Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Владимирский государственный университет
имени Александра Григорьевича и Николая Григорьевича Столетовых»

На правах рукописи

Черников Роман Сергеевич

МОДЕЛИ И АЛГОРИТМЫ ОЦЕНКИ РАБОТОСПОСОБНОСТИ ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ ЦЕНТРАЛИЗОВАННОЙ ОХРАНЫ ОБЪЕКТОВ

Специальность 2.2.15 - Системы, сети и устройства телекоммуникаций

Диссертация на соискание ученой степени

кандидата технических наук

Научный руководитель

Монахов Михаил Юрьевич

д.т.н., профессор

Владимир, 2023

Содержание

ВВЕДЕНИЕ

Актуальность темы. Под работоспособностью в работе понимается способность телекоммуникационной сети (ТКС) централизованной охраны объектов (ЦОО) обеспечивать выполнение основных функций по передаче и обработке циркулирующей информации в заданном объеме и с необходимым качеством в условиях дестабилизирующих воздействий (ДВ). По мере развития и усложнения средств, методов и форм автоматизации процессов обработки и передачи информации в ТКС ЦОО повышается уязвимость системных процессов и ресурсов, напрямую влияющая на возможность уничтожения, блокирования или искажения информации, появления в системе «нештатных» процессов, создающих ситуацию невозможности эффективного выполнения основных функций.

Причинами снижения работоспособности ТКС ЦОО являются архитектурные просчеты, ошибки реализации программных и аппаратных компонентов, преднамеренные информационные воздействия, ошибки операторов, старение оборудования. Для обеспечения системной работоспособности ТКС ЦОО должна обладать способностью предсказывать возможные вторжения – т.е. прогнозировать повышенный риск выхода из строя компонентов системы. Результатом этого может быть повышение защищенности компонентов и/или устранение уязвимостей. Для технической реализации данной способности в ТКС ЦОО должны быть предусмотрены средства моделирования и оценки информационной защищенности компонентов от прогнозируемых угроз. В настоящее время существующие ТКС ЦОО такой возможностью не обладают.

Несмотря на интеграцию в телекоммуникационные сети современных аппаратно-программных средств защиты и управления сетями, процессы контроля работоспособности автоматизированы лишь частично, отсутствуют эффективные модели и алгоритмы обнаружения и идентификации угроз и уязвимостей в

составе единой системы, что часто является основной причиной продолжительному снижению эффективности функционирования телекоммуникационной сети.

Проведенный анализ процессов ИБ в ТКС ЦОО позволяет сделать выводы об отсутствии моделей и алгоритмов, позволяющих получать количественные оценки работоспособности ТКС ЦОО в условиях дестабилизирующих факторов и противодействий нарушителей. В нормативных документах Росгвардии России также отсутствуют рекомендации по обеспечению защиты информации в ТКС ЦОО.

Таким образом, исследования, направленные на создание моделей и алгоритмов оценки работоспособности ТКС ЦОО, актуальны и имеют практическое значение в решении проблемы обеспечения качества функционирования устройств и сетей телекоммуникаций.

Степень проработанности темы исследования.

Моделирование процессов информационной защиты объектов при их централизованной охране является комплексной и требует:

- корректную декомпозицию технических средств ТКС ЦОО на структурные компоненты, выделения выполняемых функций и информационных процессов;

- классификацию защищаемых информационных ресурсов по степени конфиденциальности, целостности и доступности;

- анализа и идентификации уязвимостей и возможных угроз, использования организационных и технических защитных механизмов;

- формирования модели нарушителя.

Задачи моделирования процессов информационной защиты, охраны и безопасности в ТКС, включая системы ЦОО, решались в трудах российских ученых Медведковского И.Д., Зегжды П.Д., Малюка А.А., Шелупанова А.А., Ященко В.В., Петракова А.В., Соколова А.В., Шаньгина В.Ф., Шелухина О.И., Черемушкина А.В., Макаренко С.И., Зарубина В.С., Меньших В.В., Булгакова О.М., Магауенова Р.Г., Синилова В.Г., Членова А.Н., Герасименко В.А., Волхонского

В.В., Домарева В.В., Лукацкого А.В., Завгороднего В.И. и других. Значительный вклад в решение выделенной проблемы внесли зарубежные исследователи Р. Брэтт, К. Касперски, С. Норкатт, В. Столингс, К. Лендвер, M. Howard, R. Graham, D. Sanai, S. Manwani, M. Montoro, F. Cohen, J. Jung, D.Moore, C.Zou, W. Lou, Y. Fang и другие.

Вопросам исследования процессов ИБ в структурных компонентах ТКС ЦОО посвящено большое количество научных публикаций. Их анализ позволяет выделить следующие направления исследований:

- модели систем физической защиты объектов;
- структуры и функционирование ПЦО;
- интегрированные системы безопасности (ИСБ);
- радиоканальные системы передачи извещений и обеспечение безопасности их функционирования;
- защита информационных ресурсов при ЦОО;
- обеспечение ИБ в локальной вычислительной сети (ЛВС) ПЦО.

Модели систем физической защиты объектов рассматривались в монографиях и диссертациях [58, 66-71]. Деятельность ПЦО по охране объектов, структура ПЦО, математическое описание и модели информационных процессов ПЦО рассматривались в работах [72-77]. В [72] описываются принципы функционального описания противоправных действий по нарушению ИБ ПЦО как методическая основа формализованного представления угроз этих систем. В [73] приводится матричное представление иерархии функционального описания противоправных действий по нарушению ИБ ПЦО. В [74] представлены результаты НИР в области создания инструментального ПО, предназначенного для мониторинга показателей качества пользовательских интерфейсов комплексов средств автоматизации ПЦО. Публикация [75] посвящена вопросам организационного обеспечения деятельности подразделений вневедомственной охраны полиции по защите информации (ЗИ). Рассмотрены принципы и условия организационного обеспечения ЗИ в деятельности ПЦО. В [76] предлагается на основе топологии

охраняемых помещений, средств охраны объекта, типов элементов строительных конструкций и, используя временные параметры срабатывания извещателей, определять возможность взаимосвязи тревожных извещений с НСД. Статья [77] посвящена вопросам защиты объектов от криминальных и террористических угроз с помощью средств инженерно-технической укрепленности и технических средств охраны. В работе проведен анализ имитостойкости отдельных звеньев системы сигнализации при централизованной охране объектов с передачей тревожных извещений на ПЦО.

Функционированию объектовых средств ТСО и моделированию ИСБ на объектах защиты посвящены работы [78-86]. В частности, в [78, 85] рассматриваются протокол-ориентированные подходы к моделированию архитектур ИСБ с обоснованием внутренних конфликтов. Для каждого из подходов приводится гипотетический пример получаемой архитектуры безопасности абстрактной ИСБ. В [79] анализируется ИСБ как комплексное и рациональное прикладное решение в части организации надежной физической охраны объектов от преступных посягательств, описываются угрозы ИБ и предлагаются решения по повышению информационной защищенности.

Публикация [80] рассматривает вопросы оценки достаточности оснащения техническими средствами охраны и безопасности зданий и помещений объектов для недопущения НСД, предлагается система критериев и логических правил комплексного оценивания безопасности объектов, а также направления автоматизации процессов принятия решения на основе экспертного анализа. Статья [81] посвящена проблеме оценки ресурсов, необходимых для развертывания и функционирования системы ИБ организации. Моделированию функционирования ИСБ как информационной системы посвящены публикации [82, 83]. В [84] функционирование ИСБ интерпретируется посредством описания графа состояний. В [86] проведена формализация модели жизненного цикла ИСБ.

Вопросам ЗИ при централизованной охране посвящены публикации [87 - 94]. В [87] рассмотрены основы концепции интеллектуализации процесса кон-

троля безопасности связи в информационно-телекоммуникационной сети специального назначения. На основе анализа международных стандартов и с учетом сложившейся практики к построению систем управления сложными техническими объектами выявлены основные проблемы автоматизации контроля безопасности и предложен подход синтеза интегрированной многоагентной системы контроля с адаптивным управлением вычислительными и транспортными ресурсами. В [88] предлагается подход к оценке частных показателей доступности ИСБ, в качестве которых предлагается рассматривать живучесть, надежность, имитостойкость и криптозащищенность.

В [89] рассматриваются основные проблемы обеспечения ИБ интегрированных систем управления на начальных стадиях их жизненного цикла, связанные с деятельностью субъектов при обосновании и реализации системотехнических и технологических решений по их созданию.

Вопросам компьютерной безопасности цифровых сетей ПЦО посвящены работы [90-91]. Программный комплекс [92] предназначен для расчёта времени реагирования на проникновения на охраняемый объект. Программа производит анализ преодолеваемых участков для определения степени необходимой защиты. В работе [93] рассматриваются принципы функционального описания противоправных действий по нарушению ИБ укрупненных ПЦО как методическая основа формализованного представления угроз ИБ этих систем. В [94] рассматриваются возможные допущения и ограничения, применяемые при математической интерпретации угроз нарушения целостности и доступности информации в ТКС.

Общим вопросам ЗИ в ЛВС ПЦО посвящены публикации [95 - 104]. В [95] рассматривается формализованное представление механизмов комплексного контроля информационных процессов. Приводится аналитическое выражение для оценки эффективности контроля. В [96, 97] проведен анализ модели каналов утечки конфиденциальной информации объектов МВД на основе анализа инцидентов ИБ, рассматривается подход к формализованному представлению меха-

низмов ЗИ. В [98] предложен подход к оценке эффективности процедур ЗИ в системах охранного мониторинга. В [99] рассматривается комплекс специальных требований к технологии функционирования защищенной автоматизированной информационной системы. Публикация [100] посвящена формированию основных принципов функционально-информационного моделирования противоправных действий по реализации угроз информационным процессам и действий по ЗИ в этих системах. В [101, 102] рассмотрены подходы к обоснованию требований к времени реализации функций противодействия угрозам нарушения состояний защищенности информации систем управления комплекса безопасности на основании показателя эффективности противодействия такого рода угрозам. Статья [103] формирует подходы к структуризации функционально-информационного представления противоправных действий по реализации угроз информационным процессам в технических системах безопасности и охранного мониторинга, а также действий по ЗИ в этих системах. В [104] приводятся математические зависимости для определения характеристик информационных процессов в системах безопасности на ПЦО в условиях воздействия вредоносных программ и реализации процедур ЗИ от угроз ее искажения и блокирования компонентами антивирусной защиты.

Публикации [105 - 114] посвящены вопросам деятельности нарядов физической охраны объектов (группы задержания). В [105] представлены результаты решения оптимизационной задачи минимизации риска охранной деятельности путем поиска места расположения группы задержания.

Работа [109] рассматривает модель принятия решения по повышению эффективности функционирования подразделений полиции. Для поиска оптимального места расположения группы задержания предлагается использовать численный метод роевых частиц. Публикация [110] посвящена формирования критерия размещения групп задержания, основанном на величине возможного причиняемого ущерба. В работе приведен алгоритм поиска пунктов размещения групп задержания, приводится результат вычислительного примера. В [111] рассмотрена

методика определения расчетного показателя количества сотрудников групп задержания подразделений вневедомственной охраны для закрытия маршрутов патрулирования и участия в обеспечении общественной безопасности.

Объектом исследования диссертации является телекоммуникационная сеть централизованной охраны объектов.

Предметом исследования являются модели и алгоритмы оценки работоспособности телекоммуникационной сети централизованной охраны объектов в условиях дестабилизирующих воздействий.

Цель и задачи исследования. Целью диссертационного исследования является разработка новых моделей и алгоритмов оценки работоспособности телекоммуникационной сети централизованной охраны объектов в условиях дестабилизирующих факторов и противодействий нарушителей. Достижение поставленной цели предполагает оценку современного состояния задачи, анализ научных публикаций по рассматриваемой теме и решение следующих задач:

1. Построить модель работоспособности ТКС ЦОО, позволяющую анализировать работу телекоммуникационной сети в условиях действия дестабилизирующих воздействий.

2. Разработать средства моделирования процессов обеспечения информационной безопасности в ТКС ЦОО, включая базы данных угроз, уязвимостей компонентов ТКС ЦОО, защитных механизмов, модель нарушителя информационной безопасности.

3. Разработать алгоритмы определения степени проявления уязвимости и силы защитных механизмов ТКС ЦОО

4. Разработать методику проведения аудита работоспособности ТКС ЦОО и показать ее адекватность на практике.

Научная новизна полученных в ходе исследования результатов заключается в следующем:

1. Предложена модель работоспособности ТКС ЦОО, определяемая функцией вероятностей защищенности компонентов телекоммуникационной сети на основе анализа ее инфраструктуры и условий эксплуатации.

2. Разработаны алгоритмы:

- оценки вероятности реализации угрозы при наличии уязвимости компонента ТКС ЦОО, отличающийся вновь выявленными закономерностями между типом угроз и способами проявления уязвимостей;

- оценки вероятности опасности угроз в компонентах ТКС ЦОО с учетом защитных механизмов, отличающийся вновь выявленными закономерностями между типом угроз, способом и характером действия защитных механизмов;

- определения степени проявления уязвимостей и силы защитных механизмов, выявляемых в компонентах ТКС ЦОО, оригинальность которого основана на их декомпозиции в зависимости от условий эксплуатации компонентов.

3. Усовершенствована модель оценки вероятности информационной защищенности компонента ТКС ЦОО, оригинальность которой состоит в том, что в модель включен элемент «Нарушитель» и сопутствующие ему параметры.

Практическая значимость работы заключается в том, что предложенные в данной работе модели и алгоритмы позволяют:

- проводить оценку защищенности информационных процессов по показателям конфиденциальности, доступности и целостности в каждом из структурных компонентов ТКС ЦОО для всех режимов функционирования;

- проводить прогнозирование изменения состояния работоспособности всех структурных компонентов системы ТКС ЦОО в течении планируемого периода их эксплуатации;

- проводить оценку эффективности использования определенных защитных механизмов для повышения защищенности и работоспособности конкретных структурных компонентов системы ТКС ЦОО в конкретных режимах функционирования;

- находить структурные компоненты ТКС ЦОО, обладающие минимальной защищенностью и работоспособностью в определенных режимах функционирования, что позволяет выборочно применять защитные механизмы, усиливающие защищенность конкретных структурных элементов системы;

- прогнозировать изменение состояния работоспособности всех структурных компонентов системы ТКС ЦОО при приеме под охрану новых объектов, а, следовательно, принимать техническое решение о возможности приема под охрану объекта;

- оптимизировать дислокацию нарядов и постов групп задержания, приближая их к особенно важным, критически защищаемым объектам и повышая при этом их защищенность в конкретных режимах функционирования.

Применение предложенных в работе методик и алгоритмов позволит своевременно выявлять уязвимости функционирования объектовых комплексов ТСО и внедрять соответствующие защитные механизмы. Статистика использования данных защитных механизмов [11, 56, 58] показывает, что при этом возможно снизить уровень ложных срабатываний на ПЦО в среднем на 15-20%. Ложные срабатывания ТСО фактически являются ошибками 1 рода работоспособности функционирования ТКС ЦОО.

Расчеты работоспособности структурных компонентов ТКС ЦОО мини-ПЦО для объектов разных категорий показывают, что уровень ошибок 2 рода (допущение НСД на защищаемый объект) потенциально можно снизить путем внедрения соответствующих защитных механизмов на 8-10%.

Кроме того, полученные в работе результаты могут быть использованы для:

- повышения эффективности эксплуатации программных и технических средств структурных компонентов ТКС ЦОО за счет оптимизации их эксплуатационно-технического обслуживания;

- снижения уровня ложных срабатываний средств охранно-тревожной сигнализации на защищаемых объектах путем повышения эффективности эксплуатации объектовых комплексов ТСО;

- анализа оптимальной численности нарядов и постов физической охраны для обеспечения требуемого уровня работоспособности всех структурных компонентов системы ТКС ЦОО во всех режимах функционирования;

- экономической оценки рентабельности оказания услуг по централизован-

ной охране объектов и служить основой для расчетов тарифов по централизованной охране;

- оптимизации тактики действий нарядов физической охраны при действиях на объекте защиты при пресечении НСД нарушителя.

Результаты исследований внедрены в корпоративной телекоммуникационной сети пункта централизованной охраны отдела вневедомственной охраны по городу Владимиру – филиала ФГКУ «УВО ВНГ Российской Федерации по Владимирской области», внедрением в обеспечение работоспособности и ИБ телекоммуникационных сетей «Цербер-мониторинг», МКУ «Управление гражданской защиты» и администрации г. Владимира, а также были использованы при разработке учебных курсов во Владимирском государственном университете и Владимирском юридическом институте ФСИН России. Внедрение результатов подтверждается соответствующими актами.

Методы исследования. При решении поставленных задач применялись: анализ процессов обеспечения системной работоспособности, синтез и моделирование алгоритмов и процедур обработки информации в сетях телекоммуникаций. Научные положения работы теоретически обосновываются с помощью аппарата теории множеств, теории графов, теории вероятностей, алгебры логики, теории статистического обнаружения, математической статистики.

Положения, выносимые на защиту:

1. Синтезированные базы данных уязвимостей, угроз, защитных механизмов, типов нарушителя и их взаимосвязи обладают универсальностью и достаточностью для ТКС ЦОО.

2. Предложенная модель работоспособности позволяет прогнозировать изменения состояния ТКС ЦОО и повышать защищенность ее компонентов.

3. Разработанные средства дают возможность снизить уровень ложных срабатываний на пульте централизованной охраны (ПЦО) на15-20%, несанкционированнй доступ на защищаемый объект - на 8-10%.

Достоверность результатов диссертационного исследования подтверждается корректным использованием математических методов, результатами вычис-

лительных экспериментов, а также проведением пробных расчетов работоспособности ТКС ЦОО.

Апробация работы. Материалы диссертационной работы докладывались и обсуждались на: III Всероссийской научной конференции (с приглашением зарубежных ученых) «FISP-2021: Фундаментальные проблемы информационной безопасности в условиях цифровой трансформации», Ставрополь, 30 ноября 2021 года; 14-ой международной научно-технической конференции «Перспективные технологии в средствах передачи информации: материалы», Владимир, 06–07 октября 2021 года; V Международном пенитенциарном форуме "Преступление, наказание, исправление", Рязань, 17–19 ноября 2021 года; XIII Международной научной конференции «Шуйская сессия студентов, аспирантов, педагогов, молодых ученых», Москва-Иваново-Шуя, 25 сентября 2020 года; Международной научно-теоретической конференции адъюнктов, аспирантов, соискателей, курсантов и студентов «Человек: преступление и наказание», Рязань, 27 марта 2020 года.

Публикации*:* опубликовано 13 работ, 2 в изданиях из перечня ВАК, 2 программы ЭВМ.

Глава 1. ПРОБЛЕМА ОБЕСПЕЧЕНИЯ РАБОТОСПОСОБНОСТИ ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ ЦЕНТРАЛИЗОВАННОЙ ОХРАНЫ ОБЪЕКТОВ

Обеспечение работоспособности системы централизованной охраны объектов (ЦОО) представляет собой комплексную проблему, которая решается в направлениях нормативного регулирования ее применения, совершенствования методов и средств их разработки, обеспечения соответствующих организационно-технических условий безопасной эксплуатации.

Технической основой функционирования (взаимодействия компонентов и подсистем) системы централизованной охраны является телекоммуникационная сеть (ТКС ЦОО), связывающая компоненты в единую автоматизированную систему управления централизованной охраной.

В настоящее время злоумышленниками (нарушителями) активно развивается широкий спектр методов и технологий информационного воздействия как на ТКС ЦОО в целом, так и на отдельные ее компоненты и технологии. Реализация угроз направлена на получение НСД к информационным ресурсам и нарушение их устойчивого функционирования. Постоянно совершенствуются уже существующие и появляются новые способы и средства проведения атак, а число инцидентов информационной безопасности в ТКС ЦОО ежегодно увеличивается.

В этих условиях проблема обеспечения информационной безопасности ТКС ЦОО в различных эксплуатационных условиях становится одной из ключевых в решении задач построения работоспособной (надежной, функционально устойчивой) системы ЦОО.

В данной главе анализируются особенности телекоммуникационной сети централизованной охраны объектов, принципиальные в её работе. Вводится понятие защищенности компонентов ТКС ЦОО, как принципиального свойства обеспечения её работоспособности. Рассматриваются информационные атаки злоумышленников в качестве основных причин снижения работоспособности ТКС ЦОО. Построена концептуальная модель работоспособности ТКС ЦОО,

позволяющая анализировать работу сети в условиях действия ДВ. Предложена формальная модель работоспособности ТКС. Сформулированы и формализованы концепции модели оценки ТКС. Уточняется задача исследования.

1.1 Структура телекоммуникационной сети централизованной охраны объектов

Объектом исследования диссертации является ТКС централизованной охраны объектов.

Особенности ТКС ЦОО, принципиальные в данной работе, проанализируем при системном рассмотрении обобщенной структурной схемы ТКС ЦОО и взаимодействия ее типовых функциональных элементов.

Обобщенная структурная схема ТКС ЦОО приведена на рисунке 1.1.

ТКС ЦОО образуют следующие модули:

Комплекс объектовых средств охранно-тревожной сигнализации (КОС ОТС) объекта.

Основное назначение - осуществление выдачи тревожного извещения при обнаружении угрозы несанкционированного проникновения на охраняемый объект (охранная сигнализация) и/или выдачи извещения о нападении (тревожная сигнализация). Первичными элементами в составе КОС ОТС являются извещатели охранно-тревожной сигнализации (ОИ) [40]. ОИ защищают (блокируют) элементы строительной конструкции или внутренний объем охраняемого объекта, а основу функционирования ОИ составляет физический принцип действия его чувствительного элемента (электромагнитный, вибрационный, радиотехнический, емкостный, оптический и т.д.).

Чувствительный элемент - это первичный преобразователь, реагирующий на воздействие нарушителя на элементы строительной конструкции или внутренний объем охраняемого объекта.

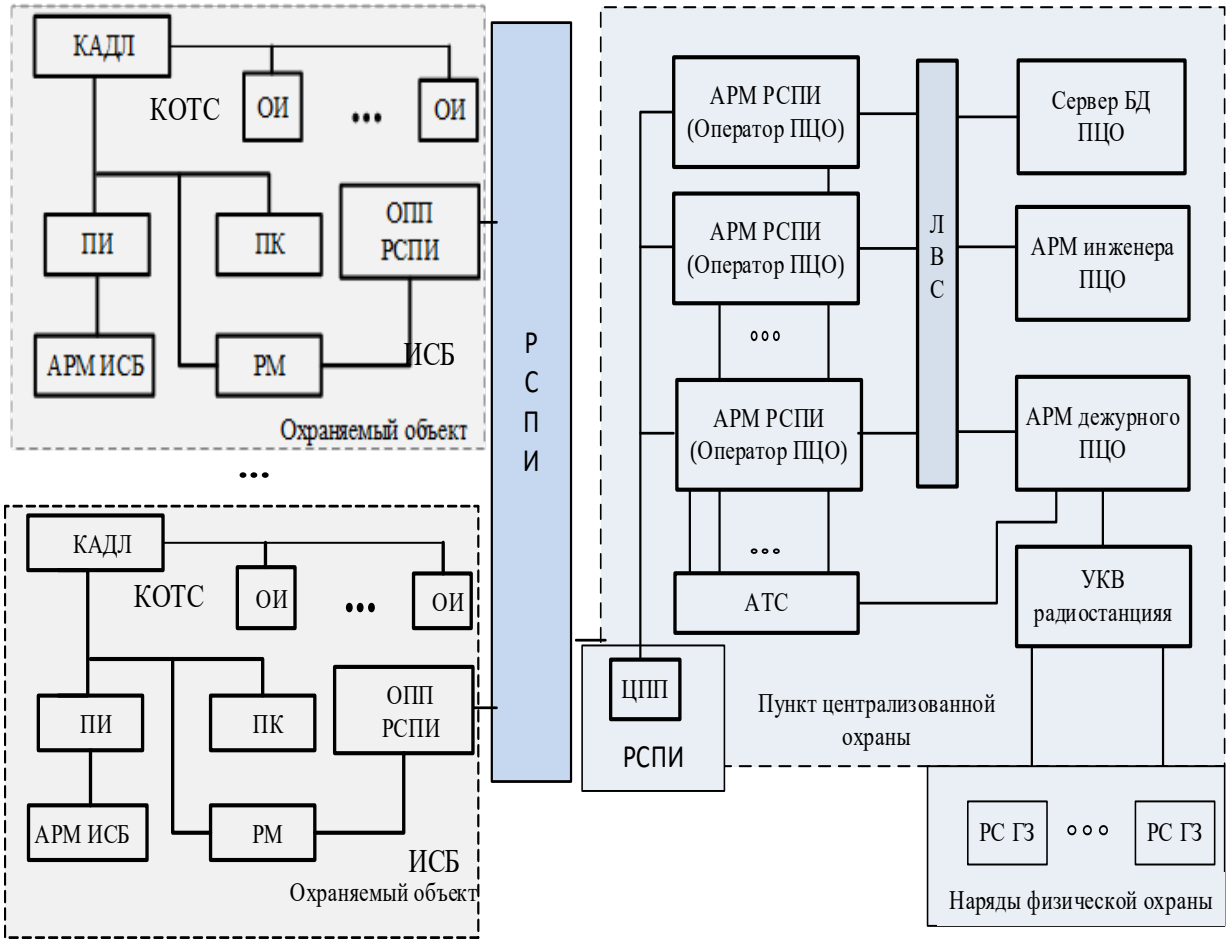

Рисунок 1.1 - Обобщенная структурная схема ТКС централизованной охраны объектов

Построение КОС ОТС регламентируются нормативными документами и стандартами [1-7, 9-11], а выпускаемые отечественные и зарубежные технические средства КОС ОТС, соответствующие требованиям Российских стандартов, включены в единый список [12]. Типовые проектные решения построения КОС ОТС для различных типов объектов приведены в [14].

В настоящее время наибольшее применение получили интегрированные системы охраны и безопасности (ИСБ), которые на программно-аппаратном уровне интегрируют различные подсистемы безопасности на защищаемом объекте [15]. Рекомендации по охране особо важных объектов с применением ИСБ приведены в [16].

На охраняемом объекте ОИ опрашиваются и передают информацию о своем состоянии на контроллер адресной двухпроводной линии (КАДЛ). КАДЛ

передает информацию от ОИ по используемому для данной ИСБ интерфейсу, например, RS-485 на АРМ ИСБ. Для передачи информации на АРМ ИСБ используется преобразователь интерфейсов (ПИ), например, RS485/USB. Далее на АРМ ИСБ происходит анализ информации о состоянии охраны объекта. На основании анализа формируются служебные и/или тревожные извещения, которые передаются на пункт централизованной охраны (ПЦО) охранной или мониторинговой компании (организации).

В программном обеспечении АРМ ИСБ заложены сценарии формирования тревожных и служебных извещений, которые активируются при срабатывании ОИ. В целом АРМ ИСБ реализует «тактику охраны» для данного объекта, которая представляет собой совокупность программных сценариев управления системой ИСБ при получении различных типов извещений от ОИ.

Для передачи тревожных извещений на ПЦО используют релейные модули (РМ), которые формируют «ПЦН выходы» по рубежам охраны с объекта на ПЦО. Согласно [2] первый рубеж охраны - это периметр защищаемого помещения, второй рубеж - внутренний объем, третий рубеж - это непосредственно охраняемые предметы или подступы к ним.

Требования к ИСБ, описание трех самых распространенных отечественных ИСБ «Орион-Про» (www.bolid.ru), «Рубеж-08» (http://www.sigma-is.ru/) и «Стрелец-Интеграл» (https://argus-spectr.ru/) приведены в Приложении 1.

Система передачи извещений (СПИ)

СПИ – это совокупность совместно действующих устройств и технических средств связи, обеспечивающих передачу информации состояния КОС ОТС операторам ПЦО.

СПИ служит для решения следующих задач:

- передача информации о состоянии охраняемых объектов,
- передача информации о проникновении на охраняемые объекты,
- передача служебных и контрольно-диагностических извещений.

Классификация СПИ приведена на рис.1.2.

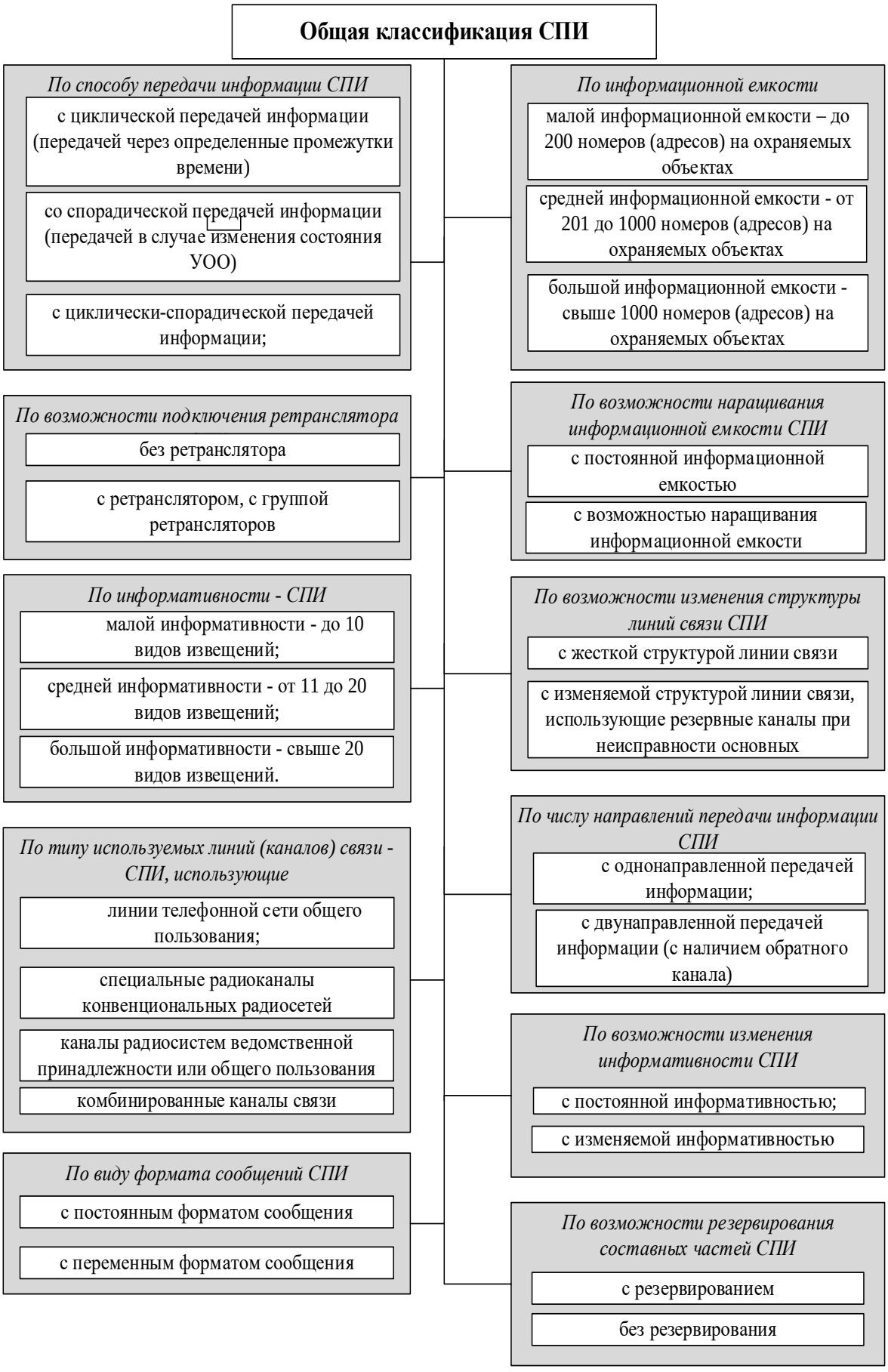

Рисунок 1.2 - Классификация СПИ

Требования к СПИ [11]:

- время обнаружения неисправности каналов передачи информации не должно превышать 120 с.

- время доставки тревожных извещений не должно превышать 15 с;

- время доставки служебных извещений не должно превышать 120 с.

Система передачи извещений радиоканальная (РСПИ) применяется для охраны нетелефонизированных объектов, от которых единственным способом передачи информации является радиосвязь, или как дополнение к телефонному каналу для повышения надёжности системы. В зависимости от типа используемого радиоканала все РСПИ можно разделить на три основные группы:

- РСПИ, использующие передачу сигнала в общедоступных частотных диапазонах (27, 433, 868 МГц);

- РСПИ, использующие передачу сигнала в выделенных частотных диапазонах (136-174МГц, 400-512МГц, 30-52МГц);

- системы мониторинга, использующие в качестве канала передачи сообщений сотовую связь стандарта GSM (GSM Voice, SMS, GPRS).

Основным преимуществом РСПИ на базе GSM является отсутствие необходимости приобретения частотного ресурса и построения сети ретрансляторов, использование существующих сетей ретрансляции, которые обеспечивают дальность действия в рамках зоны покрытия сотовой сети операторов мобильной связи.

Основными недостатками РСПИ на основе каналов сотовой связи являются:

- неопределенное время доставки SMS-сообщений;

- отсутствие гарантированного оперативного соединения (особенно во время пиковых нагрузок сети);

- тарифицированная оплата оператору;

- свободная продажа недорогих устройств подавления каналов сотовой связи.

Технические характеристики, топология, требования нормативных

стандартов к РСПИ определены в [17 - 30].

Основными достоинствами РСПИ с передачей на общедоступных или выделенных частотах являются:

- независимость от наличия телефонных линий или GSM-связи;

- оперативность и относительная простота развертывания и внедрения;

- высокая скорость передачи информации (менее секунды);

- высокая информативность сообщений;

- возможность создания системы охраны в рамках ведомства или отдельной организации.

К недостаткам указанных РСПИ можно отнести:

- необходимость получения частот и регистрация передатчиков в органах Министерства связи РФ;

- более высокая стоимость базового оборудования, программного обеспечения и их обслуживания;

- необходимость установки ретрансляторов для обслуживания больших территорий;

- отсутствие единых стандартов передачи данных.

Передача информация о ПЦН на ПЦО. Выходы РМ подключаются ко входам объектового приёмо-передатчика (ОПП) РСПИ. От ОПП РСПИ информация о ПЦН выходах передается на центральный приемо-передатчик (ЦПП) РСПИ ПЦО охранной организации. Характер информационного обмена полностью определяется типом и структурой РСПИ.

Выделим семь наиболее используемых отечественных РСПИ: Стрелец-Аргон (ЗАО «Аргус-Спектр», г. С-Петербург www.argus-spectr.ru), Иртыш-3Р (ООО НТК «ИНТЕКС», г. Омск www.intecs.ru), Приток-А- Р (ОБ «СОКРАТ», г. Иркутск www.sokrat.ru), Протон (ООО НПО «ЦЕНТР-ПРОТОН», г. Челябинск www.centerproton.ru), Струна-5 (ЗАО НПФ "Интеграл+" г. Казань www.integralplus.ru), Струна-М, Радиосеть (ООО НПП «АСБ Рекорд», г. Александров www.asbgroup.ru).

Сравнение РСПИ представлено в Приложении 2. В дальнейшем в работе

рассматривается РСПИ «Стрелец-Аргон».

К положительным чертам РСПИ «Стрелец-Аргон» следует отнести:

- шифрование информации;
- автоматическая регулировка мощности ОС;
- индикация качества связи;
- возможность сопряжения с ИСБ «Стрелец-Интеграл»;
- развитые сервисы АРМ РСПИ;
- наличие ретрансляторов в вандалоустойчивом исполнении;
- возможность перехода на резервные частоты.

Для повышения эффективности РСПИ используются ряд технических и организационных мер:

- подбор оптимального частотного диапазона, антенн, мощности передатчика;
- размещение антенн на высоких местах, но эта мера ограничена величиной потерь в кабеле;
- выбор помехоустойчивого вида модуляции и избыточного кодирования полезного сигнала;
- применение разнесенных в пространстве антенн;
- передача сигнала одновременно на двух и более частотах;
- многократное повторение передаваемого сообщения;
- применение ретрансляторов;
- создание топологии сети, где предусмотрены обходные каналы;
- постоянный контроль состояния радиоканала;
- проверка контрольной суммы сообщения;
- криптографическое кодирование (скремблирование) сигнала.

Пункт централизованной охраны (ПЦО)

ПЦО определяется существующими стандартами как совокупность технических средств для приема тревожных извещений о проникновении на охраняемые объекты, служебных и контрольно-диагностических извещений, обработки, отображения, регистрации полученной информации и представления

ее в заданном виде для дальнейшей обработки, а также для передачи команд телеуправления.

Состав оборудования ПЦО зависит от количества и состава требуемых каналов связи, количества АРМов и других факторов.

Общие требования по организации информационного обмена на ПЦО регламентированы в [31 - 34]. Общие требования к автоматизации комплекса ПЦО приведены в [11]. Типовой состав комплекса средств автоматизации ПЦО:

- АРМ администратора;
- АРМ РСПИ (оператора ПЦО);
- АРМ дежурного центра оперативного управления (ЦОУ);
- АРМ инженера ПЦО.

Функции АРМов

- АРМ РСПИ (оператора ПЦО): прием и отображение оперативной информации о тревожных ситуациях на охраняемых объектах, отображение информации о состоянии технических средств КОС ОТС, подготовка оперативной сводки по охраняемым объектам;

- АРМ дежурного ПЦО: прием и отображение тревожных извещений от АРМ РСПИ (операторов ПЦО), отображение информации о состоянии технических средств КОС ОТС, отображение протокола действий операторов ПЦО, отображение и редактирование информации о действиях и местонахождении групп задержания;

- АРМ инженера ПЦО: создание новых и редактирование существующих объектов, подготовка отчетов;

- АРМ администратора: обеспечение разграничения доступа к АРМам ПЦО, их конфигурирование, обеспечение выполнения мероприятий по обслуживанию Сервера БД, создание и редактирование информации из БД.

Передача и обработка информация о состоянии охраны объектов на АРМ РСПИ. Информация о состоянии охраны объектов передается с ЦПП РСПИ на АРМ РСПИ. Далее на АРМ РСПИ происходит анализ информации о состоянии охраны объекта. Производится периодический опрос состояния каждого объекта

с заданным временем опроса и постоянный контроль исправности канала связи с охраняемыми объектами. Автоматически формируются служебные и/или тревожные извещения оператору АРМ ДПУ. Информация передается оператору в виде визуальных и звуковых сообщений. Звук используется для привлечения внимания оператора, а конкретная информация отображается визуально в виде пиктограмм цветом (например, зеленый - норма, желтый-внимание, серый-снятие с охраны и красный - тревожное сообщение). Получив тревожное или служебное сообщение, оператор принимает решение о необходимости передачи сообщения дежурному ПЦО. Служебные сообщения не требуют реагирования наряда физической охраны, а тревожные требуют реагирования. Тревожные сообщения автоматически передаются на АРМ дежурного ПЦО по ЛВС, устно или по телефону. В данной работе рассматривается телефонный канал связи между дежурным ПЦО и оператором АРМ ДПУ.

Передача информации о состоянии охраны объектов оператором АРМ РСПИ дежурному ПЦО. Оператор АРМ РСПИ передает дежурному ПЦО служебную или тревожную информацию о состоянии охраны объектов по телефону. В качестве служебной информации может быть информация о несвоевременном (вне графика) взятии/снятии объекта с охраны, отключении электропитания на объекте и переход на резервное питание, снижение качества радиосвязи с объектом и пр. В качестве тревожных сообщений передается информация о сработавших рубежах охраны. При этом передается карточка объекта из БД ПЦО.

Обработка информации дежурным ПЦО. Получив информацию от ДПУ дежурный ПЦО принимает решение о необходимости направления ГЗ на охраняемый объект. В качестве канала связи дежурного ПЦО с ГЗ, как правило, используется открытый УКВ радиоканал в зоне действия ПЦО. Обычно посылается ГЗ, в зоне действия маршрута которой находится сработавший объект. Если ГЗ уже занята, то посылается ближайшая свободная ГЗ. ГЗ сообщает о начале выполнения отработки объекта. Для контроля действий ГЗ все радио и телефонные переговоры на ПЦО записываются. Кроме того, автотранспорт ГЗ,

как правило, оборудован средствами спутниковой навигации GPS/ГЛОНАСС и информация о местоположении ГЗ передается на ПЦО (у дежурного ПЦО на электронной карте зоны обслуживания ПЦО отслеживается перемещение всех ГЗ).

Группа задержания (ГЗ)

ГЗ является субъективным звеном цепи управления в процессе организации централизованной охраны, и технические характеристики такого звена определяются: должностными обязанностями сотрудников ГЗ; инструкцией по действиям при получении сигнала «Тревога» с охраняемого объекта и инструкциями по охране конкретного объекта. Модель прогнозирования успешности действий нарядов физической охраны по предотвращению несанкционированного доступа нарушителя на охраняемый объект представлена в работе [35].

Прибыв на объект ГЗ докладывает на ПЦО и «отрабатывает» объект, т.е. производит осмотр целостности на предмет обнаружения признаков проникновения. Если они есть, то ГЗ принимает меры по задержанию нарушителя. После повторного взятия объекта под охрану, ГЗ возвращается на свой маршрут.

1.2 Работоспособность телекоммуникационной сети централизованной охраны объектов

Предметом диссертационной работы являются модели и алгоритмы оценки работоспособности ТКС ЦОО.

Под работоспособностью в работе понимается способность ТКС ЦОО обеспечивать выполнение основных функций по передаче и обработке циркулирующей информации в заданном объеме и с необходимым качеством в условиях дестабилизирующих воздействий (ДВ).

В целом, для обеспечения системной работоспособности ТКС ЦОО должна обладать:

1. Способностью предсказывать возможные успешные вторжения – т.е. прогнозировать повышенный риск выхода из строя компонентов системы (как информационных ресурсов). Результатом этого может быть повышение вероятности защиты компонентов и/или устранение структурно-функциональных недостатков (уязвимостей) системы. Для технической реализации данной способности в ТКС ЦОО должны быть предусмотрены средства моделирования и оценки информационной защищенности компонентов от прогнозируемых угроз. В настоящее время существующие ТКС ЦОО такой возможностью не обладают.

2. Способностью поддержания штатных условий функционирования и способностью обнаруживать реализованные атаки и их последствия, как реальный выход из строя (блокирование) компонентов системы. Для технической реализации данной способности в ТКС ЦОО должны быть средства:

- позволяющие отслеживать и регистрировать нежелательные отклонения в работе ее компонентов и уведомлять системных администраторов об этом;

– анализа поведения компонентов ТКС ЦОО – сравнения действий компонентов с шаблонами некорректного использования.

Существуют и другие не менее важные свойства, напрямую влияющие на работоспособность:

3. Способность системы «обучаться», развиваться на основании информации об успешных атаках, возникновении нештатных ситуаций, изменении условий функционирования.

4. Способность к восстановлению - способность системы восстанавливать работоспособность компонентов. Цель этого - построение автоматизированной процедуры возвращения ТКС ЦОО в штатные условия функционирования.

Работоспособность ТКС ЦОО — возможность ТКС выполнять заданные функции ЦОО на заданном уровне эффективности в течение определенного времени.

Неработоспособное состояние ТКС ЦОО (неработоспособность ТКС ЦОО) - состояние ТКС, при котором значение хотя бы одного параметра, характеризующего способность ТКС выполнять заданные функции, не соответствует требованиям технической или нормативно-распорядительной документации.

В общем подходе работоспособность может включать несколько свойств:

1. Защищенность – свойство компонентов ТКС ЦОО, определяющее возможность предотвращать воздействия на них ДВ. Количественно можно оценить вероятностью защищенности компонентов системы от ДВ. Защищенность компонентов в значительной степени зависит от входящих в компоненты ТКС ЦОО средств защиты информации.

2. Способность сохранять выполнение основных функций после получения повреждений компонентов. Количественно можно оценить вероятностью формирования работоспособной структуры системы.

3. Адаптивность – свойство ТКС ЦОО поддерживать выполнение основных функций, используя элементы, не подвергшиеся поражению. Свойство адаптивности обеспечивается наличием внутри системы интеллектуальных механизмов реконфигурации вычислительного процесса обработки информации.

4. Восстанавливаемость – способность ТКС ЦОО восстанавливать состояние выполнения основных функций в течение допустимого по условиям решения задачи времени за счет внутренних ресурсов.

В данной работе делается основной акцент на обеспечение защищенности компонентов ТКС ЦОО, как наиболее принципиального свойства обеспечения ее работоспособности.

Таким образом, будем понимать под работоспособностью ТКС ЦОО информационную защищенность ее компонентов.

Работоспособность ТКС ЦОО зависит от:

1. возникновения и развития ДВ в компонентах ТКС;
2. изменения работоспособного состояния каждого компонента ТКС ЦОО под воздействием ДВ;
3. возможности функционирования работоспособного состояния каждого

компонента и их совокупности.

1.3 Причины снижения работоспособности телекоммуникационной сети централизованной охраны объектов

Большое количество случаев неработоспособности (полной или частичной) компонентов ТКС ЦОО связано с техническими проблемами ЛВС ПЦО:

- использованием в прикладных задачах на АРМах и серверах протоколов Ethernet и TCP/IP (Modbus/TCP, EtherNet/IP, PROFInet и др.), HTTP, SNMP, FTP, DHCP, OPC, DCOM, ActiveX, Java в качестве основных процедур взаимодействия информационных процессов;

- участием в процессе автоматизированной обработки информации персонала различных категорий (различная степень квалификации), их непосредственный и одновременный доступ к системным ресурсам и процессам.

Основная причина снижения работоспособности ТКС ЦОО в диссертации связывается:

- с недостаточной информационной защищенностью и с последствиями информационных атак;

- в саботаже нарушителем аппаратно-программных компонентов ТКС;

- отсутствием должного контроля за действиями персонала ПЦО;

- отсутствием необходимых профессиональных навыков персонала ПЦО.

Атакуемыми компонентами ТКС ЦОО являются, в принципе, все её структурные компоненты. Вывод среды передачи информации из строя обычно расценивается как внешнее воздействие. Возможны физическое разрушение кабелей, постановка шумов в кабеле и в радиотрактах. Узлы коммутации представляют собой инструмент маршрутизации сетевого трафика. Получение доступа к маршрутным таблицам позволяет злоумышленнику изменить путь потока информации. При атаке класса «отказ в сервисе» злоумышленник обычно заставляет узел коммутации либо передавать сообщения по неверному «тупиковому» пути, либо вообще перестать передавать сообщения.

