты (формула 3.3) ------>						0,086		0,100			0,043		0,000		0,000

Рисунок 4.20 – Фрагмент формы заполнения массива «Объектам воздействия (защиты) в разрезе подсистем П3 – П7 ПТСЗИ» (продолжение формы)

		Наименование подсистем	Подсистема обеспечения сетевой безопасности (П8)						Подсистема обеспечения непрерывности	
		Условное обозначение подсистем	П8						П9	
	№ п.п.	Наименование j-ой функции подсистемы, условное обозначение	З1	З2	З3				И	
Для выбора ОЗ аудитором		Наименование j-ой функции подсистемы КСЗИ	- межсетевое экранирование ЛВС	- обнаружение вторжений в ЛВС	- обеспечение безопасного функционирования сетевого оборудования				- резервное копирование конфигурационных файлов СрЗИ и восстановление данных из резервных копий в случаях сбоев	
		Наименование комплекса уровня ПТР КСЗИ, условное обозначение	К8	К9	К6	К7	К8	К9	К3	К7
		Объекты защиты БДУ ФСТЭК								
1	1	база данных	К8	0	К6	0	К8	0	К3	0
1	2	виртуальная машина	К8	0	0	0	К8	0	К3	0
1	6	гипервизор	К8	0	0	0	К8	0	К3	0
1	8	Данные об учетных записях	К8	0	К6	0	К8	0	К3	0
1	10	Защищаемая информация	К8	0	К6	0	К8	0	К3	0
1	12	информационная система	К8	0	0	0	К8	0	К3	0
1	15	Канал связи	К8	0	0	0	К8	0	0	0
1	17	ключевая система информационной инфраструктуры	К8	0	К6	0	К8	0	К3	0
1	20	Машинный носитель информации	К8	0	0	0	К8	0	К3	0
1	21	метаданные	К8	0	0	0	К8	0	К3	0
1	35	программно-аппаратные средства со встроенными функциями защиты	К8	0	К6	0	К8	0	К3	0
1	37	Программные средства	К8	0	К6	0	К8	0	К3	0
1	43	сервер	К8	0	0	0	К8	0	К3	0
1	44	сетевой трафик	К8	0	К6	0	К8	0	0	0
1	45	сетевой узел	К8	0	К6	0	К8	0	К3	0
1	46	система разграничения доступа хранилища больших данных	К8	0	К6	0	К8	0	К3	0
1	47	Система управления доступом встроенная в операционную систему компьютера	К8	0	0	0	К8	0	К3	0
1	49	Средство защиты информации	К8	0	К6	0	К8	0	К3	0
1	53	точка беспроводного доступа	К8	0	К6	0	К8	0	К3	0
1	55	узлы хранилища больших данных	К8	0	К6	0	К8	0	К3	0
1	57	Файлы и каталоги	К8	0	К6	0	К8	0	К3	0
1	58	Хранилище больших данных	К8	0	К6	0	К8	0	К3	0
			22	0	14	0	22	0	20	0
		Количество комплексов разного типа, реализующих j-ю функцию i-й подсистемы по выбранным объектам защиты ------>	22	0				36		20
		Доля участия каждого комплекса одного типа к общему числу связей всех комплексов разного типа по j-й функции i-й подсистемы по выбранным объектам защиты (формула 3.1)--------->	1,00	#ДЕЛ/0!	0,39	0,00	0,61	0,00	1,00	0,00
		Общее количество задействованных всех связей по всем комплексам разного типа i-й подсистемы по выбранным объектам защиты ------>						58		20
		Доля общего числа связей всех комплексов разного типа j-ой функции i-ой подсистемы по выбранным объектам защиты к общему числу связей всех комплексов разного типа i-й подсистемы по выбранным объектам защиты (формула 3.2) ------>	0,379	0,000				0,621		1,000
										442
		Доля общего числа связей всех её комплексов разного типа -ой подсистемы с выбранными объектами защиты к общему числу связей всех комплексов разного типа всех подсистем уровня ПТР по выбранным объектам защиты (формула 3.3) ------>						0,131		0,045

Рисунок 4.21 – Фрагмент формы заполнения массива «Объектам воздействия (защиты) в разрезе подсистем П8 – П9 ПТСЗИ» (конец формы)

4.2. Порядок работы пользователя с программой агрегированного оценивания функциональной эффективности ПТСЗИ

Взаимосвязь пользователей и основных компонентов программы «АОФЭ» представлена в соответствие с рисунком 4.22.

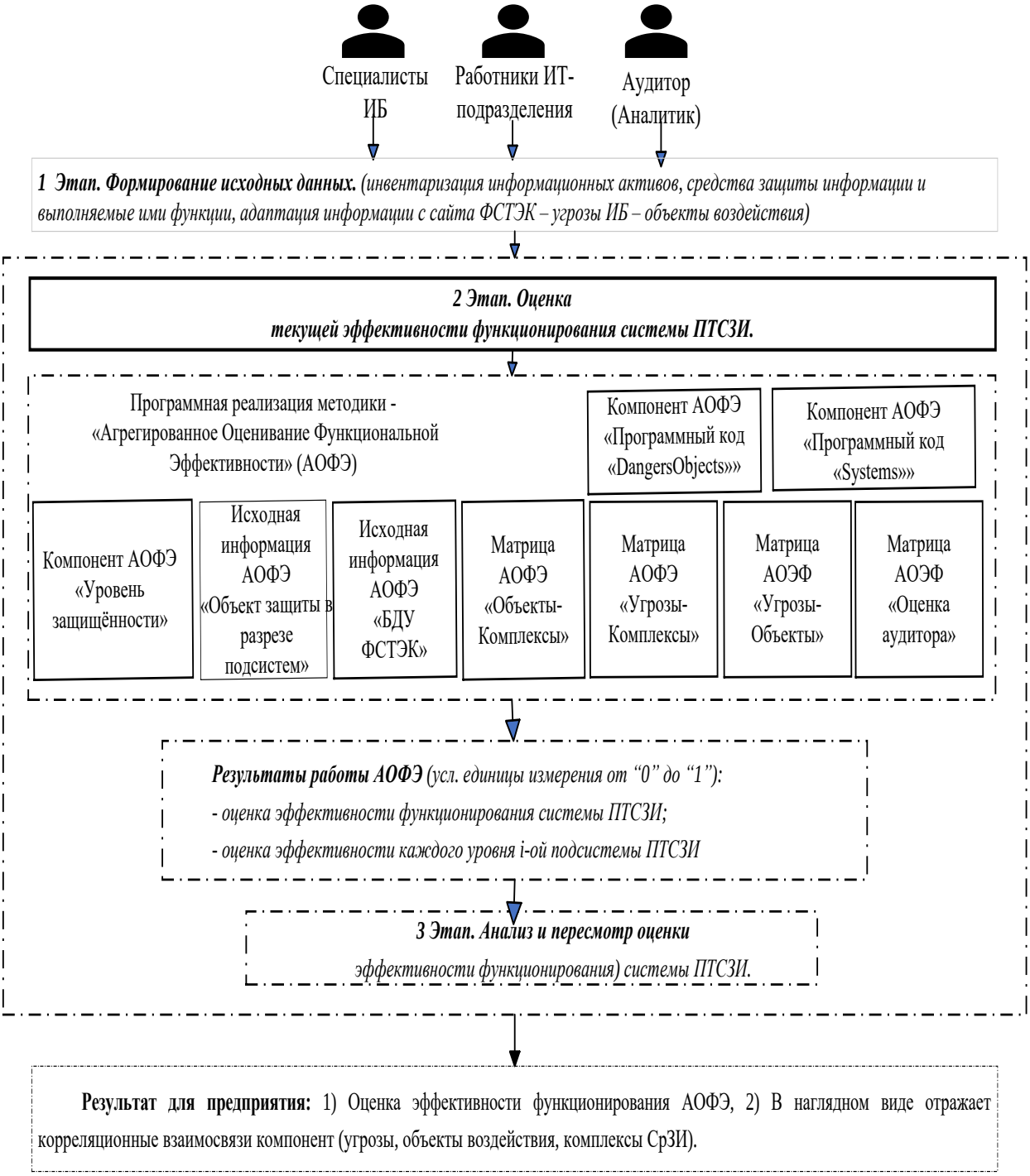


Рисунок 4.22 – Взаимосвязь пользователей и основных компонентов программы «АОФЭ»

Программа «АОФЭ» был разработан и протестирован с учётом следующих требований к программно-техническому обеспечению:

— 12th Gen Intel(R) Core(TM) i9-12900H 2.50 GHz;

— оперативная память – не менее 16 Гб;

— место на жёстком диске – не менее 29Гб для установки выполняемого кода и первичной настройки;

— ОС – Windows 10 Домашняя.

Для программной реализации методики оценки функциональной эффективности системы ПТСЗИ предприятия в рамках диссертационного исследования должны быть реализованы следующие этапы:

1 Этап. Формирование исходных данных. На данном этапе проводится инвентаризация информационных активов, включая средства защиты информации, а также проводится актуализация к использованию в «АОФЭ» иформации с сайта ФСТЭК (угрозы ИБ – объекты воздействия). На данном этапе происходит заполнение двумерных матриц: а) Эталонные значения «Объекты защиты в контексте подсистем»; б) «Угрозы» × «Комплексы средств защиты информации»; в) «Активы (Объекты воздействия)» × «Комплексы средств защиты информации»; д) Матрица «Оценка аудитора»; е) Матрица «Угрозы» × «Активы (Объекты воздействия)»; ж) актуализация информации с сайта «БДУ ФСТЭК».

– Лист «БДУ ФСТЭК» заполняется числовыми значениями из импортированной таблицы с сайта ФСТЭК России (https://bdu.fstec.ru/files/documents/thrlist.xlsx) [15]. Информация загружаемая с сайта ФСТЭК содержит взаимосвязи угроз ИБ по объектам воздействия (защиты) и свойствам информации. Экспертным путём, используя информацию с сайта ФСТЭК, формируется оптимальный список объектов воздействия (защиты). На данный момент таких объектов 58. Среди них базы данных, информационные системы, каналы связи, мобильные устройства и т.д. [102].

Заполнение матрицы исходных данных для программы «АОФЭ» по компонентам (комплексы, объекты защиты, подсистемы) происходит на листе

эталонные значения «Объекты защиты в контексте подсистем» таблицы MS Office Excel (Рисунок 4.19 и рисунок 4.20.

– Для заполнения матрицы «Угрозы» × «Активы (Объекты воздействия)» используется созданный средством VBA MS Office Excel программный код «DangersObjects» (рисунок 4.2). Порядок запуска программного кода «DangersObjects»: 1) перейти в меню программного обеспечения (ПО) MS Office Excel на вкладку «Вид»; 2) затем – «Макросы»; 3) активировать выполнение самого программного кода «DangersObjects» используя кнопку «Выполнить». Таким образом будет создана матрица «Угрозы-Объекты» размерностью 222 на 58 объектов защиты (Рисунок 4.18).

2 Этап. Оценка текущего уровня защищённости (эффективности функционирования) системы ПТСЗИ.

Далее, работниками ИТ-подразделения (администраторами серверов и/или сетей) самостоятельно или с привлечением внешних аудиторов по ИБ проводится качественная (отлично, хорошо, средне, удовлетворительно, плохо, не работает) и количественная оценка функционирования комплексов СрЗИ на соответствие предъявляемых требований к технической документации и нормативно-распорядительных документов в области ИБ предприятия. Данный этап предусматривает проведение опросов и интервьюирования лиц, сопровождающих информационную инфраструктуру предприятия, а также сбор необходимых статистических сведений по системе ПТСЗИ и их предварительный анализ.

