Министерство науки и высшего образования Российской Федерации
Федеральное государственное образовательное учреждение
высшего образования
«Тульский государственный университет»

На правах рукописи

ЧЕРНОВ ДЕНИС ВЛАДИМИРОВИЧ

МЕТОДЫ И АЛГОРИТМЫ МОДЕЛИРОВАНИЯ УГРОЗ БЕЗОПАСНОСТИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ С ПРИМЕНЕНИЕМ АППАРАТА ЭКСПЕРТНЫХ ОЦЕНОК

Специальность 2.3.6 Методы и системы защиты информации,
информационная безопасность

Диссертация на соискание ученой степени
кандидата технических наук

Научный руководитель:
доктор технических наук, доцент
Сычугов Алексей Алексеевич

Тула – 2025

ОГЛАВЛЕНИЕ

Введение

Актуальность темы исследования. В современных условиях технологического развития общества обеспечение информационной безопасности (ИБ) составляет одну из важнейших задач на всех этапах жизненного цикла промышленных систем автоматизации. Критическая информационная инфраструктура (КИИ) стала неотъемлемой частью стратегически важных для государства объектов нефтехимической, энергетической, оборонной, ракетно-космической и других отраслей промышленности, что делает объекты КИИ выгодной мишенью для потенциальных злоумышленников, ставящих своей целью нанести максимально возможный урон технологическим компаниям, отраслям экономики и репутации государства.

В соответствии с положениями Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [1] к объектам КИИ (ОКИИ) относятся информационные системы (ИС), информационно-телекоммуникационные сети (ИТКС) и автоматизированные системы управления технологическими процессами (АСУ ТП), функционирующие в одной из тринадцати ключевых сфер деятельности (нефтехимической, энергетической, оборонной, ракетно-космической и т.д.). Законом установлена обязанность выполнения владельцами ОКИИ комплекса мероприятий по оценке их значимости и реализации организационных и технических мер, направленных на обеспечение ИБ ОКИИ.

Одной из важных мер обеспечения ИБ ОКИИ является моделирование угроз безопасности информации (угроз БИ), т.е. выявление совокупности условий и факторов, которые приводят или могут привести к нарушению безопасности обрабатываемой в этих системах информации, а также к нарушению или прекращению функционирования систем и сетей.

Для моделирования угроз БИ ОКИИ в отношении которых установлена одна из трех категорий значимости в настоящее время используются хорошо зарекомендовавшие себя риск-ориентированные подходы и методики, например, изложенные в серии стандартов ГОСТ Р ИСО/МЭК 27ххх и «Методике оценки угроз безопасности информации», утвержденной ФСТЭК России от 05.02.2021г (далее – Методика ФСТЭК России от 05.02.2021г.). Указанные стандарты позволяют анализировать угрозы с учетом оценок ущерба от реализации актуальных угроз БИ. Применение существующих подходов и методик определения актуальных угроз БИ, выявления способов их реализации и оценки рисков ИБ требует привлечения высококвалифицированных специалистов в области ИБ, а также значительных временных и иных ресурсов. В современных условиях с учетом роста масштабов и сложности ОКИИ, в отношении которых не установлена одна из трех категорий значимости (незначимые ОКИИ), при применении вышеуказанных стандартов и методик, значительно увеличивается объем разнообразной информации, подлежащей анализу. Это ставит задачу дополнительной разработки методов и алгоритмов автоматизации моделирования угроз незначимых ОКИИ, основанных на развитии риск-ориентированного подхода в направлении обработки больших объемов располагаемой разнородной информации, связанной с оценкой ключевых факторов, влияющих на величину риска и ущерба от реализации угроз, с использованием знаний и опыта как экспертов - специалистов в области ИБ, так и дополнительно привлекаемых на этой стадии экспертов - профессионалов в области ИС, ИТКС, а также АСУ ТП, отличающихся своей многоуровневой структурой.

Решение указанной задачи позволит повысить объективность и достоверность оценок актуальности угроз и рисков БИ с использованием профессиональных знаний специалистов в области ОКИИ и разработанных методов и алгоритмов обработки этой информации, что в свою очередь позволит оценить влияние основных риск-образующих факторов на последствия (ущерб) от реализации актуальных угроз БИ. Программная реализация разработанных

методов и алгоритмов позволит создать инструментальные средства автоматизации процесса моделирования угроз БИ, способные дополнять существующие риск-ориентированные подходы и методики в рамках определения нарушителей, представляющих наибольшую опасность для незначимых ОКИИ, актуальных угроз БИ, а также возможных контрмер противодействия им с целью минимизации ущерба от реализации угроз БИ, что, в свою очередь, позволит повысить эффективность процесса моделирования угроз БИ и выбора комплекса защитных мер в соответствии с предъявляемыми нормативными требованиями.

Указанные обстоятельства определяют **актуальность** темы диссертационной работы.

Степень разработанности темы исследования. Результаты исследований, связанных с оценкой потенциальных нарушителей и актуальных угроз БИ, отражены в работах Бусько М.М., Васильева В.И., Власенко А. В., Вульфина А.М., Гузаирова М. Б., Жука Р.В., Котенко И.В., Кучкаровой Н.В., Машкиной И.В., Сарвепалли В., Суханова А.В., Сухостата В.В., Шелупанова А.А. и др. Вопросами контроля и обеспечения безопасности ОКИИ занимались многие ученые, что отражено в работах Ажмухамедова И.М., Андреева Ю.С., Бражука А.И., Братченко А.И., Дербишера А.В., Дойниковой Е.В., Кравченко Е.Г., Ксяо Л., Плетнева П.В., Селифанова В.В. и др.

Анализ результатов проведенных исследований показал, что при всей их значимости проблема моделирования угроз БИ ОКИИ нуждается в дальнейшей проработке. Существующие методы и алгоритмы определения потенциальных нарушителей режима ИБ и актуальных угроз БИ нуждаются в дальнейшем развитии и совершенствовании с привлечением дополнительной информации о характере и специфике КИИ, что может быть реализовано на основе применения аппарата экспертных оценок, чему и посвящена настоящая работа.

Объектом исследования диссертационной работы являются ОКИИ, в отношении которых могут быть реализованы угрозы БИ потенциальными нарушителями ИБ.

Предметом исследования диссертационной работы являются методы и алгоритмы моделирования угроз БИ в ОКИИ.

Цель диссертационной работы состоит в повышении эффективности процесса моделирования угроз БИ ОКИИ на основе разработки методов и алгоритмов интеллектуального анализа данных, позволяющих повысить достоверность и объективность результатов анализа и оценки актуальных угроз БИ с использованием аппарата экспертных оценок.

Для достижения поставленной цели в диссертационной работе необходимо решить следующие **задачи исследования:**

1. Анализ современного состояния исследований в области автоматизации процесса моделирования и определения актуальных угроз БИ ОКИИ.
2. Разработка метода определения потенциала нарушителя ИБ ОКИИ на основе вычисления матриц идентификаторов угроз БИ и метода количественной оценки степени опасности реализации угроз БИ потенциальными нарушителями ИБ ОКИИ.
3. Разработка алгоритма определения уязвимых звеньев ОКИИ и оценки уровня их защищенности.
4. Разработка алгоритма экспертной оценки степени опасности реализации угроз БИ для ОКИИ.
5. Разработка структуры и программного обеспечения автоматизированной системы моделирования угроз БИ ОКИИ, оценка эффективности ее применения в процессе обеспечения ИБ АСУ ТП.

Положения, выносимые на защиту:

1. Метод определения потенциала нарушителя ИБ ОКИИ на основе построения матриц идентификаторов угроз.
2. Метод количественной оценки степени опасности реализации угроз БИ ОКИИ потенциальными нарушителями ИБ с использованием оценок вероятностей реализации угроз БИ и ущерба от их реализации.

3. Алгоритм определения уязвимых звеньев ОКИИ и оценки их защищенности на основе предложенных матриц защищенности.

4. Алгоритм экспертной оценки степени опасности реализации угроз БИ ОКИИ.

5. Структура и программное обеспечение автоматизированной системы моделирования угроз БИ ОКИИ.

Методы исследования. Для решения поставленных в работе задач были использованы методы интеллектуального анализа данных и защиты информации, методы теории игр, экспертных оценок и системного проектирования SADT.

Научная новизна

1. Предложен метод определения потенциала нарушителя ИБ ОКИИ, основанный на применении матриц идентификаторов угроз. Метод позволяет выявить и количественно оценить располагаемый потенциал возможных нарушителей ИБ, что, в свою очередь, позволяет повысить достоверность и объективность анализа и оценки актуальных угроз БИ. Главным отличием от существующих методов является применение предложенного подхода к групповой оценке потенциалов нарушителей согласованным количеством экспертов.

2. Предложен метод количественной оценки степени опасности реализации угроз БИ ОКИИ, основанный на интеллектуальном анализе данных, имеющихся в подсистеме журналирования. Метод позволяет количественно оценить степень опасности реализации угроз БИ потенциальными нарушителями ИБ применительно к конкретному объекту КИИ. Разработанный метод дополняет располагаемые оценки специалистов в области ИБ путем формирования экспертных оценок со стороны дополнительно привлекаемых специалистов - профессионалов в области КИИ.

3. Разработан алгоритм определения и оценки защищенности уязвимых звеньев ОКИИ. Алгоритм отличается от известных тем, что использует матрицу защищенности, составленную на основе оценок показателей защищенности

уязвимых звеньев, что позволяет повысить объективность выявления актуальных угроз.

4. Предложен алгоритм экспертной оценки степени опасности реализации угроз БИ ОКИИ, который в отличие от существующих основан на применении игр с несовершенной информацией вида «злоумышленник - система защиты информации», где в качестве возможных выигрышей сторон используются оценки потенциала нарушителя, опасности реализации им угроз БИ, а также оценки защищенности уязвимых звеньев, по отношению к которым потенциальный нарушитель реализует угрозы БИ. Предложенный алгоритм позволяет дополнять перечни актуальных угроз БИ, выявленных с использованием известных методик ФСТЭК России.

Достоверность и обоснованность научных положений и выводов, полученных в диссертационной работе, подтверждается разносторонним изучением современного состояния предметной области, системным обоснованием предложенных методов и алгоритмов, не противоречащих известным положениям других авторов, апробацией полученных результатов в научных публикациях и докладах на международных и российских научно-практических конференциях, а также при решении практических задач моделирования угроз БИ.

Научная значимость диссертационной работы состоит в развитии теоретических знаний и разработке новых методов и алгоритмов моделирования угроз БИ с применением подходов и инструментария теории защиты информации, теории игр, экспертных оценок и системного анализа для построения моделей угроз БИ ОКИИ.

Практическая значимость диссертационной работы состоит в разработке алгоритмов и программного обеспечения автоматизированной системы моделирования угроз БИ ОКИИ, позволяющей повысить эффективность построения моделей угроз БИ и выбора состава мер защиты по сравнению с известными методиками. Применение разработанной системы позволяет

поддерживать актуальность сведений о возможных угрозах БИ, потенциальных нарушителях ИБ и необходимых средствах защиты информации (СЗИ).

Реализация результатов работы. Предложенные в работе методы и алгоритмы были использованы для моделирования угроз БИ ОКИИ в ООО «Комплексы системы и сети», ООО «БД Безопасность» и внедрены в учебный процесс кафедры информационной безопасности ФГБОУ ВО «Тульский государственный университет» Министерства науки и высшего образования РФ. Разработанное ПО внедрено в процессы оценки угроз в АО ЦКБА. Работа поддержана грантом РФФИ № 19-07-01107\19 «Разработка математических моделей и методов построения интеллектуальных распределенных адаптивных систем обеспечения ИБ» и грантом РТУ МИРЭА № 15/2020 «Разработка методов и алгоритмов моделирования угроз БИ».

Апробация результатов работы. Основные и промежуточные результаты исследования докладывались и обсуждались на следующих Международных научно-технических конференциях: «Вопросы кибербезопасности, моделирования и обработки информации в современных социотехнических системах» (Курск, 2018); Международная научно-техническая конференция «Автоматизация» RusAutoCon (Сочи, 2019, 2020, 2021, 2022); 12-я Международная конференция по безопасности информации и сетей, SINConf 2019 (Сочи, 2019); Международная научно-практическая конференция «Электротехнические комплексы и системы» ICOECS 2019 (Уфа, 2019); Международная научно-техническая конференция «Пром-Инжиниринг» ICIEAM (Сочи, 2023, 2024); XIV Национальная научно-техническая конференция (Москва, 2024).

Личный вклад автора. Все научные результаты диссертационного исследования и проведенной апробации получены автором самостоятельно. Постановка цели и задач, обсуждение планов исследований и полученных результатов выполнены автором совместно с научным руководителем. Программная реализация предложенных в работе методов и алгоритмов в составе

автоматизированной системы моделирования угроз БИ также выполнена автором самостоятельно.

Соответствие паспорту специальности. Результаты диссертационной работы соответствуют следующим пунктам паспорта научной специальности 2.3.6 «Методы и системы защиты информации, информационная безопасность»:

п.3 «Методы, модели и средства выявления, идентификации, классификации и анализа угроз нарушения информационной безопасности объектов различного вида и класса»;

п.8 «Анализ рисков нарушения информационной безопасности и уязвимости процессов обработки, хранения и передачи информации в информационных системах любого вида и области применения»;

п.10 «Модели и методы оценки защищенности информации и информационной безопасности объекта»;

Публикация по теме диссертации. По материалам диссертации опубликовано 30 научных работ, в том числе 4 в изданиях, рекомендованных в Перечне ВАК РФ, и 10 научных работ в изданиях, входящих в международные базы данных цитирования SCOPUS и Web of Science. Получено 1 свидетельство о государственной регистрации программы для ЭВМ.

Структура и объем работы. Диссертационная работа содержит введение, 4 главы, заключение и список источников, включающий 121 наименование. Объем работы 148 страниц, в том числе 32 таблицы, 36 рисунков и 7 приложений.

Содержание работы. В первой главе проведен анализ современного состояния исследований в области автоматизации процесса моделирования и определения актуальных угроз БИ ОКИИ, рассматриваются современные подходы к моделированию угроз БИ, включающие в себя методы оценки нарушителей и угроз, а также методы выбора защитных мер. Рассматриваются задачи оценки вероятных нарушителей и процесса моделирования угроз БИ. Выделяются основные метрики квалификации и мотивации потенциальных нарушителей БИ ОКИИ.

Вторая глава посвящена разработке методов, позволяющих проводить мероприятия по моделированию угроз БИ ОКИИ. Предложен метод определения потенциала нарушителя ИБ ОКИИ на основе построения матриц идентификаторов угроз. В качестве идентификаторов угроз в предложенном методе выступают способы реализации УБИ, представленные в Методике ФСТЭК России от 05.02.2021г. Предложены методы количественной оценки степени опасности реализации угроз БИ ОКИИ потенциальными нарушителями ИБ, оценки защищенности уязвимых звеньев ОКИИ и экспертной оценки степени опасности реализации угроз БИ ОКИИ с применением модели игры Штакельберга.

В третьей главе проводится алгоритмизация процедуры формирования модели угроз БИ ОКИИ, на основе оценок потенциалов возможных нарушителей, показателей опасности реализации ими угроз БИ и оценок защищенности фактических уязвимых звеньев. Предложены алгоритмы работы сканера безопасности, оценки опасности реализации угроз БИ, а также определения и оценки защищенности уязвимых звеньев ОКИИ. На основе указанных алгоритмов предложен алгоритм оценки опасности реализации угроз БИ ОКИИ.

В четвертой главе описывается структура разработанной автоматизированной системы моделирования угроз информационной безопасности ОКИИ (АС «МУИБ») которая позволяет экспериментально проверить эффективность разработанных методов и алгоритмов. Приводится общее описание АС «МУИБ», рассматривается графический интерфейс автоматизированной системы и основные функциональные возможности. Приводятся результаты экспериментальной проверки предложенных методов и алгоритмов с использованием разработанной АС «МУИБ».

В заключении формулируются научные и практические результаты диссертационной работы.

Прилагается список использованных литературных источников.

ГЛАВА 1. АНАЛИЗ СОВРЕМЕННОГО СОСТОЯНИЯ ЗАДАЧИ МОДЕЛИРОВАНИЯ УГРОЗ БИ ОКИИ

1.1 Нормативно-правовая и терминологическая база обеспечения БИ ОКИИ.

Вопрос обеспечения БИ ОКИИ с каждым годом стоит всё актуальнее. Аналитические отчеты по итогам 2024 года ведущих мировых производителей СЗИ и поставщиков услуг БИ свидетельствуют о возросшей доле атак на промышленные объекты с 4% от общего числа атак за период 2018 года до 9% в 2023 году, 11% в 2024 году [2-3]. Предполагаемый уровень атак на объекты, в которых функционируют ОКИИ, по итогам 2025 года составит 12-15% [4]. Согласно исследованию [5] 94% организаций столкнулись с инцидентами в сфере защиты операционных технологий (ОТ) за последний год. Анализ показал, что нарушения в сегменте информационных технологий (ИТ) способствуют выявлению уязвимостей на стыке ИТ и ОТ-инфраструктур. Среди ключевых факторов киберугроз выделяются фишинговые атаки, нацеленные на компрометацию учётных данных, а также ошибки персонала, включая некорректную настройку межсетевых экранов. Это подчеркивает уязвимость ключевых элементов национальной кибербезопасности перед сложными целевыми атаками, что требует пересмотра моделей угроз отечественными субъектами КИИ. Наиболее крупные атаки на ОКИИ в 2020-2024 г. характеризуются деструктивным информационным воздействием вирусов шифровальщиков WannaCry, Nefilim, Maze, Netwalker, RansomEXX, Conti и DoppelPaymer. Атака на американскую компанию Boeing привела к остановке конвейера по сборке узлов транспортного самолета Boeing 777. Операторы шифровальщиков все реже проводят массовые атаки, они целенаправленно

выбирают крупные компании, которые в состоянии заплатить большой выкуп, или организации, для которых приостановка деятельности опасна, и эксплуатируют наиболее распространенные уязвимости.

Доля атак с использованием шифровальщиков в 2020-2024 годах составляла 45% от общего числа атак [6-7].

Общая динамика выявленных киберинцидентов ИБ на промышленных объектах, эксплуатирующих ОКИИ с 2018 по 2024 годы, представлена на рис. 1.1.

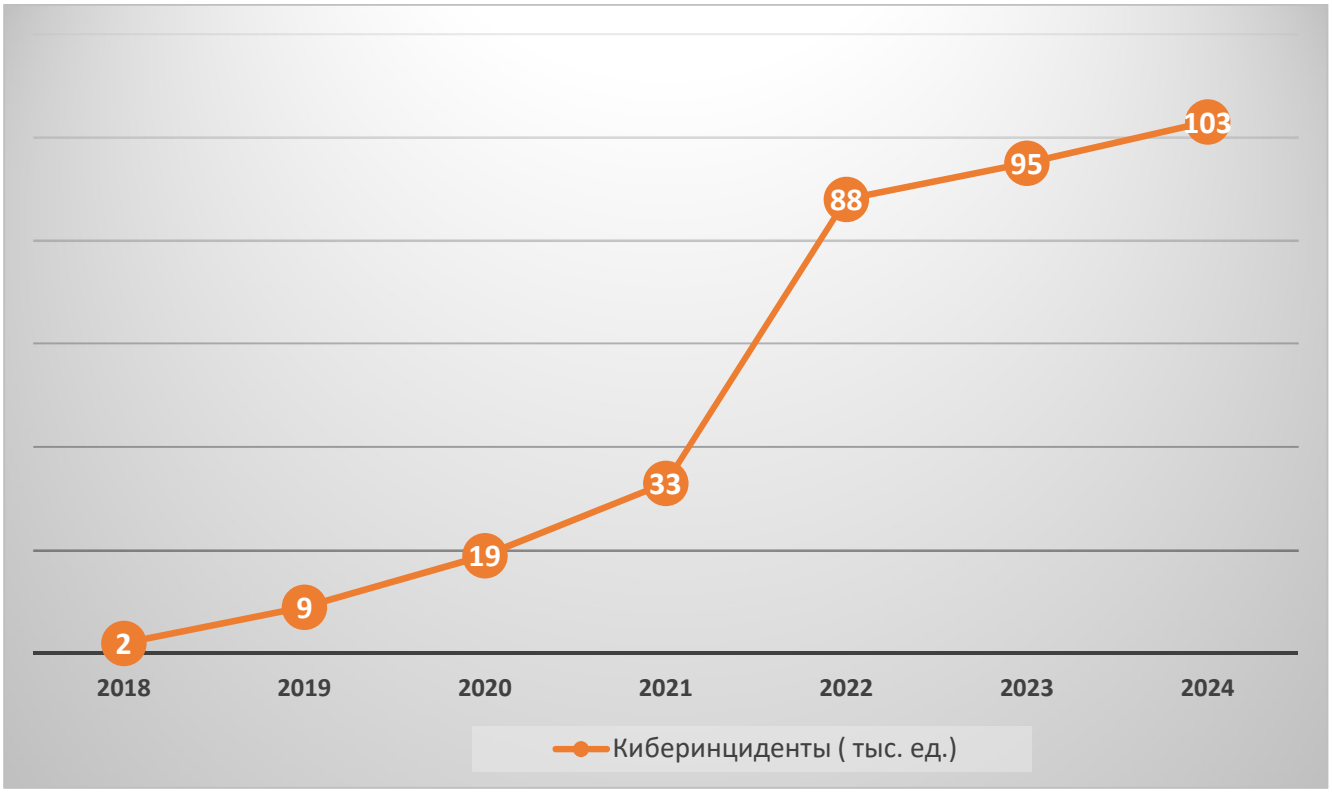


Рис. 1.1 Общая динамика выявленных инцидентов БИ ОКИИ [8]

Анализ тенденций [9] реализации кибератак с 2020 года показывает, что подходы к нарушению режима БИ ОКИИ существенно изменились. Если в 2020 году основными методами проникновения были использование внешних устройств (24% от общего количества киберинцидентов), фишинг (22%) и компрометация устройств удалённого доступа (14%), то к 2024 году структура угроз изменилась. Компрометация учетных данных (20%), атаки на цепочки поставок (15%), использование устройств с доступом в интернет (13%). Чаще всего нарушители получают доступ через АРМ (30% атак), SCADA-серверы

(25%) и программируемые логические контроллеры (ПЛК) (21%). В 70% случаев атаки сопровождаются заражением троянским ПО, предназначенным для вымогания денежных средств у субъекта КИИ. Рост количества киберинцидентов к началу 2025 года это локальная (в пределах Российской Федерации) и глобальная динамика для всей мировой ИТ-инфраструктуры. В течение последних двух лет число атак на отечественные ОКИИ выросло на 160%, в то время как в мире аналогичный показатель увеличился лишь на 17%. Наибольшее количество атак фиксируется в следующих отраслях: машиностроение (38% атак в России и 32% в мире); транспорт (24% в России и 28% в мире); производственные предприятия и добыча (19% и 22%); энергетика (19% и 18% соответственно).

Уязвимость - это любая характеристика или свойство ОКИИ, использование которой нарушителем может привести к реализации угрозы БИ. Реализуя угрозу, нарушитель использует какую-либо уязвимость ОКИИ [10].

Под угрозой БИ ОКИИ понимается совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения БИ.

В процессе функционирования ОКИИ возникает множество угроз, которые могут изменяться в режиме реального времени. Одной из важных задач обеспечения БИ ОКИИ является моделирование угроз, направленных на нарушение режима БИ.

На основании анализа [11] можно сделать вывод, что моделирование угроз - это итеративный процесс, который состоит из определения:

- активов (уязвимых звеньев) ОКИИ;
- уровня важности уязвимых звеньев для достижения целей эксплуатации ОКИИ;
- сценариев угроз для ОКИИ;
- актуальных угроз БИ;
- приоритетов по реализации мер защиты.

Моделирование угроз помогает обеспечить соответствие защиты меняющимся угрозам БИ. Результатом процесса моделирования угроз является физический документ - модель угроз БИ.

Модель угроз безопасности информации – физическое, математическое, описательное представление свойств или характеристик угроз БИ [12].

Модель угроз БИ ОКИИ должна содержать:

– краткое описание архитектуры ОКИИ;

– характеристику источников угроз БИ, в том числе модель нарушителя;

– описание всех угроз БИ, актуальных для ОКИИ.

Описание каждой угрозы БИ должно включать указания на [13]:

– источник угрозы БИ;

– уязвимости (ошибки), которые могут быть использованы для реализации (способствовать возникновению) угрозы БИ;

– возможные способы (сценарии) реализации угрозы БИ;

– возможные последствия от реализации угрозы БИ [14].

При разработке модели угроз принимаются во внимание особенности территориального расположения удаленных объектов ОКИИ при распределенном характере их функционирования, их социальный и экономический статус, режимы функционирования, используемое оборудование, персонал и другие факторы, определяющие возможность возникновения угроз БИ и их последствий.

Процесс образования актуальных угроз БИ обусловлен преднамеренными или непреднамеренными действиями физических лиц или организаций, создающими условия (предпосылки) для нарушения БИ, которые могут повлечь нарушение штатного режима функционирования или выход из строя ОКИИ, что, в свою очередь, может привести к возникновению чрезвычайной ситуации или иных негативных последствий. Включение вышеуказанных угроз в модель позволяет достичь соответствия принципу адекватности моделей.

Адекватность модели – совпадение свойств модели относительно цели моделирования и соответствующих исследуемых свойств моделируемого объекта [15].

Нормативно-методическая документация, регулирующая вопросы обеспечения БИ ОКИИ, содержит правила и рекомендации по созданию, развитию и поддержанию системы БИ ОКИИ. Федеральный закон №187-ФЗ регулирует отношения в области обеспечения безопасности КИИ РФ в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак. В соответствии с положениями данного документа принципами обеспечения безопасности КИИ являются:

– законность;

– непрерывность и комплексность обеспечения безопасности ОКИИ, достигаемые в том числе за счет взаимодействия уполномоченных федеральных органов исполнительной власти и субъектов КИИ;

– приоритет предотвращения компьютерных атак.

Постановление Правительства РФ №127 определяет порядок и сроки категорирования ОКИИ. На основании подзаконного акта устанавливаются три категории ОКИИ, которые распределяются по степени важности: первая (наивысшая), вторая и третья (низшая). Также существует вероятность, что некоторым ОКИИ категория значимости присвоена не будет. Категория значимости устанавливается в отношении ОКИИ в соответствии с пятью показателями критериев значимости. Критерии значимости определяются по пяти направлениям: социальная, политическая, экономическая и экологическая сфера, а также сферы обороны, государственной безопасности и правопорядка.

Приказ ФСТЭК России №239 устанавливает требования по обеспечению безопасности ОКИИ, в отношении которых установлена одна из категорий значимости. В соответствии с положениями данного приказа организационно-распорядительная документация на ОКИИ в обязательном порядке должна

содержать модель угроз БИ. Необходимость моделирования угроз БИ для значимых объектов КИИ определена п. 25 приказа ФСТЭК России №235.

В приказе ФСТЭК России №31 АСУ ТП представлена трехуровневой топологией:

– уровень операторского (диспетчерского) управления (верхний уровень), содержащий технологическую сеть передачи данных - ТСПД;

– уровень автоматического управления (средний уровень);

– уровень ввода (вывода) данных исполнительных устройств (нижний (полевой) уровень).

Состав многоуровневой структуры АСУ ТП представлен на рис. 1.2.

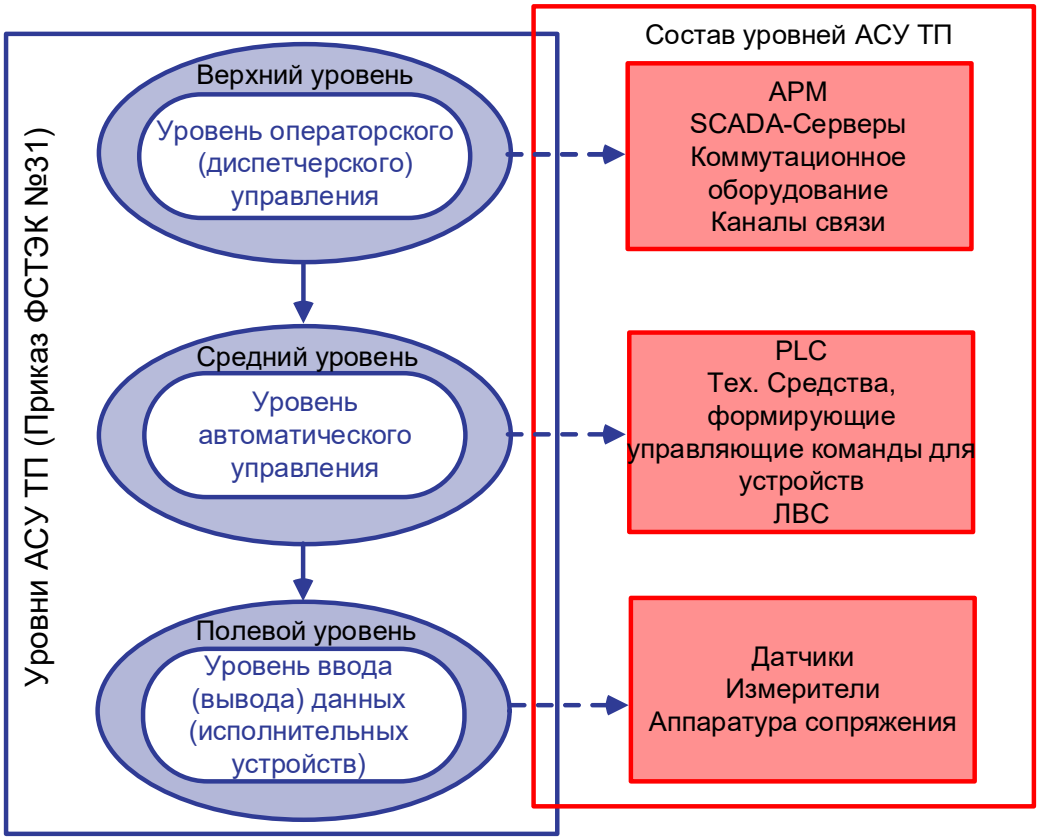


Рис. 1.2 Состав многоуровневой структуры АСУ ТП

ИС и ИТКС в отличии от АСУ ТП являются одноуровневыми системами. Актуальные руководящие документы задают общие рамки для защиты информации ОКИИ, но носят универсальный характер и не отражают всей специфики данных объектов. Это, в свою очередь, создаёт препятствия для разработки точных и релевантных моделей угроз в контексте сложных

многоуровневых АСУ ТП. Так, в документе ФСТЭК России от 02.05.2024г. «Методика оценки показателя технической защиты информации и обеспечения безопасности значимых объектов КИИ» используется опрос экспертов по заранее заготовленным вопросам, на которые даются ответы да-нет (производится качественная оценка уровня защищенности, в результате которой определяется значение показателя текущего состояния защищенности объектов КИИ (0<Кзи<=1), и соответственно выделены 3 уровня защиты от актуальных угроз БИ – состояния защищенности ОКИИ (минимальный, базовый, низкий и критический).

Основной сложностью в вопросе защиты ОКИИ (в т.ч. АСУ ТП) от деструктивных информационных воздействий является наличие большого количества векторов атаки, которые отличаются по своей реализации в зависимости от выбранного для атаки уровня ОКИИ и могут быть реализованы нарушителем [16].

Нарушитель – это лицо, предпринявшее попытку выполнения запрещенных операций (действий) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового и использующее для этого различные возможности, методы и средства [11].

Целями злонамеренных действий нарушителя, способных привести к совершению несанкционированного доступа к защищаемым ресурсам ОКИИ и нарушению принятых для системы характеристик БИ, являются:

- нарушение целостности защищаемых ресурсов;
- нарушение конфиденциальности защищаемых ресурсов;
- нарушение доступности защищаемых ресурсов;
- создание условий для последующего проведения атак.

Для описания всех возможных типов нарушителей при составлении моделей угроз используется процесс формирования модели нарушителя БИ. Модель нарушителя БИ неразрывно связана с моделью угроз БИ, т.к. нарушитель часто является как источником угроз, так и следствием [17].

В соответствии с [18] модель нарушителя – это набор предположений об одном или нескольких возможных нарушителях, их квалификации, их технических и материальных ценностях и т.д.

По результатам проведенного анализа сделан вывод о том, что задача формирования модели нарушителя БИ состоит в описательном представлении опыта, знаний, доступных ресурсов потенциальных нарушителей, необходимых им для реализации угрозы БИ, и возможной мотивации их действий.

1.2 Классификация потенциальных нарушителей БИ в задаче оценки нарушителя ОКИИ

Первичным источником угроз, реализуемых за счет несанкционированного доступа к защищаемой информации, обрабатываемой в ОКИИ, с использованием штатных средства и (или) программных и технических средств, является физическое лицо – нарушитель БИ.

Цель обеспечения БИ на этапе проектирования ОКИИ заключается в минимизации числа актуальных угроз БИ в совокупности с определением актуальных исполнителей при реализации данных угроз.

При проектировании СЗИ, критичных к отказам ОКИИ, обязательным мероприятием является формирование перечня потенциальных нарушителей БИ на этапе формирования предположений об опасности реализации тех или иных угроз БИ – формирование так называемой модели нарушителя.

Основной задачей оценки возможностей нарушителей по реализации угроз БИ является формирование предположений о типах, видах нарушителей, которые могут реализовать угрозы в ОКИИ с заданными структурно-функциональными характеристиками и особенностями функционирования, а также потенциале этих нарушителей и возможных способах реализации угроз БИ.

Анализ предметной области выявил необходимость реализации следующих основных функций построения модели нарушителя БИ ОКИИ:

– формирование представления нарушителя ОКИИ с учетом его потенциала;

– определение вербальной характеристики потенциала каждого из потенциальных нарушителей БИ;

– определение оценки опасности реализации угроз БИ ОКИИ;

– формирование перечня потенциальных нарушителей БИ для ОКИИ.

Нарушители по признаку наличия права постоянного или разового доступа в помещения, в которых размещены компоненты ОКИИ, делятся на [19]:

внешние нарушители — это физические лица, не имеющие права доступа внутрь контролируемой зоны (КЗ), в которой физически расположены ОКИИ;

внутренние нарушители — это физические лица, имеющие право доступа внутрь КЗ, включая пользователей, реализующих угрозы непосредственно на различных уровнях ОКИИ.

Внешний нарушитель не имеет непосредственного доступа к ОКИИ и ресурсам, находящимся в пределах КЗ. Подобный нарушитель имеет возможность выполнять атаки только с территории, расположенной вне КЗ, или по внешним каналам связи, используя сети связи международного обмена Интернет.

Внутренние нарушители - нарушители, осуществляющие атаки внутри КЗ.

Выделяют два основных вида внутренних нарушителей [20]:

внутренний нарушитель первого вида имеет санкционированный доступ на территорию, в здания и помещения, но не является зарегистрированным пользователем ОКИИ;

внутренний нарушитель второго вида — нарушитель, являющийся зарегистрированным пользователем ОКИИ. Данный вид нарушителя может реализовать атаки на подлежащие защите ресурсы ОКИИ, используя возможности непосредственного доступа к техническим и программным средствам, включая СЗИ.

Основные характеристики типов нарушителей БИ ОКИИ в графической форме представлены на рис. 1.3.

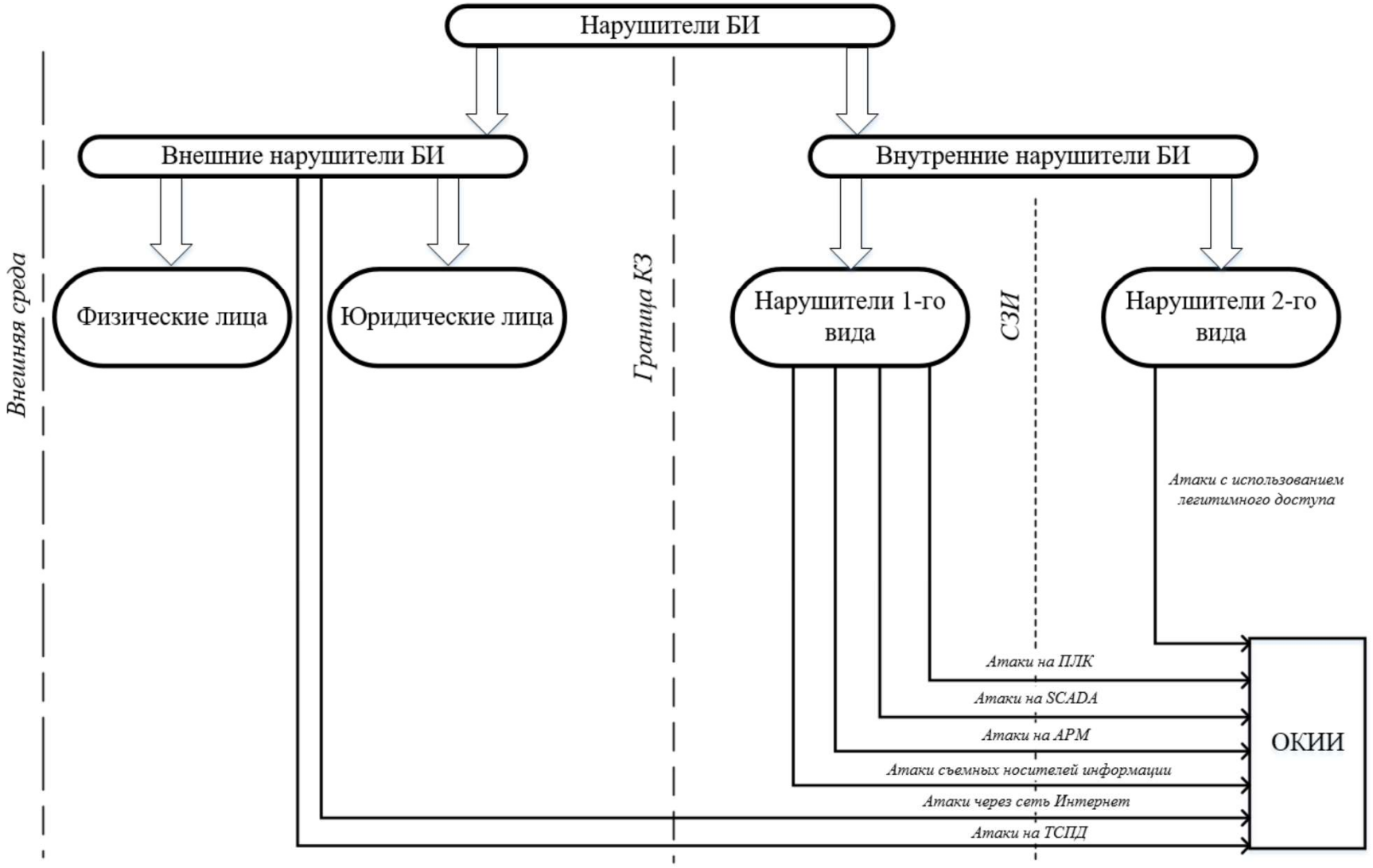


Рис. 1.3 Характеристики нарушителей БИ ОКИИ

1.3 Формирование предположений о квалификации и мотивации нарушителей БИ ОКИИ

В процессе моделирования угроз БИ учитываются возможности, предположения о квалификации и мотивации нарушителей, а также принятые субъектом КИИ организационно-технические и режимные меры. Для достижения указанных целей проводится экспертное обоснование актуальности отдельных категорий потенциальных нарушителей, которые в дальнейшем рассматриваются как возможные источники угроз БИ. В рамках данных мероприятий необходимо формировать предположения о нарушителях БИ, реализующих актуальные угрозы в отношении информации обрабатываемой ОКИИ. Выделим предположения, описывающие способы реализации угроз БИ потенциальными нарушителями:

хакеры или группировки хакеров могут работать как самостоятельно, так и в сговоре с другими типами нарушителя. В случае, когда хакеры работают самостоятельно, их финансовые возможности ограничены; в случаях же, когда хакеры выполняют деструктивные действия, вступив в сговор с другими типами нарушителя, их экономические и технические ресурсы возрастают. Как правило, хакеры обладают достаточным временем для сбора сведений о специфике технологических и информационных процессов, знают основные типы (и, как следствие, уязвимости, недекларированные возможности, жизненный цикл) ТСПД, а также аппаратного и программного обеспечения, применяемого в рамках таких процессов.