Угрозами безопасности ТКС ЦОО, как уже развернутых, так и создаваемых, могут являться:

1. уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, телекоммуникации и связи;

2. НСД к информации, циркулирующей и хранимой в ТКС ЦОО;

3. противоправные сбор и использование информации, циркулирующей в ТКС ЦОО;

4. нарушение технологии обработки информации;

5. утечка информации по техническим каналам;

6. воздействие на парольно-ключевые средства ТКС ЦОО;

7. внедрение электронных устройств для перехвата информации в технические средства обработки, хранения и передачи информации по каналам связи;

8. компрометация ключей и средств криптографической защиты информации;

9. внедрение вредоносных программ, нарушающих функционирование ТКС ЦОО, программ сбора информации;

10. перехват информации в сетях передачи данных и на линиях связи, навязывание ложной информации;

11. использование несертифицированных по требованиям безопасности информации отечественных и зарубежных средств защиты информации, средств информатизации, телекоммуникации и связи.

1.4 Модели анализа и оценки работоспособности

Функционирование ТКС ЦОО характеризуется:

1. целью;

2. режимами функционирования;

3. множеством функций;

4. множеством компонентов системы, участвующих в реализации функций;

5. множеством информационных процессов.

Цель функционирования ТКС ЦОО - обобщенное понятие, определяемое количеством, качеством и содержанием реализуемых сетью функций во всех режимах ее (сети) функционирования.

В данной работе основной целью ТКС ЦОО является организация защищенного информационного пространства взаимодействия компонентов ТКС ЦОО, обеспечивающая недопущение НСД нарушителя к информационным сетевым процессам, утечку информации по техническим каналам.

Данная цель достигается за счет:

– обеспечения надежности функционирования каналов связи;

–обеспечения конфиденциальности, доступности и целостности информации, обрабатываемой в сети.

Режимами функционирования (РФ) ТКС ЦОО будем называть определяемый в зависимости от обстановки порядок организации деятельности сил и средств, основные мероприятия, проводимые силами и средствами в режиме повседневной деятельности.

При системном подходе РФ - совокупности одновременно выполняемых функций и компонентов системы, участвующих в их реализации.

Выделим некоторые из них, которые в дальнейшем будем называть основными режимами (ОР):

1. $ОР_1$ – «Снят с охраны»;

2. $ОР_2$ - «Охрана»;

3. $ОР_3$ – «Тревога».

Полный перечень ОР приведен в главе 2.

Функциями ТКС ЦОО будем называть устойчивые активные взаимоотношения компонентов - «сетевые сценарии», на базе которых обеспечивается работоспособность режимов функционирования ТКС ЦОО.

Выделим некоторые из них, которые в дальнейшем будем называть основными функциями (ОФ):

1. ОФ1 – «Опрос ОИ по двухпроводной линии»;

2. ОФ2 – «Формирование извещений в адресной линии»;

3. ОФ3 –«Управление оператором АРМ ИСБ состоянием КОС ОТС»;

Полный перечень ОФ приведен в главе 2.

Принадлежности основных функций режимам функционирования задается таблицей 1.1 (ОР↔ОФ).

Таблица 1.1 - Принадлежности основных функций режимам функционирования (ОР↔ОФ)

Основной режим/ Основная функция	$ОР_1$	…	$ОР_a$	…	$ОР_A$
$ОФ_1$	$\delta(1,1)$		$\delta(a,1)$		$\delta(A,1)$
…	…		…		
$ОФ_b$	$\delta(1,b)$		$\delta(a,b)$		$\delta(A,b)$
…			…		…
$ОФ_B$	$\delta(1,B)$		$\delta(a,B)$		$\delta(A,B)$

$\delta(a,b) = 1$ $(a = 1,\dots,A; b = 1,\dots,B)$, если b-я ОФ «присутствует» в a-м режиме, иначе $\delta(a,b) = 0$.

Информационные процессы (ИП)ТКС ЦОО - процессы получения, создания, сбора, обработки, накопления, хранения, распространения и использования информации.

Пуск функции на исполнение сопровождается инициированием одного или нескольких информационных процессов. ИП «связывает» компоненты ТКС, образуя временно устойчивые совокупности обменов информацией между компонентами. Выделим некоторые ИП:

1. $ИП_1$ – «Опрос охранных извещателей».
2. $ИП_2$ – «Анализ информации на АРМ ИСБ».

3. $ИП_3$ – «Активация ПЦН выходов для ОПП РСПИ».

Полный перечень ИП приведен в главе 2.

Принадлежности информационных процессов основным функциям (для всех основных режимов) задается таблицей 1.2 (ОФ↔ИП).

Таблица 1.2 - Принадлежности информационных процессов основным функциям (ОФ↔ИП)

Информационный процесс/ Основная функция	$ИП_1$		$ИП_c$	…	$ИП_C$
$ОФ_1$	$\zeta(1,1)$		$\zeta(c,1)$		$\zeta(C,1)$
…	…		…		
$ОФ_b$	$\zeta(1,b)$		$\zeta(c,b)$		$\zeta(C,b)$
…			…		…
$ОФ_B$	$\zeta(1,B)$		$\zeta(c,B)$		$\zeta(C,B)$

$\zeta(c,b) = 1$ $(c = 1,\dots,C; b = 1,\dots,B)$, если c-й ИП «присутствует» в b-й ОФ, иначе $\zeta(a,b) = 0$.

Компоненты ТКС ЦОО описаны в разделе 1.1. Принадлежности компонентов информационным процессам (КОМ↔ИП) задается таблицей 1.3

Таблица 1.3 - Принадлежности компонентов информационным процессам (КОМ↔ИП)

Информационный процесс/ Компоненты	$ИП_1$	…	$ИП_c$	…	$ИП_C$
$КОМ_1$	$\eta(1,1)$		$\eta(c,1)$		$\eta(C,1)$
…	…		…		
$КОМ_d$	$\eta(1,d)$		$\eta(c,d)$		$\eta(C,d)$
…			…		…
$КОМ_D$	$\eta(1,D)$		$\eta(c,D)$		$\eta(C,D)$

$\eta(c,d)=1$ $(c=1,\dots,C; d=1,\dots,D)$, если d-й компонент «присутствует» в c-ом ИП, иначе $\eta(a,b)=0$.

Будем считать, что;

- работоспособность ТКС ЦОО обеспечивается, если ТКС ЦОО работоспособна во всех режимах ее функционирования;

- работоспособность ТКС ЦОО в конкретном режиме функционирования обеспечивается, если работоспособны все основные функции, участвующие в обеспечении данного режима;

- работоспособность основной функции ТКС ЦОО обеспечивается, если защищены все информационные процессы, участвующие в обеспечении данной функции;

- защищённость информационного процесса обеспечивается, если обеспечен требуемый уровень информационной безопасности реализующих ИП компонентов ТКС ЦОО.

Введем следующие обозначения:

- показатель работоспособности (ПР) ТКС ЦОО

$$\text{ПР}_{\text{ТКС}}=\{\text{ПР}_{\text{ТКС}}(\text{ОР}_1),\dots,\text{ПР}_{\text{ТКС}}(\text{ОР}_a),\dots,\text{ПР}_{\text{ТКС}}(\text{ОР}_A)\}, \quad (1.1)$$

здесь $\text{ПР}_{\text{ТКС}}(\text{ОР}_a)$ - показатель работоспособности ТКС ЦОО, функционирующей в a-ом основном режиме $(a=1,\dots,A)$;

- показатель работоспособности ТКС ЦОО, функционирующей в a-ом основном режиме

$$\text{ПР}_{\text{ТКС}}\ (\text{ОР}_a)=\left\{\text{ПР}(\text{ОФ}_1^a),\ \text{ПР}(\text{ОФ}_2^a),\dots,\ \text{ПР}\left(\text{ОФ}_{B_a}^a\right)\right\}, \quad (1.2)$$

где $\text{ПР}(\text{ОФ}_b^a)$ - показатель работоспособности b-й основной функции, обеспечивающей a-й ОР $(b=1,\dots,B_a)$;

- показатель работоспособности b-й основной функции, обеспечивающей a-й ОР

$$\text{ПР}(\text{ОФ}_b^a)=\left\{\text{ПЗ}\left(\text{ИП}_1^{b,a}\right),\text{ПЗ}\left(\text{ИП}_2^{b,a}\right),\dots,\text{ПЗ}\left(\text{ИП}_{C_{b,a}}^{b,a}\right)\right\}, \quad (1.3)$$

где $\text{ПЗ}\left(\text{ИП}_c^{b,a}\right)$ - показатель защищенности c-го информационного процесса, участвующего в обеспечении b-й основной функции a-го основного режима ($c = 1, \dots, C_{b,a}$). Если воспользоваться одним показателем – то это может быть минимальный показатель защищенности из всех $\text{ИП}_c^{b,a}$ («слабое звено»): $\text{ПР}(\text{ОФ}_b^a) = \min\limits_{C_{b,a}} \left\{\text{ПЗ}\left(\text{ИП}_1^{b,a}\right), \dots, \text{ПЗ}\left(\text{ИП}_{C_{b,a}}^{b,a}\right)\right\}$;

- показатель защищенности c-го ИП, участвующего в обеспечении b-й ОФ a-го ОР

$$\text{ПЗ}\left(\text{ИП}_c^{b,a}\right) = \left\{\text{ПЗ}\left(\text{КОМ}_1^{c,b,a}\right), \dots, \text{ПЗ}\left(\text{КОМ}_{D_{c,b,a}}^{c,b,a}\right)\right\}, \quad (1.4)$$

где $\text{ПЗ}\left(\text{КОМ}_d^{c,b,a}\right)$ - показатель защищенности d-го компонента ТКС ЦОО реализующего c-й информационный процесс b-й основной функции a-го ОР ($d = 1, \dots, D_{c,b,a}$). Если воспользоваться одним показателем – то это может быть минимальный показатель защищенности из всех $\text{КОМ}_d^{c,b,a}$ («слабое звено»): $\text{ПЗ}\left(\text{ИП}_c^{b,a}\right) = \min\limits_{D_{c,b,a}} \left\{\text{ПЗ}\left(\text{КОМ}_1^{c,b,a}\right), \dots, \text{ПЗ}\left(\text{КОМ}_{D_{c,b,a}}^{c,b,a}\right)\right\}$.

В дальнейшем под показателем защищенности d-го компонента ТКС ЦОО, участвующего в c-м ИП b-й ОФ a-го ОР будем понимать вероятность $p_d^{c,b,a}$ того, что обеспечен требуемый (рабочей документацией) уровень информационной безопасности.

Тогда

$$\text{ПЗ}\left(\text{ИП}_c^{b,a}\right) = \left\{p_1^{c,b,a}, \dots, p_{D_{c,b,a}}^{c,b,a}\right\}. \quad (1.5)$$

1.5. Алгоритм определения вероятности защищенности компонента ТКС ЦОО

Моделирование процесса защиты информации представляет собой сложную задачу, для решения которой могут быть применены неформальные методы сведения сложной задачи к формальному описанию с последующим её решением формальными методами. В настоящее время известны подходы к

моделированию процессов защиты информации, использующие теорию вероятностей, теорию нечетких множеств, теорию игр, теорию графов.

Вопросам моделирования состояния защиты объектов в системах ЦОО посвящены работы [1-4]. Вопросам использования экспертных оценок в задачах информационной безопасности посвящены работы [5, 6].

Чтобы количественно оценить уровень защищенности информационных ресурсов, необходимо выбрать базовую модель описания процесса защиты информации. В качестве такой многими исследователями перспективной считается модель безопасности с полным перекрытием, разработанная Хоффманом. В модели Хоффмана описывается взаимодействие «области угроз», «защищаемых объектов» и «системы защиты» (защитных механизмов).

Поскольку воздействие на компоненты ТКС ЦОО различных ДВ в значительной мере является случайным, то в качестве количественной меры безопасности целесообразно принять вероятность защищенности.

Основными параметрами модели являются:

- множество угроз (УГ) d-му компоненту ($\text{УГ}^d = \{\text{УГ}^d{}_1, \dots, \text{УГ}^d{}_g, \dots, \text{УГ}^d{}_{G_d}\}$), которые потенциально могут проявиться в рассматриваемый период времени;

- множество уязвимостей (У), выявленных в d-м компоненте ($\text{У}^d = \{\text{У}^d{}_1, \dots, \text{У}^d{}_f, \dots, \text{У}^d{}_{F_d}\}$);

- множество защитных механизмов (ЗМ) d-го компонента ($\text{ЗМ}^d = \{\text{ЗМ}^d{}_1, \dots, \text{ЗМ}^d{}_h, \dots, \text{ЗМ}^d{}_{H_d}\}$;

- матрица «угроза-уязвимость» $\text{УГ}^d/\text{У}^d = \|\lambda^d(g,f)\|, g = 1, \dots, G_d;\ f = 1, \dots, F_d,\quad 0 \le \lambda^d(g,f) \le 1$. Физический смысл $\text{УГ}^d/\text{У}^d$ - вероятность (эффективность) эксплуатации g-й угрозой f-й уязвимости;

- матрица «угроза-защитный механизм» $\text{УГ}^d/\text{ЗМ}^d = \|\mu^d(g,h)\|,\ g = 1, \dots, G_d;\ \ h = 1, \dots, H_d.\ \ 0 \le \mu^d(g,h) \le 1$. Физический смысл $\text{УГ}^d/\text{ЗМ}^d$ - «степень сопротивляемости» g -го ЗМ h -й угрозе (коэффициент силы h-го ЗМ). Если $\mu^d(g,h) = 1$, то g -я угроза перекрывается полностью.

Примем следующие уточнения и допущения модели:

1. Множество угроз формируется с использованием модели возможного нарушителя. Каждый нарушитель стремится угрожать всем компонентам, генерируя в соответствии со своей квалификацией угрозы конфиденциальности, целостности и доступности.

2. Множество угроз формируется на основе множества дестабилизирующих факторов $ДФ = \{ДФ_1, \dots, ДФ_e, \dots, ДФ_E\}$ и множества уязвимостей.

3. Каждая угроза характеризуется «степенью опасности» для работоспособности основного режима.

4. Один и тот же защитный механизм может перекрывать (защищать) одну или более одной угрозы. При этом степень эффективности защитного механизма неодинакова по отношению к различным угрозам.

Приведем порядок определения вероятности защищенности d-го компонента ТКС от g-й угрозы в виде алгоритма

Алгоритм определения вероятности защищенности компонента ТКС ЦОО от угрозы

Алгоритм 1.1

Шаг 1. Рассчитаем вероятность того, что g-я угроза «найдет» хотя бы одну из F_d уязвимостей

$$p^d(g,f) = 1 - \frac{\sum_{f=1}^{F_d}(1-\hat{\lambda}^d(g,f))}{F_d}. \quad (1.6)$$

Шаг 2. Рассчитаем вероятность «непрохождения» g -й угрозы через все H защитные механизмы компонента

$$p^d(g,h) = 1 - \frac{\sum_{h=1}^{H_d}(1-\hat{\mu}^d(g,h))}{H_d}. \quad (1.7)$$

Шаг 3. Рассчитаем показатель защищенности от k-й угрозы

$$p^d(g) = 1 - (p^d(g,f) \times (1 - p^d(g,h))). \quad (1.8)$$

В результате прохождения данного алгоритма для d-го компонента ТКС по

всем угрозам одного критерия (конфиденциальность, целостность, доступность) имеем вектор защищенности: $УГ^d{}_1, \dots, УГ^d{}_g, \dots, УГ^d{}_{G_d}$

	$УГ^d{}_1$	$УГ^d{}_2$	…	$УГ^d{}_g\dots$	$УГ^d{}_{G_d}$
$p^d(g)$	$p^d(1)$	$p^d(2)$	…	…	$p^d(G_d)$

Шаг 4. Если нужен один показатель – то это может быть минимальный показатель защищенности из всех («слабое звено»).

$$p^d = \min_{G_d}\{p^d(1), \dots, p^d(G_d)\}. \quad (1.9)$$

Конец алгоритма.

Достоинства предлагаемого подхода:

1. Наглядность. Сразу видна «недозащищенность» конкретного компонента с информационным ресурсом и самая «серьезная» угроза. Несложно формируется ранжированный список угроз, слабозащищенных компонентов, нарушителей. Это необходимо для выработки конкретных рекомендаций по повышению защищенности.

2. Повышение точности расчета за счет учета появления конкретных информационных ресурсов в разных компонентах со своими специфическими угрозами, уязвимостями, защитными механизмами

3. Простота автоматизации расчетов.

Выделим определенный недостаток модели. При анализе необходимо в качестве исходных иметь полные множества типов нарушителей, угроз, защитных механизмов и уязвимостей, а также матрицы «тип нарушителя - угроза» (показатель эффективности определенного типа нарушителя создавать ту или иную угрозу), «угроза - уязвимость» (насколько эффективно конкретная угроза может «проникать» через ту или иную уязвимость) и «угроза – защитный механизм» (насколько конкретный защитный механизм «ослабляет» ту или иную угрозу). Такие показатели могут быть получены только экспертным путем и будут отражать определенную долю субъективизма оценки.

1.6. Модель оценки работоспособности ТКС ЦОО на основе анализа ее инфраструктуры

Модель оценки работоспособности ТКС ЦОО на основе анализа ее инфраструктуры представим в виде алгоритма.

Прогнозная модель. Дает ответ на вопрос: если с определенной вероятностью будут совершены атаки известными угрозами, то будут ли компоненты адекватно защищены. В данной модели исходят из того, что в течении времени оценки ни множество угроз, ни уязвимости, ни ЗМ не меняются. Показатель работоспособности оценивается уровнем (вероятностью) защищенности компонентов ТКС ЦОО, используемых при реализации информационных процессов, задействованных в реализациях основных функций ОР.

Модель оценки работоспособности ТКС ЦОО на основе анализа ее инфраструктуры

Алгоритм 1.2

Шаг 1. $a = 1$. Начинаем с первого ОР.

Шаг 2. Сформировать множества:

- $\text{ОФ}^a = \left\{\text{ОФ}_1^a, \dots, \text{ОФ}_b^a, \dots , \ \text{ОФ}_{B_a}^a\right\}$, используя таблицу 1.1 (ОР↔ОФ);

- $\text{ИП}^{b,a} = \left\{\text{ИП}_1^{b,a}, \dots, \text{ИП}_c^{b,a}, \dots, \text{ИП}_{C_{b,a}}^{b,a}\right\}$ для всех $\text{ОФ}_b^a \quad b = 1, \dots, B_a$, используя таблицу 1.2 (ОФ↔ИП);

- $\text{КОМ}^{c,b,a} = \left\{\text{КОМ}_1^{c,b,a}, \dots, \text{КОМ}_d^{c,b,a}, \dots, \text{КОМ}_{D_{c,b,a}}^{c,b,a}\right\}$, для всех $\text{ИП}_c^{b,a} \quad c = 1, \dots, C_{b,a}$, используя таблицу 1.3 (ИП ↔ КОМ).

Шаг 3. $b = 1$. С первой ОФ режима.

Шаг 4. $\text{c} = 1$. С первого ИП функции. $\text{ПР}(\text{ОФ}_b^a) = 1$.

Шаг 5. $d = 1$. С первого компонента ИП. $\text{ПЗ}\left(\text{ИП}_c^{b,a}\right) = 1$.

Шаг 6. Выполнить действия алгоритма 1.1; $p_d^{c,b,a} = p^d$; Если $p_d^{c,b,a} < \text{ПЗ}\left(\text{ИП}_c^{b,a}\right)$ то $\text{ПЗ}\left(\text{ИП}_c^{b,a}\right) = p_d^{c,b,a}$. Если $d < D_{c,b,a}$, то $d = d + 1$, перейти к шагу 6.

Шаг 7. Если $\text{ПЗ}\left(\text{ИП}_c^{b,a}\right) < \text{ПР}(\text{ОФ}_b^a)$, то $\text{ПР}(\text{ОФ}_b^a) = \text{ПЗ}\left(\text{ИП}_c^{b,a}\right)$. Если $c < C_{b,a}$, то $c = c + 1$, перейти к шагу 5.

Шаг 8. $\text{ПР}_{\text{ТКС}}(\text{ОР}_a) = \left\{\text{ПР}(\text{ОФ}_1^a),\ \text{ПР}(\text{ОФ}_2^a), \dots,\ \text{ПР}\left(\text{ОФ}_{B_a}^a\right)\right\}$. Если $b < B_a$, то $b = b + 1$, перейти к шагу 4.

Шаг 9. Если $a \le A$, то $a = a + 1$, перейти к шагу 2. Иначе

$\text{ПР}_{\text{ТКС}} = \{\text{ПР}_{\text{ТКС}}(\text{ОР}_1), \dots, \text{ПР}_{\text{ТКС}}(\text{ОР}_a), \dots, \text{ПР}_{\text{ТКС}}(\text{ОР}_A)\}$, конец алгоритма.

1.7. Уточнение задачи исследования

В соответствии с рассмотренным подходом, перечислим основные задачи, требующие решения для достижения цели, поставленной в диссертации:

1. Формирование ограничений и допущений при описании ТКС ЦОО и телекоммуникационных процессов в ней.

2. Разработать базы данных:

- угроз конфиденциальности, доступности и целостности компонентов (как информационных ресурсов) ТКС ЦОО;

- структурно-функциональных недостатков (уязвимостей) компонентов ТКС ЦОО;

- защитных механизмов обеспечения информационной безопасности информационных ресурсов и процессов в ТКС ЦОО.

3. Разработать модель нарушителя информационной безопасности в ТКС ЦОО.

4. Сформировать матрицы:

- вероятности (эффективности) эксплуатации угрозами уязвимостей компонентов ТКС ЦОО;

- вероятности эффективности использования защитных механизмов компонентов ТКС ЦОО угрозам.

5. Разработать методику проведения аудита работоспособности ТКС ЦОО и показать ее адекватность на практике.

Выводы к главе 1

Под работоспособностью понимается способность ТКС ЦОО обеспечивать выполнение основных функций по передаче и обработке циркулирующей информации в заданном объеме и с необходимым качеством в условиях дестабилизирующих воздействий.

Основная причина снижения работоспособности ТКС ЦОО связывается с недостаточной информационной защищенностью, недостатками в работе с персоналом ПЦО, и с последствиями деструктивных воздействий нарушителей.

Для решения задач контроля процессов обеспечения работоспособности ТКС ЦОО построена концептуальная модель, составляющими элементами которой являются цели функционирования, основные режимы и функции, а также информационные процессы, связывающие компоненты ТКС ЦОО, участвующие в реализации функций.

Предложена формальная модель показателя работоспособности как функции вероятностей защищенности компонентов ТКС ЦОО от множества угроз при реализации информационных процессов основных функций, определяемых режимами. Сформулирована и формализована концепция модели оценки работоспособности на основе анализа инфраструктуры ТКС ЦОО.

Разработан алгоритм оценки вероятности информационной защищенности компонента ТКС ЦОО, основанный на модели безопасности с полным перекрытием Хоффмана, позволяющий анализировать состояние компонента в условиях множества угроз, уязвимостей и защитных механизмов.

Глава 2. РАЗРАБОТКА СРЕДСТВ МОДЕЛИРОВАНИЯ ПРОЦЕССОВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ТКС ЦОО

Моделирование процессов обеспечения информационной безопасности в ТКС принято связывать с параметрами уязвимостей, угроз, защитных механизмов, типом (моделью) нарушителя.

В главе формируются множества компонентов ТКС ЦОО, информационных процессов, объединяющих компоненты в устойчивые совокупности, обобщенных функций и режимов функционирования. Разрабатываются соответствующие матрицы специального вида, связывающие элементы выделенных множеств. Синтезируются таблицы угроз, уязвимостей и защитных механизмов типовой ТКС ЦОО. Предлагаются методики оценки показателей эффективности эксплуатации уязвимостей для реализации угроз, опасности угроз по последствиям их реализации с учетом ЗМ, вероятности посягательства с целью реализации угроз и возможности нарушителя по реализации угроз.

Уточняется модель определения вероятности защищенности компонента ТКС ЦОО.

2.1 Декомпозиция элементов модели ТКС ЦОО

Используя объектно-ориентированный подход, выполним декомпозицию типовой (базовой) структуры ТКС ЦОО с выделением следующих элементов (сущностей):

- компоненты ТКС ЦОО ($КОМ_d$);

- информационные процессы , объединяющих компоненты в устойчивые совокупности - $ИП_c$;

- множество обобщенных функций ТКС ЦОО ($0Ф_b$);

- множество основных режимов функционирования ($0Р_a$) ТКС ЦОО.

Моделирование процессов обеспечения информационной безопасности в

ТКС принято связывать с параметрами дестабилизирующих факторов, уязвимостей, угроз, защитных механизмов, типом (моделью) нарушителя.

Под дестабилизирующим фактором будем понимать объективное, текущее состояние среды функционирования ТКС ЦОО, способствующее формированию уязвимостей. Таким образом, дестабилизирующий фактор - свойство внешней среды, а уязвимости - свойство структурных элементов ТКС ЦОО.

Остальные термины описания состояния информационной безопасности ТКС ЦОО соответствуют общепринятым стандартам [43]. Характер защищенности информационных ресурсов (ИР) в ТКС ЦОО описаны в данной работе как свойства целостности, конфиденциальности и доступности по каждому из информационных процессов.

Составим полные перечни КОМ_d; ИП_c; ОФ_b; ОР_a ТКС ЦОО.

КОМ_d :

d=1 (ОИ, КДЛ);

d=2 (ПК, ПИ, АРМ ИСБ);

d=3 (Оператор АРМ ИСБ и РМ);

d=4 (ОПП РСПИ);

d=5 (Радиоканал РСПИ);

d=6 (ЦПП РСПИ);

d=7 (ЛВС, множество АРМ РСПИ; АРМ дежурного ПЦО, Сервер БД, АРМ инженера ПЦО);

d=8 (оператор АРМ РСПИ, АТС и телефонные аппараты для связи операторов АРМ РСПИ и дежурного ПЦО);

d=9 (Дежурный ПЦО);

d=10 (УКВ радиостанции дежурного ПЦО для связи с нарядами ГЗ);

d=11 (Мобильные наряды ГЗ).

Следует иметь в виду, что ТКС ЦОО представляет собой множество охраняемых объектов, множество АРМ РСПИ на ПЦО и множество ГЗ. Предметом исследования в данной работе являются именно информационные процессы в

ТКС ЦОО. Информационный обмен для структурных элементов ТКС ЦОО представляет собой цикл управления из 8 информационных процессов.

Краткое описание информационных процессов между структурными элементами ТКС ЦОО:

$ИП_1$. «Опрос охранных извещателей». ОИ в составе КОС ОТС на объекте передают информацию о своем состоянии по двухпроводной адресной линии через КДЛ на АРМ ИСБ.

$ИП_2$. «Анализ информации на АРМ ИСБ». На АРМ ИСБ анализируется и обобщается информация от контролируемых извещателей и автоматически формируются служебные и/или тревожные извещения. Данные извещения органолептически (визуальными и звуковыми сообщениями) передаются оператору ИСБ и на ПЦО. В программном обеспечении АРМ ИСБ заложены готовые сценарии формирования тревожных извещений, которые активируются при срабатывании контролируемых ОИ.

$ИП_3$. «Активация ПЦН выходов для ОПП РСПИ». Тревожные извещения от АРМ ИСБ на ПЦО передаются посредством активации реле РМ, которые формируют «ПЦН выходы» по рубежам охраны на ПЦО с охраняемого объекта.

$ИП_4$. «Передача информации от ОПП РСПИ на ПЦО». Выходы реле подключаются ко входам ОПП РСПИ, которые контролируют ПЦН выходы по рубежам охраны и передают на ПЦО по радиоканалу информацию как о состоянии контролируемых реле (тревоги), так и служебную информацию о состоянии ОПП РСПИ.

$ИП_5$. «Анализ информации на АРМ РСПИ». Информация о состоянии охраны от всех объектов централизованно поступает на ПЦО по РСПИ. Далее информация по ЛВС поступает на АРМ РСПИ, где происходит ее анализ и обобщение. ПО АРМ РСПИ автоматически формирует служебные и/или тревожные извещения оператору АРМ ДПУ, которые передается оператору ДПУ органолептически (аналогично АРМ ИСБ), в виде визуальных и звуковых сообщений.

$ИП_6$. «Передача информации от оператора АРМ РСПИ дежурному ПЦО». Оператор АРМ РСПИ, получив тревожную или важную служебную информацию, передает ее дежурному ПЦО по телефону.

$ИП_7$. «Передача тревог от дежурного ПЦО наряду ГЗ». Дежурный ПЦО анализирует полученную информацию, анализирует складывающуюся оперативную обстановку, дислокацию нарядов и принимает решение о направлении группы физического реагирования (группы задержания - ГЗ) на охраняемый объект. Информацию ГЗ передается по УКВ каналу связи в зоне действия ПЦО. При этом все радиопереговоры и телефоны на ПЦО записываются средствами аудиозаписи. Кроме того, автотранспорт наряда охраны оснащен средствами спутниковой навигации с передачей информации по связному УКВ каналу и дежурный ПЦО на электронной карте контролирует местоположение ГЗ.

$ИП_8$. «Информационный обмен ГЗ с дежурным ПЦО при отработке объекта». Получив информацию от дежурного ПЦО наряд физической охраны (ГЗ) на автотранспорте за минимально возможное время прибывает на охраняемый объект, с которого получено тревожное извещение и проводит комплекс мероприятий (блокирует и «отрабатывает» объект). ГЗ проводит осмотр целостности объекта на предмет обнаружения видимых признаков проникновения. Далее происходит либо задержание нарушителя, либо предотвращение проникновения, либо (при ложном срабатывании ТСО) вызов собственника объекта, его «зачистка» (осмотр всех помещений) и повторное взятие под охрану на ПЦО. После обработки объекта наряд возвращается на маршрут следования. Во время «отработки» объекта наряд докладывает о прибытии, результатах осмотра и др. информацию дежурному ПЦО, а также получает указания от него по связному УКВ каналу.

Множеством функций ТКС ЦОО будем называть типовые «сценарии» по сбору, обработке и передаче информации между структурными элементами в модулях. Выделим некоторые из них, которые в дальнейшем будем называть основными $ОФ_b$:

ОФ1 – «Опрос ОИ по двухпроводной линии». Происходит опрос ОИ по двухпроводной линии связи на объекте;

ОФ2 – «Формирование извещений в адресной линии». Формирование служебных и тревожных извещений о состоянии ОИ и целостности элементов строительных конструкций оператору АРМ ИСБ и активации «ПЦН выходов» РМ;

ОФ3 –«Управление оператором АРМ ИСБ состоянием КОС ОТС». Управление оператором АРМ ИСБ состоянием ОИ на объекте и передача служебных и тревожных извещений по радиоканалу РСПИ на ПЦО (ручной режим управления осуществляется в соответствии с полномочиями оператора АРМ ИСБ);

ОФ4 – «Контроль канала связи РСПИ». Передача тестовых сигналов контроля канала РСПИ на ОПП РСПИ;

ОФ5 – «Передача тревог от КОС ОТС на ПЦО по каналу РСПИ». Передача служебных и тревожных извещений по радиоканалу РСПИ на ПЦО.

ОФ6 – «Прием информации ЦПП РСПИ от ОПП РСПИ». Прием базовой станцией (ЦПП) РСПИ на ПЦО тестовых сигналов контроля канала, служебных и тревожных извещений от ОПП РСПИ и дальнейшая передача информации на АРМ РСПИ.

ОФ7 – «Обработка информации на АРМ РСПИ». Обработка информации о состоянии связи, служебных и тревожных извещений от ОПП РСПИ на АРМ РСПИ и формирование органолептических (визуальных и звуковых) сообщений оператору АРМ РСПИ.

ОФ8 – «Обработка информации и принятие решений оператором АРМ РСПИ». Обработка информации оператором АРМ РСПИ и принятие решения (сброс тревоги, постановка на контроль до определенного события с последующим принятием решения, ожидание истечения времени задержки для последующего принятия решения, передача информации дежурному ПЦО для реагирования);

ОФ9 – «Информационный обмен оператора РСПИ и дежурного ПЦО, принятие решений дежурным ПЦО». Передача тревожной или служебной информации о состоянии объекта дежурному ПЦО по телефону (или устно) для принятия

решения (реагирование (выбор группы реагирования), сброс тревоги, постановка на контроль до определенного события с последующим принятием решения, ожидание истечения времени задержки для последующего принятия решения и т.д.);

ОФ10 – «Передача тревог дежурным ПЦО наряду ГЗ». Передача информации дежурным ПЦО по УКВ каналу радиостанции ГЗ для реагирования на служебные и тревожные извещения от охраняемого объекта.

ОФ11 – «Следование ГЗ на охраняемый объект». Получение ГЗ по УКВ каналу радиостанции служебных и тревожных сообщений и дополнительной информации от дежурного ПЦО. Следование кратчайшим путем к охраняемому объекту, доклад о прибытии на охраняемый объект.

ОФ12 – «Отработка сработавшего охраняемого объекта». Блокирование охраняемого объекта ГЗ, осмотр объекта на предмет выявления несанкционированного проникновения. Доклад о результатах дежурному ПЦО;

ОФ13 – «Задержание нарушителя». Принятие мер к задержанию нарушителя (в случае выявления НСД и выполнение указаний дежурного ПЦО);

ОФ14 – «Выявление причин срабатывания КОС ОТС». Выявление причин срабатывания, вызов собственника объекта (при необходимости), зачистка и взятие под охрану (перезакрытие) объекта;

ОФ15 – «Физическая охрана объекта». Физическая охрана объекта до прибытия собственника или окончания охраняемого времени;

В процессе функционирования ТКС ЦОО можно также выделить множество режимов функционирования ТКС как совокупности одновременно выполняемых функций. Основные режимы (ОР) функционирования ТКС ЦОО:

ОР1 – Режим «Снят с охраны», объект снят с охраны (не охраняемое время);

ОР2 – Режим «Охрана», объект находится под централизованной охраной (охраняемое время);

ОР3 – Режим «Тревога», объект находится в режиме «сработки» (осуществляется реагирование наряда физической охраны на охраняемый объект, происходит «отработка» объекта);

ОР4 – Режим «Не взятие», объект находится в состоянии «Не взятия», когда невозможно принять под централизованную охрану в охраняемое время ввиду аварии (неисправности) канала связи или средств ТСО на объекте;

ОР5 – Режим «Состояние контроля», объект находится в состоянии особого контроля (наблюдения) под охраной. Например, поступило служебное извещение об отказе резервного канала связи, основного питания и прочее, т.е. объект находится под централизованной охраной, но имеются неисправности или осложнения в тактике его охраны;

ОР6 – Режим «Перезакрытие», объект находится в состоянии «перезакрытия» после срабатывания (когда вызывается собственник объекта для «зачистки» и повторного взятия под охрану). Иногда такой режим требует длительного времени, когда ГЗ остается задействованной на объекте и не может убыть на маршрут;

ОР7 – Режим «Физическая охрана», объект не может быть взят под централизованную охрану по техническим или другим причинам, и охраняется специально выставленным постом физической охраной (или постоянным объездом ГЗ). Применяется для особо важных или опасных объектов.

Матрица специального вида, связывающая структурные компоненты, информационные процессы, обобщенные функции и режимы функционирования ТКС ЦОО составлена на основании анализа результатов экспертного опроса 15 специалистов вневедомственной охраны Росгвардии России. Матрица представлена таблицей 2.1. В ней указаны номера структурных компонентов ТКС ЦОО, задействованных в ИП, номера ИП участвующих в ОФ и номера ОФ, входящих в ОР.

Таблица 2.1 - Матрица специального вида, связывающая структурные компоненты, информационные процессы, обобщенные функции и режимы функционирования ТКС ЦОО

Основной режим $ОР_a$ a=1..7 / Обобщенная функция b=1..15	Обобщенная функция $ОФ_b$ b=1..15 / Информационный процесс $ИП_c$ c=1..8	Информационный процесс $ИП_c$ c=1..8 / Структурные компоненты $КОМ_d$ d=1..11
1 / 1,2	1 / 1	1 / 1
2 / 1÷7	2 / 2	2 / 2,3
3 / 6÷14	3 / 2÷4	3 / 2,3
4 / 1÷7	4 / 4	4 / 4,5,6
5 / 1÷8	5 / 4	5 / 6,7
6 / 6÷10,14	6 / 5	6 / 8,9
7 / 15	7 / 5	7 / 9,10,11
	8 / 5,6	8 / 10,11
	9 / 6	
	10 / 7	
	11 / 8	
	12 / 8	
	13 / 8	
	14 / 8	
	15 / 8	

На рис.2.1 графически изображены связи структурных элементов рассматриваемой модели ТКС ЦОО.

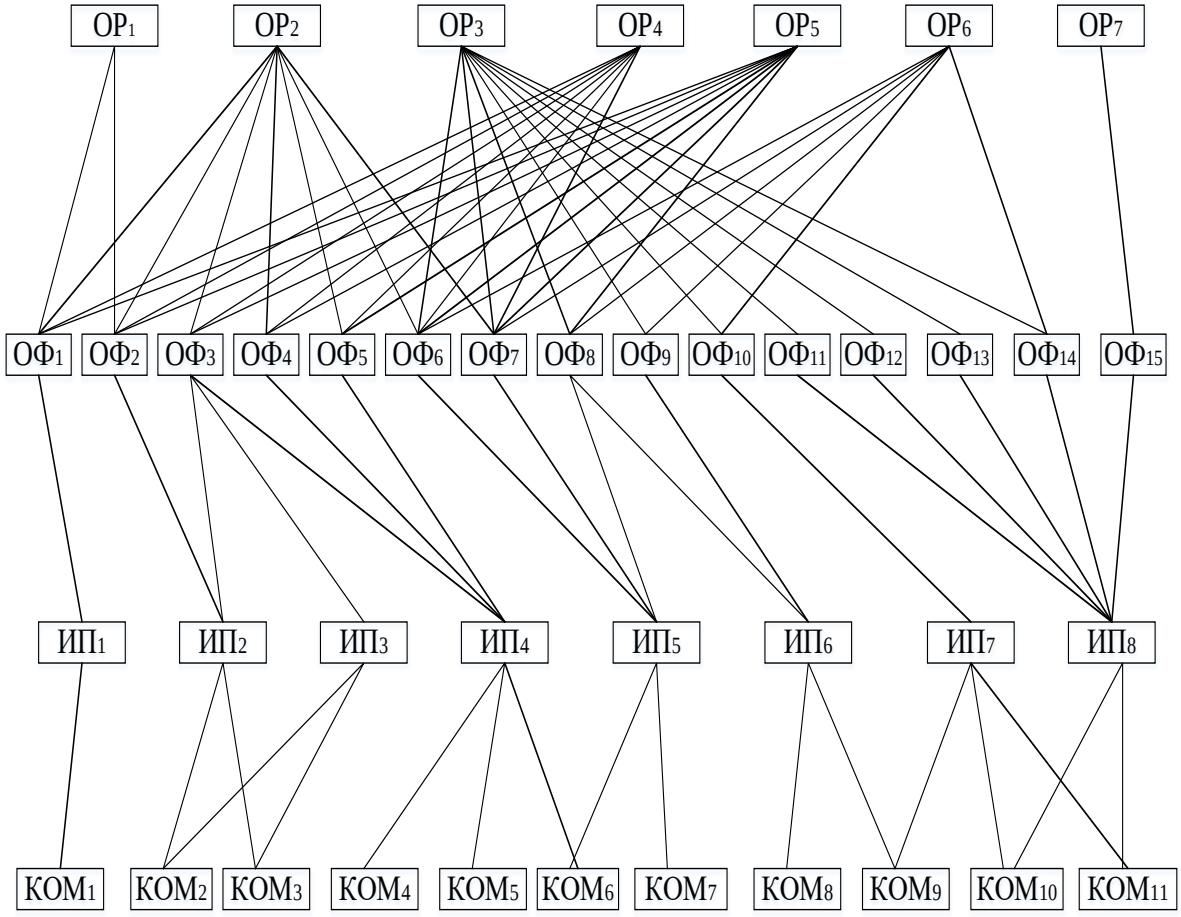

Рисунок 2.1 - Связи структурных элементов рассматриваемой модели ТКС ЦОО.

2.2 Ограничения и допущения модели ТКС ЦОО

При описании ТКС ЦОО и информационных процессов в ней в связи со слишком большой номенклатурой оборудования, разнообразием нормативно-регламентирующей базы, топологии и способов тактики охраны объектов, необходимо принять некоторые ограничения и допущения для того, чтобы четко обозначить рассматриваемую предметную область. Опишем ограничения и допущения ТКС ЦОО:

- КОС ОТС рассматривается только как ИСБ проводного типа («Орион-Про» или «Рубеж-08») с использованием двухпроводной адресной линией (двухпроводной линией связи – ДПЛС);

- работа КОС ОТС рассматривается в дежурном режиме без их саботажа со стороны нарушителей, но возможности саботажа учитываются при анализе угроз и уязвимостей структурных элементов КОС ОТС;

- рассматриваются только типовые структуры построения объектовых ОТС;

- дестабилизирующие факторы, оказывающие влияние на работу ОИ учитываются при анализе уязвимостей ОТС;

- происшествия и чрезвычайные ситуации, складывающиеся на защищаемом объекте, не рассматриваются.

- рассматривается только радиоканальная РСПИ «Стрелец-Аргон»;

- работа ОПП РСПИ рассматривается в дежурном режиме без саботажа со стороны нарушителей, и в благоприятной электромагнитной обстановке с «хорошей» оценкой качества прохождения сигналов. При этом возможности саботажа учитываются при анализе уязвимостей канала РСПИ;

- рассматривается только типовая структура включения ОПП (на примере ОПП РСПИ «Аргон»);

- правильность монтажа и влияние качества эксплуатации РСПИ не рассматриваются, но учитываются при анализе уязвимостей при передаче информации по РСПИ;

- происшествия и чрезвычайные ситуации, складывающиеся на защищаемом объекте и влияющие на передачу информации по каналу РСПИ, не учитываются;

- рассматривается только АРМ РСПИ «Стрелец-Аргон»;

- количество объектов на одном рабочем месте оператора АРМ РСПИ составляет полную возможную нагрузку в 480 охраняемых объектов;

- структура ЛВС ПЦО состоит из центрального сервера, рабочего места оператора ДПУ и рабочего места дежурного ПЦО, рабочего места инженера ПЦО. Оператор ДПУ занимается только мониторингом охраняемых объектов и не задействуется для ведения баз данных;

- дежурный ПЦО и оператор АРМ РСПИ находятся в одном помещении (зале ПЦО), информация от оператора ДПУ передается дежурному ПЦО только по телефону;

- по радиостанции с нарядами физической охраны (ГЗ) взаимодействует только дежурный ПЦО;

- функционирование всех АРМ рассматривается в дежурном режиме без отказов, аварий, сбоев и возникновения внештатных ситуаций. При этом возможности саботажа учитываются при анализе уязвимостей АРМ;

- обслуживание ЛВС и АРМ ПЦО не рассматриваются, но учитываются при анализе уязвимостей;

- вычислительная сеть ПЦО не имеет выхода в Интернет;

- личный состав ПЦО при несении службы находится в удовлетворительном эмоционального-психическом и физическом состоянии и готовы к исполнению служебных обязанностей. При этом данные факторы учитываются при анализе уязвимостей процесса принятия управленческих решений и канала передачи информации;

- личный состав ПЦО обладает достаточными знаниями, навыками и опытом для выполнения должностных обязанностей. При этом данные факторы учитываются при анализе уязвимостей процесса принятия управленческих решений и канала передачи информации.

- полагается, что автотранспорт нарядов физической охраны находится в полностью исправном состоянии и оборудован системой спутниковой навигации для мониторинга местоположения;

- полагается, что наряд физической охраны действует строго на закреплённом маршруте следования, согласно штатной дислокации;

- полагается, что наряд физической охраны полностью укомплектован исправными и штатно функционирующими средствами связи, активной обороны, вооружением, специальными средствами и другой необходимой экипировкой;

- функционирование канала радиосвязи между ПЦО и нарядами рассматривается в дежурном режиме без отказов, аварий, сбоев и возникновения внештатных ситуаций. Участники радиочастотного взаимодействия соблюдают все требования ведения радиопереговоров. При этом возможности саботажа или прослушивания радиоканала учитываются при анализе уязвимостей радиоканала передачи информации;

- личный состав нарядов физической охраны при несении службы находится в удовлетворительном эмоционального-психическом и физическом состоянии и готовы к исполнению служебных обязанностей. При этом данные факторы учитываются при анализе уязвимостей процесса реагирования нарядов ГЗ на сигналы тревоги с охраняемых объектов и достоверности передачи информации на ПЦО;

- личный состав нарядов физической охраны ГЗ обладает достаточными знаниями, навыками и опытом для выполнения должностных обязанностей. При этом данные факторы учитываются при анализе уязвимостей процесса реагирования нарядов ГЗ на сигналы тревоги с охраняемых объектов и достоверности передачи информации на ПЦО.

2.3 Множества уязвимостей, угроз и защитных механизмов

Типовым подходом [44] для определения множеств угроз, защитных механизмов и др. факторов, влияющих на состояние ТКС, является формирование наиболее обобщенных (типовых) баз данных. Список полной базы данных уязвимостей, угроз, защитных механизмов, типов нарушителя для ТКС ЦОО составлен на основании анализа результатов экспертного опроса 15 специалистов вневедомственной охраны Росгвардии России. При этом использовались нормативные источники государственных регуляторов и государственные стандарты [44 - 58]. При анализе уязвимостей, угроз и защитных механизмов для РСПИ использовались источники [21 - 27, 59 - 65]. Результаты приведены в таблицах 2.2 – 2.5.

Для конкретной ТКС ЦОО при проведении комплексного аудита ТКС производится идентификации угроз и защитных механизмов, принимается конкретная модель нарушителя. Таким образом, создается локальная модель угроз и защитных механизмов для конкретной ТКС ЦОО и эти вопросы рассмотрены в третьей главе работы.