– *Первичная настройка программы «АОФЭ» и текущая оценка эффективности функционирования ПТСЗИ.* На основе исходной информации, полученной по первому этапу, а также применяя разработанный программный код «Systems» (рисунок 4.3 и 4.2), происходит первичная инициализация (очищение значений ячеек в таблицах) и заполнение матриц защиты: а) «Угрозы» × «Комплексы средств защиты информации» (рисунок 4.11); б) «Активы (Объекты воздействия)» × «Комплексы средств защиты информации» (рисунок 4.13 по рисунок 4.17) ; в) Матрица «Оценка аудитора» (рисунок 4.11). Блок-

схема описания алгоритма работы программного кода «Systems» и результаты заполнения «матриц защиты» приведены в соответствие с рисунком 4.5. Для запуска программного кода «Systems» необходимо перейти в меню программного обеспечения (ПО) MS Office Excel на вкладку «Вид», а затем – «Макросы» и используя кнопку «Выполнить» активировать выполнение самого программного кода «Systems», либо активировать исполнение программного кода на листе «Уровень защищённости» путём нажатия кнопки «Обновить». В результате выполнения программного кода «Systems» будут заполнены «матрицы защиты». При помощи встроенных функций Excel переносятся числовые значения «матриц защиты» на лист «Уровень защищённости» (рисунок 4.6, рисунок 4.7, рисунок 4.8, рисунок 4.9, рисунок 4.10)., где будут отражаться

– доли угроз, нарушающих свойства информации (конфиденциальность, целостность, доступность);

– оценки аудитора, которые могут корректироваться в матрице «Оценка аудитора» в результате оценки комплексов и функций, выполняемых ими;

– оценки текущей эффективности функций системы ПТСЗИ по объектам защиты.

Пересмотр оценки данного этапа возможен в случаях проведения:

– модернизации системы ПТСЗИ (внедрения, вывода из промышленной эксплуатации средств защиты информации);

– инвентаризации объектов защиты системы ПТСЗИ;

– аудита системы ПТСЗИ на предмет уточнения объектов защиты, компонентов системы ПТСЗИ, соответствия выполняемых функций компонентов своему целевому назначению, работоспособности, требований регуляторов в области ИБ, требований нормативно-правовых и организационных мер.

В случае модернизации и инвентаризации порядок следования 1-го и 2-го этапов сохраняется, как было описано выше, и дальнейшее выполнение 3-го этапа требуется только в случае пересмотра аудиторской оценки и/или

оптимального распределения денежных средств.

В случае проведения аудита системы ПТСЗИ связанного с необходимостью пересмотра объектов защиты и компонент системы ПТСЗИ порядок следования 1-го и 2-го этапов сохраняется, как было описано выше. Далее, все остальные случаи проведения аудита (соответствия выполняемых функций компонентов своему целевому назначению, работоспособности, требований регуляторов в области ИБ, требований нормативно-правовых и организационных мер) затрагивают только выполнение этапа 2, а именно: внесения в лист «Оценка аудитора» значений оценки аудиторов по шкале от 0 до 1. Оценка «1» означает, что k – й комплекс полностью задействован в обеспечении j-ой функции i-й подсистемы, и удовлетворяет требованиям регуляторов по ИБ. Оценка «0» означает, что k – й комплекс совсем не задействован в обеспечении j-ой функции i-й подсистемы и не удовлетворяет требованиям регуляторов по ИБ. При этом отметим, что на оценку аудиторов могут влиять следующие факторы: уровень компетенции экспертов в области ИБ и результаты вычислений уязвимостей по интерактивному калькулятору, размещенному на сайте ФСТЭК (https://bdu.fstec.ru/calc31) [15].

Кроме того, к одной из сильных сторон программы можно отнести визуализацию задействованных в функционировании ПТСЗИ компонент с помощью 6 уровневой цветовой шкалы. Цветовая шкала позволяет наглядно в кратчайшее время определить «узкие места» в ПТСЗИ.

3 Этап. Анализ текущего уровня и пересмотр защищённости (эффективности функционирования) стемы ПТСЗИ.

Результаты данного этапа предполагает осуществить анализ текущего уровня защищённости (эффективности функционирования) системы ПТСЗИ с точки зрения проведения оптимального распределения денежных средств (ОРДС). С это целью была разработана программа «ОРДС». Программа «ОРДС» реализована при помощи Pascal (Delphi) с решателем: LPSolve IDE v5.5.2.12. Интерфейс программы «ОРДС» представлен на рисунке 4.23.

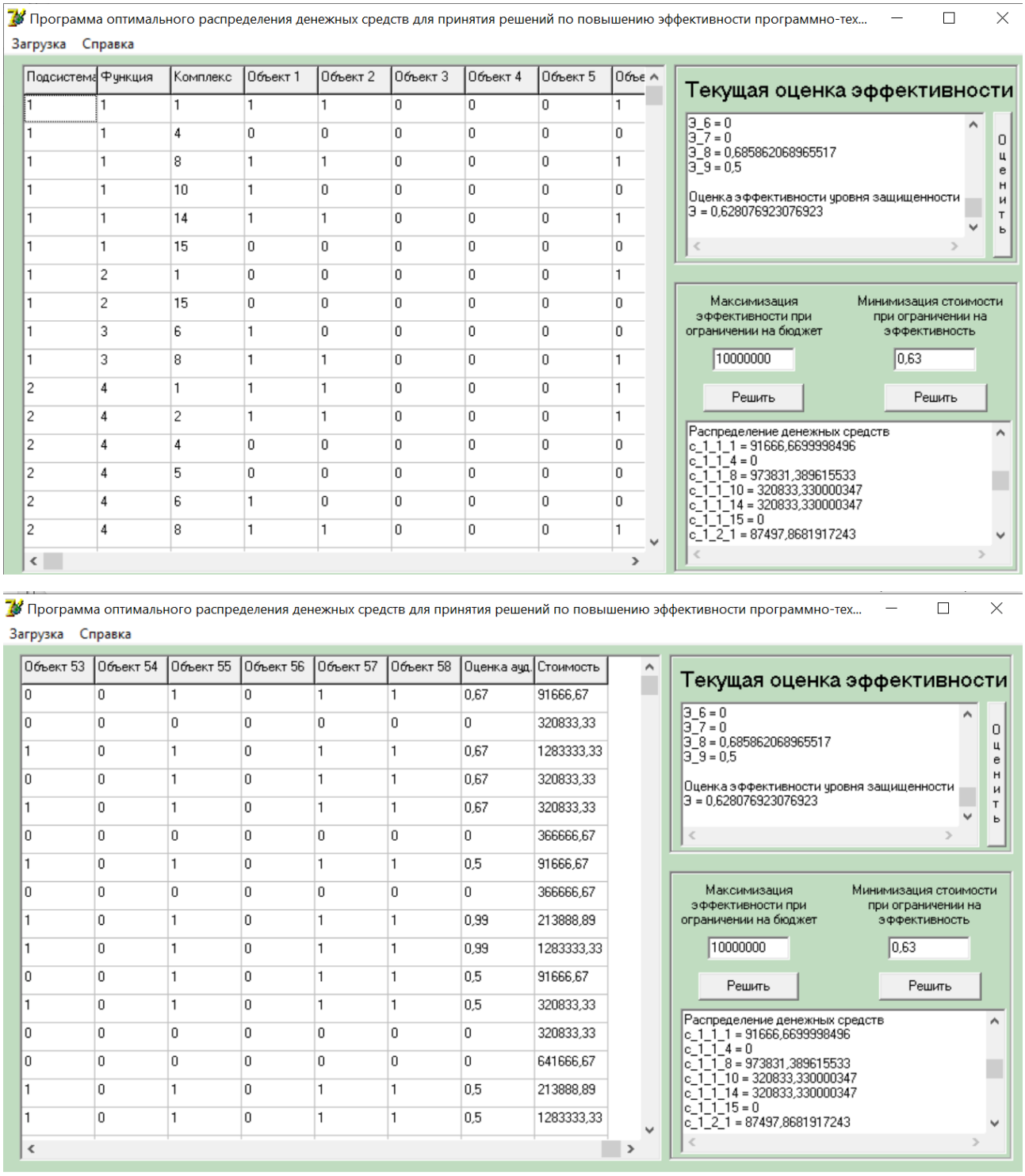


Рисунок 4.23 –Интерфейс программы «ОРДС»

Блок-схема алгоритма программы «ОРДС» представлена в соответствие с рисунком 4.24. Программа «ОРДС» реализована с использованием решателя LPSolve IDE v5.5.2.12 и ориентирована на рациональное распределение ресурсов для улучшения защитных мер.

Пользователями программы «АОФЭ» и «ОРДС» могут быть как специалисты в области анализа данных, так и исследователи, ориентированные на решение прикладных задач.

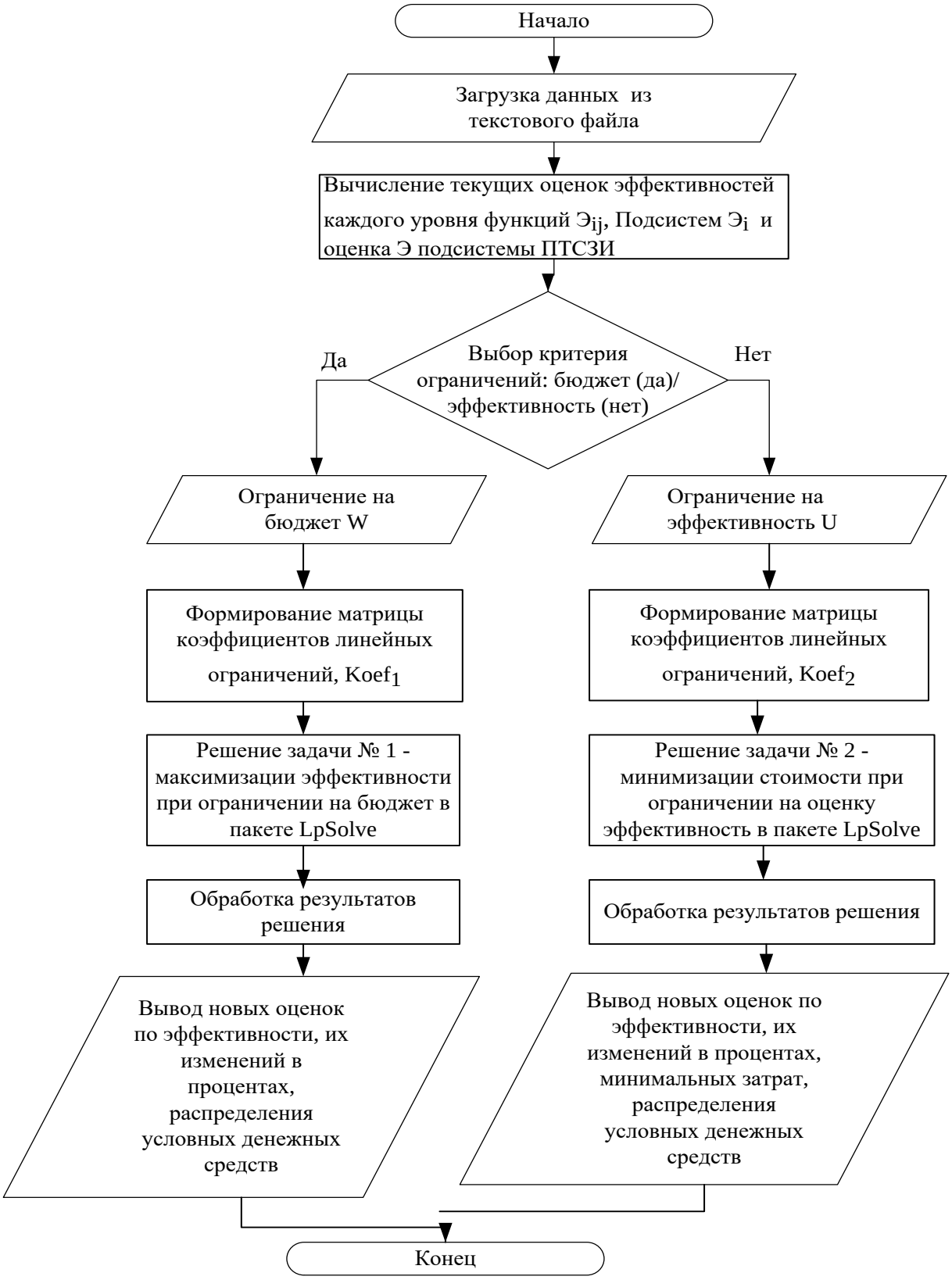


Рисунок 4.24 – Блок-схема алгоритма программы «ОРДС»

Программно-алгоритмическая реализация «АОФЭ» и «ОРДС» протестирована на исходных данных предприятия ООО «ЯНТА»

– *На первом этапе использования программы «ОРДС»*, в результате оценки эффективности функционирования предприятия ООО «ЯНТА» были определены: 1) 22 объекта воздействия в обеспечении защиты которых задействованы 7 подсистем (П1, П2, П3, П4, П5, П8, П9); 2) вектор $V=(3,2,2,2,1,0,0,3,1)$, состоящий из v_i элементов, каждый из которых показывает какое количество функций входит в i-ю подсистему; 3) множества M_i^j, содержащие номера комплексов, входящих в j-ю функцию i-й подсистемы и которые имеют вид $M_1^1=\{1,8,10,14\}$, $M_1^2=\{1\}$, $M_1^3=\{6,8\}$, $M_2^1=\{1,2,6,8,10,14\}$, $M_2^2=\{1\}$, $M_3^1=\{1\}$, $M_3^2=\{1\}$, $M_4^1=\{2\}$, $M_4^2=\{8\}$, $M_5^1=\{1\}$, $M_8^1=\{8\}$, $M_8^3=\{6,8\}$, $M_9^1=\{3\}$.