Представители разведывательных служб иностранных государств обладают высокой мотивацией, неограниченными финансовыми, техническими ресурсами, персоналом, могут привлекать любые иные типы нарушителя для достижения своих целей.

Террористические организации обладают высокой мотивацией, могут обладать техническими и экономическими ресурсами, достаточными для реализации большинства угроз БИ, в том числе с привлечением высококвалифицированных специалистов.

Криминальные структуры заинтересованы в получении прибыли. При этом финансовые и технические возможности такого типа нарушителя весьма ограничены; вероятность привлечения к реализации атак высококвалифицированных специалистов невысока.

Конкурирующие организации могут пытаться осуществлять попытки реализации угроз БИ в целях подрыва имиджа, причинения непоправимого ущерба субъекту КИИ вплоть до его разорения и банкротства.

Представители контрагентов субъектов КИИ, могут быть заинтересованы в установлении наиболее взаимовыгодного сотрудничества с субъектом, а также в получении выгоды путем обмана или злоупотребления доверием. При этом финансовые и технические затраты на реализацию угроз БИ могут быть несоизмеримы с выгодой вследствие их реализации.

Бывшие работники в случае потери лояльности вследствие увольнения могут стремиться нанести вред субъекту КИИ по личным мотивам. Чаще всего мотивом такого поведения может быть обида, возникшая из-за недостаточной оценки их роли в организации, недостаточный размер материальной компенсации, неподобающее место в корпоративной иерархии и т.п.

Разработчики и производители ПО, как правило, заинтересованы в долговременном и конструктивном сотрудничестве со своими партнёрами. Ненадлежащее исполнение обязательств сторонними организациями, внедрение ошибок, недекларированных возможностей в ПО ОКИИ влечет финансовые и репутационные риски для разработчиков и производителей ПО и может послужить основанием для расторжения договора по инициативе субъекта КИИ.

Обслуживающий персонал, не имеющий прав доступа в ОКИИ, — это нарушители, среди которых наиболее вероятно появление нелояльных или

внедренных инсайдеров, при этом они обладают, как правило, весьма низкими техническими навыками и имеют возможности действовать в пределах КЗ, ограниченные принятыми организационно-техническими мерами субъектом КИИ.

Пользователи ОКИИ с ролями «оператор» и «администратор», как правило, обладают информацией о специфике технологических и информационных процессов, типах аппаратного и программного обеспечения, многих применяемых мерах защиты. Однако мотивация такого типа нарушителя весьма низка в связи с высоким риском установления личности нарушителя в случае реализации им атаки и последующими потерями (правовыми, финансовыми и т.п.).

Сотрудники организаций, производящих обслуживание помещений, в которых размещены технические средства ОКИИ, — это сотрудники, производящие уборку таких помещений, командированные сотрудники других организаций, сотрудники сторонних организаций, размещённых в пределах охраняемой территории, и посетители, в рамках выполнения своих обязанностей на территории КЗ могут иметь физический доступ к техническим средствам, к носителям информации, но не имеют доступа к информации, хранящейся в ОКИИ.

При составлении модели нарушителя в рамках моделирования угроз БИ каждой из категорий нарушителей присвоены тип и условное обозначение. Пример для вышеперечисленных категорий нарушителей приведен в таблице 1.1.

Таблица 1.1 — Типы нарушителей

Категория нарушителя	**Тип нарушителя**	**Условное обозначение**
Хакеры или группировки хакеров	Внешний	Н1
Представители разведывательных служб иностранных государств	Внешний	Н2
Террористические организации	Внешний	Н3

Криминальные структуры	Внешний	Н4
Конкурирующие организации	Внешний	Н5
Представители контрагентов	Внешний	Н6
Бывшие работники	Внешний	Н7
Сотрудники организаций, производящих обслуживание помещений, в которых размещены технические средства ОКИИ	Внутренний (1 вида)	Н8
Обслуживающий персонал, не имеющий прав доступа в ОКИИ	Внутренний (1 вида)	Н9
Пользователи ОКИИ с ролями «оператор» и «администратор»	Внутренний (2 вида)	Н10

Как видно из таблицы 1.1, большинство категорий нарушителей относится к типу внешних нарушителей. Однако при моделировании угроз БИ каждого конкретного ОКИИ категории нарушителей могут как объединяться в группы по типу потенциальных вредоносных воздействий, так и разделяться на отдельные категории.

1.4 Методы оценки потенциала нарушителя БИ. Постановка задачи оценки нарушителя БИ ОКИИ

Основная методика оценки опасности реализации угроз БИ, используемая при моделировании угроз БИ ОКИИ, разработана ФСТЭК России [20]. Данная методика базируется на следующем определении: угроза БИ является актуальной, если имеется источник угрозы, условия для реализации угрозы, существует хотя бы один сценарий j ее реализации, а воздействие на информационные ресурсы или компоненты может привести к негативным последствиям, т.е. угроза БИ ij = [источник угрозы; условия реализации, сценарий реализации угрозы j;

негативные последствия]. В указанной методике обсуждается модель потенциального нарушителя, его уровни возможностей, а также приводится пример определения актуальных нарушителей БИ на основе качественных показателей оценки актуальности.

В работах [17,36,79] ведется работа над методами и алгоритмами количественной оценки потенциала нарушителя БИ на основе метрик CVSS.

В развитие указанных методик и подходов целесообразно разработать методы и алгоритмы определения как потенциала нарушителя, так и опасности реализации указанными нарушителями актуальных угроз БИ.

Согласно исследованию [21], методика ранжирования потенциальных нарушителей $S = \{s_i\}\left(i = \overline{1,n}\right)$ на промышленном предприятии заключается в присвоении им количественных рейтингов (оценок уровня угроз). Этот подход базируется на сравнительном анализе нарушителей по широкому спектру критериев $C = \left\{c^j\right\}\left(j = \overline{1,m}\right).$ Сравнение производится с гипотетическим «эталонным» субъектом доступа, который обладает наилучшими возможными значениями всех показателей. Таким образом, рейтинг каждого нарушителя косвенно отражает его способность реализовать угрозу по сравнению с этим идеализированным эталоном.Исходя из проведенного анализа методики ФСТЭК России [20], научных работ [22 - 27], структурированные способы реализации угроз БИ приведены в таблице 1.2.

Таблица 1.2 — Основные способы реализации угроз БИ

Обозначение способов реализации угроз БИ	**Наименование способов реализации угроз БИ**
c^1	Осуществление несанкционированного доступа к каналам связи ОКИИ, находящимся в пределах КЗ
c^2	Осуществление доступа к ОКИИ с использованием специальных программных воздействий посредством вредоносного ПО или программных закладок
c^3	Осуществление доступа с использованием элементов

	информационной инфраструктуры ОКИИ
c^4	Осуществление доступа через ИС, ИТКС и АСУ ТП взаимодействующих организаций при их подключении к ОКИИ
c^5	Установка или запуск ПО, не входящего в перечень разрешенного
c^6	Вывод из строя отдельных компонентов ОКИИ

Набор способов реализации угроз БИ, по которым выполняется оценка потенциальных нарушителей $\forall s_i$, можно представить информационным вектором

$$\vec{c}_i = \left(c_i^1,...,c_i^j,...,c_i^m\right), \quad (1.1)$$

где c_i^j – j-я компонента $j = \overline{1,m}$ информационного вектора s_i - го сотрудника, или иначе: $S_i \Leftrightarrow \vec{c}_i$.

В рейтинговом методе [21] задача ранжирования заключается в сравнении и установлении отношений предпочтения векторов, например,

$$\vec{c}_1, \le \vec{c}_l, \le ..., \le \vec{c}_2, \le ..., \quad (1.2)$$

что и означает упорядочение, многокритериальное ранжирование элементов множества S, соответственно

$$\vec{s}_1, \ge \vec{s}_l, \ge .. \vec{s}_2, \ge ..., \quad (1.3)$$

в порядке снижения уровня угрозы $t(s_i)$ по значениям параметров множества C.

Главное достоинство рейтингового метода – комплексный характер оценки уровня угроз. Однако данный метод также имеет и ряд более-менее существенных недостатков:

– в связи с тем, что модель нарушителя содержит большое число показателей, зачастую имеющих корреляционные связи между собой, влияющих на уровень угрозы, возникают трудности в комплексной оценке уровня угроз по каждому сотруднику $s_i \in S$;

– невозможность применения одних и тех же арифметических операций для значений показателей модели нарушителя, измеряемых как в количественных, так и качественных шкалах;

– использованный в неформализованной модели естественный язык хорошо передает семантику предметной области и понятен аналитику, однако на практике не позволяет точно и однозначно описать сущности и их взаимосвязи, представленные в модели нарушителя.

Согласно методике формализации нечеткой информации, основанной на лингвистическом подходе, в рамках которого в качестве значений переменных допускаются как числа, так и слова, а также предложения естественного языка, может быть проведена формализация нечеткой информации, а ее аппаратом является теория нечетких множеств. В соответствии с данной методикой понятие «нарушитель БИ ОКИИ» можно представить нечетким множеством, заданным на универсальном множестве сотрудников S

$$\widetilde{A}^j = \left\{ \frac{u^j(s_1)}{s_1}, \frac{u^j(s_2)}{s_2}, ..., \frac{u^j(s_n)}{s_n} \right\}, \tag{1.4}$$

с функцией принадлежности $u^j(s_i)$, характеризующей соответствие любого нарушителя $s_i \in S$ данному понятию.

При введении в модель показателя важности параметров задача ранжирования нарушителей формализуется следующим образом:

$$u_{\tilde{c}}(s_i) = \sum_{j=1}^{m} b^j u^j(s_i), \tag{1.5}$$

где $b^1, b^2, ..., b^m$ – неотрицательные числа $\sum_{j=1}^{m} b^j = 1$, характеризующие относительную важность способов $c^1, c^j, ..., c^m$ или их удельный вес, представленный в таблице 1.3, в модели нарушителя; $u^j(s_i)$ – значение функции принадлежности из интервала [0,1] для каждого нарушителя $s_i \in S$ по значению

каждого параметра $c^j\left(j=\overline{1,m}\right)$, которая характеризует, насколько рассматриваемый нарушитель соответствует понятию «нарушитель по j-му параметру».

Таблица 1.3 — Удельный вес способов реализации угроз БИ

Способы реализации угрозы БИ	**Удельный вес**
Осуществление несанкционированного доступа к каналам связи ОКИИ, находящимся в пределах КЗ	$b^1=0{,}25$
Осуществление доступа к ОКИИ с использованием вредоносного ПО или программных закладок	$b^2=0{,}2$
Осуществление доступа с использованием элементов информационной инфраструктуры ОКИИ	$b^3=0{,}16$
Осуществление доступа через информационные системы взаимодействующих организаций при их подключении к ОКИИ	$b^4=0{,}15$
Установка или запуск ПО, не входящего в перечень разрешенного	$b^5=0{,}14$
Вывод из строя отдельных компонентов ОКИИ	$b^6=0{,}1$

Исходя из вышеуказанного, расчеты показывают, что максимальная степень опасности для ОКИИ соответствует нарушителю с наибольшим значением функции принадлежности.

$$u_{\tilde{c}}\left(s^*\right)=\max_{s_i\in S}u_{\tilde{c}}\left(s_i\right). \tag{1.6}$$

Рассмотренные методы не учитывают угрозы, специфичные для каждого из уровней ОКИИ. Поэтому одной из задач диссертации является разработка метода определения потенциала нарушителя БИ ОКИИ, учитывающего возможные негативные последствия от атак как на ИС и ИТКС, так и на различные уровни АСУ ТП.

1.5 Опасность реализации угроз БИ в отношении ОКИИ

Функционирование ОКИИ напрямую связано с выполнением технологических и (или) информационных процессов.

Технологический процесс представляет собой ряд взаимосвязанных процессов: основных, вспомогательных и обслуживающих. Наиболее распространенные характеристики технологических процессов представлены в таблице 1.4 [28].

Таблица 1.4 — Характеристики технологических процессов

Тип процесса	**Характеристика процесса**
основной	изготовление продукции
	изготовление деталей
	управление операциями
вспомогательный	изготовление технологической оснастки (инструмента, приспособлений, штампов и т.д.)
	ремонт оборудования, зданий, сооружений
	производство и распределение различных видов энергии
обслуживающий	транспортные операции (межцеховые, межоперационные)
	складские операции
	технический контроль выполнения основных и вспомогательных процессов

Каждый из технологических процессов обладает техническими, экономическими, эргономическими свойствами, а также свойствами безопасности, описывающими его состояние. Наиболее часто встречающиеся в научных работах [29 - 31] свойства технологических процессов приведены в таблице 1.5.

Таблица 1.5 — Свойства технологических процессов

Технические	**Экономические**	**Эргономические**	**Свойства безопасности**
Точность	Материалоемкость	Удобство обслуживания	Уровень токсичности
Надежность	Энергоемкость	Удобство управления	Степень загрязнения окружающей среды
Быстродействие	Производительность		Взрывобезопасность
Контролируемость	Технологическая трудоемкость		

Информационные процессы непосредственно связаны с выполнением технологического процесса обработки информации и обладают рядом свойств, которые определяют их природу, эффективность и безопасность. Эти свойства могут варьироваться в зависимости от контекста (например, обработка данных, передача информации, хранение), но в соответствии с [32] можно выделить несколько ключевых свойств, представленных в таблице 1.6.

Таблица 1.6 — Свойства информационных процессов

Свойство	**Описание**
Достоверность	Информация должна быть точной и соответствовать действительности
Полнота	Процесс должен обеспечивать достаточный объем данных
Актуальность (своевременность)	Информация должна быть доступна в нужный момент времени
Доступность	Информация должна быть доступна авторизованным пользователям и сервисам
Конфиденциальность	Защита информации от НСД
Целостность	Данные не должны изменяться несанкционированно или теряться
Управляемость	Процесс должен поддаваться контролю и

	регулированию
Эффективность	Оптимальное использование ресурсов (времени, памяти, вычислительной мощности)
Масштабируемость	Возможность адаптации к увеличению объемов данных
Надежность	Устойчивость к сбоям и ошибкам

В отношении средств автоматизации технологических и информационных процессов, обладающих теми или иными свойствами, могут быть реализованы угрозы БИ, направленные на снижение общего уровня защиты (защищенности) ОКИИ.

Оценка опасности реализации угроз БИ отражает соотношение вероятных последствий конкретного рассматриваемого нарушения режима БИ ОКИИ к максимальному уровню ущерба от реализации угроз.

Известные в настоящее время методы оценки опасности реализации угроз БИ можно разделить на две группы: вербальные и вероятностные [33 - 34].

При вербальном подходе оценка уровня опасности угроз БИ устанавливается экспертным путём. Она выражается в виде вербальной интерпретации коэффициента, соответствующего потенциальному ущербу от реализации конкретной угрозы в рамках ОКИИ. В свою очередь, методы второй категории, основанные на принципах теории вероятностей и математической статистики, пользуются большей популярностью. Их применение предполагает сбор и анализ значительных массивов статистических данных, что позволяет сформировать необходимую информационную базу для проведения расчётов.

Вероятностные подходы нацелены на снижение объема экспертной работы за счёт уменьшения субъективного влияния каждого отдельного специалиста. Данное сокращение достигается путём соотнесения уровня опасности от реализации угроз БИ с объёмом защищаемых данных, которые обрабатываются в конкретном сегменте ОКИИ.

Разработка современных методик оценки опасности реализации угроз БИ пока не позволяет полностью исключить опрос экспертов по всем векторам атак. Основная причина этого — отсутствие в действующих нормативных и методических документах формализованных количественных показателей для оценки угроз и уязвимостей. Однако, важной задачей является минимизация субъективизма в количественных оценках опасности реализации угроз БИ, путем применения в качестве критериев оценки критичности и значимости технологических процессов, выполняемых ОКИИ. Исходя из вышеуказанного, оценка опасности в разрабатываемом методе должна представляться четкой величиной, а защищенность ОКИИ определяться посредством отношений между оценкой опасности реализации угроз БИ и возможным ущербом от реализации угроз БИ на каждом из уровней ОКИИ.

1.6 Постановка задачи моделирования угроз БИ ОКИИ

Основной целью моделирования угроз БИ является точное прогнозирование последствий, к которым может привести реализация угроз со стороны нарушителей в рамках ОКИИ. В процессе моделирования производится оценка степени опасности различных сценариев атак, потенциально ведущих к нанесению ущерба ключевым процессам — как технологическим, так и информационным. Полученные оценки служат фундаментом для обоснованного выбора комплекса защитных мер.

Под защиту в ОКИИ попадают следующие категории: системные параметры и данные измерений; информация, признанная критической согласно профилю деятельности ОКИИ; а также критические звенья инфраструктуры. К последним относятся программно-аппаратные компоненты (рабочие станции, серверы, ПЛК, сетевое оборудование), системное и прикладное ПО и средства защиты информации, развернутые на всех уровнях организации [16].

В диссертации используется термин уязвимое звено как унифицированное понятие предмета, в отношении которого потенциальными нарушителями БИ могут быть реализованы угрозы БИ. Указанный предмет, имеет различные названия в зависимости от рассматриваемых методик моделирования угроз БИ: в соответствии с [20] – объект воздействия; в методике TRIKE применяется термин «Активы»; в методике STRIDE применяется термин «сетевые компоненты»; в методике NIST-800-39 используется термин «Бизнес-процесс» или «ИТ-система»

Как отмечено в [14], для определения актуальности угроз БИ, источником которых могут быть как внешние, так и внутренние нарушители, используется двухкомпонентный показатель. Первый компонент этого вектора отражает вероятность осуществления угрозы, а второй — коэффициент, характеризующий уровень её опасности и потенциальный ущерб от её реализации.

$$\vec{U}_j = \left[R_j, D_j\right] \tag{1.7}$$

Под «Вероятностью реализации угрозы» понимается показатель, определяемый экспертным методом и характеризующий вероятность реализации возможным нарушителем БИ через потенциальные угрозы при функционировании ОКИИ.

В работе [40] рассмотрена возможность использования EPC - нотаций для построения сценариев угроз БИ в АСУ ТП. В соответствии с нормативно-правовыми документами, при наличии сценария угрозы БИ она признается актуальной для информационной системы и включается в модель угроз БИ для обоснования выбора мер и СЗИ.

В работе [36] отбор экспертов осуществляется на основе оценки их профессиональной квалификации. К ключевым критериям относятся наличие высшего образования в сфере БИ или ИТ, а также практический опыт работы в области БИ продолжительностью не менее трёх лет. Указанных специалистов ограниченное количество на рынке труда и соответственно формировать экспертную комиссию становится с каждым годом всё проблематичнее.

Путем проведения аналогий с [14] было сформулировано предположение: предварительная оценка потенциала нарушителя БИ ОКИИ (низкий, средний, высокий и т.п.) при построении модели нарушителя БИ и использование оценок опасности реализации угроз БИ на каждом из уровней ОКИИ позволит улучшить эффективность процесса моделирования угроз БИ. Вместе с тем необходимо определять нарушителей, чей потенциал недостаточен для реализации угроз.

Таким образом, целью диссертации является повышение эффективности процесса моделирования угроз БИ ОКИИ на основе разработки методов и алгоритмов интеллектуального анализа данных, позволяющих повысить достоверность и объективность результатов анализа и оценки актуальных угроз БИ с использованием аппарата экспертных оценок.

Основная научно-техническая задача заключается в преодолении особенностей существующих подходов и методик путем разработки методов и алгоритмов, допускающих расширение круга экспертов, в том числе путем привлечения специалистов в области функционирования технологических и (или) информационных процессов, выполняемых в ОКИИ.

1.7 Существующие методы и алгоритмы моделирования угроз БИ ОКИИ

Анализ комплекса условий, создающих угрозы информационной безопасности, осуществляется с помощью множества международных и российских методик. Наиболее популярные из них, применяемые для моделирования угроз [41], включают:

Международные: Методологии TRIKE, PASTA, STRIDE, NIST и иные, каталогизированные организацией EC Council на ее официальном сайте.

Отечественные: Актуальная методика ФСТЭК России по оценке угроз БИ; требования национальных стандартов серии 62443/56205, регламентирующих защищенность промышленных коммуникационных сетей и систем. Также научным сообществом предлагается использование хорошо зарекомендовавшего

себя риск-ориентированного подхода, технологий когнитивного моделирования и Text Mining, методов попарных сравнений и матриц отношений [35-36].

В целях оценки угроз БИ ОКИИ обязательным к исполнению является методический документ [20]. Данная методика ориентирована на оценку антропогенных угроз БИ, возникновение которых обусловлено действиями нарушителей и имеет в своей основе риск-ориентированный подход.

Среди международных подходов к оценке угроз БИ стоит выделить методику TRIKE, которая широко используется при моделировании угроз для ПО ОКИИ, однако данная методика может иметь применение и на аппаратном уровне промышленных систем.

В основе методики TRIKE лежит структура использования модели угроз БИ как инструмента управления рисками ОКИИ, в то время как методика [20] использует результаты оценки рисков (ущерба), проведенной обладателем информации или оператором ОКИИ.

В таблице 1.7 представлена сравнительная характеристика двух рассматриваемых методик с указанием основных критериев оценки угроз БИ.

Таблица 1.7 — Сравнительная характеристика методик оценки угроз БИ

Критерии	**Методика**	
	Методика ФСТЭК РФ	***TRIKE***
Входные данные	Риски	Активы, операции, атаки, правила, риски
Механизмы управления	Нормативные акты, техническая и эксплуатационная документация, технологические процессы, БДУ, векторы атак	Нормативные акты, техническая и эксплуатационная документация, технологические процессы
Механизмы исполнения	Экспертная группа, программные средства	Экспертная группа, программные и средства
Перечень угроз	Общий перечень угроз БИ, содержащийся в БДУ	Генерация угроз экспертной группой
Векторы атак	Базы данных: CAPEC, ATT&CK, OWASP и др.	Генерируемое аппаратными средствами дерево атак

Оценка рисков	Результаты оценки рисков используются при оценке угроз	По результатам оценки угроз
Результаты	Отражаются в модели угроз	Отражаются в модели угроз
Наличие ПО	Отсутствует	Есть

По результатам анализа характеристик методик, представленных в таблице 1.7, можно сделать вывод о различающихся подходах при формировании перечней угроз ОКИИ.

В целях визуализации различий рассматриваемых методик на примере ОКИИ – АСУ ТП проведено функциональное моделирование с применением методологии IDEF0. На рис. 1.4 представлена функциональная модель процесса оценки угроз БИ в соответствии с методикой ФСТЭК РФ.

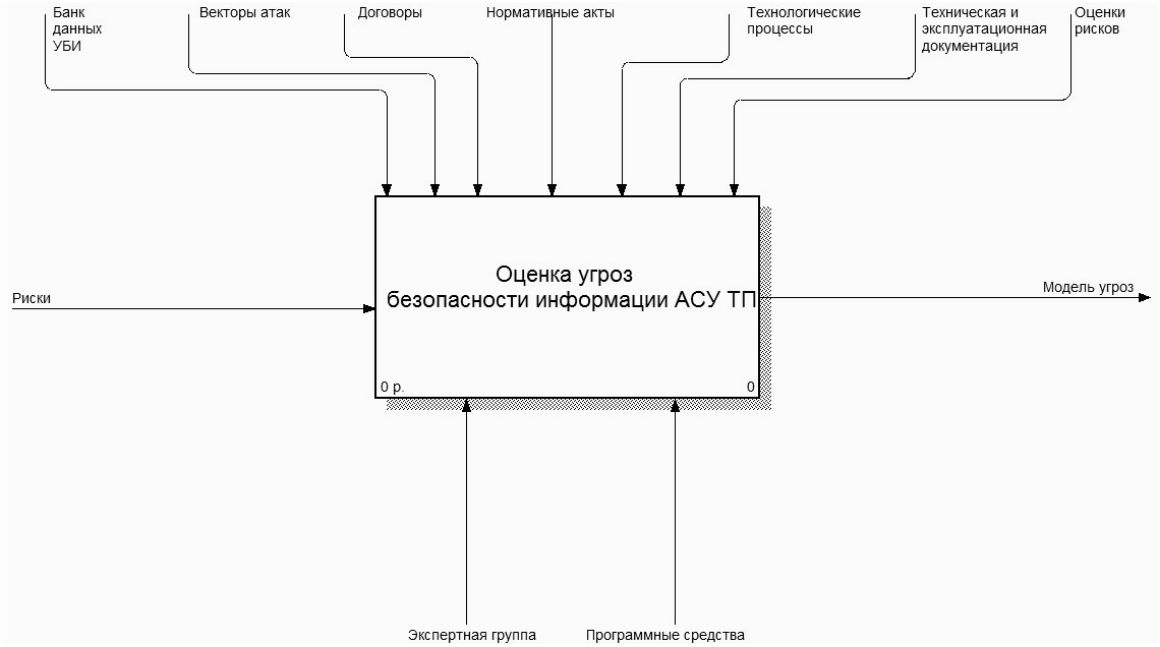


Рис. 1.4 IDEF0-модель методики ФСТЭК РФ

В соответствии с методикой ФСТЭК РФ, угроза БИ i возможна, если имеется нарушитель или иной источник угрозы $N(i)$, объект $O(i)$, на который осуществляются воздействия, способы реализации угроз БИ $R(i)$, а реализация угрозы может привести к негативным последствиям $P(i)$. Таким образом, угрозы БИ, характерные для ОКИИ, будут определяться на основании (1.8).

$$U_i = [N(i); O(i); R(i); P(i)]. \quad (1.8)$$

Угроза может реализовываться потенциальным нарушителем относительно объектов воздействия.

Объект воздействия — это информационные ресурсы и компоненты систем и сетей, несанкционированный доступ к которым или воздействие на которые в ходе реализации угроз БИ может привести к негативным последствиям [20].

В качестве объектов потенциального воздействия могут рассматриваться физические устройства, ПО, информационные массивы, пользователи, технологические процессы и сетевые ресурсы.

Эффективное построение модели угроз требует четкой идентификации всех возможных объектов воздействия, а также детального анализа их атрибутов и потенциальных уязвимостей.

Основные типы объектов воздействия:

Физические устройства: серверы, рабочие станции, маршрутизаторы, коммутаторы. Потенциальные нарушители могут попытаться получить физический доступ к устройствам, чтобы нарушить работу ОКИИ.

ПО: приложения, операционные системы и другие программные продукты являются одними из наиболее распространенных объектов воздействия.

Данные: любая информация, хранящаяся в ОКИИ, является потенциальным объектом воздействия. Атаки могут быть направлены на кражу данных, изменение их содержания или уничтожение.

Пользователи: люди, работающие с системой, также могут стать объектами воздействия. Например, нарушитель может использовать методы социальной инженерии для компрометации ОКИИ.

Процессы: процессы, выполняющиеся в системе, такие как передача данных по сети, обработка транзакций. Нарушение указанных процессов может привести к сбоям в работе ОКИИ или утечке информации.

Сетевые ресурсы: сетевые сервисы, такие как веб-серверы, почтовые сервера и DNS-сервера. Нарушители могут пытаться вывести ресурсы ОКИИ из строя или перехватить передаваемые данные.

В таблице 1.8 представлен перечень объектов воздействия и их компонентов в соответствии с [20].

Таблица 1.8 — Перечень объектов воздействия и их компонентов

К.1	К.1.5	К.1.7.2	К.2.4.4
Программное	Прикладное ПО	Веб-клиент	Средство обнаружения
К.1.1	К.1.5.1	К.1.7.3	К.2.4.5
Микропрограммное	Клиент электронной	Веб-интерфейс	Другие средства защиты
К.1.1.1	К.1.5.2	К.1.7.4	К.2.5
Прошивка (встроенная	Мессенджер	Другие примеры веб-	Интерфейсы сервисного
К.1.1.2	К.1.5.3	К.2	К.2.5.1
UEFI/BIOS	Среда управления	Программно-аппаратные	Распаянные на плате
К.1.2	К.1.5.4	К.2.1	К.3
Системное программное	Виртуальная машина	Периферийное	Сетевые компоненты
К.1.2.1	К.1.5.5	К.2.1.1	К.3.1
Операционная система	Система управления	Принтер	Канал передачи данных
К.1.2.2	К.1.5.6	К.2.1.2	К.3.1.1
Мобильная	Мобильное приложение	Монитор	Проводной канал передачи
К.1.2.3	К.1.5.7	К.2.1.3	К.3.1.2
Программная оболочка	Скрипт автоматизации	Мышь	Беспроводной канал передачи
К.1.2.4	К.1.5.8	К.2.1.4	К.3.2
Драйвер	Система мониторинга	Клавиатура	Протокол передачи данных
К.1.2.5	К.1.5.9	К.2.1.5	К.3.2.1
Утилита	Клиент системы	Микрофон	Протоколы аутентификации
К.1.2.6	К.1.5.10	К.2.1.6	К.3.2.2
Загрузчик операционной	Клиент IP-телефонии	Веб-камера	Протоколы обмена данными
К.1.2.7	К.1.5.11	К.2.1.7	К.3.2.3
Гипервизор	Пакет офисного ПО	Другие периферийные	Другие примеры протоколов
К.1.3	К.1.5.12	К.2.2	К.4
Сервисное ПО	ПО для проектирования и	Интерфейсы ввода/вывода	Пользователи
К.1.3.1	К.1.5.13	К.2.2.1	К.4.1
Системные и сетевые	Система управления	Интерфейс подключения	Привилегированные
К.1.3.2	К.1.5.14	К.2.2.2	К.4.1.1
Терминальный сервер	Контейнер	Интерфейс подключения	Администратор
К.1.3.3	К.1.5.15	К.2.2.3	К.4.1.2
Веб-сервер	Веб-браузер	Интерфейс подключения	Разработчик
К.1.3.4	К.1.5.16	К.2.2.4	К.4.1.3
Система управления	Оркестратор контейнеров	Интерфейс подключения	Тестировщик
К.1.3.5	К.1.6	К.2.2.5	К.4.1.4
Файловый сервер	Программное СЗИ	Интерфейс подключения	Модератор
К.1.3.6	К.1.6.1	К.2.2.6	К.4.1.5
Сервер электронной	Антивирусные средства	Интерфейс подключения	Сотрудник технической
К.1.3.7	К.1.6.2	К.2.2.7	К.4.2
Сервер	Агент системы защиты	Датчики	Непривилегированные
К.1.3.8	К.1.6.3	К.2.2.8	К.4.2.1
Сервер IP-телефонии	Межсетевой экран	Сетевой интерфейс	Непривилегированный
К.1.3.9	К.1.6.4	К.2.3	К.4.2.2
DNS-сервер	ПО системы резервного	Устройство хранения	Клиент организации
К.1.3.10	К.1.6.5	К.2.3.1	К.1.4.2
Сервер каталогов	Средства разграничения	Система хранения данных	Средства тестирования и
К.1.3.11	К.1.6.6	К.2.3.2	К.1.7.1
Система	Средства анализа	Съемный машинный	Веб-сайт
К.1.4	К.1.6.7	К.2.4	К.2.4.3
Инструментальное ПО	Другие средства защиты	Программно-аппаратное	Межсетевой экран
К.1.4.1	К.1.7	К.2.4.1	
ПО для разработки кода	Веб-приложение	Криптошлюз	

Стоит отметить, что к полевому уровню АСУ ТП относятся компоненты объектов воздействия К.2.2.8 Сетевой интерфейс объекта воздействия О6. Активное сетевое оборудование.

Актуальность (опасность реализации) возможных угроз БИ определяется наличием хотя бы одного сценария каждого способа реализации возможной угрозы БИ в соответствии с (1.9).

$$U_i^s = F(i,s), \tag{1.9}$$

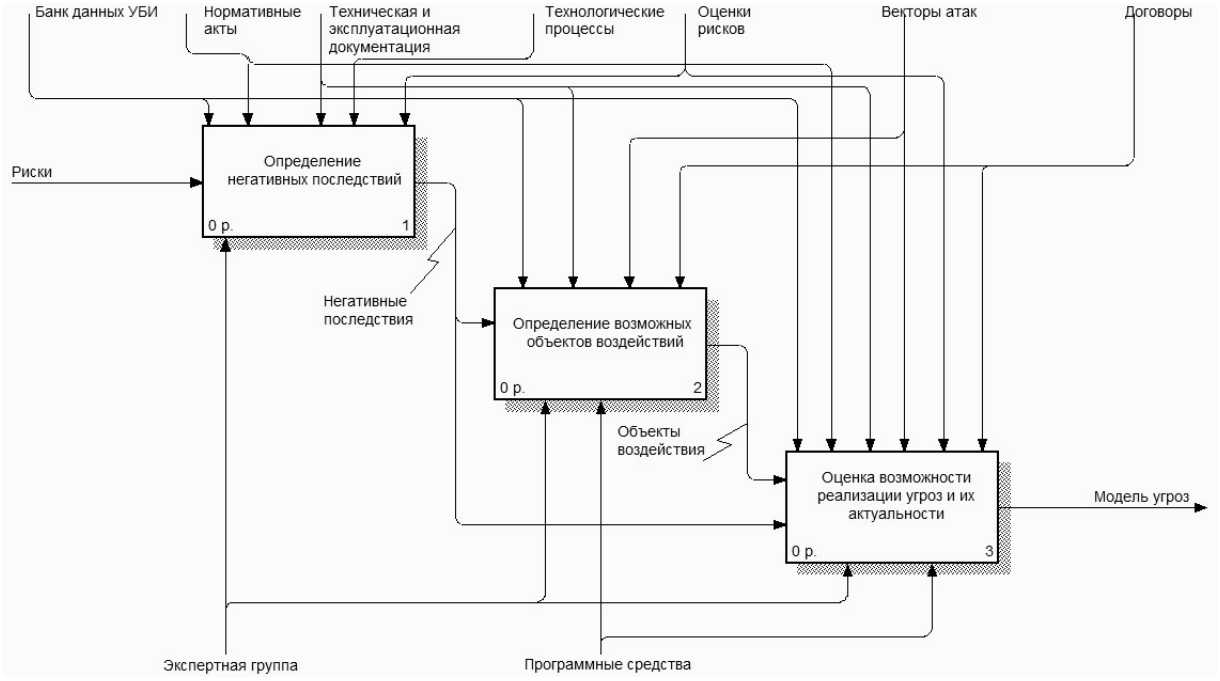
где $F(i,s) \in \{0,1\}$ – функция принадлежности для угроз, характеризующая актуальность i-й угрозы при наличии s сценариев её реализации.

В соответствии с результатами определения сценариев реализации угроз, функция принадлежности $F(i,k)$ принимает значения:

0 – неактуальная угроза, $s = 0$;

1 – актуальная угроза, $s \geq 1$.

Сценарий определяется для каждого нарушителя на основании выполнения последовательности действий, представленных декомпозицией функционального блока Оценка угроз БИ рис. 1.5.



1.5 Декомпозиция функционального блока Оценка угроз БИ методики ФСТЭК РФ

На рис. 1.6 продемонстрирована функциональная модель процесса оценки угроз БИ в соответствии с методикой TRIKE.

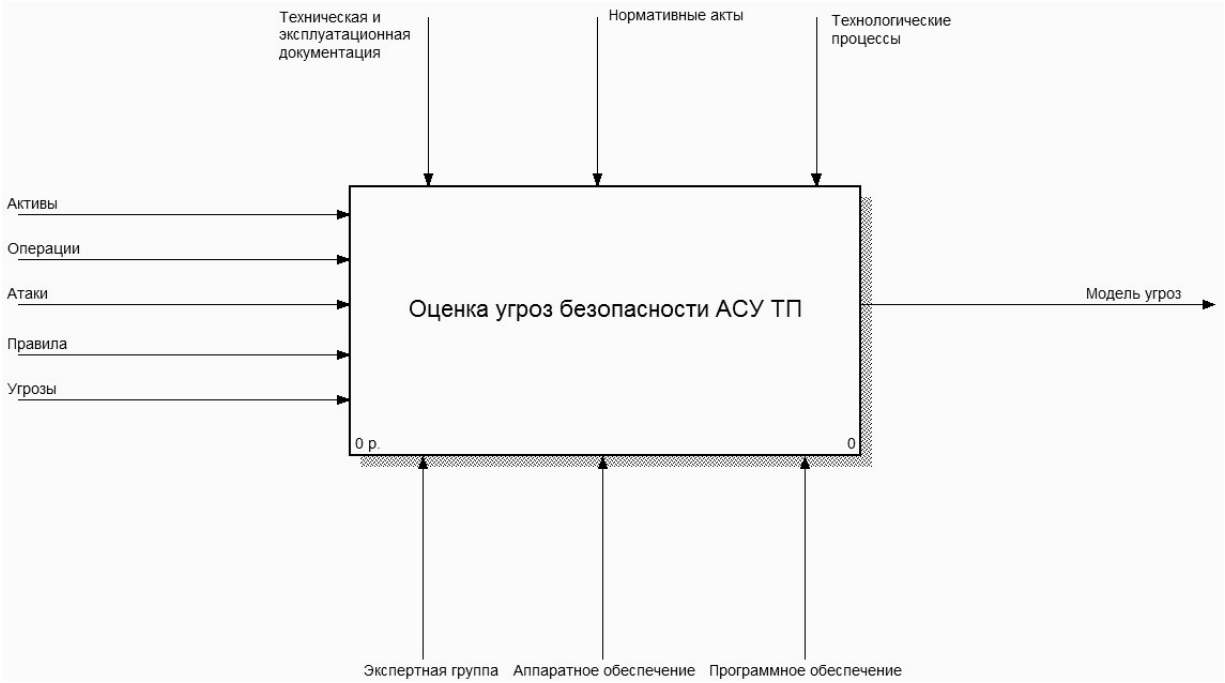


Рис. 1.6 IDEF0-модель методики TRIKE

Согласно методологии TRIKE, перечень угроз информационной безопасности формируется на базе разработанной «модели требований» по определенному алгоритму. Первоначально для каждой разрешенной операции генерируется угроза типа «отказ в обслуживании». Затем набор разрешенных операций преобразуется в набор запрещенных действий, для каждого из которых создается угроза «повышение привилегий».

На следующем этапе для каждой разрешенной операции дополнительно формируются угрозы повышения привилегий как для полностью, так и для частично запрещенных операций. Завершающим шагом является добавление угрозы «социальной ответственности», которая предполагает возможность использования субъектом данной системы для атаки на другие системы [43]. Полученная модель угроз с применением TRIKE может быть формализована в соответствии с выражением 1.10.

$$U_{di} = \sum_{d=1}^{n} \left(U_d(a) + \sum_{i=1}^{3} U_{\bar{d}}(b_i) \right), \qquad (1.10)$$

где U_d - угрозы в отношении операций $d=\overline{1,n}$, $U_d(a)$ - функция, характеризующая угрозу категории «отказ в обслуживании» в отношении операций d, а функция $U_{\bar{d}}(b_i)$ описывает угрозы категории «повышение привилегий» $b_i, i=\overline{1,3}$, для инвертированной операции $\bar{d}$ при следующих условиях: b_1 - угроза полностью запрещенного действия, b_1 - угроза частично запрещенного действия, b_1 - угроза «социальной ответственности».