Таблица 2.2 - Базовый перечень уязвимостей структурных компонентов ТКС ЦОО

$У_1$	Нарушение условий эксплуатации ТСО
$У_2$	Некорректное функционирование ТСО
$У_3$	Некорректная оценка ситуации и ошибки управления оператором
$У_4$	Нарушение условий эксплуатации объектовых блоков РСПИ
$У_5$	Некорректное функционирование ЛВС
$У_6$	Низкий уровень организации работы
$У_7$	Неправильная оценка ситуации и ошибки управления дежурным ПЦО
$У_8$	В БД хранится информация разной степени конфиденциальности
$У_9$	Некорректные должностные инструкции / неопределённость ответственности за нарушения ПИБ
$У_{10}$	Отсутствие/неполный контроль за выполнением требований разграничения доступа
$У_{11}$	Для информационного обмена используются нерегламентированные технические средства
$У_{12}$	Терминалы оставляются без присмотра в рабочие и нерабочие часы. Данные отображаются на компьютерных экранах, оставленных без присмотра
$У_{13}$	Изменения в программы АРМов вносятся без их предварительного утверждения
$У_{14}$	Имеют место выходы из строя операционной системы (по неизвестным причинам)
$У_{15}$	Диски/другие носители оставляются в ящиках столов, не делается архивных копий дисков/других носителей
$У_{16}$	Конфигурация аппаратных средств не соответствует предъявляемым требованиям

Таблица 2.3 - Базовый перечень угроз структурных компонентов ТКС ЦОО

$УГ_1$	Не прохождение сигнала (обрыв в двухпроводной линии, не срабатывание извещателя, обрыв связи между контроллером ДПЛС и АРМ ИСБ, между релейными модулями и объектовым блоком РСПИ)
$УГ_2$	Подмена сообщения (адреса извещателя, типа извещения) в ДПЛС
$УГ_3$	Установка (изменение) временной задержки в передаче сообщения в линии связи ДПЛС или между преобразователем интерфейсов и ПК, несвоевременное срабатывание реле
$УГ_4$	Съем информации с ДПЛС с целью анализа
$УГ_5$	Специальное формирование ложных извещений
$УГ_6$	Не срабатывание реле релейных модулей
$УГ_7$	Не прохождение сигнала радиосвязи РСПИ от объекта до ПЦО
$УГ_8$	Саботаж канала радиосвязи РСПИ от объекта до ПЦО
$УГ_9$	Несвоевременное прохождение тревожных и служебных извещений от объекта до ПЦО
$УГ_{10}$	Неправильное распознавание извещений с охраняемых объектов до ПЦО переданных через РСПИ
$УГ_{11}$	Неправильная идентификация объекта с которого пришла информация
$УГ_{12}$	Подмена сообщений от объекта до ПЦО
$УГ_{13}$	Съем информации с канала связи РСПИ с целью анализа
$УГ_{14}$	Специальное формирование ложных извещений по каналу РСПИ
$УГ_{15}$	Ошибки и некорректная работа АРМ ПЦО
$УГ_{16}$	Осуществление НСД в ЛВС ПЦО, перехват трафика для анализа сети ЛВС
$УГ_{17}$	Перехват управления АРМ ПЦО нарушителем, проникшим в здание ПЦО
$УГ_{18}$	Ошибки администраторов БД ПЦО
$УГ_{19}$	Подмена администраторов и операторов
$УГ_{20}$	Подмена оборудования ТСО
$УГ_{21}$	Обрыв канала связи и/или снижение пропускной способности сети
$УГ_{22}$	Удаленное управление АРМ ДПУ и дежурного ПЦО, изменения в БД ПЦО
$УГ_{23}$	Пропуск «цели» (не реагирование оператором) на тревожное сообщение АРМ РСПИ

Продолжение таблицы 2.3

$УГ_{24}$	Задержка реагирования оператором РСПИ на тревожное сообщение АРМ РСПИ
$УГ_{25}$	Неправильное восприятие оператором информации о сработавшем объекте, и/или о типе сообщения с объекта
$УГ_{26}$	Пропуск «цели» (не реагирование дежурным ПЦО) на тревожное сообщение от оператора АРМ РСПИ
$УГ_{27}$	Задержка реагирования на тревожное сообщение дежурным ПЦО от оператора АРМ РСПИ
$УГ_{28}$	Неправильное восприятие дежурным ПЦО информации о сработавшем объекте, и/или о типе сообщения
$УГ_{29}$	Пропадание связи, отсутствие связи ПЦО с ГЗ из-за неисправности оборудования или помех в канале
$УГ_{30}$	Задержка передачи информации для ГЗ из-за помех в канале
$УГ_{31}$	Неправильное восприятие старшим ГЗ (дежурным ПЦО) информации о сработавшем объекте, и/или о типе сообщения
$УГ_{32}$	Саботаж канала связи УКВ ПЦО с ГЗ, с целью постановки помех и невозможности сеанса связи
$УГ_{33}$	Прослушивание канала связи УКВ ПЦО с ГЗ с целью формирования тактики действий нарушителя
$УГ_{34}$	Вмешательство в канал связи УКВ с целью передачи ГЗ ложной информации (подмена дежурного ПЦО)

Таблица 2.4 - Базовый перечень защитных механизмов структурных компонентов ТКС ЦОО

$ЗМ_1$	Обеспечение требований по условиям эксплуатации ТСО
$ЗМ_2$	Обеспечение штатного функционирования ТСО
$ЗМ_3$	Контроль работы оператора ИСБ
$ЗМ_4$	Обеспечение требований по условиям эксплуатации РСПИ
$ЗМ_5$	Контроль и обеспечение штатного функционирования объектовых блоков РСПИ
$ЗМ_6$	Обеспечение штатного функционирования ЛВС ПЦО
$ЗМ_7$	Обеспечение штатного функционирования АРМ РСПИ
$ЗМ_8$	Обеспечение штатной работы операторов АРМ РСПИ
$ЗМ_9$	Обеспечение штатной работы дежурных ПЦО
$ЗМ_{10}$	Обеспечение штатной передачи информации от дежурных ПЦО нарядам охраны
$ЗМ_{11}$	Обеспечение штатной работы нарядов физической охраны
$ЗМ_{12}$	Обеспечение ИБ на ПЦО

Таблица 2.5 – Распределение угроз ТКС ЦОО по доступности, целостности и конфиденциальности

Доступность (№ угрозы)	Целостность (№ угрозы)	Конфиденциальность (№ угрозы)
1,3,5,6,7,8,9,14,15,16, 17,18,19,20,21,22,23, 24,26,27,29,30,32,34	2,3,5,6,9,10,11,12,14, 15,16,17,18,19,20,22, 24,25,27,28,30,31,34	2,4,12,13,15,16,17, 18,19,20,22,33,34

Для практического использования типовых баз данных уязвимостей, угроз и защитных механизмов для анализа работоспособности ТКС ЦОО необходимо установить связи между этими базами в типовой структуре ТКС ЦОО.

Матрица связности угроз, уязвимостей, защитных механизмов и структурных компонентов ТКС ЦОО составлена на основании анализа результатов экспертного опроса 15 специалистов вневедомственной охраны Росгвардии России. Матрица связности представлена в таблице 2.6.

Таблица 2.6 - Матрица связи угроз, уязвимостей, защитных механизмов и структурных компонентов типовой ТКС ЦОО

Номера угроз $УГ^d{}_g \ g = 1..34$ / Номера уязвимостей $У^d{}_f \ f = 1..16$	Номера угроз $УГ^d{}_g \ g = 1..34$ / Номера защитных механизмов $ЗМ^d{}_h \ h = 1..12$	Номера уязвимостей $У^d{}_f \ f = 1..16$ / Структурные компоненты $КОМ_d$ d=1..11	Номера защитных механизмов $ЗМ^d{}_h \ h = 1..12$ / Структурные компоненты $КОМ_d$ d=1..11
1 / 1;2	1 / 1;2	1 / 1;2	1 / 1;2;4
2 / 2	2 / 1;2;3	2 / 1;2	2 / 1;2;4
3 / 1;2;3	3 / 2;3	3 / 3	3 / 3
4 / 2	4 / 2;3	4 / 4;5;6	4 / 4;5
5 / 1;2	5 / 1;2;3	5 / 7	5 / 4;5;6
6 / 1; 2; 3	6 / 1;2;3	6 / 7;8;11	6 / 7
7 / 4	7 / 4;5	7 / 9;11	7 / 7

Продолжение таблицы 2.6

8 / 4	8 / 4;5	8 / 7	8 / 8
9 / 4	9 / 5;7	9 / 7;8;9;11	9 / 9
10 / 4;8;10	10 / 5;7;8	10 / 7	10 / 9;10;11
11 / 4;8;10	11 / 7;8	11 / 7;9;10	11 / 11
12 / 4	12 / 4;5;7	12 / 7	12 / 7÷11
13 / 4	13 / 4;5;7	13 / 7	
14 / 4	14 / 4;5;7	14 / 7	
15 / 5;6;8;10 ; 13;14;16	15 / 6;7	15 / 7	
16 / 5;6;11;12; 13;14;15;16	16 / 6;7;12	16 / 7	
17 / 5;6;11;12; 13;14;15;16	17 / 6;7;12		
18 / 5;6;8;9;10; 11;13;14;16	18 / 8;9;12		
19 / 5;6;9;11;12; 13;14;15;16	19 / 12		
20 / 6;11; 14;15;16	20 / 6;8;12		
21 / 5;6;13; 14;15;16	21 / 6		
22 / 5;6;11;12; 13;14;15;16	22 / 12		
23 / 6;8;9;10;11; 12;13;14;16	23 / 8		
24 / 5;6;8;9;10; 11; 12;13;14;16	24 / 8		
25 / 5;6;8;9;10; 11; 12;13;14;16	25 / 8		
26 / 6;7;8;9;10; 11; 12;13;14;16	26 / 9		
27 / 6;7;9;11; 12;13;14;16	27 / 9		
28 / 6;7;9;11	28 / 9		
29 / 11	29 / 9;10		
30 / 11	30 / 10;11;12		

Окончание таблицы 2.6

31 / 11	31 / 10;11		
32 / 6;11	32 / 10; 12		
33 / 11	33 / 11;12		
34 / 11	34 / 10;12		

2.4 Алгоритм оценки $\lambda^d(g,f)$ - вероятности эксплуатации угрозой уязвимости компонента ТКС ЦОО

$\lambda^d(g,f)$ – является величиной вероятностной, зависящей от большого количества внешних факторов, поэтому будем считать ее случайно распределенной по нормальному закону с математическим ожиданием, равным оценке $\mu = \hat{\lambda}^d(g,f)$ и среднеквадратическим отклонением (коэффициентом масштаба) $\sigma^2 = 0.1$. Таким образом, вероятность эксплуатации g-й угрозой f -й уязвимости

$$\lambda^d(g,f) = N(\mu;\sigma^2) = N(\hat{\lambda}^d(g,f);0.1). \quad (2.1)$$

По аналогии с [40] предлагается ввести 10 градаций влияния $\hat{\lambda}^d(g,f)$ на функционирование ТКС: от 1 – «Незначительное», до 10 – «Катастрофическое», приводящее ТКС в нерабочее состояние на длительное время.

Выполним декомпозицию элементов модели «Множество уязвимостей» и «Множество угроз» в соответствии со следующим подходом.

«Множество уязвимостей» в d-м компоненте $У^d$.

Пусть для уязвимостей будет следующая классификация $У^d(f, lf, mf, nf)$:

f – текущий номер уязвимости;

$l\,f$ – индекс, определяющий тип угроз, вызываемых данной уязвимостью (1 –уязвимость, вызывающая угрозу целостности ИР; 2 – конфиденциальности; 3 – доступности; 4 – целостности и конфиденциальности; 5 – целостности и доступности; 6 – конфиденциальности и доступности; 7 – целостности, конфиденциальности и доступности);

mf – индекс, определяющий способ выявления уязвимости (1 – проявляется очевидно в процессе эксплуатации (ошибки, сбои и пр.); 2 – выявляется нормативно при изучении документации; 3 – выявляется объективно при изучении протоколов, логов, журналов и пр.; 4 – определяется по расчетной методике статистически на основе статистики эксплуатации; 5 – выявляется вероятностно, субъективно, на основе косвенных показателей; 6 – выявляется субъективно, в ходе общения с субъектами или оперативным путем (негласным контролем);

nf - индекс, определяющий характер проявления уязвимостей (1 – постоянная, 2 – периодическая редкая, 3 – периодическая частая; 4 – случайная, стохастическая). Количество индексов классификации и количество градаций по индексам определяется особенностями информационного процесса. Чем больше индексов классификации и количество градаций, тем более точное описание можно получить.

Например, запись $У^2(1,3,2,4)$ в модели означает, что анализируется для компонента второго типа (ПК, ПИ, АРМ ИСБ) первая уязвимость (Нарушение условий эксплуатации ТСО), угрозы доступности, уязвимость выявляется нормативно, при изучении документации и она (уязвимость) случайная.

Множество угроз (УГ) d-му компоненту $УГ^d{}_g$, которые потенциально могут проявиться в рассматриваемый период времени.

Пусть для угроз для d-го компонента будет следующая классификация $УГ^d(g, lg, ng)$:

g – текущий номер угрозы;

lg – индекс, определяющий тип угроз (1 –угроза целостности ИР; 2 – конфиденциальности; 3 – доступности; 4 – целостности и конфиденциальности; 5 – целостности и доступности; 6 – конфиденциальности и доступности; 7 – целостности, конфиденциальности и доступности);

ng – индекс, определяющий характер проявления угрозы (1 – постоянная, 2 – периодическая редкая, 3 – периодическая частая; 4 – случайная, стохастическая).

Например, запись $УГ^1(2,1,3)$ в модели означает, что анализируется для компонента первого типа (ОИ, КДЛ), вторая угроза (Подмена сообщения (адреса извещателя, типа извещения) в ДПЛС) при нарушении целостности и такая угроза периодически частая.

Предлагается качественно определить влияние на $\lambda^d(g,f)$ каждой пары «тип уязвимости/тип угрозы» с индексами, соответственно $(lf;mf;nf)$ и $(lg;ng)$, как минимальное (min), максимальное (max) и среднее (сред) влияние. При этом, считаем опасность угроз и уязвимостей одинаковым.

Введем:

- $\varphi^d(lf,mf,nf)$ – показатель «влияния» уязвимости на $\lambda^d(g,f)$, отдельно выделим $\varphi^d(lf)$ – показатель «влияния» типа угроз, вызываемых данной уязвимостью на $\lambda^d(g,f)$; $\varphi^d(mf)$ - показатель «влияния» способа выявления уязвимости на $\lambda^d(g,f)$; $\varphi^d(nf)$ - показатель «влияния» характера проявления уязвимостей на $\lambda^d(g,f)$;

- $\varphi^d(lg;ng)$ – показатель «влияния» угрозы на $\lambda^d(g,f)$, отдельно выделим $\varphi^d(lg)$ - показатель «влияния» типа угрозы на $\lambda^d(g,f)$; $\varphi^d(ng)$ - показатель «влияния» характера проявления угрозы на $\lambda^d(g,f)$.

Правило качественной оценки $\varphi^d(lf)$.

Если $lf = 7$ то $\varphi^d(lf) = "max"$,

если $lf \in \{4;5;6\}$ то $\varphi^d(lf) =$ "сред",

иначе $\varphi^d(lf) = "min"$ $(lf \in \{1;2;3\})$;

Правило качественной оценки $\varphi^d(mf)$.

Если $mf \in \{1;2;3\}$ то $\varphi^d(mf) = "max"$,

если $mf = 4$ то $\varphi^d(mf) =$ "сред",

иначе $\varphi^d(mf) = \min(mf \in \{5;6\})$;

Правило качественной оценки $\varphi^d(nf)$.

Если $nf \in \{1;3\}$ то $\varphi^d(nf) = "max"$,

если $nf = \{4\}$ то $\varphi^d(nf) =$ "сред",

иначе $\varphi^d(nf) = "min"$ $(nf = 2)$.

Правило качественной оценки $\varphi^d(lf, mf, nf)$.

Правило 2.1

$\varphi^d(lf)$	$\varphi^d(mf)$	$\varphi^d(nf)$	$\varphi^d(lf, mf, nf)$
"max"	"max" или "сред"	"max" или "сред"	"max"
"max"	"max" или "сред" или "min"	"min" или "сред"	"сред"
"max"	"min"	"max"	"сред"
"сред"	"сред" или "max" или "min"	"сред" или "max"	"сред"
"сред"	"сред" или "max"	"min"	"сред"
"сред"	"min"	"min"	"min"
"min"	"min" или "сред"	"min" или "сред"	"min"
"min"	"max" или "min"	"min" или "max"	"сред"
"min"	"max" или "сред"	"max" или "сред"	"сред"

Правило качественной оценки $\varphi^d(lg)$.

Если $lg = 7$ то $\varphi^d(lg) =$ "max",

если $lg \in \{4; 5; 6\}$ то $\varphi^d(lg) =$ "сред",

иначе $\varphi^d(lg) =$ "min" $(lg \in \{1; 2; 3\})$;

Правило качественной оценки $\varphi^d(ng)$.

Если $ng \in \{1; 3\}$ то $\varphi^d(ng) =$ "max",

если $ng = 4$ то $\varphi^d(ng) =$ "сред",

иначе $\varphi^d(ng) =$ "min" $(ng = 2)$.

Правило качественной оценки $\varphi^d(lg; ng)$

Правило 2.2

$\varphi^d(lg)$	$\varphi^d(ng)$	$\varphi^d(lg;ng)$
"max"	"max"	"max"
"max"	"сред" или "min"	"сред"
"сред"	"max" или "сред" или "min"	"сред"
"min"	"max"	"сред"
"min"	"сред"	"сред"
"min"	"min"	"min"

Рассмотрев все возможные варианты пар «Уязвимость – Угроза», эксперты выделили 10 устойчивых комбинаций, влияющих на возможность реализации угрозы как одно из списка: «Незначительное», «Низкое», «Ниже среднего», «Среднее», «Выше среднего», «Приемлемое», «Существенное», «Значительное», «Весьма значительное», «Катастрофическое».

С помощью логических конструкций мы формализовали данный подход. Переход от качественных значений к количественным (вероятностям) производится равномерно от 0,1 до 1,0 с шагом 0.1.

Правило количественной оценки $\hat{\lambda}^d(g,f)$:

Правило 2.3

если $(\varphi^d(lf,mf,nf) = »max») \wedge (lf = 7) \wedge (\varphi^d(lg;ng) = »max»)$ то $\hat{\lambda}^d(g,f) =$ »Катастрофическое» (1,0), если $(\varphi^d(lf,mf,nf) = »max») \wedge (lf \neq 7) \wedge (\varphi^d(lg;ng) = »max»)$ то $\hat{\lambda}^d(g,f) =$ »Весьма значительное» (0,9), если $(\varphi^d(lf,mf,nf) =$ "max") $\wedge (\varphi^d(lg;ng) =$ "сред") то $\hat{\lambda}^d(g,f) =$ "Значительное" (0,8), если $(\varphi^d(lf,mf,nf) =$ сред) $\wedge (\varphi^d(lg;ng) =$ "max") то $\hat{\lambda}^d(g,f) =$ "Существенное" (0,7), если $(\varphi^d(lf,mf,nf) =$

"max") ∧ ($\varphi^d(lg; ng) =$ "min") то $\hat{\lambda}^d(g, f) =$ "Приемлемое" (0,6), если ($\varphi^d(lf, mf, nf) =$ "min") ∧ ($\varphi^d(lg; ng) =$ "max") то $\hat{\lambda}^d(g, f) =$ "Выше среднего" (0,5), если ($\varphi^d(lf, mf, nf) =$ "сред") ∧($\varphi^d(lg; ng) =$ "сред") то $\hat{\lambda}^d(g, f) =$ "Среднее" (0,4), если ($\varphi^d(lf, mf, nf) =$ "сред") ∧ ($\varphi^d(lg; ng) =$ "min") то $\hat{\lambda}^d(g, f) =$ "Ниже среднего" (0,3), если ($\varphi^d(lf, mf, nf) =$ "min") ∧ ($\varphi^d(lg; ng) =$ "сред") то $\hat{\lambda}^d(g, f) =$ "Низкое" (0,2), иначе $\hat{\lambda}^d(g, f) =$ "Незначительное" (0,1) (($\varphi^d(lf, mf, nf) =$ "min")∧($\varphi^d(lg; ng) =$ "min").

Алгоритм

Исходные данные: матрица связи угроз и уязвимостей

Шаг 1. $f = 1$. Начиная с первой угрозы

Шаг 2 Начиная с первой уязвимости, связанной с текущей угрозой.

Шаг 3. вычислить $\hat{\lambda}^d(g, f)$

Шаг 4. Если есть еще уязвимости, связанные с угрозой с номером g, то перейти к следующей $f = f + 1$, перейти к шагу 3 иначе если не последняя угроза ($g \leq 34$) то $g = g + 1$ перейти к шагу 2 иначе конец алгоритма

2.5 Алгоритм оценки $\mu^d(g, h)$ - вероятности опасности угроз по последствиям их реализации с учетом защитных механизмов

$\mu^d(g, h)$ – является величиной вероятностной, зависящей от большого количества внешних факторов, поэтому будем считать ее случайно распределенной по нормальному закону с математическим ожиданием, равным оценке $\mu = \mu^d(g, h)$ и среднеквадратическим отклонением (коэффициентом масштаба) $\sigma^2 = 0.1$. Таким образом, вероятность эксплуатации g-й угрозой f -й уязвимости

$$\mu^d(g, h) = N(\mu; \sigma^2) = N(\hat{\mu}^d(g, h); 0.1) \quad (2.2)$$

По аналогии с [40] предлагается ввести 10 градаций влияния $\hat{\mu}^d(g,h)$ на функционирование ТКС: от 1 – «Незначительное», до 10 – «Катастрофическое», приводящее ТКС в нерабочее состояние на длительное время.

Выполним декомпозицию элементов модели «Множество защитных механизмов» и «Множество угроз».

Множество защитных механизмов угрозам d-му компоненту ЗМ^d .

Пусть для защитных механизмов $\text{ЗМ}^{\boldsymbol{d}}(h,p,k,nh)$ будет следующая классификация:

h – текущий номер защитного механизма;

p - индекс, определяющий тип защитного механизма (1 – организационный; 2 - программный; 3 - технический; 4 – криптографический);

k - индекс, определяющий тип действия защитного механизма (1 – предотвращение угрозы; 2 – недопущение угрозы; 3 – повышения вероятности обнаружения угрозы; 4 – снижение вероятности реализации угрозы; 5 – предупреждение о реализации);

nh - индекс, определяющий характер действия защитного механизма (1 – постоянный, 2 – периодический редкий, 3 – периодический частый; 4 – случайный, стохастический).

Например, запись $\text{ЗМ}^1(2,2,1,2)$ в модели означает, что анализируется для компонента первого типа (ОИ, КДЛ) второй защитный механизм программного типа (Обеспечение штатного функционирования ТСО), при обеспечении предотвращения угрозы, причем действие его периодически редкое.

Множество угроз (УГ) d-му компоненту $\text{УГ}^d{}_g$, которые потенциально могут проявиться в рассматриваемый период времени предложено в предыдущем разделе.

Предлагается качественно определить влияние на $\hat{\mu}^d(g,h)$ каждой пары «тип защитного механизма / тип угрозы» с индексами, соответственно $(p;k;nh)$и $(lg;ng)$, как минимальное (min), максимальное (max) и среднее (сред) влияние. При этом, считаем опасность угроз одинаковой.

Для этого введем:

- $\varphi^d(p;k;nh)$ – показатель «влияния» типа h-го ЗМ на $\hat{\mu}^d(g,h)$;

- $\varphi^d(lg;ng)$ – показатель «влияния» типа g-й угрозы на $\hat{\mu}^d(g,h)$.

Правило качественной оценки $\varphi^d(h;p;k;nh)$. Аналогично $\varphi^d(lf,mf,nf)$ выделим из $\varphi^d(h;p;k;nh)$ составляющие $\varphi^d(k)$; $\varphi^d(nh)$

Правило 2.4

Если $k=5$ то $\varphi^d(k)=$"max",

если $k\in\{3;4\}$ то $\varphi^d(k)=$"сред", иначе $\varphi^d(k)=$"min" $(k\in\{1;2\})$;

Если $nh=2$ то $\varphi^d(nh)=$"max",

если $nh=4$ то $\varphi^d(nh)=$"сред",

иначе $\varphi^d(nh)=$"min") $nh\in\{1;3\}$).

Величину $\varphi^d(h;p;k;nh)$ определим из $\varphi^d(k)$; $\varphi^d(nh)$ в полном соответствии с правилом 2.2. Правило качественной оценки $\varphi^d(lg;ng)$ построено по правилу 2.2.

Правило количественной оценки $\hat{\mu}^d(g,h)$.

Правило 2.5

Если $(\varphi^d(p;k;nh)=$"max"$)\wedge(k=5)\wedge(\varphi^d(lg;ng)=$"$max$"$)$ то $\hat{\mu}^d(g,h)=1$,

если $(\varphi^d(p;k;nh)=$"max"$)\wedge(k\neq5)\wedge(\varphi^d(lg;ng)=$"$max$"$)$ то $\hat{\mu}^d(g,h)=0{,}9$,

если $(\varphi^d(p;k;nh)=$"max"$)\wedge(\varphi^d(lg;ng)=$"сред") то $\hat{\mu}^d(g,h)=0{,}8$,

если $(\varphi^d(p;k;nh)=$ "сред"$)\wedge(\varphi^d(lg;ng)=$"$max$") то $\hat{\mu}^d(g,h)=0{,}7$,

если $(\varphi^d(p;k;nh)=$"max"$)\wedge(\varphi^d(lg;ng)=$"$min$") то $\hat{\mu}^d(g,h=0{,}6$,

если $(\varphi^d(p;k;nh)=$"min"$)\wedge(\varphi^d(lg;ng)=$"$max$") то $\hat{\mu}^d(g,h)=0{,}5$,

если $(\varphi^d(p;k;nh)=$ "сред"$)\wedge(\varphi^d(lg;ng)=$"сред") то $\hat{\mu}^d(g,h)=0{,}4$,

если $(\varphi^d(p;k;nh)=$ "сред"$)\wedge(\varphi^d(lg;ng)=$"$min$") то $\hat{\mu}^d(g,h)=0{,}3$,

если $(\varphi^d(p;k;nh)=$ "min"$)\wedge(\varphi^d(lg;ng)=$"сред") то $\hat{\mu}^d(g,h)=0{,}2$,

иначе $\hat{\mu}^d(g,h)=0{,}1$ $((\varphi^d(p;k;nh)=$ "min"$)\wedge(\varphi^d(lg;ng)=$"$min$").

Алгоритм

Исходные данные: матрица связи угроз и защитных механизмов

Шаг 1. $f = 1$. Начиная с первой угрозы

Шаг 2 Начиная с первого ЗМ, связанного с текущей угрозой.

Шаг 3. вычислить $\hat{\mu}^d(g, h)$

Шаг 4. Если есть еще защитные механизмы, связанные с угрозой с номером g, то перейти к следующему ЗМ $h = h + 1$, перейти к шагу 3 иначе если не последняя угроза ($g \leq 34$) то $g = g + 1$ перейти к шагу 2 иначе конец алгоритма.

2.6 Усовершенствованная модель определения вероятности защищенности компонента ТКС ЦОО от угроз

Введем дополнительный элемент модели - «Нарушитель».

Пусть для модели нарушителя $\mathrm{H}(q, s)$ будет следующая классификация:

q - индекс, определяющий тип нарушителя по возможности доступа к ИР ТКС (1 – внутренний нарушитель, который может быть осведомлен об оперативной информации в ТКС; 2 – внутренний нарушитель, который имеет доступ и может модифицировать информацию в ТКС; 3 – внутренний нарушитель, который имеет доступ к ИР и принимает решения по реагированию; 4 – внешний нарушитель, не обладающий информацией об объекте и доступом к ИР ТКС; 5 – внешний нарушитель, обладающий информацией об объекте, но не имеющий доступа к ИР в ТКС; 6 – внешний нарушитель, обладающий информацией об объекте и который может быть осведомлен об оперативной информации в ТКС; 7 – внешний нарушитель, обладающий информацией об объекте, имеющий доступ и способный модифицировать или саботировать информацию в ТКС);

s - индекс, определяющий оснащенность нарушителя (1 – неоснащенный; 2 – частично оснащенный; 3 – полностью оснащенный, имеющий любые технические и программные средства);

Например, запись $\mathrm{H}(1,2)$ в модели означает, что рассматривается внутренний нарушитель, который может быть осведомлен об оперативной информации в ТКС и частично оснащенный техническими и программными средствами.

Дополнительно введем параметр $NP(g,\text{Н})$ - коэффициент, учитывающий возможности нарушителя при всех благоприятных условиях реализовать угрозу ($0 \leq NP(q,s) \leq 1$).

Предлагается качественно определить влияние на $NP(g,\text{Н})$ каждой пары «тип нарушителя / тип угрозы» с индексами, соответственно (q,s) и $(lg;ng)$, как минимальное (min), максимальное (max) и среднее (сред) влияние.

Для этого введем:

- $\varphi^d(q,s)$ – показатель «влияния» типа нарушителя на $NP(g,\text{Н})$;

- $\varphi^d(lg;ng)$ – показатель «влияния» типа угрозы на $NP(g,\text{Н})$.

Правило качественной оценки $\varphi^d(q,s)$. Аналогично $\varphi^d(lf,mf,nf)$ выделим из $\varphi^d(q,s)$ составляющие $\varphi^d(q)$; $\varphi^d(s)$

Правило 2.6

Если $q \in \{1;2;3;7\}$ то $\varphi^d(q) = "max"$,

если $q \in \{5;6\}$ то $\varphi^d(q) =$ "сред",

иначе $\varphi^d(q) = "min"$ $(q = 4)$;

Если $s = 3$ то $\varphi^d(s) = "max"$,

если $s = 2$ то $\varphi^d(s) =$ "сред",

иначе $\varphi^d(s) = "min"$ $(s = 1)$;

Величину $\varphi^d(q,s)$ определим из $\varphi^d(q)$; $\varphi^d(s)$ в полном соответствии с правилом 2.2. Правило качественной оценки $\varphi^d(lg;ng)$ построено по правилу 2.2.

Правило количественной оценки $\widehat{NP}(g,\text{Н})$.

Правило 2.7

Если $(\varphi^d(q,s) = "max") \wedge (q = 1) \wedge (\varphi^d(lg;ng) = "max")$ то $\widehat{NP}(g,\text{Н}) = 0.01$

если $(\varphi^d(q,s) = "max") \wedge (q \neq 1) \wedge (\varphi^d(lg;ng) = "max")$ то $\widehat{NP}(g,\text{Н}) = 0.1$,

если $(\varphi^d(q,s) = "max") \wedge (\varphi^d(lg;ng) =$ "сред") то $\widehat{NP}(g,\text{Н}) = 0{,}2$,

если $(\varphi^d(q,s) =$ "сред") $\wedge (\varphi^d(lg;ng) = "max")$ то $\widehat{NP}(g,\text{Н}) = 0{,}3$,

если ($\varphi^d(q,s) = "max"$) $\wedge$ ($\varphi^d(lg;ng) = "min"$) то $\widehat{NP}(g,\text{Н}) = 0.4$,

если ($\varphi^d(q,s) = "min"$) $\wedge$ ($\varphi^d(lg;ng) = "max"$) то $\widehat{NP}(g,\text{Н}) = 0{,}5$,

если ($\varphi^d(q,s) =$ "сред") $\wedge$ ($\varphi^d(lg;ng) =$ "сред") то $\widehat{NP}(g,\text{Н}) = 0{,}6$,

если ($\varphi^d(q,s) =$ "сред") $\wedge$ ($\varphi^d(lg;ng) = "min"$) то $\widehat{NP}(g,\text{Н}) = 0{,}7$,

если ($\varphi^d(q,s) =$ "min") $\wedge$ ($\varphi^d(lg;ng) =$ "сред") $\widehat{NP}(g,\text{Н}) = 0{,}8$, иначе $\widehat{NP}(g,\text{Н}) = 0{,}9$ (($\varphi^d(q,s) =$ "min")$\wedge$($\varphi^d(lg;ng) = "min"$).

Дополнительно введем параметр $YP(g,t)$ - вероятность посягательства с целью реализации угроз $0 \leq YP(g,t) \leq 1$, здесь t - индекс, определяющий категорию охраняемого объекта по [11, 45] (1 – А1; 2 – А2; 3 – А3; 4 – Б1; 5 – Б2).

$YP(g,t)$ – является величиной вероятностной, зависящей от большого количества внешних факторов, поэтому будем считать ее случайно распределенной по нормальному закону с математическим ожиданием, равным оценке $\mu = \widehat{YP}(g,t)$ и среднеквадратическим отклонением (коэффициентом масштаба) $\sigma^2 = 0.1$. Таким образом:

$$YP(g,t) = N(\mu;\sigma^2) = N(\widehat{YP}(g,t);0.1) \qquad (2.3)$$

Предлагается качественно определить влияние на $YP(g,t)$ каждой пары «категория охраняемого объекта / тип угрозы» с индексами, соответственно t и $(lg;ng)$, как минимальное (min), максимальное (max) и среднее (сред) влияние.

Для этого введем:

- $\varphi^d(t)$ – показатель «влияния» категории охраняемого объекта на $YP(g,t)$;

- $\varphi^d(lg;ng)$ – показатель «влияния» типа g-й угрозы на $YP(g,t)$.

Правило качественной оценки $\varphi^d(t)$.

Правило 2.8

Если $t \in \{1;2\}$ то $\varphi^d(t) = "max"$,

если $t \in \{3;4\}$ то $\varphi^d(t) =$ "сред",

иначе $\varphi^d(t) = "min"$ $(t = 5)$

Правило качественной оценки $\varphi^d(lg;ng)$ построено по правилу 2.2.

Правило количественной оценки $\widehat{YP}(g,t)$.

Правило 2.9

Если ($\varphi^d(t) = "max") \wedge (t = 1) \wedge (\varphi^d(lg;ng) = "max")$ то$\widehat{YP}(g,t). = 1$,

если ($\varphi^d(t) = "max") \wedge (t \neq 1) \wedge (\varphi^d(lg;ng) = "max")$ то $\widehat{YP}(g,t). = 0.9$,

если ($\varphi^d(t) = "max") \wedge (\varphi^d(lg;ng) =$ "сред") то $\widehat{YP}(g,t) = 0{,}8$,

если ($\varphi^d(t) =$ "сред") $\wedge (\varphi^d(lg;ng) = "max")$ то $\widehat{YP}(g,t) = 0{,}7$,

если ($\varphi^d(t) = "max") \wedge (\varphi^d(lg;ng) = "min")$ то $\widehat{YP}(g,t) = 0{,}6$,

если ($\varphi^d(t) = "min") \wedge (\varphi^d(lg;ng) = "max")$ то $\widehat{YP}(g,t) = 0{,}5$,

если ($\varphi^d(t) =$ "сред") $\wedge (\varphi^d(lg;ng) =$ "сред") то $\widehat{YP}(g,t) = 0{,}4$,

если ($\varphi^d(t) =$ "сред") $\wedge (\varphi^d(lg;ng) = "min")$ то $\widehat{YP}(g,t) = 0{,}3$,

если ($\varphi^d(t) = "min") \wedge (\varphi^d(lg;ng) =$ "сред") то $\widehat{YP}(g,t) = 0{,}2$, иначе $\widehat{YP}(g,t) = 0{,}1$ (($\varphi^d(t) = "min") \wedge (\varphi^d(lg;ng) = "min")$.

В алгоритм 1.1 внесем изменения. Рассчитаем вероятность эксплуатации g-й угрозой f -й уязвимости для d-го структурного компонента ТКС ЦОО

$$p^d(g,f) = 1 - \frac{\sum_{f=1}^{F_d}(1-\hat{\lambda}^d(g,f))}{F_d} \quad (2.4)$$

Рассчитаем вероятность опасности угроз по последствиям их реализации с учетом ЗМ, или «степень сопротивляемости» g - й угрозе h -го ЗМ для d-го структурного компонента ТКС ЦОО

$$p^d(g,h) = 1 - \frac{\sum_{h=1}^{H_d}(1-\hat{\mu}^d(g,h))}{H_d} \quad (2.5)$$

Рассчитаем показатель защищенности d-го структурного элемента ТКС ЦОО от g-й угрозы

$$p^d(g) = 1 - [p^d(g,f) \times (1 - p^d(g,h)]. \quad (2.6)$$

Замечание.

При формировании модели структуры ТКС ЦОО следует учитывать, что на ПЦО охраняется довольно большое количество объектов, от нескольких десятков

до сотен. Структурные компоненты ТКС ЦОО КОМ$_d$ (d=1 (ОИ, КДЛ); d=2 (ПК, ПИ, АРМ ИСБ); d=3 (Оператор АРМ ИСБ и РМ); d=4 (ОПП РСПИ); d=5 (Радиоканал РСПИ) относятся к каждому из охраняемых объектов, а компоненты d=6 (ЦПП РСПИ); d=7 (ЛВС, множество АРМ РСПИ; АРМ дежурного ПЦО, Сервер БД, АРМ инженера ПЦО); d=8 (оператор АРМ РСПИ, АТС и телефонные аппараты для связи операторов АРМ РСПИ и дежурного ПЦО); d=9 (Дежурный ПЦО); d=10 (УКВ радиостанции дежурного ПЦО для связи с нарядами ГЗ); d=11 (Мобильные наряды ГЗ) относятся ко всем объектам сразу.

Пусть всего на ПЦО охраняется N объектов разных категорий [11,45]:

$$N = N|_{t=1} + N|_{t=2} + N|_{t=3} + N|_{t=4} + N|_{t=5}\ . \qquad (2.7)$$

Здесь $N|_{t=1}$ – количество охраняемых объектов категории А1;

$N|_{t=2}$ – количество охраняемых объектов категории А2;

$N|_{t=3}$ – количество охраняемых объектов категории А3;

$N|_{t=4}$ – количество охраняемых объектов категории Б1;

$N|_{t=5}$ – количество охраняемых объектов категории Б2.

Тогда

$$p^d(g) = \min_{t=1,\dots,5}\left(\frac{\sum_{n=1}^{N|_t}\left(p^d(g)\right)}{N|_t}\right). \qquad (2.8)$$

Следует указать, что формула (2.6) определяет защищенность d-го структурного элемента ТКС ЦОО от g-й угрозы в условиях отсутствия попытки нарушителя осуществлять НСД.

Если рассматривать деструктивные действия нарушителя по осуществлению НСД, то данную формулу необходимо дополнить коэффициентами $\widehat{YP}(g,t)$ и $\widehat{NP}(g,\mathrm{H})$. Таким образом, защищенность d-го структурного элемента ТКС ЦОО от g-й угрозы, во время попытки нарушителя типа $\mathrm{H}(q,s)$ осуществить НСД на охраняемый объект категории t будет выражаться как:

$$p^d(g)|_{\mathrm{H}(q,s)} = [1 - [p^d(g,f) \times \left(1 - p^d(g,h)\right)] \times$$
$$\times \left[1 - \left(\widehat{YP}(g,t) \times \widehat{NP}(g,\mathrm{H})\right)\right], \qquad (2.9)$$

а выражение (2.8) будет:

$$p^d(g)|_{\mathrm{H}(q,s)} = \min_{t=1,\dots,5}\left(\frac{\sum_{n=1}^{N|_t}(p^d(g)|_{\mathrm{H}(q,s)})}{N|_t}\right). \quad (2.10)$$

Защищенность информационных процессов $\mathrm{ИП}_c$ определим как минимальную из вероятностей $p^d(g)|_{\mathrm{H}(q,s)}$ защищенности структурных компонентов, входящих в информационный процесс (структурный компонент входит в информационный процесс) по таблице 2.1

$$p(\mathrm{ИП}_c)|_{\mathrm{H}(q,s)} = \min\{p^d(g)|_{\mathrm{H}(q,s)}\},\ if\ \mathrm{КОМ}_d\ \ni \{\mathrm{ИП}_c\}. \quad (2.11)$$

Аналогично, защищенность обобщенных функций $\mathrm{ОФ}_b$ определим как минимальную из вероятностей $p(\mathrm{ИП}_c)|_{\mathrm{H}(q,s)}$ защищенности информационных процессов, входящих в обобщенную функцию (информационный процесс входит в обобщенную функцию) по таблице 2.1

$$p(\mathrm{ОФ}_b)|_{\mathrm{H}(q,s)} = \min\{p(\mathrm{ИП}_c)|_{\mathrm{H}(q,s)}\},\ if\ \mathrm{ИП}_c \ni \{\mathrm{ОФ}_b\}. \quad (2.12)$$

Аналогично, защищенность основных режимов функционирования $\mathrm{ОР}_a$ определим как минимальную из вероятностей $p(\mathrm{ОФ}_b)|_{\mathrm{H}(q,s)}$ защищенности обобщенных функций, входящих в основной режим функционирования (обобщенная функция входит в основной режим функционирования ТКС ЦОО) по таблице 2.1.

$$p(\mathrm{ОР}_a)|_{\mathrm{H}(q,s)} = \min\{p(\mathrm{ОФ}_b)|_{\mathrm{H}(q,s)}\},\ if\ \mathrm{ОФ}_b \ni \{\mathrm{ОР}_a\}. \quad (2.13)$$

Рассмотрим «идеальное» ПЦО, на котором для всех защищаемых объектов фактически нет уязвимостей и присутствуют все возможные защитные механизмы, т.е. $p^d(g,f) \to 0;\ p^d(g,h) \to 1$.

Пусть $p^d(g,f)_{MIN}$; $p^d(g,h)_{MAX}$ обнаруженные при обследовании ПЦО и защищаемых объектов все «минимальные угрозы» и «максимальные защитные механизмы», тогда выражение

$$\Delta p^d(g) = max[p^d(g,f)_{MIN}; (1 - p^d(g,h)_{MAX})] \quad (2.14)$$

определяет максимальную системную погрешность моделирования работоспособности ТКС ЦОО (погрешность классификации, ранжирования, интерпретации результатов и экспертных оценок при моделировании).

Полная погрешность моделирования работоспособности ТКС ЦОО может быть оценена и фактически, на основании статистики НСД по итогам функционирования ПЦО на протяжении весьма длительного срока (в виду небольшого количества попыток НСД на защищаемые объекты может потребоваться несколько лет)

$$\Delta_{\Sigma} p(g) = \left| \frac{K_{\text{НСД}}}{K_{\text{ПОП}}} - P(\min(\text{OP}_{\text{a}})) \right|, \quad (2.15)$$

где $\Delta_{\Sigma} p(g)$ – полная погрешность моделирования работоспособности ТКС ЦОО; $K_{\text{НСД}}$ – количество НСД за отчетный период; $K_{\text{ПОП}}$ количество зафиксированных попыток НСД за отчетный период; $P(\min(\text{OP}_{\text{a}}))$ – оценка вероятности выполнения основных режимов функционирования ТКС ЦОО, рассчитанная по предлагаемым алгоритмам.

Величину $P_{\text{НСД}} = 1 - p(\text{OP}_2) > P_{\text{ПОР}}$ можно считать критерием возможности осуществления проникновения на защищаемый объект. При низком уровне защищенности и обеспечения работоспособности ТКС ЦОО в основном режиме работы ОР№2 (режим охраны объектов) возможно допущение НСД.

Выводы к главе 2

На основе объектно-ориентированного подхода сформированы составляющие расчетную модель ТКС ЦОО множества компонентов, информационных процессов, объединяющих компоненты в устойчивые совокупности, обобщенных функций и режимов функционирования. Разработаны матрицы специального вида, связывающие элементы выделенных множеств.

На основе нормативных источников государственных регуляторов, стандартов, отраслевых руководящих документов и «лучших практик» моделирования процессов обеспечения информационной безопасности в телекоммуникационных системах, а также учитывая мнение специалистов вневедомственной

охраны Росгвардии России, синтезированы базы данных уязвимостей, угроз, защитных механизмов, типов нарушителя и их взаимосвязи, отличающиеся универсальностью и разумной достаточностью для систем данного типа, что позволяет эффективно и с небольшими затратами времени строить модели угроз конкретной ТКС ЦОО.

Разработана методика оценки вероятности (эффективности) эксплуатации угрозой уязвимости компонента ТКС ЦОО. Методика основана на предложенной классификации угроз по типу и характеру проявления, уязвимостей – по типу угроз, вызываемых данной уязвимостью, способу выявления уязвимости, характеру ее проявления. На основе логико-вероятностного подхода и экспертных оценок разработаны формальные правила количественной оценки вероятности эксплуатации угрозой уязвимости. Методика позволяет упростить расчетную модель оценки защищенности за счет хранения не огромных массивов качественных параметров, а только алгоритмов (правил).

Разработана методика оценки вероятности опасности угроз по последствиям их реализации с учетом защитных механизмов. Методика основана на предложенной классификации защитных механизмов по типу, способу и характеру его действия. На основе логико-вероятностного подхода и экспертных оценок разработаны формальные правила количественной оценки вероятности опасности угроз, что позволяет упростить расчетную модель за счет хранения алгоритмов (правил).

Усовершенствована модель определения вероятности защищенности компонента ТКС ЦОО от угроз. В известную модель включен элемент «Нарушитель» и сопутствующие ему параметры: коэффициент, учитывающий возможности нарушителя реализовать угрозу, вероятность посягательства с целью реализации угроз, категории охраняемых объектов, что позволяет более точно моделировать процессы обеспечения информационной безопасности (больше факторов, влияющих на защищенность).

Глава 3 АЛГОРИТМЫ ОПРЕДЕЛЕНИЯ СТЕПЕНИ ПРОЯВЛЕНИЯ УЯЗВИМОСТИ И СИЛЫ ЗАЩИТНЫХ МЕХАНИЗМОВ ТКС ЦОО

Уязвимости ТКС ЦОО – это присущие объекту свойства, потенциально приводящие к нарушению безопасности информации и обусловленные недостатками процесса функционирования объекта, свойствами архитектуры ТКС ЦОО, протоколами обмена и интерфейсами, применяемыми программным обеспечением и аппаратной платформой, условиями эксплуатации.

Под способами защиты (далее защитными механизмами обеспечения ИБ) понимаются организованные возможности средств и мероприятий, осуществляемых в ТКС ЦОО с целью полной или частичной реализации одного или нескольких методов (стратегий, функций) защиты.

Методика анализа защищенности ставит задачу «привязки» уязвимостей и защитных механизмов к каждому компоненту ТКС ЦОО и далее к каждому информационному ресурсу, хранимому или обрабатываемому на данном оборудовании.