– *На втором этапе использования программы «ОРДС»*, используя результаты «АОФЭ» и сценарные условия текущих затрат на техническую поддержку и сопровождение СрЗИ 2018-2022гг., как исходные данные, с помощью «ОРДС» оценивается текущая оценка эффективности системы ПТСЗИ и её компонент.

– *На третьем этапе*, с помощью «ОРДС» решается задача ЛП с целевой функцией (3.16), линейными ограничениями (3.9)-(3.14), (3.17) и условиями неотрицательности переменных (3.15). Данная задача эквивалентна задаче (3.8), (3.9)-(3.15). Решение задачи (3.9) – (3.17) даёт ответ на вопрос, как распределить имеющуюся сумму W, чтобы максимизировать функциональную эффективность ПТСЗИ и всех её компонентов.

На данном этапе было установлено ограничение на затраты (бюджет) W =10 млн. руб. В результате решения задачи было получено следующее распределение установленной суммы затрат по комплексам СрЗИ задействованных для выполнения функций подсистем: $c_{1,1,1}$ =91666,67 руб., $c_{1,1,8}$ =973831,39 руб., $c_{1,1,10}$ = 320833,33 руб., $c_{1,1,14}$ = 320833,33 руб., $c_{1,2,1}$ = 87497,8

7 руб., $c_{2,4,1}$ = 91666,67 руб., $c_{2,4,2}$ = 320833,33 руб., $c_{2,4,6}$ =213888,89 руб., $c_{2,4,8}$ = 983558,59 руб., $c_{2,4,10}$ = 320833,33, руб., $c_{2,4,14}$ = 320833,33 руб., $c_{2,5,1}$ = 87 497,87 руб., $c_{3,6,1}$ =88555,62 руб., $c_{3,7,1}$ =88555,62 руб., $c_{5,10,1}$ =87497,87 руб., $c_{8,18,6}$ =213888,89 руб., $c_{8,18,8}$ =1187829,87 руб., $c_{9,19,3}$=4199897,52 руб. .

Результаты, приведенные в таблице 4.2, демонстрируют увеличение показателя функциональной эффективности ПТСЗИ на предприятии ООО «ЯНТА» с коэффициента 0,63 до 0,98, что стало возможным благодаря привлечению дополнительных финансовых инвестиций в размере 10 млн руб.

Таблица 4.2 – Результаты расчётов по программе «ОРДС»

Оценка функциональной эффективности ПТСЗИ			Оценка функциональной эффективности подсистем ПТСЗИ		Распределение финансовых средств для повышения эффективности функционирования подсистем ПТСЗИ	
Символ	При текущих затратах в 22 млн. руб.	При W=10 млн. руб. (привлечение финансовых инвестиций)	Эффективность	При текущих затратах в 22 млн. руб.	При W=10 млн. руб. (привлечение финансовых инвестиций)	
Э	0,63	**0,98**	$Э_1$	0,73	**0,98**	**1 794 662,59**
			$Э_2$	0,5	**0,98**	**2 339 112,01**
			$Э_3$	0,33	**0,98**	**177 111,25**
			$Э_4$	0,99	**0,99**	**0**
			$Э_5$	0,5	**0,98**	**87 497,87**
			$Э_8$	0,69	**0,98**	**1 401 718,76**
			$Э_9$	0,5	**0,98**	**4 199 897,52**

Как следует из таблицы 4.2, общая эффективность (Э) ПТСЗИ до оптимизации составляла 0,63, что отражет недостаточную сбалансированность и результативность применения отдельных подсистем ПТСЗИ. Кроме того,

таблица содержит оценку функциональной эффективности отдельных подсистем ПТСЗИ «до» (текущая эффек-тивность) и «после» оптимизации.

Для большинства подсистем (например, $Э_1$, $Э_2$, $Э_3$, $Э_5$, $Э_8$, $Э_9$) текущая эффективность составляла от 0,33 до 0,73, указывая на наличие "узких мест" в защите информации. Для выполнения мероприятий по повышению функциональной эффективности ПТСЗИ и её компонентов было установлено ограничение на привлечение дополнительных финансовых инвестиций в размере 10 млн рублей с целью решить задачу по перераспределению финансовых ресурсов так, чтобы устранить неэффективные элементы, максимизировав при этом общую эффективность ПТСЗИ. В результате, после перераспределения средств: 1) эффективность каждой подсистемы была доведена до значений 0,98, за исключением подсистемы $Э_4$, чья эффективность и «до» оптимизации была на высоком уровне 0,99; 2) эффективность (Э) ПТСЗИ возросла до 0,98, что близко к максимально возможному значению.

Таким образом, следуя разработанному плану финансовых вложений при ограничении на затраты, эффективность предприяти действительно может быть повышена.

Решение второй задачи ЛП (3.9) – (3.13), (3.15), (3.18), (3.19) даёт ответ на вопрос, какие минимальные затраты необходимы и как их распределить, чтобы обеспечить заданный уровень функциональной эффективности $U=0,63$ для ПТСЗИ и всех её компонентов. В результате решения установлено, что минимальные затраты на обеспечение указанного уровня эффективности защиты информации составят 1,68 млн. руб.

В заключении данного раздела необходимо отметить, что конкретные детали программной реализации зависят от структуры и требований нормативно распорядительных актов в области ИБ предприятия и системы ПТСЗИ, что возможно в каждом конкретном случае (например – подключение дополнительных сегментов АСУТП) может потребовать частичной адаптации разработанной методики и описанных выше шагов в соответствии с конкретным контекстом и целями предприятия.

4.3. Выводы по главе

В четвёртой главе описаны и апробированы созданные две программы: программа «Агрегированное оценивание функциональной эффективности» (АОФЭ) для реализации методики агрегированного оценивания и визуализации компонент системы ПТСЗИ, а также программа «Оптимальное распределение денежных средств» для принятия решений по повышению эффективности ПТСЗИ предприятия – «ОРДС». В главе представлены блок-схемы алгоритмов программ: «АОФЭ» и «ОРДС». Программа «ОРДС» реализована с использованием решателя LPSolve IDE v5.5.2.12 и ориентирована на рациональное распределение ресурсов для улучшения защитных мер. Пользователями программы «АОФЭ» и «ОРДС» могут быть как специалисты в области анализа данных, так и исследователи, ориентированные на решение прикладных задач.

Формирование матриц, используемых в программе «АОФЭ», основано на концептах и взаимосвязях, определённых в онтологической модели системы ПТСЗИ (глава 2). Это позволило в рамках рассматриваемой главы автоматизировать создание двумерных матриц с помощью макросов «DangersObjects» и «Systems», обеспечив согласованность данных и корректность расчётов. Также эта программа обеспечивает визуализацию всех задействованных компонентов в матричной форме, используя 6 уровневую цветовую шкалу. Это упрощает анализ и интерпретацию данных.

На предприятии ООО «ЯНТА», используя программы «АОФЭ» и «ОРДС», проведена оценка эффективности функционирования системы ПТСЗИ и решены две задачи линейного программирования (ЛП) об оптимальном распределении денежных средств на совершенствование ПТСЗИ, в первой из которых для заданного бюджетного ограничения максимизируется нижняя граница функциональной эффективности ПТСЗИ и всех её компонентов, а во второй минимизируются суммарные затраты для обеспечения заданного уровня функциональной эффективности ПТСЗИ и всех её компонентов. Получен акт внедрения.

Заключение

В диссертационной работе получены следующие результаты.

1. Выявлены недостатки существующих методов и показателей ИБ. Особое внимание уделено проблеме получения достоверных исходных данных при экспертном оценивании, учитывая разные типы организаций. Проведён анализ современных подходов к онтологическому моделированию СЗИ. Показана значимость онтологий как инструмента унификации терминологии, структурирования данных, повышения качества анализа с точки зрения выбора наилучших решений в области затрат на ИБ и снижения влияния субъективных факторов.

2. На основе результатов системного анализа, разработана подробная онтологическая модель ПТСЗИ и её составляющих компонентов. Эта модель не только формализует знания о компонентах системы, но и служит методологической основой для разработки алгоритмического обеспечения и методики агрегированного оценивания эффективности её функционирования. Созданные модели определения исходных данных позволили выделить ключевые показатели функциональной эффективности, структурировать их по уровням и обеспечить логическую взаимосвязь между компонентами системы.

3. Разработано алгоритмическое обеспечение агрегированного оценивания эффективности функционирования ПТСЗИ предприятия через систематизацию её компонентов (объектов защиты, угроз, комплексов средств защиты, подсистем и функций подсистем), что позволило построить: кубическую матрицу «Угрозы – Активы – Комплексы средств защиты информации»; связанные двумерные матрицы и модели эффективности, включая визуализацию результатов оценивания.

4. Сформулированы две задачи ЛП: а) задача максимизации нижней границы функциональной эффективности ПТСЗИ и всех её компонентов при заданном ограничении на бюджет; б) задача минимизации бюджетных затрат для обеспечения заданного уровня функциональной эффективности ПТСЗИ. Это позволяет повысить эффективность соответствующих управленческих решений.

5. Созданы две программы: программа «АОФЭ» для реализации методики

агрегированного оценивания и визуализации компонентов ПТСЗИ, а также программа «ОРДС» для принятия решений по повышению функциональной эффективности ПТСЗИ предприятия.

6. Используя программы «АОФЭ» и «ОРДС» на предприятии ООО «ЯНТА» проведена оценка состояния ПТСЗИ и выработаны рекомендации по повышению её функциональной эффективности с учётом бюджета. Получен акт внедрения.

Список сокращений

АРМ	-	автоматизированное рабочее место
АРМ АС	-	автоматизированное рабочее место, обрабатывающих конфиденциальную информацию
АРМ ПТБ	-	автоматизированное рабочее место, обрабатывающих конфиденциальную информацию с повышенными требованиями к безопасности
АСО	-	активное сетевое оборудование
АСУ ТП	-	автоматизированная система управления технологическим процесом.
БЗ	-	база знаний
ИА	-	информационный актив.
ИБ	-	информационная безопасность.
ИС	-	информационная система.
ИТ	-	информационные технологии
КПЦ	-	ключевой показатель цели
КПЭ	-	ключевой показатель эффективности
КСЗИ	-	комплексная система защиты информации
ЛВС	-	локальная вычислительная сеть.
МСБ	-	малый средний бизнес
МЭ	-	межсетевой экран.
НКК	-	нечеткие когнитивные карты
НСД	-	несанкционированный доступ.
ОС	-	операционная система.
ПО	-	программное обеспечение.
ПТСЗИ	-	программно-техническая система защиты информации.
СЗИ	-	система защиты информации
СХД	-	система хранения данных
СМИБ	-	система менеджмента информационной безопасности
СрЗИ	-	средство защиты информации.
ФХД	-	финансово-хозяйственная деятельность

Список использованных источников

1 Авдуевский В. С. [и др.] Надежность и эффективность в технике: – Т. 1 Методология. Организация. Терминология / под ред. А. И. Рембезы. М: Машиностроение, 1986. – 224 с.