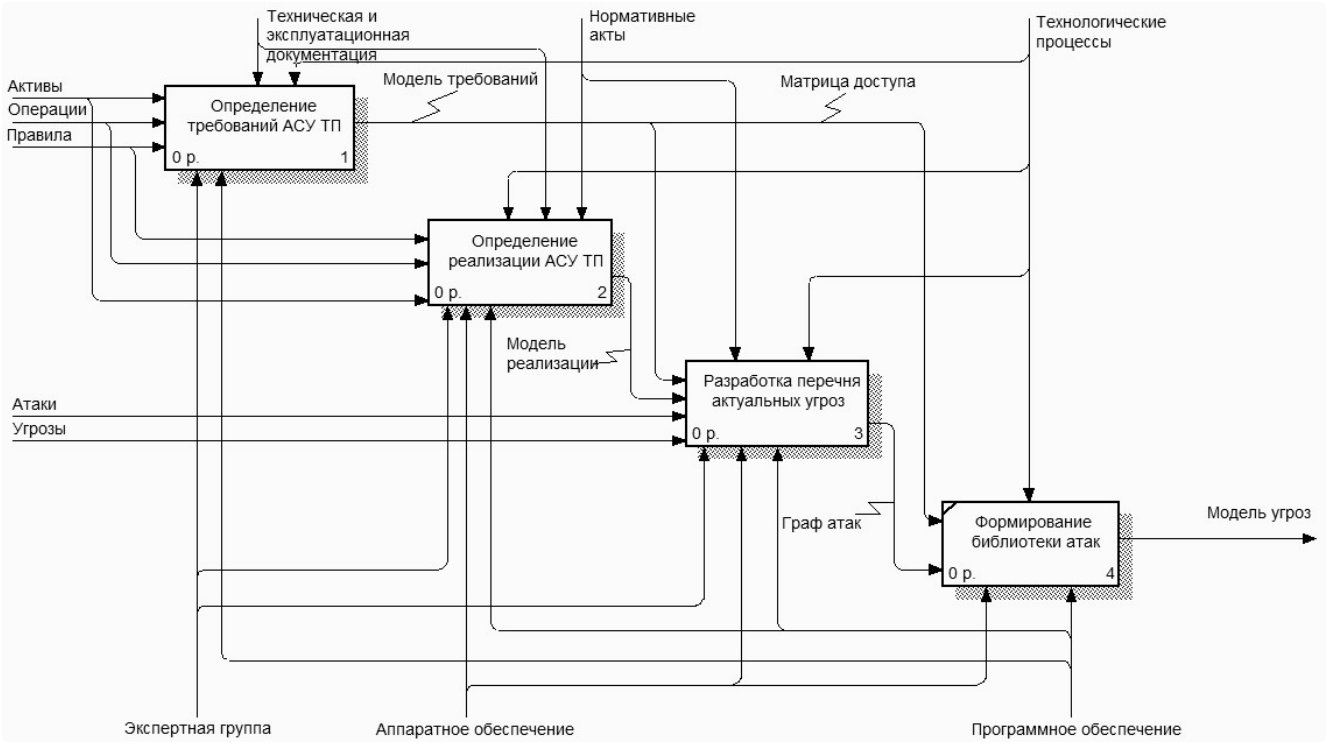


Рис. 1.7 Декомпозиция функционального блока Оценка угроз БИ методики TRIKE

На рис. 1.7 представлена декомпозиция функционального блока «оценка угроз безопасности информации АСУ ТП», отражающая формализованное представление подходов к моделированию угроз БИ. Декомпозиции, представленные на рис 1.6 и 1.7, визуализируют основные отличия методик, в частности, наличие в методике TRIKE библиотеки атак, основанной на риск-ориентированном подходе оценки угроз БИ.

Основное отличие рассматриваемых методик заключается в том, что методика TRIKE подразумевает автоматизированное построение графа атак на

ОКИИ по завершении формирования конечного перечня угроз БИ, формируя библиотеки атак на основе однотипных путей графа, а методика ФСТЭК РФ использует типовые техники, используемые для построения сценариев реализации угроз БИ.

Можно выделить основные недостатки рассмотренных методик:

1) Неполнота: рассмотренные методики могут не заложить все возможные (библиотеки атак) сценарии угроз, что может привести к неполной оценке рисков и некорректной оценке опасности реализации угроз БИ.

2) Неспособность прогнозирования новых угроз: рассмотренные методики основываются на анализе известных угроз и их типовых сценариев. Однако появление новых типов угроз может быть недостаточно предсказуемым и даже неуместным, поэтому методики могут быть неспособны полностью оценить новые угрозы БИ или прогнозировать их.

3) Ограничение области использования: методика TRIKE зачастую не применяется отечественными специалистами в области БИ, и её использование может быть ограничено только оценкой угроз, связанных с ИС ввиду некорректных результатов моделирования угроз для ИТКС и АСУ ТП.

4) Статический характер: рассмотренные методики моделирования угроз БИ могут не учитывать изменения во внутренней и внешней среде ввиду наличия риск-ориентированного подхода, что может фактически привести к реализации устаревших методов защиты.

5) Отсутствие квалифицированных специалистов: методика моделирования угроз требует от специалистов высокой квалификации в области БИ и мотивирование разработанных сценариев актуальными угрозами.

Таким образом, методика ФСТЭК РФ фокусируется на оценке возможностей и ресурсов нарушителя, тогда как подход TRIKE ориентирован на анализ состояния средств защиты информации и последующее моделирование угроз. У рассмотренных методик есть основной недостаток, поскольку они имеют в своей основе риск-ориентированный подход при оценке опасности реализации

угроз БИ и не подразумевают рассмотрение каждого уровня ОКИИ в отдельности, что создает предпосылки к завышению оценок защищенности отдельных узлов и компонентов ОКИИ ввиду их незначительности относительно общей топологии и архитектуры ОКИИ и соответственно менее подвержены риску быть атакованными нарушителями.

1.8 Выводы по первой главе

1. Выполнен анализ нормативно-правовой и терминологической базы обеспечения БИ ОКИИ. Проведена аналитика наиболее крупных атак на промышленную информационную инфраструктуру. Описана многоуровневая структура ОКИИ.

2. По результатам проведения анализа предметной области сформулирована задача построения модели нарушителя БИ ОКИИ. Представлена классификация потенциальных нарушителей, а также перечислены их основные характеристики, позволяющие формировать предположения об их квалификации и мотивации.

3. Проанализированы методы оценки потенциала нарушителя БИ. Осуществлена постановка задачи оценки нарушителей ОКИИ, учитывающей возможные негативные последствия от атак на различные уровни ОКИИ.

4. Рассмотрены методы определения оценки опасности реализации угроз БИ потенциальными нарушителям. Выдвинуто следующее предположение: Разрабатываемый метод должен предполагать количественное выражение уровня опасности, при этом защищенность ОКИИ предлагается оценивать через корреляцию между вероятностью реализации угроз ИБ и масштабом потенциального ущерба на каждом уровне ОКИИ.

5. Рассмотрены отдельные отечественные и зарубежные методики моделирования угроз БИ ОКИИ. По результатам подробного анализа сделаны выводы об их отдельных достоинствах и недостатках.

6. Выделена основная цель и задачи диссертационной работы.

ГЛАВА 2. МЕТОДОЛОГИЧЕСКОЕ ОБЕСПЕЧЕНИЕ МОДЕЛИРОВАНИЯ УГРОЗ БИ ОКИИ

2.1 Метод определения потенциала нарушителя БИ ОКИИ с использованием матрицы идентификаторов угроз.

Рассмотренные в главе 1 методы определения потенциала нарушителя информационной безопасности опираются не на текущие угрозы, реализуемые на различных уровнях ОКИИ, а определяют потенциал нарушителя в зависимости от его возможностей по реализации угроз БИ. Так, нарушители с неограниченным техническим функционалом в рассмотренных методах по умолчанию являются нарушителями с высоким потенциалом для всех существующих угроз вне зависимости от уровня ОКИИ, на который осуществляется негативное воздействие. Однако рассматривать подобных нарушителей в качестве потенциальных для всех без исключения ОКИИ некорректно, ввиду возможного отсутствия мотивации нарушителя на реализацию угроз БИ. Указанная проблема возникает из-за отсутствия численной оценки потенциала нарушителя, а также применения исключительно вербальных метрик. В рамках решения указанной проблемы предложен метод, основанный на экспертных оценках.

Пусть E_i – оценка потенциала i -го нарушителя, а E_{ij} - оценка потенциала i -го нарушителя j-м экспертом, а C_{mj} -идентификатор возможности реализации угрозы (способ реализации угрозы) m_i, $m = 1..M$, определенный для нарушителя экспертом при следующем условии: $C_{mj} = 1$ – существует способ реализации угрозы БИ рассматриваемым нарушителем, $C_{mj} = 0$ – способ реализации угрозы БИ не существует для рассматриваемого нарушителя.

В качестве идентификаторов угроз в разработанном методе выступают способы реализации угроз БИ, представленные в документе [20]. Используемая в диссертации анкета опроса экспертов для выявления потенциальных нарушителей БИ ОКИИ представлена в приложении 1.

По результатам экспертной оценки для каждого опрашиваемого эксперта формируется матрица идентификаторов угроз

$$C_i = \begin{pmatrix} c_{11} & \cdots & c_{1J} \\ \vdots & \ddots & \vdots \\ c_{M1} & \cdots & c_{MJ} \end{pmatrix}. \quad (2.1)$$

Возникающая при этом субъективность индивидуальной оценки потенциала нарушителя исключается путем применения группового экспертного оценивания. По результатам опроса всех экспертов формируется множество матриц идентификаторов угроз $\overline{C} = \{C_1, C_2, C_3 ... C_z\}$, где z-общее количество матриц идентификаторов угроз.

Для решения задачи определения согласованности мнения экспертов предложено использовать метод анализа входных данных с помощью вычисления коэффициента конкордации Кендалла-Смита [44 - 45], в результате применения которого формируется множество согласованных матриц идентификаторов угроз $\widetilde{C} = \{C_1, C_2, C_3 ... C_\gamma\}$, где γ- количество матриц идентификаторов угроз после процедуры определения согласованности мнения экспертов при условии $\gamma \le z$.

На основании экспертных оценок, представленных в виде матрицы идентификаторов угроз, потенциал нарушителя E_{ij}, определенный экспертом j, вычисляется как среднее арифметическое каждого столбца матрицы C_i для всех γ- матриц идентификаторов угроз.

$$E_{ij} = \frac{\sum_{\gamma=1}^{M} \widetilde{C}_{ij}}{M}, E_{ij} \in [0;1] \quad (2.2)$$

Обобщенная оценка потенциала нарушителя E_i. определяется выражением:

$$E_i = \frac{\sum_{\gamma=1}^{J} E_{i\gamma}}{J}, E_i \in [0;1]. \quad (2.3)$$

На заключительном шаге метода вычисляются средние значения потенциалов для каждого из k - уровней ОКИИ в соответствии с полученными для каждого уровня оценками потенциалов $E_i^k = \{E_i^1, E_i^2, E_i^3\}$, где $i = 1,...\gamma$.

Как указано в [46], выбранные и реализованные в ОКИИ в рамках его системы защиты, меры защиты информации, как минимум, должны обеспечивать нейтрализацию (блокирование) угроз БИ относительно потенциала нарушителя в соответствии с таблицей 2.1.

Таблица 2.1 — Требования по защите ОКИИ

Класс защищенности ОКИИ	**Потенциал нарушителя**
1	Высокий
2	Средний
3	Низкий

В рамках процесса моделирования угроз БИ определение численных показателей потенциалов нарушителей, не позволяет осуществить переход к выбору мер защиты ОКИИ на основании нормативно-методической документации в области БИ Российской Федерации ввиду определения потенциала в ней в вербальных величинах (низкий, средний, высокий потенциалы). Для согласования количественных оценок потенциала нарушителей с положениями нормативной документации предлагается провести корреляционный анализ между результатами, полученными по предлагаемой методике, и вербальными описаниями возможностей нарушителей, приведенными в таблице 2.2. Указанные вербальные характеристики были предложены в ходе апробации метода, в результате которой было установлено, что смещение шкалы оценок в сторону увеличения пороговых значений ведет к уменьшению количества потенциальных нарушителей и в расчетных условиях приводит к отсутствию потенциальных нарушителей как на отдельных уровнях

ОКИИ, так и объекта в целом. Указанные характеристики не противоречат и дополняют рассчитанные значения количественной оценки потенциалов нарушителей [36, 79, 121]

Таблица 2.2 — Корреляция характеристик потенциала

Диапазон значений *E*	**Вербальная характеристика потенциала нарушителя**
<0.1	недостаточный для реализации угрозы
0.1-0.3	Низкий
0.3-0.6	Средний
>0.6	Высокий

В рамках проведения ряда экспериментов по определению корректных соотношений численных и вербальных показателей было установлено, что в условиях опроса большого количества экспертов $j \geq 10$ и количества рассматриваемых угроз $m \geq 10$, численные показатели потенциалов отдельных нарушителей находятся в диапазоне от 0 до 0.1 ввиду согласованности мнения экспертов. В целях исключения указанных нарушителей из рассмотрения в модели угроз БИ предложено принимать их потенциал как недостаточный для реализации угроз БИ, что позволит повысить эффективность предложенного метода.

Таким образом, метод определения потенциала нарушителя БИ ОКИИ с использованием матрицы идентификаторов угроз позволяет провести групповую оценку действий потенциальных нарушителей, выявить, случайны или нет полученные оценки, а также осуществить обоснованный переход к выбору мер защиты информации на основании соотношений потенциала нарушителя и классов защищенности ОКИИ. Строгость оценки определяется корректностью применения метода, а случайность полученной оценки определяется в рамках вычисления коэффициента конкордации матриц идентификаторов угроз.

2.2 Метод количественной оценки опасности реализации угроз БИ потенциальным нарушителем БИ ОКИИ.

Потенциал злоумышленника характеризует объем ресурсов, которые он готов затратить на осуществление атаки на ОКИИ. Однако данный параметр не учитывает степень реальной опасности, которую представляют его действия для конкретного объекта). Уровень риска реализации угроз существенно различается для ИС, ИТКС и АСУ ТП, поскольку каждая из указанных систем обладает уникальными механизмами функционирования и различными комплексами защитных мер.

Для адекватной количественной оценки опасности реализации угроз БИ необходимо предложить метод, который бы интегрировал в расчеты технические спецификации ОКИИ, учитывал их иерархическое построение, а также позволял прогнозировать масштаб ущерба от возможного вывода из строя СЗИ в результате успешной реализации угроз БИ.

В основу разработанного метода положены нечеткие оценки защищенности ИС, предложенные в [47 - 49].

Пусть возможные комбинации угроз БИ для ОКИИ представлены множеством $H=\{h_1,h_2,h_3..h_i\}$, где $h_i \in H$ - совокупность угроз БИ, которая может быть реализована потенциальным нарушителем с некоторой вероятностью. Следовательно, можно говорить о множестве вероятностей $P=\{P_{h_1},P_{h_2},P_{h_3}...P_{h_\tau}\}$ и при этом справедливо равенство $\sum P_{h_\tau}=1$.

Величина ущерба от реализации угроз БИ представлена множеством $N_h=\{N_{h_1},N_{h_2},N_{h_3}...N_{h_\tau}\}$. При этом справедливо выражение: $0 \le N_{h_\tau} \le N_{\max}$. По отношению к ОКИИ могут быть реализованы наборы угроз множества $\widetilde{H}$ = { $\widetilde{H}_1=H_1 \vee H_3$, $\widetilde{H}_2=H_2 \vee H_4$, $\widetilde{H}_3=H_1 \vee H_2 \vee H_i \ldots \widetilde{H}_\tau$ } с вероятностями их

реализации $\widetilde{P} = \{\widetilde{P}_1, \widetilde{P}_2, \widetilde{P}_3 ... \widetilde{P}_\tau\}$ при выполнении условия $\sum_{i=1}^{\tau} \widetilde{P}_i = 1$. В таком случае суммарный ущерб от реализации наборов угроз будет определяться на основании выражения 2.4

$$\sum_{i=1}^{\tau} \widetilde{N}_i = N_{\max} = 1, \tag{2.4}$$

которое соответствует правилу 2.5

$$\widetilde{N}_i = \frac{N_i}{N_{\max}}. \tag{2.5}$$

Величина ущерба N_h не является постоянной величиной и отличается в зависимости от конкретных угроз из множества H, вероятности P возникновения указанных угроз БИ и выполняемых технологических процессов из множества $Q = \{q_1, q_2, q_3 .. q_m\}$ [50]. Тогда общую величину ущерба от реализации всех угроз потенциальным нарушителем можно представить в виде функции

$$N_\Sigma = f(H, P, Q). \tag{2.6}$$

Выражение 2.6 не учитывает особенности выполняемых технологических и (или) информационных процессов и многоуровневую структуру ОКИИ. Указанные особенности предложено определять в рамках вычисления ущерба $N_{h_i}(k,t)$ от реализации каждой из множества угроз в момент времени *t* при их выполнении на каждом из *k* - уровней ОКИИ в соответствии с функцией 2.7

$$N_\Sigma = f(H, P, N_{h_i}(k,t)). \tag{2.7}$$

Пусть количественная оценка опасности реализации угроз БИ $L(t)$ будет зависеть от суммарной величины ущерба N_Σ, наносимого объекту в результате реализации множества угроз H. Тогда вероятность, что угрозы БИ не будут реализованы в ОКИИ, может быть определена как степень защищённости системы в соответствии с выражением 2.8

$$\overline{P} = \prod_{i=1}^{\tau} (1 - P_{h_i}), 0 \le P_{h_i} \le 1. \quad (2.8)$$

В случае нанесения ущерба от реализации всех угроз N_{h_i} при условии $0 \le N_{h_i} \le N_{\max}$ ОКИИ понесет суммарный ущерб, взвешенный с учетом вероятности

$$N_{\Sigma} = \sum_{i=1}^{\tau} N_{h_i} P_{h_i}, 0 \le N_{\Sigma} \le N_{\max}. \quad (2.9)$$

Таким образом, выражение 2.9 определяет уровень потенциального ущерба в случае невозможности выполнения технологического процесса, а уровень максимального возможного ущерба определяется как $N_{\max} = \sum N_{h_i}$ при суммарной вероятности $\sum P_{h_\tau} = 1$.

Количественная оценка опасности реализации угроз БИ нарушителями заключается в определении суммарного ущерба от реализации каждой угрозы в отношении технологических и (или) информационных процессов ОКИИ. При этом суммарный ущерб определяется в условиях негативного воздействия на каждом из её уровней угрозообразующих факторов, таких как, критичность нарушения процесса и значимость выполняемых процессов для достижения целей эксплуатации ОКИИ, которые в наихудшем случае приводят к максимальному возможному ущербу.

В работе [47] автором предложено определять ущерб от реализации конкретного деструктивного действия $N_{h_i}(t) < 1$ без учета уровней ОКИИ на основе эвристических оценок пользователей системы в разные моменты времени. Указанный способ определения ущерба корректен для оценки реализации угроз БИ отдельных файлов в памяти ИС и ИТКС и не применим для АСУ ТП, поскольку не учитывает следующих важных особенностей автоматизации технологических процессов, критичности и значимости выполняемых технологических процессов.

В диссертации предложено вычислять ущерб $N_{h_i}(t)$ на основе оценок критичности технологического и (или) информационного процесса и уровня его значимости в соответствии с выражением 2.10. на каждом из уровней ОКИИ.

$$N_{h_i}(t) = \sum_{q=1}^{a} D_q R_{kq}(t), \tag{2.10}$$

где $R_{kq}(t)$ — оценка критичности нарушения технологического и (или) информационного процесса потенциальным нарушителем на каждом из k-уровней ОКИИ; D_q — оценка уровня значимости (вес) процесса для достижения целей эксплуатации ОКИИ.

Оценку критичности нарушения технологического и (или) информационного процесса предложено определять в соответствии с выражением 2.11, свойственным методике анализа видов и последствий потенциальных дефектов (Potential Failure Mode and Effects Analysis, FMEA) [51 - 52].

$$R_{kq}(t) = \prod_{n=1}^{3} O_{nq}(t), R_{kq}(t) \in [0;1]. \tag{2.11}$$

В подсистеме журналирования большинства современных SCADA – систем верхнего уровня АСУ ТП и промышленных файерволов ИС и ИТКС содержатся следующие значения необходимые для получения критичности нарушения процесса $R_{kq}(t)$:

- $O_{1q}(t)$ — вероятность нарушения процесса q, т.е. количество срабатывания типа «отказ в обслуживании» за рассматриваемый промежуток времени;

- $O_{2q}(t)$ — вероятность невыявления нарушения процесса q до его появления, т.е. узел был недоступен, однако причина отказа не была выявлена;

- $O_{3q}(t)$ — вероятность прекращения процесса q, т.е. общее количество итераций опроса оборудования, при которых за рассматриваемый промежуток времени узел ОКИИ в сети был недоступен.

Анализу значимости технологических и (или) информационных процессов посвящено множество исследований отечественных и зарубежных ученых, отражающих различные подходы к данной проблеме, однако большинство из них базируются на оценке качества выполняемого процесса [53 - 56].

Для оценки уровня значимости выполняемых технологических и (или) информационных процессов ОКИИ в диссертации предложено использовать вербально-числовую шкалу Харрингтона. В соответствии с [57] уровень значимости (вес) процессов необходимо оценивать по совокупности их свойств. Для данных целей использован безразмерный обобщенный показатель, учитывающий всю совокупность необходимых свойств. В качестве показателя для технологических и (или) информационных процессов принимается обобщенная функция Харрингтона D_q [58].

Назначение функции Харрингтона - установление соответствия между полученными значениями показателей свойств процессов и лингвистическими оценками значимости того или иного технологического и (или) информационного процесса, а соответственно и ОКИИ в целом.

Обобщенная функция значимости D_q для q процессов рассчитывается как среднее геометрическое частных функций значимости $d_{\mu q}$ на основании экспертных предположений о значимости каждого свойства в соответствии с выражением 2.12

$$D_q = \sqrt[s]{\prod_{\mu=1}^{s} d_{\mu q}^{v_{\mu q}}}, D_q \in [0;1], \qquad (2.12)$$

где s – количество свойств процессов согласно таблице 1.5 главы 1 диссертации; μ – номер свойства в ранжированной последовательности свойств $\mu = \{1,2,...,s\}$, $d_{\mu q}$ – частная функция значимости для свойства μ процесса q, $v_{\mu q}$ – весовой коэффициент значимости свойства μ процесса q. На основании функции Харрингтона с односторонним ограничением, математическая зависимость

численной оценки от показателя свойства процесса выражается следующей экспоненциальной функцией [59]:

$$d = \exp(-\exp(-y)), \tag{2.13}$$

где y — кодированное значение частного показателя, то есть его значение в условном масштабе.

Если задано одностороннее ограничение и используется функция 2.13 то значение y можно определить графически - путем построения номограммы, либо аналитически. В диссертации используется способ аналитического вычисления значения y, описанный в [60].

Модернизация функции Харрингтона для исследования технологических процессов начинается с упразднения отрицательного участка шкалы y [61]. При этом ее нулевое значение начинается числом 0,3 шкалы значимости d. Так же, как и в функции Харрингтона, значения оси y заканчиваются числом 4 без единиц измерения. Кривая значимости d для любого из q технологических процессов начинается с точки 0,3 функции и заканчивается значением, приближающимся к единице. Таким образом, благодаря модернизации, все рассчитываемые значения оценочных технологических процессов будут иметь только положительные значения и графическая зависимость 2.13 примет вид в соответствии с рис. 2.1.

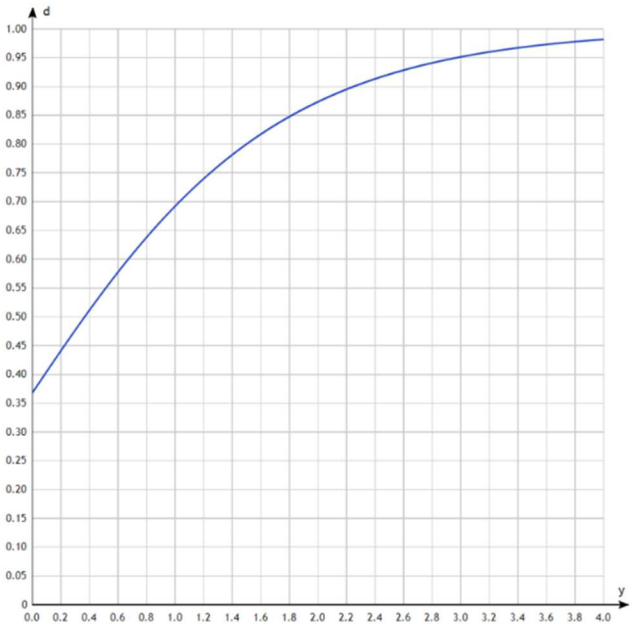


Рисунок 2.1 — Зависимость численной оценки от показателя свойства

Таким образом, в соответствии со шкалой Харрингтона значения односторонней функции $d_{\mu q}$ для процессов q изменяются в интервале от 0 до 1. Значение $d_{\mu q} = 1$ соответствует наиболее желаемой величине μ-го свойства.

Наиболее часто используемые границы градаций значимости (хорошо, плохо, очень плохо) не могут быть корректно применены для оценки технологических процессов. В диссертации предложены границы градаций на основании строгих интервальных диапазонов для каждой лингвистической оценки значимости свойства технологического процесса, в соответствии с таблицей 2.4. Численные значения градаций шкалы Харрингтона получены на основе анализа и обработки большого массива статистических экспертных данных [57].

Таблица 2.4 — Границы градаций значимости

Лингвистическая оценка	**Диапазон значений функции** $d_{\mu q} = \exp(-\exp(-y))$
Отсутствие свойства не затрагивает работу ОКИИ	$0{,}8 \le d_{\mu q} < 1$
Отсутствие свойства не приводит к остановке ОКИИ, но требует вмешательства администратора безопасности	$0{,}63 \le d_{\mu q} < 0{,}8$
Отсутствие свойства приводит к кратковременной остановке ОКИИ	$0{,}37 \le d_{\mu q} < 0{,}63$
Отсутствие свойства приводит к ОКИИ	$0{,}2 \le d_{\mu q} < 0{,}63$
Отсутствие свойства приводит к неконтролируемым последствиям для функционирования ОКИИ	$0 \le d_{\mu q} < 0{,}2$

На следующем этапе метода проводится процедура ранжирования ряда свойств процесса q в порядке возрастания суммы рангов.

Весовой коэффициент значимости свойства μ соответствует месту, которое свойство занимает в полученном ранжированном ряду на основании выражения 2.14

$$v_\mu = \frac{\mu}{2^{\mu-1}}. \qquad (2.14)$$

Чем выше коэффициент значимости свойства технологического и (или) информационного процесса для достижения целей эксплуатации ОКИИ, тем больший ущерб от его отсутствия будет нанесен системе в целом.

Графическая зависимость весового коэффициента значимости свойства процесса от положения в ранжируемом ряду представлена на рис. 2.2.

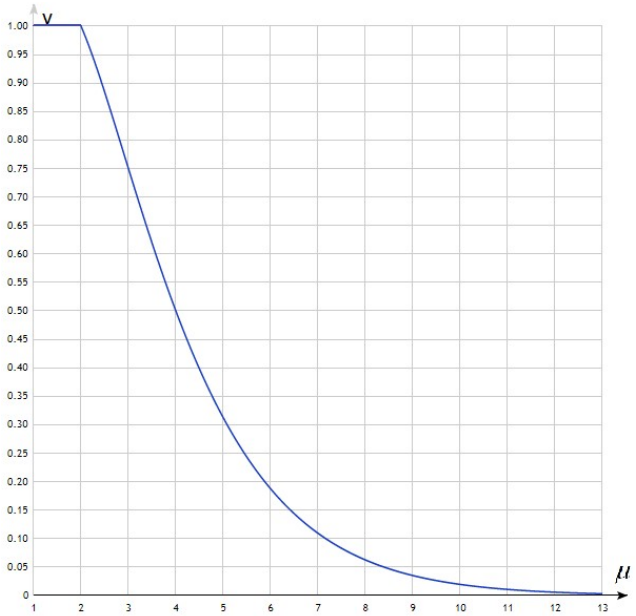


Рисунок 2.2 — Зависимость коэффициента значимости от положения в ранжируемом ряду

Таким образом, для определения обобщенной оценки значимости технологического процесса по формуле 2.14 необходимо все частные показатели свойств технологического процесса перевести в кодированные значения *y*. Далее необходимо вычислить частные функции значимости $d_{\mu s}$ на основании линейных и нелинейных преобразований, представленных в [57, 60].

Учитывая 2.11 и 2.12, выражение 2.9 для определения оценки опасности реализации угроз БИ принимает следующий вид

$$L(t) = \frac{\sum_{i=1}^{\tau}\left(\left[\prod_{n=1}^{3} O_{nq}(t)\right]\sqrt[s]{\prod_{\mu=1}^{s} d_{\mu q}^{v_{\mu q}}}\right)P_{h_i}}{N_{\max}}. \qquad (2.15)$$

Фактически экспертное мнение специалистов, участвующих в оценке опасности реализации угроз потенциальными нарушителями БИ ОКИИ, сводится к расстановке свойств технологических и (или) информационных процессов по степени их значимости для достижения целей эксплуатации объекта и не требует от опрашиваемых экспертов профильных знаний в области БИ. Используемый в диссертации лист экспертного ранжирования свойств процессов представлен в приложении 2.

Полученные значения оценки опасности реализации угроз БИ позволяют осуществить переход к определению экспертной оценки опасности реализации угроз, которые рассмотрены в п. 2.4 диссертации.

2.3 Метод оценки защищенности уязвимых звеньев ОКИИ на основании матрицы защищенности

Уязвимыми звеньями в ОКИИ выступают программные, аппаратные или программно-аппаратные средства, в отношении которых возможна реализация угроз БИ. В состав уязвимых звеньев также могут включаться СЗИ ввиду потенциальной угрозы их безопасности перед действиями нарушителей БИ.

Поскольку угрозы БИ могут быть реализованы потенциальными нарушителями в отношении не всех уязвимых звеньев, при осуществлении процесса моделирования угроз БИ важно определить фактические уязвимые звенья, характерные именно для рассматриваемого ОКИИ и их защищенность. Фактическими являются уязвимые звенья, в отношении которых имеется

информация о наличии в них актуальных уязвимостей - недостатков (слабостей) программного (программно-технического) средства или объекта в целом, которые могут быть использованы для реализации угроз БИ [62].

В диссертации предложено определять защищенность фактических уязвимых звеньев на основании применяемых в ОКИИ мер защиты из состава, представленного в документе [13].

Меры защиты - это действия, процедуры и механизмы, способные обеспечить безопасность от возникновения угрозы БИ, уменьшить уязвимость, ограничить воздействие инцидента в системе безопасности, обнаружить инциденты и облегчить восстановление уязвимых звеньев [63]. Эффективная безопасность обычно требует комбинации различных мер защиты для обеспечения заданных уровней безопасности при защите уязвимых звеньев. Например, механизмы контроля доступа, применяемые на ОКИИ, должны подкрепляться аудитом, определенным порядком действий персонала, его обучением, а также физической защитой. Часть мер защиты может быть обеспечена внешними условиями, свойствами уязвимого звена или может уже существовать в прикладном или системном ПО.

Пусть $G_k = \{g_{k1}, g_{k2}, g_{k3} \ldots g_{kn}\}$ – вектор, отражающий возможные уязвимые звенья n в ОКИИ при следующих условиях: $g_{ij} \in \{0,1\}$, $i = \overline{1,k}$, $j = \overline{1,n}$. Элемент g_{kn} может принимать следующие значения:

$g_{kn} = 0$ – отрицательный ответ для k – уровня ОКИИ,

$g_{kn} = 1$ – положительный ответ для k – уровня ОКИИ.

Значение элемента g_{kn}=0 говорит об отсутствии информации о конкретной уязвимости по результатам работы сканера безопасности или о согласованном экспертном мнении, об отсутствии необходимости включения уязвимого звена в перечень фактических для k – уровня. Значение элемента g_{kn}=1 – об обнаружении уязвимостей сканером безопасности или о согласованном экспертном мнении о необходимости включения уязвимого звена в перечень

фактических на k – уровне объекта. Уязвимость «выявлена» означает, что она известна специалисту, выполняющему процесс моделирования угроз БИ, и обнаружена с помощью сканера безопасности. Вектор G_k служит индикатором наличия уязвимых звеньев на всех уровнях рассматриваемой ОКИИ. Идентификация указанных уязвимостей может производиться как автоматизированными средствами (сканерами безопасности), так и путем экспертного анализа, проводимого экспертной группой.

Пусть вектор $A_k = \{a_{k1}, a_{k2}, a_{k3}...a_{km}\}$, отражающий применение мер защиты m в целях повышения защищенности уязвимого звена n на каждом из уровней ОКИИ, будет определяться как

$$\forall g_n \in G_{k,n} \exists A_{k,m}, \tag{2.16}$$

при следующих значениях элементов вектора $A_{k,m}$

$a_m = 0$ – отрицательный ответ для k – уровня,

$a_m = 1$ – положительный ответ для k – уровня.

Вектор $A_{k,m}$ характеризует применение той или иной меры защиты на рассматриваемом уровне ОКИИ. В зависимости от применяемых СЗИ значение элемента $a_m = 0$ указывает на отсутствие реализации рассматриваемой меры защиты, $a_m = 1$ – мера защиты реализована на рассматриваемом уровне объекта.

В качестве механизма определения применяемых мер защиты в ОКИИ может выступать экспертный метод, а также экспертные системы, реализующие инвентаризацию СЗИ. Используемая в диссертации опросная анкета экспертов представлена в приложении 3. Полный перечень мер защиты, реализуемых для ОКИИ различных категорий значимости и классов защищенности представлен в [13].

Произведение векторов $G_{k,n}$ и $A_{k,m}$ определяет матрицу защищенности уязвимого звена на каждом из k - уровней АСУ ТП

$$\mathbf{W} = G_{k,n} \cdot A_{k,m}. \quad (2.17)$$

Наличие фактического уязвимого звена и соответствующей ему уязвимости в условиях отсутствия соответствующей меры защиты указывает на низкую степень защищенности рассматриваемого уязвимого звена.

В соответствии с выражением 2.17 в случае реализации мер защиты для уязвимых звеньев, которые были исключены из перечня фактических, матрица защищенности **W** будет содержать оценки защищенности для уязвимых звеньев, которые не относятся к рассматриваемому уровню ОКИИ, а в отдельных случаях и объекта в целом. Для устранения указанного недостатка в диссертации предложено использовать вектор $I = \{1,1,1...m\}$, состоящий из единиц.

$$\mathbf{W}_k = G_{k,n} \cdot (I - A_{k,m})^T. \quad (2.18)$$

Каждый элемент матрицы указывает на наличие уязвимостей в системе защиты ОКИИ.

Для получения обобщенной оценки по всем уровням ОКИИ воспользуемся выражением 2.19 для определения среднего арифметического значения защищенности уязвимых звеньев

$$W = \frac{\sum_{k=1}^{k} \mathbf{W}_k}{k} = \frac{\sum_{k=1}^{k} G_{k,n} \cdot (I - A_{k,m})_T}{k}. \quad (2.19)$$

К преимуществам предложенного метода оценки защищенности уязвимых звеньев относится возможность уменьшения общего количества субъективных оценок экспертных групп за счет возможности использования результатов работы сканеров безопасности и открытых банков данных уязвимостей (БДУ). Метод позволяет комплексно подойти к обнаружению возможных путей атаки и систематизировать экспертные знания о недостатках действующих или внедряемых механизмов защиты. Она служит практическим инструментом для аудита защищенности объектов КИИ, полезным при формировании

специализированных моделей угроз для каждого из уровней ОКИИ, а также для автономных сегментов сетевой и информационной инфраструктуры.

2.4 Метод экспертной оценки опасности реализации угроз БИ ОКИИ с применением модели игры Штакельберга

Многие из существующих методов оценки актуальности и опасности реализации угроз БИ (ENISA, RMF, ISO 27005, РС БР ИББС-2.2) нацелены на качественный анализ ключевых факторов, которые непосредственно определяют уровень рисков. К подобным факторам, несомненно, относятся актуальные угрозы БИ ОКИИ [64 - 66]. В то же время большое количество отечественных научных работ посвящено оценке актуальности и опасности материализации угроз, базирующиеся на гипотезах о потенциальной мотивации, квалификации и ресурсной базе злоумышленников [67 - 70]. Вместе с тем, проанализированные методы не принимают во внимание указанные аспекты при определении уровня актуальности и критичности угроз, текущую защищенность объекта и не предусматривают использование оценок опасности реализации угроз БИ на каждом из уровней ОКИИ.

В разрабатываемом методе предложено использовать оценки опасности реализации угроз потенциальными нарушителями, обладающими оценками их потенциалов, как меру воздействия на каждый из уровней ОКИИ в случае отсутствия или несовершенства СЗИ. В таком случае мерой защиты информации можем считать оценку защищенности уязвимых звеньев ОКИИ, метод определения которой описан в п. 2.3 диссертации.

Поскольку заранее предугадать тактику и стратегию потенциального нарушителя не представляется возможным, задача обеспечения БИ ОКИИ рассматривается через призму теорий риска и принятия решений в условиях неопределённости. Данный подход признаёт, что в такой ситуации разработка

единственной оптимальной стратегии защиты, направленной против неизвестной угрозы ИБ, является невыполнимой.

В работе [72] оптимизация ресурсов информационной безопасности осуществляется с помощью теории игр. Важной для разрабатываемого метода оценки является предложенная в [72] концепция смешанной стратегии для распределения ресурсов СЗИ. Эффективность защиты, понимаемая как «выигрыш», напрямую зависит от вложенных средств: чем они выше, тем выше и уровень защищенности [73]. Для нарушителя эта зависимость инвертирована: увеличение ресурсов СЗИ уменьшает его потенциальный успех.

В диссертации используется вариант применения теории игр с несовершенной информацией. Нарушитель БИ имеет возможность выбирать стратегию нападения, получив некоторую информацию, поскольку имеет представление о СЗИ. Данная модель может описывать действия как внутреннего, так и внешнего нарушителей. СЗИ имеет преимущество в форме первого выбора своей стратегии, основанной на предположении о потенциале нарушителя и опасности реализации им угроз БИ. Ввиду вышеизложенного математический аппарат, свойственный играм с несовершенной информацией, более всего подходит для решения поставленной задачи экспертной оценки опасности реализации угроз БИ для ОКИИ.

Таким образом, предлагаемый метод основан на моделировании взаимодействия пары «злоумышленник – система защиты информации» в виде игры, основанной на модели Штакельберга [74].

В модели Штакельберга может возникать ситуация, когда один игрок обладает большей информацией о стратегии другого игрока. Это называется асимметричной или несовершенной информацией. Несовершенная информация возникает, когда нарушитель имеет больше информации о своем потенциале и оценках защищенности уязвимых звеньев, чем СЗИ.

Информация о степени защиты каждого из уровней ОКИИ, а также о выигрыше нарушителя и СЗИ ОКИИ для игры Штакельберга сформирована в

табличной форме. Коэффициенты выигрыша для нарушителя в игре выбираются в соответствии с его потенциалом E (п. 2.1 диссертации), а коэффициенты выигрыша для системы защиты информации в соответствии с оценкой защищенности фактических уязвимых звеньев W (п. 2.3 диссертации). Коэффициент выигрыша СЗИ в случае успешной реализации угрозы БИ характеризуется оценкой опасности реализации угроз БИ потенциальным нарушителем $L(t)$ (п. 2.2. диссертации). В качестве среднего возможного выигрыша принимается максимальная возможная величина ущерба от реализации угроз БИ $N_{\max}$.