В главе разрабатываются алгоритмы определения степени проявления уязвимости и силы защитных механизмов ТКС ЦОО

3.1 Уязвимости ТКС ЦОО

Представим всю совокупность уязвимостей ТКС ЦОО в виде множества

$$У = \{У_1, \dots, У_f, \dots, У_F\}. \quad (3.1)$$

В таблице 3.1 перечислены все уязвимости, которые потенциально могут присутствовать в компонентах ТКС ЦОО. Данный перечень составлен на основе руководящих документов ФСТЭК, Росгвардии и «лучших» практик построения систем защиты информации при решении аналогичных задач.

Таблица 3.1 – Перечень уязвимостей ТКС ЦОО

Обозначение	Наименование уязвимости	Компоненты (ИП), ОФ
1	2	3
$У_1$	Нарушение условий эксплуатации ТСО	ОИ ОТС, КАДПЛ, АРМ ИСБ (ИП1), АРМ ИСБ (ИП2), АРМ ИСБ, АРМ ОТС(ИП3), РМ ОТС, ОПП РСПИ, ЦПП РСПИ (ИП4), ОФ1-ОФ3
$У_2$	Некорректное функционирование ТСО	ОИ ОТС, КАДПЛ, АРМ ИСБ (ИП1), АРМ ИСБ (ИП2), АРМ ИСБ, АРМ ОТС(ИП3), ОФ1-ОФ3
$У_3$	Некорректная оценка ситуации и ошибки управления оператором	ЦПП РСПИ, АРМ РСПИ (оператора ПЦО), Сервер БД, ЛВС, ОФ7- ОФ8
$У_4$	Нарушение условий эксплуатации объектовых блоков РСПИ	РМ ОТС, ОПП РСПИ, ЦПП РСПИ (ИП4), ОФ4-ОФ6
$У_5$	Некорректное функционирование ЛВС	ЦПП РСПИ, АРМ РСПИ (оператора ПЦО), Сервер БД, ЛВС (ИП5), АРМ РСПИ (оператора ПЦО), АРМ дежурного ПЦО, АТС, ЛВС (ИП6), ОФ7, ОФ8
$У_6$	Низкий уровень организации работы	ЦПП РСПИ, АРМ РСПИ (оператора ПЦО), Сервер БД, ЛВС (ИП5), АРМ РСПИ (оператора ПЦО), АРМ дежурного ПЦО, АТС, ЛВС (ИП6), АРМ дежурного ПЦО, УКВ радиостанция, ЛВС (ИП7), УКВ радиостанция, РС ГЗ ((ИП8), ОФ8- ОФ15
$У_7$	Неправильная оценка ситуации и ошибки управления дежурным ПЦО	ЦПП РСПИ, АРМ РСПИ (оператора ПЦО), Сервер БД, ЛВС (ИП5), АРМ РСПИ (оператора ПЦО), АРМ дежурного ПЦО, АТС, ЛВС (ИП6), АРМ дежурного ПЦО, УКВ радиостанция, ЛВС (ИП7), УКВ радиостанция, РС ГЗ ((ИП8), ОФ8- ОФ15
$У_8$	В БД хранится информация разной степени конфиденциальности	АРМ ИСБ (ИП2), ЦПП РСПИ, АРМ РСПИ (оператора ПЦО), Сервер БД, ЛВС (ИП5), ОФ3, ОФ7, ОФ8
$У_9$	Некорректные должностные инструкции / неопределённость ответственности за нарушения ПИБ	ЦПП РСПИ, АРМ РСПИ (оператора ПЦО), Сервер БД, ЛВС (ИП5), АРМ РСПИ (оператора ПЦО), АРМ дежурного ПЦО, АТС, ЛВС (ИП6), АРМ дежурного ПЦО, УКВ радиостанция, ЛВС (ИП7), УКВ радиостанция, РС ГЗ ((ИП8), ОФ3, ОФ7-ОФ15
$У_{10}$	Отсутствие/неполный контроль за выполнением требований разграничения доступа	АРМ ИСБ (ИП2), ЦПП РСПИ, АРМ РСПИ (оператора ПЦО), Сервер БД, ЛВС (ИП5), ОФ3, ОФ7, ОФ8

Окончание таблицы 3.1

$У_{11}$	Для информационного обмена используются нерегламентированные технические средства	ОИ ОТС, КАДПЛ, АРМ ИСБ (ИП1), АРМ ИСБ (ИП2), АРМ ИСБ, АРМ ОТС(ИП3), РМ ОТС, ОПП РСПИ, ЦПП РСПИ (ИП4), ЦПП РСПИ, АРМ РСПИ (оператора ПЦО), Сервер БД, ЛВС (ИП5), АРМ РСПИ (оператора ПЦО), АРМ дежурного ПЦО, АТС, ЛВС (ИП6), АРМ дежурного ПЦО, УКВ радиостанция, ЛВС (ИП7), УКВ радиостанция, РС ГЗ ((ИП8), ОФ3, ОФ7- ОФ10
$У_{12}$	Терминалы оставляются без присмотра в рабочие и нерабочие часы. Данные отображаются на компьютерных экранах, оставленных без присмотра	АРМ ИСБ (ИП2), ЦПП РСПИ, АРМ РСПИ (оператора ПЦО), Сервер БД, ЛВС (ИП5), ОФ3, ОФ7, ОФ8
$У_{13}$	Изменения в программы АРМов вносятся без их предварительного утверждения	АРМ ИСБ (ИП2), ЦПП РСПИ, АРМ РСПИ (оператора ПЦО), Сервер БД, ЛВС (ИП5), ОФ3, ОФ7, ОФ8
$У_{14}$	Имеют место выходы из строя операционной системы (по неизвестным причинам)	АРМ ИСБ (ИП2), ЦПП РСПИ, АРМ РСПИ (оператора ПЦО), Сервер БД, ЛВС (ИП5),, ОФ3, ОФ7, ОФ8
$У_{15}$	Диски/другие носители оставляются в ящиках столов, не делается архивных копий дисков/других носителей	АРМ ИСБ (ИП2), ЦПП РСПИ, АРМ РСПИ (оператора ПЦО), Сервер БД, ЛВС (ИП5), ОФ3, ОФ7, ОФ8
$У_{16}$	Конфигурация аппаратных средств не соответствует предъявляемым требованиям	АРМ ИСБ (ИП2), АРМ ИСБ, АРМ ОТС(ИП3), РМ ОТС, ОПП РСПИ, ЦПП РСПИ (ИП4), ЦПП РСПИ, АРМ РСПИ (оператора ПЦО), Сервер БД, ЛВС (ИП5), АРМ РСПИ (оператора ПЦО), АРМ дежурного ПЦО, АТС, ЛВС (ИП6), АРМ дежурного ПЦО, УКВ радиостанция, ЛВС (ИП7), УКВ радиостанция, РС ГЗ ((ИП8), ОФ3, ОФ7- ОФ10

В таблице 3.1 обозначены:

ИП 1. «Опрос охранных извещателей».

ИП 2. «Анализ информации на АРМ ИСБ».

ИП 3. «Активация ПЦН выходов для ОПП РСПИ».

ИП 4. «Передача информации от ОПП РСПИ на ПЦО».

ИП 5. «Анализ информации на АРМ РСПИ».

ИП 6. «Передача информации от оператора АРМ РСПИ дежурному ПЦО».

ИП 7. «Передача тревог от дежурного ПЦО наряду ГЗ».

ИП 8. «Информационный обмен ГЗ с дежурным ПЦО при отработке объекта».

ОФ1 – «Опрос ОИ по двухпроводной линии»;

ОФ2 – «Формирование извещений в адресной линии»;

ОФ3 –«Управление оператором АРМ ИСБ состоянием КОС ОТС»;

ОФ4 – «Контроль канала связи РСПИ»;

ОФ5 – «Передача тревог от КОС ТСО на ПЦО по каналу РСПИ»;

ОФ6 – «Прием информации ЦПП РСПИ от ОПП РСПИ»;

ОФ7 – «Обработка информации на АРМ РСПИ»;

ОФ8 – «Обработка информации и принятие решений оператором АРМ РСПИ»;

ОФ9 – «Информационный обмен оператора РСПИ и дежурного ПЦО»;

ОФ10 – «Передача тревог дежурным ПЦО наряду ГЗ»;

ОФ11 – «Следование ГЗ на охраняемый объект»;

ОФ12 – «Отработка сработавшего охраняемого объекта»;

ОФ13 – «Задержание нарушителя»;

ОФ14 – «Выявление причин срабатывания КОС ОТС»;

ОФ15 – «Физическая охрана объекта».

Множество У представим в виде объединения подмножеств уязвимостей, «присущих» компонентам ТКС ЦОО

$$\text{У} = \text{У}^1 \cup \text{У}^2 \cup \ldots \cup \text{У}^d \cup \ldots \cup \text{У}^D. \qquad (3.2)$$

Заметим, что отдельные уязвимости вида $\text{У}^d{}_f$ могут встречаться в разных компонентах - подмножествах (3.2). В дальнейшем для простоты будем считать, что конкретные уязвимости «закрепляются» за «своими» компонентами. Так для d-го компонента пронумерованное множество уязвимостей представим в виде: $\text{У}^d = \left\{\text{У}^d{}_1, \ldots, \text{У}^d{}_f, \ldots, \text{У}^d_{F_d}\right\}$, где $F_d \in F$.

Далее рассматриваем уязвимости одного (d-го) компонента ТКС ЦОО.

Считаем, что каждая f-я уязвимость ($f = 1, \ldots, F_d$) может быть однозначно идентифицирована (распознана) в компоненте по $r_{f_d} \in R$ идентификационным признакам (критериям), здесь R - множество всех возможных

идентификационных признаков уязвимостей: $R = \left\{r_{\text{У}_1}, \dots, r_{\text{У}_f}, \dots, r_{\text{У}_F}\right\}$, $r_{\text{У}_f}$ - подмножество идентификационных признаков f-й уязвимости компонента.

Идентификационным признаком уязвимости назовем такое событие (состояние, фактор, причина) в компоненте ТКС ЦОО, которое определяет вид уязвимости (из заданного перечня) и способствует реализации соответствующей угрозы информационной безопасности.

Пронумеруем элементы подмножества идентификационных признаков f-й уязвимости компонента

$$r_{\text{У}_f} = \left\{r_{\text{У}_f 1}, \dots, r_{\text{У}_f u_f}, \dots, r_{\text{У}_f U_f}\right\}. \quad (3.3)$$

Пример 3.1. Уязвимость «Нарушение условий эксплуатации ТСО» с соответствующими идентификационными признаками.

Уязвимость «Нарушение условий эксплуатации ТСО» с соответствующими идентификационными признаками приведены в таблице 3.2.

Таблица 3.2 – Уязвимость У_1 с соответствующими идентификационными признаками

Обозначение уязвимости	Наименование уязвимости	Обозначение и наименование элементов $r_{\text{У}_1}$ - подмножества идентификационных признаков уязвимости У_1
У_1	Нарушение условий эксплуатации ТСО	$r_{\text{У}_1 1}$ - Климатические условия (температура, влажность, запыленность) не соответствуют РД
		$r_{\text{У}_1 2}$ - Свободный доступ к щитам ОТС и оборудованию управления ТСО
		$r_{\text{У}_1 3}$ - Не опечатаны коммутационные коробки и средства ОТС
		$r_{\text{У}_1 4}$ - Форс-мажорные ситуации (техногенные аварии), приводящие к отказу ТСО
		$r_{\text{У}_1 5}$ - Допускаются лица, не имеющие соответствующих лицензий и допусков, а также электромонтеры без соответствующих проверок

Конец примера.

3.2 Степень проявления уязвимости

Предполагаем, что одна и та же уязвимость, находясь в разных компонентах ТКС ЦОО, находящейся в разных условиях эксплуатации, может проявляться более или менее. Такой качественной оценке сопоставим количественный эквивалент $s_{У_f} \in [0,1]$, где $s_{У_f}$ - степень проявления f-й уязвимости.

$s_{У_f}$ показывает, какая часть f-й уязвимости, характеризующейся множеством $r_{У_f}$ идентификационных признаков, присутствует (проявляется) в данном компоненте.

Введем дополнительную категорию – «вес» идентификационного признака f-й уязвимости - $\tilde{r}_{У_f u_f} \in [0,1]$, сумма весов всех признаков данной f-й уязвимости равна 1: $\sum_{u_f=1}^{U_f} \tilde{r}_{У_f u_f} = 1$

Значение $\tilde{r}_{У_f u_f}$ (веса идентификационного признака) определяется экспертами на основе важности данного признака для идентификации уязвимости, чем более специфичен признак для данной уязвимости, чем точнее он характеризует уязвимость, тем большим значением веса он обладает.

Пример 3.2 Определение экспертами весов идентификационных признаков уязвимости $У_1$

В экспертном анализе воспользуемся методом ранжирования. При этом методе каждый эксперт упорядочивает (ранжирует) идентификационные признаки уязвимости по убыванию важности, присваивая им числа - ранги**.** В случае, когда эксперт не может различить по важности два или более признака, он приписывает им одинаковые (связные) ранги.

Экспертизу проводили четыре эксперта, оценили пять признаков по шкале от 1 до 5. Результаты экспертизы представлены в таблице 3.2.

Таблица 3.2 – Результаты экспертов по оценке важности идентификационных признаков уязвимости $У_1$

Идентификационные признаки уязвимости $У_1$ - Нарушение условий эксплуатации ТСО	Эксперты			
	Э₁	Э₂	Э₃	Э₄
$r_{У_1 1}$ - Климатические условия (температура, влажность, запыленность) не соответствуют РД	5	4.5	4	5
$r_{У_1 2}$ - Свободный доступ к щитам ОТС и оборудованию управления ТСО	3	4.5	5	4
$r_{У_1 3}$ - Не опечатаны коммутационные коробки и средства ОТС	4	3	3	1.5
$r_{У_1 4}$ - Форс-мажорные ситуации (техногенные аварии), приводящие к отказу ТСО	2	1	2	1.5
$r_{У_1 5}$ - Допускаются лица, не имеющие соответствующих лицензий и допусков, а также электромонтеры без соответствующих проверок	1	2	1	1

Согласованность мнений экспертов определим с помощью расчета коэффициента конкордации Кендалла: $\frac{12\tilde{S}}{\hat{n}^2(\tilde{m}^3-\tilde{m})} = \frac{12*132}{4^2(5^3-5)} \approx 0.8$, здесь $\tilde{S}$– сумма квадратов отклонений всех оценок рангов каждого объекта экспертизы от среднего значения; $\hat{n}$– число экспертов; $\tilde{m}$ – число идентификационных признаков - объектов экспертизы. Коэффициент конкордации характеризует высокую согласованность мнений экспертов, что позволяет продолжить решение задачи.

Результаты расчетов отражены в таблице 3.3.

Таблица 3.3 – Результаты расчетов весов признаков

Идентификационный признак	Средний ранг	Вес признака
$r_{У_1 1}$	4.63	$\tilde{r}_{У_1 1}$ =0.32
$r_{У_1 2}$	4.13	$\tilde{r}_{У_1 2}$ =0.28
$r_{У_1 3}$	2.88	$\tilde{r}_{У_1 3}$ =0.20
$r_{У_1 4}$	1.63	$\tilde{r}_{У_1 4}$ =0.11
$r_{У_1 5}$	1.25	$\tilde{r}_{У_1 5}$ =0,09

Конец примера.

Степень проявления идентификационного признака уязвимости.

Введем множество $r^*_{\text{У}_f u_f}$ качественных параметров, характеризующих степень проявления u_f-го идентификационного признака f-й уязвимости:

$$r^*_{\text{У}_f u_f} = \left\{ r^*_{\text{У}_f u_f 1}, \dots, r^*_{\text{У}_f u_f q(u_f)}, \dots, r^*_{\text{У}_f u_f Q(u_f)} \right\}. \quad (3.4)$$

Пример 3.3 Качественные параметры, характеризующие степень проявления идентификационных признаков уязвимости У_1

Пример качественных параметров, характеризующих степень проявления идентификационных признаков уязвимости У_1 приведён в таблице 3.4.

Таблица 3.4 - Пример качественных параметров, характеризующих степень проявления идентификационных признаков уязвимости У_1

Обозначение и наименование элементов $r_{\text{У}_1}$ - подмножества идентификационных признаков уязвимости У_1	Параметры, характеризующие степень проявления идентификационных признаков уязвимости У_1
$r_{\text{У}_1 1}$ - Климатические условия (температура, влажность, запыленность) не соответствуют РД	$r^*_{\text{У}_1 11}$ - Критические нарушения (отличаются более 50% от нормы), приводят выходу из строя ТСО
	$r^*_{\text{У}_1 12}$ - Значительные нарушения (от 20 до 50% от нормы), приводят к нарушению режима эксплуатации ТСО и повышают вероятность отказов
	$r^*_{\text{У}_1 13}$ - Незначительные нарушения (от 10 до 20% от нормы), приводят к сокращению срока службы ТСО
	$r^*_{\text{У}_1 14}$ - Допустимые отклонения (до 10% от нормы), приводят к сокращению срока службы ТСО
$r_{\text{У}_1 2}$ - Свободный доступ к щитам ОТС и оборудованию управления ТСО	$r^*_{\text{У}_1 21}$ - Свободный доступ любых сотрудников объекта
	$r^*_{\text{У}_1 22}$ - Свободный доступ любых сотрудников объекта и посетителей
	$r^*_{\text{У}_1 23}$ - Свободный доступ любых сотрудников объекта и посетителей к АРМ ИСБ

Окончание таблицы 3.4

$r_{\text{у}_13}$ - Не опечатаны коммутационные коробки и средства ОТС	$r^*_{\text{у}_131}$ - Не опечатывание более 50% коммутационных средств
	$r^*_{\text{у}_132}$ - Не опечатывание менее 50% коммутационных средств
$r_{\text{у}_14}$ - Форс-мажорные ситуации (техногенные аварии), приводящие к отказу ТСО	$r^*_{\text{у}_141}$ - Весьма вероятно для данного компонента
	$r^*_{\text{у}_142}$ - Мало вероятно для данного компонента
	$r^*_{\text{у}_143}$ - Почти невероятно для данного компонента
$r_{\text{у}_15}$ - Допускаются лица, не имеющие соответствующих лицензий и допусков, а также электромонтеры без соответствующих проверок	$r^*_{\text{у}_151}$ - Весьма вероятно для данного компонента
	$r^*_{\text{у}_152}$ - Мало вероятно для данного компонента
	$r^*_{\text{у}_153}$ - Почти невероятно для данного компонента

Такой качественной оценке сопоставим количественный эквивалент степени (доли) проявления u_f-го идентификационного признака f-й уязвимости: $\widetilde{r^*}_{\text{у}_f u_f q(u_f)} \in [0,1]$,

$\widetilde{r^*}_{\text{у}_f u_f q(u_f)}$ определяется по вкладу элемента в значение признака. Заметим, что параметры, характеризующие степени проявления идентификационных признаков уязвимостей, взаимоисключающие, то есть для анализа выбирается только одно значение параметра, зависящее от типа компонента, режима и текущих условий функционирования ТКС ЦОО.

Результаты расчета весов идентификационных признаков уязвимостей и степеней их проявления сведены в таблицу 3.5.

Таблица 3.5 - Результаты расчета весов идентификационных признаков уязвимостей и степеней их проявления

Обозначение и наименование элементов подмножества идентификационных признаков уязвимости. Вес признака	Параметры, характеризующие степень проявления идентификационных признаков уязвимости	Степень проявления идентификационного признака уязвимости
$У_1$ - Нарушение условий эксплуатации ТСО		
$r_{У_11}$ - Климатические условия (температура, влажность, запыленность) не соответствуют РД $\tilde{r}_{У_11}$ =0,32	$r^*_{У_111}$ - Критические нарушения (отличаются более 50% от нормы), приводят выходу из строя ТСО	$\widetilde{r^*}_{У_111} = 1$
	$r^*_{У_112}$ - Значительные нарушения (от 20 до 50% от нормы), приводят к нарушению режима эксплуатации ТСО и повышают вероятность отказов	$\widetilde{r^*}_{У_112} = 0.7$
	$r^*_{У_113}$ - Незначительные нарушения (от 10 до 20% от нормы), приводят к сокращению срока службы ТСО	$\widetilde{r^*}_{У_113} = 0.5$
	$r^*_{У_114}$ - Допустимые отклонения (до 10% от нормы), приводят к сокращению срока службы ТСО	$\widetilde{r^*}_{У_114} = 0.3$
$r_{У_12}$ - Свободный доступ к щитам ОТС и оборудованию управления ТСО $\tilde{r}_{У_12} = 0,28$	$r^*_{У_121}$ - Свободный доступ любых сотрудников объекта	$\widetilde{r^*}\lambda_{У_121} = 0.7$
	$r^*_{У_122}$ - Свободный доступ любых сотрудников объекта и посетителей	$\widetilde{r^*}_{У_122} = 1$
$r_{У_13}$ - Не опечатаны коммутационные коробки и средства ОТС $\tilde{r}_{У_13}$= 0,20	$r^*_{У_131}$ - Не опечатывание более 50% коммутационных средств	$\widetilde{r^*}_{У_131} = 0.7$
	$r^*_{У_132}$ - Не опечатывание менее 50% коммутационных средств	$\widetilde{r^*}_{У_132} = 0.5$
$r_{У_14}$ - Форс-мажорные ситуации (техногенные аварии), приводящие к отказу ТСО $\tilde{r}_{У_14}$= 0,11	$r^*_{У_141}$ - Весьма вероятно для данного компонента	$\widetilde{r^*}_{У_141} = 0.9$
	$r^*_{У_142}$ - Мало вероятно для данного компонента	$\widetilde{r^*}_{У_142} = 0.5$
	$r^*_{У_143}$ - Почти невероятно для данного компонента	$\widetilde{r^*}_{У_143} = 0.2$
$r_{У_15}$ - Допускаются лица, не имеющие соответствующих лицензий и допусков, а также электромонтеры без соответствующих проверок $\tilde{r}_{У_15}$=0,09	$r^*_{У_151}$ - Всегда для данного компонента	$\widetilde{r^*}\lambda_{У_151} = 1$
	$r^*_{У_152}$ – Имеются отдельные факты для данного компонента	$\widetilde{r^*}_{У_152} = 0.7$
	$r^*_{У_153}$ – Просроченные лицензии	$\widetilde{r^*}_{У_153} = 0.5$

Продолжение таблицы 3.5

$У_2$ - Некорректное функционирование ТСО		
$r_{У_{21}}$ - Имеются ошибки проектирования $\tilde{r}_{У_{21}}= 0.2$	$r^*_{У_{211}}$ - Критические, приводящие к не срабатыванию ТСО при НСД	$\tilde{r}^*_{У_{211}} = 1$
	$r^*_{У_{212}}$ - Значительные, снижающие надежность защиты объектов и недоблокировкам уязвимых мест возможного проникновения	$\tilde{r}^*_{У_{212}} = 0.7$
	$r^*_{У_{213}}$ - Незначительные, снижающие надежность защиты объектов	$\tilde{r}^*_{У_{213}} = 0.2$
$r_{У_{22}}$ - Выявлены шибки монтажа извещателей $\tilde{r}_{У_{22}}= 0.15$	$r^*_{У_{221}}$ - Критические, приводящие к не срабатыванию ТСО при НСД	$\tilde{r}^*_{У_{221}} = 1$
	$r^*_{У_{222}}$ - Значительные, снижающие надежность защиты объектов и недоблокировкам уязвимых мест возможного проникновения	$\tilde{r}^*_{У_{222}} = 0.7$
	$r^*_{У_{223}}$ - Не значительные, снижающие надежность защиты объектов	$\tilde{r}^*_{У_{223}} = 0.2$
$r_{У_{23}}$ - Имеются ошибки программирования извещателей и/или контроллера ДПЛС $\tilde{r}_{У_{23}}= 0.15$	$r^*_{У_{231}}$ - Критические, приводящие к несрабатыванию ТСО при НСД	$\tilde{r}^*_{У_{231}} = 1$
	$r^*_{У_{232}}$ - Значительные, снижающие надежность защиты объектов и недоблокировкам уязвимых мест возможного проникновения	$\tilde{r}^*_{У_{232}} = 0.7$
	$r^*_{У_{233}}$ - Незначительные, снижающие надежность защиты объектов	$\tilde{r}^*_{У_{233}} = 0.3$
$r_{У_{24}}$ - Выявлены нарушения эксплуатационно-технического обслуживания ТСО $\tilde{r}_{У_{24}}= 0.20$	$r^*_{У_{241}}$ - Отсутствие эксплуатационно-технического обслуживания в течении последних 3 лет	$\tilde{r}^*_{У_{241}} = 0.2$
	$r^*_{У_{242}}$ - Отсутствие эксплуатационно-технического обслуживания в течении последних 5 лет	$\tilde{r}^*_{У_{242}} = 0.4$
	$r^*_{У_{243}}$ - Отсутствие эксплуатационно-технического обслуживания в течении всего срока эксплуатации	$\tilde{r}^*_{У_{243}} = 0.7$
$r_{У_{25}}$ - Отсутствие электрического заземления $\tilde{r}_{У_{25}}= 0.10$	$r^*_{У_{251}}$ - Имеется	$\tilde{r}^*_{У_{251}} = 0.4$
$r_{У_{26}}$ - Прокладка ДПЛС открытым способом $\tilde{r}_{У_{26}} = 0.10$	$r^*_{У_{261}}$ - Более 50% коммуникаций	$\tilde{r}^*_{У_{261}} = 0.4$
	$r^*_{У_{262}}$ - Менее 50% коммуникаций	$\tilde{r}^*_{У_{262}} = 0.2$
	$r^*_{У_{263}}$ - Менее 10% коммуникаций	$\tilde{r}^*_{У_{263}} = 0.1$

Продолжение таблицы 3.5

$r_{У_2 7}$ - Превышение срока эксплуатации $\tilde{r}_{У_2 7} = 0.09$	$r^*_{У_2 71}$ - Превышение срока эксплуатации (8 лет) на 2 года	$\tilde{\tilde{r}}^*_{У_2 71} = 0.2$
	$r^*_{У_2 72}$ - Превышение срока эксплуатации (8 лет) на 5 лет	$\tilde{\tilde{r}}^*_{У_2 72} = 0.3$
	$r^*_{У_2 73}$ - Превышение срока эксплуатации (8 лет) на 8 лет	$\tilde{\tilde{r}}^*_{У_2 73} = 0.5$
$У_3$ - Некорректная оценка ситуации и ошибки управления оператором/дежурным		
$r_{У_3 1}$ – Низкая / недостаточная квалификация $\tilde{r}_{У_3 1}$= 0.27	$r^*_{У_3 11}$ – Опыт и навыки отсутствуют (стаж работы менее 1 месяца) - возможны критические ошибки	$\tilde{\tilde{r}}^*_{У_3 11} = 1$
	$r^*_{У_3 12}$ – Опыт и навыки минимальные (от 1 до 6 месяцев) - возможны значительные ошибки	$\tilde{\tilde{r}}^*_{У_3 12} = 0.7$
	$r^*_{У_3 13}$ – Опыт и навыки от 6 месяцев до года - возможны незначительные ошибки	$\tilde{\tilde{r}}^*_{У_3 13} = 0.4$
	$r^*_{У_3 14}$ – Опыт и навыки более года - ошибки маловероятны	$\tilde{\tilde{r}}^*_{У_3 14} = 0.2$
$r_{У_3 2}$ – Плохое психофизическое состояние $\tilde{r}_{У_3 2}$= 0.23	$r^*_{У_3 21}$ – Вероятность очень высокая (болезнь, режим работы суточный, замена на сутки отсутствующего сотрудника)	$\tilde{\tilde{r}}^*_{У_3 21} = 1$
	$r^*_{У_3 22}$ – Вероятность высокая (постпохмельное состояние, возраст более 55 лет, хроническая болезнь)	$\tilde{\tilde{r}}^*_{У_3 22} = 0.5$
	$r^*_{У_3 23}$ – Вероятность имеется (бытовые проблемы, стресс)	$\tilde{\tilde{r}}^*_{У_3 23} = 0.3$
	$r^*_{У_3 24}$ – Вероятность низкая (психоэмоциональное состояние удовлетворительное)	$\tilde{\tilde{r}}^*_{У_3 24} = 0.1$
$r_{У_3 3}$ – Высокая загрузка (большое количество охраняемых объектов) $\tilde{r}_{У_3 3}$= 0.19	$r^*_{У_3 31}$ – Очень высокая нагрузка (более 100 тревожных сообщений в сутки)	$\tilde{\tilde{r}}^*_{У_3 31} = 1$
	$r^*_{У_3 32}$ – Высокая нагрузка (более 60 тревожных сообщений в сутки)	$\tilde{\tilde{r}}^*_{У_3 32} = 0.7$
	$r^*_{У_3 33}$ – Средняя нагрузка (от 20 до 60 тревожных сообщений в сутки)	$\tilde{\tilde{r}}^*_{У_3 33} = 0.2$
	$r^*_{У_3 34}$ – Низкая нагрузка (менее 20 тревожных сообщений в сутки)	$\tilde{\tilde{r}}^*_{У_3 34} = 0.1$

Продолжение таблицы 3.5

$r_{У_{з}4}$ – Плохой (низкий) уровень отображения акустической или визуальной информации на АРМ $\tilde{r}_{У_{з}4}$= 0.31	$r^*_{У_{з}41}$ – Удовлетворительный уровень представления информации	$\tilde{\tilde{r}}^*_{У_{з}41} = 0.5$
	$r^*_{У_{з}42}$ – Низкий уровень представления информации	$\tilde{\tilde{r}}^*_{У_{з}42} = 0.8$
$У_4$ - Нарушение условий эксплуатации объектовых блоков РСПИ		
$r_{У_41}$ – Климатические условия (температура, влажность, запыленность) не соответствуют РД $\tilde{r}_{У_41}$= 0.1	$r^*_{У_411}$ – Критические нарушения (отличаются более 50% от нормы), приводят выходу из строя ТСО	$\tilde{\tilde{r}}^*_{У_411} = 1$
	$r^*_{У_412}$ – Значительные нарушения (от 20 до 50% от нормы), приводят к нарушению режима эксплуатации ТСО и повышают вероятность отказов	$\tilde{\tilde{r}}^*_{У_412} = 0.7$
	$r^*_{У_413}$ – Не значительные нарушения (от 10 до 20% от нормы), приводят к сокращению срока службы ТСО	$\tilde{\tilde{r}}^*_{У_413} = 0.5$
	$r^*_{У_414}$ – Допустимые отклонения (до 10% от нормы), приводят к сокращению срока службы ТСО	$\tilde{\tilde{r}}^*_{У_414} = 0.3$
$r_{У_42}$ – Используемая модуляция $\tilde{r}_{У_42}$= 0.1	$r^*_{У_421}$ - Современные типы модуляции с удовлетворительной помехозащищенностью	$\tilde{\tilde{r}}^*_{У_421} = 0.1$
	$r^*_{У_422}$ - Модуляция с низкой помехозащищенностью	$\tilde{\tilde{r}}^*_{У_422} = 0.5$
$r_{У_43}$ – Необеспечение электромагнитной совместимости $\tilde{r}_{У_43}$= 0.5	$r^*_{У_431}$ – Электромагнитная ситуация не приемлемая (по количеству ложных срабатываний и пропаданию связи) – уровень ложных срабатываний в 2 раза выше среднего уровня; кол-во пропаданий связи более 2 раз в сутки	$\tilde{\tilde{r}}^*_{У_431} = 1$
	$r^*_{У_432}$ – Электромагнитная ситуация сложная– уровень ложных срабатываний выше среднего уровня; кол-во пропаданий связи не менее 1 раза в сутки	$\tilde{\tilde{r}}^*_{У_432} = 0.5$
	$r^*_{У_433}$ – Электромагнитная ситуация в пределах нормы– уровень ложных срабатываний не выше среднего уровня; кол-во пропаданий связи не более 2 раз в неделю	$\tilde{\tilde{r}}^*_{У_433} = 0.1$

Продолжение таблицы 3.5

$r_{У_{44}}$ – Работоспособность р/ст или антенно-фидерного устройства $\tilde{r}_{У_{44}}= 0.3$	$r^*_{У_{441}}$ – Критическая неисправность, нет возможности передачи информации	$\tilde{r}^*_{У_{441}} = 1$
	$r^*_{У_{442}}$ – Значительная, серьезная неисправность, разборчивость информации менее 50%	$\tilde{r}^*_{У_{442}} = 0.8$
	$r^*_{У_{443}}$ – Значительная неисправность, неразборчивость информации от 20 до 50%	$\tilde{r}^*_{У_{443}} = 0.5$
	$r^*_{У_{444}}$ – Незначительная неисправность, неразборчивость информации менее 20%	$\tilde{r}^*_{У_{444}} = 0.2$
$У_5$ - **Некорректное функционирование ЛВС**		
$r_{У_{51}}$ – ЛВС проведена открытым способом $\tilde{r}_{У_{51}}= 0.29$	$r^*_{У_{511}}$ – ЛВС проведена в коробах без опечатывания, доступ возможен	$\tilde{r}^*_{У_{511}} = 0.7$
	$r^*_{У_{512}}$ – ЛВС проведена открытым способом, доступ возможен	$\tilde{r}^*_{У_{512}} = 0.7$
$r_{У_{52}}$ – Имеются ошибки проектирования $\tilde{r}_{У_{52}}= 0.71$	$r^*_{У_{521}}$ – Критические	$\lambda_{У_{521}} = 1$
	$r^*_{У_{522}}$ – Значительные, снижающие надежность функционирования и защиту объектов	$\tilde{r}^*_{У_{522}} = 0.7$
	$r^*_{У_{523}}$ – Не значительные, снижающие надежность функционирования и защиту объектов	$\tilde{r}^*_{У_{523}} = 0.3$
$У_6$ **- Низкий уровень организации работы**		
$r_{У_{61}}$ – Нечеткие должностные инструкции работы ПЦО $\tilde{r}_{У_{61}}= 0.38$	$r^*_{У_{611}}$ – Низкий уровень должностных инструкций	$\tilde{r}^*_{У_{611}} = 0.5$
	$r^*_{У_{612}}$ – Удовлетворительный уровень должностных инструкций	$\tilde{r}^*_{У_{612}} = 0.1$
	$r^*_{У_{613}}$ – Критический уровень (почти никто ничего не знает)	$\tilde{r}^*_{У_{613}} = 0.9$
$r_{У_{62}}$ – Отсутствие / нерегулярный контроль действий персонала $\tilde{r}_{У_{62}}= 0.40$	$r^*_{У_{621}}$ – Отсутствует контроль действий персонала	$\tilde{r}^*_{У_{621}} = 0.8$
	$r^*_{У_{622}}$ – Нерегулярный контроль действий персонала	$\tilde{r}^*_{У_{622}} = 0.3$
$r_{У_{63}}$ – Отсутствие / нерегулярный инструктаж/обучение $\tilde{r}_{У_{63}}= 0.22$	$p_{У_{631}}$ – Отсутствует инструктаж	$\tilde{r}^*_{У_{631}} = 0.5$
	$r^*_{У_{632}}$ – Отсутствует инструктаж и обучение	$\tilde{r}^*_{У_{632}} = 0.8$
	$r^*_{У_{633}}$ – Нерегулярный инструктаж / обучение	$\tilde{r}^*_{У_{633}} = 0.1$

Продолжение таблицы 3.5

$У_7$ - **Неправильная оценка ситуации и ошибки управления дежурным ПЦО**		
$r_{У_71}$ – Качество телефонной связи между оператором РСПИ и дежурным ПЦО $\tilde{r}_{У_71}$= 0.15	$r^*_{У_711}$ – Удовлетворительное	$\tilde{\tilde{r}}^*_{У_711} = 0.2$
	$r^*_{У_712}$ – Неудовлетворительное	$\tilde{\tilde{r}}^*_{У_712} = 0.8$
$r_{У_72}$ – Интенсивность работы дежурного ПЦО $\tilde{r}_{У_72}$= 0.37	$r^*_{У_721}$ – Очень высокая нагрузка (более 100 тревожных сообщений в сутки)	$\tilde{\tilde{r}}^*_{У_721} = 0.8$
	$r^*_{У_722}$ – Высокая нагрузка (более 60 тревожных сообщений в сутки)	$\tilde{\tilde{r}}^*_{У_722} = 0.5$
	$r^*_{У_723}$ – Средняя нагрузка (от 20 до 60 тревожных сообщений в сутки)	$\tilde{\tilde{r}}^*_{У_723} = 0.1$
$r_{У_73}$ – Наличие визуального контакта и возможность непосредственной акустической связи между оператором РСПИ и дежурным ПЦО $\tilde{r}_{У_73}$= 0.09	$r^*_{У_731}$ – Не имеется	$\tilde{\tilde{r}}^*_{У_731} = 1$
$r_{У_74}$ – Наличие на ПЦО посторонних бытовых средств аудио и видеоаппаратуры, отвлекающих внимание операторов и дежурного ПЦО $\tilde{r}_{У_74}$= 0.07	$r^*_{У_741}$ –имеются	$\tilde{\tilde{r}}^*_{У_741} = 1$
$r_{У_75}$ – Удаленность ГЗ за пределами зоны связи или нахождение ГЗ в «мертвой зоне» $\tilde{r}_{У_75}$= 0.12	$r^*_{У_751}$ – Объект в зоне неуверенного приема	$\tilde{\tilde{r}}^*_{У_751} = 0.7$
	$r^*_{У_752}$ – Объект вне зоны действия радиостанции ПЦО	$\tilde{\tilde{r}}^*_{У_752} = 1$
$r_{У_76}$ – Наличие у ГЗ средств определения их местоположения на электронной карте у дежурного ПЦО $\tilde{r}_{У_76}$= 0.11	$r^*_{У_761}$ – Не имеются	$\tilde{\tilde{r}}^*_{У_761} = 1$

Продолжение таблицы 3.5

$r_{У_7 7}$ – Возможность использования резервных частот или ретранслятора. Наличие дублирующего канала связи $\tilde{r}_{У_7 7}$= 0.09	$r^*_{У_7 71}$ – Не имеется возможность использования резервных частот или ретранслятора	$\tilde{\tilde{r}}^*_{У_7 71} = 0.7$
	$r^*_{У_7 72}$ – Не имеется возможность использования резервных частот или ретранслятора и нет дублирующего канала связи	$\tilde{\tilde{r}}^*_{У_7 72} = 1$
	$r^*_{У_7 73}$ – Нет дублирующего канала связи	$\tilde{\tilde{r}}^*_{У_7 73} = 0.4$
$У_8$ - В БД хранится информация разной степени конфиденциальности		
$r_{У_8 1}$ – Способ хранения информации $\tilde{r}_{У_8 1}$= 0.05	$r^*_{У_8 11}$ – Вся информация хранится централизованно на данном устройстве	$\tilde{\tilde{r}}^*_{У_8 11} = 1$
$r_{У_8 2}$ – Логическое разделение информации $\tilde{r}_{У_8 2} = 0.19$	$r^*_{У_8 21}$ – Нет разделения информации по степени конфиденциальности	$\tilde{\tilde{r}}^*_{У_8 21} = 0.8$
	$r^*_{У_8 22}$ – Нет разделения информации	$\tilde{\tilde{r}}^*_{У_8 22} = 0.5$
	$r^*_{У_8 23}$ – Нет разделения информации по степени конфиденциальности и по типу	$\tilde{\tilde{r}}^*_{У_8 23} = 1$
$rh_{У_8 3}$ – Система хранения информации $\tilde{r}_{У_8 3}$= 0.21	$r^*_{У_8 31}$ – Для хранения информации используется ftp-сервер	$\tilde{\tilde{r}}^*_{У_8 31} = 0.5$
	$r^*_{У_8 32}$ – Для хранения информации используются сетевые папки	$\tilde{\tilde{r}}^*_{У_8 32} = 0.7$
	$r^*_{У_8 33}$ – Для хранения информации используются локальные папки	$\tilde{\tilde{r}}^*_{У_8 33} = 0.7$
$r_{У_8 4}$ – Тип устройства хранения $\tilde{r}_{У_8 4}$= 0.22	$r^*_{У_8 41}$ – Данные хранятся на неспециализированном оборудовании (например, на рабочей станции)	$\tilde{\tilde{r}}^*_{У_8 41} = 1$
$r_{У_8 5}$ – Ответственное лицо, контролирующее процесс хранения информации $\tilde{r}_{У_8 5}$= 0.33	$r^*_{У_8 51}$ – Нет ответственного лица, контролирующего процесс хранения информации	$\tilde{\tilde{r}}^*_{У_8 51} = 0.4$
$У_9$ - Некорректные должностные инструкции / неопределённость ответственности за нарушения ПИБ		
$r_{У_9 1}$ – Должностные инструкции отсутствуют или давно не обновлялись $\tilde{r}_{У_9 1}$= 0.30	$r^*_{У_9 11}$ – Должностные инструкции отсутствуют	$\tilde{\tilde{r}}^*_{У_9 11} = 0.8$
	$r^*_{У_9 12}$ – Должностные инструкции имеются, но составлены формально, без привязки к политике информационной безопасности	$\tilde{\tilde{r}}^*_{У_9 12} = 0.5$
	$r^*_{У_9 13}$ – Должностные инструкции давно не обновлялись	$\tilde{\tilde{r}}^*_{У_9 13} = 0.2$

Продолжение таблицы 3.5

$r_{\text{у}_9 2}$ – Политика ИБ $\tilde{r}_{\text{у}_9 2}$= 0.70	$r^*_{\text{у}_9 21}$ – Отсутствует политика информационной безопасности	$\widetilde{r^*}_{\text{у}_9 21} = 1$
У_{10} - Отсутствие/неполный контроль за выполнением требований разграничения доступа		
$r_{\text{у}_{10} 1}$ – Журнал учета доступа к данным $\tilde{r}_{\text{у}_{10} 1}$= 0.50	$r^*_{\text{у}_{10} 11}$ – Журнал учета доступа к данным не ведется	$\widetilde{r^*}_{\text{у}_{10} 11} = 1$
	$r^*_{\text{у}_{10} 12}$ – Журнал учета доступа к данным ведется формально	$\widetilde{r^*}_{\text{у}_{10} 12} = 0.5$
	$r^*_{\text{у}_{10} 13}$ – Установлен комплекс для контроля за разграничением доступа, но автоматическое заполнение журнала не производится	$\widetilde{r^*}_{\text{у}_{10} 13} = 0.7$
$r_{\text{у}_{10} 2}$ – Администратор не получает уведомления от системы разграничения доступа $\tilde{r}_{\text{у}_{10} 2}$= 0.50	$r^*_{\text{у}_{10} 21}$ – Не проводятся периодические проверки требований разграничения доступа	$\widetilde{r^*}_{\text{у}_{10} 21} = 0.7$
	$r^*_{\text{у}_{10} 22}$ – Установлен комплекс для контроля за разграничением доступа, но автоматическое оповещение не производится	$\widetilde{r^*}_{\text{у}_{10} 22} = 0.7$
У_{11} - Для информационного обмена используются нерегламентированные технические средства		
$r_{\text{у}_{11} 1}$ – Существует действующий регламент использования технических средств обработки информации $\tilde{r}_{\text{у}_{11} 1}$=1	$r^*_{\text{у}_{11} 11}$ – Не имеется	$\widetilde{r^*}_{\text{у}_{11} 11} = 1$
	$r^*_{\text{у}_{11} 12}$ – Неполный контроль за соблюдением порядка информационного обмена	$\widetilde{r^*}_{\text{у}_{11} 12} = 0.5$
У_{12} - Терминалы оставляются без присмотра в рабочие и нерабочие часы. Данные отображаются на компьютерных экранах, оставленных без присмотра		
$r_{\text{у}_{12} 1}$ – Физический доступ несанкционированных пользователей к терминалам $\tilde{r}_{\text{у}_{12} 1}$= 0.58	$r^*_{\text{у}_{12} 11}$ – Имеется	$\widetilde{r^*}_{\text{у}_{12} 11} = 1$

Продолжение таблицы 3.5

$r_{y_{12}2}$ – Функция автоматического выключения монитора $\tilde{r}_{y_{12}2}$= 0.42	$r^*_{y_{12}21}$ – На терминалах не настроена функция автоматического выключения монитора. Установлен комплекс для контроля за разграничением доступа, но автоматическое оповещение не производится	$\tilde{r}^*_{y_{12}21} = 1$
	$r^*_{y_{12}22}$ – Сотрудники покидают терминалы, не выключив свою учетную запись, имеется функция автоматического выключения монитора	$\tilde{r}^*_{y_{12}22} = 0.7$
$У_{13}$ - Изменения в программы АРМов вносятся без их предварительного утверждения		
$r_{y_{13}1}$ – Документация по разработке и модификации ПО $\tilde{r}_{y_{13}1}$= 0.27	$r^*_{y_{13}11}$ – Отсутствует регламент по разработке программного обеспечения	$\tilde{r}^*_{y_{13}11} = 0.4$
	$r^*_{y_{13}12}$ – Документация по разработке / модификации программного обеспечения не ведется	$\tilde{r}^*_{y_{13}12} = 0.7$
$r_{y_{13}2}$ – Защита исходного кода $\tilde{r}_{y_{13}2}$= 0.28	$r^*_{y_{13}21}$ – Не используется специальное ПО для защиты исходного кода при разработке	$\tilde{r}^*_{y_{13}21} = 0.5$
$r_{y_{13}3}$ – Руководство не контролирует деятельность программистов $\tilde{r}_{y_{13}3}$= 0.44	$r^*_{y_{13}31}$ – Контроль не ведется	$\tilde{r}^*_{y_{13}31} = 1$
	$r^*_{y_{13}32}$ – Контроль ведется периодически	$\tilde{r}^*_{y_{13}32} = 0.5$
$У_{14}$ - Имеют место выходы из строя операционной системы (по неизвестным причинам)		
$r_{y_{14}1}$ – Операционная система периодически зависает $\tilde{r}_{y_{14}1}$= 0.60	$r^*_{y_{14}11}$ – Система часто выходит из строя, долго не приходит в нормальное состояние	$\tilde{r}^*_{y_{14}11} = 1$
	$r^*_{y_{14}12}$ – Система очень редко выходит из строя но через некоторое время приходит в норму	$\tilde{r}^*_{y_{14}12} = 0.5$
$r_{y_{14}2}$ – Ошибки настройки (конфигурирования) операционной системы $\tilde{r}_{y_{14}2}$= 0.40	$r^*_{y_{14}21}$ – Низкая квалификация системного администратора	$\tilde{r}^*_{y_{14}21} = 0.7$
	$r^*_{y_{14}22}$ – Ошибки не вызваны объективными причинами	$\tilde{r}^*_{y_{14}22} = 0.5$

Окончание таблицы 3.5

$У_{15}$ - **Диски/другие носители оставляются в ящиках столов, не делается архивных копий дисков/других носителей**		
$r_{У_{15}1}$ – Специальные ящики в столах сотрудников с запорным устройством для хранения съемных носителей $\tilde{r}_{У_{15}1}$= 0.18	$r^*_{У_{15}11}$ – Не имеются	$\widetilde{r^*}_{У_{15}11} = 1$
$r_{У_{15}2}$ – Архивные копии дисков/других носителей $\tilde{r}_{У_{15}2}$= 0.52	$p_{У_{15}21}$ – Архивные копии не создаются автоматически при помощи специального программного обеспечения	$\widetilde{r^*}_{У_{15}21} = 1$
$r_{У_{15}3}$ – Регламент по организации хранения съемных носителей информации и резервному копированию $\tilde{r}_{У_{15}3}$= 0.12	$r^*_{У_{15}31}$ – Не существует	$\widetilde{r^*}_{У_{15}31} = 1$
	$r^*_{У_{15}32}$ – Составлен формально	$\widetilde{r^*}_{У_{15}32} = 0.5$
$r_{У_{15}4}$ – Порядок доступа посетителей в помещения с компьютерами $\tilde{r}_{У_{15}4}$= 0.18	$r^*_{У_{15}41}$ – Не регламентирован	$\widetilde{r^*}_{У_{15}41} = 1$
$У_{16}$ - **Конфигурация аппаратных средств не соответствует предъявляемым требованиям**		
$r_{У_{16}1}$ – Аппаратные средства $\tilde{r}_{У_{16}1}$=1	$r^*_{У_{16}11}$ – Не выдают требуемой производительности	$\widetilde{r^*}_{У_{16}11} = 0.7$
	$r^*_{У_{16}12}$ – Удовлетворительные, не выдают требуемой производительности, срок эксплуатации от 5 до 8 лет	$\widetilde{r^*}_{У_{16}12} = 0.5$
	$r^*_{У_{16}13}$ – Не удовлетворительные , часто выходят из строя срок эксплуатации более 8 лет	$\widetilde{r^*}_{У_{16}13} = 1$

Степень проявления f-й уязвимости определим по формуле:

$$s_{У_f} = \sum_{u_f=1}^{U_f} \tilde{r}_{У_f u_f} \widetilde{r^*}_{У_f u_f q(u_f)}. \quad (3.5)$$

Для наглядности представим описанную выше модель идентификации уязвимостей для одного *d*-го компонента и одной уязвимости $У_f$ в виде дерева,

где вершины - уязвимость, идентификационные признаки и параметры, характеризующие степень проявления идентификационных признаков уязвимости. Корень дерева – единица оборудования - компонент ТКС ЦОО (обозначена *d*).