2 Азгальдов Г.Г. Теория и практика оценки качества товаров (основы квалиметрии) / Г.Г. Азгальдов. – М.: Экономика, 1982. – 256 с.

3 Акофф Расселл Л. Менеджмент в XXI веке (Преобразование корпорации) / Пер. с англ. Ф. П. Тарасенко. – Томск: Изд-во Том. ун-та, 2006. – 418 с.

4 Акофф, Рассел Линкольн. Основы исследования операций / Р. Л. Акофф, М. В. Сасиени ; пер. с англ. и предисл. В. Я. Алтаева ; под ред. И. А. Ушакова. – Москва : Мир, 1971. – 534 с.

5 Артюхин Г.А. Теория систем и системный анализ. Практикум принятия решений / Г.А. Артюхин. – Казань: КГАСУ, 2016. – С. 165.

6 Аршинский В.Л., Аршинский Л.В., Доржсурэн Х. Оценка качества функционирования станции Улан-Баторской железной дороги на основе онтологического и продукционного моделирования // Современные наукоемкие технологии, 2018, – № 5. – С. 16-20.

7 Аршинский Л.В. Логико-аксиологический подход к оценке состояния систем // Современные технологии. Системный анализ. Моделирование. Иркутск: ИрГУПС. 2013. – №3(39). – С. 140-146.

8 Аршинский Л.В. Методика агрегированного оценивания систем с поддержкой ключевых компонентов // Онтология проектирования, 2015.– Т. 5. № 2 (16). – С. 223-232.

9 Аршинский Л.В. Необходимость и достаточность при агрегировании на основе неубывающих функций / Л.В. Аршинский, В.Л. Аршинский // Онтология проектирования, 2022. – Т. 12. – №1. – С.93-105. DOI: 10.18287/2223-9537-2022-12-1-93-105.

10 Бабенко Л.К. Защита данных геоинформационных систем [Текст] / Л.К. Бабенко, А.С. Басан, И.Г. Журкин, О.Б. Макаревич. – М.: Гелиос АРВ, 2010. – 336 с.

11 Бабенко Л.К. Алгоритмы «распределенных согласований» для оценки вычислительной стойкости криптоалгоритмов [Текст] / Л.К. Бабенко. – М.: Издательство ЛКИ, 2008. – 112 с.

12 Бабенко Л.К. Защита данных геоинформационных систем [Текст] / Л.К. Бабенко, А.С. Басан, И.Г. Журкин, О.Б. Макаревич. – М.: Гелиос АРВ, 2010. – 336 с.

13 Бабенко Л.К. Новые технологии электронного бизнеса и безопасности [Текст] / Л.К. Бабенко, В.А. Быков, О.Б. Макаревич, О.Б. Спиридонов. – М.: Радио и связь, 2002. – 512 с.

14 Бабенко Л.К. Современные алгоритмы блочного шифрования и методы их анализа [Текст] / Л.К. Бабенко, Е.А. Ищукова. – М.: Гелиос АРВ, 2006. – 376 с.

15 Банк данных угроз безопасности информации. [Электронный ресурс]. URL: https://bdu.fstec.ru/vul, свободный (дата обращения: 18.05.2024).

16 Баранова Е.К. Анализ и управление рисками в сфере информационной безопасности // Безопасность информационных технологий. – 2009. –Т. 16, №1. – С.98.

17 Баранова Е.К. Методики анализа и оценки рисков информационной безопасности//Вестник Московского университета им. С.Ю. Витте. Сер. 3: Образовательные ресурсы и технологии. 2015. № 1(9). С. 73-79.

18 Баранова Е. К., Забродоцкий А. С. Процедура применения методологии анализа рисков OCTAVE в соответствии со стандартами серии ИСО/МЭК 27000- 27005 // Образовательные ресурсы и технологии. 2015. No 2. С. 73-80.

19 Безсонов Н.В. Методическое пособие для расчета экономического эффекта от использования изобретений и рационализаторских предложений (инструктивно-методические). – М.: ВНИИПИ, 1985. – 104 с.

20 Беллман, Ричард. Динамическое программирование и современная теория управления [Текст] / Р. Беллман, Р. Калаба ; Пер. с англ. Е. Я. Ройтенберга ; Под ред. Б. С. Разумихина. – Москва : Наука, 1969. – 118 с. : черт.; 20 см.

21 Борщёв А. Практическое агентное моделирование и его место в арсенале аналитика / А. Борщёв // Exponenta PRO, 2004. #3-4(7-8). – С. 38-47.

22 Боярский К.К. Концептуальные модели в базах знаний // К.К. Боярский, Е.А. Каневский, Г.В. Лезин. -URL: https://cyberleninka.ru/article/n/kontseptualnye-modeli-v-bazah-znaniy/viewer. (дата обращения: 15.05.2024).

23 Бубакар И., Будько М.Б., Будько М.Ю., Гирик А.В. Онтологическое обеспечение управления рисками информационной безопасности. Труды Института системного программирования РАН. 2021;33(5):41-64. Режим доступа URL: https://doi.org/10.15514/ISPRAS-2021-33(5)-3, свободный (дата обращения: 03.11.2024).

24 Васильев, В. И. Построение нечетких когнитивных карт для анализа и управления информационными рисками вуза / В. И. Васильев, И. А. Савина, И. И. Шарипова // Вестник Уфимского государственного авиационного технического университета. – 2008. – Т. 10, № 2. – С. 199-209.

25 Винер Н. Кибернетика, или Управление и связь в животном и машине. / Пер. с англ. И.В. Соловьева и Г.Н. Поварова; Под ред. Г.Н. Поварова. – 2-е издание. – М.: Наука; Главная редакция изданий для зарубежных стран, 1983. – 344 с

26 Волкова В.Н. Системный анализ информационных комплексов / В.Н. Волкова. – СПб.: Лань, 2016. – С. 336.

27 Воронов М.В. Введение с системный анализ / М.В. Воронов. – Тирасполь: Полиграфист, 2011. – С. 224.

28 Выборнова О.Н. Управление рисками обработки информации на основе экспертных оценок: дис. ... канд. техн. наук: 05.13.01, 05.13.19. – Кубан. гос. технол. ун-т, Астрахань, 2017 – 174 с.

29 Гаврилова, Т. А. Базы знаний интеллектуальных систем / Т. А. Гаврилова, В. Ф. Хорошевский. – Санкт-Петербург : Питер, 2000. – 384 с. – (Учебник). – ISBN 5-272-00071-4.

30 Гаврилова, Т. А. Инженерия знаний. Модели и методы : учебник / Т. А. Гаврилова, Д. В. Кудрявцев, Д. И. Муромцев. – Санкт-Петербург : Издательство «Лань», 2016. – 324 с. – (Учебники для вузов. Специальная литература). – ISBN 978-5-8114-2128-2.

31 Глухов Н. И., Наседкин П. Н., Милько Д. С. Онтологическая модель управления информационными потоками на предприятии с учетом уровней конфиденциальности // Информационные технологии и математическое моделирование в управлении сложными системами. 2021. № 3 (11). С. 59-66.

32 Глухов Н.И. Оценка информационных рисков предприятия: учебное пособие. – Иркутск: ИрГУПС, 2013. – 148 с.

33 Глухов Н.И. Разработка элементов комплексной системы защиты информации предприятия / Н.И. Глухов, П.Н. Наседкин // Информационные технологии и математическое моделирование в управлении сложными системами, 2021. – № 1 (9). – С. 35-42.

34 ГОСТ 25010–2015 Требования и оценка качества систем и программного обеспечения (SQuaRE). Модели качества систем и программных продуктов URL: http://ingraf.su/wp-content/uploads/GOST-R-ISO-MEK-25010-2015.pdf (дата обращения: 26.05.2024).

35 ГОСТ 28806-90 Качество программных средств. Термины и определения. URL: https://pdf.standartgost.ru/catalog/Data2/1/4294825/4294825913.pdf (дата обращения: 26.05.2024).

36 ГОСТ Р 50922–2006 Защита информации. Основные термины и определения. – М.: Стандартинформ, 2006. – 12 с.

37 ГОСТ Р ИСО 31010–2011. Менеджмент риска. Методы оценки риска. – М.: Стандартинформ, 2012. – 74 с.

38 ГОСТ Р ИСО/МЭК 15408-1–2012. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. – Ч. 1. Введение и общая модель / Утв. и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 15 ноября 2012 г. № 814-ст. [Электронный ресурс]. – Режим доступа: http://docs.cntd.ru/document/ 1200101777, свободный (дата обращения: 18.05.2024).

39 ГОСТ Р ИСО/МЭК 27001–2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. – М.: Стандартинформ, 2008. – 26 с.

40 Грибова, В. В. Онтология диагностики процессов / В. В. Грибова, Е. А. Шалфеева // Онтология проектирования. – 2019. – Т. 9, № 4(34). – С. 449-461. – DOI 10.18287/2223-9537-2019-9-4-449-461.

41 Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками [Текст] / П.Н. Девянин. – М.: ГЛТ,2013. – 338 с.

42 Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками [Текст] / П.Н. Девянин. – М.: ГЛТ, 2013. – 338 с.

43 Дорофеев Р.С. Совместное использование методологий квалиметрической экспертизы и онтологии для оценки качества технологий изготовления изделий / Р.С. Дорофеев, С.С. Сосинская // Информационные и математические технологии в науке и управлении: Сб. трудов XVI Байкальской всерос. конференции. Ч. 2. – Иркутск: ИСЭМ СО РАН, 2010. – С. 138-145.

44 Дорофеев Р.С. Методология и программная реализация совместного использования онтологии и квалиметрической экспертизы при оценке качества станков / Р.С. Дорофеев // Вестник ИрГТУ, 2013. – №3. – С. 16-23.

45 Дробин В. У. [и др.] Надежность и эффективность в технике: Т. 3 Эффективность технических систем / под общ.ред. В. Ф. Уткина, Ю. В. Крючкова. М: Машиностроение, 1988. 328 с.

46 Евстафьев, Г.А. Нечеткие когнитивные карты применительно к управлению рисками информационной безопасности [Текст] / Г.А. Евстафьев // Известия Южного федерального университета. Технические науки. – 2009. – Т. 100. – №11. – С. 45-52.

47 Емалетдинов, Л. Ю. Анализ подходов к оценке рисков информационной безопасности в корпоративных информационных сетях / Л. Ю. Емалетдинова, И. В. Аникин // Вестник Казанского государственного энергетического университета. – 2015. – № 1(25). – С. 55-67.

48 Еременко, Е.А. Анализ рисков информационной безопасности на основе стандарта ISO/IEC 31010 / Еременко Е.А., Сафронова А.С. // Современные информационные и электронные технологии: науч. журн. – Украина, г. Одесса. – 2014. –Т. 1. № 15– С. 135–136.

49 Ермак, В.Д. Системы. Системные принципы. Системный подход / В.Д. Ермак // Соционика, 1997. – № 2. – URL: http://socionicasys.org/biblioteka/statji/sistemnij-podhod. (дата обращения: 20.02.2024).

50 Жук, А. П. Оценка финансовых затрат на построение средств защиты информации с помощью системы поддержки принятия решений / А. П. Жук, Д. Л. Осипов, А. А. Гавришев // Инфокоммуникационные технологии. – 2015. – Т. 13, № 4. – С. 451-457. – DOI 10.18469/ikt.2015.13.4.15.