Пусть для множества угроз H существуют оценки защищенности $W_{i,k}$ каждого из $к$ – уровней ОКИИ

$$\forall W_{i,k} \in H \exists B, 0 \le b_{i,k} \le 1, \tag{2.20}$$

при условии, что оценка $b_i \ge 0{,}5$ указывает на опасность (актуальность) i -й угрозы для рассматриваемого уровня ОКИИ.

Тогда функция определения актуальности угроз БИ ОКИИ будет иметь следующий вид

$$B = f(E, L, W, N). \tag{2.21}$$

В целях описания предложенного метода и построения сценария реализации актуальных угроз БИ воспользуемся коэффициентами выигрыша, представленными в таблице 2.5. Выигрыш нарушителя в случае реализации СЗИ равен 0, а максимально возможный ущерб $N_{\max}$ от реализации всех угроз потенциальным нарушителем $N_{\max} = 1$.

Таблица 2.5 — Игра Штакельберга для трехуровневого ОКИИ (АСУ ТП)

	Уровень 1		**Уровень 2**		**Уровень 3**	
	+	-	+	-	+	-
СЗИ	W_1 0,846	$L_1(t)$ 0,674	W_2 0,734	$L_2(t)$ 0,356	W_2 0,922	$L_3(t)$ 0,892
Н	0	E_1 0,736	0	E_2 0,583	0	E_3 0,467

Условные обозначения:

Уровень 1 – верхний уровень ОКИИ (АСУ ТП);

Уровень 2 – средний уровень ОКИИ (АСУ ТП);

Уровень 3 – нижний уровень ОКИИ (АСУ ТП);

СЗИ – система защиты информации; Н – нарушитель;

+ – АСУ ТП защищена;

- – АСУ ТП не защищена.

Для оценки приоритетности реализации использования стратегии защиты всех уровней ОКИИ и выигрыша СЗИ в таблице 2.6 представлена игра Штакельберга в стратегической форме [75].

Таблица 2.6 — Представление игры Штакельберга в стратегической форме

	СЗИ (Уровень 1)	**СЗИ (Уровень 2)**	**СЗИ (Уровень 3)**
Н (Уровень 1)	0,846 0	0,356 0,583	0,892 0,467
Н (Уровень 2)	0,674 0,736	0,734 0	0,892 0,467
Н (Уровень 3)	0,674 0,736	0,356 0,583	0,922 0

Для нахождения оценки приоритетности реализации использования стратегии защиты b_i и выигрыша n находятся решения (например, методом Гаусса) системы уравнений (2.22), полученной из стратегической формы игры.

$$\begin{cases} 0{,}846b_1 + 0{,}356b_2 + 0{,}892b_3 = 0{,}736 \\ 0{,}674b_1 + 0{,}734b_2 + 0{,}892b_3 = 0{,}583 \\ 0{,}674b_1 + 0{,}356b_2 + 0{,}922b_3 = 0{,}467 \end{cases} \quad (2.22)$$

получены следующие значения оценок: $b_1 = 0{,}16$, $b_2 = 0{,}07$, $b_3 = 0{,}93$, $n = N_{\max} P$. Рассчитанные значения указывают на то, что СЗИ, защищая верхний и средний уровни ОКИИ с оценками 16% и 7% соответственно, а нижний уровень с оценкой 94%, получит средний выигрыш, равный максимальной возможной величине

ущерба от реализации угроз БИ $N_{\max} = 1$ при условии - угроза актуальна, если $B \geq 0,5$. Т.е. наиболее вероятно появление угрозы БИ на нижнем уровне ОКИИ.

Таким образом, моделирование игры Штакельберга для нескольких уязвимых звеньев дает представление об опасности тех или иных угроз БИ для каждого уровня ОКИИ и позволяет определить, на каком уровне наиболее ожидаемо появление той или иной угрозы. Однако применение только игры с несовершенной информацией для оценки опасности реализации угроз не в полной мере учитывает условия эксплуатации ОКИИ.

В целях устранения вышеуказанного недостатка выделены основные предполагаемые условия эксплуатации ОКИИ, которые приводят к проведению успешной атаки нарушителем: S_1 – отсутствие протоколов шифрования при передаче информации; S_2 – нарушение целостности информации и управляющих сигналов; S_3 – отсутствие доступа к сервисам ОКИИ.

Каждое из условий S_i характеризуется теми или иными угрозами БИ и определяется на основании опроса специалистов в области физической и информационной безопасности. Классификация угроз БИ может быть проведена по множеству признаков, однако, как в зарубежных документах Harmonized Threat and Risk Assessment Methodology и CSE, так и в отечественном стандарте ГОСТ Р ИСО/МЭК 1335-1-2006 угрозы БИ принято разделять по природе возникновения. Основными угрозами БИ ОКИИ в соответствии с [76] являются:

– угрозы нарушения конфиденциальности – угрозы, при которых информация становится тем, кто не располагает полномочиями доступа к ней;

– угрозы нарушения целостности – угрозы, связанные с вероятностью модификации информации, хранящейся в ОКИИ;

– угрозы нарушения доступности - создание условий, при которых доступ к процессу или информации будет либо заблокирован, либо возможен за время, которое не обеспечит выполнение тех или иных шагов технологического и (или) информационного процесса ОКИИ.

Таким образом, угрозы БИ можно представить в виде функции 2.24

$$f(S_1, S_2, S_3). \quad (2.24)$$

На основе перечисленных условий и угроз, представленных в таблице 2.8, были определены потенциальные состояния ОКИИ. Эти состояния описываются конкретными комбинациями угроз БИ и формируют обобщенную абстрактную модель угроз. В рамках данного этапа моделирования также разрабатываются предложения, направленные на снижение потенциального ущерба от осуществления идентифицированных угроз БИ. Абстрактная модель угроз систематизирует перечень возможных угроз БИ и является так называемой базовой моделью угроз и соответствует описанию последствий реализации угроз БДУ ФСТЭК РФ, что позволяет реализовывать поэтапное исследование всех известных угроз БИ.

Таблица 2.7 — Абстрактная модель угроз безопасности ОКИИ

Состояние системы		**Угрозы**	**Рекомендации**
1.	$S_1 \& S_2 \& S_3$	К, Ц, Д	Внедрение СЗИ
2.	$\overline{S}_1 \& S_2 \& S_3$	Ц, Д	Настройка подсистемы контроля целостности
3.	$S_1 \& \overline{S}_2 \& S_3$	К, Д	Внедрение системы криптографической защиты (СКЗИ) и резервного копирования информации
4.	$S_1 \& S_2 \& \overline{S}_3$	К, Ц	Внедрение СКЗИ. Настройка подсистемы контроля целостности
5.	$S_1 \& \overline{S}_2 \& \overline{S}_3$	К	Внедрение СКЗИ
6.	$\overline{S}_1 \& S_2 \& \overline{S}_3$	Ц	Настройка подсистемы контроля целостности
7.	$\overline{S}_1 \& \overline{S}_2 \& S_3$	Д	Внедрение системы резервного копирования информации
8.	$\overline{S}_1 \& \overline{S}_2 \& \overline{S}_3$	-	Периодическое тестирование и модернизация СЗИ

На следующем шаге осуществляется переход к оценке опасности реализации угроз БИ на основе оценок уровня возможностей нарушителя БИ, что

обусловлено возможностью проведения атак на систему различными типами нарушителей. Описание уровней возможностей нарушителя подробно изложено на электронном ресурсе БДУ ФСТЭК РФ. Уровень возможностей нарушителя определяется набором предположений о нарушителе ИБ и может быть представлен в виде функции

$$f(X_1, X_2, X_3, X_4), \tag{2.25}$$

где X_1 - предположение о мотивации нарушителя; X_2 - предположение о наличии логического доступа в ОКИИ; X_3 - предположение о квалификации нарушителя; X_4 - предположение о знаниях нарушителя об объекте.

Для успешной реализации угроз ИБ необходимо, чтобы как минимум три атрибута нарушителя оценивались как истинные. Если же два или более предположений о его характеристиках оказываются ложными, его потенциал считается недостаточным для реализации угрозы.

Таблица 2.8 — Таблица истинности для функции потенциала нарушителя

Оцениваемые характеристики нарушителя				**Оценка уровня возможностей нарушителя**
X_1	X_2	X_3	X_4	$f(X_1, X_2, X_3, X_4)$
0	0	0	0	0
0	0	0	1	0
0	0	1	0	0
0	0	1	1	0
0	1	0	0	0
0	1	0	1	0
0	1	1	0	0
0	1	1	1	1
1	0	0	0	0
1	0	0	1	0
1	0	1	0	0
1	0	1	1	1
1	1	0	0	0
1	1	0	1	1
1	1	1	0	1
1	1	1	1	1

На основании таблицы 2.8 построена совершенная дизъюнктивная нормальная форма (СДНФ) оценки уровня возможностей ОКИИ.

$$f(X_1,X_2,X_3,X_4)=(\overline{X}_1\,\&\,X_2\,\&\,X_3\,\&\,X_4)\vee(X_1\,\&\,\overline{X}_2\,\&\,X_3\,\&\,X_4)\vee$$
$$\vee(X_1\,\&\,X_2\,\&\,\overline{X}_3\,\&\,X_4)\vee(X_1\,\&\,X_2\,\&\,X_3\,\&\,\overline{X}_4)\vee(X_1\,\&\,X_2\,\&\,X_3\,\&\,X_4). \quad (2.26)$$

Упростив запись функции потенциала нарушителя методом минимизации логических функций с использованием карт Карно [77,78], получим наборы верных предположений об уровне возможностей нарушителя

$$f(X_1,X_2,X_3,X_4)=(X_1\,\&\,X_2\,\&\,X_3)\vee(X_1\,\&\,X_2\,\&\,X_4)$$
$$\vee(X_1\,\&\,X_3\,\&\,X_4)\vee(X_2\,\&\,X_3\,\&\,X_4). \quad (2.27)$$

В качестве примера, учитывая уровень возможностей нарушителя БИ (2.27), в таблице 2.9 систематизирован перечень актуальных угроз БИ для ОКИИ. Перечень составлен для сценария, в котором угрозы нарушения целостности и доступности нейтрализованы за счет выполнения рекомендаций, изложенных в пунктах 6 и 7 таблицы 2.7.

Таблица 2.9 — Актуальные угрозы

Угрозы от внешних хакеров **(H1, H2, H3, H4, H5)**	Угрозы от неквалифицированных внутренних нарушителей **(H9, H11)**
$S_1\,\&\,S_2\,\&\,S_3\,\&\,X_1\,\&\,X_2\,\&\,X_3$	$S_1\,\&\,S_2\,\&\,S_3\,\&\,X_1\,\&\,X_2\,\&\,X_4$
$S_1\,\&\,\overline{S}_2\,\&\,S_3\,\&\,X_1\,\&\,X_2\,\&\,X_3$	$S_1\,\&\,\overline{S}_2\,\&\,S_3\,\&\,X_1\,\&\,X_2\,\&\,X_4$
$S_1\,\&\,S_2\,\&\,\overline{S}_3\,\&\,X_1\,\&\,X_2\,\&\,X_3$	$S_1\,\&\,S_2\,\&\,\overline{S}_3\,\&\,X_1\,\&\,X_2\,\&\,X_4$
$S_1\,\&\,\overline{S}_2\,\&\,\overline{S}_3\,\&\,X_1\,\&\,X_2\,\&\,X_3$	$S_1\,\&\,\overline{S}_2\,\&\,\overline{S}_3\,\&\,X_1\,\&\,X_2\,\&\,X_4$
Угрозы от внешних неквалифицированных нарушителей **(H6, H7, H8)**	Угрозы от внутренних нарушителей **(H10)**
$S_1\,\&\,S_2\,\&\,S_3\,\&\,X_2\,\&\,X_3\,\&\,X_4$	$S_1\,\&\,S_2\,\&\,S_3\,\&\,X_1\,\&\,X_3\,\&\,X_4$
$S_1\,\&\,\overline{S}_2\,\&\,S_3\,\&\,X_2\,\&\,X_3\,\&\,X_4$	$S_1\,\&\,\overline{S}_2\,\&\,S_3\,\&\,X_1\,\&\,X_3\,\&\,X_4$
$S_1\,\&\,S_2\,\&\,\overline{S}_3\,\&\,X_2\,\&\,X_3\,\&\,X_4$	$S_1\,\&\,S_2\,\&\,\overline{S}_3\,\&\,X_1\,\&\,X_3\,\&\,X_4$
$S_1\,\&\,\overline{S}_2\,\&\,\overline{S}_3\,\&\,X_2\,\&\,X_3\,\&\,X_4$	$S_1\,\&\,\overline{S}_2\,\&\,\overline{S}_3\,\&\,X_1\,\&\,X_3\,\&\,X_4$

В процессе формирования результирующей таблицы угроз БИ предложено проводить группирование актуальных угроз БИ, представленных в БДУ ФСТЭК РФ по типу нарушителей, указанных в таблице 1.1. и на основании оценок потенциалов нарушителей, полученных методом, предложенным в п. 2.1.

диссертации. Разработанный метод позволяет выделить наиболее подверженные угрозам БИ уровни ОКИИ, а также наборы актуальных угроз БИ, в том числе группировать угрозы по уровням ОКИИ и уровню возможностей нарушителей.

2.5 Выводы по второй главе

1. Предложен метод количественной оценки потенциалов нарушителей БИ ОКИИ, имеющий в своей основе сформированные в виде матриц идентификаторов угроз предположения о нарушителях БИ в соотношении со сложностью реализации угрозы и возможностью получения нарушителем доступа к объекту. Сформулирована и решена задача субъективности индивидуальной оценки потенциалов нарушителей.

2. Разработан и сформулирован метод оценки опасности реализации угроз БИ на каждом уровне ОКИИ на основании критичности и уровня значимости (веса) технологических процессов с использованием методики анализа видов и последствий потенциальных дефектов FMEA и функции Харрингтона, позволяющие минимизировать экспертное участие в оценке возможностей потенциального нарушителя при реализации угрозы БИ.

3. Предложен метод определения и оценки защищенности уязвимых звеньев ОКИИ. Метод ориентирован на многоуровневую архитектуру АСУ ТП, относящихся к ОКИИ, и основан на предположении о том, что наличие фактического уязвимого звена и соответствующей ему уязвимости в условиях отсутствия соответствующей защитной меры указывает на низкую степень защищенности рассматриваемого уязвимого звена.

4. Предложен метод экспертной оценки опасности реализации угроз БИ ОКИИ, основанный на применении результатов моделирования игры Штакельберга с различными коэффициентами выигрышей. Метод позволяет выделить наиболее подверженные угрозам БИ уровни объекта, а также наборы актуальных угроз БИ.

ГЛАВА 3. АЛГОРИТМИЧЕСКОЕ ОБЕСПЕЧЕНИЕ МОДЕЛИРОВАНИЯ УГРОЗ БИ ОКИИ

3.1 Формирование модели нарушителя на основе предположений о его потенциале и возможных последствиях реализации угроз БИ.

Общая идея предлагаемого алгоритма формирования модели нарушителя БИ ОКИИ заключается в формировании перечня (на основании общего описания внутренних и внешних нарушителей, используя методы формализации нечеткой информации,) потенциальных нарушителей БИ ОКИИ, в отношении которых экспертами выдвигаются предположения об их квалификации и мотивации. Затем на основании метода оценки потенциала нарушителей с использованием матриц идентификаторов угроз описанного в п. 2.1. диссертации для каждого нарушителя определяется его потенциал. Следующий шаг заключается в оценке опасности реализации угроз БИ потенциальным нарушителем с использованием оценок критичности и значимости технологических и (или) информационных процессов на каждом из уровней ОКИИ.

На основании оценок потенциалов возможных нарушителей и коэффициентов опасности реализации ими угроз БИ, используя оценки возможного и максимально возможного ущерба для ОКИИ и принимаемых организационных и технических мер защиты, формируется перечень потенциальных нарушителей.

Экспертное обоснование возможностей нарушителей, рассматриваемых в качестве потенциальных источников угроз ИБ ОКИИ, базируется на анализе их квалификации, мотивации и имеющихся ресурсов с учетом противодействия со стороны существующих организационных, технических и режимных защитных мер.

3.2 Алгоритм определения потенциала нарушителя БИ ОКИИ

Потенциал нарушителя - мера усилий, затрачиваемых нарушителем при реализации угроз БИ.

Анализ возможностей, мотивации и ресурсов злоумышленника осуществляется с использованием различных методик определения его потенциала, описанных в [79–80]. Данные подходы и методы позволяют более точно прогнозировать реальные угрозы БИ, поскольку предполагают структурированный подход к определению уровня опасности нарушителя, включая классификацию типов нарушителей (внутренние/внешние, уровень подготовки), анализ используемых ими уязвимостей и оценку вероятности успешной атаки.

При всей значимости рассмотренных подходов в них не рассматриваются аппаратные уязвимости, человеческий фактор и недостатки организационно-технических мер, которые часто эксплуатируются злоумышленниками. Также в них отмечается статичность анализа: динамически возникающие уязвимости или комбинированные атаки не учитываются при определении потенциала нарушителя. Рассмотренные подходы требуют значительных ресурсов для сбора данных о нарушителе, что затрудняет её использование в небольших организациях – субъектах КИИ. Предлагаемые оценки потенциала нарушителя слишком субъективны ввиду отсутствия четких метрик оценки и процедуры согласования оценок экспертов.

По результатам определения потенциала нарушителя ИБ в соответствии с [81 - 82] рассчитывается показатель «Вероятность реализации угрозы».

Вероятность реализации угрозы информационной безопасности — это количественная оценка возможности осуществления атаки на объект КИИ с учётом его структурно-функциональных свойств и специфики работы. Данный показатель рассчитывается как максимальная вероятность реализации угрозы

наиболее мощным нарушителем через критические уязвимости и определяется следующим образом:

$$R_j = \max_{i,j}(U_i * E_j), \tag{3.1}$$

где U_i – вероятность реализации уязвимости через i-е уязвимое звено; E_j – потенциал j-го нарушителя для реализации угрозы через рассматриваемую уязвимость. Данный потенциал определяется исходя из сформированных предположений о нарушителях в соотношении со сложностью реализации угрозы БИ и возможностью получения нарушителем доступа к ОКИИ.

Задача определения потенциала нарушителя применительно к ОКИИ сводится к нахождению потенциалов $E_k = \{E_{k1}, E_{k1}, ..., E_{kj}\}$ для каждого из $k = \overline{1,\gamma}$ уровней объекта [83].

Потенциал нарушителя классифицируется по трем уровням в зависимости от его ресурсной базы и технических возможностей:

– Высокий потенциал характерен для субъектов, обладающих ресурсами, сопоставимыми с крупным предприятием, корпорацией или государством. Они способны самостоятельно проводить фундаментальные исследования, разрабатывать и применять сложные инструменты для эксплуатации уязвимостей.

– Средний потенциал характерен организованным группам или отдельным организациям, которые могут создавать и задействовать специализированные средства для атак, но их масштабы и возможности ограничены.

– Низкий потенциал подразумевает, что нарушитель не имеет собственных мощностей для разработки вредоносного ПО и вынужден полагаться на приобретение и использование уже готовых эксплойтов и инструментов.

В диссертации предложено введение дополнительного уровня потенциала нарушителя – недостаточный для реализации угрозы. Данный уровень потенциала применим к нарушителям, которые обладают одним из признаков низкого потенциала.

Блок-схема предлагаемого алгоритма решения поставленной задачи представлена на рис. 3.1. Предложенный алгоритм основан на методе, описанном в п. 2.1 диссертации.

Соответствие принадлежности оцениваемых характеристик рассматриваемы потенциальным нарушителям определяется на основе экспертного метода путем заполнения опросных листов, приведенных в приложении 1 диссертации.

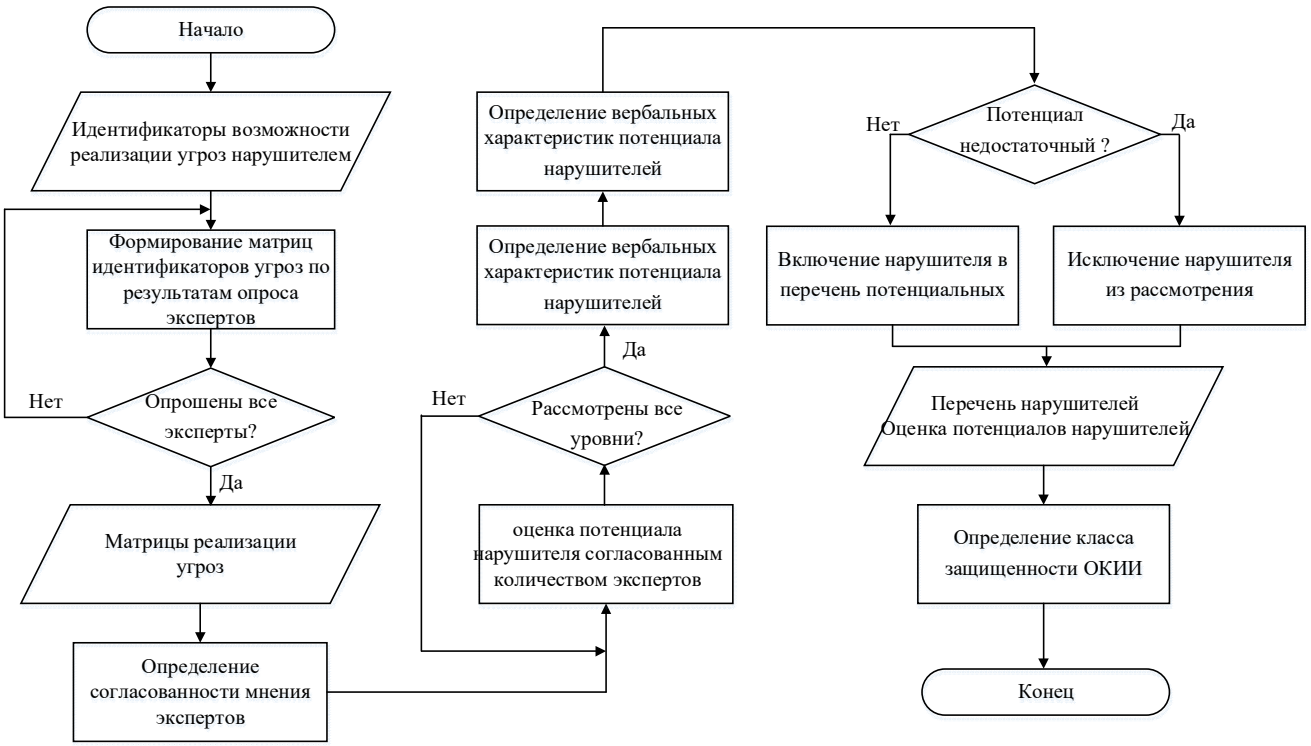


Рис. 3.1 Алгоритм определения потенциала нарушителя БИ ОКИИ

Этап формирования матрицы идентификаторов угроз необходим для осуществления комплексного экспертного подхода к оценке опасности реализации угроз БИ для рассматриваемых нарушителей. Матрицы идентификаторов угроз формируются по результатам опроса каждого конкретного эксперта, позволяя перейти к групповому оцениванию потенциалов нарушителей в соответствии с методом, описанным в п. 2.1 диссертации.

Разработанный алгоритм может иметь значительную практическую ценность для специалистов в области БИ, поскольку использование матрицы защищенности позволяет минимизировать субъективность при анализе уязвимостей, что способствует более точному выявлению слабых мест. Алгоритм

систематизирует процесс оценки, упрощая идентификацию угроз БИ. На основе полученных данных о потенциальных нарушителях специалисты смогут целенаправленно распределять ресурсы для усиления наиболее уязвимых звеньев ОКИИ. Алгоритм может быть интегрирован в действующие системы управления информационной безопасностью, дополняя такие фреймворки, как NIST CSF, ГОСТ Р ИСО/МЭК 27ххх, «Методика ФСТЭК России от 05.02.2021г.

Таким образом, разработанный метод вносит вклад в повышение устойчивости КИИ и может быть полезен как для аудиторов, так и для специалистов по БИ, отвечающих за защиту критически важных объектов.

3.3 Алгоритм построения модели угроз БИ ОКИИ

В соответствии с [20] наличие источника угрозы и уязвимого звена, которое может быть использовано для реализации угрозы, свидетельствует о ее наличии. В соответствии с данным определением механизм обнаружения уязвимых звеньев необходим для идентификации всех принципиально реализуемых в ОКИИ угроз БИ.

Понятие уязвимое звено тесно связано с определением уязвимостей для ОКИИ. Уязвимостью называют свойство ИС, ИТКС или АСУ ТП, обуславливающее возможность реализации угроз БИ [84]. Таким образом, имеется высокая положительная корреляция между уязвимостями и уязвимыми звеньями, поскольку возникновение тех или иных уязвимостей в ОКИИ приводит к появлению соответствующих уязвимых звеньев в объекте.

Методы определения уязвимых звеньев можно разделить на 3 группы: экспертные, сетевое сканирование и комбинированные. К экспертным методам относится метод диаграмм потоков информации [85], который для представления полученных уязвимых звеньев использует деревья атак. Наиболее распространенный экспертный метод определения уязвимых звеньев заключается в использовании доступных источников информации для поиска сведений об

уязвимостях и их дальнейшей оценке группой профильных специалистов на предмет соответствия уязвимым звеньям рассматриваемой системы [86-87]. В качестве открытых источников информации об уязвимостях, соответствующих рассматриваемым уязвимым звеньям ОКИИ, используются следующие источники: БДУ ФСТЭК, база данных уязвимостей CVE Details, базы MITRE ATT&CK и CAPEC [88 - 91]. В качестве основного источника угроз БИ в диссертации использована БДУ ФСТЭК.

БДУ ФСТЭК включает в себя базу данных уязвимостей ПО и описание угроз БИ, характерных, в первую очередь, для ИС, ИТКС и АСУ ТП [92].

Сетевое сканирование является техническим методом определения уязвимых звеньев ОКИИ и связано, в первую очередь, с применением аппаратно-программных комплексов – сканеров безопасности. Исследованиям в области сканирования уязвимостей уделено большое внимание со стороны научного сообщества [93 - 97].

К наиболее известным сканерам безопасности на российском рынке относятся XSpider, MaxPatrol, RedCheck, Сканер-ВС и Ревизор сети 3.0. Алгоритм работы сканеров безопасности, основанный на функциональных характеристиках отмеченного выше программного обеспечения, приведен на рис. 3.2.

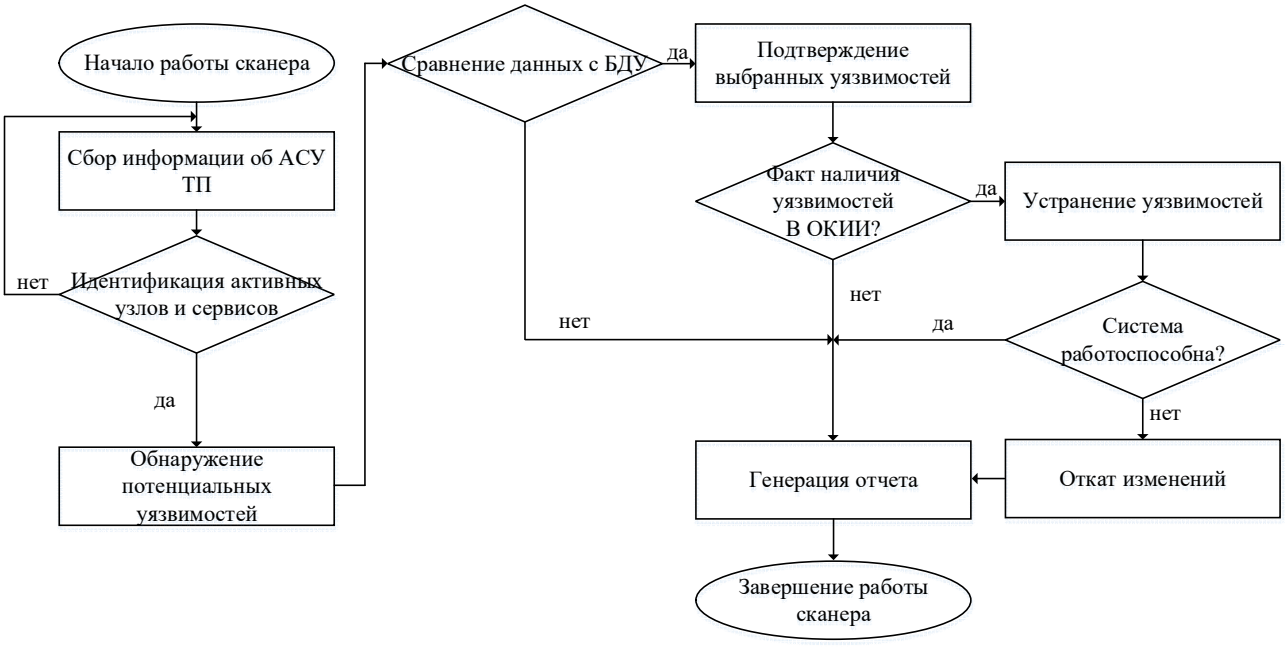


Рисунок 3.2 —Алгоритм работы сканера безопасности

Принятие обоснованных решений по оценке защищенности уязвимых звеньев зависит от реализованных мер защиты информации в ОКИИ и обеспечивается в процессе детального анализа подсистем БИ, применяемых СЗИ, условий функционирования каждого из уровней ОКИИ и использования уязвимых звеньев на каждом из уровней. Поэтому определение условий эксплуатации уязвимых звеньев является важной задачей при разработке метода определения и оценки защищенности уязвимых звеньев ОКИИ, алгоритм которого представлен на рис. 3.3.

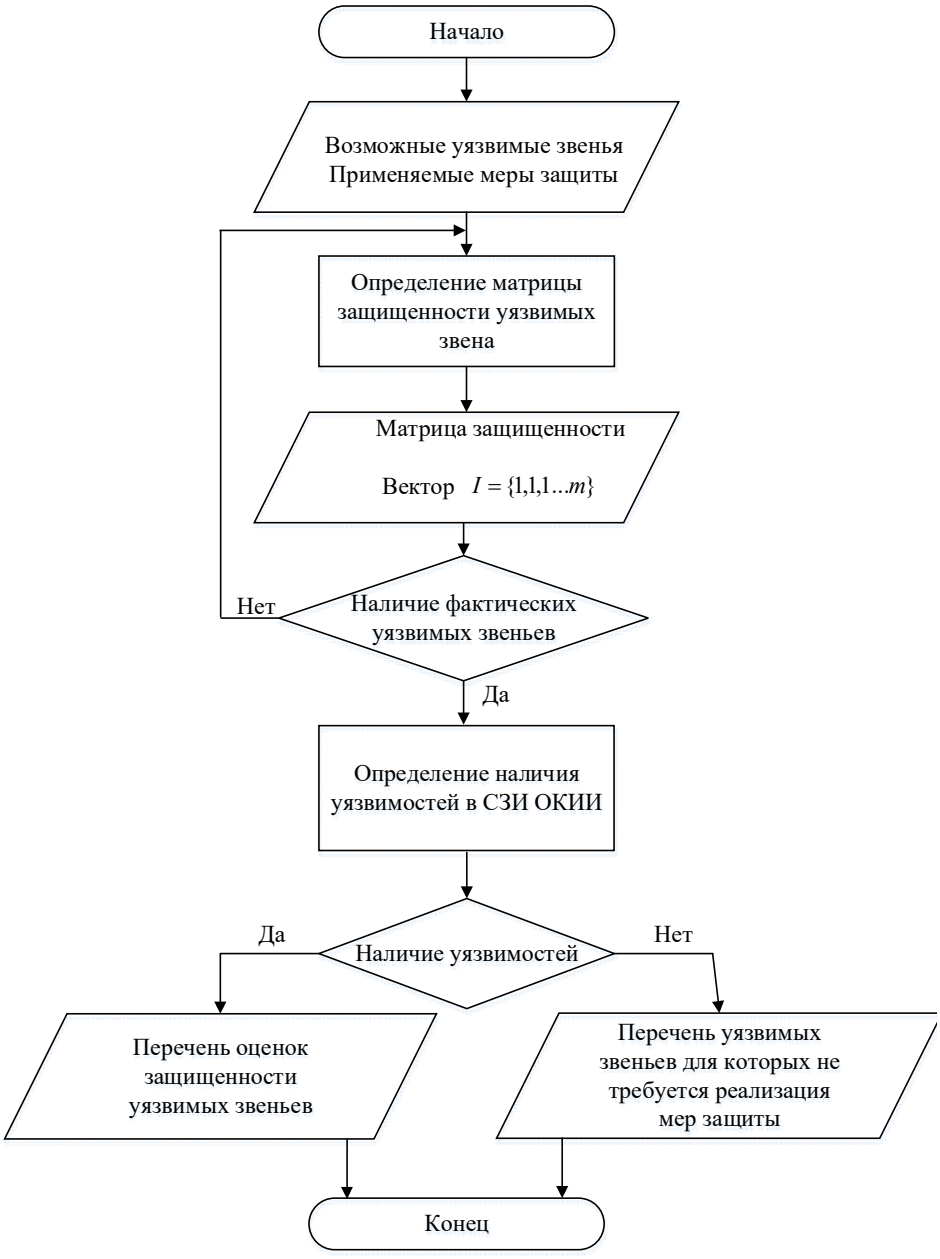


Рисунок 3.3 — Алгоритм определения и оценки защищенности уязвимых звеньев

При определении фактических уязвимых звеньев может проводиться экспертный анализ ОКИИ путем анкетирования ответственных сотрудников или специалистов в предметной области, а также сканирование объекта на предмет наличия уязвимостей.

Все возможные угрозы БИ ОКИИ реализуются потенциальными нарушителями в отношении тех или иных уязвимых звеньев. При построении оценки опасности реализации угроз БИ из всех возможных уязвимых звеньев важно выявить именно те, которые могут быть использованы для реализации угрозы, и применить в отношении них соответствующие защитные меры. Таким образом, используя описанные в главах 2 и 3 методы и алгоритмы, был предложен метод экспертной оценки степени опасности реализации угроз БИ ОКИИ, блок-схема которого представлена на рис. 3.4.

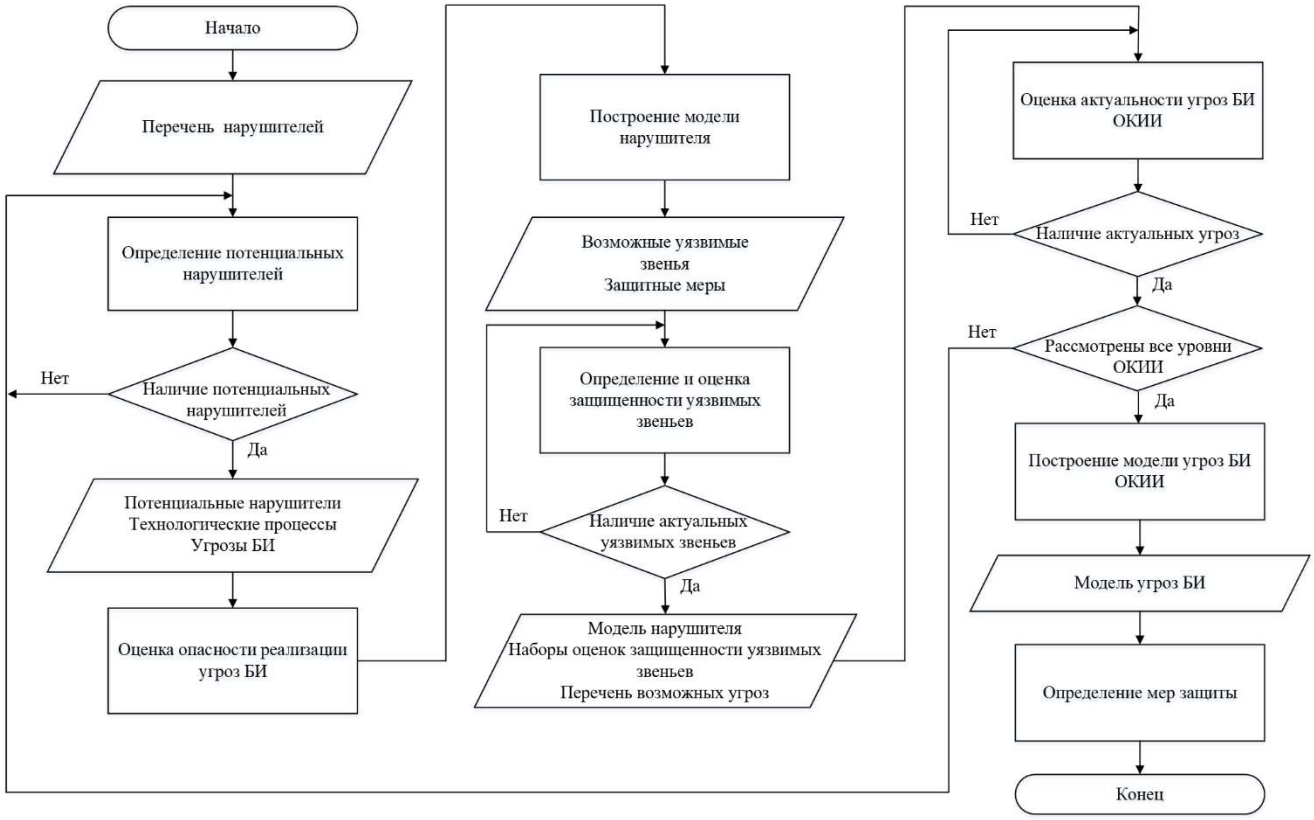


Рисунок 3.4 — Алгоритм экспертной оценки степени опасности реализации угроз БИ ОКИИ

Предложенный в диссертации метод определения и оценки защищенности уязвимых звеньев ОКИИ относится к типу комбинированных методов и заключается в выявлении слабых мест рассматриваемого ОКИИ в контексте потенциальных уязвимостей объекта и вероятности реализации уязвимостей через уязвимые звенья. Комбинированные методы определения уязвимых звеньев сочетают в себе особенности экспертных методов и методов сетевого сканирования.

Предложенный алгоритм отличается от рассмотренных в главе 1 наличием оценок опасности реализации угроз БИ для каждого из уязвимых звеньев на каждом из уровней ОКИИ каждым из потенциальных нарушителей режима БИ, в то время как алгоритмы TRIKE и ФСТЭК РФ имеют в своей основе риск-ориентированный подход при оценке опасности реализации угроз БИ и не подразумевают рассмотрение каждого уровня ОКИИ в отдельности.

3.3.1 Постановка задачи выбора мер защиты

Важную роль в построении адекватной модели угроз БИ ОКИИ играет выбор мер защиты, применяемых на каждом уровне ОКИИ. Согласно [98], защита информации — это реализация правовых, организационных и технических мер для: защиты данных от уничтожения, изменения, блокировки, копирования, неправомерного предоставления и распространения; обеспечения конфиденциальности; соблюдения законного права на доступ к информации.

Согласно ФСТЭК России [45], система защиты информации в ОКИИ формируется на основе применения базового набора мер, которые структурированы по трём ключевым направлениям: правовому, организационному и техническому. Определение базового набора мер защиты основывается на категории значимости и классе защищенности ОКИИ. Вопросы определения класса защищенности ОКИИ на основании потенциала нарушителя БИ рассмотрены в п. 2.1 диссертации.