Вершины: идентификационные признаки уязвимости $У_f$ - $r_{У_f1}$, $r_{У_f2}$; параметры, характеризующие степень проявления идентификационных признаков уязвимости - $r^*_{У_1 11}$, $r^*_{У_1 12}$, $r^*_{У_1 21}$, $r^*_{У_1 22}$ и $r^*_{У_1 23}$.

Отношения между сущностями представляются ребрами, соединяющими соответствующие вершины. Ребра снабжены весами: ребро между компонентом и уязвимостью имеют вес $S_{У_f}$; ребра между уязвимостью и идентификационными признаками имеют веса $\tilde{r}_{У_f1}$ и $\tilde{r}_{У_f2}$; ребра между признаками и параметрами, характеризующими степени проявления идентификационных признаков уязвимости имеют веса $\tilde{r}^*_{У_1 11}$, $\tilde{r}^*_{У_1 12}$, $\tilde{r}^*_{У_1 21}$, $\tilde{r}^*_{У_1 22}$ и $\tilde{r}^*_{У_1 23}$. Дерево представлено на рисунке 3.1.

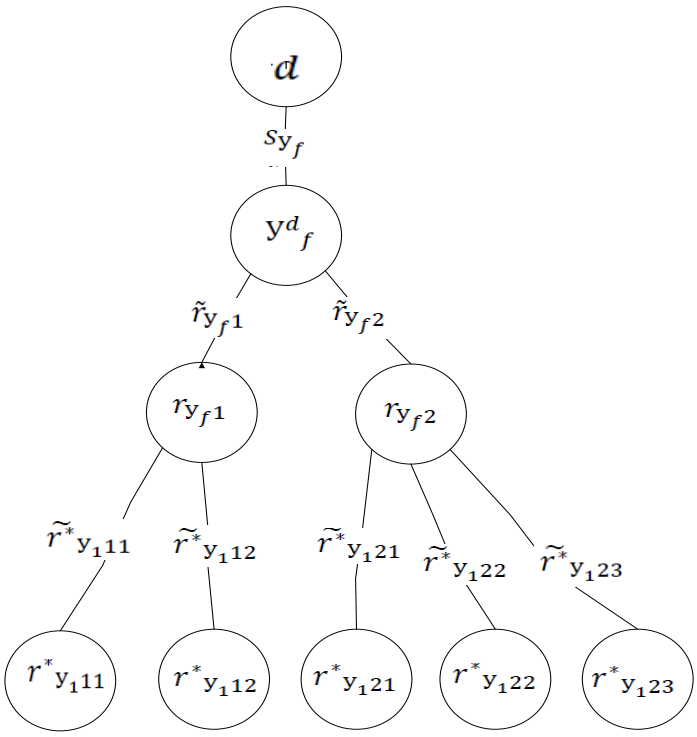

Рисунок 3.1 – Упрощенное представление разработанной модели идентификации уязвимостей в виде дерева

Алгоритм проявления уязвимостей d-го компонента

Алгоритм 3.1

Исходные данные:

1. множество потенциально возможных уязвимостей $\text{У}^d = \{\text{У}^d{}_1, \dots, \text{У}^d{}_f, \dots, \text{У}^d_{F_d}\}$, где $F_d \in F$.

2. Для каждой $\text{У}^d{}_f$ имеются $r_{f_d} \in R$ признаков. (R - множество всех возможных идентификационных признаков уязвимостей).

3. $s\text{У}_{f_{\text{ПОР}}}$ (минимально возможное проявление)

Шаг 1. $f = 1$. Начинаем с первой уязвимости.

Шаг 2. Пронумеруем элементы подмножества идентификационных признаков f-й уязвимости компонента $r\text{У}_f = \{r\text{У}_f 1, \dots, r\text{У}_f u_f, \dots, r\text{У}_f U_f\}$.

Шаг 3. Введем категорию – «вес» (важность) признака $\tilde{r}\text{У}_f u_f \in [0,1]$, (определен экспертами, $\sum_{u_f=1}^{U_f} \tilde{r}\text{У}_f u_f = 1$).

Шаг 4. Введем множество $r^*\text{У}_f u_f$ взаимоисключающих качественных параметров, характеризующих степень проявления u_f-го идентификационного признака f-й уязвимости: $r^*\text{У}_f u_f = \{r^*\text{У}_f u_f 1, \dots, r^*\text{У}_f u_f q(u_f), \dots, r^*\text{У}_f u_f Q(u_f)\}$. Качественной оценке сопоставим количественный эквивалент - $\widetilde{r^*}\text{У}_f u_f q(u_f) \in [0,1]$, $\widetilde{r^*}\text{У}_f u_f q(u_f)$ определяется экспертами по вкладу элемента в значение признака.

Шаг 5. Степень проявления f-й уязвимости определим по формуле $s\text{У}_f = \sum_{u_f=1}^{U_f} \tilde{r}\text{У}_f u_f \widetilde{r^*}\text{У}_f u_f q(u_f)$.

Шаг 6. Если $s\text{У}_f < s\text{У}_{f_{\text{ПОР}}}$ то $s\text{У}_f = 0$ (уязвимость отсутствует).

Если $f = F_d$ то конец алгоритма, иначе $f = f + 1$, перейти к шагу 2.

3.3 Защитные механизмы ТКС ЦОО

Концепция обеспечения ИБ ТКС ЦОО должна удовлетворять следующей совокупности требований:

- должны существовать методы защиты гарантированного обеспечения требуемого уровня безопасности;

- должны быть определены способы практической реализации выбранного метода (или совокупности методов) защиты;

- необходимо располагать средствами реализации всех необходимых мероприятий по ЗИ.

Под методом (стратегией, функцией) защиты понимается совокупность однородных в функциональном отношении мероприятий и способов, регулярно осуществляемых в ТКС ЦОО различными средствами с целью обеспечения условий, необходимых для обеспечения заданного уровня ИБ. К таким методам, как правило, относят:

1) предупреждение условий возникновения дестабилизирующих факторов (ДФ);

2) предупреждение непосредственного проявления ДФ;

3) обнаружение проявившихся ДФ;

4) предупреждение воздействия на защищаемую информацию ДФ;

5) обнаружение воздействия ДФ на информацию;

б) ограничение воздействия ДФ на информацию;

7) ликвидация последствий локализованного обнаруженного воздействия ДФ на информацию.

Под способами защиты (далее защитными механизмами обеспечения ИБ) понимаются организованные возможности средств и мероприятий, осуществляемых в ТКС ЦОО с целью полной или частичной реализации одного или нескольких методов (стратегий, функций) защиты.

Основными требованиями, предъявляемыми к множеству защитных механизмов, являются репрезентативность и реализуемость. Под репрезентативностью понимается достаточность их для обеспечения требуемого уровня эффективности осуществления методов защиты, а под реализуемостью - возможность реализации имеющимися техническими средствами и организационно-техническими мероприятиями (далее «Средства» - СР).

Перечислим защитные механизмы обеспечения ИБ, характерные для ТКС ЦОО:

1) Обеспечение требований по условиям эксплуатации ТСО.
2) Обеспечение штатного функционирования ТСО.
3) Контроль работы оператора ИСБ.
4) Обеспечение требований по условиям эксплуатации РСПИ.
5) Контроль и обеспечение штатного функционирования объектовых блоков РСПИ.
6) Обеспечение штатного функционирования ЛВС ПЦО.
7) Обеспечение штатного функционирования АРМ РСПИ.
8) Обеспечение штатной работы операторов АРМ РСПИ.
9) Обеспечение штатной работы дежурных ПЦО.
10) Обеспечение штатной передачи информации от дежурных ПЦО нарядам охраны.
11) Обеспечение штатной работы нарядов физической охраны.
12) Обеспечение ИБ на ПЦО.

Весьма сложной и практически нерешенной является проблема оценки эффективности осуществления одного или нескольких методов применением того или иного защитного механизма или их совокупностью. Ввиду большого влияния случайных факторов наиболее подходящими для этих целей, очевидно, являются различные неформальные методы оценивания.

Представим множество защитных механизмов (ЗМ)

$$ЗМ = \{ЗМ_1, \dots, ЗМ_h, \dots, ЗМ_H\}. \quad (3.6)$$

Множество ЗМ представим в виде объединения подмножеств защитных механизмов, «присущих» компонентам ТКС ЦОО

$$ЗМ = ЗМ^1 \cup ЗМ^2 \cup \ldots \cup ЗМ^d \cup \ldots \cup ЗМ^D. \quad (3.7)$$

Заметим, что отдельные ЗМ вида $ЗМ^d{}_h$ могут встречаться в разных компонентах. В дальнейшем для простоты будем считать, что конкретные ЗМ «закрепляются» за «своими» компонентами. Так для d-го компонента пронумерованное множество ЗМ представим в виде:

$$ЗМ^d = \{ЗМ^d{}_1, \ldots, ЗМ^d{}_h, \ldots, ЗМ^d_{H_d}\}, \quad (3.8)$$

где $H_d \in H$.

Далее рассматриваем ЗМ одного (d-го) компонента ТКС ЦОО.

Каждый защитный механизм может быть реализован разными средствами и мероприятиями. Например, ЗМ «Обеспечение штатного функционирования ТСО» может быть реализован девятью разнообразными средствами и мероприятиями:

1) эксплуатационно-техническим обслуживанием с соблюдением всех сроков и объемов;

2) обеспечением технического сопровождения монтажа ТСО и входным контролем аппаратуры ТСО;

3) монтажом проводов средств ТСО скрытым способом;

4) заземлением ТСО;

5) защитой от НСД щитов ТСО, коммутационных изделий и АРМ ИСБ;

6) своевременным ремонтом и недопущением превышений сроков эксплуатации ТСО;

7) обучением электромонтеров и персонала ПЦО и собственников объектов, эксплуатирующих ТСО;

8) наличием обменного фонда ТСО;

9) использованием вандалозащищенных извещателей и средств ТСО и извещателей раннего обнаружения.

3.4 Сила защитного механизма

Предполагаем, что один и тот же защитный механизм, находясь в разных компонентах и в разных условиях функционирования, может проявляться более или менее, защищать компонент с разной «силой». Такой качественной оценке сопоставим количественный эквивалент:

$$w_{\text{ЗМ}_h} \in [0,1], \qquad 3.9$$

где $w_{\text{ЗМ}_h}$ - сила (степень проявления) h-го защитного механизма.

$w_{\text{ЗМ}_h}$ показывает, какая часть максимально возможной силы h-го защитного механизма, характеризующейся множеством технических средств и организационно-технических мероприятий (СР) его (механизма) конкретной реализации в ТКС ЦОО, реально защищает компонент ($\text{СР}_{\text{ЗМ}_h} = \{\text{СР}_{\text{ЗМ}_h 1}, \dots, \text{СР}_{\text{ЗМ}_h z_h}, \dots, \text{СР}_{\text{ЗМ}_h Z_h}\}$).

Полный перечень защитных механизмов и соответствующих им технических средств и организационно-технических мероприятий приведен в таблице 3.6.

Таблица 3.6 - Перечень защитных механизмов и соответствующих им технических средств и организационно-технических мероприятий

Наименование и обозначение ЗМ	Информационный процесс (компоненты), ОФ	Обозначение и наименование технических средств и организационно-технических мероприятий
Обеспечение требований по условиям эксплуатации ТСО ЗМ_1	ИП 1 (ОИ ОТС, КАДПЛ, АРМ ИСБ), ОФ1	$\text{СР}_{\text{ЗМ}_1 1}$ – Выполнение требований по климатическим условиям эксплуатации, поддержание необходимой температуры, влажности и пр.
		$\text{СР}_{\text{ЗМ}_1 2}$ – Выполнение требований монтажа ТСО, недопустимость воздействия на средства ТСО дестабилизирующих факторов
		$\text{СР}_{\text{ЗМ}_1 3}$ – Своевременное и качественное обследование охраняемых объектов

Продолжение таблицы 3.6

Обеспечение штатного функционирования ТСО $ЗМ_2$	ИП 1 (ОИ ОТС, КАДПЛ, АРМ ИСБ), ИП3 (АРМ ИСБ, РМ ОТС), ОФ1, ОФ3	$СР_{ЗМ_21}$ – Наличие эксплуатационно-технического обслуживания с соблюдением всех сроков и объемов
		$СР_{ЗМ_22}$ – Обеспечение технического сопровождения монтажа ТСО и 100% входного контроля аппаратуры ТСО
		$СР_{ЗМ_23}$ – Обеспечение монтажа проводов средств ТСО скрытым способом
		$СР_{ЗМ_24}$ – Обязательное заземление ТСО
		$СР_{ЗМ_25}$ – Обеспечение защиты от НСД щитов ТСО, коммутационных изделий и АРМ ИСБ
		$СР_{ЗМ_26}$ – Своевременный ремонт и не допущение превышений сроков эксплуатации ТСО
		$СР_{ЗМ_27}$ – Обучение электромонтеров и персонала ПЦО и собственников объектов, эксплуатирующих ТСО
		$СР_{ЗМ_28}$ – Наличие и использование обменного фонда ТСО
		$СР_{ЗМ_29}$ – Использование вандалозащищщенных извещателей и средств ТСО и извещателей раннего обнаружения
Контроль работы оператора ИСБ $ЗМ_3$	ИП 2 (АРМ ИСБ), ОФ2, ОФ3	$СР_{ЗМ_31}$ – Проверка состояния персонала перед работой
		$СР_{ЗМ_32}$ –Недопущения суточных режимов работы и переутомления персонала
		$СР_{ЗМ_33}$ –Постоянный гласный и негласный контроль за работой персонала
		$СР_{ЗМ_34}$ –Создание оперативного резерва для замены персонала
		$СР_{ЗМ_35}$ –Индивидуально-воспитательная работа с персоналом объекта
		$СР_{ЗМ_36}$ –Тестирование, в т.ч. и психологическое при подборе персонала
		$СР_{ЗМ_37}$ –Регламентное обслуживание АРМ ИСБ

Продолжение таблицы 3.6

Обеспечение требований по условиям эксплуатации РСПИ $ЗМ_4$	ИП 4 (РМ ОТС, ОПП РСПИ, ЦПП РСПИ), ОФ3-ОФ5	$СР_{ЗМ_41}$ – Не допущение действия дестабилизирующих факторов на объектовые и пультовые блоки РСПИ
		$СР_{ЗМ_42}$ – Выбор частот в соответствии с электромагнитно обстановкой на объекте
		$СР_{ЗМ_43}$ – Правильный монтаж антенн объектовых блоков РСПИ, контроль программирования объектовых блоков РСПИ
		$СР_{ЗМ_44}$ – Обеспечение электромагнитной совместимости на объекте
Контроль и обеспечение штатного функционирования объектовых блоков РСПИ $ЗМ_5$	ИП 4 (РМ ОТС, ОПП РСПИ, ЦПП РСПИ), ИП 5 (ЦПП РСПИ, АРМ РСПИ (оператора ПЦО), Сервер БД, ЛВС), ОФ3-ОФ8	$СР_{ЗМ_51}$ – Правильный выбор типа использованной модуляции в РСПИ
		$СР_{ЗМ_52}$ –Правильный выбор формата передачи информации в РСПИ
		$СР_{ЗМ_53}$ –Наличие криптозащиты в канале передачи
		$СР_{ЗМ_54}$ –Вандалозащищенность объектового блока РСПИ
Обеспечение штатного функционирования ЛВС ПЦО $ЗМ_6$	ИП5 (ЦПП РСПИ, АРМ РСПИ (оператора ПЦО), Сервер БД, ЛВС), ИП6 (АРМ РСПИ (оператора ПЦО), АРМ дежурного ПЦО, АТС, ЛВС), ИП7 (АРМ дежурного ПЦО, УКВ радиостанция, ЛВС), ОФ6-ОФ10	$СР_{ЗМ_61}$ –Недопущение НСД к ЛВС ПЦО
		$СР_{ЗМ_62}$ –Наличие политики ИБ в организации и соблюдение политики ИБ
		$СР_{ЗМ_63}$ –Аппаратные средства ЛВС, их технические характеристики
		$СР_{ЗМ_64}$ –Защита **в**ыхода в глобальные сети, использование защищенных протоколов и VPN
		$СР_{ЗМ_65}$ –Наличие сетевых экранов и качество их программирования и настройки
		$СР_{ЗМ_66}$ –Наличие антивирусных средств защиты и периодичность их обновления
		$СР_{ЗМ_67}$ –Использование криптозащищённых протоколов
		$СР_{ЗМ_68}$ –Постоянное повышение **у**ровня профессиональной подготовки операторов и администраторов ЛВС ПЦО
		$СР_{ЗМ_69}$ –Проведение ЛВС скрытым способом и не использование в ЛВС средств Wi-Fi

Продолжение таблицы 3.6

Обеспечение штатного функционирования АРМ РСПИ $ЗМ_7$	ИП5 (ЦПП РСПИ, АРМ РСПИ (оператора ПЦО), Сервер БД, ЛВС), ИП6 (АРМ РСПИ (оператора ПЦО), АРМ дежурного ПЦО, АТС, ЛВС), ОФ6-ОФ9	$СР_{ЗМ_71}$ – Обучение электромонтеров и персонала ПЦО и собственников объектов, эксплуатирующих ТСО
		$СР_{ЗМ_72}$ – Недопущение НСД к АРМ РСПИ
		$СР_{ЗМ_73}$ – Наличие и использование обменного фонда ТСО
		$СР_{ЗМ_74}$ – Наличие сертификатов и лицензий на ПО, рекомендации и разрешений на ПО от руководящих организаций
		$СР_{ЗМ_75}$ – Обеспечение качественного отображения акустической или визуальной информации на экране ПК
Обеспечение штатной работы операторов АРМ РСПИ $ЗМ_8$	ИП5 (ЦПП РСПИ, АРМ РСПИ (оператора ПЦО), Сервер БД, ЛВС), ИП6 (АРМ РСПИ (оператора ПЦО), АРМ дежурного ПЦО, АТС, ЛВС), ИП7 (АРМ дежурного ПЦО, УКВ радиостанция, ЛВС), ОФ6-ОФ10	$СР_{ЗМ_81}$ – Проверка состояния персонала перед работой
		$СР_{ЗМ_82}$ – Недопущения суточных режимов работы и переутомления персонала
		$СР_{ЗМ_83}$ – Постоянный гласный и негласный контроль за работой персонала
		$СР_{ЗМ_84}$ – Создание оперативного резерва для замены персонала
		$СР_{ЗМ_85}$ – Индивидуально-воспитательная работа с персоналом объекта
		$СР_{ЗМ_86}$ – Тестирование, в т.ч. и психологическое при подборе персонала
		$СР_{ЗМ_87}$ – Недопущение высокой загруженности операторов АРМ (очень большое количество охраняемых объектов)
		$СР_{ЗМ_88}$ – Обеспечение четкой регламентации и организации работы операторов АРМ ДПУ (нечеткие должностные инструкции)
		$СР_{ЗМ_89}$ – Обеспечение высокого уровня гласного и негласного контроля работы операторов АРМ со стороны руководства ПЦО, установка средств аудиозаписи переговоров и видеокамер в зале ПЦО
		$СР_{ЗМ_810}$ – Недопущение выхода тлф. линий за пределы ПЦО (использование внутренней АТС ПЦО)
		$СР_{ЗМ_811}$ – Обеспечение прямой связи между оператором РСПИ и дежурным ПЦО или резервного канала связи
		$СР_{ЗМ_812}$ – Обеспечение визуального контакта и возможности непосредственной акустической связи между оператором РСПИ и дежурным ПЦО

Продолжение таблицы 3.6

Обеспечение штатной работы дежурных ПЦО $ЗМ_9$	ИП6 (АРМ РСПИ (оператора ПЦО), АРМ дежурного ПЦО, АТС, ЛВС), ИП7 (АРМ дежурного ПЦО, УКВ радиостанция, ЛВС), ОФ8, ОФ9	$СР_{ЗМ_91}$ – Обучение дежурных ПЦО
		$СР_{ЗМ_92}$ – Проверка состояния дежурных ПЦО перед работой
		$СР_{ЗМ_93}$ – Недопущения суточных режимов работы и переутомления дежурных ПЦО
		$СР_{ЗМ_94}$ – Постоянный гласный и негласный контроль за работой дежурных ПЦО
		$СР_{ЗМ_95}$ – Создание оперативного резерва для замены дежурных ПЦО
		$СР_{ЗМ_96}$ – Индивидуально-воспитательная работа с дежурных ПЦО
		$СР_{ЗМ_97}$ – Тестирование, в т.ч. и психологическое при подборе дежурных ПЦО
		$СР_{ЗМ_98}$ – Недопущение высокой загруженности дежурных ПЦО (очень большое количество охраняемых объектов)
		$СР_{ЗМ_99}$ – Обеспечение четкой регламентации и организации работы дежурных ПЦО (нечеткие должностные инструкции)
		$СР_{ЗМ_910}$ – Обеспечение высокого уровня гласного и негласного контроля работы дежурных ПЦО со стороны руководства ПЦО, установка средств аудиозаписи переговоров и видеокамер в зале ПЦО
Обеспечение штатной передачи информации от дежурных ПЦО нарядам охраны $ЗМ_{10}$	ИП6 (АРМ РСПИ (оператора ПЦО), АРМ дежурного ПЦО, АТС, ЛВС), ИП7 (АРМ дежурного ПЦО, УКВ радиостанция, ЛВС), ИП8 (УКВ радиостанция, РС ГЗ), ОФ8-ОФ15	$СР_{ЗМ_{10}1}$ – Обеспечение постоянной исправности и резервирования средств радиосвязи, комплекса мероприятий по эксплуатационному обслуживанию средств связи
		$СР_{ЗМ_{10}2}$ – Контроль электромагнитной обстановки
		$СР_{ЗМ_{10}3}$ – Вандалозащищенность средств связи и антенн средств связи, недопущение к ним посторонних лиц
		$СР_{ЗМ_{10}4}$ – Планирование дисклокации маршрутов ГЗ с учетом обеспечения качественно связи
		$СР_{ЗМ_{10}5}$ – Обеспечение возможности использования резервных частот и ретрансляторов
		$СР_{ЗМ_{10}6}$ – Обеспечение автоматической проверки на р/ст качества связи
		$СР_{ЗМ_{10}7}$ – Наличие дублирующих каналов связи и современных помехозащищенных видов модуляции
		$СР_{ЗМ_{10}8}$ – Наличие скремблерных средств защиты информации в радиоканале
		$СР_{ЗМ_{10}9}$ – Наличие криптографических средств защиты информации в радиоканале

Окончание таблицы 3.6

Обеспечение штатной работы нарядов физической охраны $ЗМ_{11}$	ИП8 (УКВ радиостанция, РС ГЗ), ОФ11-ОФ15	$СР_{ЗМ_{11}1}$ – Обучение наряда ГЗ
		$СР_{ЗМ_{11}2}$ – Проверка состояния наряда ГЗ перед работой
		$СР_{ЗМ_{11}3}$ – Недопущения суточных режимов работы и переутомления наряда ГЗ
		$СР_{ЗМ_{11}4}$ – Постоянный гласный и негласный контроль за работой наряда ГЗ
		$СР_{ЗМ_{11}5}$ – Создание оперативного резерва для замены наряда ГЗ
		$СР_{ЗМ_{11}6}$ – Индивидуально-воспитательная работа с нарядом ГЗ
		$СР_{ЗМ_{11}7}$ – Тестирование, в т.ч. и психологическое при подборе наряда ГЗ
		$СР_{ЗМ_{11}8}$ – Недопущение высокой загруженности наряда ГЗ (очень большое количество охраняемых объектов)
		$СР_{ЗМ_{11}9}$ – Обеспечение четкой регламентации и организации работы наряда ГЗ (нечеткие должностные инструкции)
		$СР_{ЗМ_{11}10}$ – Обеспечение высокого уровня гласного и негласного контроля работы наряда ГЗ со стороны руководства ПЦО, установка средств аудиозаписи переговоров и видеокамер в зале ПЦО
Обеспечение ИБ на ПЦО $ЗМ_{12}$	ИП5 (ЦПП РСПИ, АРМ РСПИ (оператора ПЦО), Сервер БД, ЛВС), ИП6 (АРМ РСПИ (оператора ПЦО), АРМ дежурного ПЦО, АТС, ЛВС), ИП7 (АРМ дежурного ПЦО, УКВ радиостанция, ЛВС), ОФ6-ОФ10	$СР_{ЗМ_{12}1}$ – Выполнение требований политики ИБ
		$СР_{ЗМ_{12}2}$ – Выполнение требований разграничение доступа ИР на ПЦО
		$СР_{ЗМ_{12}3}$ – Выполнение требований по хранению носителей
		$СР_{ЗМ_{12}4}$ – Выполнение требований по резервированию критических ИР
		$СР_{ЗМ_{12}5}$ – Выполнение требований к аппаратной части ИС ПЦО
		$СР_{ЗМ_{12}6}$ – Выполнение требований по проведению аудита ИБ на ПЦО

Введем дополнительные параметры:

- параметр наличия / отсутствия элемента технических средств и организационно-технических мероприятий h-го защитного механизма $\zeta(\text{ЗМ}_h, z_h) = 1$, если $\text{СР}_{\text{ЗМ}_h z_h}$ «выявлен» при анализе ЗМ_h, иначе $\zeta(\text{ЗМ}_h, z_h) = 0$;

- вес (показатель важности) $\text{СР}_{\text{ЗМ}_h z_h}$ в h-м защитном механизме $\widetilde{w}(\text{ЗМ}_h, z_h) \in [0,1]$, при этом $\sum_{,z_h=1}^{Z_h} \widetilde{w}(\text{ЗМ}_h, z_h) = 1$.

Значение веса $\widetilde{w}(\text{ЗМ}_h, z_h)$ определяется экспертами.

При данном подходе сила защитного механизма

$$w_{\text{ЗМ}_h} = \sum_{z_h=1}^{Z_h} \widetilde{w}(\text{ЗМ}_h, z_h) * \zeta(\text{ЗМ}_h, z_h). \quad (3.10)$$

Результаты расчета весов (показатель важности) защитных механизмов сведены в таблицу 3.7.

Таблица 3.7 - Результаты расчета весов (показателей важности) защитных механизмов

ЗМ_h	$\text{СР}_{\text{ЗМ}_h z_h}$	$\widetilde{w}(\text{ЗМ}_h, z_h)$	ЗМ_h	$\text{СР}_{\text{ЗМ}_h z_h}$	$\widetilde{w}(\text{ЗМ}_h, z_h)$
ЗМ_1	$\text{СР}_{\text{ЗМ}_1 1}$	0.36	ЗМ_8	$\text{СР}_{\text{ЗМ}_8 1}$	0.10
	$\text{СР}_{\text{ЗМ}_1 2}$	0.36		$\text{СР}_{\text{ЗМ}_8 2}$	0.07
	$\text{СР}_{\text{ЗМ}_1 3}$	0.28		$\text{СР}_{\text{ЗМ}_8 3}$	0.10
ЗМ_2	$\text{СР}_{\text{ЗМ}_2 1}$	0.15		$\text{СР}_{\text{ЗМ}_8 4}$	0.07
	$\text{СР}_{\text{ЗМ}_2 2}$	0.08		$\text{СР}_{\text{ЗМ}_8 5}$	0.06
	$\text{СР}_{\text{ЗМ}_2 3}$	0.08		$\text{СР}_{\text{ЗМ}_8 6}$	0.08
	$\text{СР}_{\text{ЗМ}_2 4}$	0.08		$\text{СР}_{\text{ЗМ}_8 7}$	0.08
	$\text{СР}_{\text{ЗМ}_2 5}$	0.15		$\text{СР}_{\text{ЗМ}_8 8}$	0.09
	$\text{СР}_{\text{ЗМ}_2 6}$	0.13		$\text{СР}_{\text{ЗМ}_8 9}$	0.11
	$\text{СР}_{\text{ЗМ}_2 7}$	0.15		$\text{СР}_{\text{ЗМ}_8 10}$	0.10
	$\text{СР}_{\text{ЗМ}_2 8}$	0.10		$\text{СР}_{\text{ЗМ}_8 11}$	0.08
	$\text{СР}_{\text{ЗМ}_2 9}$	0.08		$\text{СР}_{\text{ЗМ}_8 12}$	0.06

Окончание таблицы 3.7

$ЗМ_3$	$СР_{ЗМ_3 1}$	0.12	$ЗМ_9$	$СР_{ЗМ_9 1}$	0.11
	$СР_{ЗМ_3 2}$	0.12		$СР_{ЗМ_9 2}$	0.08
	$СР_{ЗМ_3 3}$	0.23		$СР_{ЗМ_9 3}$	0.13
	$СР_{ЗМ_3 4}$	0.15		$СР_{ЗМ_9 4}$	0.10
	$СР_{ЗМ_3 5}$	0.12		$СР_{ЗМ_9 5}$	0.08
	$СР_{ЗМ_3 6}$	0.12		$СР_{ЗМ_9 6}$	0.07
	$СР_{ЗМ_3 7}$	0.14		$СР_{ЗМ_9 7}$	0.11
$ЗМ_4$	$СР_{ЗМ_4 1}$	0.20		$СР_{ЗМ_9 8}$	0.09
	$СР_{ЗМ_4 2}$	0.24		$СР_{ЗМ_9 9}$	0.11
	$СР_{ЗМ_4 3}$	0.24		$СР_{ЗМ_9 10}$	0.12
	$СР_{ЗМ_4 4}$	0.32	$ЗМ_{10}$	$СР_{ЗМ_{10} 1}$	0.14
$ЗМ_5$	$СР_{ЗМ_5 1}$	0.22		$СР_{ЗМ_{10} 2}$	0.12
	$СР_{ЗМ_5 2}$	0.28		$СР_{ЗМ_{10} 3}$	0.11
	$СР_{ЗМ_5 3}$	0.17		$СР_{ЗМ_{10} 4}$	0.13
	$СР_{ЗМ_5 4}$	0.33		$СР_{ЗМ_{10} 5}$	0.12
$ЗМ_6$	$СР_{ЗМ_6 1}$	0.12		$СР_{ЗМ_{10} 6}$	0.11
	$СР_{ЗМ_6 2}$	0.08		$СР_{ЗМ_{10} 7}$	0.13
	$СР_{ЗМ_6 3}$	0.12		$СР_{ЗМ_{10} 8}$	0.07
	$СР_{ЗМ_6 4}$	0.13		$СР_{ЗМ_{10} 9}$	0.07
	$СР_{ЗМ_6 5}$	0.07	$ЗМ_{11}$	$СР_{ЗМ_{11} 1}$	0.10
	$СР_{ЗМ_6 6}$	0.17		$СР_{ЗМ_{11} 2}$	0.11
	$СР_{ЗМ_6 7}$	0.10		$СР_{ЗМ_{11} 3}$	0.10
	$СР_{ЗМ_6 8}$	0.10		$СР_{ЗМ_{11} 4}$	0.10
	$СР_{ЗМ_6 9}$	0.11		$СР_{ЗМ_{11} 5}$	0.11
$ЗМ_7$	$СР_{ЗМ_7 1}$	0.14		$СР_{ЗМ_{11} 6}$	0.09
	$СР_{ЗМ_7 2}$	0.16		$СР_{ЗМ_{11} 7}$	0.09
	$СР_{ЗМ_7 3}$	0.22		$СР_{ЗМ_{11} 8}$	0.09
	$СР_{ЗМ_7 4}$	0.26		$СР_{ЗМ_{11} 9}$	0.10
	$СР_{ЗМ_7 5}$	0.22		$СР_{ЗМ_{11} 10}$	0.11
			$ЗМ_{12}$	$СР_{ЗМ_{12} 1}$	0.18
				$СР_{ЗМ_{12} 2}$	0.18
				$СР_{ЗМ_{12} 3}$	0.14
				$СР_{ЗМ_{12} 4}$	0.18
				$СР_{ЗМ_{12} 5}$	0.18
				$СР_{ЗМ_{12} 6}$	0.14

Алгоритм определения силы защитных механизмов *d*-го компонента.

Алгоритм 3.2

Исходные данные

1. множество защитных механизмов $ЗМ = \{ЗМ_1, \dots, ЗМ_h, \dots, ЗМ_H\}$;
2. множество $СР_{ЗМ_h} = \{СР_{ЗМ_h 1}, \dots, СР_{ЗМ_h z_h}, \dots, СР_{ЗМ_h z_h}\}$ технических средств и организационно-технических мероприятий определяющих ${ЗМ^d}_h$;
3. вес (показатель важности, определяется экспертами) $СР_{ЗМ_h z_h}$ в h-м защитном механизме $\tilde{w}(ЗМ_h, z_h) \in [0,1]$, при этом $\sum_{,z_h=1}^{Z_h} \tilde{w}(ЗМ_h, z_h) = 1$;
4. $w_{ЗМ_{h\,ПОР}}$ (минимально возможная сила).

Шаг 1. Пронумеруем элементы множества ЗМ для *d*-го компонента: $ЗМ^d = \{{ЗМ^d}_1, \dots, {ЗМ^d}_h, \dots, ЗМ^d_{H_d}\}$, где $H_d \in H$.

Шаг 2. $h = 1$ (с первого защитного механизма)

Шаг 3. Определить и запомнить все $\zeta(ЗМ_h, z_h)$ - параметр наличия / отсутствия элемента $СР_{ЗМ_h z_h}$ в $ЗМ_h$ - $\zeta(ЗМ_h, z_h) = 1$, если $СР_{ЗМ_h z_h}$ «выявлен» при анализе $ЗМ_h$, иначе $\zeta(ЗМ_h, z_h) = 0$;

Шаг 4. Силу защитного механизма определим по формуле $w_{ЗМ_h} = \sum_{z_h=1}^{Z_h} \tilde{w}(ЗМ_h, z_h) * \zeta(ЗМ_h, z_h)$.

Шаг 5. Если $w_{ЗМ_h} < w_{ЗМ_{h\,ПОР}}$ то $w_{ЗМ_h} = 0$ (защитный механизм отсутствует). Если $h = H_d$ то конец алгоритма, иначе $h = h + 1$, перейти к шагу 3.

Основываясь на предложенных моделях, можно составить анкеты для опроса компетентных сотрудников ЦОО или внешних аудиторов с целью определить степень проявления существующих в ТКС ЦОО уязвимостей и силы ЗМ.

В качестве вопросов могут выступать идентификационные признаки, вариантами ответа в таком случае должны быть значения параметров каждого признака. Рассчитав значение $s_{У_f}$ по формуле (3.5), получим степень проявления данной уязвимости в компоненте ТКС ЦОО. Силу того или иного защитного механизма определяем суммой весов выявленных технических средств и организационно-технических мероприятий, сопутствующих данному защитному механизму по формуле (3.10). Если $s_{У_f}$ (или $w_{ЗМ_h}$) мало отличаются от 0 (или меньше наперед задаваемого порога), то при грубом анализе можно считать, что данная уязвимость или данный защитный механизм для определенного компонента системы отсутствуют.

Выводы к главе 3

Уязвимости– это присущие ТКС ЦОО свойства, потенциально приводящие к нарушению информационной безопасности и обусловленные недостатками процесса функционирования, свойствами архитектуры ТКС ЦОО, условиями эксплуатации. В результате анализа современных систем охраны, руководящих документов ФСТЭК, Росгвардии и лучших практик обеспечения ИБ систем телекоммуникаций выявлено 16 уязвимостей, типовых (характерных) для ТКС централизованной охраны объектов.

Разработан алгоритм определения степени проявления в компонентах ТКС ЦОО уязвимостей. Алгоритм основан на экспертном анализе идентификационных признаков уязвимости, определении степени их значимости, значений параметров признаков, что позволяет автоматизировать процесс анализа защищенности, адаптировать решаемую задачу под конкретную реализацию ТКС ЦОО, режиму ее функционирования, условиям внешней среды. Разработаны расчётные таблицы для практического определения степени проявления уязвимости, связывающие идентификационные признаки уязвимости с параметрами их проявления.

Под защитными механизмами обеспечения ИБ (способами защиты) понимаются организованные возможности средств и мероприятий, осуществляемых в ТКС ЦОО с целью полной или частичной реализации одного или нескольких методов (стратегий, функций) защиты.

В результате анализа современных систем охраны, руководящих документов ФСТЭК, Росгвардии и лучших практик обеспечения ИБ систем телекоммуникаций выявлено 12 защитных механизмов обеспечения ИБ, типовых (характерных) для ТКС централизованной охраны объектов.

Разработан алгоритм определения силы защитных механизмов, идентифицированных в компонентах ТКС ЦОО. Алгоритм основан на экспертном анализе множества технических средств и организационно-технических мероприятий, связанных с компонентом ТКС, и определяет долю максимально возможной силы защитного механизма, реально защищающего компонент, что позволяет автоматизировать процесс анализа защищенности, адаптировать решаемую задачу под конкретную реализацию ТКС ЦОО, режиму ее функционирования, условиям внешней среды. Разработаны расчётные таблицы для практического определения силы защитных механизмов, идентифицированных в компонентах ТКС ЦОО.

Глава 4. АВТОМАТИЗАЦИЯ ОЦЕНКИ РАБОТОСПОСОБНОСТИ ТКС ЦОО

В главе предлагается обобщенный алгоритм автоматизированной оценки работоспособности ТКС ЦОО на основе анализа защищенности информационных процессов. Разрабатывается алгоритм анализа адекватности и применимости модели оценки работоспособности. Приводится пример расчетов оценки работоспособности ТКС для конкретного мини-ПЦО, анализируются результаты практической оценки защищенности структурных элементов и информационных процессов ТКС ЦОО для объектов разных категорий и двух типов нарушителей.

4.1. Алгоритмы анализа и оценки работоспособности ТКС ЦОО

Обобщенный алгоритм автоматизированной оценки работоспособности ТКС на основе анализа защищенности информационных процессов в ТКС ЦОО состоит из следующих основных процедур:

1. Процедура формирования экспертных баз данных дестабилизирующих факторов, уязвимостей, угроз, защитных механизмов, оценки проявления уязвимостей и защитных механизмов при проведении аудита ИБ компонентов ТКС ЦОО.

Процедура состоит из следующих этапов:

1.1 Вводятся данные об экспертах (их количество, уровень образования, должность). Эта информация необходима для применения в расчетах средних значений обобщённых экспертных оценок и расчетах коэффициентов конкордации. Данная информация будет составлять базу данных №1 **(**БД-1**);**

Предварительная обработка мнений экспертов.

Пусть имеется k — число экспертов, принимающих участие в опросе с целью получения экспертных оценок. Оценки даются по n - количеству показателей и каждая оценка эксперта r_{ij}- ранг i-го показателя, определённый j–ым экс-

пертом. Для простоты обработки информации для каждого показателя будет одинаковое количество градаций (например, 10 градаций, т.е. r_{ij} может принимать значения целых чисел от 1 до 10). Как правило, для обработки экспертных оценок большое значение имеет важность (значимость) каждого из показателей и степень квалификации эксперта. Пусть $q_j -$ оценка важности показателя, определённая j–м экспертом по $a -$ количеству градаций (например, по 10 градациям) и пусть $p_j -$ оценка j–ого эксперта в соответствии с его уровнем знаний (образование и соответствие занимаемой должности) и опытом (например, стаж работы), определяемая каждым экспертом по $b -$ количеству градаций (например, по 10 градациям); p_j – не определяется самими экспертами, а назначается, исходя из априорно известной объективной информации об экспертах. В таком случае пусть vq_j – весовой коэффициент для оценки важности по каждому из показателей, определённый j–м экспертом. И пусть vp_j – весовой коэффициент значимости мнения j–ого эксперта (он один для всех показателей). Тогда

$$vq_j = \frac{q_j \cdot k}{\sum_{j=1}^{k}(\frac{q_j}{a})} \text{ и } vp_j = \frac{p_j \cdot k}{\sum_{j=1}^{k}(\frac{p_j}{b})}, \quad (4.1)$$

где n — число показателей; k — число экспертов; r_{ij} — ранг i–ого показателя определённый j–м экспертом; $\hat{r}_{ij} = r_{ij} \cdot vq_j \cdot vp_j$ – оценка i–ого показателя определённым j-м экспертом с учетом весовых показателей важности оцениваемого параметра и квалификации эксперта.

Коэффициент конкордации Кендалла W — это некоторое число от 0 до 1, характеризующее степень согласованности мнений экспертов (в виде рангов) по совокупности критериев.

$$W = \frac{12}{(n^3-n)}\sum_{i=1}^{n}\{(\frac{1}{k}\sum_{j=1}^{k}\hat{r}_{ij} - \frac{n+1}{2})^2\} \quad (4.2)$$

При $W = 0$ согласованность мнений экспертов отсутствует, а при $W = 1$ — согласованность полная. Обычно считается, что согласованность вполне достаточна, если $W \geq 0{,}5$. Далее рассчитанную величину коэффициента конкорда-

ции следует оценивать по критерию Пирсона (χ^2) с определенным уровнем значимости (B), т.е. максимальной вероятностью неправильного результата работы экспертов. Обычно задавать значимость достаточно в пределах B =0,005 – 0,05. Оценка по критерию Пирсона дается по формуле $\chi^2{}_{\text{РАСЧ}}|_{B=0,05} = W \cdot k \cdot (k - 1)$. Если расчетная величина выше табличной величины $\chi^2{}_{\text{РАСЧ}} > \chi^2{}_{\text{ТАБЛ}}$ (с избранным уровнем значимости), мнения экспертов окончательно признаются согласованными. Если нет, то использовать экспертные оценки считается невозможным и нужно менять состав экспертной группы. В окончательном виде, по каждому показателю (при условии согласованности мнений экспертов, $W \geq 0,5$) формируется база данных экспертных оценок $R_n\{\overline{r}_i\}$, где $\overline{r}_i = \frac{\sum_{j=1}^{k} \hat{r}_{ij}}{k}$ $(i = 1 \dots n)$. По сути, это среднее арифметическое взвешенных (после весовых коэффициентов) оценок экспертов i-го конкретного параметра.

1.2. Составляются опросные листы экспертов для определения дестабилизирующих факторов, уязвимостей, угроз, защитных механизмов, характерных для ТКС ЦОО. Кроме того, опросные листы формируют: компоненты ТКС ЦОО (КОМ_d); информационные процессы, объединяющие компоненты в устойчивые совокупности - ИП_c; множество обобщенных функций ТКС ЦОО (ОФ_b); множество основных режимов функционирования (ОР_a) ТКС ЦОО; матрица смежности, связывающая структурные компоненты, информационных процессы, обобщенные функции и режимы функционирования ТКС ЦОО; распределение угроз ТКС ЦОО по доступности, целостности и конфиденциальности; матрица связности угроз, уязвимостей, защитных механизмов и структурных компонентов типовой ТКС ЦОО. Кроме того, эксперты в ходе опроса и консультация, сообща формируют:

- правила оценки $\lambda^d(g, f)$ вероятности (эффективности) эксплуатации угрозой уязвимости компонента ТКС ЦОО;

- правила оценки $\mu^d(g, h)$ - вероятности опасности угроз по последствиям их реализации с учетом ЗМ («степень сопротивляемости» h -го ЗМ g-й угрозе);

- правила оценки параметра $NP(g, \text{Н})$ - коэффициент, учитывающий возможности нарушителя при всех благоприятных условиях реализовать угрозу;

- правила оценки параметра $YP(g, t)$ - вероятность посягательства с целью реализации угроз.