51 Загорулько, Ю. А. Система автоматизированного построения онтологий научных предметных областей на основе паттернов онтологического проектирования / Ю. А. Загорулько, Г. Б. Загорулько, В. К. Шестаков // Распределенные информационно-вычислительные ресурсы (DICR-2022) : Сборник трудов XVIII Российской конференции с международным участием, Новосибирск, 05–08 декабря 2022 года / Под редакцией С.А. Рылова, Ю.И. Молородова, А.А. Жирнова, Ю.Н. Синявского. – Новосибирск: Федеральное государственное бюджетное научное учреждение

«Федеральный исследовательский центр информационных и вычислительных технологий», 2022. – С. 77-82. – DOI 10.25743/DIR.2022.41.72.013.

52 Зегжда Д.П. Основы безопасности информационных систем [Текст] / Д.П. Зегжда. – М.: Горячая линия – Телеком, 2000. – 452 с.

53 Зегжда Д.П. Обеспечение киберустойчивости программно-конфигурируемых сетей на основе ситуационного управления / Д.П. Зегжда, Е.Ю. Павленко // Проблемы информационной безопасности. Компьютерные системы, 2018. – № 1. – С. 160-168.

54 Зегжда П.Д. Применение рядов смежности для распознавания предфрактальных графов при оценке кибербезопасности VANET-сетей / П.Д. Зегжда, Д.В. Иванов, Д.А. Москвин, А.А. Иванов // Проблемы информационной безопасности. Компьютерные системы, 2018. – № 1. – С. 10-26.

55 Зегжда, П.Д. Системологический подход в информационных технологиях на примере проектирования средств получения и средств защиты информации: дис. … д-ра техн. наук: 05.13.19 / Зегжда Петр Дмитриевич. – СПб, 1996. – 304 с.

56 Зегжда, П.Д. Методология динамической защиты / П.Д. Зегжда, Д.П. Зегжда // Материалы международной научной конференции по проблемам безопасности и противодействия терроризму. Интеллектуальный центр МГУ. 2-3 ноября 2005 г. – М.: МЦНМО. – 2006. – 480 с., стр. 216–230.

57 Исследование уровня информационной безопасности в компаниях России и СНГ за 2019 год [Электронный ресурс]. – Режим доступа: https://searchinform.ru/ research-2019, свободный (дата обращения: 17.04.2024).

58 Иванченко П.Ю., Кацуро Д.А., Медведев А.В., Трусов А.Н. Математическое моделирование информационной и экономической безопасности на

предприятиях малого и среднего бизнеса // Фундаментальные исследования. – 2013. – № 10-13. – С. 2860-2863; URL: https://fundamental-research.ru/ru/article/view?id=32923 (дата обращения: 22.09.2024).

59 Каталевский Д.Ю. Системная динамика и агентное моделирование: необходимость комбинированного подхода. – URL: https://www.anylogic.ru/upload/iblock/740/7408de9e68d2dd7a8f40eac1899f9cf4.pdf. (дата обращения: 15.05.2024).

60 Клименко, И.С. Информационная безопасность и защита информации: модели и методы управления [Текст] / И.С. Клименко. – Москва: НИЦ ИНФРА-М, 2022–180 с.

61 Клименко И.С. Алгоритм сетевого планирования и управления на базе инновационных технологий [Текст] / И.С. Клименко // Математические методы и модели в исследовании актуальных проблем экономики России. – Уфа: Аэтерна, 2016. – С. 289–294.

62 Клименко И.С. Инновационные технологии в образовании, науке, управлении. Практикум для разработчика деловых игр [Текст]: учебное пособие / И.С. Клименко. – Алматы: Отан, 2015. – 143 с.

63 Клименко И.С. Интеграция методов формального и неформального моделирования в процедуре обоснования принимаемых решений [Текст] / И.С. Клименко // Методологические проблемы моделирования социально-экономических процессов. – Уфа: Аэтерна, 2014. – С. 158–160.

64 Клименко И.С. ИТ моделирования процесса управления сложными социально-экономическими системами [Текст] / И.С. Клименко, П.Ф. Клименко // Материалы Межд. научно-практ. конф. – Екатеринбург: УПИ, 2011. – С. 553–559.

65 Клименко И.С. Методология и технология компьютерной поддержки принятия решений в условиях неопределенности [Текст] / И.С. Клименко // Вестник науки КСТУ. – 2008. – № 2. – С. 99–105.

66 Клименко И.С. Методология и технология моделирования [Текст]: сб. науч. тр. / И.С. Клименко. – СПб., 2006. – С. 61–66.

67 Клименко И.С. Модели и методы управления [Текст]: учебное пособие/ И.С. Клименко. – Алматы: ОТАН, 2015. – 187 с.

68 Клименко И.С. Некоторые аспекты компьютерной системы поддержки принятия решений [Текст] / И.С. Клименко, П.Ф. Клименко [Текст] / Материалы межд. науч.-методол. конф. Актуальные проблемы развития ВШ. – СПб., 2006. – С. 146–154.

69 Клименко И.С. О некоторых инструментальных средствах управления сложными социально-экономическими системами [Текст] / И.С. Клименко, П.Ф. Клименко // Наука. – 2012. – № 3. – С. 63–69.

70 Клименко И.С. Особенности применения многокритериальных задач в оперативном управлении [Текст] / И.С. Клименко, П.Ф. Клименко // Studii economici: Revista stiintifi ca. – ULIM, Chisinau, 2014. – № 3–4. – С. 82–87.

71 Клименко И.С. Применение компьютерной технологии для экономической интерпретации результатов решения оптимизационной задачи [Текст] / И.С. Клименко // Материалы межд. науч.-практ. конф. – Рудный, 2009. – С. 419–424.

72 Клименко И.С. Проблемно-ориентированная система управления качеством подготовки специалистов на базе информационных технологий [Текст]: автореф. ... д-ра техн. наук: 05.13.01 / И.С. Клименко. – Алматы, 2010. – 48 с.

73 Клименко И.С. Решение задачи управления информационной безопасностью методом динамического программирования [Текст] / И.С. Клименко, Т.В. Кухарова // XVI Международная научная конференция «Технопрогресс»: сборник научных трудов. – Кемерово, Технопрогресс. – 2017. – С. 37–43.

74 Клименко И.С. Теория игр в системе поддержки принятия экономических решений [Текст] / И.С. Клименко // Междисциплинарный подход к исследованию экономики: сборник материалов III Международной научно-практической конференции. – Уфа: РИЦ БашГУ, 2017. – С. 192–197.

75 Клименко И.С. Управление качеством подготовки специалистов: теория и практика [Текст]: монография/ И.С. Клименко. – Костанай: Костанай-полиграфия, 2010. – 252 с.

76 Клименко И.С. Философия, методология и технология моделирования [Текст] / И.С. Клименко // Материалы межд. науч.-методол. конф. Актуальные проблемы развития высшей школы. – СПб., 2006. – С. 200–206.

77 Клименко И.С. Экономическая кибернетика: экономико-математическое моделирование [Текст] / И.С. Клименко. – Рудный: РИИ, 2002. – 187 с.

78 Клименко, И. С. От технологии 2С к технологии 2Д : Настольная книга разработчика деловых игр / И. С. Клименко. – Saarbruken : Palmarium Academic Publishing, 2014. – 285 с. – ISBN 978-3-8473-9892-9.

79 Клименко, И. С. Теория систем и системный анализ : Учебное пособие / И. С. Клименко. – Москва : Российский новый университет, 2014. – 264 с.

80 Климов С.М. Методика оценки возможного ущерба от нарушения безопасности информации автоматизированной системы // Изв. ТРТУ. – 2003. – № 4 (33). – С. 27–31.

81 Конев А. А. Подход к описанию структуры системы защиты информации / А. А.Конев, Е. М. Давыдова // Доклады ТУСУР. – 2013. – № 2(28). – С. 107–111.

82 Корниенко А.А. – М.: ФГБОУ «Учебно-методический центр по образованию на железнодорожном транспорте», 2014. – ч. 1. Методология и система обеспечения информационной безопасности на железнодорожном транспорте. – 440 с.

83 Кулик С.Д. Специальные средства для обеспечения информационной безопасности / С.Д. Кулик // Безопасность информационных технологий,

2015. – [S.l]. – Т. 22. – №. 2. – ISSN 2074-7136. – URL: https://bit.mephi.ru/ index.php /bit/article/view/114 (дата обращения: 20.02.2024).

84 Кулик С.Д. Исследование эффективности фактографического поиска в информационных системах / С.Д. Кулик. – Изд. Радиотехника, 2004. – №1326-В2004. – Библ. Указат. №9(391). – 251 с.

85 Кулик С.Д. Нейросетевые алгоритмы и автоматизированные фактографические информационные системы / С.Д. Кулик //Нейрокомпьютеры: разработка, применение, 2015. – № 12. – С. 58-65.

86 Кулик С.Д. Обеспечение информационной безопасности и фактографические системы / С.Д. Кулик// Безопасность информационных технологий, 2015. – [S.l.]. – Т. 22. – №. 1. – ISSN 2074-7136. – URL: https://bit.mephi.ru/ index.php/bit/article/view/199 (дата обращения: 20.02.2024).

87 Кулик С.Д. Последовательный анализ и нейронные сети в фактографических информационных системах/ С.Д. Кулик //Нейрокомпьютеры: разработка, применение, 2018. – № 9. – С. 53-60.

88 Легчекова Е.В. Метод расчета риска информационной безопасности / Е.В. Легчекова, О.В. Титов // Сб. науч. статей междунар. науч.-практ. конф. «Проблемы и перспективы электронного бизнеса». – Гомель: Изд-во Белорус. торгово-эконом. ун-та потребительской кооперации. – 2017. – С. 87-89.

89 Лычкина Н.Н. Имитационное моделирование экономических процессов. Учебное пособие для слушателей программы eMBI / Н.Н. Лычкина. – М.: Академия АйТи, 2005. – 164 с.

90 Льюнг Л. К овыпуклению критериев идентификации систем // Автомат. и телемех., 2019, № 9, 45–63; Autom. Remote Control, 80:9 (2019), С. 1591–1606.

91 Массель, А.Г., Гаськова. Д.А. Онтологический инжиниринг для разработки интеллектуальной системы анализа угроз и оценки рисков кибербезопасности энергетических объектов // Онтология проектирования.

Ontology of Designing. 2019. – Режим доступа https://dlib.eastview.com/browse/doc/53904780, свободный (дата обращения: 03.11.2024).

92 Массель Л.В. Применение онтологического, когнитивного и событийного моделирования для анализа развития и последствий чрезвычайных ситуаций в энергетике / Л.В. Массель // Проблемы безопасности и чрезвычайных ситуаций, 2010. – №2. – С. 34-43.

93 Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации [Текст] / А.А. Малюк. – М.: ГЛТ, 2004. – 280 с.

94 Медведев, А. В. Оптимизационная математическая модель информационной безопасности / А. В. Медведев // Научные исследования в современном мире. Теория и практика : Сборник избранных статей Всероссийской (национальной) научно-практической конференции, Санкт-Петербург, 10 октября 2021 года. – Санкт-Петербург: Частное научно-образовательное учреждение дополнительного профессионального образования Гуманитарный национальный исследовательский институт «НАЦРАЗВИТИЕ», 2021. – С. 66-68.

95 Месарович М. Теория иерархических многоуровневых систем [Текст] / М. Месарович, Д. Мако, Я. Такахара. – М.: Мир, 1973. – 311 с.

96 Метод Дельфи. [Электронный ресурс]. – Режим доступа: https://blog.wikium.ru/metod-ekspertnoj-otsenki-delfi-i-ego-primenenie.html, свободный (дата обращения: 15.05.2024).

97 Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры (утв. ФСТЭК РФ, 2007)

98 Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утв. ФСТЭК РФ, 14.02.2008)

99 Методика управления рисками ИБ компании Microsoft. [Электронный ресурс]. – Режим доступа: https://safe- surf.ru/specialists/article/ 5194/587935/#%D0%9E%D0%B1%D0%B7%D0%BE%D1%80%20%D0% BC%D0%B5%D1%82%D0%BE%D0%B4%D0%B8%D0%BA%D0%B8%2 0Microsoft, свободный (дата обращения: 15.05.2024).