В целях упрощения алгоритмизации и автоматизации предложенных в диссертации методов разработана и отражена на рисунках 3.5. и 3.6 схема

базовых наборов мер защиты. Принимая во внимание многоуровневую структуру АСУ ТП, относящихся к ОКИИ, а также учитывая наличие возможных нарушителей БИ с отличающимся потенциалом на разных уровнях, целесообразно осуществлять принятие решения о выборе мер защиты информации индивидуально на каждом уровне системы. Разработанная схема базовых мер защиты позволит визуализировать меры защиты, предлагаемые для реализации по результатам выполнения процесса моделирования угроз БИ ОКИИ на каждом из уровней объекта.

Использование теоретико-множественных методов при решении задач ИБ, включая обоснование выбора защитных мер, детально исследовано в [99–103]. Основными преимуществами данных методов, обуславливающими их популярность, являются: способность к аппроксимации качественных показателей, работа с нечёткими входными данными и лингвистическими критериями, а также высокая скорость моделирования сложных динамических систем с возможностью их сравнения с требуемой точностью.

Пусть A – конечное множество мер защиты информации, определенных в [46] $A = \{ИАФ.0; ИАФ.1; .....; ИПО.4\}$.

Принимая во внимание разделение мер защиты на базовые наборы в соответствии с определяемым классом защищенности ОКИИ, представим базовые наборы в виде подмножеств множества A следующим образом:

B_{k_1} – конечное подмножество, включающее в свой состав базовый набор мер, предписанный классу защищенности К3 ($B_{k_1} \subset A$); B_{k_2} – предписанный классу защищенности К2 ($B_{k_2} \subset A$); B_{k_3} – классу защищенности К1 ($B_{k_3} \subset A$).

В диссертации рассмотрена модель [104], где уровням ОКИИ соответствуют различные классы защищенности. Меры защиты в данной модели могут быть либо универсальными (общими для всех классов), либо специфичными (применимыми только к определенным базовым наборам мер конкретных классов).

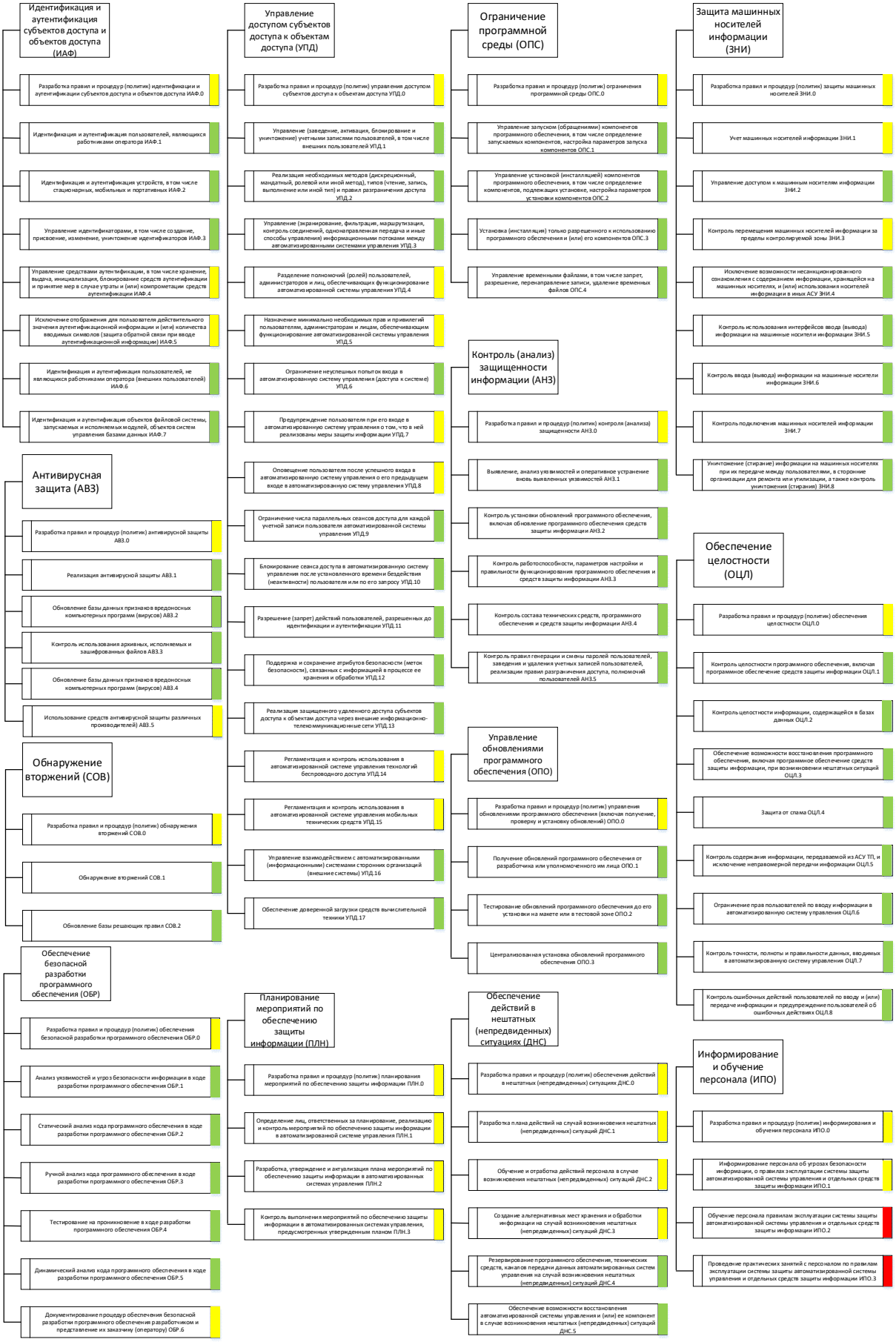


Рисунок 3.5 — Схема базовых наборов мер защиты ОКИИ

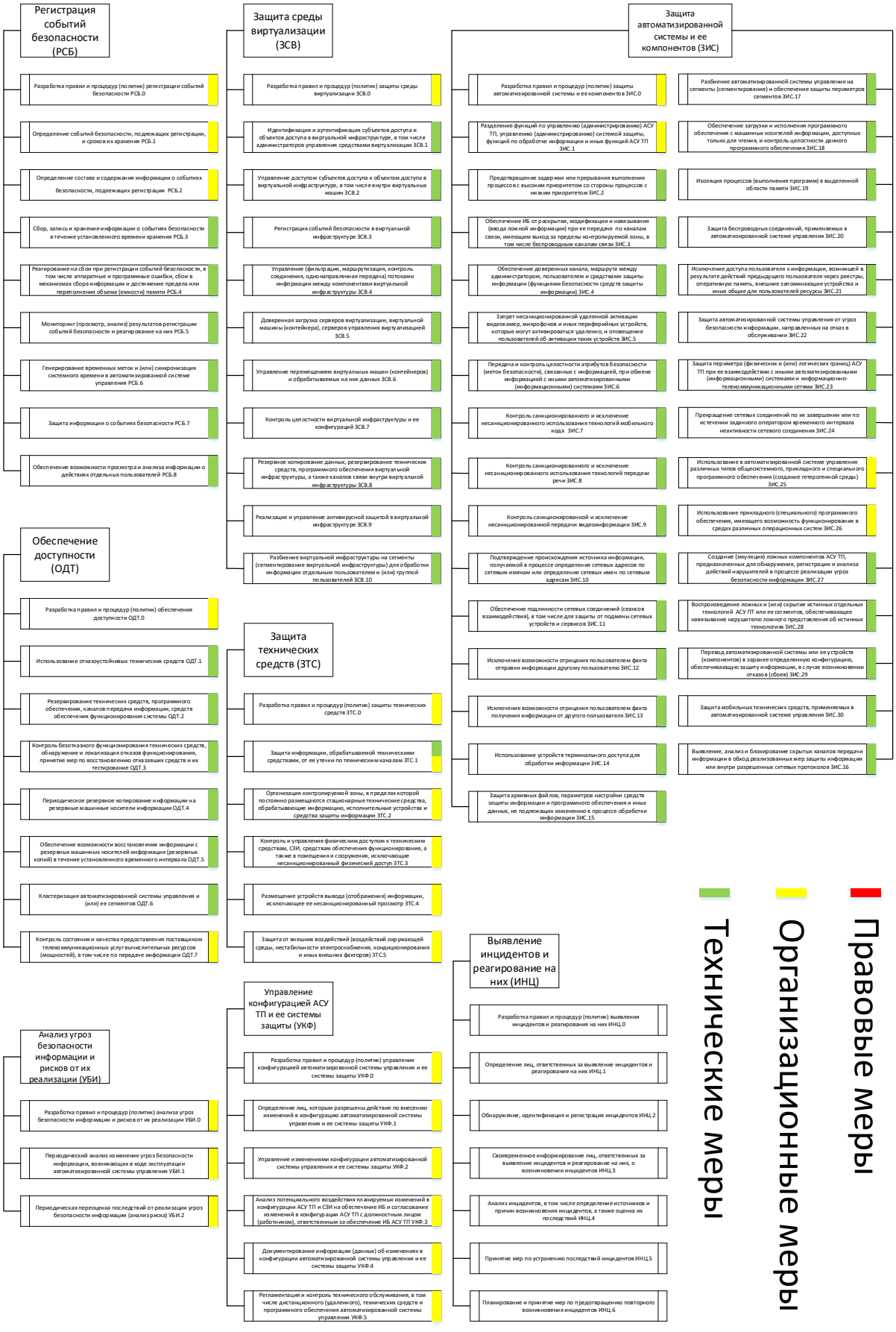


Рисунок 3.6 — Схема базовых наборов мер защиты ОКИИ

3.3.2 Минимальный набор мер защиты

В поставленной задаче минимальному набору мер защиты (МН) для всех уровней ОКИИ будет соответствовать пересечение рассматриваемых множеств

$$B_{k_1} \cap B_{k_2} \cap B_{k_3} = \{x \mid x \in B_{k_1} \,\&\, x \in B_{k_2} \,\&\, x \in B_{k_3}\}. \quad (3.1)$$

Анализируя выражение (3.1), можно сделать следующий вывод: в МН принимается решение о включении только тех мер, которые необходимы для применения на каждом уровне ОКИИ. Если та или иная мера не применяется в любом из уровней системы, то она исключается из рассмотрения.

Внедрение МН сопряжено с незначительными техническими и финансовыми затратами. Однако его эффективность для обеспечения информационной безопасности ограничена, поскольку он не учитывает необходимость применения специализированных мер защиты для различных уровней ОКИИ.

3.3.3 Базовый набор мер защиты

Для устранения выявленных недостатков был сформирован базовый набор защитных мер (БН), универсальный для всех уровней ОКИИ. В его состав вошли меры, являющиеся обязательными как минимум для двух уровней системы.

$$(B_{k_1} \cap B_{k_2}) \cup (B_{k_2} \cap B_{k_3}) \cup (B_{k_1} \cap B_{k_3}) = \{x \mid x \in B_{k_1} \,\&\, x \in B_{k_2}\} \cup \{x \mid x \in B_k$$

$$\cup \{x \mid x \in B_{k_1} \,\&\, x \in B_{k_3}\} = \begin{vmatrix} x \in B_{k_1} = k_1 \\ x \in B_{k_2} = k_2 \\ x \in B_{k_3} = k_3 \end{vmatrix} = (k_1 \,\&\, k_3) \cup k_2) \cup (k_1 \,\&\, k_3) \quad (3.2)$$

Использование БН является оптимальным вариантом организации СЗИ. Однако практики применения мер исключительно из БН не учитывают структурно-функциональных характеристик, особенностей функционирования и внедряемых информационных технологий ОКИИ.

3.3.4 Адаптированный базовый набор мер защиты

Для исключения нарушений в работе создаваемой СЗИ введено выражение (3.3), определяющее состав адаптированного базового набора защитных мер

(АБН). Данное выражение позволяет оптимизировать выбор мер безопасности и гарантировать устойчивое функционирование СЗИ.

$$(B_{k_1} \cup B_{k_2} \cup B_{k_3}) \setminus (B_{k_1} \cap B_{k_2}) \cup (B_{k_2} \cap B_{k_3}) \cup (B_{k_1} \cap B_{k_3}) \quad (3.3)$$

АБН представляет собой комплекс ответных мер СЗИ, обеспечивающих её адаптацию к изменяющимся условиям внешней среды, модификациям структуры и функционала ОКИИ, а также достижение целевых показателей его функционирования.

Использование АБН позволяет изменить изначально выбранный БН в части его максимальной адаптации применительно к структуре, реализации и особенностям эксплуатации ОКИИ. При адаптации БН учитываются требования по БИ, изложенные в документе [13] и ассоциированные с категорией значимости ОКИИ, определяемой по результатам процедуры категорирования ОКИИ. Главной проблемой реализации АБН является отсутствие сопоставления защитных мер с актуальными угрозами БИ.

3.3.5 Уточнение адаптированного базового набора мер защиты

Для решения обозначенной проблемы предлагается уточнение адаптированного базового набора мер защиты (УАБН). Данная процедура осуществляется на основе оценки способности текущего АБН адекватно противостоять всем актуальным угрозам БИ, характерным для ОКИИ, либо снижать уровень риска их реализации с учетом конкретных условий его функционирования. Уточнение АБН осуществляется с учетом не выбранных ранее мер из множества A и определяется выражением (3.4) для УАБН.

$$A \setminus B_{k_1} \cup B_{k_2} \cup B_{k_3} = \{x \mid x \in A \,\&\, x \notin B_{k_1} \,\&\, x \notin B_{k_2} \,\&\, x \notin B_{k_3}\} \quad (3.4)$$

УАБН является наиболее приближенным к максимальному перечню возможных мер БИ, однако в соответствии с [105] не отражает правовых мер защиты информации ввиду несогласованности с требованиями организационно- и нормативно-методической документации в области БИ. В качестве устранения данной несогласованности выполняется дополнение УАБН. На данном этапе, набор УАБН дополняется мерами, обеспечивающими выполнение требований БИ,

установленными локальными правовыми актами, национальными стандартами, организационно-распорядительной документацией субъекта КИИ в области защиты информации и будет соответствовать выражению для УАБН.

3.3.6 Получение обобщенных показателей класса защищенности ОКИИ

На основании выделенных множеств базовых наборов мер для классов защищенности ОКИИ рассмотрено четыре перечня наборов мер МН, БН, АБН и УАБН. Графическое отображение пересечения множеств наборов мер представлено на рис. 3.7 в виде диаграмм Эйлера-Венна.

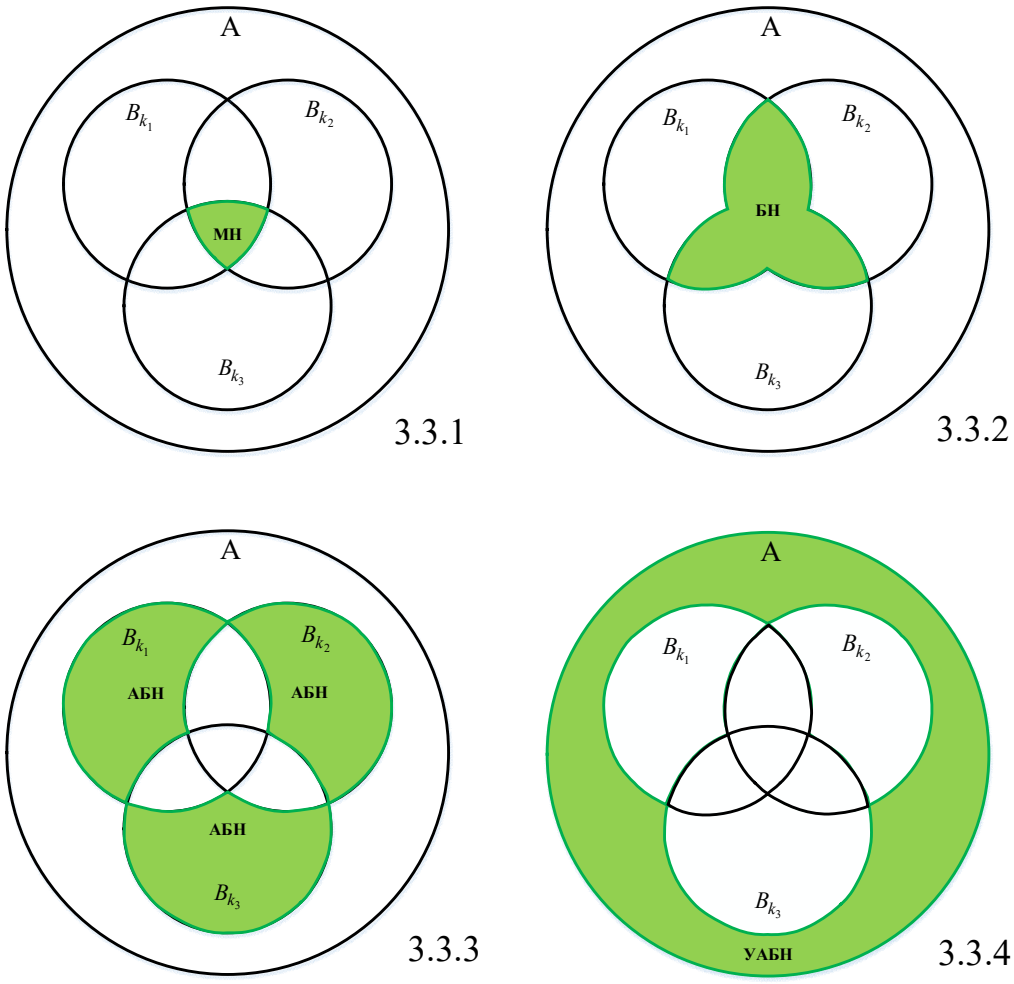


Рисунок 3.7 — Диаграммы пересечения множеств наборов мер

В соответствии с [106] обозначение кругов, соответствующих каждому подмножеству из множества мер защиты, возможно в любом порядке. В случае совпадения классов защищенности для двух отдельных уровней ОКИИ задача выбора мер защиты сводится к определению отношений двух множеств.

На основании полученных показателей класса защищенности может осуществляться переход к выбору конкретных мероприятий по БИ ОКИИ и выбору СЗИ, удовлетворяющих требованиям к классу защищенности на каждом уровне ОКИИ в соответствии с документами [13, 46].

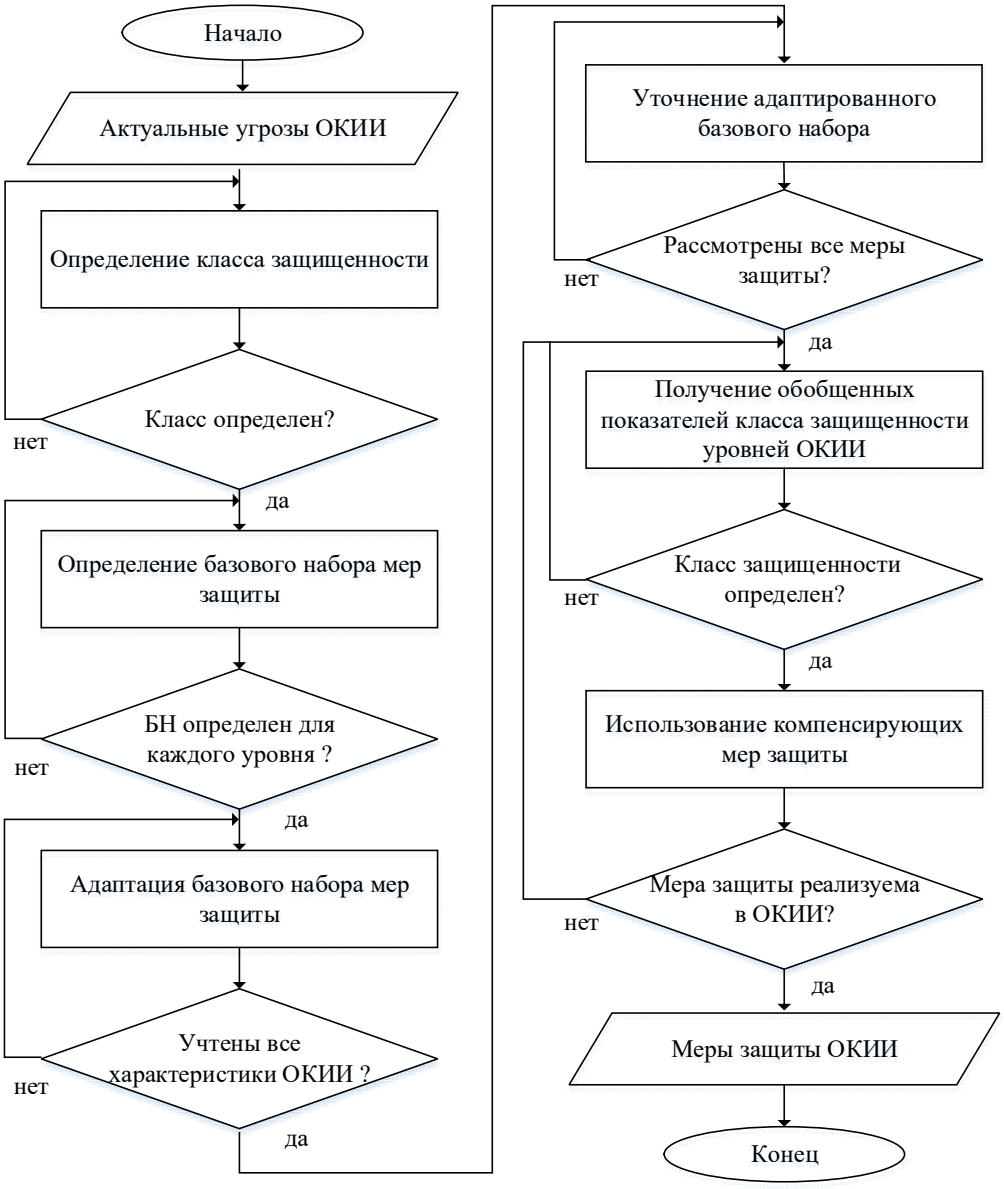


Рисунок 3.8 — Алгоритм выбора мер защиты ОКИИ

На рис. 3.8 представлен алгоритм выбора мер защиты ОКИИ, разработанный в соответствии с положениями п. 3.3.2 – 3.3.6.

На основании сформулированных п. 1.4 предположений о нарушителях ИБ, корреляционных зависимостей потенциалов нарушителей ИБ, представленных в п. 3.1, а также БН ограничений и принимаемых организационных и технических

мер определяются соотношения между потенциалами нарушителей и БН. В качестве примера данные соотношения приведены в таблице 3.1.

Таблица 3.1 — Соотношения между потенциалами нарушителей и БН

Потенциал	**Нарушитель**		**Уровень ОКИИ**	**Класс защищённости ОКИИ**
	Внутренний	**Внешний**		
недостаточный для реализации угрозы	(Н6) (Н8)	(Н9)	нижний	не предъявляется требований к защищенности
	Нет потенциальных нарушителей	-	средний	
	Нет потенциальных нарушителей	-	верхний	
низкий	(Н1) (Н2) (Н3) (Н4) (Н5) (Н7)	(Н10)	нижний	К3
	(Н5) (Н6) (Н7) (Н8)	(Н9) (Н10)	средний	
	(Н3) (Н4) (Н7) (Н8)	(Н10)	верхний	
средний	Нет потенциальных нарушителей	Нет потенциальных нарушителей	нижний	К2
	Нет потенциальных нарушителей	Нет потенциальных нарушителей	средний	
	(Н5)	(Н9)	верхний	
высокий	Нет потенциальных нарушителей	Нет потенциальных нарушителей	нижний	К1
	(Н1) (Н2) (Н3) (Н4)	Нет потенциальных нарушителей	средний	
	(Н1) (Н2) (Н6)	Нет потенциальных нарушителей	верхний	

На основании проведенного анализа соотношений из таблицы 3.1 можно сделать вывод об исключении из БН мер защиты, направленных на противодействие нарушителям 6,8,9, что имеет прямое отражение на диаграмме Эйлера-Венна 3.4.2.

В качестве дополнительного эксперимента проведена адаптация БН. Адаптация проведена на основании включения или исключения мер защиты в зависимости от их необходимости на том или ином уровне ОКИИ, в целях

противодействия рассматриваемым нарушителям ИБ. Переход от БН к АБН отражен в таблице 3.2.

Таблица 3.2 — Результаты адаптации БН ОКИИ (АСУ ТП)

Уровень АСУ ТП	**Нарушители**										**ОКЗ**
	Н1	Н2	Н3	Н4	Н5	Н6	Н7	Н8	Н9	Н10	
нижний	КЗ	КЗ	КЗ	КЗ	КЗ	КЗ	КЗ	КЗ	КЗ	х	КЗ
средний	К1	К1	К1	К1	К2	К2	К2	К2	К2	х	К1
верхний	К1	К1	К3	К3	К2	К1	К3	К3	К2	х	К1

По результатам эксперимента наблюдается отсутствие необходимости дополнения мер защиты при адаптации БН верхнего уровня ОКИИ. На среднем уровне системы адаптация БН необходима по мерам защиты от деструктивных действий нарушителей 5,6,7,8,9. Нижний уровень требует адаптации мер защиты по нарушителям 6,8 и 9. Общим для всех уровней ОКИИ является необходимость исключения из рассмотрения мер защиты, связанных с нарушителем 10 на основании его потенциала для реализации угрозы на всех уровнях ОКИИ. Принимая во внимание выражение 3.3 и графическое отражение 3.3.3, получены обобщенные показатели класса защищенности ОКИИ (ОКЗ в таблице 3.2) на каждом уровне ОКИИ, в соответствии с которыми осуществляется переход к выбору СЗИ, удовлетворяющим требованиям к классу защищенности на каждом уровне ОКИИ.

Разработанные модель и алгоритм выбора мер защиты ОКИИ позволяют вывести дефиницию «адаптация базового набора мер защиты ОКИИ»: адаптацией базового набора мер защиты ОКИИ называется процесс изменения изначально выбранных наборов мер защиты на всех уровнях ОКИИ в части их максимальной оптимизации с учетом категории значимости ОКИИ применительно к структуре и потенциалам возможных нарушителей БИ.

3.4 Выводы по третьей главе

1. Разработан алгоритм формирования модели нарушителя ОКИИ с использованием предположений о его потенциале и возможных последствиях реализации угроз БИ.

2. Предложен алгоритм решения задачи определения потенциала нарушителя информационной безопасности ОКИИ на основе наборов оцениваемых характеристик условий функционирования, исполняемых технологических процессов, а также технологического процесса обработки информации в ОКИИ.

3. Предложен алгоритм оценки опасности реализации угроз потенциальным нарушителем БИ ОКИИ на основе результатов оценки опасности реализации угроз БИ в виде четких значений на каждом уровне ОКИИ.

4. Разработаны алгоритмы работы сканера безопасности, предназначенного для определения фактических уязвимых звеньев в общей структуре определения и оценки защищенности уязвимых звеньев ОКИИ.

5. Предложен алгоритм построения модели угроз БИ ОКИИ, основанный на оценке защищенности уязвимых звеньев от действий потенциальных нарушителей и реализованных мер защиты.

6. Сформулирована и решена задача выбора мер защиты на всех уровнях ОКИИ. В рамках решения задачи определены минимальный, базовый, адаптированный и уточненный адаптированный наборы мер защиты. Описан переход к адаптированному базовому набору мер защиты и его уточнению.

ГЛАВА 4. РАЗРАБОТКА И ПРИМЕНЕНИЕ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ МОДЕЛИРОВАНИЯ УГРОЗ БИ ОКИИ

4.1 Разработка архитектуры автоматизированной системы

Автоматизированная система (АС) представляет собой организационно-техническую систему, обеспечивающую выработку решений на основе автоматизации информационных процессов в различных сферах деятельности (управление, проектирование, производство) или их сочетаниях [107]. АС выдаёт информацию, основываясь на входных данных, помогающих лицу, принимающему решение (ЛПР) быстро и точно оценить ситуацию и принять то или иное решение в отношении обеспечения БИ ОКИИ. В качестве ЛПР может выступать лицо, уполномоченное на проведение мероприятий по БИ субъекта КИИ, либо организация, имеющая все необходимые виды лицензий на осуществление работ по обеспечению БИ, а также администратор БИ.

Разработанная автоматизированная система моделирования угроз информационной безопасности ОКИИ (АС «МУИБ») должна позволять проводить мероприятия по моделированию угроз БИ с применением средств автоматизации на каждом из уровней (полевой, средний и верхний) многоуровневых АСУ ТП, а также в ИС и ИТКС.

Автоматизированная система «МУИБ» проектируется с учетом ряда ключевых требований:

– Достоверность и актуальность данных. АС обязана предоставлять надежную и своевременную информацию, необходимую для выявления существующих угроз БИ на каждом уровне ОКИИ.

– Аналитический функционал и поддержка принятия решений. В задачи системы входит анализ текущей ситуации, формирование обоснованных рекомендаций по противодействию угрозам БИ, а также предоставление пояснений к предлагаемым решениям.

– Коммуникационная архитектура (Communication Driven). Система должна принадлежать к классу, основанному на коллективном экспертном мнении.

– Унификация данных. Архитектура системы должна обеспечивать единообразие обработки информации, независимо от ее исходного формата.

– Масштабируемость обработки. Система должна демонстрировать одинаковую эффективность и применять идентичные принципы обработки как для малых объемов данных, так и для работы с крупными массивами информации [108].

На рисунке 4.1 представлена структура АС «МУИБ», реализующая предложенные в главах 2 и 3 диссертации методы и алгоритмы.

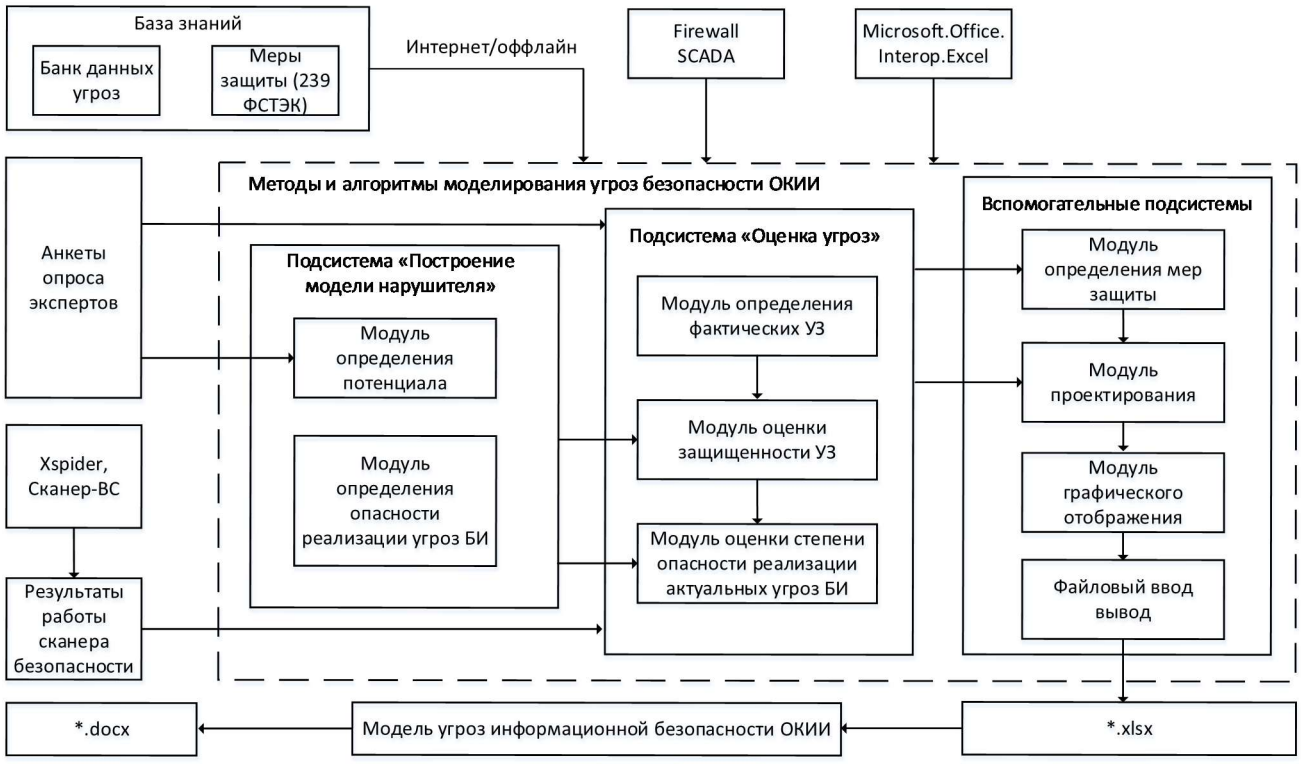


Рисунок 4.1 — Структура АС «МУИБ»

В целях соответствия вышеуказанным требованиям структура АС «МУИБ» имеет блоковую архитектуру с соответствующими логическими элементами и этапами их функционирования [109 - 110]. Основным блоком АС «МУИБ» ИБ является *«Методы и алгоритмы моделирования угроз БИ ОКИИ»,* реализующий предложенные в диссертации решения для оценки опасности реализации угроз БИ. В основе данного блока лежат подсистемы *«Построение модели нарушителя»*, *«Оценка угроз»* и *«Вспомогательные подсистемы»*.

Проведенный в первой главе анализ предметной области позволил определить ключевую функциональную задачу АС «МУИБ»:

создание детализированной модели каждого из уровней информационной системы в контексте оценки угроз ИС, ИТКС или АСУ ТП: физического расположения уязвимых звеньев ОКИИ, структурно-функциональных характеристик ОКИИ, используемых каналов передачи данных, взаимодействия с внешними сетями, объектов и субъектов доступа, характеристик БИ ОКИИ, описания уязвимых звеньев ОКИИ, требующих защиты;

– формирование подробного описания внутренних и внешних нарушителей;

– оценка потенциала нарушителей ИБ АСУ ТП;

– оценка опасности реализации угроз БИ ОКИИ потенциальными нарушителями;

– определение уязвимых звеньев на каждом из уровней ОКИИ;

– оценка защищенности уязвимых звеньев на каждом из уровней АСУ ТП;

– формирование перечня возможных угроз из БДУ ФСТЭК;

– оценка опасности реализации актуальных угроз БИ на каждом уровне ОКИИ, построение перечня актуальных угроз;

– выдача рекомендаций по выбору мер защиты на каждом из уровней ОКИИ.

Предложенная функциональная модель процесса *«Моделирование угроз БИ АСУ ТП»* в графической нотации IDEF0 представлена на рис. 4.2 [111 - 113].

В качестве инструмента для функционального моделирования был использован инструмент CA Erwin Process Modeler, представляющий собой мощное средство моделирования, которое поддерживает моделирование процессов, выполняемых ПО в соответствии с методологией IDEF0 [114 - 115].

Рисунок 4.2 — Функциональная модель процесса

«Моделирование угроз БИ ОКИИ»

В основе функциональной модели осуществлен переход к декомпозиции функциональных блоков, характеризующих основные операции при моделировании угроз ОКИИ с применением АС «МУИБ». Декомпозиция функционального блока А00 – «Моделирование угроз» представлена на рис. 4.3. Разработанная модель декомпозиции определяет логический порядок реализации ключевых функций процесса моделирования угроз безопасности информации объектов КИИ. Данный порядок построен в строгом соответствии с положениями действующих нормативно-правовых актов в сфере защиты критической информационной инфраструктуры, а также с учетом рекомендаций ведущих международных и отечественных стандартов в области ИБ, анкет экспертного опроса, представленных в приложениях к диссертации и БДУ ФСТЭК.

Декомпозиция функций моделирования угроз БИ (согласно приложениям и БДУ ФСТЭК) помогает выявить аспекты работы субъекта КИИ. Мониторинг данных аспектов через АС «МУИБ» создает базис для анализа эффективности внедренных мер безопасности — как технических, так и организационных.

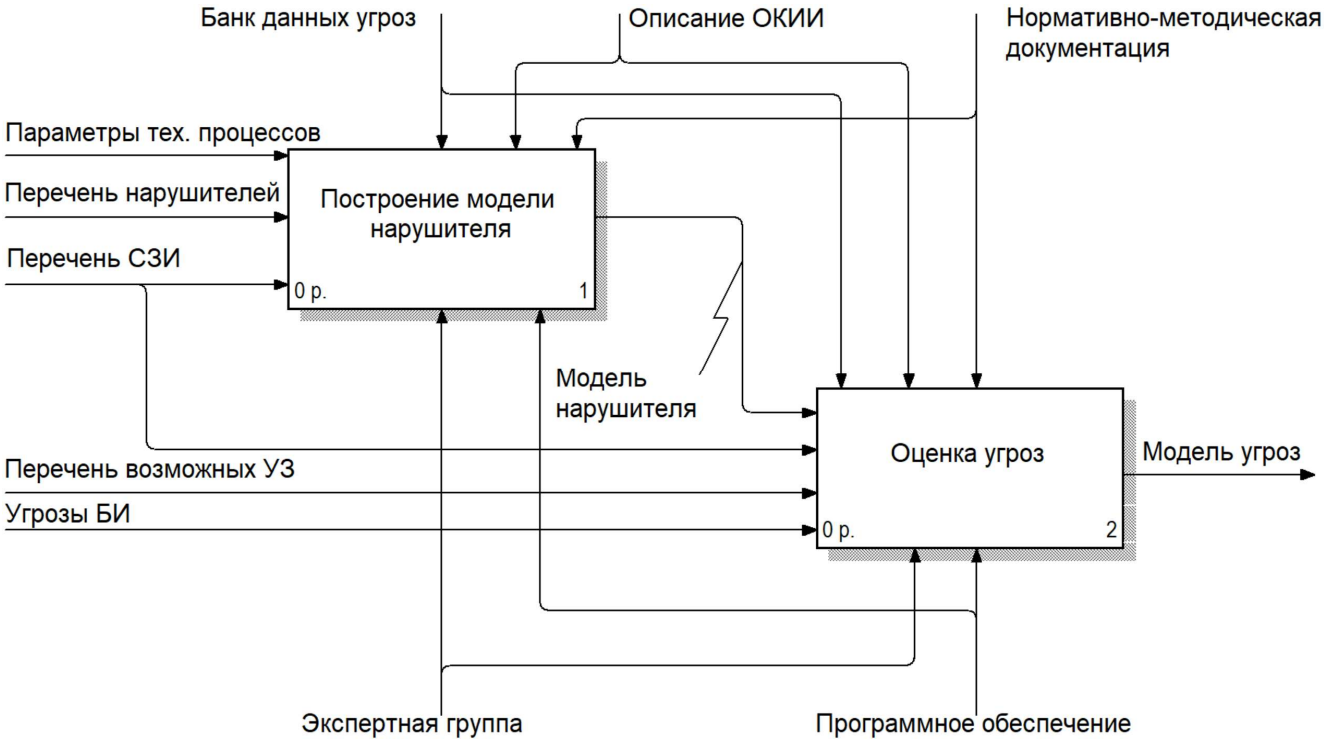


Рисунок 4.3 — Декомпозиция блока «Моделирование угроз БИ ОКИИ»

Рисунок 4.4 содержит детализированное представление алгоритма построения модели нарушителя ОКИИ в виде функциональной модели. Эта схема, соответствующая второму уровню декомпозиции, визуализирует последовательность основных этапов моделирования нарушителей ОКИИ блока *«оценка нарушителей БИ ОКИИ»*: «Общее описание внутренних и внешних нарушителей»,

«Формирование предположений о квалификации и мотивации», «Определение потенциала» и «Оценка опасности реализации угроз». Все перечисленные модули, в свою очередь, могут быть разбиты на компоненты и представлены в виде схемы последующего уровня детализации на основании методов и алгоритмов, описанных в главах 2 и 3. Результатом выполнения функционального блока *«оценка нарушителей БИ ОКИИ»* является модель нарушителя в текстовой и

графических формах, выполненная на основании сведений о потенциальных нарушителях, применяемых СЗИ и выполняемых технологических и (или) информационных процессах в ОКИИ.