1.3. Данные опросных листов по п.1.2 обрабатываются по формулам 4.1-4.2, в результате чего из всех материалов, предложенных экспертами составляются:

- списки компонентов (КОМ_d) информационных процессов (ИП_c), обобщенных функций (ОФ_b), основных режимов функционирования (ОР_a), характерные для типовой ТКС ЦОО, приведены в главе 2;

- матрица смежности, связывающая структурные компоненты, информационных процессы, обобщенные функции и режимы функционирования ТКС ЦОО, она приведена в таблице 2.1;

- базовый перечень уязвимостей структурных компонентов ТКС ЦОО, он приведен в таблице 2.2;

- базовый перечень угроз структурных компонентов ТКС ЦОО, он приведен в таблице 2.3;

- базовый перечень защитных механизмов структурных компонентов ТКС ЦОО, он приведен в таблице 2.4;

- формируется матрица распределение угроз ТКС ЦОО по доступности, целостности и конфиденциальности, она приведена в таблице 2.5;

- формируется матрица связности угроз, уязвимостей, защитных механизмов и структурных компонентов типовой ТКС ЦОО, она приведена в таблице 2.6;

- правила оценки $\lambda^d(g, f)$ - вероятности (эффективности) эксплуатации угрозой уязвимости компонента ТКС ЦОО (Правила 2.1-2.3);

- правила оценки $\mu^d(g, h)$ - вероятности опасности угроз по последствиям их реализации с учетом ЗМ («степень сопротивляемости» h - го ЗМ g-й угрозе) (Правила 2.1 - 2.3);

- правила оценки параметра $NP(g, \text{Н})$ - коэффициент, учитывающий возможности нарушителя при всех благоприятных условиях реализовать угрозу (Правила 2.6 - 2.7);

- правила оценки параметра $YP(g, t)$ - вероятность посягательства с целью реализации угроз (Правила 2.8-2.9).

1.4. Вся информация по п.1.3. заносится в базу исходных начальных данных №2 **(**БД-**2);**

1.5. Аналогично п.1.2 составляются опросные листы экспертов для определения: перечня идентификационных признаков для идентификации уязвимостей при проведении обследования (аудита) ТКС ЦОО; оценка весов идентификационных признаков уязвимостей и степеней их проявления для каждой из уязвимостей каждого структурного компонента ТКС ЦОО; перечня защитных механизмов и соответствующих им технических средств и организационно-технических мероприятий; оценка весов (показателей важности) защитных механизмов при проведении аудита ТКС ЦОО;

1.6. Данные опросных листов по п.1.5 обрабатываются по формулам 4.1-4.2, в результате чего из всех материалов, предложенных экспертами составляются:

- перечень идентификационных признаков для идентификации уязвимостей при проведении аудита ТКС ЦОО, оценка весов идентификационных признаков уязвимостей и степеней их проявления для каждой из уязвимостей каждого структурного компонента ТКС ЦОО (таблица 3.5);

- перечень защитных механизмов и соответствующих им технических средств и организационно-технических мероприятий (таблица 3.6);

- оценка весов (показателей важности) защитных механизмов при проведении аудита ТКС ЦОО (таблица 3.7);

1.7. Вся информация по п.1.6. заносится в базу данных №3 определения степени проявления уязвимости и силы защитных механизмов при обследовании (аудите) ТКС ЦОО **(**БД-3**).**

2. Процедура формирования баз данных о структурных компонентах конкретной ТКС ЦОО для конкретного ПЦО.

Процедура состоит из следующих этапов:

2.1. Для каждого защищаемого объекта ПЦО в процессе аудита (обследования) собирается следующая информация:

2.1.1. по результатам обследования (аудита) объекта определяем степень проявления идентификационного признака уязвимости для каждой уязвимости (информация из табл.3.5 и в базе данных БД-3) по компонентам с d=1 по d=5 (охраняемые объекты и каналы связи от них). По формуле 3.5. определяем степень проявления f-й уязвимости. Уязвимости, превышающие установленный пороговый уровень, включаем в список учитываемых;

2.2.2. классифицируем найденные уязвимости по признакам $У^{d}_{f;lf;mf;nf}$;

2.2.3. по результатам обследования (аудита) объекта определяем степень «силы» для каждого защитного механизма (информация из таблицы 3.7 и в БД-3) по компонентам с d=1 по d=5. По формуле 3.10 определяем степень проявления силы для каждого f-го защитного механизма. Защитные механизмы, превышающие установленный пороговый уровень, включаем в список учитываемых;

2.2.4. классифицируем найденные защитные механизмы по признакам $ЗМ^{d}_{h;p;k;nh}$;

2.2.5. составляем список актуальных угроз для данного объекта, используя матрицу смежности между угрозами и уязвимостями (информация из таблицы 3.7 и в БД-2);

2.2.6. составляем оценки $\hat{\lambda}^{d}(g,f)$ - вероятности (эффективности) эксплуатации угрозой уязвимости для каждой из актуальных для объекта угроз (по правилам 2.1; 2.2; 2.3, которые есть в базе данных БД-2). Принимаем оценку как математическое ожидание и используя ГСЧ (генератор случайных чисел) формируем оценку $\hat{\lambda}^{d}(g,f)$ как нормально распределенную случайную величину;

2.2.7. составляем оценки $\hat{\mu}^{d}(g,h)$ - вероятности опасности угроз по последствиям их реализации с учетом ЗМ для каждой из актуальных для объекта угроз

(по правилам 2.4; 2.5, которые есть в БД-2). Принимаем оценку как математическое ожидание и используя ГСЧ (генератор случайных чисел) формируем оценку $\hat{\mu}^d(g,h)$ как нормально распределенную случайную величину;

2.2.8. составляем оценки $\widehat{YP}(g,t)$ - вероятность посягательств с целью реализации угроз для каждой из актуальных для объекта угроз (по правилам 2.8; 2.9, которые есть в БД-2). Принимаем оценку как математическое ожидание и используя ГСЧ (генератор случайных чисел) формируем оценку $\widehat{YP}(g,t)$ как нормально распределенную случайную величину;

2.2.9. вся информация по п.2.1.1 – п.2.2.9 - данные для расчета ($\hat{\lambda}^d(g,f)$; $\hat{\mu}^d(g,h)$; $\widehat{YP}(g,t)$) по компонентам с d=1 по d=5 (охраняемые объекты и каналы связи от них) ТКС ЦОО заносится в БД -4;

2.2. повторяем пункты п.2.1.1 – п.2.2.9 для каждого из охраняемых на ПЦО объектов;

2.3. повторяем пункты п.2.1.1 – п.2.2.9 для всех остальных структурных компонентов с d=6 по d=11.

3. Процедура оценки работоспособности ТКС ЦОО для конкретного ПЦО.

Процедура состоит из следующих этапов:

3.1. Задаем нарушителя информационной безопасности $\mathrm{H}(q,s)$. В начальных условиях задается, что в одно и то же время на каждом объекте на ТКС ЦОО может воздействовать только один нарушитель. Воздействие нарушителей на объектовые и централизованные компоненты ТКС ЦОО во времени также не пересекается;

3.2. составляем оценки $\widehat{NP}(g,\mathrm{H})$- коэффициент, учитывающий возможности нарушителя при всех благоприятных условиях реализовать угрозу (по правилам 2.6; 2.7, которые есть в БД-**2**;

3.3. зададим данные о количестве охраняемых объектов по категориям (5 категорий по формуле 2.7). Для компонентов с d=1 по d=5 (охраняемые объекты и каналы связи) рассчитаем оценку работоспособности $p^d(g)$ и $p^d(g)|_{\mathrm{H}(q,s)}$ по (2.4 – 2.10 и данные БД-4) для случаев отсутствия воздействия нарушителя, и в случае попытки НСД со стороны нарушителя $\mathrm{H}(q,s)$. Далее для компонентов с

d=6 по d=11 рассчитаем оценку работоспособности $p^d(g)$ и $p^d(g)|_{\mathrm{H}(q,s)}$ по (2.4 – 2.10) для случаев отсутствия воздействия нарушителя, и в случае попытки НСД со стороны нарушителя типа $\mathrm{H}(q,s)$;

3.4. с учетом матрицы распределение угроз ТКС ЦОО по доступности, целостности и конфиденциальности (таблица 2.5 и БД-2 и данные БД-4) рассчитаем оценку работоспособности компонентов ТКС ЦОО $p^d(g)|_{\mathrm{H}(q,s)}$ в разрезе доступности, целостности и конфиденциальности;

3.5. с учетом матрицы смежности, связывающей структурные компоненты, информационных процессы, обобщенные функции и режимы функционирования ТКС ЦОО (таблица 2.1 и БД-2 и данные БД-4) рассчитаем оценку работоспособности каждого из информационных процессов ТКС ЦОО (алгоритм 1.2) в целом и в разрезе доступности, целостности и конфиденциальности;

3.6. с учетом матрицы смежности, связывающей структурные компоненты, информационных процессы, обобщенные функции и режимы функционирования ТКС ЦОО (таблица 2.1 и БД-2 и данные БД-4) рассчитаем оценку работоспособности каждой из обобщенных функций ТКС ЦОО (алгоритм 1.2) в целом и в разрезе доступности, целостности и конфиденциальности;

3.7. с учетом матрицы смежности, связывающей структурные компоненты, информационные процессы, обобщенные функции и режимы функционирования ТКС ЦОО (таблица 2.1 и БД-2 и данные БД-4) рассчитаем оценку работоспособности каждого из основных режимов функционирования ТКС ЦОО (алгоритм 1.2) в целом и в разрезе доступности, целостности и конфиденциальности;

3.8. результаты расчетов по п.3.1 – 3.7. заносится в базу данных результатов расчетов **(**БД -5**)**;

3.9. интерпретируем результаты расчетов в виде многомерных векторов, расчетных таблиц или диаграмм, графиков и выводим для пользователя в сравнении с данными предыдущих расчетов (при их наличии);

3.10. повторяем пункты 3.1-3.10 для других типов нарушителей (при необходимости).

Процедура №1 выполняется только один раз при подготовке автоматизированных средств расчетов. Процедура №2 выполняется при каждой переоценке показателей работоспособности ТКС ЦОО конкретного ПЦО. Процедура №3 выполняется при каждом расчете работоспособности ТКС ЦОО по итогам проведенного аудита и при изменении типа нарушителя.

В дополнении к данным процедурам, возможно создание методики автоматизации формирования перечня мероприятий по повышению защищенности информационных процессов и работоспособности ТКС ЦОО по итогам проведенного аудита.

Для анализа защищенности информационных процессов в ТКС ЦОО необходимо формирование и ведение нескольких баз данных. В основном данные базы формируются на основании экспертных опросов квалифицированных экспертов в данной предметной области.

На рисунках 4.1 - 4.4. приведены алгоритмы анализа и оценки работоспособности ТКС ЦОО.

Процедура №1 формирования экспертных баз данных дестабилизирующих факторов, уязвимостей, угроз, защитных механизмов, оценки проявления уязвимостей и защитных механизмов при проведении аудита ИБ компонентов ТКС ЦОО

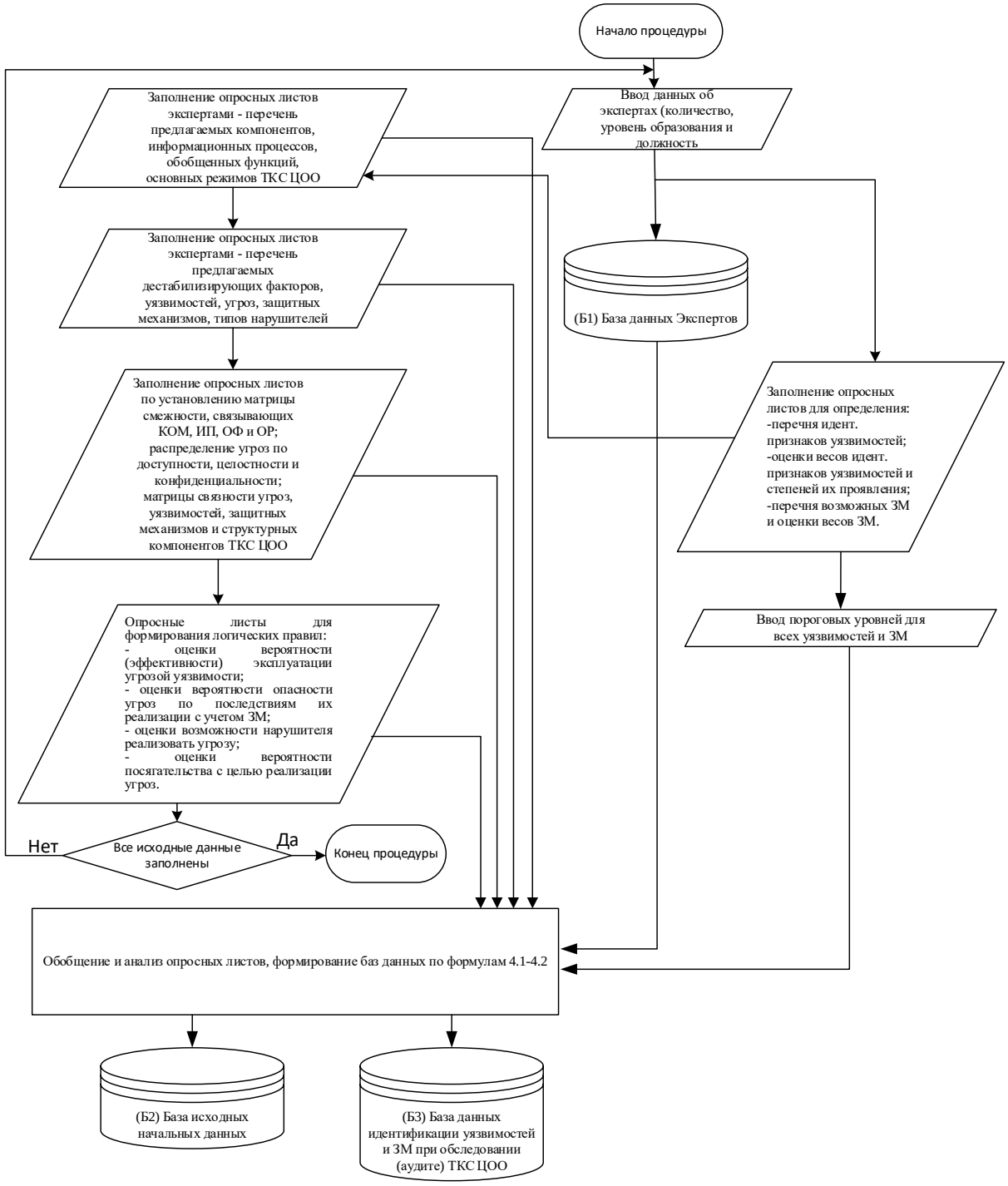

Рисунок 4.1 - Процедура №1 формирования экспертных баз данных дестабилизирующих факторов, уязвимостей, угроз, защитных механизмов, оценки проявления уязвимостей и защитных механизмов при проведении аудита ИБ компонентов ТКС ЦОО

Процедура №2 формирования баз данных о структурных компонентах конкретной ТКС ЦОО для конкретного ПЦО (ЧАСТЬ 1, объектовая часть)

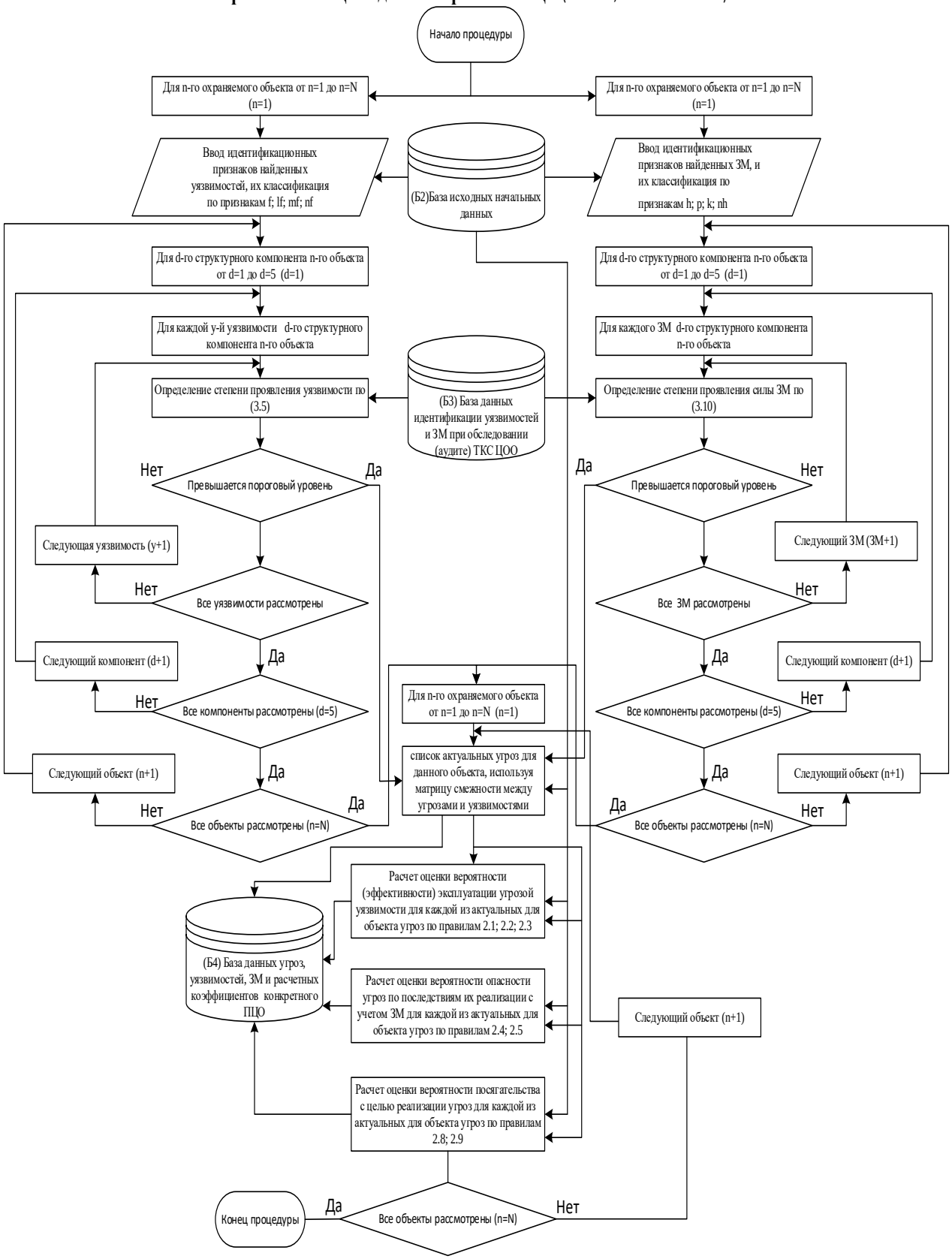

Рисунок .4.2 - Процедура №2 формирования баз данных о структурных компонентах конкретной ТКС ЦОО для конкретного ПЦО (ЧАСТЬ 1, объектовая часть)

Процедура №2 формирования баз данных о структурных компонентах конкретной ТКС ЦОО для конкретного ПЦО (ЧАСТЬ 2, ПЦО)

Рисунок 4.3 - Процедура №2 формирования баз данных о структурных компонентах конкретной ТКС ЦОО для конкретного ПЦО (ЧАСТЬ 2, ПЦО)

Процедура №3 оценки работоспособности ТКС ЦОО для конкретного ПЦО

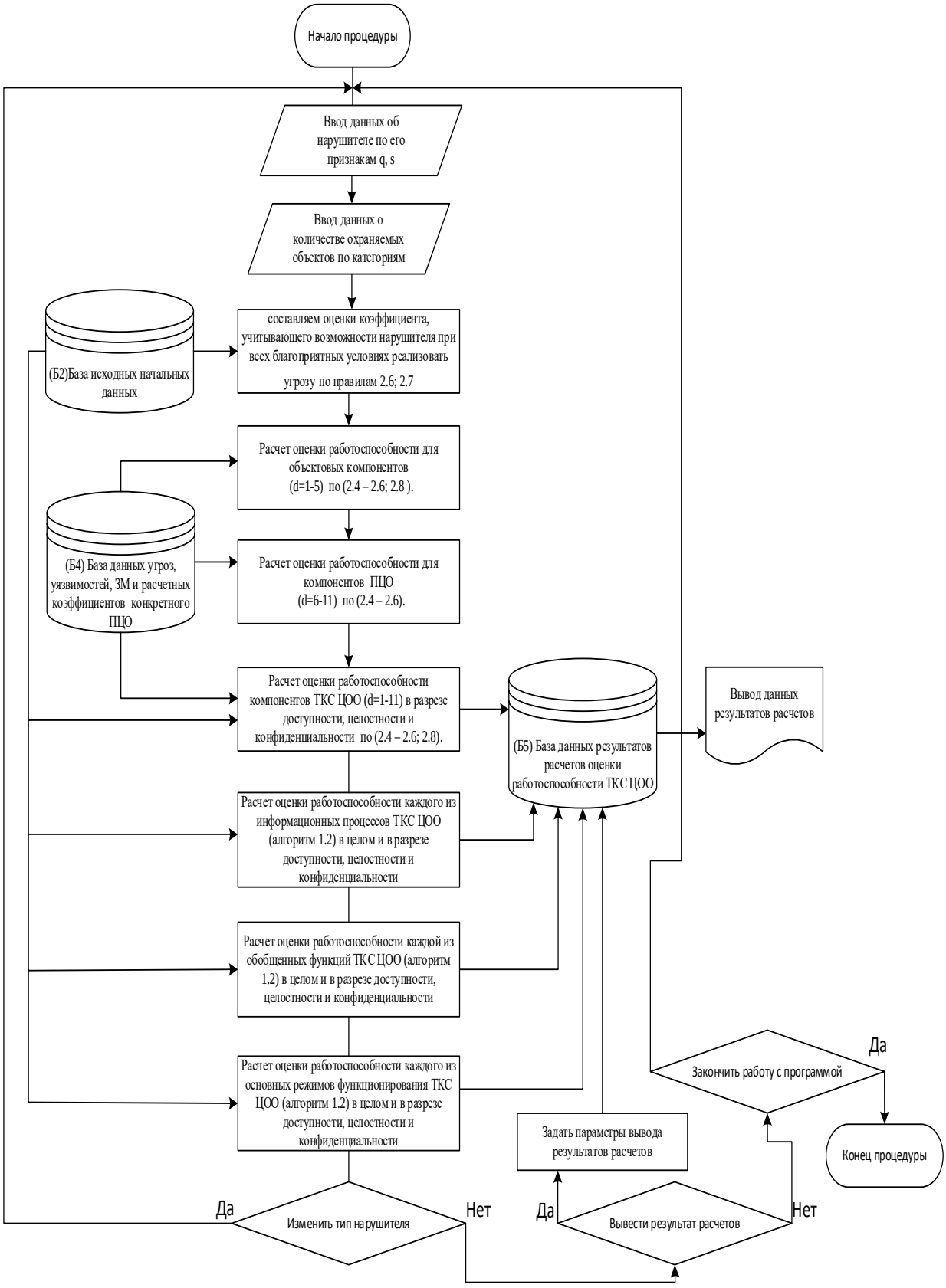

Рисунок 4.4 - Процедура №3 оценки работоспособности ТКС ЦОО для конкретного ПЦО

4.2. Анализ адекватности и применимости модели оценки работоспособности ТКС ЦОО

При расчетах оценки защищенности информационных процессов и работоспособности ТКС ЦОО в различных ОР и для различных типов нарушителей, должны существовать некоторые пороговые значения защищенности. По результатам расчетов можно сделать вывод о том, удовлетворительная или неудовлетворительная защищенность информационных процессов и работоспособность ТКС ЦОО для обеспечения централизованной охраны объектов разной категории важности по [16, 45].

Величины пороговых значений защищенности информационных процессов и работоспособности ТКС ЦОО определяются при экспертном опросе специалистов в данной предметной области для различных ОР, типов нарушителей и объектов разной категории важности.

Адекватности и применимость рассматриваемой модели определяется ошибками, возникающими из-за несоответствия исходных расчетных данных реальному положению дел для конкретной ТКС ЦОО. Такая ситуация возникает из-за несовершенства методики проведения аудита ТКС ЦОО, но главным образом из-за ошибок оператора, проводящего аудит при заполнении базы данных опросных шаблонов по существующим дестабилизирующим факторам, уязвимостям и защищаемым информационным ресурсам.

Дестабилизирующие факторы, объективно характеризующие среду функционирования ТКС ЦОО, регламентированы нормативно-распорядительной документаций ПЦО [5 - 10, 32, 45, 56]. Поэтому предположим, что ошибки оператора связаны исключительно с обнаружением уязвимостей, у которых индекс mf =5;6 – индекс, определяющий способ выявления уязвимости (5 – выявляется вероятностно, субъективно, на основе косвенных показателей; 6 – выявляется субъективно, в ходе общения с субъектами или оперативным путем (негласным контролем)).

Для таких уязвимостей (*mf* =5; 6) могут быть неправильно определены индексы lf – индекс, определяющий тип угроз, вызываемых данной уязвимостью, и nf - индекс, определяющий характер проявления уязвимостей. В результате неправильно определяется и показатель $\lambda^d(g,f)$, который определяет вероятность (эффективность) эксплуатации угрозой уязвимости компонента ТКС ЦОО.

Ошибки оператора можно считать случайными и зависящими от опыта, стажа, квалификации сотрудника. В первом приближении можно предположить, что сотрудники по квалификации имеют градации как с большим опытом (например, порог *pp*= 3% ошибок при заполнении БД); опытные (например, *pp*=5% ошибок) и малоопытные (например, *pp*=10% ошибок) в заполнении опросных листов по уязвимостям, у которых индекс *mf* =5;6.

Предлагается из всех уязвимостей (*mf*=5;6) случайным образом по равномерному распределению выбирать *pp* процент уязвимостей, у которых имеются ошибки ввода данных. Для таких выбранных уязвимостей случайным образом по равномерному распределению выбирать индекс lf или nf, в котором произошла ошибка, и случайным образом по равномерному распределению выбирается значение индекса lf или nf. Таким образом, заносится БД опроса аудита с эмуляцией случайных ошибок оператора.

Для анализа адекватности и применимости модели проводится эталонный расчет оценки защищенности информационных процессов и работоспособности ТКС ЦОО в различных ОР и для различных типов нарушителей. Далее проводится сравнение данных эталонного расчета с пороговыми значениями защищенности информационных процессов и работоспособности ТКС ЦОО и делаются выводы об удовлетворительной или неудовлетворительной защищенности.

Далее необходимо провести статистически большое (например, не менее 40-50) количество аналогичных расчетов по БД опроса аудита с эмуляцией случайных ошибок оператора и сделать сравнение данных расчетов с пороговыми значениями. Далее сравниваются выводы об удовлетворительной или неудовлетворительной защищенности эталонного расчета и тестовых расчетов по БД с эмуляцией случайных ошибок оператора.

Критерием адекватности и применимости модели будет являться процент ошибок первого и второго рода тестовых расчетов по БД с эмуляцией случайных ошибок оператора по сравнению с эталонными расчетами. Ошибкой первого рода является результат, когда эталонный расчет показал удовлетворительную защищенность, а тестовый расчет показал неудовлетворительную защищенность (ложная тревога). Ошибкой второго рода является результат, когда эталонный расчет показал неудовлетворительную защищенность, а тестовый расчет удовлетворительную защищенность (пропуск цели).

Обычно для технических систем в данной предметной области процент ошибок (уровень значимости) первого рода не должен превышать уровень в 5%, а ошибок второго рода 1%.

Аналогичным образом, по динамике изменения процентного соотношения ошибок первого и второго рода, можно оценивать и внесение изменений в математику логико-вероятностного описания расчетной методики модели ТКС ЦОО.

Обобщенный алгоритм оценки адекватности и применимости модели оценки работоспособности ТКС ЦОО представлен на рис.4.5.

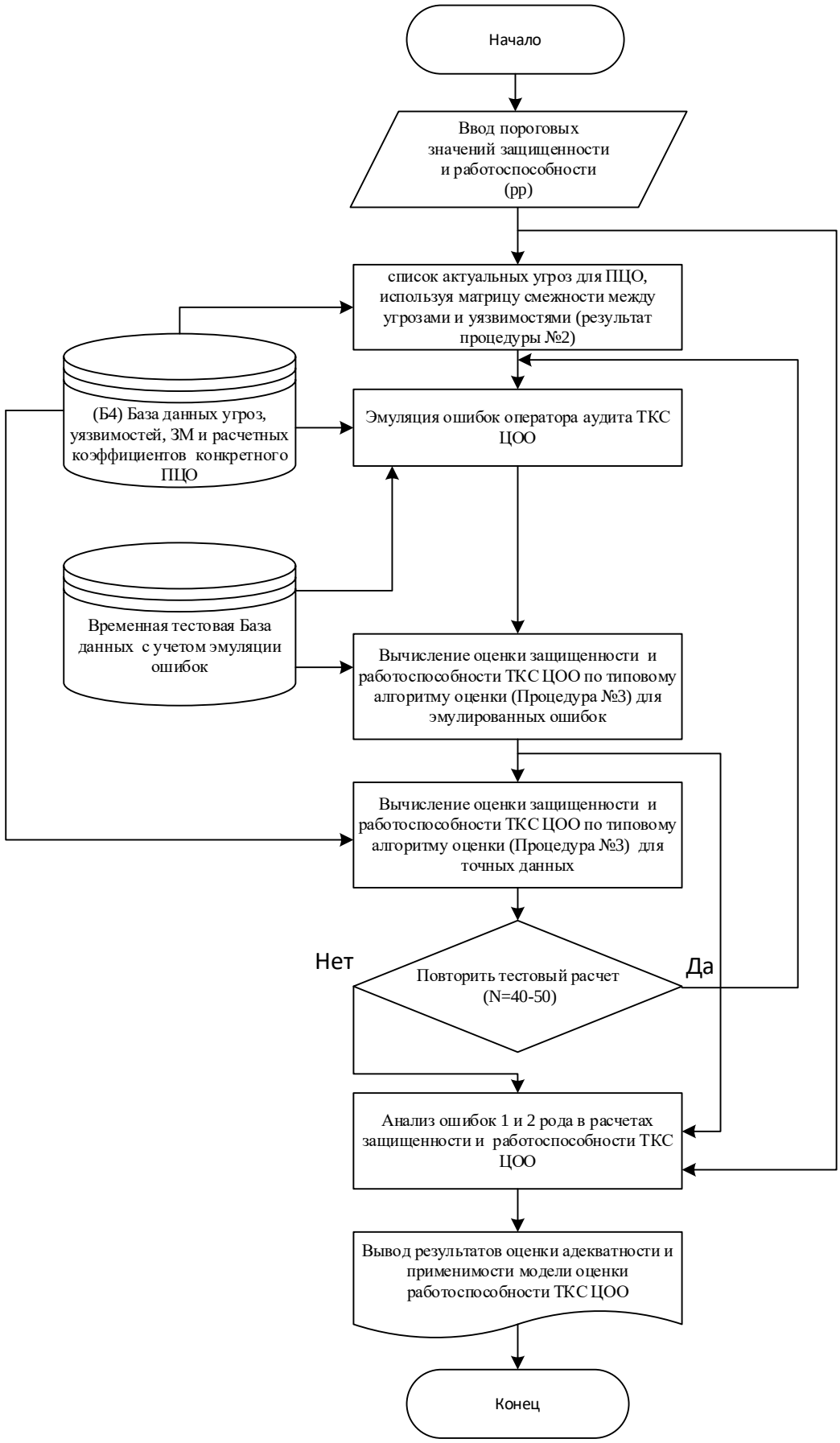

Рисунок 4.5 - Обобщенный алгоритм оценки адекватности и применимости модели оценки работоспособности ТКС ЦОО

4.3. Пример расчетов оценки работоспособности ТКС ЦОО для конкретного ПЦО

Будем полагать, что имеется ТКС ЦОО малого ПЦО (в терминологии [32] микро-ПЦО) и для него выполняются условия ограничений и допущений, изложенные в п.2.2. Кроме того, будем полагать, что в одно и то же время с одного объекта может поступать только одно служебное или тревожное извещение (т.е. только один нарушитель может предпринимать попытку НСД на защищаемый объект). Попытки проникновения на один и тот же объект не пересекаются во времени.

Исходные данные для конкретного ПЦО и охраняемых объектов взяты из практики функционирования мини-ПЦО, но данные об объектах защиты являются обезличенными.

1. Исходные данные для охраняемых объектов.

Пусть охраняется на мини-ПЦО 25 объектов, из них категории А1 -5 (N1-N5); А2-5 (N6-N10); А3-5 (N11-N15); Б1-5 (N16-N20); Б2-5 (N21-N25). По результатам обследований объектов, составлена таблица уязвимостей (для объектов – структурных компонентов d1 – d5) выявляются уязвимости $У_1 - У_4$. Все данные по обследованию уязвимостей объектов приведены в таблице 4.1. Для упрощения расчетов в примере, примем уязвимости и ЗМ в каждой из категорий объектов одинаковыми.

Установленные пороги приемлемости уязвимостей и ЗМ объектовых комплексов ТСО можно для данного расчетного примера установить следующим образом: А1 – 0,2; А2 – 0,25; А3 – 0,3; Б1 – 0,35; Б2 – 0,4. В случае, если веса идентификационных признаков уязвимостей (по 3.5) превышают пороговые значения, уязвимости (и угрозы ими вызываемые) следует учитывать в расчетах.

Таблица 4.1 - Данные по обследованию уязвимостей объектовых комплексов ТСО защищаемых объектов ТКС ЦОО

N объекта	$\widetilde{r^*}_{y_{fu_fq(u_f)}}$ Степень проявления идентификационного признака уязвимости для объектов (из табл.3.5)
1-5	$\widetilde{r^*}_{y_114} = 0.3; \widetilde{r^*}_{y_132} = 0.5; \widetilde{r^*}_{y_142} = 0.5; \widetilde{r^*}_{y_213} = 0.2; \widetilde{r^*}_{y_223} = 0.2; \widetilde{r^*}_{y_233} = 0.3;$ $\widetilde{r^*}_{y_263} = 0.1; \widetilde{r^*}_{y_314} = 0.2; \widetilde{r^*}_{y_324} = 0.1; \widetilde{r^*}_{y_341} = 0.5; \widetilde{r^*}_{y_414} = 0.3; \widetilde{r^*}_{y_421} = 0.1;$ $\widetilde{r^*}_{y_433} = 0.1; \widetilde{r^*}_{y_444} = 0.2$
6-10	$\widetilde{r^*}_{y_113} = 0.5; \widetilde{r^*}_{y_132} = 0.5; \widetilde{r^*}_{y_142} = 0.5; \widetilde{r^*}_{y_153} = 0.5; \widetilde{r^*}_{y_213} = 0.2; \widetilde{r^*}_{y_223} = 0.2;$ $\widetilde{r^*}_{y_233} = 0.3; \widetilde{r^*}_{y_251} = 0.4; \widetilde{r^*}_{y_263} = 0.1; \widetilde{r^*}_{y_271} = 0.2; \widetilde{r^*}_{y_313} = 0.4; \widetilde{r^*}_{y_324} = 0.1;$ $\widetilde{r^*}_{y_341} = 0.5; \widetilde{r^*}_{y_413} = 0.5; \widetilde{r^*}_{y_421} = 0.1; \widetilde{r^*}_{y_433} = 0.1; \widetilde{r^*}_{y_444} = 0.2$
11-15	$\widetilde{r^*}_{y_113} = 0.5; \widetilde{r^*}_{y_131} = 0.7; \widetilde{r^*}_{y_142} = 0.5; \widetilde{r^*}_{y_152} = 0.7; \widetilde{r^*}_{y_212} = 0.7; \widetilde{r^*}_{y_223} = 0.2;$ $\widetilde{r^*}_{y_232} = 0.7; \widetilde{r^*}_{y_241} = 0.2; \widetilde{r^*}_{y_251} = 0.4; \widetilde{r^*}_{y_262} = 0.2; \widetilde{r^*}_{y_272} = 0.3; \widetilde{r^*}_{y_312} = 0.7;$ $\widetilde{r^*}_{y_323} = 0.3; \widetilde{r^*}_{y_333} = 0.2; \widetilde{r^*}_{y_341} = 0.5; \widetilde{r^*}_{y_413} = 0.5; \widetilde{r^*}_{y_421} = 0.1; \widetilde{r^*}_{y_433} = 0.1;$ $\widetilde{r^*}_{y_444} = 0.2$
16-20	$\widetilde{r^*}_{y_112} = 0.7; \widetilde{r^*}_{y_131} = 0.7; \widetilde{r^*}_{y_141} = 0.9; \widetilde{r^*}_{y_152} = 0.7; \widetilde{r^*}_{y_212} = 0.7; \widetilde{r^*}_{y_222} = 0.7;$ $\widetilde{r^*}_{y_232} = 0.7; \widetilde{r^*}_{y_242} = 0.4; \widetilde{r^*}_{y_251} = 0.4; \widetilde{r^*}_{y_262} = 0.2; \widetilde{r^*}_{y_272} = 0.3; \widetilde{r^*}_{y_312} = 0.7;$ $\widetilde{r^*}_{y_323} = 0.3; \widetilde{r^*}_{y_333} = 0.2; \widetilde{r^*}_{y_341} = 0.5; \widetilde{r^*}_{y_413} = 0.5; \widetilde{r^*}_{y_421} = 0.1; \widetilde{r^*}_{y_433} = 0.1;$ $\widetilde{r^*}_{y_444} = 0.2$
21-25	$\widetilde{r^*}_{y_112} = 0.7; \widetilde{r^*}_{y_121} = 0.7; \widetilde{r^*}_{y_131} = 0.7; \widetilde{r^*}_{y_141} = 0.9; \widetilde{r^*}_{y_151} = 1.0; \widetilde{r^*}_{y_212} = 0.7;$ $\widetilde{r^*}_{y_222} = 0.7; \widetilde{r^*}_{y_232} = 0.7; \widetilde{r^*}_{y_243} = 0.7; \widetilde{r^*}_{y_251} = 0.4; \widetilde{r^*}_{y_261} = 0.4; \widetilde{r^*}_{y_272} = 0.3;$ $\widetilde{r^*}_{y_312} = 0.7; \widetilde{r^*}_{y_323} = 0.3; \widetilde{r^*}_{y_332} = 0.7; \widetilde{r^*}_{y_341} = 0.5; \widetilde{r^*}_{y_413} = 0.5; \widetilde{r^*}_{y_421} = 0.1;$ $\widetilde{r^*}_{y_432} = 0.5; \widetilde{r^*}_{y_444} = 0.2$

Далее определим защитные механизмы для объектовых комплексов ТСО ($ЗМ_1 - ЗМ_5$) по результатам обследования объектов. Все данные по обследованию ЗМ объектов приведены в таблице 4.2.

Таблица 4.2 - Данные по обследованию защитных механизмов для объектовых комплексов ТСО защищаемых объектов ТКС ЦОО

N объ-екта	Наличие и тип защитного механизма и весовые коэффициенты (из таблицам 3.6 и 3.7)
1-5	$СР_{ЗМ_11}$ (0,36); $СР_{ЗМ_12}$ (0,36); $СР_{ЗМ_13}$ (0,28); $СР_{ЗМ_21}$ (0,15); $СР_{ЗМ_22}$ (0,08); $СР_{ЗМ_23}$ (0,08); $СР_{ЗМ_24}$ (0,08); $СР_{ЗМ_25}$ (0,15); $СР_{ЗМ_26}$ (0,13); $СР_{ЗМ_27}$ (0,15); $СР_{ЗМ_28}$ (0,10); $СР_{ЗМ_31}$ (0,12); $СР_{ЗМ_32}$ (0,12); $СР_{ЗМ_33}$ (0,23); $СР_{ЗМ_34}$ (0,15); $СР_{ЗМ_35}$ (0,12); $СР_{ЗМ_36}$ (0,12); $СР_{ЗМ_37}$ (0,14); $СР_{ЗМ_41}$ (0,20); $СР_{ЗМ_42}$ (0,24); $СР_{ЗМ_43}$ (0,24); $СР_{ЗМ_44}$ (0,32); $СР_{ЗМ_51}$ (0,22); $СР_{ЗМ_52}$ (0,28)
6-10	$СР_{ЗМ_11}$ (0,36); $СР_{ЗМ_13}$ (0,28); $СР_{ЗМ_21}$ (0,15); $СР_{ЗМ_23}$ (0,08); $СР_{ЗМ_24}$ (0,08); $СР_{ЗМ_25}$ (0,15); $СР_{ЗМ_27}$ (0,15); $СР_{ЗМ_31}$ (0,12); $СР_{ЗМ_32}$ (0,12); $СР_{ЗМ_33}$ (0,23); $СР_{ЗМ_36}$ (0,12); $СР_{ЗМ_37}$ (0,14); $СР_{ЗМ_41}$ (0,20); $СР_{ЗМ_42}$ (0,24); $СР_{ЗМ_43}$ (0,24); $СР_{ЗМ_44}$ (0,32); $СР_{ЗМ_51}$ (0,22); $СР_{ЗМ_52}$ (0,28)
11-15	$СР_{ЗМ_11}$ (0,36); $СР_{ЗМ_21}$ (0,15); $СР_{ЗМ_25}$ (0,15); $СР_{ЗМ_27}$ (0,15); $СР_{ЗМ_31}$ (0,12); $СР_{ЗМ_32}$ (0,12); $СР_{ЗМ_37}$ (0,14); $СР_{ЗМ_41}$ (0,20); $СР_{ЗМ_42}$ (0,24); $СР_{ЗМ_43}$ (0,24); $СР_{ЗМ_44}$ (0,32); $СР_{ЗМ_51}$ (0,22); $СР_{ЗМ_52}$ (0,28)
16-20	$СР_{ЗМ_25}$ (0,15); $СР_{ЗМ_27}$ (0,15); $СР_{ЗМ_31}$ (0,12); $СР_{ЗМ_37}$ (0,14); $СР_{ЗМ_41}$ (0,20); $СР_{ЗМ_42}$ (0,24); $СР_{ЗМ_43}$ (0,24); $СР_{ЗМ_44}$ (0,32); $СР_{ЗМ_51}$ (0,22); $СР_{ЗМ_52}$ (0,28)
21-25	$СР_{ЗМ_25}$ (0,15); $СР_{ЗМ_31}$ (0,12); $СР_{ЗМ_42}$ (0,24); $СР_{ЗМ_43}$ (0,24); $СР_{ЗМ_51}$ (0,22); $СР_{ЗМ_52}$ (0,28)

В случае, если веса ЗМ (по 3.10) превышают пороговые значения, эти ЗМ следует учитывать в расчетах.

2. Исходные данные для ПЦО.

По результатам обследования ПЦО, составлена таблица уязвимостей (для ПЦО – структурных компонентов d6 – d11) выявляются уязвимости $У_3 - У_{16}$. Все данные по обследованию уязвимостей ПЦО приведены в таблице 4.3.

Таблица 4.3 - Данные по обследованию уязвимостей ПЦО ТКС ЦОО

Уязви-мость	$\widetilde{r^*}_{\text{у}_f u_f q(u_f)}$ Степень проявления идентификационного признака уязвимости для ПЦО (из табл.3.5)
У_3	$\widetilde{r^*}_{\text{у}_3 14} = 0.2; \widetilde{r^*}_{\text{у}_3 23} = 0.3; \widetilde{r^*}_{\text{у}_3 33} = 0.2; \widetilde{r^*}_{\text{у}_3 41} = 0.5$
У_4	$\widetilde{r^*}_{\text{у}_4 14} = 0.3; \widetilde{r^*}_{\text{у}_4 21} = 0.1; \widetilde{r^*}_{\text{у}_4 32} = 0.5; \widetilde{r^*}_{\text{у}_4 44} = 0.2$
У_5	$\widetilde{r^*}_{\text{у}_5 12} = 0.7; \widetilde{r^*}_{\text{у}_5 23} = 0.3$
У_6	$\widetilde{r^*}_{\text{у}_6 11} = 0.5; \widetilde{r^*}_{\text{у}_6 22} = 0.3; \widetilde{r^*}_{\text{у}_6 31} = 0.5$
У_7	$\widetilde{r^*}_{\text{у}_7 11} = 0.2; \widetilde{r^*}_{\text{у}_7 23} = 0.1; \widetilde{r^*}_{\text{у}_7 31} = 1; \widetilde{r^*}_{\text{у}_7 41} = 1; \widetilde{r^*}_{\text{у}_7 51} = 0.7; \widetilde{r^*}_{\text{у}_7 61} = 1;$ $\widetilde{r^*}_{\text{у}_7 73} = 0.4$
У_8	$\widetilde{r^*}_{\text{у}_8 11} = 1;\ \widetilde{r^*}_{\text{у}_8 22} = 0.5; \widetilde{r^*}_{\text{у}_8 32} = 0.7; \widetilde{r^*}_{\text{у}_8 41} = 1; \widetilde{r^*}_{\text{у}_8 51} = 0.4$
У_9	$\widetilde{r^*}_{\text{у}_9 12} = 0.5; \widetilde{r^*}_{\text{у}_9 21} = 1$
У_{10}	$\widetilde{r^*}_{\text{у}_{10} 12} = 0.5; \widetilde{r^*}_{\text{у}_{10} 22} = 0.7$
У_{11}	$\widetilde{r^*}_{\text{у}_{11} 12} = 0.5$
У_{12}	$\widetilde{r^*}_{\text{у}_{12} 21} = 1;$
У_{13}	$\widetilde{r^*}_{\text{у}_{13} 12} = 0.7; \widetilde{r^*}_{\text{у}_{13} 21} = 0.5; \widetilde{r^*}_{\text{у}_{13} 31} = 1$
У_{14}	$\widetilde{r^*}_{\text{у}_{14} 12} = 0.5; \widetilde{r^*}_{\text{у}_{14} 22} = 0.5$
У_{15}	$\widetilde{r^*}_{\text{у}_{15} 11} = 1; \widetilde{r^*}_{\text{у}_{15} 32} = 0.5; \widetilde{r^*}_{\text{у}_{15} 41} = 1$
У_{16}	$\widetilde{r^*}_{\text{у}_{16} 12} = 0.5$

Установленные пороги приемлемости уязвимостей и ЗМ для ПЦО можно для данного расчетного примера установить на уровне 0,2. В случае, если веса идентификационных признаков уязвимостей (по 3.5) превышают пороговые значения, уязвимости (и угрозы ими вызываемые) следует учитывать в расчетах.