100 Методический документ «Методика оценки угроз безопасности информации» (утв. Федеральной службой по техническому и экспортному контролю 5 февраля 2021 г.). – 83 с.

101 Методический документ. Утвержден ФСТЭК России 11 февраля 2014 г. «Меры защиты информации в государственных информационных системах» [Электронный ресурс]. URL : https://fstec.ru/component/attachments/ download/675 (дата обращения: 09.06.2024).

102 Милько Д.С. Экспертная система оценки угроз безопасности информации. Формальное представление объектов воздействия / Д.С. Милько, П.Н. Наседкин // Молодая наука Сибири: электрон. науч. журн. – 2021. – № 2 (12) [Электронный ресурс]. – Режим доступа: http://mnv.irgups.ru/toma/212-2021, свободный (дата обращения: 03.05.2024).

103 Мирсанова О.А. К вопросу об оценке эффективности затрат на информационную безопасность / О.А. Мирсанова. – URL: https://www.academia.edu/ 18137465/ (дата обращения: 20.02.2024).

104 Наседкин П.Н. Анализ востребованности компонентов уровня программно-технических решений КСЗИ предприятия с точки зрения обеспечения базовых требований по информационной безопасности / П.Н. Наседкин // Информационные технологии и математическое моделирование в управлении сложными системами, 2022. – № 2(14). – С. 50-64. – DOI 10.26731/2658-3704.2022.2(14).50-64.

105 Наседкин П.Н. Методика оценки уровня защищённости программно-технических решений комплексной системы защиты информации предпри-

ятия [Текст]/П.Н. Наседкин, М.П. Базилевский// Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. – М.: Информатика, вычислительная техника и управление. – 2023. – №3. С.87 –93.

106 Наседкин П.Н. Оценка состояния комплексной системы защиты информации на основе онтологий/П. Н. Наседкин, Л.В. Аршинский//Информационные и математические технологии в науке и управлении. 2023. № 1 (29). С. 158-177.

107 Наседкин, П.Н. Применение нечёткого присоединённого логического вывода в оценке эффективности функционирования комплексной системы защиты информации предприятий / П.Н. Наседкин, Л.В. Аршинский, Н.И. Глухов // Теоретические и прикладные вопросы реализации проектов в области информационной безопасности: Материалы межвузовской научно-теоретической конференции (в рамках Сибирского форума «Информационная безопасность – 2021»). – Новосибирск: Сибирский государственный университет телекоммуникаций и информатики, 2021. – С. 42-52.

108 Нестеров, С. А. Информационная безопасность : учебник и практикум для академического бакалавриата / С. А. Нестеров. – Москва : Издательство Юрайт, 2019. – 321 с. – (Университеты России). – ISBN 978-5-534-00258-4. – Текст : электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/434171 (дата обращения: 22.09.2024).

109 Наседкин П. Н. Формализация модели информационной безопасности предприятия в виде многокритериальной задачи линейного программирования / П. Н. Наседкин, М. П. Базилевский // Моделирование, оптимизация и информационные технологии. – 2023. – Т. 11, № 3(42). – С. 10-11. – DOI 10.26102/2310-6018/2023.42.3.021.

110 Носков С.И. Технология моделирования объектов с нестабильным функционированием и неопределенностью в данных. Иркутск: РИЦ ГП «Облинформпечать»; 1996. 320 с.

111 Об информации, информационных технологиях и о защите информации: федеральный закон от 27.07.2006 № 149-ФЗ (с изменениями и дополнениями от: 9 марта 2021 г.) // Гарант. – URL : https://base.garant.ru/12148555/ (дата обращения: 09.06.2024).

112 Оптнер С.Л. Системный анализ для решения деловых и промышленных проблем [Текст] / С.Л. Оптнер. – М.: Сов. Радио, 1969. – 216 с.

113 Петухов Г. Б., Якунин В. И. Методологические основы внешнего проектирования целенаправленных процессов и целеустремленных систем. М: АСТ, 2006. 504 с.

114 Перечень технической и технологической документации, национальных стандартов и методических документов, необходимых для выполнения работ и (или) оказания услуг, установленных Положением о лицензировании деятельности по технической защите конфиденциальной информации, утвержденным постановлением Правительства Российской Федерации от 3 февраля 2012 г. № 79. // ФСТЭК России URL: https://fstec.ru/dokumenty/vse-dokumenty/perechni/perechen-tekhnicheskoj-dokumentatsii-natsionalnykh-standartov-i-metodicheskikh-dokumentov-ot-12-avgusta-2020-g?highlight=WyJcdTA0NDBcdTA0NDNcdTA0M2FcdTA0M2VcdTA0MzJcdTA0M2VcdTA0MzRcdTA0NGZcdTA0NDlcdTA0MzhcdTA0MzUiLCJcdTA0NDBcdTA0NDNcdTA0M2FcdTA0M2VcdTA0MzJcdTA0M2VcdTA0MzRcdTA0NGZcdTA0NDlcdTA0MzhcdTA0M2NcdTA0MzgiLCJcdTA0NDBcdTA0NDNcdTA0M2FcdTA0M2VcdTA0MzJcdTA0M2VcdTA0MzRcdTA0NGZcdTA0NDlcdTA0MzhcdTA0NDUiLCJcdTA0NDBcdTA0NDNcdTA0M2FcdTA0M2VcdTA0MzJcdTA0M2VcdTA0MzRcdTA0NGZcdTA0NDlcdTA0MzhcdTA0M2MiLCJcdTA0NDBcdTA0NDNcdTA0M2FcdTA0M2VcdTA0MzJcdTA0M2VcdTA0MzRcdTA0NGZcdTA0NDlcdTA0NDNcdTA0NGUiLCJcdTA0NDBcdTA0NDNcdTA0M2FcdTA0M2VcdTA0MzJcdTA0M2VcdTA0MzRcdTA0NGZcdTA0NDlcdTA0MzVcdTA0MzNcdTA0M2UiLCJcdTA0NDBcdTA0NDNcdTA0M2FcdTA0M2VcdTA0MzJcdTA0M2

VcdTA0MzRcdTA0NGZcdTA0NDlcdTA0MzhcdTA0MzkiLCJcdTA0NDBcdTA0NDNcdTA0M2FcdTA0M2VcdTA0MzJcdTA0M2VcdTA0MzRcdTA0NGZcdTA0NDlcdTA0MzVcdTA0M2MiLCJcdTA0MzRcdTA0M2VcdTA0M2FcdTA0NDNcdTA0M2NcdTA0MzVcdTA0M2RcdTA0NDJcdTA0M2VcdTA0MzIiLCJcdTA0MzRcdTA0M2VcdTA0M2FcdTA0NDNcdTA0M2NcdTA0MzVcdTA0M2RcdTA0NDJcdTA0M2VcdTA0MzIiXQ== (дата обращения: 09.06.2024).

115 Плетнев П.В. Методика количественного определения рисков информационной безопасности / Плетнев П.В., Белов В.М. // Перспективы развития информационных технологий. 2011. № 5. С. 66-70.

116 Плетнёв П.В. Алгоритмы и методики оценки угроз информационной безопасности в сетях и системах телекоммуникаций: дис. ... канд. техн. наук: 05.12.13. – Сибирский гос. университет телекоммуникаций и автоматики, Новосибирск, 2017 – 322 с.

117 РС БР ИББС- 2.2- 2009. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения информационной безопасности. Введ. 2010-01-01. М., 2009. 23 с.

118 Ричард Эрнест Беллман, И. Гликсберг, О. Гросс Некоторые вопросы математической теории процессов управления. – Москва: Издательство «Мир»: Редакция литературы по математическим наукам, 1974. – 336 с.

119 Рогозин Е. А., Качаева Г. И., Попов А. Д., Показатели эффективности функционирования при разработке систем защиты информации от несанкционированного доступа в автоматизированных информационных системах // Вестник ДГТУ. Технические науки. 2018. №1. URL: https://cyberleninka.ru/article/n/pokazateli-effektivnosti-funktsionirovaniya-pri-razrabotke-sistem-zaschity-informatsii-ot-nesanktsionirovannogo-dostupa-v (дата обращения: 08.06.2024).

120 СЗИ «Страж NT». Руководство администратора. URL: https://guardnt.ru/doc/gnt_40_admin_guide.pdf (дата обращения: 26.05.2024).

121 Система защиты информации от несанкционированного доступа «Страж NT». Описание применения. URL: https://guardnt.ru/doc/gnt_40_app_guide.pdf (дата обращения: 26.05.2024).

122 Смирнов С.В. Онтологии как смысловые модели / С.В. Смирнов // Онтология проектирования, 2013. – №2. – С.12-19.

123 Советов Б.Я. Моделирование систем [Текст] / Б.Я. Советов. – М.: Высшая школа, 2009. – 343 с.

124 Советов Б.Я.,Теория информационных процессов и систем : учебник для студ. высш. учеб. заведений / [Б.Я.Советов, В.А.Дубенецкий, В.В.Цехановский и др.] ; под ред. Б.Я.Советова. – М. : Издательский центр «Академия», 2010. – 432 с.

125 Соколов А.В. Информационно-поисковые системы / / А.В Соколов. – М.: Радио и связь, 1981. – С. 152.

126 Сосинская, С.С. Разработка системы для расчёта рейтинга преподавателей на основе квалиметрического подхода и онтологии / С.С. Сосинская, Р.С. Дорофеев, А.С. Дорофеев // Онтология проектирования. – 2019. – Т.9. – №2(32). – С.214-224. – DOI: 10.18287/2223-9537-2019-9-2-214-224.

127 Улыбин А.В. Мультиагентный подход в имитационном моделировании / А.В. Улыбин, А.А. Арзамасцев// Вестник ТГУ, 2010. -Т. 15. -Вып.5. – С. 1470-1471.

128 Управление рисками информационной безопасности в России. Управление рисками информационной безопасности. – Режим доступа: https://halzen.ru/internet/upravlenie-riskami-informacionnoi-bezopasnosti-v-rossii-upravlenie-riskami.html, свободный (дата обращения: 09.05.2024).

129 Управление рисками. Модель безопасности с полным перекрытием [Электронный ресурс] – Режим доступа: https://intuit.ru/studies/courses/962/387/lecture/8990, свободный (дата обращения: 16.12.2024).

130 ФСТЭК России. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации [Электронный ресурс]. – URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/rukovodyashchij-dokument-ot-30-marta-1992-g-2?highlight=WyJcdTA0M2ZcdTA0M2VcdTA0M2FcdTA0MzBcdTA0MzdcdTA0MzBcdTA0NDJcdTA0MzVcdTA0M2JcdTA0MzVcdTA0M2MiLCJcdTA0M2ZcdTA0M2VcdTA0M2FcdTA0MzBcdTA0MzdcdTA0MzBcdTA0NDJcdTA0MzVcdTA0M2JcdTA0NGZcdTA0M2MiLCJcdTA0M2ZcdTA0M2VcdTA0M2FcdTA0MzBcdTA0MzdcdTA0MzBcdTA0NDJcdTA0MzVcdTA0M2JcdTA0NGZcdTA0M2NcdTA0MzgiLCJcdTA0M2ZcdTA0M2VcdTA0M2FcdTA0MzBcdTA0MzdcdTA0MzBcdTA0NDJcdTA0MzVcdTA0M2JcdTA0NGYiLCJcdTA0M2ZcdTA0M2VcdTA0M2FcdTA0MzBcdTA0MzdcdTA0MzBcdTA0NDJcdTA0MzVcdTA0M2JcdTA0MzgiLCJcdTA0M2ZcdTA0M2VcdTA0M2FcdTA0MzBcdTA0MzdcdTA0MzBcdTA0NDJcdTA0MzVcdTA0M2JcdTA0MzVcdTA0MzkiLCJcdTA0M2ZcdTA0M2VcdTA0M2FcdTA0MzBcdTA0MzdcdTA0MzBcdTA0NDJcdTA0MzVcdTA0M2JcdTA0NGMiLCJcdTA0M2ZcdTA0M2VcdTA0M2FcdTA0MzBcdTA0MzdcdTA0MzBcdTA0NDJcdTA0MzVcdTA0M2JcdTA0NGZcdTA0NDUiLCJcdTA0M2ZcdTA0M2VcdTA0M2FcdTA0MzBcdTA0MzdcdTA0MzBcdTA0NDJcdTA0MzVcdTA0M2JcdTA0NGUiLCJcdTA0M2ZcdTA0M2VcdTA0M2FcdTA0MzBcdTA0MzdcdTA0MzBcdTA0NDJcdTA0MzVcdTA0M2JcdTA0MzUiXQ== (дата обращения: 09.06.2024).