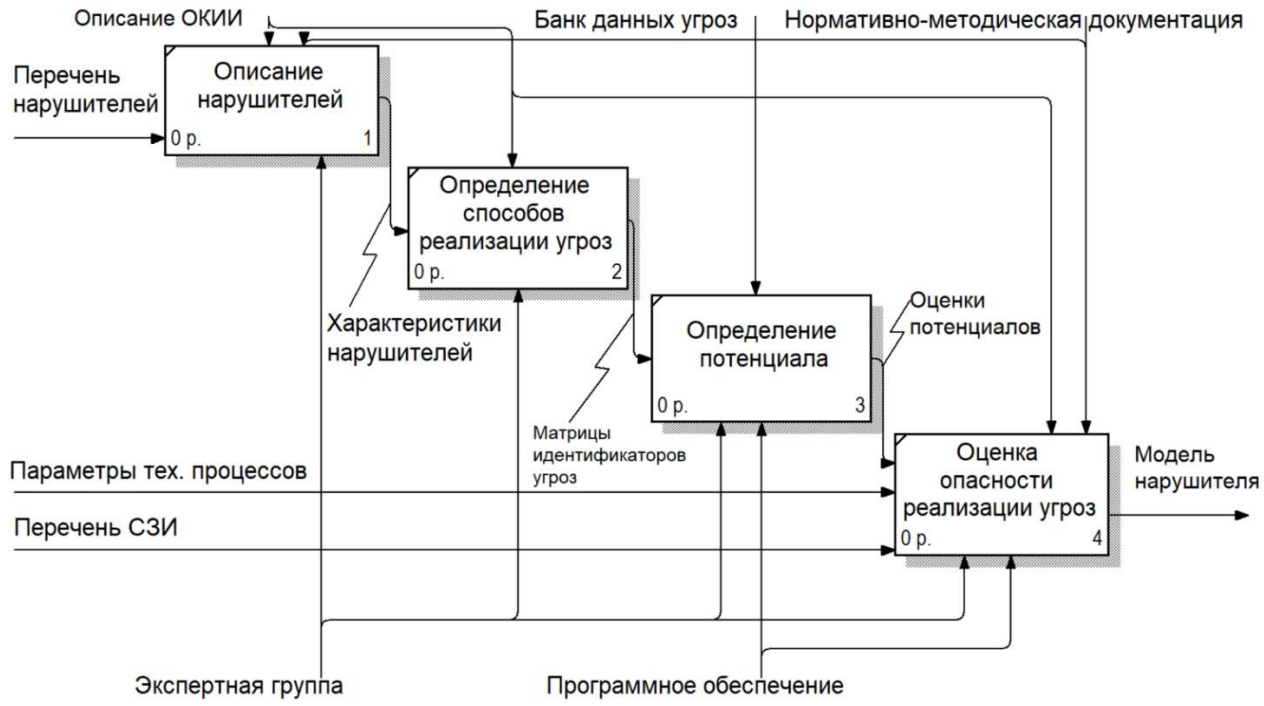


Рисунок 4.4 — Функциональная модель второго уровня «Построение модели нарушителя»

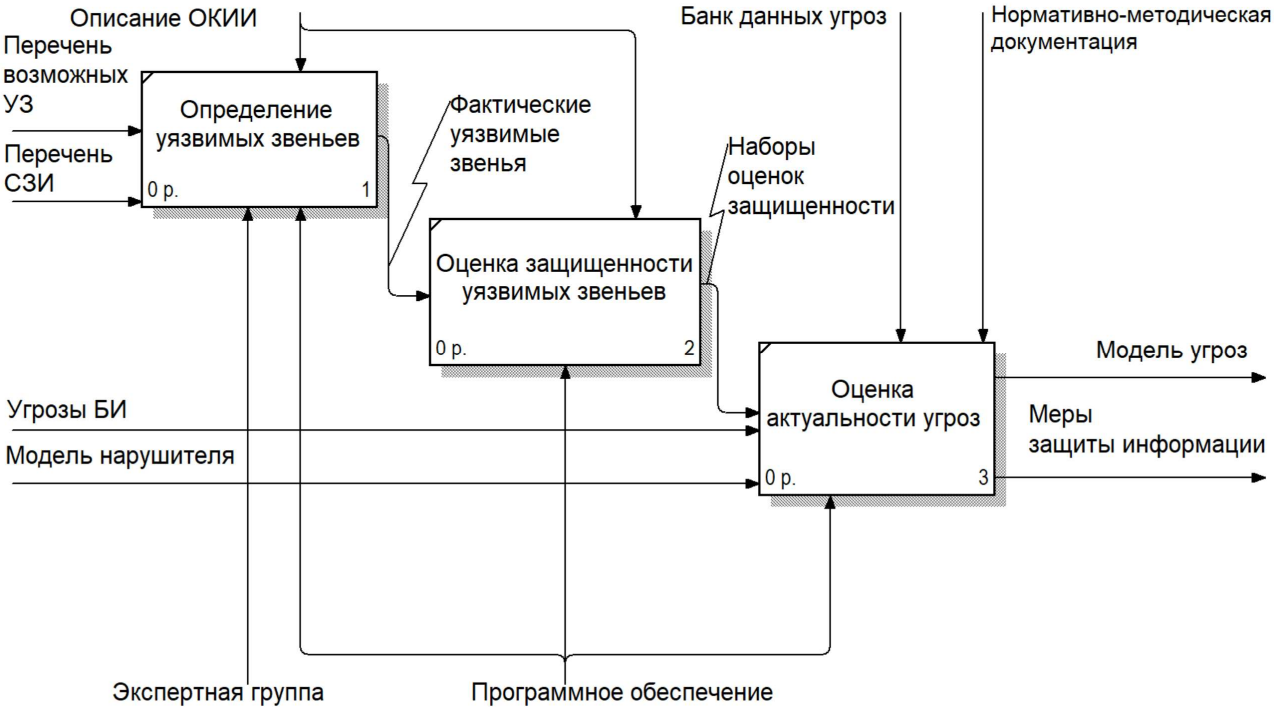


Рисунок 4.5 — Функциональная модель второго уровня «Оценка угроз»

На рис. 4.5 представлена декомпозиция функционального блока *«оценка угроз»*, которая отображает основные этапы моделирования нарушителей ОКИИ. Результатом выполнения функционального блока *«оценка угроз АСУ ТП»* является модель угроз ОКИИ в текстовой и графических формах, составленная на основании результатов выполнения функционального блока *«оценка нарушителей БИ ОКИИ»* и перечня уязвимых звеньев ОКИИ.

Информационная модель, построенная с помощью технологии IDEF1X (рис. 4.6), служит для отражения основных данных, которые являются результатом работы функций, их свойств и связей друг с другом.

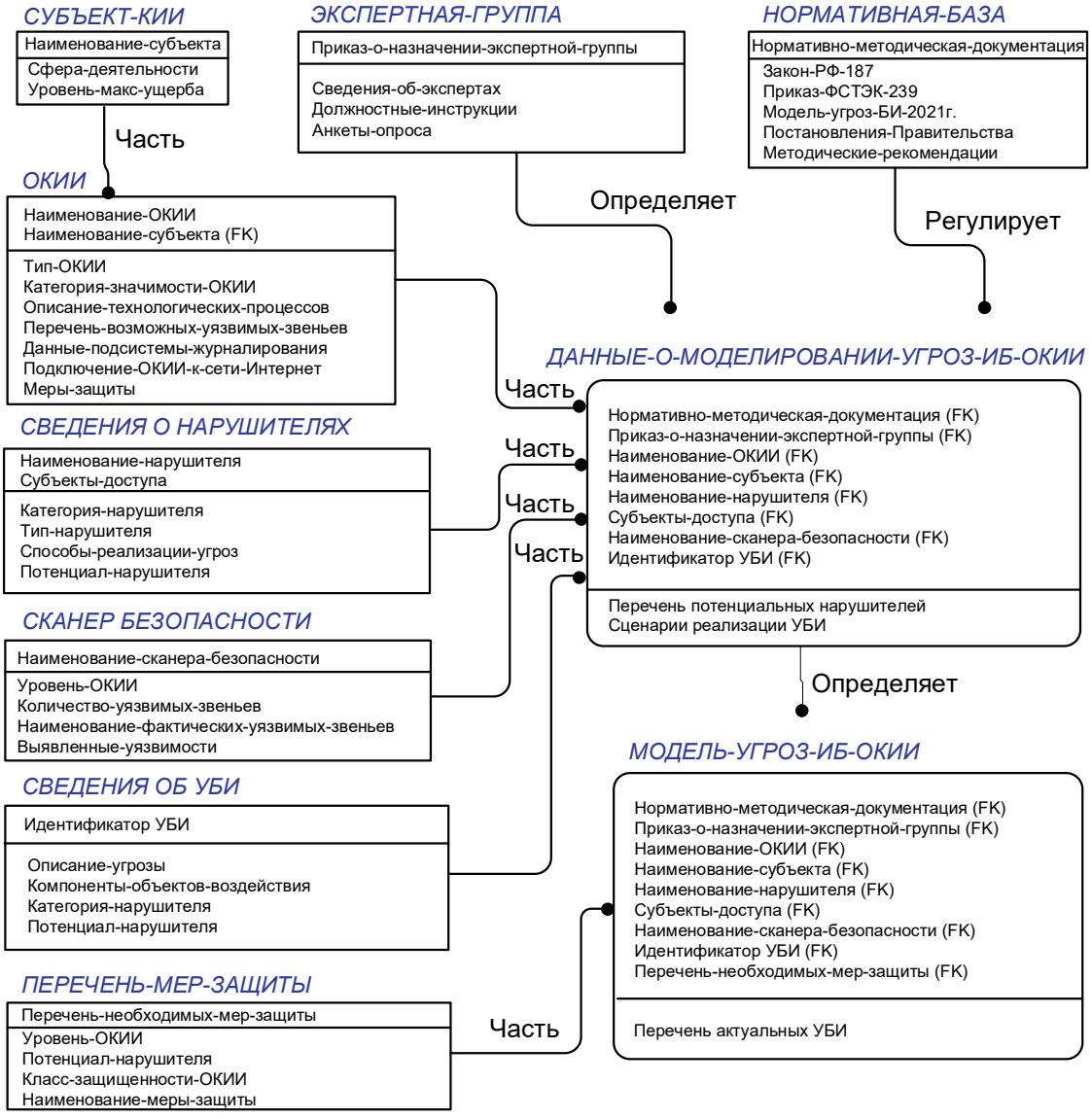


Рисунок 4.6 — Информационная модель экспертной оценки степени опасности реализации угроз БИ ОКИИ

Системное моделирование обеспечивает визуализацию и эффективное отображение процесса моделирования угроз БИ ОКИИ. В результате проведенного исследования была систематизирована информация, необходимая для реализации функций процесса, определены основные этапы моделирования угроз БИ, а также проанализирована динамика функциональных, информационных и ресурсных аспектов процесса.

Результатом применения методологий IDEF0 и IDEF1x является построение функциональной схемы, проектируемой АС «МУИБ», описывающей все необходимые процессы с точностью, достаточной для однозначного моделирования деятельности объекта.

4.2 Программная реализация АС «МУИБ»

В качестве основного инструмента разработки АС «МУИБ» выбран язык программирования C#. Данный выбор был обусловлен следующими достоинствами языка программирования C#: безопасность, архитектурная нейтральность, переносимость, высокая производительность, многопоточность, динамичность, простота использования, ориентация на объекты [116 - 117]. Листинг основных модулей программного обеспечения представлен в приложении 7 к диссертации.

В целях программной реализации основных подсистем разрабатываемого программного обеспечения был использован пакет Microsoft.Office.Interop.Excel. Данный пакет, включает в свой состав необходимый набор библиотек для организации взаимодействия прикладной части и пользовательского интерфейса АС «МУИБ».

Краткое описание основных классов, используемых в АС «МУИБ», представлено в таблице 4.1.

Таблица 4.1 — Основные классы программного обеспечения АС «МУИБ»

Имя и краткое описание класса	**Свойства класса**	**Методы класса**
Form1_Main	– Количество нарушителей; – Количество уязвимых звеньев; – Количество угроз БИ.	– Построение графика потенциалов нарушителей; – Построение графика характеристик реализации уязвимостей; – Построение графика классов защищенности.
Form2_ThreatModel	– Количество нарушителей; – Массив типов нарушителей; – Массив вероятностей реализации угроз БИ верхнего уровня; – Массив вероятностей реализации угроз БИ среднего уровня; – Массив вероятностей реализации угроз БИ полевого уровня;	– Оценка опасности реализации угроз БИ; – Формирование перечня актуальных угроз.
Form3_Intruder's_Model	– Количество нарушителей; – Количество уязвимых звеньев; – Массив типов нарушителей.	– Оценка потенциалов нарушителей; – Оценка опасности реализации угроз БИ.
Form4_Protective_Measures	– Общее количество мер защиты; – Потенциалы нарушителя; – Класс защищенности уровней ОКИИ; – Категория значимости ОКИИ.	– Выбор мер защиты; – Выгрузка в проект.
Form5_BDU	– Текущие дата и время; – Количество угроз БИ.	– Загрузка актуальной информации БДУ с сайта ФСТЭК РФ.
Form6_Attacker_Potential	– Массив анкетных данных; – Массив потенциалов нарушителей; – Количество параметров оценки; – Количество нарушителей;	– Определение потенциальных нарушителей; – Ручное заполнение; – Автоматическое заполнение;

	– Счетчик анкет.	– Выгрузка в проект.
Form7_ Implementation	– Массив уязвимых звеньев; – Массив мер защиты; – Массив потенциалов нарушителей; – Оценка наличия уязвимости.	– Ручное заполнение; – Заполнение из сканера безопасности; – Расчет характеристик реализации уязвимых звеньев; – Выгрузка в проект.
Form8_Graph1	– Количество уязвимых звеньев.	– Построение графика характеристик реализации уязвимых звеньев; – Выгрузка в проект.
Form9_Graph2	– Количество нарушителей.	– Построение графика потенциалов нарушителей; – Выгрузка в проект.
Form10_ Choice	– Количество мер защиты; – Количество рассматриваемых уровней ОКИИ; – Количество нарушителей – Массив уязвимых звеньев; – Массив классов защищенности.	– Определение максимального класса защищенности; – Построение базового набора мер защиты; – Адаптация базового набора мер защиты; – Выгрузка в проект.

На рисунке 4.7. представлена диаграмма классов АС «МУИБ», подробно отражающая иерархическую структуру разработанного ПО.

Для достижения целей корректного функционирования разработанной автоматизированной системы в её корневом каталоге должны находиться четыре файла формата Microsoft Excel (*.xlsx), содержащие информацию о функционировании и внешних условиях эксплуатации ОКИИ. Файлы предустанавливаются системой по умолчанию. Вместе с тем предусмотрена возможность оперативной загрузки файлов посредством сети международного обмена Интернет.

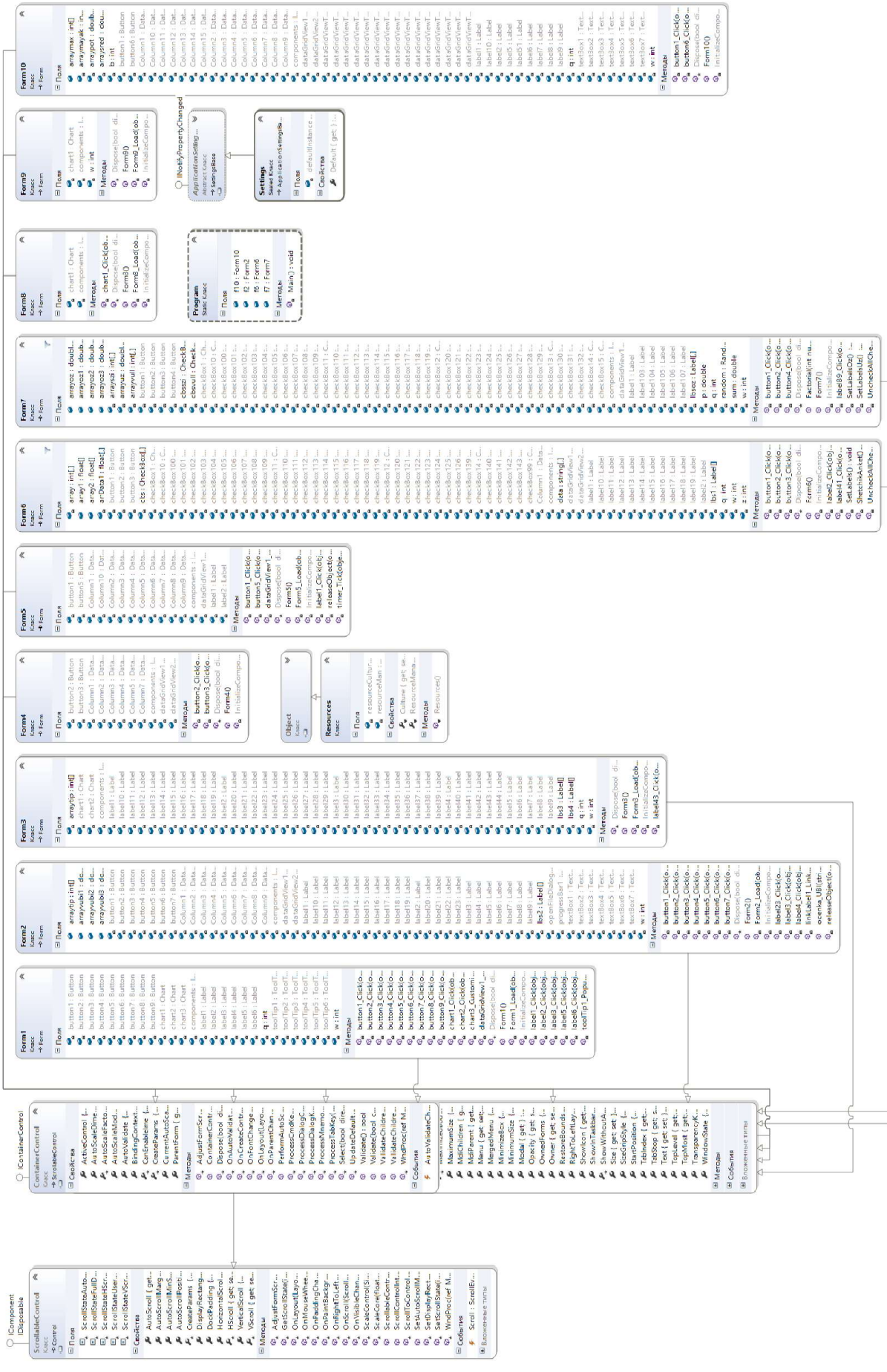


Рисунок 4.7 — Диаграмма классов АС «МУИБ»

Краткое описание структуры файлов, необходимых для корректного функционирования АС «МУИБ», представлено в таблице 4.2.

Таблица 4.2 — Структура файлов, используемых АС «МУИБ»

Имя файла и относительный путь к нему	**Назначение файла**	**Структура файла**
Mzi.xlsx	Содержит перечисление возможных мер защиты ОКИИ	– Идентификатор меры защиты; – Наименование меры обеспечения безопасности значимого объекта; – Применимость меры защиты для 3 класса защищенности; – Применимость меры защиты для 2 класса; – Применимость меры защиты для 1 класса.
Thrlist.xlsx	Содержит перечисление возможных угроз БИ ОКИИ	– Идентификатор угрозы; – Наименование угрозы; – Описание угрозы; – Источник угрозы; – Объект воздействия; – Нарушение конфиденциальности; – Нарушение целостности; – Нарушение доступности.
Survey.xlsx	Содержит информацию в отношении нарушителей ИБ ОКИИ в соответствии с приложением 1. Данный файл подлежит к заполнению каждым из опрашиваемых экспертов в предметной области.	– Количество критериев оценки нарушителей; – Критерии оценки нарушителей; – Количество нарушителей; – Положительный ответ – 1; – Отрицательный ответ – 0.
Scan.xlsx	Содержит результаты проверки ОКИИ сканером безопасности. В АС «МУИБ» реализована поддержка отчетов сканера безопасности XSpider.	– Уровень ОКИИ; – Количество уязвимых звеньев; – Наименование уязвимых звеньев; – Выявленные уязвимости.

Результатом работы АС «МУИБ» является проект, включающий в свой состав файлы оценки угроз БИ для рассматриваемого ОКИИ. Файлы проекта могу быть использованы как в качестве составного элемента организационно-распорядительной документации на объект, так и в качестве дополнительных данных для решения комиссии в рамках проведения аттестационных испытаний на соответствие требованиям по защите ОКИИ.

Краткое описание структуры файлов проекта, реализуемых разработанным ПО, представлено в таблице 4.3.

Таблица 4.3 — Структура файлов проекта, формируемого АС «МУИБ»

Имя файла и относительный путь к нему	**Назначение файла**	**Структура файла**
Потенциалы_нарушителей.xlsx	Содержит информацию о числовых значениях потенциала каждого конкретного вида нарушителей ИБ ОКИИ. Предусмотрена цифровая градация потенциалов в зависимости от вербальных характеристик, представленных в таблице 2.1.	– Вид нарушителя; – Числовое значение потенциала нарушителя.
Оценки_угроз.xlsx	Содержит информацию о числовых значениях оценок опасности реализации угроз БИ ОКИИ.	– Идентификатор угрозы безопасности информации; – Наименование угрозы безопасности информации; – Значение оценки опасности реализации угрозы на каждом из уровней ОКИИ.
Опасность реализации_угроз.xlsx	Содержит информацию об оценке опасности реализации угроз БИ. Предусмотрена цифровая градация угроз в зависимости от их актуальности на каждом из уровней ОКИИ.	– Идентификатор угрозы безопасности информации; – Оценка актуальности угрозы на каждом из уровней ОКИИ.

Класс_защищенности.xlsx	Содержит результаты определения общего класса защищенности для каждого из уровней ОКИИ по результатам адаптации БН мер защиты.	– Уровень ОКИИ; – Результат вычисления класса защищенности относительно каждого из видов нарушителей; – Общий класс защищенности для ОКИИ.
Защитные_меры.xlsx	Содержит перечисление мер защиты, необходимых к реализации на каждом из уровней ОКИИ в целях минимизации последствий реализации актуальных угроз БИ.	– Уровень ОКИИ; – Мера защиты.

Файлы проекта подлежат формированию как в автоматическом, так и в ручном режимах. В целях формирования файлов проекта пользователем АС «МУИБ» реализован соответствующий функционал.

4.3 Исходные данные по объекту внедрения АС «МУИБ» - промышленная АСУ ТП.

В целях подтверждения правильности моделирования угроз информационной безопасности, выполняемых предложенными методами и алгоритмами, проведен вычислительный эксперимент.

В качестве ОКИИ, в отношении которого моделируются угрозы БИ с применением АС «МУИБ», рассматривается промышленная АСУ ТП, автоматизирующая технологический процесс выпуска металлических изделий, имеющий следующие технологические процессы:

- пескоструйная обработка;
- шлифовка поверхности;
- торцевание заготовки;
- сверление технологических отверстий;

– травление и гравировка;

– комплектование изделия.

Управление и контроль перечисленными технологическими процессами производится с применением АСУ ТП, обеспечивающих сбор показаний с контрольно-измерительных приборов, автоматический контроль состояния процесса и сигнализацию о его нарушении, управление приводами механизмов станков с числовым программным управлением.

Локальная АСУ ТП, обладающая следующими признаками: присвоенный третий класс защищенности, трехуровневое построение и наличие каналов связи с внешними сетевыми ресурсами.

Компоненты АСУ ТП размещены в производственных цехах, операторских/диспетчерских помещениях, кроссовых/аппаратных помещениях в пределах контролируемой зоны.

Нижний уровень промышленной АСУ ТП. Состав:

– датчики и иные измерительные приборы;

– двигатели, клапаны и иные управляемые механизмы;

– преобразователи сигналов.

Оборудование нижнего уровня обеспечивает:

– контроль и измерение технологических параметров;

– преобразование сигналов с первичных преобразователей и передачу их на средний уровень;

– Организация процесса получения управляющих сигналов и их трансляция на механизмы и оборудование ОКИИ.

Средний уровень промышленной АСУ ТП. Состав:

– ПЛК;

– преобразователи сигналов и протоколов;

– модули ввода-вывода;

– корзины ввода-вывода;

- станции распределённого ввода-вывода;
- промышленный персональный компьютер с функцией ПЛК.

Средний уровень обеспечивает выполнение следующих функций:

- сбор и обработку результатов измерений датчиков нижнего уровня;
- регулирование технологического процесса и управление механизмами нижнего уровня;
- индикация состояния системы и сигнализация об аварийных состояниях;
- передача информации для верхнего уровня и передача команд операторов на нижний уровень АСУ ТП.

Верхний уровень промышленной АСУ ТП.Состав:

- общую инфраструктуру АСУ ТП (в том числе ТСПД);
- сервер АСУ ТП;
- операторские панели;
- операторские и инженерные станции;
- преобразователи сигналов связи;
- коммутаторы и иное сетевое оборудование.

Оборудование верхнего уровня обеспечивает:

- сбор данных со среднего уровня и их обработку;
- отображение состояния управляемых и контролируемых объектов, компонентов АСУ ТП;
- дистанционное управление ходом технологического процесса;
- протоколирование событий;
- создание архивных и резервных копий баз данных;
- контроль за работой оборудования и информацией.

АСУ ТП функционирует в изолированном сетевом сегменте, не имеющем подключения к сетям общего пользования, включая Интернет. Удаленный доступ для внешних организаций заблокирован.

Функциональная схема комплекса АСУ ТП приведена на рис. 4.8.

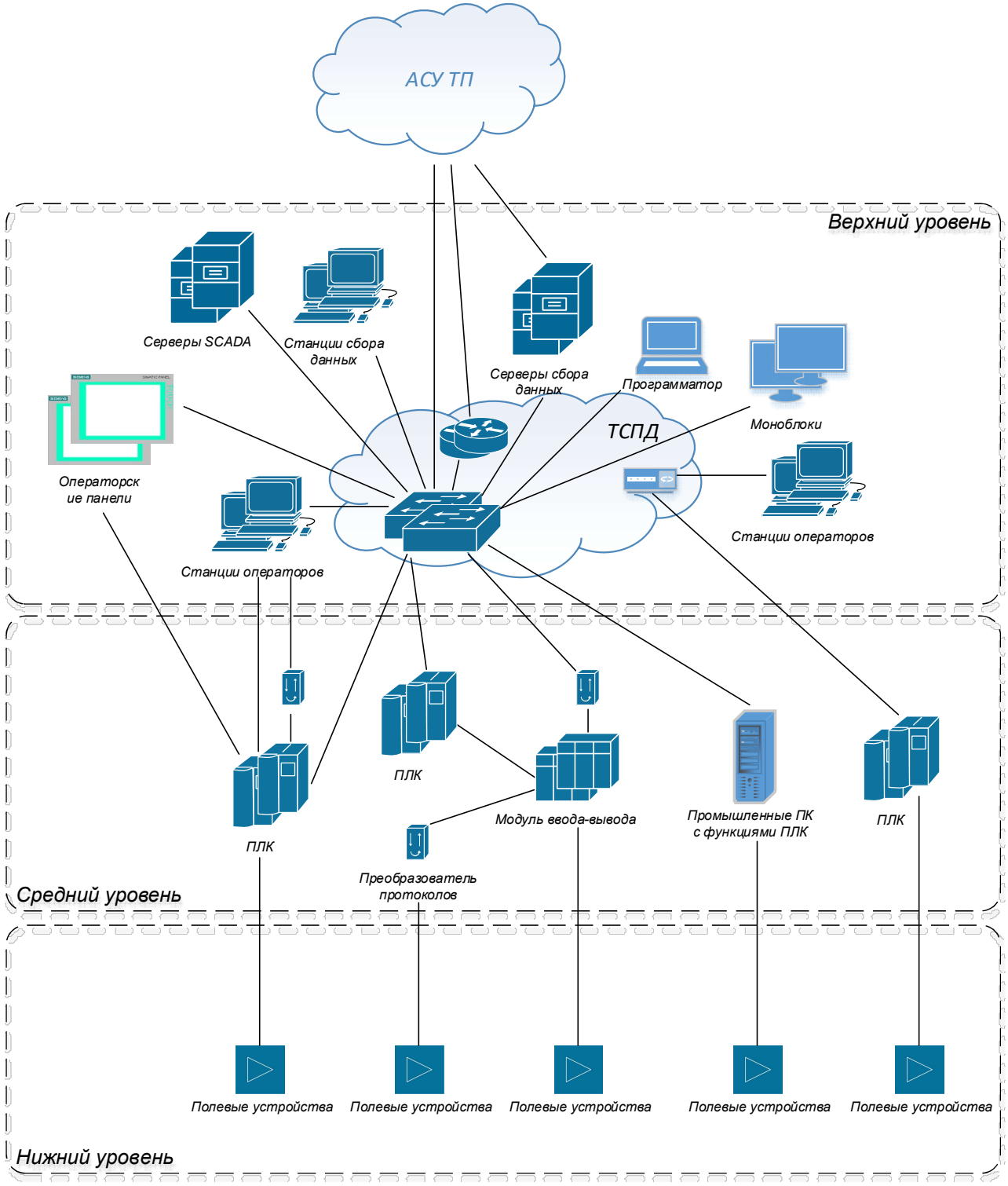


Рисунок 4.8 — Функциональная схема обследуемой АСУ ТП

В таблице 4.4 указаны общие сведения о каналах и протоколах передачи данных между компонентами промышленной АСУ ТП.

Таблица 4.4 — Каналы передачи данных между компонентами АСУ ТП

№ п/п	Наименование каналов	Назначение	Технология (тип кабеля)
1.	Нижний уровень – средний уровень	Каналы взаимодействия компонентов нижнего и среднего уровней	RS-232, RS-485, Modbus, Modbus RTU/ TCP/ Plus, Profibus, сухие контакты, витая пара,
2.	Средний уровень	Каналы взаимодействия между компонентами среднего уровня	RS-232, RS-485, Витая пара,
3.	Средний уровень – верхний уровень	Каналы взаимодействия компонентов среднего и верхнего уровней	Витая пара, волокно-оптические линии связи (далее – ВОЛС)
4.	Верхний уровень	Каналы взаимодействия между компонентами верхнего уровня	Сухие контакты, Fast Ethernet, Gigabit Ethernet, Ethernet

В целях описания технологического процесса обработки информации, циркулирующей в промышленной АСУ ТП необходимо произвести инвентаризацию каналов связи. Результаты инвентаризации представлены в таблице 4.5.

Таблица 4.5 — Перечень подключений АСУ ТП к внешним сетям и информационным системам

№ п/п	Сеть/сегмент	Назначение	Удаленные компоненты
1.	АСУ ТП	Передача данных в автоматизированную систему оперативно-диспетчерского управления и систему исполнения производства	Сервер сбора данных
2.	Производители оборудования	Удалённое сопровождение компонентов АСУ ТП	АРМ работников сторонней организации

Перечень видов информации, обрабатываемой в АСУ ТП, в отношении которой могут возникать угрозы, приведен в таблице 4.6.

Таблица 4.6 — Перечень видов информации, обрабатываемой в АСУ ТП и подлежащей защите

№ п/п	Вид информации	Содержание информации	Процессы, в которых используется	Компоненты сбора/ввода	Компоненты обработки
1	Телеизмерения (AI - Analog Input)	Информация от датчиков, средств измерения, преобразователей о количественной оценке характеристик контролируемого процесса (давления, расхода, температуры пр.)	Получение текущей информации о состоянии системы и механизмов	Устройства среднего и нижнего (полевого) уровней	Серверы; АРМ операторов; Операторские панели; Информационные табло
2	Телесигнализация (DI - Digital Input)	Информация о дискретных изменениях состояния объекта (например, включен/выключен, норма/авария и т.п.)		Устройства среднего и нижнего (полевого) уровней	Серверы; АРМ операторов; Операторские панели; Информационные табло
3	Телеуправление (DO - Digital Output)	Команды управления положением или состоянием дискретных объектов с конечным множеством состояний	Управление исполнительными элементами	Устройства среднего и нижнего (полевого) уровней	Серверы; АРМ операторов; Операторские панели
4	Телерегулирование (AO - Analog Output)	Команды управления положением или состоянием дискретных объектов с непрерывным множеством состояний		Устройства среднего и нижнего (полевого) уровней	Серверы; АРМ операторов; Операторские панели
5	Входные параметры производственного процесса	Исходные данные производственного процесса, вводимые оператором (номер заказа, наименование заказчика, параметры заказа, др.)	Определение параметров выполнения технологического процесса	АРМ операторов; Операторские панели	Серверы; АРМ операторов; Операторские панели
6	Конфигурации ПЛК, серверов, АРМ операторов	Файлы с логикой технологического процесса, составом технических средств, мнемосхемами	Хранение параметров конфигурации АСУ ТП и их восстановлен	ПЛК; Серверы; АРМ операторов	Серверы; Инженерные станции; Любые носители информации

	, операторских панелей АСУ ТП и иных компонентов в составе АСУ ТП		ие в случае возникновения сбоев		(жесткие диски, съемные запоминающие устройства, сетевые хранилища)
7	Аварийные события, ошибки в работе технологического оборудования	Информация об аварийных событиях о неисправностях в работе технологического оборудования АСУ ТП и рабочих событиях, содержащаяся в журнале событий и аварий прикладного ПО АСУ ТП, информация об ошибках в ОС	Регистрация событий на компонентах для последующего анализа	Все компоненты АСУ ТП	Серверы; АРМ операторов; Операторские панели; Информационные табло; Инженерные станции
8	Учётные данные	Учётные записи пользователей и обслуживающего персонала АСУ ТП	Идентификация и аутентификация при доступе к компонентам АСУ ТП	ПЛК; Серверы; АРМ операторов; Операторские панели	ПЛК; Серверы; АРМ операторов; Операторские панели
9	Архивные данные	Архив (резервная копия) измерений величин, служебной и технической информации	Резервное копирование и архивирование данных АСУ ТП	Серверы; АРМ операторов; Операторские панели	Серверы; АРМ операторов; Операторские панели

Субъекты, имеющие доступ к АСУ ТП, приведены в таблице 4.7 в соответствии с используемыми ролями доступа.

Таблица 4.7 — Субъекты, имеющие доступ к АСУ ТП

№ п/п	Роль	Обязанности	Доступ к компонентам	Права доступа
1.	Оператор АСУ ТП	Управление технологическим процессом, в частности,	Доступ к АРМ оператора и панели оператора	Ограниченные права доступа в рамках функциональной роли

		управление агрегатами, задвижками, вспомогательным оборудованием и системами		
2.	Администратор АСУ ТП	Сопровождение программно-аппаратных средств АСУ ТП	Физический и логический доступ ко всем компонентам	Полные права доступа ко всем компонентам АСУ ТП и в части АСУ ТП ограниченные права доступа в рамках функциональной роли
3.	Администратор системы резервного копирования	Сопровождение системы резервного копирования	Физический и логический доступ ко всем компонентам	Полные права доступа ко всем компонентам АСУ ТП
4.	Обслуживающая организация (Сервисная)	Сопровождение программно-аппаратных средств АСУ ТП	Физический и логический доступ ко всем компонентам	Полные права доступа ко всем компонентам АСУ ТП

Первоначальная регистрация пользователей в АСУ ТП, например, создание учетной записи и назначение прав не производится, допущенные работники работают под групповой учётной записью. Предоставление прав доступа работнику осуществляется после прохождения им обучения работе в АСУ ТП, в зависимости от его функциональных обязанностей и роли в ОС и прикладном ПО АСУ ТП.

Авторизация пользователя в АСУ ТП осуществляется по групповому идентификатору (логину) и паролю. Учётные записи хранятся локально на серверах, операторских и инженерных станциях, операторских панелях АСУ ТП.

Пользователи АСУ ТП в рамках своих функциональных обязанностей и в зависимости от своей роли могут осуществлять контроль и управление автоматизированными технологическими процессами средствами, доступ к которым предоставлен им в целях выполнения своих функциональных обязанностей.

Возможны следующие способы ввода информации в АСУ ТП:

- вручную с помощью клавиатуры;

– передача данных из одной АСУ ТП в другую.

Использование пользователями съемных носителей информации (далее – СНИ) в АСУ ТП не запрещено. В рамках технического обслуживания АСУ ТП администраторы АСУ ТП могут использовать СНИ. Учёт СНИ не производится.

При организации автоматизированной обработки информации в ОКИИ, принимаются во внимание ряд мер для обеспечения БИ, сформулированных в нормативно-методической документации ФСТЭК России в целях обеспечения конфиденциальности, целостности и доступности сведений. По окончании мероприятий по внедрению мер защиты должны быть достигнуты следующие результаты:

1) Сформулирован уровень конфиденциальности сведений – открытая информация. Четко определен класс защищенности (КЗ) – 3КЗ, а также кто и при каких условиях имеет к ней доступ (субъект доступа);

2) Составлен перечень лиц, имеющих доступ к указанным сведениям. Составлен список сотрудников, которым будет предоставлен автоматизированный доступ к сведениям, и определен АРМ, на котором будет производиться обработка указанных сведений.

3) Разработана автоматизация процедуры доступа. Созданы процедуры и механизмы, которые позволяют ограничить доступ к защищаемой информации с использованием дискреционного или мандатного механизмов управления доступом.

4) Обеспечен контроль и аудит доступа к сведениям (мониторинг безопасности). Внедрена система контроля доступа, которая позволяет отслеживать, кто и когда имел доступ к защищаемой информации и какую информацию они получили в случае успешной реализации угрозы БИ.

5) Установить СЗИ НСД, в том числе при соединении с внешними сетями (межсетевое экранирование).

6) Обеспечить защиту всех АРМ, серверов, ПЛК и прочих компонентов системы от вредоносных программ и атак путем внедрения средств антивирусной защиты, а также системы обнаружения вторжений.

7) Принять меры по защите сведений на всех уровнях конфиденциальности сведений, включая обеспечения БИ открытой информации. Включить шифрование сведений (обеспечение конфиденциальности сведений), контроль за передачей информации (обеспечение целостности сведений), создание резервных копий (обеспечение доступности сведений).

8) Обеспечить безопасность носителей информации. Защитить материальные носители информации (компакт-диски, внешние жесткие магнитные диски, флешки и т.д.) от несанкционированного доступа и копирования.

Современные, сертифицированные на соответствие требованиям по защите информации, программно-аппаратные средства позволяют автоматизировать вышеуказанные мероприятия для различных ОС, включая Unix-системы. Наиболее известные из них: Secret Net, Dallas Lock, Аккорд-Х, ИНАФ, Блокхост-Сеть. В целях выполнения рекомендаций указа Президента РФ № 250, в части импортозамещения СЗИ, возможно использование сертифицированной на соответствие требованиям по защите информации, ОС ASTRA LINUX SPECIAL EDITION, имеющую в своем составе подсистемы реализующие вышеуказанные мероприятия. В случае необходимости шифрования информации, обрабатываемой ОКИИ, могут применяться следующие программно-аппаратные средства криптографической защиты информации (ПАК СКЗИ): Континент, VipNet Coordinator, ФПСУ-IP.

Немаловажными мероприятиями являются тренинги и обучение персонала, которые имеют доступ к информации в ОКИИ, правилам работы с информацией ограниченного доступа и порядком работы с АРМ, оснащенными СЗИ НСД [16].

Описание фактических уязвимых звеньев - компонентов объекта воздействия, в отношении которых могут быть реализованы угрозы безопасности

информации, обрабатываемой в АСУ ТП, и которые подлежат оценке угроз БИ, приведено в таблице 4.8.