Далее определим защитные механизмы для ПЦО ($ЗМ_4 - ЗМ_{12}$) по результатам обследования ПЦО. Все данные по обследованию ЗМ ПЦО приведены в таблице 4.4.

Таблица 4.4 - Данные по обследованию ЗМ ПЦО ТКС ЦОО

ЗМ	Наличие и тип защитного механизма и весовые коэффициенты (из табл.3.6 и 3.7)
$ЗМ_4$	$СР_{ЗМ_42}$ (0,24); $СР_{ЗМ_43}$ (0,24)
$ЗМ_5$	$СР_{ЗМ_51}$ (0,22); $СР_{ЗМ_52}$ (0,28)
$ЗМ_6$	$СР_{ЗМ_61}$ (0,12); $СР_{ЗМ_63}$ (0,12); $СР_{ЗМ_64}$ (0,13); $СР_{ЗМ_65}$ (0,07); $СР_{ЗМ_66}$ (0,17); $СР_{ЗМ_68}$ (0,10)
$ЗМ_7$	$СР_{ЗМ_71}$ (0,14); $СР_{ЗМ_73}$ (0,22); $СР_{ЗМ_75}$ (0,22)
$ЗМ_8$	$СР_{ЗМ_82}$ (0,07); $СР_{ЗМ_83}$ (0,10); $СР_{ЗМ_87}$ (0,08); $СР_{ЗМ_88}$ (0,09); $СР_{ЗМ_89}$ (0,11)
$ЗМ_9$	$СР_{ЗМ_91}$ (0,11); $СР_{ЗМ_92}$ (0,08); $СР_{ЗМ_93}$ (0,13); $СР_{ЗМ_94}$ (0,10); $СР_{ЗМ_98}$ (0,09); $СР_{ЗМ_910}$ (0,11)
$ЗМ_{10}$	$СР_{ЗМ_{10}1}$ (0,14); $СР_{ЗМ_{10}4}$ (0,13); $СР_{ЗМ_{10}5}$ (0,12); $СР_{ЗМ_{10}7}$ (0,13)
$ЗМ_{11}$	$СР_{ЗМ_{11}1}$ (0,10); $СР_{ЗМ_{11}2}$ (0,10); $СР_{ЗМ_{11}4}$ (0,10); $СР_{ЗМ_{11}8}$ (0,09); $СР_{ЗМ_{11}9}$ (0,10); $СР_{ЗМ_{11}10}$ (0,11)
$ЗМ_{12}$	$СР_{ЗМ_{12}4}$ (0,18); $СР_{ЗМ_{12}5}$ (0,18)

По результатам исходных данных были определены актуальные угрозы (частная модель) для ТКС ЦОО конкретного мини-ПЦО и ЗМ, характерные для данного мини-ПЦО. Так же по результатам обследования была проведена классификация актуальных уязвимостей, актуальных ЗМ и угроз, результаты представлены в таблице 4.5

Таблица 4.5 - Классификация актуальных уязвимостей, ЗМ и угроз по результатам проведения обследования

Уязвимости $У^{d}_{f;lf;mf;nf}$				Защитные механизмы $ЗМ^{d}_{h;p;k;nh}$				Угрозы $УГ^{d}_{g;lg;ng}$		
f	*lf*	*mf*	*nf*	*h*	*p*	*k*	*nh*	*g*	*lg*	*ng*
Для объектовых комплексов ТСО										
1	7	1	1	1	3	1	1	1	3	4
2	4	1	3	2	1	2	3	2	4	2
3	7	3	4	3	1	2	3	3	5	3
4	4	2	3	4	3	4	3	4	2	2
				5	3	5	2	5	5	2
								6	5	4
								7	3	3
								8	3	2
								9	5	4
								10	1	4
								11	1	4
								12	4	2
								13	2	2
								14	5	2
Для ПЦО										
3	7	3	4	4	3	4	3	15	7	4
4	4	2	3	5	3	5	2	16	7	2
5	7	1	1	6	2	4	1	17	7	2
6	7	2	1	7	2	5	1	18	7	2
7	2	5	1	8	1	3	1	19	7	2
8	2	3	1	9	1	2	1	20	7	2
9	2	2	3	10	3	2	1	21	3	2
10	7	2	3	11	1	2	1	22	7	2
11	7	5	3	12	2	5	3	23	3	4

Окончание таблицы 4.5

12	2	6	3					24	5	4
13	2	5	4					25	1	4
14	2	3	4					26	3	4
15	7	6	3					27	5	2
16	7	4	1					28	1	4
								29	3	2
								30	5	4
								31	1	2
								32	3	2
								33	2	3
								34	7	2

Расчеты были выполнены для двух типов нарушителей. Нарушитель №1 (q=6; s=2) опасный внешний и нарушитель №2 (q=4; s=1) внешний случайный.

Все остальные расчеты выполнены на основании исходных данных по п.4.1 согласно алгоритму анализа и оценки работоспособности ТКС ЦОО. Основные результаты расчетов приведены на рисунках 4.6 и 4.7. По результатам расчетов можно рекомендовать критерии установления пороговых требований по обеспечению защищенности ТКС ЦОО для объектов разных категорий значимости согласно таблице 4.6.

Таблица 4.6 - Пороговые значения защищенности ТКС ЦОО для охраняемых объектов разных категорий значимости для всех типов нарушителей

Категория объекта	Уровень порога защищенности $P_{ПОР}$
А1	0,95-0,98
А2	более 0,93
А3	более 0,90
Б1	более 0,88
Б2	более 0,85

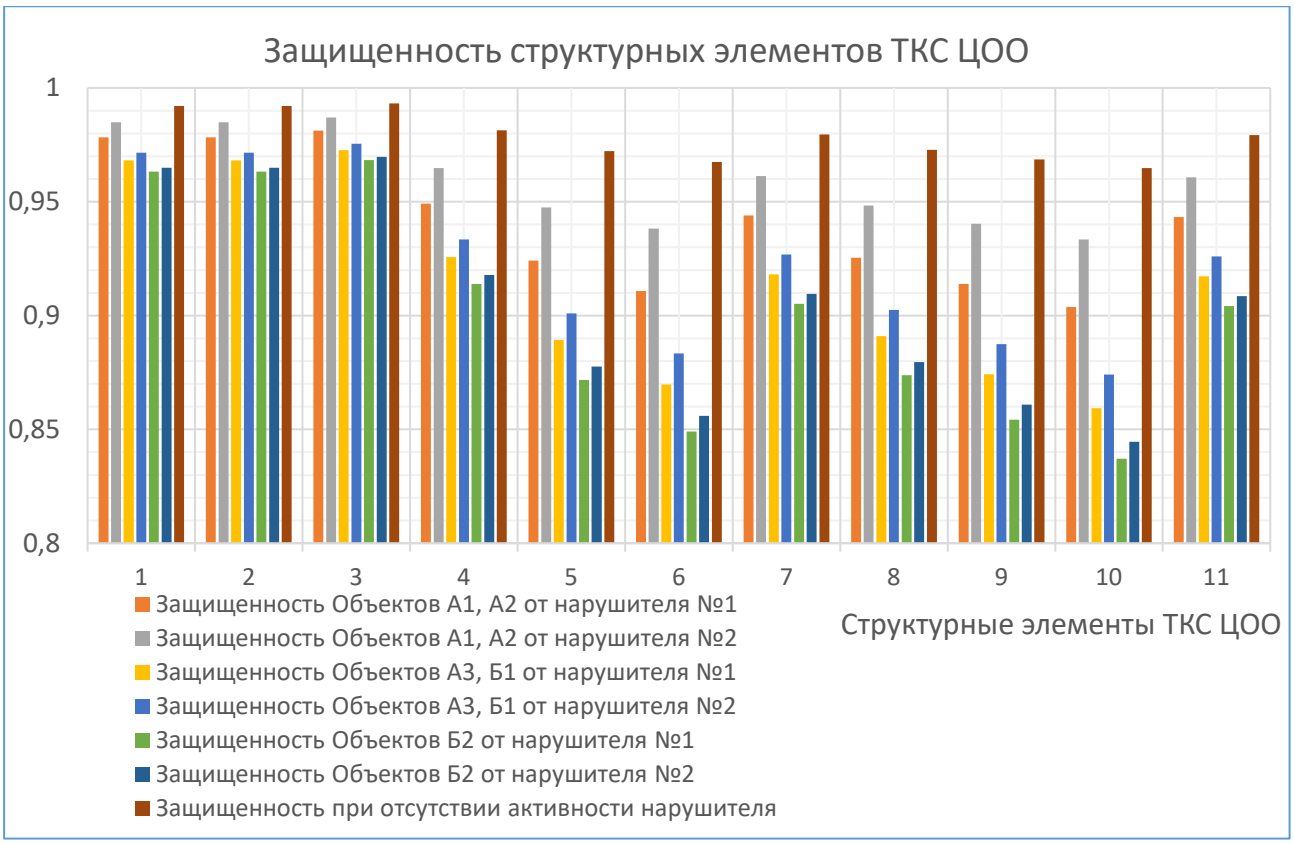

Рисунок 4.6 - Защищенность структурных элементов ТКС ЦОО

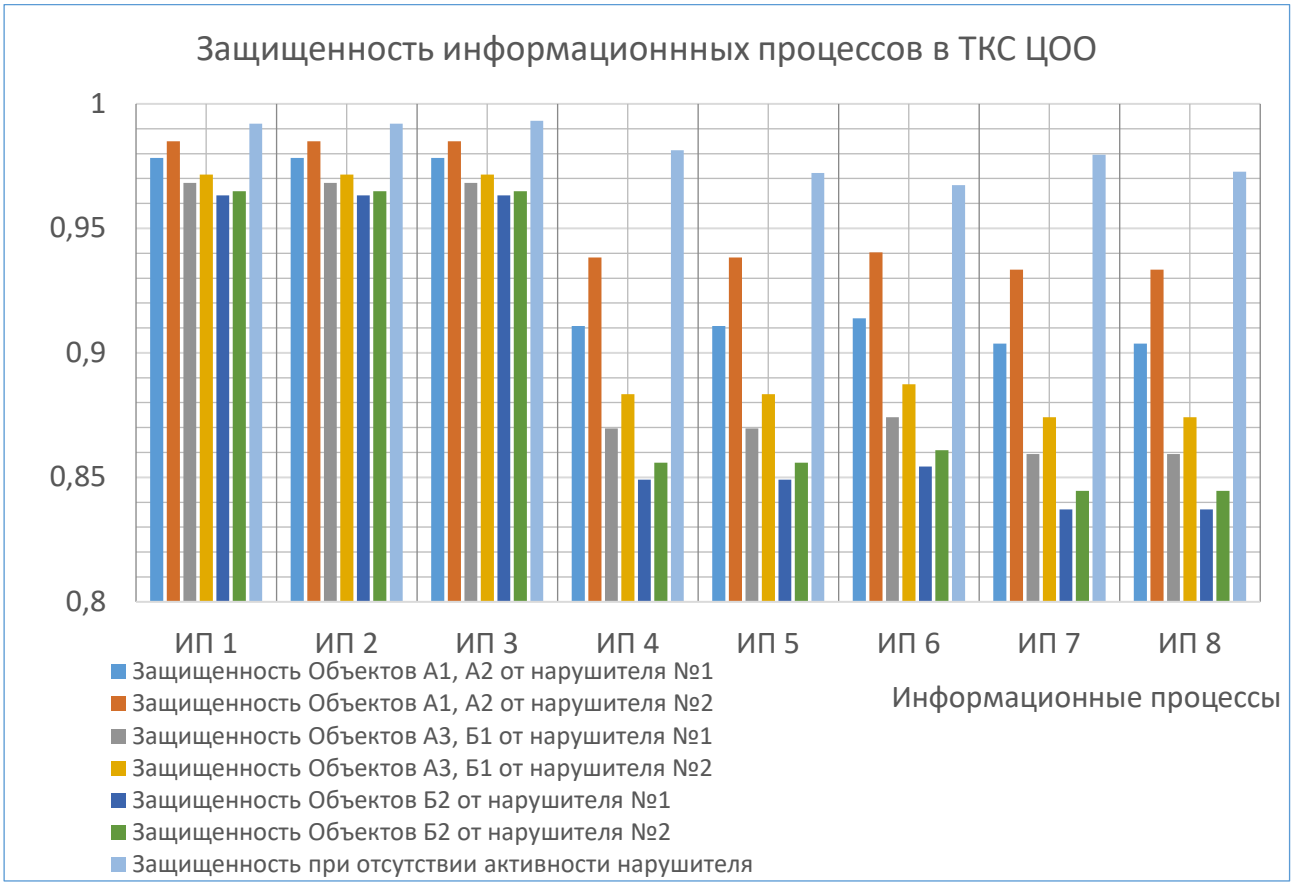

Рисунок 4.7 - Защищенность информационных процессов ТКС ЦОО

Выводы к главе 4

Составлен обобщенный алгоритм автоматизированной оценки работоспособности ТКС ЦОО на основе анализа защищенности информационных процессов в ТКС. Данный алгоритм состоит из процедур формирования экспертных баз данных, баз данных о структурных компонентах конкретной исследуемой ТКС конкретного ПЦО, оценки работоспособности ТКС.

При автоматизации расчетов необходимо ведение баз данных экспертов, структурных компонентов, информационных процессов, обобщенных функций, основных режимов функционирования; матриц связности уязвимостей, угроз, защитных механизмов и структурных компонентов; распределения угроз по доступности, целостности и конфиденциальности; правил оценки вероятности эксплуатации угрозой уязвимости, опасности угроз, возможностей нарушителя; список актуальных угроз, данные о количестве охраняемых объектов по категориям; расчетные оценки работоспособности структурных компонентов ТКС ЦОО для данного типа нарушителя

Предложен алгоритм анализа адекватности и применимости модели оценки работоспособности ТКС ЦОО. Для анализа адекватности модели предлагается ввести ошибки оператора при вводе данных уязвимостей и защитных механизмов по результатам обследования ТКС. Предлагается сделать статистически большое количество расчетов по БД опроса аудита с эмуляцией случайных ошибок оператора. Критерием адекватности и применимости модели будет являться процент ошибок первого и второго рода тестовых расчетов по сравнению с эталонными расчетами (без ошибок). При этом процент ошибок (уровень значимости) первого рода не должен превышать уровень в 5%, а ошибок второго рода 1%.

Проведен пробный пример расчетов оценки работоспособности ТКС ЦОО для конкретного мини-ПЦО. С этой целью были собраны и обезличены данные по результатам обследования о 25 объектах разных категорий. При расчетах ис-

пользовались условия ограничений и допущений, изложенные в п.2.2. В результате были получены расчеты защищенности структурных элементов и информационных процессов ТКС ЦОО для объектовых разных категорий и двух типов нарушителей.

По результатам расчётов выявлено, что защищенность объектов для всех категорий превышает 80%, что соответствует фактическому состоянию охраны по экспертным оценкам, наиболее слабым структурным элементом является связь дежурного ПЦО с нарядами охраны. При снижении категории объекта, его уровень защищенности падает, что объясняется ростом недостатков в организации охраны, увеличением уязвимостей и снижении количества и качества функционирования защитных механизмов. При повышении возможностей нарушителя (повышении опасности нарушителя), защищенность объектов всех категорий снижается.

Расчеты работоспособности структурных компонентов ТКС ЦОО мини-ПЦО для объектов разных категорий показывают, что уровень ошибок 2 рода (возможность допущения НСД на защищаемый объект) отличается у них примерно на 8-10%. При этом основное отличие у объектов разных категорий состоит в снижении эффективности действия защитных механизмов объектовых комплексов ТСО при снижении категории объектов. В целом результаты расчетов соответствуют сложившейся практике функционирования ТКС ЦОО.

По результатам расчетов даны рекомендации по установлению уровней защищённости объектов в зависимости от категории охраняемых объектов.

ЗАКЛЮЧЕНИЕ

Основная причина снижения работоспособности ТКС ЦОО связывается с недостаточной информационной защищенностью, недостатками в работе с персоналом ПЦО, и с последствиями деструктивных воздействий нарушителей. Предложена формальная модель показателя работоспособности как функции вероятностей защищенности компонентов ТКС ЦОО от множества угроз при реализации информационных процессов основных функций, определяемых режимами. Сформулирована и формализована концепция модели оценки работоспособности на основе анализа инфраструктуры ТКС ЦОО.

Предложена формальная модель показателя работоспособности как функции вероятностей защищенности компонентов ТКС от множества угроз.

Синтезированы базы данных уязвимостей, угроз, защитных механизмов, типов нарушителя и их взаимосвязи, отличающиеся универсальностью и разумной достаточностью для систем данного типа.

Выявлено 16 уязвимостей и 12 защитных механизмов обеспечения ИБ, типовых (характерных) для ТКС централизованной охраны объектов, синтезированы базы данных уязвимостей, угроз, защитных механизмов, типов нарушителя и их взаимосвязи, отличающиеся универсальностью и разумной достаточностью для систем данного типа, что позволяет эффективно и с небольшими затратами времени сроить модели угроз конкретной ТКС ЦОО.

Разработаны алгоритмы: (1) оценки вероятности реализации угрозы при наличии уязвимости компонента ТКС ЦОО, отличающийся вновь выявленными закономерностями между типом угроз и способами проявления уязвимостей; (2) оценки вероятности опасности угроз в компонентах ТКС ЦОО с учетом защитных механизмов, отличающийся вновь выявленными закономерностями между типом угроз, способом и характером действия защитных механизмов; (3) определения степени проявления уязвимостей и (4) силы защитных механизмов, выявляемых в компонентах ТКС ЦОО, оригинальность которого основана на их декомпозиции в зависимости от условий эксплуатации компонентов.

Усовершенствована модель оценки вероятности информационной защищенности компонента ТКС ЦОО, оригинальность которой состоит в том, что в модель включен элемент «Нарушитель» и сопутствующие ему параметры.

Разработан обобщенный алгоритм автоматизированной оценки работоспособности ТКС ЦОО на основе анализа защищенности ИП в ТКС. При автоматизации расчетов предлагается ведение баз данных экспертов, структурных компонентов, информационных процессов, обобщенных функций, основных режимов, матриц связности уязвимостей, угроз, ЗМ и структурных компонентов, распределения угроз по доступности, целостности и конфиденциальности, правил оценки вероятности эксплуатации угрозой уязвимости, опасности угроз, возможностей нарушителя.

Проведены расчеты работоспособности ТКС ЦОО для мини-ПЦО. Собраны данные по результатам обследования о 25 объектах разных категорий. В результате были получены оценки защищенности структурных компонентов и информационных процессов для объектов разных категорий и типов нарушителей. Выявлено, что самым низко защищённым компонентом являются объектовые комплексы ТСО.

Расчеты работоспособности структурных компонентов ТКС мини-ПЦО показывают, что уровень ошибок 2 рода (допущение НСД на защищаемый объект) отличается у них примерно на 8-10%. При этом основное отличие у объектов разных категорий состоит в снижении эффективности действия ЗМ объектовых комплексов ТСО при снижении категории объектов. В целом результаты расчетов соответствуют сложившейся практике функционирования ТКС ЦОО.

Научное развитие исследований в данном направлении автор связывает с дальнейшей автоматизацией процессов оценки работоспособности ТКС ЦОО, что позволит оперативно прогнозировать изменение состояния работоспособности всех структурных компонентов ТКС ЦОО при приеме под охрану новых объектов.

СПИСОК ИСПОЛЬЗУЕМЫХ ТЕРМИНОВ И СОКРАЩЕНИЙ

ГЗ - группа задержания

ДВ - дестабилизирующие воздействия

ДФ - дестабилизирующие факторы

ЗМ - защитные механизмы

ЗИ - защита информации

ИБ - информационная безопасность

ИП - информационные процессы

ИСБ - интегрированные системы безопасности

КАДПЛ или КАДЛ - контроллер адресной двухпроводной линии

КОС ОТС - комплекс объектовых средств охранно-тревожной сигнализации

ЛВС - локальная вычислительная сеть

НСД - несанкционированный доступ к информации

ОИ - извещатели охранно-тревожной сигнализации

ОПП - объектовый приёмо-передатчик

ОР - основные режимы функционирования

ОФ - основные функции

ПИ - преобразователь интерфейсов

ПЗ - показатель защищенности

ПР - показатель работоспособности ТКС ЦОО

ПЦО - пункт централизованной охраны

РМ - релейные модули

РСПИ - радиоканальная система передачи извещений

РФ - Режим функционирования

СПИ - система передачи извещений

ТКС - телекоммуникационная сеть

ЦОО - централизованная охрана объектов

ЦОУ - центр оперативного управления

ЦПП - центральный приемо-передатчик

GSM (англ. Global System for Mobile Communications) - стандарт сотовой связи

СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ Р 52551-2016 Системы охраны и безопасности. Термины и определения.

2. ГОСТ 26342-84 Средства охранной, пожарной и охранно- пожарной сигнализации. Типы, основные параметры и размеры.

3. ГОСТ Р52435—2005 «Технические средства охранной сигнализации. Классификация. Общие технические требования и методы испытаний», 2005.– С. 24.

4. ГОСТ Р 52436-2005 Приборы приемно-контрольные охранной и охранно-пожарной сигнализации. Классификация. Общие технические требования и методы испытаний.

5. Методическое пособие по выбору и применению пассивных оптико-электронных инфракрасных извещателей. Р 78.36.036-2013. М.: ФКУ НИЦ «Охрана», 2013. – С.195.

6. Применение радиоволновых и комбинированных извещателей с целью повышения обнаруживающей способности и помехозащищенности. Методическое пособие. Р 78.36.022-2012. М.: ФКУ НИЦ «Охрана», 2012. – С.120.

7. Выбор и применение технических средств охранной, тревожной сигнализации и средств инженерно-технической укрепленности для оборудования объектов. Рекомендации. РД 78.36.006-2005 – 2005. М.: ФКУ НИЦ «Охрана», 2005. – С.124.

8. Методическое пособие по выбору и применению охранных поверхностных звуковых извещателей для блокировки остекленных конструкций закрытых помещений. Р 78.36.044-2014. М.: ФКУ НИЦ «Охрана», 2014. – С.92.

9. Выбор и применение активных оптико-электронных извещателей для блокировки внутренних и внешних периметров, дверей, окон, витрин и подступов к отдельным предметам. Методические рекомендации. Р 78.36.050-2015. М.: ФКУ НИЦ «Охрана», 2015. – С.92.

10. Единые требования к системам передачи извещений, объектовым техническим средствам охраны и охранным сигнально-противоугонным устройствам

автотранспортных средств, предназначенным для применения в подразделениях вневедомственной охраны войск национальной гвардии Российской Федерации. М.: ФКУ НИЦ «Охрана», 2018. – С.89.

11. Инженерно-техническая укрепленность и оснащение техническими средствами охраны объектов и мест проживания и хранения имущества граждан, принимаемых под централизованную охрану подразделениями вневедомственной охраны войск национальной гвардии Российской Федерации. Методические рекомендации. Р 078-2019. М.: ФКУ НИЦ «Охрана», 2019. – 58 с.

12. Список технических средств безопасности, удовлетворяющих «Единым требованиям к системам передачи извещений, объектовым техническим средствам охраны и охранным сигнально-противоугонным устройствам автотранспортных средств, предназначенным для применения в подразделениях вневедомственной охраны войск национальной гвардии Российской Федерации» М.: ФКУ НИЦ «Охрана», 2018. – С.75.

13. Типовые проектные решения оснащения техническими средствами охраны объектов различных категорий, охраняемых подразделениями вневедомственной охраны полиции. Методические рекомендации. Р 78.36.051-2015. М.: ФКУ НИЦ «Охрана», 2015. – С. 109.

14. Типовые проектные решения по оборудованию техническими средствами охраны частных домов, коттеджей и иных мест хранения имущества граждан. Методические рекомендации. Р 074-2018. М.: ФКУ НИЦ «Охрана», 2019. – С. 133.

15. ГОСТ Р 57674-2017 Интегрированные системы безопасности. Общие положения.

16. Рекомендации по охране особо важных объектов с применением интегрированных систем безопасности. Р 78.36.018-2011. М.: ФКУ НИЦ «Охрана», 2011. – С.73.

17. Рекомендации по выбору и применению средств обнаружения проникновения в зависимости от степени важности и опасности охраняемых объектов. Р 069-2017. М.: ФКУ НИЦ «Охрана», 2017. – С.160.

18. ГОСТ Р 56102.1-2014 Системы централизованного наблюдения. Часть 1. Общие положения.

19. ГОСТ Р 56102.2-2015 Системы централизованного наблюдения. Часть 2. Подсистема объектовая. Общие технические требования и методы испытаний.

20. Рекомендации по выбору и применению объектового оборудования проводных систем передачи извещений, устойчивых к несанкционированному обходу. Р 065-2017. М.: ФКУ НИЦ «Охрана», 2019. – С. 68.

21. Применение оборудования радиоканальных систем передачи извещений (РСПИ). Рекомендации. Р 78.36.048-2015. М.: ФКУ НИЦ «Охрана», 2015. – С. 182.

22. Применение оборудования с использованием защищённых каналов передачи данных, представляемых операторами сотовой связи. Методические рекомендации. Р 78.36.053-2015. М.: ФКУ НИЦ «Охрана», 2015. – С.26.

23. Обзор-2015 Модернизация серийно выпускаемых радиоканальных систем передачи извещений (РСПИ), а также подсистем с использованием каналов сотовой связи. Аналитический обзор. М.: ФКУ НИЦ «Охрана», 2015. – С. 27.

24. Применение современных видов модуляции и организация обмена информацией в радиоканальных системах передачи извещений: Методические рекомендации Р061-2017. – М.: ФКУ «НИЦ «Охрана» Росгвардии, 2017. – С. 50.

25. Гавришев А.А. Повышение защищенности беспроводных систем безопасности: аналитический обзор публикаций. Вестник НГУ 2017 г.

26. Эсауленко А. В. Моделирование и обеспечение надежности радиоканала в системах безопасности: Автореф. дис. канд. техн. наук. Воронеж, 2015. – С.19.

27. Гавришев А. А., Жук А. П., Осипов Д. Л. Анализ технологий защиты радиоканала охранно-пожарных сигнализаций от несанкционированного доступа // Тр. СПИИРАН. 2016. Вып. 4 (47). С. 28–45.

28. ГОСТ Р 55017-2012 Пульты централизованного наблюдения для использования в системах противокриминальной защиты. Требования к информации.

29. Обзор-2015. Исследование современных методов персональной идентификации в целях применения в системах централизованного наблюдения. Аналитический обзор. М.: ФКУ НИЦ «Охрана», 2015. – С. 88.

30. Защита локальных вычислительных сетей пунктов централизованной охраны при использовании глобальной сети Интернет для передачи данных между объектовым и пультовым оборудованием СПИ. Методические рекомендации. Р 78.36.045-2014. М.: ФКУ НИЦ «Охрана», 2014. – С. 200.

31. Введение в сетевую тематику, управление и эксплуатация ЕИТКС ОВД Российской Федерации. Учебное пособие. Воронеж: Воронежский институт МВД России, 2014. – С. 263.

32. Инструкция по действиям персонала пунктов централизованной охраны в штатных и нештатных ситуациях, возникающих в ходе обеспечения централизованной охраны объектов и мест проживания и хранения имущества граждан. Методические рекомендации Р 079-2019. – М.: ФКУ НИЦ «Охрана», 2019. – С. 16.

33. Тельный А. В., Монахов М. Ю. Динамическая модель прогнозирования успешности действий нарядов физической охраны по предотвращению несанкционированного доступа нарушителя на охраняемый объект //Динамика сложных систем-XXI век. – 2017. – Т. 11. – №.3. – С. 102-109.

34. А.В. Тельный; В.А. Вилкова; Р.С. Черников «Об эффективности использования технических средств контроля несения службы нарядами физической охраны» // в сборнике: III Всероссийской научной конференции (с приглашением зарубежных ученых) «Фундаментальные проблемы информационной безопасности в условиях цифровой трансформации», 29 ноября – 01 декабря, Ставрополь, Россия, 2021

35. Лазарев, И. В. К вопросу об оценке эффективности комплекса технических средств систем охраны / И. В. Лазарев // Охрана, безопасность, связь. – 2021. – № 6-2. – С. 142-144.

36. М.Ю. Монахов; А.В. Тельный; Р.С. Черников; В.А. Вилкова «Использование рекуррентных методов в прогнозировании состояния защищенности информационных ресурсов телекоммуникационной сети» // в сборнике: Перспективные технологии в средствах передачи информации - ПТСПИ-2021 Материалы XIV международной научно-технической конференции. г. Владимир, 2021

37. А.В. Тельный, М.Ю. Монахов «Формирование динамической модели оценки показателей надежности объектовых комплексов технических средств охранной сигнализации» // Динамика сложных систем - XXI век. – 2015, № 4. – С. 34-41.

38. А.В. Тельный, Ю.М. Монахов, М.Ю. Монахов «Оценка защищенности информационных ресурсов организации от несанкционированного доступа нарушителей в здания и помещения» Известия высших учебных заведений. Технология текстильной промышленности №5 2016. – С. 259-263.

39. М.Ю. Монахов; А.В. Тельный; Р.С. Черников; В.А. Вилкова «Логико-вероятностный подход в оценке безопасности телекоммуникационной системы централизованной охраны объектов» // в сборнике: Перспективные технологии в средствах передачи информации - ПТСПИ-2021 Материалы XIV международной научно-технической конференции. г. Владимир, 2021.

40. В.А. Шаров, Р.С. Черников, А.В. Тельный «О типовом методологическом подходе анализа показателей состояния информационной безопасности на основе использования экспертных оценок» // В сборнике: Шуйская сессия студентов, аспирантов, педагогов, молодых ученых. Материалы XIII Международной научной конференции. Шуя, 2020. – С. 230-233.

41. А.В. Тельный, Е.И. Яковлева, А.Г. Романова О проведении аудита защищенности организационного канала утечки информации, составляющей коммерческую тайну организации // Системы управления, связи и безопасности. 2019. №2. – С. 36-277.

42. Hoffman L.J. Modern Methods for Computer Security and Privacy. New York: Prentice Hall; 1977. 268 p.

43. ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения».

44. Методический документ. Методика оценки угроз безопасности информации. М.: ФСТЭК России, 2021. – С.86.

45. Обследование объектов, охраняемых или принимаемых под охрану подразделениями вневедомственной охраны войск национальной гвардии Российской Федерации. Методические рекомендации Р 063-2017. М.: ФКУ НИЦ «Охрана», 2017. – С. 50.

46. ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования»

47. ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения»

48. ГОСТ Р 52447-2005 «Защита информации. Техника защиты информации. Номенклатура показателей качества»

49. ГОСТ Р ИСО 7498-2-99 «Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации»

50. ГОСТ Р ИСО/МЭК ТО 19791-2008 «Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем»

51. ГОСТ Р ИСО/МЭК 27007-2014 «Информационная технология. Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности»

52. ГОСТ Р ИСО/МЭК 27033-3-2014 «Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 3. Эталонные сетевые сценарии. Угрозы, методы проектирования и вопросы управления»

53. ФСТЭК РФ RD 1992.03.30.01 «Автоматизированные системы. Защита от несанкционированного доступа к информации Классификация автоматизированных систем и требования по защите информации»

54. ФСТЭК РФ RD 1992.03.30.02 «Средства вычислительной техники Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации»

55. ФСТЭК РФ RD 1992.03.30.03 «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации»

56. Ложные срабатывания технических средств охранной сигнализации и методы борьбы с ними. Методические рекомендации. Р 076 – 2018. М.: ФКУ НИЦ «Охрана», 2018. –С. 41 с.

57. Меньших В.В., Калков Д.Ю. Обоснование состава и структуры моделей поддержки принятия решений в укрупнённом пункте централизованной охраны с использованием системного подхода / журнал «Вестник Воронежского института МВД России №2/2015.»

58. Шепитько Г.Е. Проблемы охранной безопасности объектов: монография. 2-е изд. – М.: АЭБ, 2010. – С. 208.

59. ГОСТ Р 50009-2000 Совместимость технических средств электромагнитная. Технические средства охранной сигнализации. Требования и методы испытаний.

60. Мироненко Я. Электромагнитная совместимость в беспроводных системах охраны // Алгоритм безопасности. 2013. № 3. С. 50–55.

61. Михайлов А. Выбор оптимального метода кодирования в РСПИ // Технологии защиты. 2016. № 1. URL: http://www.tzmagazine.ru/jpage.php?uid1=1496&uid2=1497 &uid3=1507 (дата обращения 10.05.2021).

62. Брауде-Золотарев Ю. Алгоритмы безопасности радиоканалов // Алгоритм безопасности. 2013. № 1. С. 64–66.

63. Жук А. П., Гавришев А. А. Альтернативный подход повышения структурной скрытности сигналов-переносчиков устройства имитозащиты контролируемых объектов // Спецтехника и связь. 2015. № 2. С. 59–63.

64. И.М. Нурмухаметов, А.А. Клочков, Д.А. Николаев «О перспективах развития систем передачи извещений, работающих по каналам, предоставляемым операторами сотовой связи» // Алгоритм Безопасности № 6, 2018 г.

65. Тельный А. В. «О некоторых аспектах достоверности мониторинга радиоканальных систем передачи извещений» [Текст] // X международная научно-техническая конференция «Перспективные технологии в средствах передачи информации» – ПТСПИ – 2013, Владимир, 26-28 июня 2013г. Владимир: Издательство ВлГУ т.1. 223с, 2013. . – С. 118-120.

66. Оленин Ю.А. Системы и средства управления физической защитой объектов: монография. Пенза: инф.-изд. центр ПГУ, 2002. . – С. 212.

67. Быстров С.Ю. Анализ и оптимизация систем физической защиты особо важных объектов: специальность 05.13.01 «Системный анализ, управление и обработка информации»: автореферат диссертации на соискание ученой степени кандидата технических наук / Быстрой Сергей Юрьевич. – Пенза 2004.

68. Ахлюстин С. Б. Математическое моделирование оценки защищенности объектов с эргатическими интегрированными системами безопасности: специальность 05.13.18 «Математическое моделирование, численные методы и комплексы программ»: автореферат диссертации на соискание ученой степени кандидата технических наук / Ахлюстин Сергей Борисович. – Воронеж 2019.

69. Калков Д. Ю. Модели и алгоритмы оптимизации порядка проверки охраняемых объектов при получении сигналов тревоги: специальность 05.13.18 «Математическое моделирование, численные методы и комплексы программ»: автореферат диссертации на соискание ученой степени кандидата технических наук / Калков Дмитрий Юрьевич. – Воронеж 2016.

70. Абросимова, Е.М. Модели и процедуры оценки эффективности противодействия угрозам информационной безопасности укрупненных пунктов централизованной охраны: специальность 05.13.19 «Методы и системы защиты информации, информационная безопасность»: автореферат диссертации на соискание ученой степени кандидата технических наук / Абросимова Евгения Михайловна. – Воронеж, 2015.

71. Рогожин, А.А. Модели и алгоритмы оценки надежности интегрированных систем безопасности охраняемых объектов: специальность 05.13.18 «Математическое моделирование, численные методы и комплексы программ»: автореферат диссертации на соискание ученой степени кандидата технических наук / Рогожин Александр Александрович. – Воронеж, 2017.

72. Абросимова, Е. М. Методические основы формализованного представления угроз информационной безопасности укрупненных пунктов централизованной охраны / Е. М. Абросимова, С. В. Зарубин // Вестник Воронежского института МВД России. – 2014. – № 1. – С. 112-119.

73. Абросимова, Е. М. Функциональное представление противоправных действий по проникновению на охраняемые объекты / Е. М. Абросимова, Т. Б. Ходырев, В. С. Зарубин // Вестник Воронежского института МВД России. – 2014. – № 4. – С. 290-298.

74. Кротов, А. И. К вопросу автоматизации процесса выбора качественного программного обеспечения в условиях цифровой трансформации / А. И. Кротов, А. Н. Морозов, С. А. Гришин // Академический вестник войск национальной гвардии Российской Федерации. – 2020. – № 1. – С. 57-61.

75. Абросимова, Е. М. Организация защиты информации в пунктах централизованной охраны отделов вневедомственной охраны полиции / Е. М. Абросимова, И. В. Щербакова // Символ науки: международный научный журнал. – 2015. – № 11-1. – С. 10-12.

76. Тельный, А. В., Р. С. Черников «Алгоритм обработки тревожных извещений объектовых средств охранной сигнализации для снижения уровня ложных срабатываний» // Системы управления, связи и безопасности. – 2019. – №4. – С. 140-162.

77. Таравков, М. В. Имитостойкость систем тревожной сигнализации / М. В. Таравков // Охрана, безопасность, связь. – 2021. – № 6-1. – С. 117-123.

78. Буйневич, М. В. Архитектурные модели комплексной и интегрированной безопасности информационных систем: сравнительный анализ подходов / М. В. Буйневич, О. В. Ложкина, А. Ю. Ярошенко // Научно-аналитический журнал

Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России. – 2021. – № 1. – С. 100-108.

79. Гущина, А. А. К вопросу защиты информации систем охраны и безопасности объектов / А. А. Гущина, П. Д. Коратаев, М. Ю. Пакляченко // Охрана, безопасность, связь. – 2021. – № 6-1. – С. 25-32.

80. Тельный А.В., Монахов М.Ю., Монахов Ю.М. Автоматизация оценки достаточности технических средств охраны и безопасности для защиты от несанкционированного доступа производственного объекта Известия высших учебных заведений. Технология текстильной промышленности №5 2016. – С. 263-267.

81. Модель определения затрат вычислительных ресурсов для развертывания интегрированной системы безопасности / К. В. Пителинский, И. А. Простов, С. С. Амфитеатрова, Д. А. Ермолатий // Вопросы защиты информации. – 2021. – № 3(134). – С. 45-51.

82. Моделирование функционирования интегрированной системы безопасности как информационной системы / С. В. Белокуров, О. А. Кондратов, В. Н. Третьяков, А. В. Меркулов // Актуальные проблемы деятельности подразделений УИС: сборник материалов Всероссийской научно-практической конференции, Воронеж, 20 мая 2021 года. – Воронеж: Издательско-полиграфический центр "Научная книга", 2021. – С. 186-189.

83. Белокуров, С. В. Анализ уровня защищенности современных интегрированных систем безопасности / С. В. Белокуров, В. Н. Третьяков, А. В. Меркулов // Актуальные проблемы деятельности подразделений УИС: Сборник материалов Всероссийской научно-практической конференции: в 2-х томах, Воронеж, 23 октября 2020 года / Ответственный за выпуск Д. Г. Зыбин. – Воронеж: Воронежский институт Федеральной службы исполнения наказаний России, 2020. – С. 253-260.

84. Анализ графа состояний функционирования интегрированной системы безопасности / С. В. Белокуров, О. А. Кондратов, В. Н. Третьяков, А. В. Мерку-

лов // Актуальные проблемы деятельности подразделений УИС: сборник материалов Всероссийской научно-практической конференции, Воронеж, 20 мая 2021 года. – Воронеж: Издательско-полиграфический центр «Научная книга», 2021. – С. 189-191.

85. К вопросу об архитектуре комплексных и интегрированных систем безопасности: протокол-ориентированный подход / М. В. Буйневич, К. Е. Израилов, В. В. Покусов, А. Ю. Ярошенко // Актуальные проблемы защиты и безопасности: Труды XXIV Всероссийской научно-практической конференции РАРАН, Санкт-Петербург, 31 марта – 03 2021 года. – Москва: Российская академия ракетных и артиллерийских наук, 2021. – С. 377-383.

86. Логинов, И. В. Формирование подхода к разработке модели жизненного цикла интегрированных систем безопасности / И. В. Логинов, В. Г. Сосунов // Вопросы безопасности. – 2021. – № 4. – С. 50-60. – DOI 10.25136/2409-7543.2021.4.37121.

87. Лепешкин, О. М. Концепция интеллектуализации контроля безопасности связи в информационно-телекоммуникационной сети специального назначения / О. М. Лепешкин, Ю. К. Худайназаров // Состояние и перспективы развития современной науки по направлению «Информационная безопасность»: Сборник статей III Всероссийской научно-технической конференции, Анапа, 21–22 апреля 2021 года. – Анапа: Федеральное государственное автономное учреждение "Военный инновационный технополис "ЭРА", 2021. – С. 697-709.

88. А.В. Тельный, М.Ю. Монахов, Г.Е. Монахова «Частные показатели доступности интегрированных систем безопасности для предприятий текстильной промышленности» Известия высших учебных заведений. Технология текстильной промышленности №5 2018. – С. 235-239.

89. Зацаринный, А. А. Процессные аспекты нормативного регулирования работ по комплексному обеспечению информационной безопасности и интероперабельности интегрированных систем управления / А. А. Зацаринный, С. В. Козлов // Информатика: проблемы, методы, технологии : Материалы XXI Международной научно-методической конференции, Воронеж, 11–12 февраля 2021

года. – Воронеж: Общество с ограниченной ответственностью "Вэлборн", 2021. – С. 1167-1176.

90. Использование маршрутизаторов для защиты пультового оборудования ПЦО при работе с объектовыми СПИ по сети Интернет / А. В. Голубев, В. А. Николаев, А. Н. Осипов, З. И. Голубева // Алгоритм безопасности. – 2018. – № 4. – С. 58-60.

91. Воробьев П. Некоторые вопросы защищенности цифровых сетей ОВО // Специализированный информационно-аналитический журнал о проблемах безопасности. 2014. № 4.

92. Свидетельство о государственной регистрации программы для ЭВМ №2015610579 Российская Федерация. Программа математического моделирования противодействия угрозам информационной безопасности укрупнённых пунктов централизованной охраны: № 2014619474: заявл. 22.09.2014; опубл. 14.01.2015 / Г. Ю. Белый, Е. М. Абросимова, В. С. Зарубин, С. В. Скрыль ; заявитель федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Воронежский государственный университет».

93. Абросимова, Е. М. Методические основы формализованного представления угроз информационной безопасности укрупненных пунктов централизованной охраны / Е. М. Абросимова, С. В. Зарубин // Вестник Воронежского института МВД России. – 2014. – № 1. – С. 112-119.

94. О некоторых допущениях в математической интерпретации угроз нарушения целостности и доступности информации в компьютерных системах / В. Н. Финько, В. С. Зарубин, В. В. Киселев, С. Н. Хаустов // Информация и безопасность. – 2009. – Т. 12. – № 4. – С. 625-626.

95. Зарубин, С. В. Оценка эффективности механизмов комплексного контроля информационных процессов / С. В. Зарубин, В. С. Зарубин, А. И. Кротов // Современные инновации в науке и технике: сборник научных трудов 11-й Всероссийской научно-технической конференции с международным участием,

Курск, 15–16 апреля 2021 года. – Курск: Юго-Западный государственный университет, 2021. – С. 74-77.

96. Воробьев, А. В. Построение модели каналов утечки конфиденциальной информации объектов МВД на основе анализа инцидентов информационной безопасности объектов информатизации / А. В. Воробьев // Актуальные вопросы эксплуатации систем охраны и защищенных телекоммуникационных систем: Сборник материалов Всероссийской научно-практической конференции, Воронеж, 10 июня 2021 года. – Воронеж: Воронежский институт Министерства внутренних дел Российской Федерации, 2021. – С. 78-80.

97. Зарубин, С. В. К вопросу определения информационного объема программных средств защиты информации в автоматизированных системах безопасности / С. В. Зарубин, В. С. Зарубин, А. Р. Фамильнов // Современные инструментальные системы, информационные технологии и инновации : Сборник научных трудов XVI Международной научно-практической конференции, Курск, 18–19 марта 2021 года / Отв. редактор М.С. Разумов. – Курск: Юго-Западный государственный университет, 2021. – С. 93-97.

98. Зарубин, В. С. Двухуровневое управление механизмами защиты информации в системах охранного мониторинга / В. С. Зарубин, С. В. Зарубин // Перспективы развития технологий обработки и оборудования в машиностроении : Сборник научных статей 3-й Всероссийской научно-технической конференции с международным участием, Курск, 15–16 февраля 2018 года / Ответственный редактор А.А. Горохов. – Курск: Закрытое акционерное общество "Университетская книга", 2018. – С. 110-114.

99. Перминов, Г.В. Концептуальная модель технологии функционирования защищенной автоматизированной информационной системы / Г. В. Перминов, С. В. Зарубин // Охрана, безопасность, связь. – 2019. – Т. 1. – № 4(4). – С. 192-197.

100. Зарубин, С.В. Функционально-информационное моделирование противоправных действий по реализации угроз информационным процессам в автоматизированных комплексах охраны и действий по защите информации в этих

системах / С. В. Зарубин // Фундаментальные проблемы системной безопасности: Материалы школы-семинара молодых ученых, посвященной 60-летию запуска первого в мире искусственного спутника Земли, Севастополь, 13–15 сентября 2017 года. – Севастополь: Цифровая полиграфия, 2017. – С. 204-208.

101. Зарубин, С. В. Формализованное представление угроз информационной безопасности в комплексах инженерно-технических средств систем физической защиты / С. В. Зарубин, Т. Б. Ходырев // Актуальные проблемы деятельности подразделений УИС : Сборник материалов Всероссийской научно-практической конференции, Воронеж, 25 мая 2017 года. – Воронеж: Издательско-полиграфический центр "Научная книга", 2017. – С. 98-101.

102. Зарубин, С. В. К вопросу о показателе эффективности противодействия угрозам безопасности информационных систем управления / С. В. Зарубин, Т. Б. Ходырев // Охрана, безопасность, связь. – 2017. – № 1-1. – С. 112-115.

103. Зарубин, В. С. Подходы к моделированию механизмов защиты информации в технических системах безопасности и охранного мониторинга / В. С. Зарубин, С. В. Зарубин // Общественная безопасность, законность и правопорядок в III тысячелетии. – 2017. – № 3-3. – С. 272-278.

104. Никитина, Ю. С. Особенности унифицированного математического представления показателя эффективности мер противодействия проникновению на охраняемые объекты в условиях вредоносного воздействия на информацию интегрированных систем безопасности / Ю. С. Никитина, С. В. Зарубин, В. А. Половинкин // Общественная безопасность, законность и правопорядок в III тысячелетии. – 2016. – № 1-2. – С. 219-224.