131 ФСТЭК РФ. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация

автоматизированных систем и требования по защите информации. [Электронный ресурс]. – URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/rukovodyashchij-dokument-ot-30-marta-1992-g-3?highlight=WyJcdTA0NDFcdTA0MzhcdTA0NDFcdTA0NDJcdTA0MzVcdTA0M2MiLCJcdTA0NDFcdTA0MzhcdTA0NDFcdTA0NDJcdTA0MzVcdTA0M2NcdTA0NDMiLCJcdTA0NDJcdTA0NDBcdTA0MzVcdTA0MzFcdTA0M2VcdTA0MzJcdTA0MzBcdTA0M2RcdTA0MzhcdTA0NGZcdTA0M2MiLCJcdTA0NDJcdTA0NDBcdTA0MzVcdTA0MzFcdTA0M2VcdTA0MzJcdTA0MzBcdTA0M2RcdTA0MzhcdTA0MzkiLCJcdTA0NDJcdTA0NDBcdTA0MzVcdTA0MzFcdTA0M2VcdTA0MzJcdTA0MzBcdTA0M2RcdTA0MzhcdTA0NGYiLCJcdTA0NDJcdTA0NDBcdTA0MzVcdTA0MzFcdTA0M2VcdTA0MzJcdTA0MzBcdTA0M2RcdTA0MzhcdTA0NGZcdTA0M2NcdTA0MzgiLCJcdTA0NDJcdTA0NDBcdTA0MzVcdTA0MzFcdTA0M2VcdTA0MzJcdTA0MzBcdTA0M2RcdTA0MzhcdTA0NGUiLCJcdTA0NDJcdTA0NDBcdTA0MzVcdTA0MzFcdTA0M2VcdTA0MzJcdTA0MzBcdTA0M2RcdTA0MzhcdTA0NGZcdTA0NDUiLCJcdTA0NDJcdTA0NDBcdTA0MzVcdTA0MzFcdTA0M2VcdTA0MzJcdTA0MzBcdTA0M2RcdTA0MzhcdTA0MzVcdTA0M2MiLCJcdTA0NDJcdTA0NDBcdTA0MzVcdTA0MzFcdTA0M2VcdTA0MzJcdTA0MzBcdTA0M2RcdTA0MzhcdTA0MzUiXQ== (дата обращения: 09.06.2024).

132 Черников Б. В., Поклонов Б. Е. Оценка качества программного обеспечения: Практикум: учебное пособие. М.: ИД «ФОРУМ»: ИНФРА-М, 2012. 400 с.

133 Шаньгин В. Ф. Комплексная защита информации в корпоративных системах:учебное пособие. М.: Форум, Инфра-М, 2010. 592 с.ISBN 978-5-16-003746-2.

134 Шелупанов А.А. Специальные вопросы информационной безопасности [Текст]: монография / А.А. Шелупанов, Р.В. Мещеряков. – Томск: Издво Института ОА СОРАН, 2003. – 224 с.

135 Шинаков, К. Е. Минимизация рисков нарушения безопасности при построении системы защиты персональных данных : специальность 05.13.19 "Методы и системы защиты информации, информационная безопасность" : диссертация на соискание ученой степени кандидата технических наук / Шинаков Кирилл Евгеньевич, 2018. – 256 с.

136 Шумский А.А. Системный анализ в защите информации [Текст]: учебное пособие для вузов / А.А. Шумский, А.А. Шелупанов. – М.: Гелиос АРВ, 2005. – 220 с.

137 Шумский А.А. Системный анализ в защите информации [Текст]: учебное пособие для вузов / А.А. Шумский, А.А. Шелупанов. – М.: Гелиос АРВ, 2005. – 220 с.

138 Эленберг М.С. Имитационное моделирование: учеб пособие / М.С. Эленберг, Н.С. Цыганков. – Красноярск: Сиб. федер. ун-т, 2017. – 128 с.

139 Юсупов Р. М., Мусаев А. А. Особенности оценивания эффективности информационных систем и технологий. // Труды СПИИРАН. – 2017. – № 2 (51). – С. 5 – 34.

140 Abdelkader Magdi Shaaban, Thomas Gruber and Christoph Schmittner. 2019. An ontology-based security tool for mission-critical cyber-physical systems. In Proceedings of the 23rd International Conference on Systems and Software Products – Volume B (SPLC '19). Association for Computing Machinery, New York, NY, USA, 207-210. – Режим доступа URL: https://doi.org/10.1145/3307630.3342397, свободный (дата обращения: 03.11.2024).

141 Arogundade, O.T., Abayomi-Alli, A. & Misra, S. An Ontology-Based Security Risk Management Model for Information Systems. Arab J Sci Eng 45, 6183–6198 (2020). – Режим доступа URL https://doi.org/10.1007/s13369-020-04524-4, свободный (дата обращения: 03.11.2024).

142 Aven, T. Foundations of Risk Analysis: A Knowledge and Decision-Oriented Perspective. Wiley, 2003. – Режим доступа:

https://www.amazon.com/Foundations-Risk-Analysis-Decision-Oriented-Perspective/dp/0471495484, свободный (дата обращения: 03.11.2024).

143 Biyashev R., Nyssanbayeva S., Kapalova N., Khakimov R., Modular models of the cryptographic protection of information // International Conference on Computer Networks and Information Security (CNIS2015), Changsha, China. 2015. P.393-398.

144 Biyashev R.G. The Development of a Structural Scheme of National Segment in a Protected Cross-Border Space [Текст] / R.G. Biyashev, S.E. Nyssanbayeva, Ye.Y. Begimbayeva // International Conference on Advanced Material Science and Environmental Engineering. – Chiang Mai, Thailand, 2016. – P. 250–252.

145 Book: "BowTies in Risk Management: A Concept Book for Process Safety" by CCPS (Center for Chemical Process Safety). Published by Wiley in 2018. – Режим доступа: https://www.aiche.org/ccps/resources/publications/books/bow-ties-risk-management-concept-book-process-safety, свободный (дата обращения: 03.11.2024).

146 CERT-RMM Resilience Management Model. Carnegie Mellon University, 2016. – Режим доступа: https://insights.sei.cmu.edu/library/cert-resilience-management-model-a-maturity-model-for-managing-operational-resilience/, свободный (дата обращения: 03.11.2024).

147 Checkland, Peter. Systems thinking, systems practice / Peter Checkland. – Repr. – Chichester etc. : Wiley, 1990. – XIV, 330 с. : ил.; 24 см.; ISBN 0-471-27911-0

148 Choi, Ch. Ontology-based access control model for security policy reasoning in cloud computing / Ch. Choi, Ju. Choi, P. Kim // The Journal of Supercomputing. – 2014. – Vol. 67, No. 3. – P. 711-722. – Режим доступа URL: https://www.semanticscholar.org/paper/Ontology-based-access-control-model-for-security-in-Choi-Choi/bd7d5c9a091e4db524aad6fb639a237b1c5042b3, свободный (дата обращения: 03.11.2024).

149 CIS RAM v2.1. Center for Internet Security, 2023. – Режим доступа: https://www.cisecurity.org/insights/white-papers/cis-ram-risk-assessment-method, свободный (дата обращения: 03.11.2024).

150 CISWG, USA (2005). «Report of the Best Practies and Metrics Teams», Corporate Information Security Working Group, Goverment Reform Committee. – Режим доступа: http://www.educause.edu/ir/library/pdf/CSD3661.pdf, свободный (дата обращения: 09.05.2023).

151 COBIT 5 Framework Framework for IT Governance and Management. ISACA, 2012. – Режим доступа: https://quadrosoft.by/images/pdf/baza_znanij/Cobit-5_frm_rus_0813.pdf, свободный (дата обращения: 03.11.2024).

152 COSO 2017 г. «Концептуальные основы управления рисками организации: интеграция со стратегией и управлением деятельностью». [Электронный ресурс]. – Режим доступа: https://sdo.pgups.ru/pluginfile.php/724560/mod_resource/content/1/0_coso%20erm%202017%20rules-of-game-changing.pdf, свободный (дата обращения: 15.05.2023).

153 COSO. Управление рисками организации. Интегрированная модель. М: 2004 – 111 с. [Электронный ресурс] – Режим доступа: http://www.aoosk.ru/about/vnutrenniy-kontrol-upravlenie-riskami /D%20COSO%20UR.pdf, свободный (дата обращения: 15.05.2023).

154 Dijkstra E.W. Self-stabilizing systems in spite of distributed control // Communications of the ACM. – 1974. – Vol. 17. – P. 643–644. – doi:10.1145/361179.361202

155 FEA Consolidated Reference Model Document. URL: https://www.reginfo.gov/public/jsp/Utilities/FEA_CRM_v23_Final_Oct_2007_Revised.pdf (дата обращения: 26.05.2023).

156 Fenz, S. and Neubauer, T. (2018), "Ontology-based information security compliance determination and control selection on the example of ISO 27002", Information and Computer Security, Vol. 26 No. 5, pp. 551-567. – Режим доступа: https://doi.org/10.1108/ICS-02-2018-0020, свободный (да-та обращения: 03.11.2024).

157 Gómez-Pérez, A., Fernández-López, M., Corcho, O. (eds.) Ontological Engineering: With Examples from the Areas of Knowledge Management, e-Commerce and the Semantic Web, pp. 1-45. Springer, London (2004). Режим доступа URL: https://link.springer.com/book/10.1007/b97353, свободный (дата обращения: 03.11.2024).

158 Gruber, T. R. A translation approach to portable ontology specifications / T. R. Gruber // Knowledge Acquisition. – 1993. – Режим доступа URL: https://www.semanticscholar.org/paper/A-translation-approach-to-portable-ontology-Gruber/5120f65919f77859a974fcc1ad08f72b2918b8ec, свободный (дата обращения: 03.11.2024).

159 Hubbard, D., Seiersen, R. How to Measure Anything in Cybersecurity Risk. Wiley, 2016. – Режим доступа: https://www.amazon.com/How-Measure-Anything-Cybersecurity-Risk/dp/1119085292, свободный (дата обращения: 03.11.2024).

160 Humphreys Ted, Plate Angelika, UK (2006). «Measuring the effectiveness of your ISMS implementations based on ISO/IEC 27001», BSI. – Режим доступа: https://123docz.net/document/13739149-bsi-bip-0074-2006.htm, свободный (дата обращения: 09.05.2023).

161 ISO/IEC 31010:2019. Risk management – Risk assessment techniques. ISO, 2019 – Режим доступа: https://www.iso.org/obp/ui/en/#iso:std:iec:31010:ed-2:v1:en,fr, свободный (дата обращения: 03.11.2024).

162 ISO/IEC TR 13335 Information technology – Guidelines for the management of IT Security (Информационная технология. Методы безопасности. Руководство по управлению безопасностью).

163 ISO/IEC TR 27016 Information technology – Security techniques – Information security management – Organizational economics (ISO/IEC TR 27016:2014).

164 ISO/IEC TR 9126-2:2003 Software engineering – Product quality – Part 2: External metrics.URL: https://www.iso.org/standard/22750.html (дата обращения: 26.05.2023).

165 ISO/IEC TR 9126-3:2003 Software engineering – Product quality – Part 3: Internal metrics. URL: https://www.iso.org/standard/22891.html (дата обращения: 26.05.2023).

166 ISO/IEC TR 9126-4:2004 Software engineering – Product quality – Part 4: Quality in use metrics. URL: https://www.iso.org/standard/39752.html (дата обращения: 26.05.2023).