Таблица 4.8 — Описание уязвимых звеньев АСУ ТП, требующих защиты

№ п/п	Уязвимое звено (компонент объекта воздействия)	Описание компонента	Примечание
1.	Информация, обрабатываемая в АСУ ТП, на средствах отображения графической, видео- и буквенно-цифровой информации	Угрозы утечки видовой информации реализуются за счет просмотра информации с экранов дисплеев мониторов и других средств отображения графической и буквенно-цифровой информации, входящих в состав АСУ ТП.	-
2.	Данные, обрабатываемые АСУ ТП	В случае получения прямого доступа к информации, обрабатываемой в АСУ ТП, могут быть нарушены основные характеристики их безопасности (конфиденциальность, целостность, доступность), что может привести к негативным последствиям для АСУ ТП.	-
3.	Базовая система ввода-вывода компьютера	Несанкционированный доступ к базовой системе ввода/вывода (BIOS/UEF) дает возможность перехвата управления загрузкой ОС и получения прав доступа локального администратора.	В составе применяемых во всех АСУ ТП технических средств используются компоненты, включающие в свою архитектуру базовую систему ввода/вывода.
4.	Каналы связи	В случае получения доступа к каналам связи возможен перехват защищаемой информации.	В структуру АСУ ТП входят каналы связи.
5.	Технические средства АСУ ТП	Технические средства АСУ ТП подвержены угрозам физического доступа и нарушения их функционирования, а также получения посредством них доступа к иным объектам защиты.	В АСУ ТП используются ПЭВМ, мониторы, принтеры, ноутбук (администраторами АСУ ТП), модули ввода-вывода, ПЛК, датчики, преобразователи др.
6.	Носители информации	Носители информации в наибольшей степени подвержены угрозам безопасности со стороны злоумышленника. Все носители сведений конфиденциального характера должны быть учтены в установленном порядке. Характер	В АСУ ТП используются различные виды носителей информации с целью обработки информации: НЖМД, оптические компакт-диски, флеш-накопители

		работы с носителями информации в АСУ ТП должен находиться под контролем ответственных лиц.	и бумажные носители.
7.	Общесистемное ПО	К общесистемному ПО относится системное и микропрограммное ПО.	-
8.	Объекты файловой системы	Файлы, каталоги, библиотеки, метаданные и др. Получение злоумышленником прямого доступа к объектам файловой системы создает предпосылки к нарушению конфиденциальности, целостности и доступности информации в АСУ ТП.	-
9.	Состав, маршрутно-адресная информация, сетевые службы и иные характеристики сети и ее узлов, сетевое ПО, сетевой трафик, сетевой узел	Информация о сетевой инфраструктуре предоставляет злоумышленнику возможности для реализации сетевых атак и других угроз, использующих уязвимости сети, и нарушения характеристик безопасности информации, обрабатываемой в АСУ ТП.	В АСУ ТП используется сетевое оборудование.
10.	Учётные данные пользователя	Кража учетных данных предоставляет нарушителю возможность несанкционированного доступа к АСУ ТП, что может повлечь за собой сбои в ее функционировании или полный отказ. Следовательно, механизмы аутентификации относятся к числу наиболее уязвимых элементов системы.	
11.	Прикладное ПО	Угрозы, связанные с получением несанкционированного доступа к прикладному ПО, дают возможность нарушения основных характеристик безопасности информации, обрабатываемой в АСУ ТП.	-
12.	СЗИ и информация о них	Применяемые СЗИ призваны снижать опасность большинства угроз, поэтому нарушение их работоспособности должно быть исключено.	СЗИ НСД, антивирусное ПО
13.	Сетевое оборудование	Информация о сетевой инфраструктуре предоставляет злоумышленнику возможности для реализации сетевых атак и других угроз, использующих уязвимости сети, и нарушения характеристик безопасности информации, обрабатываемой в АСУ ТП.	В АСУ ТП используется сетевое оборудование.

Важно отметить, что указанный перечень уязвимых звеньев промышленной АСУ ТП является неполным, поскольку в процессе моделирования угроз БИ с применением АС «МУИБ» проводится дополнительное сканирование уязвимостей сканером безопасности, по результатам которого данный перечень дополняется новыми фактическими уязвимыми звеньями.

4.3 Результаты применения методик ФСТЭК РФ в процессе моделирования угроз БИ промышленной АСУ ТП

В целях проведения экспериментальных исследований разработанных методов и алгоритмов в качестве элемента сравнения использовался процесс моделирования угроз БИ, обрабатываемой в описанной выше промышленной АСУ ТП, относящейся к ОКИИ, осуществляемый в соответствии с методикой [20] и адаптированной с учётом специфики уязвимых звеньев АСУ ТП и основных задач по обеспечению БИ ОКИИ.

Исходные данные для оценки опасности реализации угроз БИ:

– БДУ ФСТЭК России (bdu.fstec.ru);

– негативные последствия от реализации (возникновения) угроз БИ;

– объекты воздействия угроз БИ и виды воздействий на них;

– виды и категории актуальных нарушителей, которые могут реализовывать угрозы БИ, в том числе непреднамеренные угрозы, и их возможности в ИТ - инфраструктуре субъекта КИИ;

– актуальные способы реализации (возникновения) угроз БИ.

В результате анализа исходных данных определяются осуществляемые нарушителем воздействия на информационные ресурсы и компоненты АСУ ТП, в результате которых возможно нарушение безопасности информации и (или) нарушение или прекращение функционирования АСУ ТП.

Угроза БИ возможна, если имеется хотя бы один сценарий ее реализации.

Чтобы угроза безопасности информации считалась актуальной, должен существовать хотя бы один вариант (сценарий) того, как ее можно осуществить. Указанные сценарии описывают все возможные способы реализации для каждой угрозы.

В приложении 4 представлен перечень актуальных угроз БИ с описанием сценариев реализации указанных угроз, включающий способы их реализации, объекты воздействия, источники угроз и негативные последствия, которые могут наступать в случае реализации указанных угроз.

По результатам применения методики ФСТЭК РФ для моделирования угроз информационной безопасности промышленной АСУ ТП выявлено 15 актуальных угроз БИ без разделения по уровням АСУ ТП. Общее количество мер защиты, необходимых для минимизации последствий реализации актуальных угроз информационной безопасности, – 155. На получение результатов моделирования угроз затрачено 59 человеко-часов.

4.4 Результаты применения АС «МУИБ» в процессе моделирования угроз БИ промышленной АСУ ТП.

Процедура построения модели угроз БИ ОКИИ с применением разработанной АС «МУИБ» состоит из трёх основных этапов.

Каждый из этапов связан с заполнением анкет экспертами или специалистами в предметной области, представленных в приложениях 1-3. Главное окно разработанного программного обеспечения представлено на рис. 4.9.

На первом этапе оператор может вручную ввести информацию относительно основных критериев оценки потенциальных нарушителей ОКИИ нажатием кнопки *«Заполнить вручную»,* расположенной на форме Attacker potential, представленной на рис. 4.10.

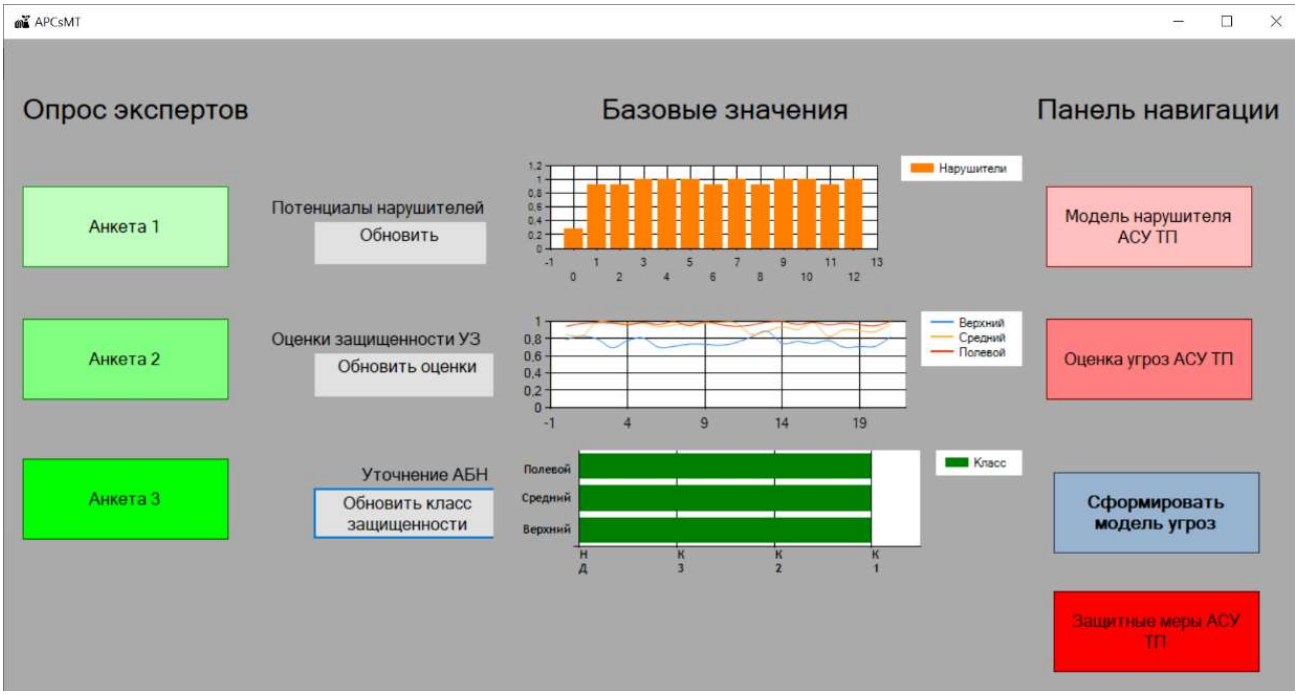


Рисунок 4.9 — Главное окно АС «МУИБ»

Ввиду возможности группового экспертного оценивания потенциалов предусмотрен счетчик обработанных анкет. Результаты оценки потенциалов выгружаются оператором в проект нажатием на кнопку *«Выгрузить в проект»*.

Результаты оценки потенциалов нарушителей в процессе моделирования угроз БИ промышленной АСУ ТП по результатам опроса десяти экспертов представлен на рис. 4.10.

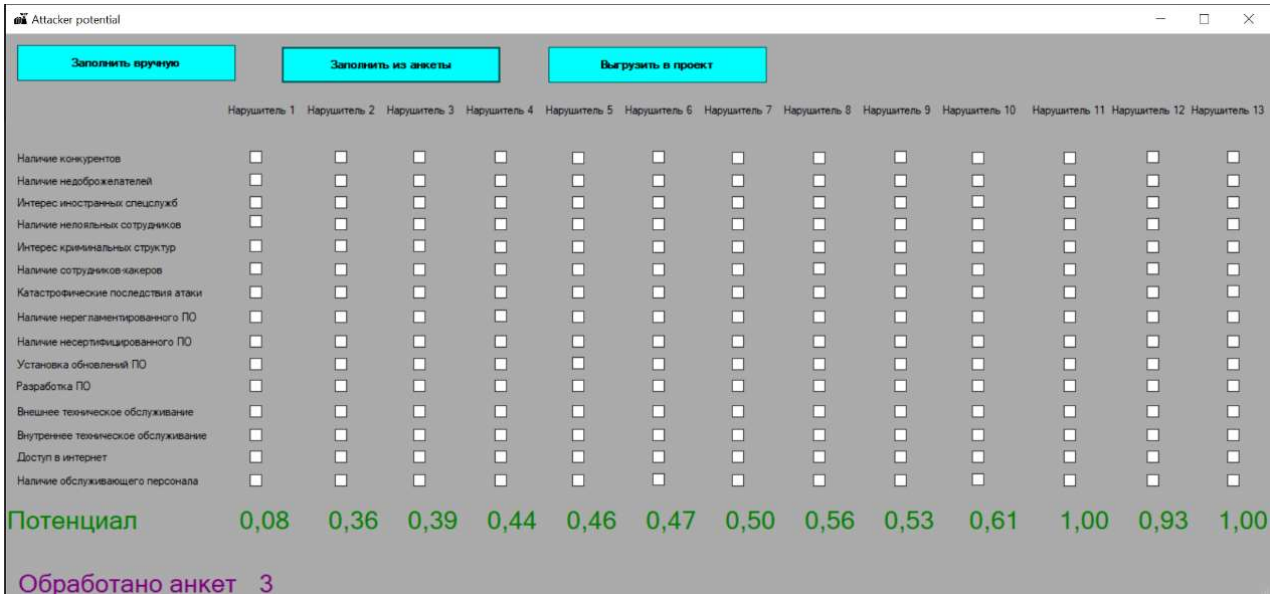


Рисунок 4.10 — Форма Attacker potential АС «МУИБ»

Также предусмотрено автоматическое формирование оценок потенциалов нарушителей на основании опросных листов, представленных в приложении 1, нажатием на кнопку *«Заполнить из анкеты»*.

На основании расчета потенциалов нарушителей в АС «МУИБ» на форме Intruder’s Model формируется модель нарушителя промышленной АСУ ТП в виде графического отображения, представленного на рис. 4.11. Графическое отображение и вербальные характеристики потенциалов нарушителей выгружаются в директорию проекта в виде файла *Intruder_Model.xlsx*.

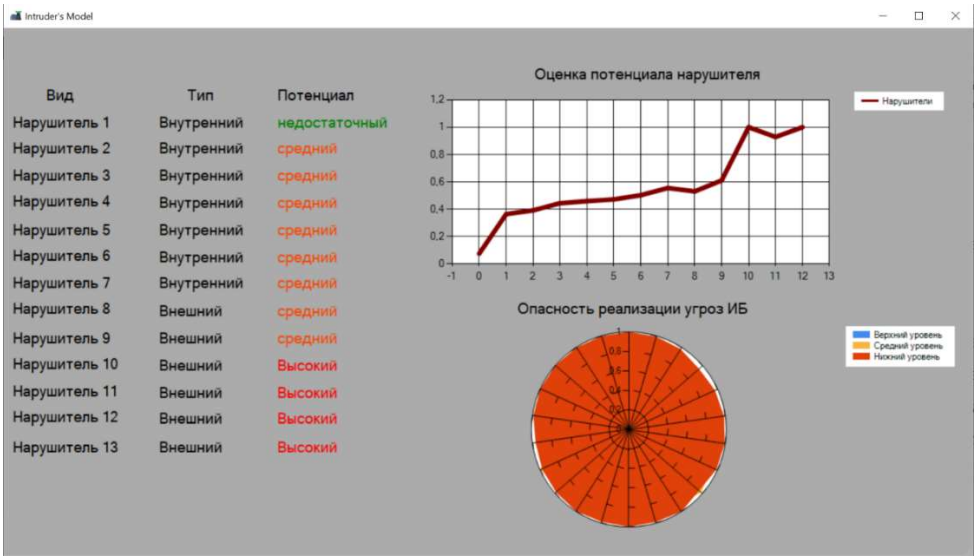


Рисунок 4.11 — Форма Intruder’s Model АС «МУИБ»

По завершении процесса формирования модели нарушителя оператором осуществляется переход ко второму этапу построения модели угроз на форме Security assessment, графическое изображение которой представлено на рис. 4.12.

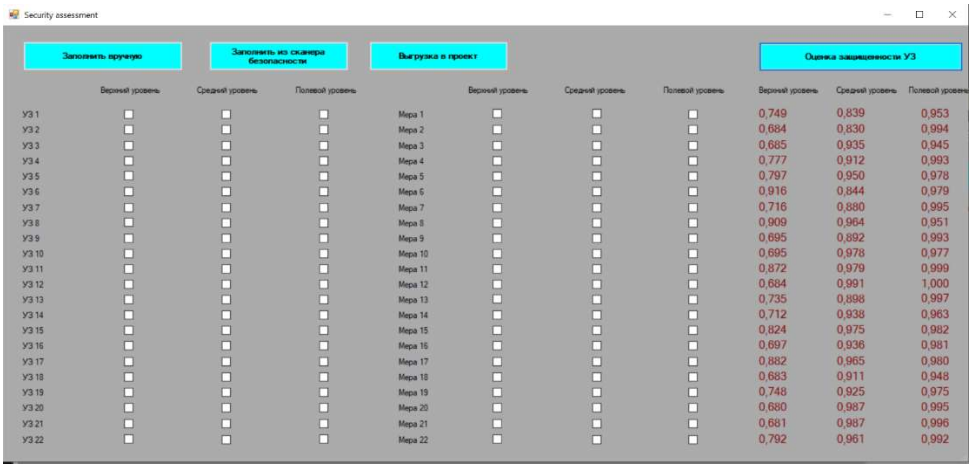


Рисунок 4.12 — Форма Security assessment АС «МУИБ»

Оператор вручную вводит информацию о наличии уязвимых звеньев на каждом из уровней АСУ ТП нажатием кнопки *«Заполнить вручную»*. Результаты оценки защищенности уязвимых звеньев формируются автоматически и могут быть выгружены оператором в директорию проекта в виде файла *Security_assessment.xlsx* нажатием на кнопку *«Выгрузить в проект»*. Дополнительно в АС «МУИБ» реализована возможность ввода информации о наличии уязвимых звеньев АСУ ТП на основании результатов работы сканера безопасности на каждом из уровней АСУ ТП. Результаты работы сканера безопасности в рассматриваемой АСУ ТП приведены в таблице 4.10.

Таблица 4.10 — результаты работы сканера безопасности на среднем уровне промышленной АСУ ТП

XSPIDER	***DATE***	***VUL***
Средний уровень АСУ ТП	***Уязвимые звенья***	
TCP/139 - NetBIOS		
	ID	Уязвимость
	8175	Не требуется подписывание SMB
	1094	LanManager и ОС
	8336	Время узла
	1061	Имя компьютера и домен
	8217	Настройки SMB2
	8106	Список служб RPC, доступных через Named Pipes
Нижний уровень АСУ ТП	***Уязвимые звенья***	
TCP/49154 - RPC mstask.exe		
	ID	Уязвимость
	1071	Планировщик заданий
	8107	Список служб RPC, доступных через TCP/IP
System		
	ID	Уязвимость
	180245	MAC-адрес сканируемого адаптера
	8123	Маршрут к сканируемому хосту
	1222	ОС
	8134	Ответ на ICMP-запрос метки времени
Верхний уровень АСУ ТП	***Уязвимые звенья***	
TCP/139 - NetBIOS		

	ID	Уязвимость
	8175	Не требуется подписывание SMB
	1094	LanManager и ОС
	8336	Время узла
	1061	Имя компьютера и домен
	8217	Настройки SMB2
	8106	Список служб RPC, доступных через Named Pipes

В целях применения результатов автоматизированного сканирования безопасности был разработан модуль маппинга отчетов безопасности программного обеспечения XSpider 7.8 производства компании Positive Technologies. Данный сканер безопасности имеет сертификат соответствия ФСТЭК РФ № 3247. В целях корректного маппинга отчета о результатах сканирования в АС «МУИБ» разработан шаблон настроек сканера безопасности XSpider 7.8. Параметры шаблона отражены на рис. 4.13.

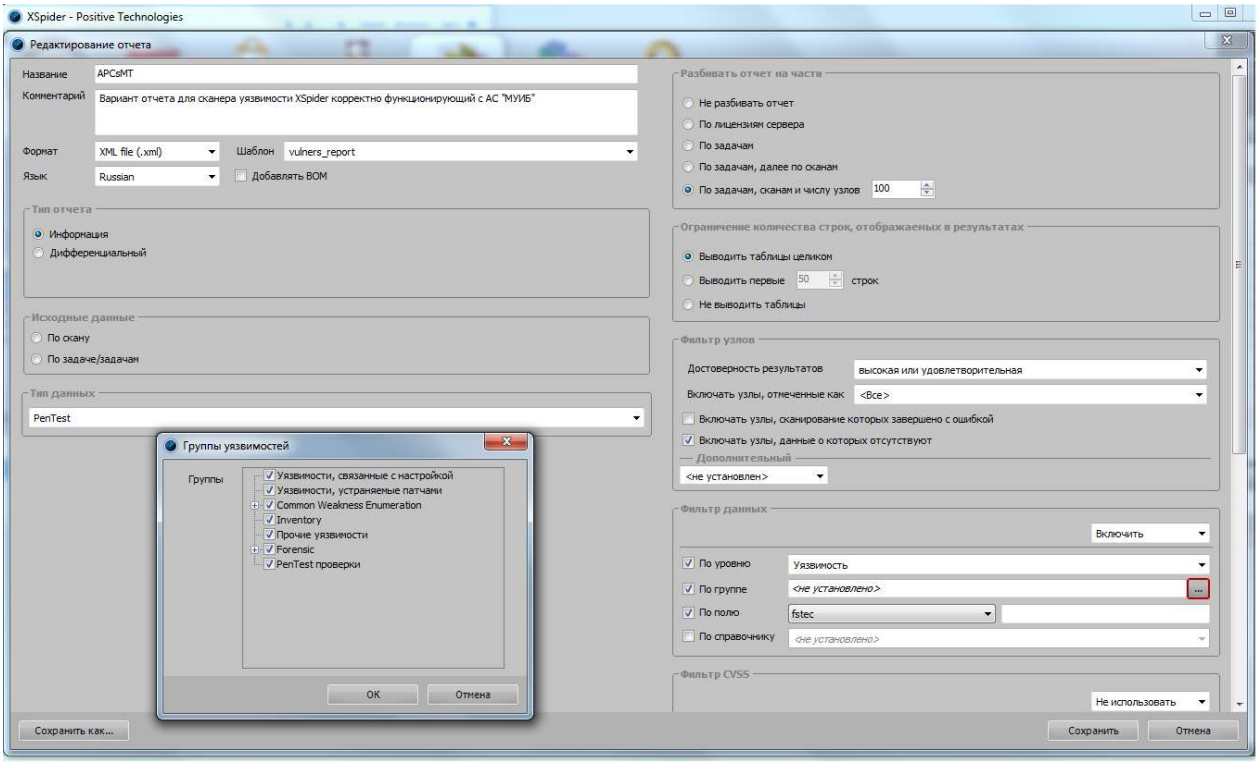


Рисунок 4.13 — Шаблон настроек XSpider 7.8 для АС «МУИБ»

На следующем этапе осуществляется переход к форме Determining the danger of implementing threats для оценки опасности реализации угроз БИ. Для этого необходимо загрузить анкету, представленную в приложении 2, путем нажатия

клавиши «*Заполнить из анкеты оценки значимости свойств*» или внести их вручную, а также заполнить оценки FMEA, полученные для каждого технологического процесса в АСУ ТП из SCADA системы или промышленного фаервола.

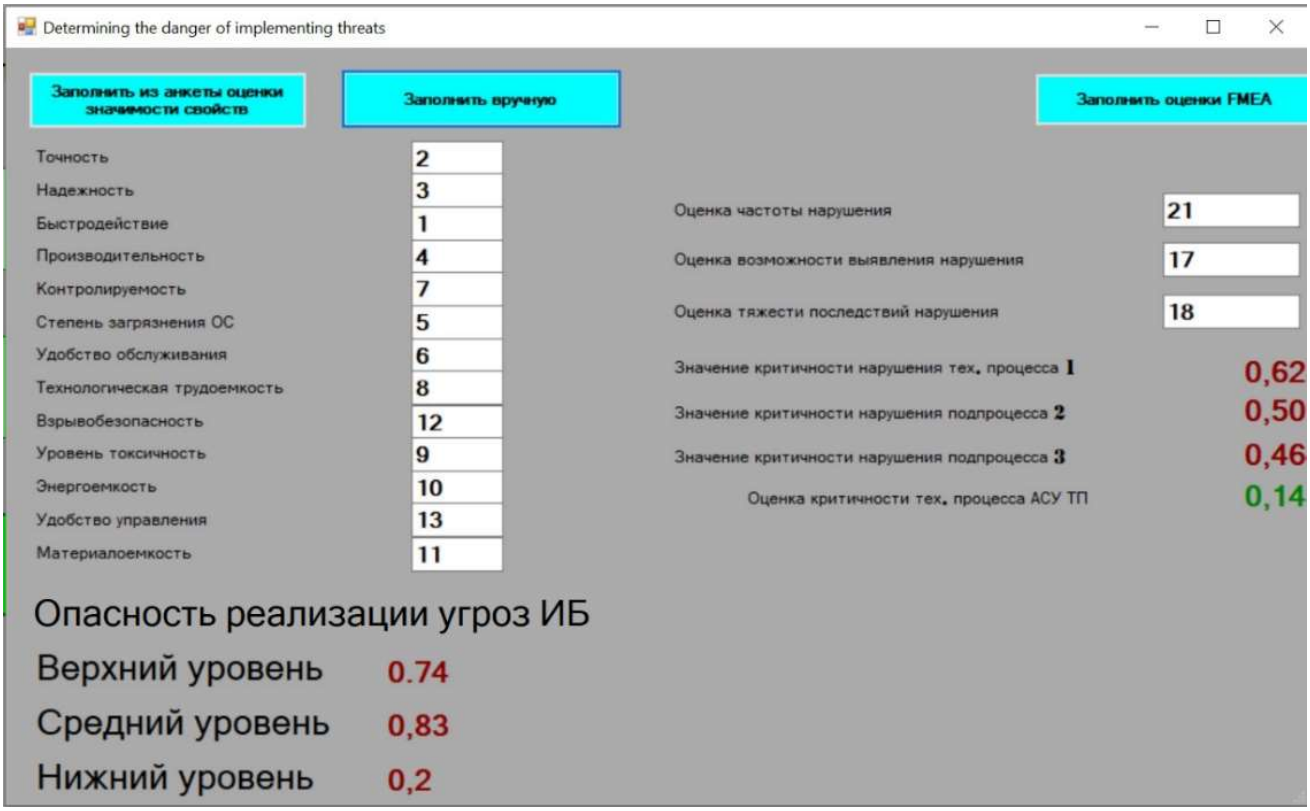


Рисунок 4.14 — Форма определения оценок опасности реализации угроз БИ

Модель угроз промышленной АСУ ТП формируется в АС «МУИБ» на форме Threat Model, представленной на рис. 4.15., на базе трех ключевых элементов: определения уязвимых мест АСУ ТП, оценки их защищенности и анализа степени опасности возможных угроз БИ. Нажатием кнопки *«Оценка опасности реализации угроз»* оператор получает числовые оценки и графическое отображение опасности реализации угроз БИ из перечня БДУ ФСТЭК, предустановленного в разработанном ПО. Нажатием кнопки *«БДУ ФСТЭК»* оператор имеет возможность загрузить актуальный перечень угроз БИ, представленный на электронном ресурсе https://bdu.fstec.ru/files/documents/thrlist.xlsx. Получение перечня актуальных угроз БИ для каждого из уровней АСУ ТП доступно оператору при нажатии на кнопку *«Актуальные угрозы»*.

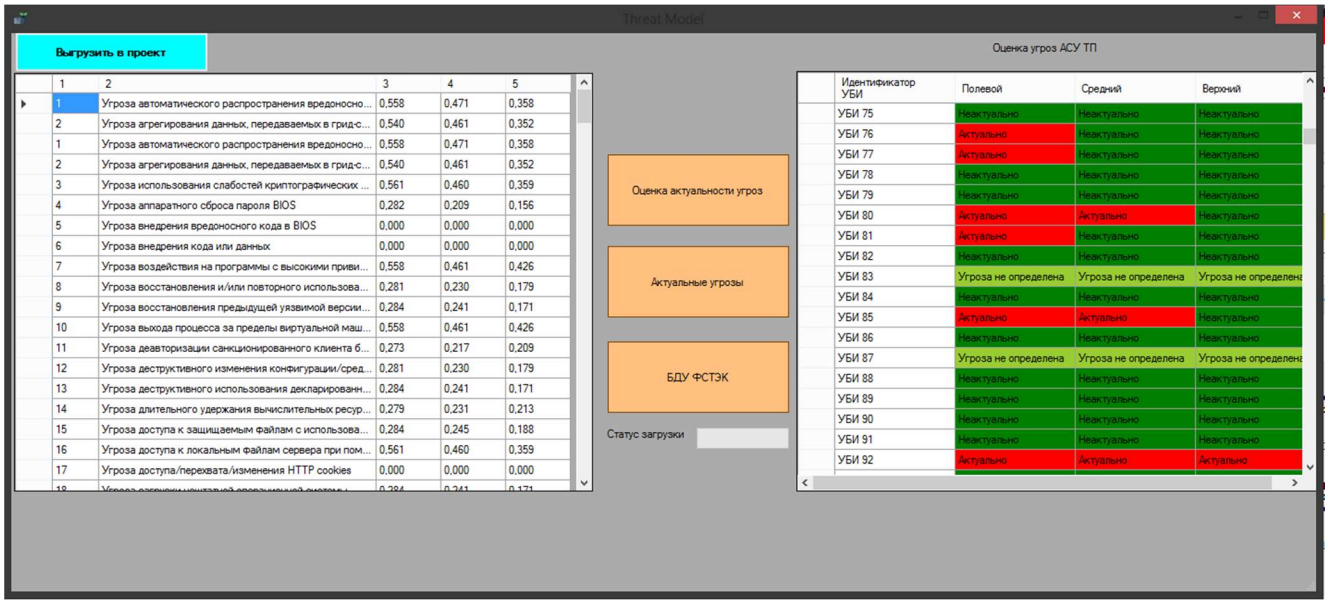


Рисунок 4.15 — Форма Threat Model АС «МУИБ»

Полученные результаты оценок угроз АСУ ТП в графическом виде, а также перечень актуальных угроз БИ выгружаются оператором в директорию проекта в виде файла *Threat_Model.xlsx* нажатием кнопки *«Выгрузить в проект»*.

Результаты оценки угроз и актуальные угрозы БИ, обследуемой с помощью АС «МУИБ» ОКИИ, представлены в таблицах 4.11 и приложении 5 диссертации. Результаты оценок угроз УБИ.003, УБИ.004, УБИ.005, УБИ.006 АСУ ТП в графическом виде с описанием расчётов оценок опасности для каждой из угроз представлены в приложении 6. Указанные расчеты с построением поверхностной диаграммы распределения оценок опасности реализации графа сценария реализации угрозы БИ строятся для каждой из угроз, представленных в БДУ ФСТЭК России.

Таблица 4.11 — актуальные угрозы БИ ОКИИ, полученные с применением АС «МУИБ»

Уровень ОКИИ	**Актуальные угрозы БИ**	
Верхний	**От внешних хакеров**	**От неквалифицированных внутренних нарушителей**
	УБИ.031; 065; 071; 089; 100; 113; 124; 145.	УБИ.031; 089; 090; 093; 157; 160; 179.
	От внешних	**От внутренних**

	неквалифицированных нарушителей	**нарушителей**
	УБИ. 071; 090; 157; 160.	УБИ. 005; 069; 113; 124; 145; 152.
Средний	**Угрозы от внешних хакеров**	**Угрозы от неквалифицированных внутренних нарушителей**
	УБИ.204; 206; 208.	УБИ.184; 209; 211.
	Угрозы от внешних неквалифицированных нарушителей	**Угрозы от внутренних нарушителей**
	УБИ.207; 209; 211.	УБИ. 005; 212.
Нижний	**Угрозы от внешних хакеров**	**Угрозы от неквалифицированных внутренних нарушителей**
	УБИ.027; 107.	УБИ.023; 027; 107.
	Угрозы от внешних неквалифицированных нарушителей	**Угрозы от внутренних нарушителей**
	УБИ.069; 099.	УБИ. 005.

Ниже на рисунке 4.16 представлен граф связей нарушителей БИ и актуальных угроз БИ для верхнего уровня АСУ ТП.

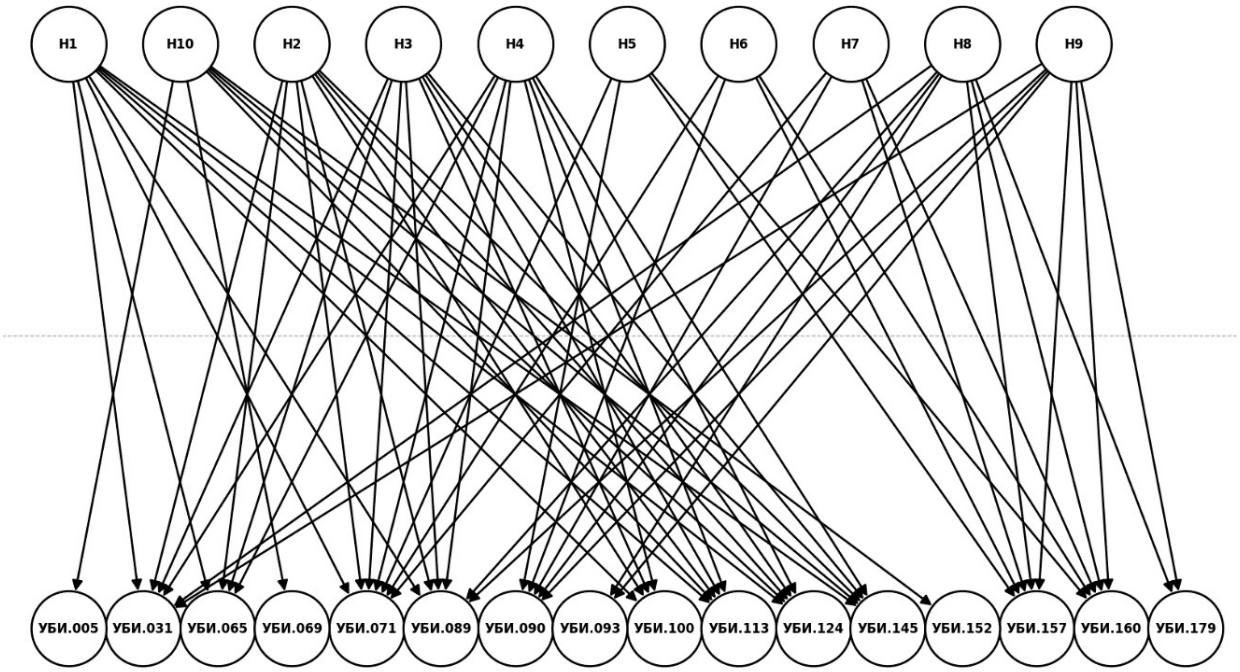


Рисунок 4.16 — Граф связи нарушителей и угроз БИ на верхнем уровне

По окончании процесса моделирования угроз БИ промышленной АСУ ТП с применением АС «МУИБ» оператором осуществляется переход к завершающему третьему этапу. Третий этап связан с выбором БН и АБН защитных мер АСУ ТП на основании модели, представленной в п. 3.3 диссертации. Выбор защитных мер проводится в процессе моделирования угроз промышленной АСУ ТП в целях минимизации последствий реализации обнаруженных актуальных угроз БИ на каждом из уровней АСУ ТП. Полученные результаты определения обобщенных классов защищенности каждого из уровней обследуемой промышленной АСУ ТП приводятся на форме Choice of protection measures (рис. 4.17).

Рисунок 4.17 — Форма Choice of protection measures АС «МУИБ»

Полученные обобщенные классы защищенности (ОК) в графическом виде выгружаются оператором в директорию проекта в виде файла *Protection_Measures.xlsx* нажатием кнопки *«Выгрузить в проект»*. Результаты определения УАБН ОК, обследуемого ОКИИ, представлены на рисунке 4.17. На основании полученных АБН и УАБН сформирован и представлен в таблице 4.12 перечень защитных мер, необходимых к внедрению в обследуемой промышленной АСУ ТП.

Таблица 4.12 — Перечень защитных мер, необходимых к внедрению

Уровень АСУ ТП	**Меры защиты**
Полевой	ИАФ.1; ИАФ.2; ИАФ.3; ИАФ.4; ИАФ.5; ИАФ.7; УПД.0; УПД.1; УПД.2; УПД.4; УПД.5; УПД.6; УПД.10; УПД.11; УПД.13; УПД.14; ЗНИ.0; ЗНИ.1; ЗНИ.2; ЗНИ.5; ЗНИ.7; ЗНИ.8; АУД.0; АУД.1; АУД.2; АУД.3; АУД.4; АУД.6; АУД.7; АУД.8; АУД.10; АВЗ.0; АВЗ.1; АВЗ.2; АВЗ.4; ОЦЛ.0; ОЦЛ.1; ОДТ.4; ОДТ.5; ОДТ.6; ОДТ.8; ЗТС.0; ЗТС.2; ЗТС.3; ЗТС.4; ЗТС.5; ЗИС.0; ЗИС.1; ЗИС.2; ЗИС.3; ЗИС.5; ЗИС.6; ЗИС.8; ЗИС.19; ЗИС.20; ЗИС.21; ЗИС.32; ЗИС.34; ЗИС.35; ЗИС.38; ЗИС.39; ИНЦ.0; ИНЦ.1; ИНЦ.2; ИНЦ.3; ИНЦ.4; ИНЦ.5; ИНЦ.6; УКФ.0; УКФ.2; УКФ.3; ОПО.1; ОПО.2; ОПО.3; ОПО.4; ПЛН.0; ПЛН.1; ПЛН.2; ДНС.0; ДНС.1; ДНС.2; ДНС.5; ИПО.0; ИПО.1; ИПО.2; ИПО.4.
Средний	Не требуется
Верхний	ИАФ.1; ИАФ.2; ИАФ.3; ИАФ.4; ИАФ.5; ИАФ.7; УПД.0; УПД.1; УПД.2; УПД.3; УПД.4; УПД.5; УПД.6; УПД.9; УПД.10; УПД.11; УПД.13; УПД.14; ОПС.0; ОПС.1; ОПС.2; ЗНИ.0; ЗНИ.1; ЗНИ.2; ЗНИ.5; ЗНИ.6; ЗНИ.7; ЗНИ.8; АУД.0; АУД.1; АУД.2; АУД.3; АУД.4; АУД.5; АУД.6; АУД.7; АУД.8; АУД.9; АУД.10; АВЗ.0; АВЗ.1; АВЗ.2; АВЗ.4; АВЗ.5; СОВ.0; СОВ.1; СОВ.2; ОЦЛ.0; ОЦЛ.1; ОЦЛ.3; ОЦЛ.4; ОЦЛ.5; ОДТ.0; ОДТ.1; ОДТ.2; ОДТ.3; ОДТ.4; ОДТ.5; ОДТ.6; ОДТ.8; ЗТС.0; ЗТС.2; ЗТС.3; ЗТС.4; ЗТС.5; ЗИС.0; ЗИС.1; ЗИС.2; ЗИС.3; ЗИС.4; ЗИС.5; ЗИС.6; ЗИС.8; ЗИС.13; ЗИС.16; ЗИС.19; ЗИС.20; ЗИС.21; ЗИС.27; ЗИС.32; ЗИС.33; ЗИС.34; ЗИС.35; ЗИС.38; ЗИС.39; ИНЦ.0; ИНЦ.1; ИНЦ.2; ИНЦ.3; ИНЦ.4; ИНЦ.5; ИНЦ.6; УКФ.0; УКФ.2; УКФ.3; ОПО.1; ОПО.2; ОПО.3; ОПО.4; ПЛН.0; ПЛН.1; ПЛН.2; ДНС.0; ДНС.1; ДНС.2; ДНС.3; ДНС.4; ДНС.5; ИПО.0; ИПО.1; ИПО.2; ИПО.4; ИПО.4.

После выполнения заключительного этапа моделирования угроз БИ ОКИИ на главном окне АС «МУИБ» формируются в графическом виде отображения базовых значений потенциалов нарушителей, оценки защищенности уязвимых звеньев, а также ОК, обследуемого ОКИИ в соответствии с рис. 4.18.