105. Пьянков, О. В. Апробация численного метода поиска оптимального места расположения группы задержания / О. В. Пьянков, Д. О. Смышников // Вестник Воронежского института МВД России. – 2021. – № 1. – С. 62-71.

106. Грибенюк, И. И. Действия группы задержания вневедомственной охраны при осмотре местности и задержании правонарушителей в различных ситуациях несения службы / И. И. Грибенюк // Практика служебно-боевого применения войск при проведении специальных операций и мероприятий : Сборник

научных статей по материалам межвузовской конференции, Новосибирск, 16 апреля 2021 года. – Новосибирск: Новосибирский военный институт имени генерала армии И.К. Яковлева войск национальной гвардии Российской Федерации, 2021. – С. 155-163.

107. Копылов, А. Н. Алгоритм поиска оптимального местоположения группы задержания при выполнении задач по охране объектов / А. Н. Копылов // Вестник Воронежского института МВД России. – 2021. – № 2. – С. 100-107.

108. Пьянков, О. В. Численный метод поиска оптимального места расположения группы задержания / О. В. Пьянков, А. Н. Копылов, Д. О. Смышников // Вестник Воронежского института МВД России. – 2020. – № 2. – С. 52-58.

109. Пьянков, О. В. Модель принятия решения по повышению оперативности реагирования групп задержания с применением роевых алгоритмов / О. В. Пьянков, А. В. Попов // Вестник Воронежского института МВД России. – 2020. – № 4. – С. 73-83.

110. Смышников, Д. О. Математическая модель размещения групп задержания при осуществлении охранной деятельности / Д. О. Смышников // Вестник Воронежского института МВД России. – 2019. – № 1. – С. 83-90.

111. Сошнева, Д. А. Определение оптимального количества групп задержания на обслуживаемой территории / Д. А. Сошнева // Охрана, безопасность, связь. – 2019. – Т. 1. – № 4(4). – С. 105-109.

112. Применение общего логико-вероятностного метода для анализа технических, военных организационно-функциональных систем и вооруженного противоборства: монография / В.И. Поленин [и др.]; под общ. ред. А.С. Можаева. – СПб.: НИКА, 2011. –С. 410

113. Классификация методов защиты информации на основе кластерного анализа / В. В. Меньших, М. В. Питолин, О. В. Пьянков, И. В. Щербакова. // Воронеж: Вестник ВГТУ. – 2009. – Т. 5. – № 6. – С. 203 – 205.

114. Пьянков, О.В. Оптимизация процессов обработки сообщений в системах передачи информации // Вестник Воронежского института МВД России. – 2016. – № 2 – С. 183 – 190.

115. Тельный, А.В., Черников, Р.С. Алгоритм обработки тревожных извещений объектовых средств охранной сигнализации для снижения уровня ложных срабатываний // Системы управления, связи и безопасности. – 2019. – № 4. – С. 140-162.

116. Тельный, А. В., Черников, Р. С., Яковлева, Е. И. О возможности локализации местоположения устройства съема информации по радиоканалу // Проектирование и технология электронных средств. – 2020 – № 2. – С. 16-22.

117. Черников, Р. С., Путренкова, К. А. Актуальные проблемы обеспечения информационной безопасности объектов уголовно-исполнительной системы // Вестник ФКУ НИИИТ ФСИН России: научно-практическое издание. – Тверь, 2019. – С. 140-143.

118. Тельный, А.В., Монахов, М.Ю., Черников, Р.С., Вилкова, В.А. Логико-вероятностный подход в оценке безопасности телекоммуникационной системы централизованной охраны объектов // в сборнике ПТСПИ-2021 Материалы XIV международной научно-технической конференции. г. Владимир. – 2021. – С. 218-222.

119. Тельный, А. В., Черников, Р. С., Шаров, В. А. О возможности использования ситуационной видеоаналитики // Шуйская сессия студентов, аспирантов, педагогов, молодых ученых: Материалы XIII Международной научной конференции, Москва-Иваново-Шуя. – 2020. –С. 224-227.

120. Черников, Р. С., Тельный, А. В., Шаров, В. А. О типовом методологическом подходе анализа показателей состояния информационной безопасности на основе использования экспертных оценок // Материалы XIII Международной научной конференции, Москва-Иваново-Шуя. – 2020. – С. 230-233.

121. Черников, Р. С. Особенности методики применения нелинейных локаторов при проведении мероприятий по обнаружению технических средств и устройств // V Международный пенитенциарный форум "Преступление, наказание, исправление": Сборник тезисов. – Рязань: Академия права и управления ФСИН. – 2021. – С. 307-311.

122. Черников, Р. С., Тельный, А. В., Вилкова, В. А. Об эффективности использования технических средств контроля несения службы нарядами физической охраны // FISP-2021: Фундаментальные проблемы информационной безопасности в условиях цифровой трансформации: Сборник докладов III Всероссийской научной конференции (с приглашением зарубежных ученых), Ставрополь. – 2021. - С. 100-105.

123. Черников, Р. С., Монахов, М. Ю., Тельный, А. В., Вилкова, В. А. Использование рекуррентных методов в прогнозировании состояния защищенности информационных ресурсов телекоммуникационной сети // в сборнике ПТСПИ-2021 Материалы 14-ой международной научно-технической конференции, Владимир. – 2021. – С. 218-222.

124. Черников, Р. С. Особенности методики применения сканерных приемников и программно-аппаратных комплексов радиоконтроля // Актуальные вопросы информатизации: Сборник материалов IV круглого стола. – ФКУ НИИИТ ФСИН России Тверь. – 2022. – С. 276-282.

125. Черников, Р. С. Некоторые аспекты применения биометрической идентификации в учреждениях и органах уголовно-исполнительной системы // Информационные технологии в УИС. – 2020. – № 3. –С. 53-58.

126. Черников Р.С. Программа оценки вероятности опасности угроз по последствиям их реализации с учетом защитных механизмов [Текст]: свидетельство о регистрации программы для ЭВМ №2022682661 / Матвеева Е.А., Вилкова В.А., Тельный А.В., Монахов М.Ю. - №2022682661; заявл. 20.10.2022; зарегистр. 24.11.2022.

127. Черников Р.С. Программа оценки вероятности эксплуатации угрозой уязвимости компонента ТКС ЦОО [Текст]: свидетельство о регистрации программы для ЭВМ №2022680341 / Матвеева Е.А., Вилкова В.А., Тельный А.В., Монахов М.Ю. - №2022680341; заявл. 20.10.2022; зарегистр. 31.10.2022.

128. Черников, Р. С. Обеспечение информационной безопасностиобъектов уголовно- исполнительной системы / Р. С. Черников, Р. Н. Тихомиров. – Владимир : Владимирский юридический институт Федеральной службы исполнения наказаний, 2022. – 80 с. – ISBN 978-5-93035-776-9.

Приложение 1.

Описание распространенных интегрированных систем безопасности

Общие требования к интегрированным системам безопасности (ИСБ) следующие:

- ИСБ должны соответствовать требованиям ГОСТ Р 57674-2017. Системы, входящие в состав ИСБ, должны обеспечивать необходимую аппаратную, программную и эксплуатационную совместимость между собой. В ТУ на ИСБ (системы и отдельные технические средства, входящие в состав ИСБ) должны быть указаны назначение, основные технические характеристики систем и технические средства в зависимости от возложенных на них функций;

- АРМ локальных ИСБ должны исключать возможность автоматического (программного) сброса (пропадания с устройств визуального отображения информации) поступивших тревожных извещений, сброс (отработка) извещений должна осуществляться исключительно оператором АРМ;

- возникновение криминальной угрозы, выявленной системой тревожной сигнализации (СТС), системой охранной сигнализации (СОС) или системой охранной телевизионной (СОТ) должно переводить систему контроля и управления доступом (СКУД) в режим реагирования на соответствующую криминальную угрозу, по алгоритму, учитывающему специфики защищаемого объекта. Для обеспечения возможности сопряжения ИСБ с СПИ, получающими извещения о состоянии охраняемого объекта посредством замыкания/размыкания электрических контактов устройств объектовых оконечных, в составе ИСБ должны входить технические средства, имеющие релейные выходы, обеспечивающие тактику, согласующуюся с тактикой работы СПИ;

- программное обеспечение (ПО) ИСБ в целом и отдельных ТС в составе ИСБ должно быть защищено от НСД. Требования по защите ПО должны обеспечиваться средствами разграничения доступа к ПО с помощью использования паролей с разделением по предоставляемым правам. ПО ИСБ в целом и отдель-

ных ТС в составе ИСБ должно соответствовать требованиям надежности и эффективности по ГОСТ 28195-89 и должно быть устойчиво к случайным или преднамеренным воздействиям следующего вида: отключение питания ТС; программный сброс ТС; аппаратный сброс ТС; случайное нажатие клавиш или их сочетания с частотой от 1 до 10 нажатий в секунду в течение не менее 10 минут.

После указанных воздействий и перезапуска ПО, должна сохраняться работоспособность ИСБ и сохранность ранее полученных данных.

СТС и СОС, входящие в состав ИСБ, должны:

- осуществлять контроль состояние ШС;

- контролировать работоспособность и состояние входящих в нее ТС, интерфейсов и линии связи;

- осуществлять управление постановкой и снятием с охраны;

- обеспечивать возможность формирования и передачи тревожных и служебных извещений на АРМ локальной ИСБ и (или) ПЦН;

- обеспечивать работоспособность при отключении основного источника электропитания, получая электропитание от резервного источника электропитания, в течение времени, необходимого для восстановления работоспособности основного источника электропитания (конкретное значение времени зависит от категории электроснабжения защищаемого объекта и должно указываться в технической документации на ИСБ);

- не выдавать ложных извещений при переходе электропитания с основного источника электропитания на резервный и обратно.

Адресные ШС СТС и СОС должны соответствовать требованиям ГОСТ 52436-2005. Время от момента перехода любого адресного извещателя в тревожный режим до момента отображения тревожного извещения на световых и звуковых охранных оповещателях, индикаторных панелях, пультах управления, АРМ и ПЦН не должно превышать 10 с. В СТС и СОС должны быть реализованы функции управления внешними световым и звуковым оповещателями со следующей тактикой оповещения.

Для светового оповещателя: СОС снят с охраны - оповещатель находится в режиме отсутствия свечения; СТС и СОС в дежурном режиме - оповещатель находится в режиме непрерывного свечения; СТС и СОС в тревожном режиме - оповещатель находится в режиме прерывистого свечения с частотой повторения от 0,5 до 2 Гц.

Для звукового оповещателя: СОС снят с охраны, СТС и СОС в дежурном режиме - оповещатель выключен; СТС и СОС в тревожном режиме - оповещатель включен на ограниченное время. СТС и СОС должны иметь возможность подключения ТС, имеющих не менее двух реле с переключающимися контактами.

Технические средства, входящие в состав СТС и СОС, должны иметь возможность программного или аппаратного задания следующих тактик работы релейных выходов: «охранный ПЦН», «световой оповещатель», «звуковой оповещатель».

Требования к устройствам постановки/снятия с охраны. ТС СТС и СОС, производящие постановку/снятие с охраны при помощи клавиатуры должны применять коды разрядностью не менее четырех знаков. В СТС и СОС, использующих такие ТС должна быть предусмотрена защита от подбора кода (при троекратном введении неверного кода должно происходить временное блокирование возможности введения кода, а после троекратного блокирования - формироваться извещение о тревоге). В ТС, с помощью которых осуществляется постановка на охрану и снятие с охраны, не допускается применение в качестве устройств снятия с охраны тумблеров, кнопок и т.п. Изменение настроек и режимов работы ТС СТС и СОС должно быть невозможно при нахождении СТС и СОС в режиме охраны.

Описание распространенных ИСБ

«Орион-Про».

Структурная схема ИСБ представлена на Рисунке П1.1.

ИСБ «Орион-Про» представляет собой совокупность аппаратных и программных средств для организации систем охранно-пожарной сигнализации, контроля доступа, видеонаблюдения, автоматического пожаротушения, а также для создания систем контроля и диспетчеризации объектов. Система обеспечивает:

- Сбор, обработку, передачу, отображение и регистрацию извещений о состоянии шлейфов охранной, тревожной и пожарной сигнализации;
- Контроль и управление доступом (управление преграждающими устройствами типа шлагбаум, турникет, ворота, шлюз, дверь и т. п.);
- Видеонаблюдение и видеоконтроль охраняемых объектов;
- Управление пожарной автоматикой объекта;
- Взаимодействие с инженерными системами зданий;
- Модульную структуру, позволяющую оптимально оборудовать как малые, так и очень большие распределенные объекты;
- Защищенный протокол обмена по каналу связи между приборами.

Основные технические данные локальной ИСБ "Орион"

Количество приборов, подключаемых к линии интерфейса RS-485	до 127
Количество зон, объединяемых в разделы	до 16 000
Количество зон, объединяемых в разделы (ПКУ «С2000М»)	до 2048
Количество разделов	до 10 000
Количество разделов (ПКУ «С2000М»)	до 512
Количество точек доступа	до 254
Количество выходов для управления внешними устройствами	до 16 000
Количество выходов для управления внешними устройствами (ПКУ «С2000М»)	до 255
Количество пользователей (АРМ «Орион Про»)	не ограничено
Количество пользователей (ПКУ «С2000М»)	до 2047
Длина линии интерфейса RS-485	до 3 000

Рисунок П1.1 - Структурная схема ИСБ «Орион-Про» (www.bolid.ru)

Состав ИСБ «Орион-Про». Для построения адресной охранной сигнализации используются (Рисунок П1.2): контроллер двухпроводной линии связи «С2000-КДЛ» или «С2000-КДЛ-2И» и адресные извещатели: «С2000-ИК» - охранный объёмный оптико-электронный извещатель; «С2000-ИК исп.02» - охранный объёмный оптико-электронный извещатель с защитой от животных до 10 кг; «С2000-ИК исп.04» - охранный объёмный оптико-электронный извещатель с формой зоны обнаружения типа «штора»; «С2000-ШИК» — охранный оптико-электронный поверхностный извещатель; «С2000-ПИК» — охранный объёмный потолочный оптико-электронный извещатель; «С2000-СТ» — охранный поверхностный звуковой извещатель; «С2000-СТ исп.03» - охранный поверхностный звуковой извещатель с функцией антимаскирования; «С2000-СТИК» — охранный совмещённый объёмный оптико-электронный и поверхностный звуковой извещатель; «С2000-ПИК-СТ» - потолочный охранный совмещённый объёмный оптико-электронный и поверхностный звуковой извещатель; «С2000-ПИРОН» - уличный охранный объёмный оптико-электронный извещатель с защитой от животных до 20 кг; «С2000-ПИРОН-Ш» - уличный охранный оптико-электронный поверхностный извещатель с защитой от животных до 20 кг; «С2000-В» — охранный вибрационный поверхностный извещатель; «С2000-СМК» — охранный магнитоконтактный извещатель («С2000-СМК Эстет» в исполнении для металлических дверей); «С2000-КТ» тревожная кнопка.

Для управления различными исполнительными устройствами (например, световыми и звуковыми оповещателями) могут использоваться сигнально-пусковые блоки «С2000-СП2» и/или «С2000-СП2 исп.02» (с контролем пусковых цепей). Тактику работы любого релейного выхода можно запрограммировать, как и привязку срабатывания (от конкретного шлейфа или от группы шлейфов). Также в адресную линию контроллера «С2000-КДЛ» можно включать адресные расширители «С2000-АР1» (адресная метка), «С2000-АР2» (2 ШС), «С2000-АР8» (8 ШС), к которым, в свою очередь, могут подключаться неадресные извещатели с питанием от отдельного источника.

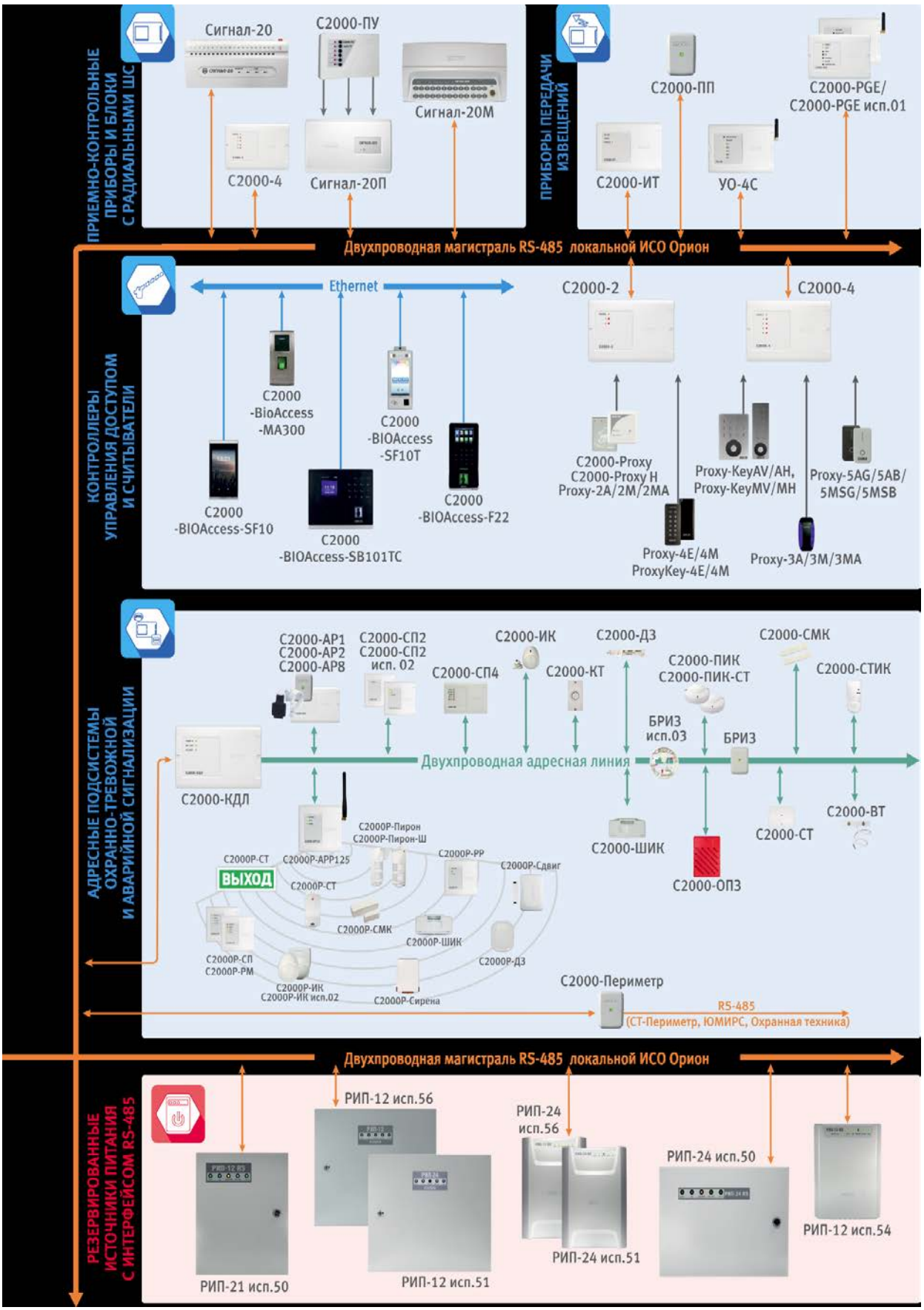

Рисунок П1.2 Структура ОТС для ИСБ «Орион-Про»

ИСБ «Рубеж-08».

Интегрированная система безопасности "РУБЕЖ-08" - комплекс, состоящий из прибора приемно-контрольного охранно-пожарного и управления ППКОПУ 01059-1000-3 «Р-08» и дополнительного оборудования к нему. Комплекс, состоящий из прибора ППКОПиУ "Р-08" и дополнительного оборудования, служит основой для создания ИСБ средних и крупных объектов, в состав которых входят подсистемы: охранной сигнализации, тревожной сигнализации, пожарной сигнализации, технологической сигнализации, контроля и управления доступом, управления исполнительными устройствами. Аппаратная интеграция подсистем на уровне оборудования и независимость работы от компьютера обеспечивают высокую эффективность и надежность функционирования системы. Основные возможности:

- Аппаратная интеграция подсистем на уровне оборудования
- Поддержка до 1000 объектов технических средств (шлейфов сигнализации, точек доступа, исполнительных устройств) сигнализации
- Подключение до 256 сетевых устройств к двум линиям связи, обеспечивающим обмен информацией по протоколу RS485
- Контроль шлейфов пожарных извещателей всех типов (ДИП, ИДПЛ)
- Контроль шлейфов технологических систем (газоанализаторов, кондиционирования, датчиков утечки воды, газа)
- Организация работы тамбур-шлюзов
- Постоянный контроль линий связи и шлейфов сигнализации
- Встроенный язык макропрограммирования Рубеж Скрипт
- Встроенный 4-х строчный ЖК-дисплей
- Современный дружественный интерфейс оператора, позволяющий выдавать сообщения на дисплей БЦП (Блок Центральный Процессорный) в терминах объекта охраны, с указанием названий помещений
- Многоуровневая система разграничения полномочий операторов и пользователей системы

- Восемь вариантов исполнения БЦП, в том числе со встроенным блоком бесперебойного питания, а также врезном исполнении
- Исполнение всех сетевых устройств в конструктивах IP20 и IP65
- Программное обеспечение для организации АРМ различных служб системы безопасности (ПО Р-08)

Общая структурная схема ИСБ «Рубеж-08» представлена на рисунке П1.3

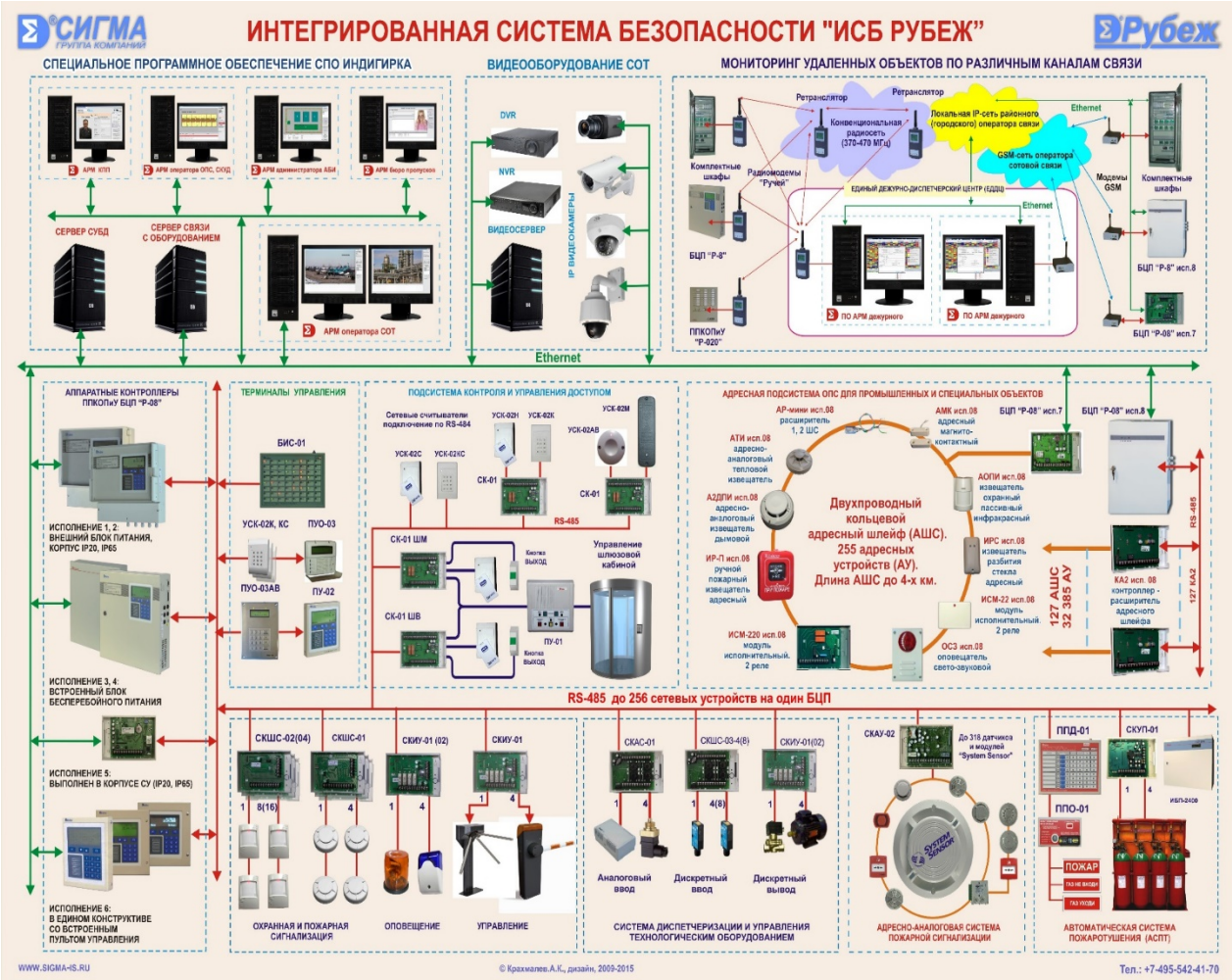

Рисунок П13 - Структурная схема ИСБ «Рубеж-08» (http://www.sigma-is.ru/)

ИСБ «Стрелец-Интеграл»

Решаемые задачи: пожарная безопасность объекта; охранная и технологическая безопасность объекта; локация персонала на территории объекта внутри здания по сигналам датчиков и вне здания по спутникам GPS/ ГЛО-

НАСС; пейджинг (общее, групповое, индивидуальное оповещение). Особенности ИСБ «Стрелец-Интеграл»: глобальный роуминг для всех устройств: надежность и живучесть системы; 10 лет работы от батарей; 2000 радиоустройств в системе; 3 сек скорость запуска; 1200 м дальность связи; высокая помехоустойчивость; автоматическое программирование всех параметров по радиосети; браслет - локация внутри и вне здания. персональное автоматическое оповещение о пожаре; пейджинг -рассылка информационных сообщений с контролем доставки.

Структурная схема ИСБ «Стрелец-Интеграл» приведена на рисунке П1.4.

Технические характеристики	
Дальность связи (открытое пространство): - между радиорасширителями; - между радиорасширителем и дочерним устройством (режим повышенной дальности); - между радиорасширителем и дочерним устройством (стандартный режим)	 до 2 000 м до 3500 м до 1200 м
диапазон рабочих частот	864-865; 868,0-868,2; 868,7-869,2 МГц
мощность излучения, не более	25 мВт
количество частотных каналов	6 шт.
диапазон рабочих температур	-30..+55 °С

Радиоканальные устройства Стрелец-ПРО, адресные устройства линии СЛ-240, а также неадресные шлейфы и выходы устройств линии S2 функционируют в составе сегмента (рисунок П1.5) в единой логике и управляются контроллером сегмента (КСГ).

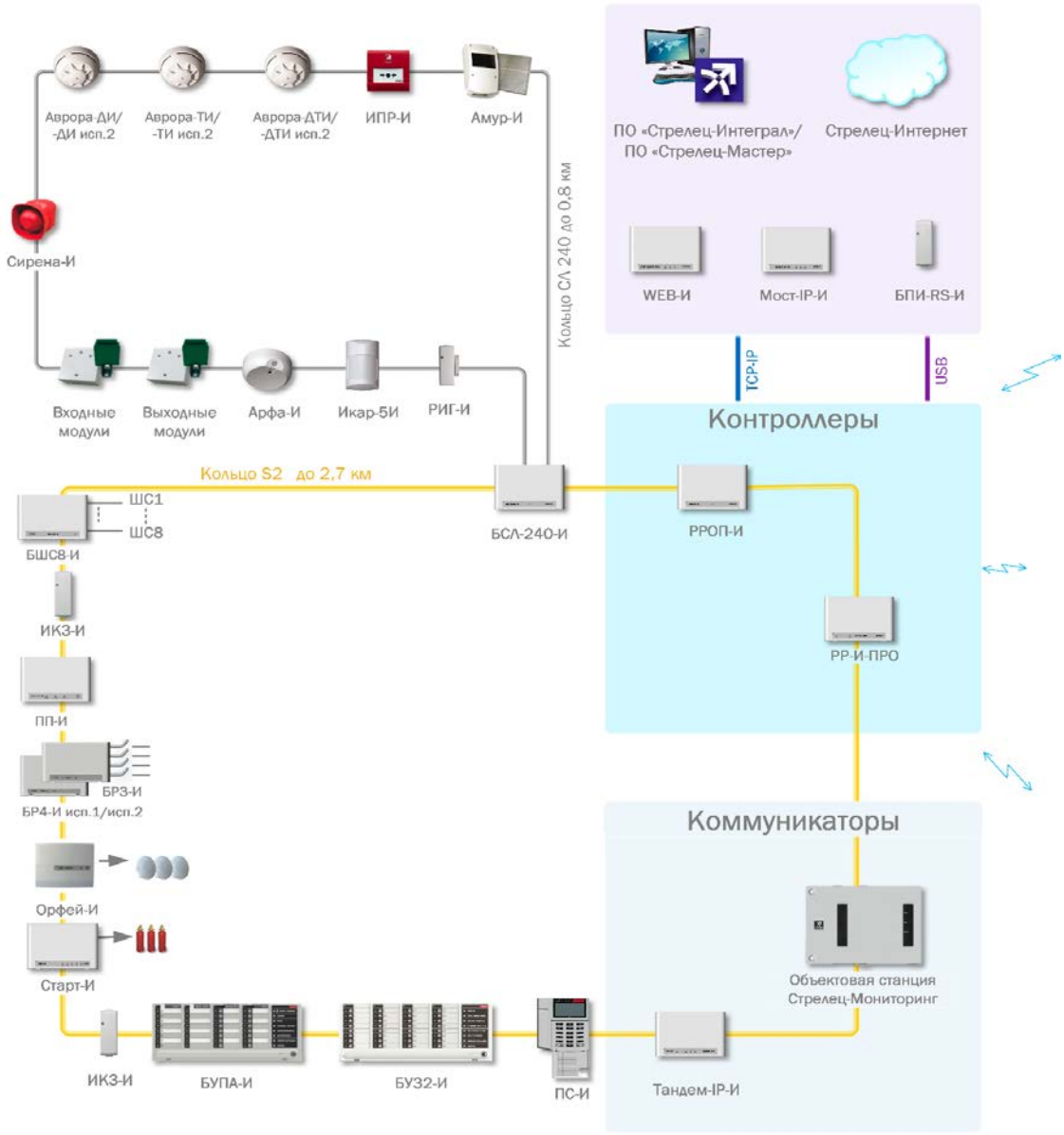

Рисунок П1.4 - Структурная схема ИСБ «Стрелец-Интеграл»

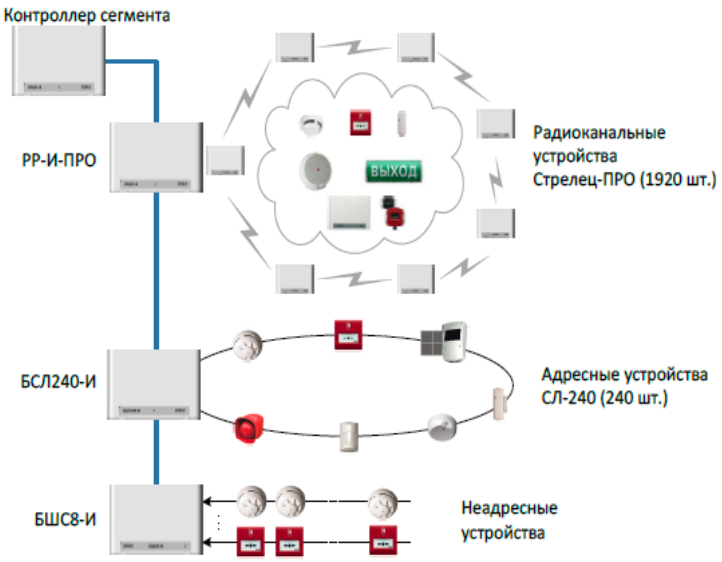

Рисунок П1.5 - Схема сегмента ИСБ «Стрелец-Интеграл»

Характеристики радиоканального интерфейса: частотные диапазоны работы – 864-865 МГц, 868-868,2 МГц, 868,7-869,2 МГц; количество рабочих каналов – 6; автоматическая смена канала при невозможности передачи по основному каналу; максимальная излучаемая мощность – не более 25 мВт; Период передачи контрольных сигналов – 2 мин. период контроля связи – 5 мин, 10 мин (программируется). Сетевая топология контроллеров – многосвязная сеть с динамической маршрутизацией. Максимальное количество контроллеров, автоматически подключающихся к родительскому контроллеру – 31 шт. Максимальное количество участков ретрансляции – 10. Сетевая топология контроля дочерних устройств Стрелец-ПРО – «Звезда». Родительский контроллер выбирается устройством автоматически в зависимости от условий радиосвязи. Максимальное количество дочерних устройств, автоматически подключающихся к контроллеру (коэффициент разветвлённости) – 256 шт. Максимальное количество устройств на одном частотном канале в зоне взаимной радиовидимости – не менее 2000 шт. Автоматическая подстройка рабочей частоты, автоматическая регулировка мощности. Динамическое кодирование информации и механизм динамической двухсторонней аутентификации для исключения возможности постороннего вмешательства в работу радиосистемы и подмены радиоустройств.

Приложение 2

Таблица П2 - Технические характеристики радиоканальных систем передачи информации

РСПИ	Стрелец-Аргон	Иртыш-3Р	Приток-А-Р	Протон	Струна-5	Струна-М	Радиосеть
1	2	3	4	5	6	7	8
Предприятие-изготовитель	ЗАО «Аргус-Спектр», г. С-Петербург	ООО НТК «ИНТЕКС», г. Омск	ОБ «СОКРАТ», г. Иркутск	ООО НПО «ЦЕНТР-ПРОТОН», г. Челябинск	ЗАО НПФ "Интеграл+" г. Казань	ООО НПП «АСБ Рекорд», г. Александров	
Сайт	www.argus-spectr.ru	www.intecs.ru	www.sokrat.ru	www.centerproton.ru	www.integralplus.ru	www.asbgroup.ru	
Количество охраняемых объектов (информационная емкость), максимальная	8152	(1000 на 7 частотах)	250 (250 радионаправлений до 30 проводных приборов на направлении)	2000 (на одной частоте), 16000 (на 8-ми частотах)	4096	20 (до 160 на 8 частотах или 1280 с учѐтом ретрансляции)	2048 (информационная ѐмкость 65536) (1500 при контроле канала 120с)
Диапазоны рабочих частот, МГц	146 - 174 403 - 470	130 - 174 430 - 480	136 - 174 430 - 470	146 - 174 403 - 470	146 - 174 401 - 470	166,7 - 167,5 458,45 - 460 468,45 - 469	450 - 453 460 - 463
Класс излучения	-	-	16K0F2D	12K0F1D	16K0F2D	16K0F1D	8K0F1D
Ширина канала, кГц	25	12,5 или 25	12,5 или 25	25	25	25	12,5
Длительность посылки, мс	От 17 до 56	От 250 до 350	150	160	75	50	30
Кол-во посылок в сеансе	1	1	1	6 - 16	1	1	1
Вид модуляции	ЧМ	ЧМ	FSK	ЧМ	FFSK	ЧМ	ЧМ

Продолжение таблицы П2

1	2	3	4	5	6	7	8
Направленность: -1 однонаправленная; - 2 вунаправленная; А - асинхронная; С - синхронная	2 А	2 С	2 С	2 А	2 С	1 (от объектов) / 2С (от РТ до пульта)	2С
Автоматическая смена рабочего канала	Да	Да	Нет	Нет	Да	Нет	Да
Период передачи тестовых сообщений	30 с - 20 мин.	1 с - 30 мин.	30 - 150 с	30 с. - 4 ч (4 ч.- по умолчанию)	132 с (период опроса при полной емкости системы)	5,8 - 8,9 с	5 - 140 с
Маршрутизация	динамическая	статическая	статическая	статическая	статическая	статическая	статическая
Контроль канала	от 2 мин. до 6 часов, при времени контроля в 120 с - 200 объектов, одна Fраб.	не более 50 сек (100 объектов), при времени контроля в 120 с, 240 объектов, одна $F_{раб.}$	30...150 с, при времени контроля в 120 с - 250 объектов, одна $F_{раб.}$	3 до 1440 мин. (24 ч. По умолчанию), при времени контроля в 120 с - 60 объектов, одна $F_{раб}$	при времени контроля в 120 с - 1024 блоков радиоканальных + 3072 блоков проводных, одна $F_{раб.}$	при времени контроля в 120 с - 20 блоков одна $F_{раб.}$	40с на 100 объектов; 120с на 1500 объектов; 150с на 2048 объектов, две $F_{раб.}$
Мощность передатчиков	(0,025 – 5) Вт	0,8/1/5 Вт	1 - 5 Вт	2/6 Вт	1,5 - 5 Вт	2 Вт	0,1 - 5 Вт (авторегулирование)
Мощность ретрансляторов	(0,025 – 5) Вт	0,8/5 Вт (ПЦН 10…25)	25 Вт (ПЦН до 50)	2/6 Вт	5 - 20 Вт	0,1 - 5 Вт (руч. установка)	0,1 - 5 Вт (руч. установка)

Окончание таблицы П2

1	2	3	4	5	6	7	8
Дальность объект - ПЦН (без ретрансляторов)	3 -15 км	до 30 км	до 30 км	до 30 км	30 км в условиях города	25 км	до 25 км
Количество ретрансляторов	каждый объектовый блок (до 15 участков ретрансляции)	теоретически каждый двухсторонний объектовый блок	до 3	до 7	Зависит от выделенного частотного ресурса, но не более 16 шт.	8	1 (до 128 РТ «СтрунымМ»)
Архитектура	параллельно, звезда, последовательно	параллельно, звезда последовательно	звезда	параллельно, последовательно, звезда	параллельно, звезда	параллельно, звезда	звезда (с центром не на ПЦО)
Поддерживаемые ППКОП	Стрелец-Интеграл, Стрелец	Иртыш-3Р	Приток-А	Стрелец, Орион, LARS, Visonic	Струна-5	Струна-3	Струна-3, Радиосеть

Приложение 3.

Акты внедрения результатов диссертационного исследования

АКТ ВНЕДРЕНИЯ
научной и (или) научно-технической продукции

1. Наименование научной продукции: Модели и алгоритмы оценки работоспособности телекоммуникационной сети централизованной охраны объектов.

2. Вид научной продукции: диссертационное исследование.

3. Исполнитель(и) НИР: Черников Р.С., преподаватель кафедры специальной техники и информационных технологий ВЮИ ФСИН России, капитан внутренней службы.

4. Сведения о внедрении научной продукции: результаты диссертационного исследования «Модели и алгоритмы оценки работоспособности телекоммуникационной сети централизованной охраны объектов» используются в образовательном процессе ВЮИ ФСИН России при изучении темы № 6 дисциплины «Информационная безопасность» по специальности 40.05.02 Правоохранительная деятельность и по направлению подготовки 40.03.01 «Юриспруденция».

5. Сведения об эффективности внедрения научной продукции в деятельность подразделений (категорий сотрудников), а также в образовательный процесс образовательных организаций ФСИН России: результаты диссертационного исследования включают в себя описание структуры телекоммуникационной сети централизованной охраны объектов, а также параметры работоспособности телекоммуникационной сети централизованной охраны объектов, алгоритмы оценки вероятности (эффективности) эксплуатации угрозой уязвимости компонента телекоммуникационной сети, опасности угроз по последствиям их реализации, методику определения степени проявления уязвимостей и силы защитных механизмов, идентифицированных в компонентах телекоммуникационной сети объекта охраны. Данные результаты используются в образовательном процессе ВЮИ ФСИН России, способствуя практико-ориентированному освоению обучающимися профессиональных компетенций, предусмотренных рабочей программой дисциплины «Информационная безопасность». Сведения об эффективности внедрения научной продукции в образовательный процесс обсуждены на заседаниях кафедры специальной техники и информационных технологий ВЮИ ФСИН России 13 октября 2022 г. (протокол № 3) и методического совета ВЮИ ФСИН России 19 октября 2022 г. (протокол № 3).

Заместитель начальника ВЮИ ФСИН России
по учебной работе
полковник внутренней службы Е.С. Ткаченко
«26» октября 2022 г.

Подпись Е.С. Ткаченко заверяю
Начальник секретариата ВЮИ ФСИН России
07.11 (ФИО, подпись) 2022

УТВЕРЖДАЮ
Начальник управления
Муниципального казённого
учреждения
«Управление гражданской защиты
г.Владимира»

_____ Б.Н. Беликов
«___» _____ 2022 года

АКТ ВНЕДРЕНИЯ

результатов диссертационной работы Черникова Романа Сергеевича
«Модели и алгоритмы оценки работоспособности
телекоммуникационной сети централизованной охраны объектов»

Результаты диссертационной работы Черникова Романа Сергеевича «Модели и алгоритмы оценки работоспособности телекоммуникационной сети централизованной охраны объектов» использованы в работах по обеспечению информационной безопасности корпоративной телекоммуникационной сети МКУ «Управление гражданской защиты г. Владимира» в части своевременного выявления уязвимости функционирования объектовых комплексов ТСО и задействования соответствующих защитных механизмов.

Заместитель начальника управления А.И. Винарчик

УТВЕРЖДАЮ
И.о. начальника управления информатизации,
телекоммуникаций и делопроизводства
администрации города Владимира

Для документов

_____ С.Д. Шутов
27 сентября 2022 года

г. Владимир

АКТ

внедрения результатов диссертационной работы Черникова Романа Сергеевича «Модели и алгоритмы оценки работоспособности телекоммуникационной сети централизованной охраны объектов»

Результаты диссертационной работы Черникова Романа Сергеевича «Модели и алгоритмы оценки работоспособности телекоммуникационной сети централизованной охраны объектов», представленной на соискание учёной степени кандидата технических наук, использованы в обеспечении информационной безопасности в единой информационно-телекоммуникационной сети органов управления муниципального образования город Владимир (телекоммуникационной сети — ТКС) для:

1. Проведения оценки защищённости информационных процессов по показателям конфиденциальности, доступности и целостности в каждом из структурных компонентов ТКС централизованной охраны объектов (ЦОО) для всех режимов функционирования.
2. Проведения оценки эффективности использования определённых защитных механизмов для повышения защищённости и работоспособности конкретных структурных компонентов системы ТКС ЦОО в конкретных режимах функционирования.
3. Поиска структурных компонентов ТКС ЦОО, обладающих минимальной защищённостью и работоспособностью в определённых режимах функционирования, что позволяет выборочно применять защитные механизмы, усиливающие защищённость конкретных структурных элементов системы.

Применение предложенных в работе методик и алгоритмов позволит своевременно выявлять уязвимости функционирования объектовых комплексов технических средств охраны и внедрять соответствующие защитные механизмы.

Консультант отдела телекоммуникаций И.А. Синицын

ЦЕНТУРИОН
Охранная группа

работаем честно

№ _____ от « ___ » _____ 2022 г.

АКТ

о практическом применении результатов диссертационной работы

Результаты диссертационной работы Черникова Романа Сергеевича «Модели и алгоритмы оценки работоспособности телекоммуникационной сети централизованной охраны объектов» были апробированы и практически использованы для снижения уровня ложных срабатываний средств охранной сигнализации защищаемых объектов на ПЦО ООО «ЧОО «Центурион-2007» в г. Владимир. По результатам применения организационных и технических мероприятий, изложенных в исследовании наблюдалось снижение уровня ложных срабатываний средств охранной сигнализации на 5-10% за 1-2 квартал 2022 года.

Исполнительный директор
ООО «ЧОО «Центурион-2007» М.А. Миронов

Тел. + 7 919 021-07-07
mironov@centurion33.ru
centurion33.ru

ФЕДЕРАЛЬНАЯ СЛУЖБА
ВОЙСК НАЦИОНАЛЬНОЙ ГВАРДИИ
РОССИЙСКОЙ ФЕДЕРАЦИИ
**Федеральное государственное
казенное учреждение «Управление
вневедомственной охраны войск национальной
гвардии Российской Федерации по
Владимирской области»**
(ФГКУ «УВО ВНГ России по Владимирской области»)
ул. Студенческая, 18, Владимир, 600005

_____ №_____

на №_____ от _____

АКТ

о практическом применении результатов диссертационного исследования Черникова Р.С., выполненного на тему «Модели и алгоритмы оценки работоспособности телекоммуникационной сети централизованной охраны объектов»

Результаты диссертационной работы по анализу уязвимостей телекоммуникационной сети централизованной охраны объектов и формированию защитных механизмов для снижения вероятности реализации угроз информационным ресурсам в телекоммуникационной сети, были использованы в практической деятельности ПЦО г. Владимира отдела вневедомственной охраны г. Владимира. Внедрение результатов исследования позволило снизить уровень ложных срабатываний объектовых комплексов ТСО в целом по ПЦО на 6% за первое полугодие 2022 года.

Заместитель начальника
полковник полиции Д.А. Нестеров

Исп.: Ю.Н. Бобылев
(4922) 77 78 34
12.06.2022

УТВЕРЖДАЮ
И.о. проректора по образовательной
деятельности Владимирского
государственного университета имени А.Г. и
Н.Г. Столетовых

_____/Панфилов А.А.
«____»_____2023г.

АКТ
о внедрении результатов диссертационного исследования
Черникова Романа Сергеевича в учебный процесс ВлГУ

Результаты диссертационного исследования Черникова Р.С., выполненного по теме «Модели и алгоритмы оценки работоспособности телекоммуникационной сети централизованной охраны объектов», внедрены в учебный процесс кафедры информатики и защиты информации и кафедры радиотехники и радиосистем.

Разработанные в диссертации теоретические положения и практические разработки использованы в учебном процессе при подготовке бакалавров и магистров по направлению «Информационная безопасность» и специалистов по специальности «Информационно-аналитические системы безопасности» в рамках проведения учебных занятий по дисциплинам «Защита информации от утечки по техническим каналам», «Моделирование информационно-аналитических систем», «Принципы построения, проектирования и эксплуатации информационно-аналитических систем» и «Телекоммуникации». Результаты работы использованы при проведении лекционных, лабораторных и практических занятий, а также в научно-исследовательской работе и дипломном проектировании студентов.

Заведующий кафедрой ИЗИ _____ Монахов М.Ю.

Заведующий кафедрой РТиРС _____ Корнеева Н.Н.

«16» января 2023г.