167 Jelen G., SSE-CMM Security Metrics, ISSEA. – Режим доступа: http://www.sse-cmm.org/metric/metric.asp, свободный (дата обращения: 09.05.2023).

168 Jonsson Erland, «An Integrated Framework for Security and Dependability, Chalmers University of Technology». – Режим доступа: http://www.windowsecurity.com/uplarticle/5/Paradigms-nspw98-print.rev0001.fm55.pdf, свободный (дата обращения: 09.05.2023).

169 Kohonen T., “Self-Organizing Maps,” 3rd Edition, Springer-Verlag, Berlin, Heidelberg, New York, 2001, 501 p. https://dx.doi.org/10.1007/978-3-642-56927-2

170 Kormos C., Using Security Metrics to Assess Risk management Capabilities, National Security Agency. – Режим доступа: http://csrc.nist.gov/nissc/1999/proceeding/papers/p29.pdf, свободный (дата обращения: 09.05.2023).

171 Kovacich Gerald, USA (1997). « Information Systems Security Metrics Management», Computers & Security, Vol. 16, pp. 610-618. – Режим доступа: https://www.semanticscholar.org/paper/Information-systems-security-metrics-management-Kovacich/6b027b75a228caba425c89d53955b26adb5216d2, свободный (дата обращения: 09.05.2023).

172 Krunoslav, Arbanas., Mirko, Čubrilo. "Ontology in Information Security." Journal of information and organizational sciences, 39 (2015).:107-136. – Режим доступа URL: https://typeset.io/papers/ontology-in-information-security-2q3hvabws5, свободный (дата обращения: 03.11.2024).

173 L. Pan & A. Tomlinson, Int. J. of Safety and Security Eng., Vol. 6, No. 2 (2016) 270–281).- Режим доступа: https://www.witpress.com/elibrary/sse-volumes/6/2/1170, свободный (дата обращения: 09.05.2023).

174 Lennon B. Elizabeth, USA (2003), «IT Security Metrics, Information Technology Laborator», NIST, Information Security News: ITL Bulletin for August 2003. – Режим доступа: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=150707, свободный (дата обращения: 09.05.2023).

175 NATIONAL INFORMATION SYSTEMS SECURITY (INFOSEC) GLOSSARY – Режим доступа: https://docplayer.net/18620742-National-information-systems-security-infosec-glossary.html, свободный (дата обращения: 09.05.2023).

176 Payne C. Shirley USA (2006). «A Guide to Security Metrics», SANS Institute. – Режим доступа: https://sansorg.egnyte.com/dl/kiYWJmz3vh, свободный (дата обращения: 09.05.2023).

177 Peltier, T. R. Information Security Risk Analysis. Auerbach Publications, 2001. – Режим доступа: https://www.taylorfrancis.com/books/mono/10.1201/b12444/information-security-risk-analysis-thomas-peltier, свободный (дата обращения: 03.11.2024).

178 Robinson Chad, USA (2004), “Collecting Effective Security Metrics”, Robert Frances Group, http://www.csoonline.com/article/219182/collecting-effective-security-metrics

179 Sajko, Mario. (2014). Measuring and Evaluating the Effectiveness of Information Security. [Электронный ресурс]. – Режим доступа: https://www.researchgate.net/publication/328783419_Measuring_and_Evaluating_the_Effectiveness_of_Information_Security (дата обращения: 09.06.2024).

180 SSE-CMM System Security Engineering Capability Maturity Model. Carnegie Mellon University, 1999. – Режим доступа: https://archive.org/details/DTIC_ADA393329/mode/2up, свободный (дата обращения: 03.11.2024).

181 Swanson Marianne, et. All., USA (2003). «Security Metrics Guide for Information Technology Systems», NIST Special Publication 800-55. [Электронный ресурс]. – Режим доступа: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-55.pdf, свободный (дата обращения: 09.05.2023).

182 Vaughn Rayford B., Jr, (2002). Information Assurance Measures and Metrics – State of Practice and Proposed Taxonomy, Proceedings of the 36th Hawaii International Conference on System Sciences. – Режим доступа: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-55.pdf, свободный (дата обращения: 09.05.2023).

183 L.A. Zadeh, "Fuzzy sets," Information and Control, vol. 8, no. 3, pp. 338–353, 1965.– Режим доступа: https://home.iitk.ac.in/~avrs/ManyValuedLogic/Zadeh-1965.pdf, свободный (дата обращения: 25.11.2024).

Приложение А

Акт о внедрении результатов диссертационного исследования

Общество с ограниченной
ответственностью (ООО) «ЯНТА»

Байкальская ул., 265 д., Иркутск г., 664050
Тел./факс (395-2)35-77-22
www.yantacom.ru
E-mail:up@yantacom.ru
ИНН/КПП 3827017493/381150001

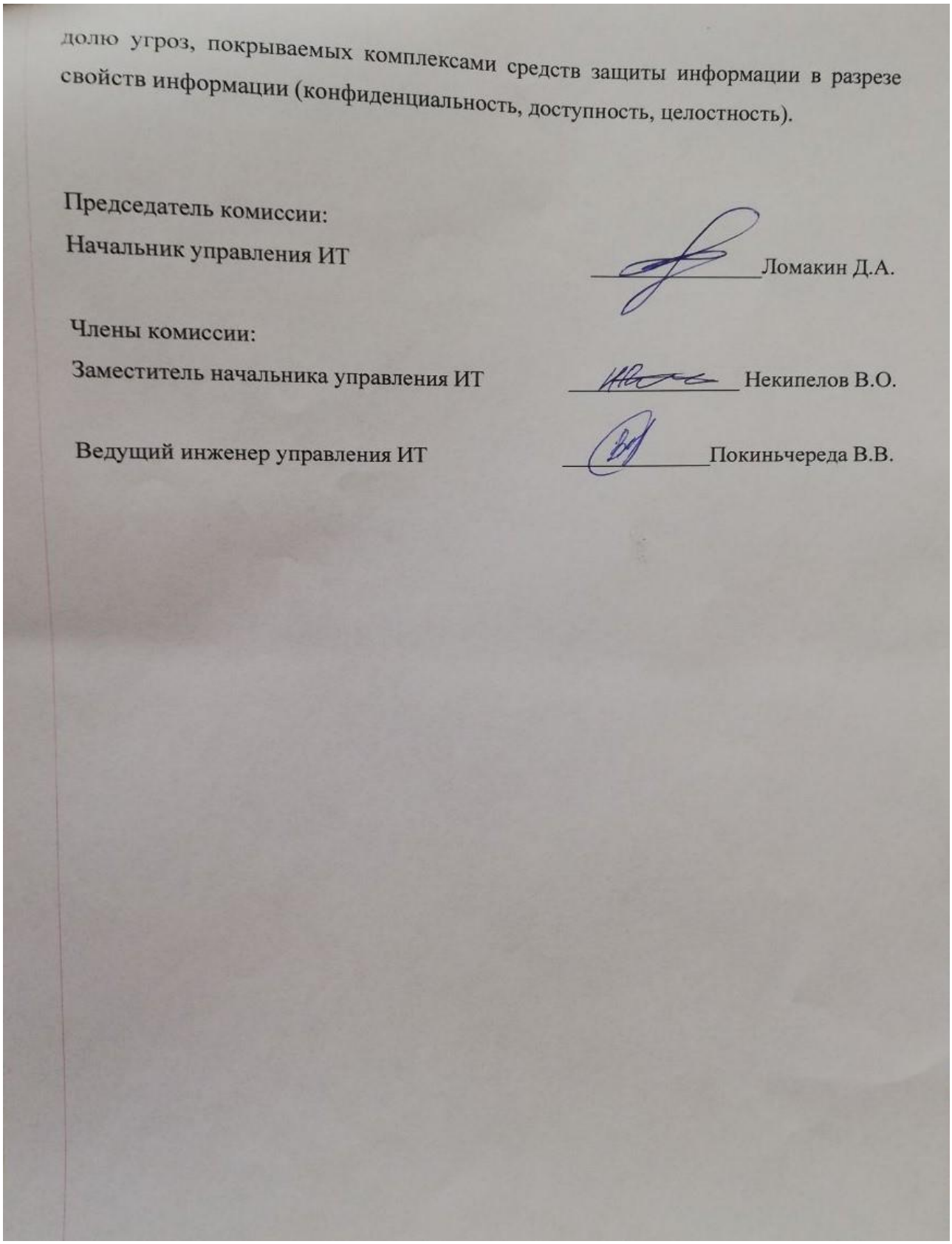
УТВЕРЖДАЮ
Исполнительный директор
ООО «Янта»
_____ Худилов Е.В.
«19» марта 2023 г.

АКТ
о внедрении результатов диссертационного исследования

Комиссия в составе: председателя – начальника управления ИТ Ломакина Д.А., членов комиссии: заместителя начальника управления ИТ Некипелова В.О. и ведущего инженера управления ИТ Покиньчереда В.В., составили настоящий акт о том, что результаты диссертационного исследования П.Н. Наседкина по теме «Методика оценки функциональной эффективности подсистемы программно-технических решений комплексной системы защиты информации предприятия» используются в текущей деятельности ООО «Янта» для обеспечения защиты информации и отказоустойчивости информационных систем предприятия в виде рекомендаций по повышению уровня защищённости ПТР КСЗИ.

Использование указанных результатов позволяет: повысить эффективность в управлении безопасностью предприятия; оптимизировать затраты на мероприятия по защите информационных активов; сократить время в оценке уровня защищённости ПТР КСЗИ; визуализировать наиболее критичные комплексы средств защиты информации в общей структуре защиты уровня ПТР; определить

Рисунок А.1 – Акт о внедрении результатов исследования (лист 1)



долю угроз, покрываемых комплексами средств защиты информации в разрезе свойств информации (конфиденциальность, доступность, целостность).

Председатель комиссии:
Начальник управления ИТ _____ Ломакин Д.А.

Члены комиссии:
Заместитель начальника управления ИТ _____ Некипелов В.О.

Ведущий инженер управления ИТ _____ Покиньчереда В.В.

Рисунок А.2 – Акт о внедрении результатов исследования (лист 2)

Приложение Б

Свидетельства о государственной регистрации программ для ЭВМ

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2023618996

Создание матрицы по укрупненной группировке объектов воздействия со стороны угроз безопасности информации и построение с учётом прототипа онтологической модели Комплексной Системы Защиты Информации (КСЗИ) корреляционных взаимосвязей: «Объект воздействия - Комплексы СрЗИ», «Угрозы - Комплексы СрЗИ», «Угрозы - Объекты воздействия»

Правообладатель: ***Федеральное государственное бюджетное образовательное учреждение высшего образования «Иркутский государственный университет путей сообщения» (ФГБОУ ВО ИрГУПС) (RU)***

Авторы: ***Наседкин Павел Николаевич (RU), Сверкунов Владимир Александрович (RU)***

Заявка № **2023618179**

Дата поступления **25 апреля 2023 г.**

Дата государственной регистрации в Реестре программ для ЭВМ ***03 мая 2023 г.***

Руководитель Федеральной службы по интеллектуальной собственности

Ю.С. Зубов

Рисунок Б.1 – Свидетельство о государственной регистрации программ для ЭВМ № 2023618996 от 03.05.2023г.

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2024616201

Программа оптимального распределения денежных средств для принятия решений по повышению эффективности программно-технических комплексов защиты информации предприятия

Правообладатель: ***Федеральное государственное бюджетное образовательное учреждение высшего образования «Иркутский государственный университет путей сообщения» (ФГБОУ ВО ИрГУПС) (RU)***

Авторы: ***Наседкин Павел Николаевич (RU), Базилевский Михаил Павлович (RU)***

Заявка № **2024615001**
Дата поступления **11 марта 2024 г.**
Дата государственной регистрации
в Реестре программ для ЭВМ ***18 марта 2024 г.***

Руководитель Федеральной службы по интеллектуальной собственности

Ю.С. Зубов

Рисунок Б.2 – Свидетельство о государственной регистрации программ для ЭВМ № 2024616201 от 18.03.2024г.