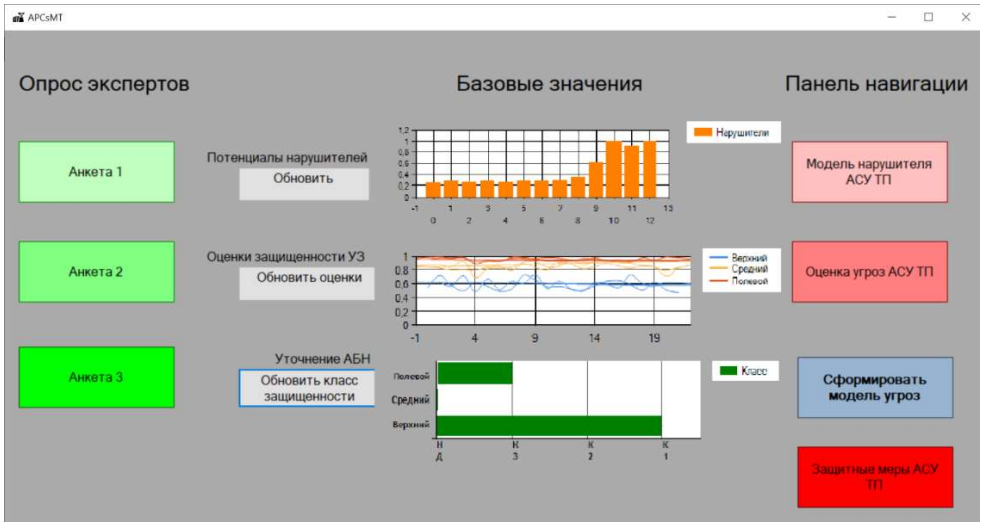


Рисунок 4.18 Графическое отображение сценариев реализации угроз БИ ОКИИ

Вышеперечисленные графические отображения сценариев реализации угроз БИ автоматически группируются в файл *Threat_Graph.xlsx* и добавляются в директорию проекта моделирования угроз. Таким образом, результатом моделирования угроз БИ ОКИИ - промышленной АСУ ТП, с применением АС «МУИБ» является директория проекта в памяти АРМ оператора с набором файлов формата *.xlsx, представленных на рис. 4.19.

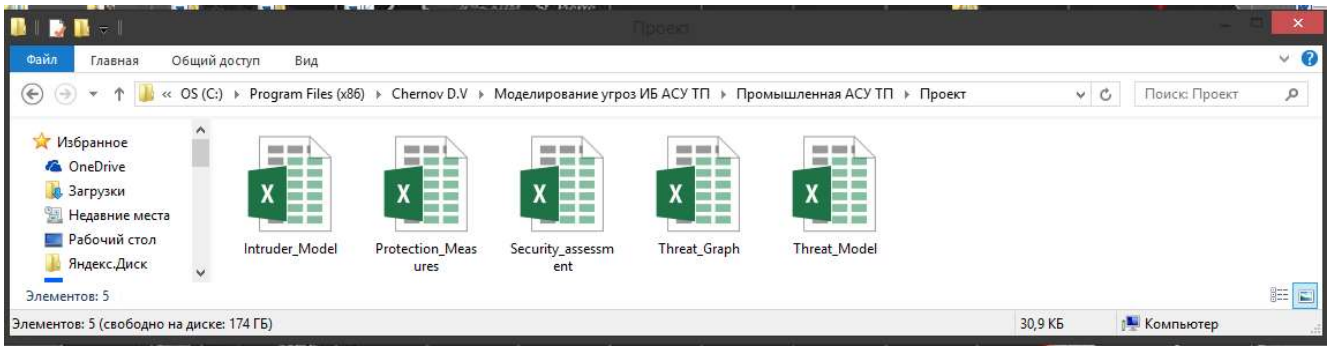


Рисунок 4.19 — Директория проекта моделирования угроз БИ

По результатам применения АС «МУИБ» для моделирования угроз БИ промышленной АСУ ТП выявлены 25 актуальных угроз. Общее количество мер защиты, необходимых для минимизации последствий реализации актуальных угроз БИ, – 201. На получение результатов моделирования угроз затрачено 30 человеко-часов.

В целях сравнительной оценки результатов моделирования угроз в условиях применения разработанной АС «МУИБ» с полученными результатами в рамках применения Методики ФСТЭК России от 05.02.2021г. и зарубежной методики TRIKE применена методология оценки показателя эффективности $ЭФ$ программного обеспечения, подробно описанная в работах [119 - 120].

$$ЭФ = \frac{\sum АУ + \sum МЗ}{ВЗ}, \tag{4.1}$$

где $\sum АУ = АУв + АУс + АУн$ — общее количество выявленных актуальных угроз для всех уровней ОКИИ; $\sum МЗ = МЗв + МЗс + МЗн$ — общее количество мер защиты предложенных для минимизации последствий реализации

актуальных угроз БИ; *ВЗ* — общее количество времени, затраченного на получение результатов моделирования угроз БИ.

Наибольшую эффективность продемонстрировала разработанная АС «МУИБ». Полученные результаты представлены в таблице.

Таблица 4.13 — Показатели эффективности моделирования угроз

Показатели	**Методика ФСТЭК**	**TRIKE**	**АС «МУИБ»**
$\sum АУ$ *ед.*	15	10	25
$\sum МЗ$ *ед.*	155	95	201
ВЗ час	59	66	30
ЭФ ед./час	2,88	1,59	7,53

Таким образом, экспериментально установлено, что разработанная АС «МУИБ» позволяет повысить эффективность моделирования угроз безопасности информации потенциальными нарушителями АСУ ТП с 2,88 до 7,66 (более чем в 2,6 раз) суммарного числа выявленных актуальных угроз и предложенных мер защиты в час по сравнению с методикой ФСТЭК и более чем в 4 раза по сравнению с зарубежной методикой TRIKE.

4.5 Выводы по четвертой главе

1. Разработанная на базе описанных в диссертации методов и алгоритмов АС «МУИБ» позволяет автоматизировать этапы построения моделей угроз ОКИИ с учетом специфики исполняемых технологических и (или) информационных процессов и нормативных документов в области обеспечения БИ ОКИИ. АС «МУИБ» объединяет подсистемы: «Построение модели нарушителя», «Оценки угроз», а также вспомогательных подсистем.

2. Апробация АС «МУИБ» показала его практическую пригодность при оценке угроз БИ ОКИИ субъектов критической информационной инфраструктуры.

3. В условиях неочевидности и недостатка данных АС «МУИБ» выступает инструментом поддержки для эксперта, сокращая время, затрачиваемое на

проведение необходимых мероприятий по моделированию угроз АСУ ТП и повысить их эффективность с 2,88 до 7,66 (более чем в 2,6 раз) суммарного числа выявленных актуальных угроз БИ и предложенных мер защиты в час по сравнению с рассмотренными методиками.

ЗАКЛЮЧЕНИЕ

В рамках диссертационного исследования были сформулированы и решены задачи, связанные с разработкой методических основ и алгоритмической базы для моделирования угроз БИ ОКИИ.

Основными научными и практическими результатами диссертационной работы являются:

1. Разработан метод определения потенциала нарушителя ИБ ОКИИ, основанный на применении матриц идентификаторов угроз, которые позволяют количественно описать степень опасности реализации угроз БИ для каждого из возможных нарушителей. Главным отличием от существующих методов является применение подхода к групповой оценке потенциалов нарушителей на основании вычислений матриц идентификаторов угроз.

2. Предложен метод количественной оценки степени опасности реализации угроз БИ ОКИИ, который в отличие от существующих имеет в основе оценки вероятностей реализации угроз БИ и ущерба от их реализации. Метод позволяет оценить степень опасности реализации угроз БИ потенциальным нарушителем ИБ по отношению к конкретной ИС, ИТКС или АСУ ТП. Разработанный метод дополняет располагаемые экспертные оценки, полученные от специалистов в области ИБ, путем формирования дополнительных экспертных оценок от привлекаемых специалистов-профессионалов в области функционирования системы.

3. Разработан алгоритм определения и оценки защищенности уязвимых звеньев ОКИИ. Алгоритм отличается от известных тем, что использует матрицу защищенности, составленную из оценок показателей защищенности отдельных уязвимых звеньев. Разработанный алгоритм позволяет повысить объективность оценки уровня защищенности ОКИИ.

4. Предложен алгоритм экспертной оценки степени опасности реализации угроз БИ ОКИИ. В отличие от существующих разработанный алгоритм основан на применении игр с несовершенной информацией вида «злоумышленник-система защиты информации», где в качестве возможных выигрышей сторон используются оценки потенциала нарушителя ИБ, опасности реализации им угроз БИ, а также оценки защищенности уязвимых звеньев, по отношении к которым потенциальный нарушитель реализует угрозы БИ. Предложенный алгоритм позволяет дополнять перечни актуальных угроз, выявленных с использованием известных методик ФСТЭК России.

5. Разработана структура и программное обеспечение автоматизированной системы моделирования угроз БИ ОКИИ. Результаты сравнительной оценки эффективности применения данной системы для конкретной промышленной АСУ ТП показали, что ее применение обеспечивает повышение показателя эффективности построения моделей угроз БИ по соотношению числа выявленных актуальных угроз БИ и предложенных мер защиты более, чем в 2,6 раз по сравнению с отечественной методикой ФСТЭК России, и более, чем в 4 раза по сравнению с зарубежной методикой TRIKE.

6. Результаты работы внедрены в производственные и бизнес-процессы обеспечения ИБ ряда предприятий: ООО «Комплексы системы и сети», АО ЦКБА, ООО «БД Безопасность», ФГБОУ ВО «Тульский государственный университет».

Дальнейшим развитием исследования может быть разработка на основе предложенных методов и алгоритмов системы противодействия угрозам БИ ОКИИ от реализации уязвимостей «нулевого дня». Результаты и выводы, полученные в диссертации, могут быть использованы для написания методических рекомендаций и учебных пособий.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ И УСЛОВНЫХ ОБОЗНАЧЕНИЙ

АБН – адаптированный базовый набор защитных мер

АРМ – автоматизированное рабочее место

АС «МУИБ» – автоматизированная система моделирования угроз информационной безопасности автоматизированных систем управления технологическими процессами

АСУ ТП – автоматизированная система управления технологическими процессами

БН – базовый набор защитных мер

ИБ – информационная безопасность

ИС – информационная сеть

ИТКС – информационно-телекоммуникационная сеть

КЗ – контролируемая зона

КИИ – критическая информационная инфраструктура

ЛВС – локальная вычислительная сеть

МН – минимальный набор защитных мер

ОКЗ – обобщенный класс защищенности

ОКИИ – объект критической информационной инфраструктуры

ПО – программное обеспечение

СЗИ – средства защиты информации

СНИ – съемный носитель информации

ТСПД – технологическая сеть передачи данных

УАБН – уточненный адаптированный базовый набор защитных мер

ФСТЭК – Федеральная служба по техническому и экспортному контролю

PLC (ПЛК) – программируемый логический контроллер

SCADA – диспетчерское управление и сбор данных

СПИСОК ЛИТЕРАТУРЫ

1. Федеральный закон №187-ФЗ от 26.07. 2017 г. «О безопасности критической информационной инфраструктуры Российской Федерации» // Собрание законодательства РФ. – 2017. – № 31 (часть I). – ст. 4736.
2. Christopher Caridi, John Dwyer. X-Force Threat Intelligence Index 2024. IBM Corporation. [Электронный ресурс]. – Режим доступа: https://newsletter.radensa.ru/wp-content/uploads/2024/03/IBM-XForce-Threat-Intelligence-Index-2024.pdf, свободный (дата обращения: 24.03.2025).
3. Positive Technologies. Актуальные киберугрозы: IV квартал 2023 года, [Электронный ресурс]. – Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2023-q4/ свободный (дата обращения: 24.03.2025).
4. Kaspersky ICS CERT. Ландшафт угроз для систем промышленной автоматизации Первый квартал 2025 года. [Электронный ресурс]. – Режим доступа: file:///C:/Users/CKBA/Downloads/kaspersky-ics-cert-threat-landscape-for-industrial-automation-systems-q1-2025-ru.pdf, свободный (дата обращения: 24.03.2025).
5. TXOne Networks. Annual OT/ICS Cybersecurity Report 2024. [Электронный ресурс]. – Режим доступа: https://digital.txone.com/media/txone-networks-2024-annual-ics-ot-cybersecurity- report/contents (дата обращения: 24.03.2025).
6. Positive Technologies. Актуальные угрозы кибербезопасности 3 квартал 2020 года. [Электронный ресурс]. – Режим доступа: https://www.ptsecurity.com/ ru-ru/research/analytics/cybersecurity-threatscape-2020-q3/#id5, свободный (дата обращения: 17.04.2025).
7. Leading U.S. laser developer IPG Photonics hit with ransomware. [Электронный ресурс]. – Режим доступа: https://www.bleepingcomputer.com/news/security/

leading-us-laser-developer-ipg-photonics-hit-with-ransomware, свободный (дата обращения: 18.05.2025).

8. Ландшафт угроз для систем промышленной автоматизации. Четвертый квартал 2024 – регионы. Kaspersky ICS CERT. [Электронный ресурс]. – Режим доступа: https://ics-cert.kaspersky.ru/publications/reports/2025/03/17/threat-landscape-for-industrial-automation-systems-regionsq4-2024/, свободный (дата обращения: 18.03.2025).
9. ЭАЦ ГК InfoWatch. Тенденции развития киберинцидентов АСУ ТП. Аналитический отчет за 2024 год. [Электронный ресурс]. – Режим доступа: https://www.infowatch.ru/sites/default/files/analytics/files/tendentsii-razvitiya-kiberintsidentov-asu-tp-za-dve-tysyachi-dvadtsat-chetyvertiy-god.pdf, свободный (дата обращения: 24.03.2025).
10. Каменских А.Н., Бортник Д.А. Анализ рекомендаций по защите автоматизированных систем управления с целью выявления типичных уязвимостей // Вестник Пермского национального исследовательского политехнического университета. Электротехника, информационные технологии, системы управления. – 2016. – № 17 – С. 48-60.
11. Горюхина Е. Ю. Информационная безопасность: учебное пособие / Горюхина Е.Ю., Литвинова Л.И., Ткачева Н.В. – Электрон. текстовые данные. – Воронеж: Воронежский Государственный Аграрный Университет им. Императора Петра Первого. – 2015. – 221 с.
12. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. – М.: Стандартинформ. – 2008. – 8 с.
13. Приказ ФСТЭК России от 25.12.2017 № 239. Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации. [Электронный ресурс]. – Режим доступа: https://fstec.ru/en/53-normotvorcheskaya/akty/prikazy/1592-prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239, свободный (дата обращения: 18.05.2025).

14. Новикова Е. Ф., Хализев В.Н. Разработка модели угроз для объектов критической информационной инфраструктуры с учетом методов социальной инженерии // Прикаспийский журнал: управление и высокие технологии. – 2019. – № 4(48). – С. 127-135. – DOI 10.21672/2074-1707.2019.48.4.127-135.
15. Кубланов М. С. Проверка адекватности математических моделей // Научный вестник Московского государственного технического университета гражданской авиации. – 2015. – № 211 (1) – С. 29-36.
16. Чернов Д.В., Сычугов А.А. Анализ современных требований и проблем обеспечения информационной безопасности автоматизированных систем управления технологическими процессами // Нейрокомпьютеры. Разработка, применение.М.: Радиотехника, – 2018. – №8. – С. 38-46.
17. Чебанов А.С., Жук Р.В. Модель нарушителя комплексной системы обеспечения ИБ объектов защиты // Известия Юго-Западного государственного университета. Серия: Управление, вычислительная техника, информатика. Медицинское приборостроение. – 2013. – № 1 – С. 171-173.
18. Политика безопасности информационных систем: учебно-методическое пособие / Белоусова Е.С., Буй П.М.; М-во трансп. и коммуникаций Респ. Беларусь, Белорус. гос. ун-т трансп. – Гомель: БелГУТ. – 2016. – 38 с.
19. Власенко А. В. Анализ характеристик определения нарушителя при моделировании угроз ИБ в информационных системах персональных данных / А. В. Власенко, Р. В. Жук // Электронный сетевой политематический журнал "Научные труды КубГТУ". – 2016. – № 16. – С. 99-104.
20. Методический документ ФСТЭК России. Методика определения угроз безопасности информации в информационных системах. [Электронный ресурс]. – Режим доступа: https://fstec.ru/component/attachments/download/2919, свободный (дата обращения 05.05.2025).

21. Сычев В.М. Формализация модели внутреннего нарушителя информационной безопасности // Вестник МГТУ им. Н.Э. Баумана. Сер. «Приборостроение». – 2015. – №2 – С. 92-106.
22. Шогенов Т. К. Вопросы технического обеспечения проведения оперативно-розыскного мероприятия «Снятие информации с технических каналов связи» // Спецтехника и связь. – 2013. – № 6 – С. 28-31.
23. Смык С.В. Анализ возможностей средств специального программно-технического воздействия // Перспективы развития информационных технологий. – 2014. – № 19 – С. 159-164.
24. Андреев Ю. С., Дергачев А. М., Жаров Ф. А. Информационная безопасность автоматизированных систем управления технологическими процессами // Известия высших учебных заведений. Приборостроение. – 2019. – Т. 62 – № 4 – С. 331-339.
25. Егошин Н.С. Модель угроз безопасности информации, передаваемой через Интернет / Егошин Н.С., Конев А.А., Шелупанов А.А. // Информация и безопасность. – 2018. – Т. 21 – № 4 – С. 530-533.
26. Скрыпников А.В., Попов А.Д., Рогозин Е.А. Экспериментальный метод определения вероятностно-временных характеристик систем защиты информации от несанкционированного доступа в автоматизированных информационных системах // Вестник Воронежского государственного университета инженерных технологий. – 2017. – Т. 79 – № 4 (74) – С. 90-96.
27. Богаченко Н.Ф. Анализ проблем управления разграничением доступа в крупномасштабных информационных системах // Математические структуры и моделирование. – 2018. – № 2 (46), – С. 135-152.
28. Головицына М. В. Методы, модели и алгоритмы в автоматизированной подготовке и оперативном управлении производством РЭС. Монография – Москва: ИНФРА-М. – 2019. – 276 с.

29. Парфеньева И.Е., Шмелева А.А. Оценка качества технологических процессов в системе менеджмента качества организации // Технические науки – от теории к практике. – 2015 – № 3 (40), – С. 119-129.
30. Технологические процессы в техническом сервисе машин и оборудования: учеб. пособие – М.: ИНФРА-М. – 2020. – 346 с.
31. Дербишер А.В. Управление технологическими процессами в машиностроении и приборостроении – М.: Издательство стандартов. – 1977. – 164 с.
32. Авсентьев А. О. Определение ценности информации // Доклады ТУСУР. – 2016. – №1. – С. 21-24..
33. В. И. Васильев. Система поддержки принятия решений по обеспечению информационной безопасности автоматизированной системы управления технологическими процессами / В. И. Васильев, В. Е. Гвоздев, М. Б. Гузаиров, А. Д. Кириллова // Информация и безопасность. – 2017. – Т. 20, № 4. – С. 618-623. – EDN ZSUJYN.
34. Гузаиров, М. Б. Разработка моделей принятия решений по оперативному управлению защитой информации на основе численной оценки вероятности атаки / М. Б. Гузаиров, И. В. Машкина, Т. Х. Тухватшин // Известия ЮФУ. Технические науки. – 2008. – № 8(85). – С. 18-24.
35. Васильев В. И., Вульфин А. М., Кучкарова Н. В. Методика оценки актуальных угроз и уязвимостей на основе технологий когнитивного моделирования и Text Mining // Системы управления, связи и безопасности. – 2021. – №3. – С. 110-134.
36. Жук Р. В. Методика и алгоритмы определения актуальных угроз информационной безопасности в информационных системах персональных данных: дис. канд. технических наук: 2.3.6. // Краснодар. – 2021. – 156 с.
37. Гузаиров М. Б. Сравнительный анализ алгоритмов когнитивного моделирования при оценке рисков информационной безопасности / М. Б. Гузаиров, А. М. Вульфин, В. М. Картак [и др.] // Труды Института

системного анализа Российской академии наук. – 2019. – Т. 69, № 4. – С. 62-69.

38. Кучкарова Н. В. Оценка актуальных угроз и уязвимостей объектов КИИ с использованием технологий интеллектуального анализа текстов: дис. канд. технических наук: 2.3.6. // Уфа. – 2023. – 183 С.
39. Машкина И. В. Идентификация угроз на основе построения семантической модели информационной системы // Вестник УГАТУ: Научный журнал. Серия «Управление, вычислительная техника и информатика». – 2008. – № 11 – С. 208-214.
40. Заид Алкилани М. О., Машкина И. В. Разработка сценариев атак для оценки угроз нарушения информационной безопасности в промышленной сети // Проблемы информационной безопасности. Компьютерные системы. – 2024. – № 1(58). – С. 96-109.
41. Chernov D.V., Sychugov A.A. Method of identifying and assessing of automated process control systems vulnerable elements // Proceedings of the 12th International Conference on Security of Information and Networks (SIN '19). ACM, New York, NY, USA, Article 19 – 2019. – DOI:10.1145/3357613.3357633.
42. Миняев А.А. Моделирование угроз безопасности информации в территориально-распределенных информационных системах // Наукоемкие технологии в космических исследованиях Земли. – 2021. – Т. 13. – № 2. – С. 52–65. Doi: 10.36724/2409-5419-2021-13-2-52-65
43. Chernov D.V. Application TRIKE Methodology When Modeling Threats to APCs Information SecurityAdvances in Automation III. RusAutoCon 2021 // Springer, Cham.Lecture Notes in Electrical Engineering. – 2022. – vol. 857 – DOI: 10.1007/ 978-3-030-94202-1.
44. Кендэл М. Ранговые корреляции. М. : Статистика. – 1975. – 218 с.
45. Кузьмин И.Е., Баранова Е. М., Борзенкова С.Ю. Разработка системы вычисления степени согласованности мнений экспертов в сфере информационной безопасности методом нахождения коэффициента

конкордации. Известия Тульского государственного университета. Технические науки. – 2020. – № 5. – С.11-18.

46. Приказ ФСТЭК России от 14.03.2014 г. № 31. Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на К, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды [Электронный ресурс]. – Режим доступа: URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/868-prikaz-fstek-rossii-ot-14-marta-2014-g-n-31, свободный (дата обращения 24.08.2023).
47. Суханов А. В. Нечеткие оценки защищенности информационных систем / А. В. Суханов // Информация и космос. – 2013. – № 1. – С. 107-110.
48. Костогрызов А. И. О моделях и методах вероятностного анализа защиты информации в стандартизованных процессах системной инженерии // Вопросы кибербезопасности. – 2022. – № 6(52). – С. 71-82. DOI 10.21681/2311-3456-2022-6-71-82.
49. Плетнев П.В. Алгоритмы и методики оценки угроз ИБ в сетях и системах телекоммуникаций: дис. канд. технических наук: 05.12.13 // – Новосибирск, – 2017. – 172 С.
50. Chernov D.V., Sychugov A.A. Determining the Hazard Quotient of Destructive Actions of Automated Process Control Systems Information Security Violator // 2020 International Russian Automation Conference. – 2020. – pp. 566-570, – DOI: 10.1109/RusAutoCon49822.2020.9208036.
51. Chernov D.V. Application of the method of determining the degree of danger of destructive actions to solve the problem of information security of APCs // 2020 International Conference on Electrotechnical Complexes and Systems. – 2020. – pp. 1-4, – DOI: 10.1109/ICOECS50468.2020.9278479.
52. Babeshko E., Kharchenko V. and Gorbenko A. Applying FMEA technique for SCADA-Based ICS Dependability Assessment and Ensuring", 2008 Third

International Conference on Dependability of Computer Systems DepCoS-RELCOMEX, – 2008. – DOI: 10.1109/DepCoS-RELCOMEX. 2008.23

53. Ажмухамедов И. М. Моделирование на основе экспертных суждений процесса оценки информационной безопасности // Вестник АГТУ. Серия: Управление, вычислительная техника и информатика. – 2009. – №2. – С. 22-29.
54. Малюк В. И. Производственный менеджмент: учебник для академического бакалавриата – М.: Издательство Юрайт. – 2019. – 249 С.
55. Федюкин В.К. Управление качеством производственных процессов: учеб. пособие – М.: КНОРУС. – 2012. – 232 С.
56. Мартынова М.В. Повышение эффективности управления технологическим процессом формирования структур интегральных элементов / Дисс. канд. техн. наук, спец. 05.13.06. – Владикавказ. 2– 011. – 139 С.
57. Буткевич Р.В., Клочков Ю.С., Яницкая Т.С. Методические основы количественного оценивания технологических процессов // Известия Самарского научного центра Российской академии наук. – 2005. – Т. 7 – №2 – С. 456-463.
58. Пичкалев А.В. Обобщенная функция желательности Харрингтона для сравнительного анализа технических средств // Космические аппараты и технологии. – 2012. – № 1 – С. 25-28.
59. Кравченко Е. Г., Забарина Т. Ю., Степанов А. А. Методика оценки качества технологических процессов // Современные материалы, техника и технологии. – 2016. – №. 1 (4) – С. 118-121.
60. Шарманов В.В., Романович М.А. Использование преобразованной функции желательности Харрингтона для расчета индекса качества строительного производства // Инженерный вестник Дона. – 2023. – № 10 (106), – С. 54-70.
61. Юсупова Г.Ф. Использование функции желательности в оценке уровня техносферной безопасности территории // Социально-экономические и

технические системы: исследование, проектирование, оптимизация. – 2017. – № 3 – С. 67-81.

62. Маслов Г.Г., Трубилин Е.И. Функция Харрингтона в исследованиях сельскохозяйственной техники // Таврический вестник аграрной науки. – 2022. – № 3(31). – С. 116–124.
63. Национальный стандарт РФ ГОСТ Р 56545-2015. Защита информации. Уязвимости информационных систем. Правила описания уязвимостей. (утв. приказом Федерального агентства по техническому регулированию и метрологии от 19 августа 2015 г. № 1180-ст).
64. Национальный стандарт РФ ГОСТ Р ИСО/МЭК 13335-1-2006. Информационная технология. Методы и средства обеспечения безопасности. (утв. приказом Федерального агентства по техническому регулированию и метрологии от 19 декабря 2006 г. № 317-ст).
65. ENISA Threat Landscape - The year in review. European Union Agency for Cybersecurity (ENISA). – 2020. – 26 p.
66. ISO/IEC 27005:2011. Information technology. Security techniques. Information security risk management (second edition). 2011. – Switzerland: ISO/IEC - 68 p. [Электронный ресурс]. – Режим доступа: https://www.iso.org/standard/56742.html, свободный (дата обращения: 15.10.2024).
67. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения информационной безопасности. Рекомендации в области стандартизации Банка России. РС БР ИББС-2.2-2009. [Электронный ресурс]. – Режим доступа: https://cbr.ru/statichtml/file/59420/st22_09.pdf, свободный (дата обращения: 16.10.2023).
68. Дрюков Н.Ю., Ермаков И.В., Ермаков Н.В. Методика построения модели угрозы информационной безопасности // Научно-технический вестник информационных технологий, механики и оптики. – 2008. – №. 51 – С. 181-185.

69. Поляничко М.А., Пунанова К.В. Оценивание актуальности инсайдерских угроз на основе нечеткого метода анализа иерархий // Вестник Воронежского института МВД России. – 2019. – № 3 – С. 88-98.
70. Анищенко В.В., Криштофик А.М. Комплексная Оценка угроз безопасности // Известия Южного федерального университета. Технические науки. – 2007. – Т. 76 – № 1 – С. 54-60.
71. Басалова Г.В. Применение методов теории игр в системах обнаружения вторжений // Известия ТулГУ. Технические науки. – 2017. №10 – С. 207–216.
72. Воронин В.В., Сухоруков Я.П. Аспекты разработки частной модели угроз безопасности информации в типовых информационных системах // Вестник Приамурского государственного университета им. Шолом-Алейхема. – 2020. – № 1 (38) – С. 24-33. – DOI: 10.24411/2227-1384-2020-10003.
73. Новожилова М.В., Овечко К.А. Применение теории игр в задачах информационной защиты // Харьков: Радиоэлектроника и информатика. – 2006. – №3 – С. 65-68.
74. Абраамян А.А. О некоторых моделях процессов управления информационной безопасностью финансовых систем // Автореферат диссертации на соискание ученой степени кандидата технических наук. [Электронный ресурс]. – Режим доступа: https://iiap.sci.am/pdf/ashot_abrahamyan.pdf, свободный (дата обращения: 07.02.2025).
75. L. Xiao, T. Chen, J. Liu. Anti-jamming trans-mission Stackelberg game with observation errors // IEEE Commun. Lett. – 2015. – vol. 19 – no. 6 – pp. 949-952
76. Chernov D.V., Sychugov A.A. Mathematical modeling of information security threats of automated process control systems. 2019 International Conference on Electrotechnical Complexes and Systems (ICOECS). – 2019. – pp. 1-4. – DOI:10.1109/ICOECS46375.2019.8950023
77. Гатчин Ю.А., Сухостат В.В. Теория информационной безопасности и методология защиты информации, – СПб.: СПбГУ ИТМО, 2010. – 98 с.

78. C. Zhang, L. Ge, Z. Zhong, X. You. Karnaugh map-aided combinational logic design approach with bistable molecular reactions // Proc. IEEE Intl. Conf. on Digital Signal Proc. (DSP). – 2015. – DOI: 10.1109/ICCAD.2013.6691194.
79. Жук Р.В. Способ определения потенциала нарушителя безопасности информации и реализуемых им уязвимостей программного обеспечения // Труды учебных заведений связи. – 2021. – №2. – С. 95–101.
80. Костин В.Н. Оценка потенциала опасности нарушителей на основе информационного метода и метода главных компонент // Информационные технологии и вычислительные системы. – 2016. – № 3 – С. 74–81.
81. Бусько М.М. Количественная оценка актуальности угроз информационной безопасности в проектируемых информационных системах // Современные тенденции в социально-экономических и гуманитарных науках: теория и практика: сборник научных трудов. – 2017. – С. 285-289.
82. Ряполова Е.И. Расчет уровня защищенности подсистемы конфиденциального документооборота на основе криптографических средств защиты // Norwegian Journal of Development of the International Science. – 2019. – № 34-1 – С. 48-52.
83. Чернов Д.В., Сычугов А.А. Определение коэффициента опасности деструктивных действий нарушителя информационной безопасности АСУ ТП // Фундаментальные проблемы управления производственными процессами в условиях перехода к индустрии 4.0. Челябинск: Издательский центр ЮУрГУ. – 2020. – С. 206-207.
84. Чернов Д.В., Сычугов А.А. Оценка действий нарушителя информационной безопасности автоматизированной системы управления технологическими процессами // Инновационные научные исследования в современном мире: теория, методология, практика. – 2020. – С. 64-69.
85. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. – М.: Стандартинформ. – 2008. – 12 С.

86. Frank Swiderski, Window Snyder. Threat Modeling // Microsoft Press. – 2004. – DOI: 10.1049/sbra011e_ch6.
87. Бегаев А.Н., Кашин С.В., Маркевич Н.А. Выявление уязвимостей и недекларированных возможностей в программном обеспечении – СПб: Университет ИТМО. – 2020. – 38 С.
88. Абрамова Т. В., Аралбаев Т. З. Анализ пространственно-временной модели угроз для распределенной автоматизированной системы управления процессом транспортировки нефтегазового сырья // Вестник УГАТУ. – 2020. – №1 (87). – С. 76-84.
89. National Infrastructure Protection Center. CyberNotes [Электронный ресурс]. – Режим доступа: http: // www.irational.org / APD / IPC / cyberissue4.pdf, свободный (дата обращения: 25.04.2025).
90. Дойникова Е.В., Чечулин А.А., Котенко И.В. Оценка защищенности компьютерных сетей на основе метрик cvss // Информационно-управляющие системы. – 2017. – №. 6 (91) – С. 76-87.
91. Федорченко А.В., Чечулин А.А., Котенко И.В. Исследование открытых баз уязвимостей и оценка возможности их применения в системах анализа защищенности компьютерных сетей // Информационно-управляющие системы. – 2014. – №. 5 (72) – С. 72-79.
92. Котенко И. В., Дойникова Е. В. Система оценки уязвимостей CVSS и ее использование для анализа защищенности компьютерных систем // Защита информации. Инсайд. – 2011. – № 5(41). – С. 54-60.
93. NCircle Vulnerability Scoring Document [Электронный ресурс]. – Режим доступа: http://index-of.es/z0ro-Repository-3/ncircle_vulnerability_scoring-2.pdf, свободный (дата обращения: 20.04.2025).
94. Котенко И. В., Хмыров С. С. Анализ моделей и методик, используемых для атрибуции нарушителей кибербезопасности при реализации целевых атак // Вопросы кибербезопасности. – 2022. – №4 (50). – С. 52-79.

95. Киздермишов А.А. К вопросу о применении CVE-совместимых сетевых сканеров // Вестник Адыгейского государственного университета. Серия 4: Естественно-математические и технические науки. – 2015. – №. 1 (154) – С. 136-140.
96. Киздермишов А.А. К вопросу о построении модели нарушителя правил разграничения доступа к пользовательским информационном ресурсам // Вестник Адыгейского государственного университета. Серия 4: Естественно-математические и технические науки. – 2015. – № 2(161) – С. 134-138.
97. Ожиганова М.И., Колесников А.В., Колодяжная А.Ю. Повышение уровня информационной защищенности корпоративной компьютерной сети за счет разработанных модулей сканирования сетевых ресурсов // Перспективы развития информационных технологий. – 2015. – № 24 – С. 183-190.
98. Кавчук Д.А., Матвеев Ю.Н. Автоматический анализ защищенности информационных систем без использования формальных спецификаций // Научно-технический вестник информационных технологий, механики и оптики. – 2017. – Т. 17 – № 3 – С. 431-438.
99. Дойникова Е.В., Котенко И.В. Оценивание защищенности и выбор контрмер для управления кибербезопасностью: монография. – М.: РАН, 2021. – 184 с.
100. Валеев С. С., Иерархическая динамическая система управления информационной безопасностью информационной системы предприятия / С. С. Валеев, Н. В. Кондратьева, М. Б. Гузаиров, А. С. Исмагилова // Инженерный вестник Дона. – 2023. – № 11(107). – С. 154-164.
101. Медведев Н.В., Троицкий И. И., Цирлов В.Л. К вопросу об использовании аппарата теории нечетких множеств при анализе рисков информационной безопасности // Вестник Московского государственного технического университета им. Н. Э. Баумана. Серия «Приборостроение». – 2011. – С. 25-30.
102. Ненадович Д.М., Шахтарин Б.И. Методы теории нечетких множеств в задачах безопасности инфокоммуникационных сетей // Вестник Московского

государственного технического университета им. Н. Э. Баумана. Серия «Приборостроение». – 2006. – №. 3 – С. 88-96.

103. Vijay Sarvepalli. Practical Math for Your Security Operations. [Электронный ресурс]. – Режим доступа: URL: https://insights.sei.cmu.edu/blog/practical-math-for-your-security-operations-part-1-of-3/, свободный (дата обращения: 24.05.2025).
104. Вавичкин Н. А. Математические модели в информационной безопасности // Безопасность информационного пространства 2017: XVI Всероссийская научно-практическая конференция студентов, аспирантов, молодых ученых – Екатеринбург: Изд-во Урал. ун-та, 2018. – С. 148-150.
105. Чернов Д.В. О выборе мер обеспечения информационной безопасности автоматизированных систем управления технологическими процессами. Моделирование, оптимизация и информационные технологии. – 2021. – 9(2). – С. 1-9. – DOI: 10.26102/2310-6018/2021.33.2.016.
106. Селифанов В.В., Степанова С.В., Чернов Д.В. Особенности выбора средств защиты информации в государственных информационных системах // Известия тульского государственного университета. Технические науки. – 2018. – Вып. 10. – С. 18-21.
107. Белова Е.А. Уровни саморазвития личности в контексте использования электронно-образовательных ресурсов // Вестник Тамбовского университета. Серия: Гуманитарные науки. – 2015. – № 6 (146) – С. 17-27.
108. РД 50-680-88. Методические указания. Автоматизированные системы. Основные положения. [Электронный ресурс]. – Режим доступа: https://docs.cntd.ru/document/1200006976, свободный (дата обращения: 21.04.2025).
109. Бурлаков М.Е. Двухклассификационная искусственная иммунная система Вестник Самарского государственного университета. – 2014. – № 7 (118) – С. 207-220.
110. Селифанов В. В., Звягинцева П. А. Применение методов автоматизации при определении актуальных угроз безопасности информации в

информационных система с применением банка данных угроз ФСТЭК России // Интерэкспо Гео-Сибирь. – 2017. – № 1. – С. 202-209.

111. Бражук А.И. Структура методики моделирования угроз компьютерных систем на основе предметно-ориентированных моделей // Компьютерные технологии и анализ данных (CTDA’2020) : материалы II Междунар. науч.-практ. конф., Минск, 23–24 апр. 2020 г. / БГУ, 2020. – С. 220-224.
112. Шибанов С.В. Моделирование активных правил в нотации IDEF0 // Труды Международного симпозиума «Надежность и качество». – 2012. – Т. 1 – С. 436-438.
113. Зимовец О.А. Представление диаграмм в нотациях DFD, IDEF0 и BPMN с помощью системно-объектных моделей «Узел-функция-объект» // Экономика. Информатика. – 2011. – Т. 114 № 19-1 – С. 133–144.
114. Горбаченко В.И., Убиенных Г.Ф., Бобрышев Г.В. Проектирование информационных систем с CA ERwin Modeling Suite 7.3: учебное пособие. – Пенза: Изд-во ПГУ, 2012. – 154 с.
115. Kapulin D., Russkikh P. and Moor, I. Application solution for preparing business processes information for the 1C: Enterprise platform using ERwin process modeler \\ Journal of Physics: Conference Series. – 2019. – pp1333. – DOI: 10.1088/1742-6596/1333/7/072008.
116. Шикуть А.В., Аристов Б.К., Просуков Е.А. Особенности. Достоинства и преимущества использования C# в приложениях // Символ науки. – 2016. – № 11-3 – С. 180-185.
117. Денискин А.В. Многопоточность в языке программирования C# // Academy. – 2017. – № 2 (17) – С. 21-24.
118. Горбылев А.Л. Адаптированная модель угроз безопасности информации в ключевых системах информационных инфраструктур. // Сборник статей международной научно-практической конференции автоматизация: проблемы, идеи, решения. – 2017. – Т. 1 – С. 35-43.

119. Зацаринный А.А., Ионенков Ю.С. Некоторые аспекты оценки эффективности информационных систем // Системы и средства информации. – 2016. – № 26 (3) – С. 122-135.
120. Булыгина О.В., Емельянов А.А. Системный анализ в управлении: учеб. пособие. Под ред. д-ра экон. наук, проф. Емельянова А.А.. – 2-е изд., перераб. и доп. – М.: ФОРУМ: ИНФРА-М, 2017. – 450 с.
121. Дроботун Е.Б., Цветков О.В. Построение модели угроз безопасности информации в автоматизированной системе управления критически важными объектами на основе сценариев действий нарушителя // Программные продукты и системы. – 2016. – № 3 (115), – С. 42-50.

ПРИЛОЖЕНИЕ 1.

Анкета опроса для выявления потенциальных нарушителей БИ ОКИИ

№ п/п	Содержание вопроса (способ реализации угроз БИ)	Ответ	Тип нарушителя БИ[1]									
			Н1	Н2	Н3	Н4	Н5	Н6	Н7	Н8	Н9	Н10
1.	Имеются ли у субъекта КИИ конкуренты?											
2.	Возможно ли наличие недоброжелателей у руководителей субъекта КИИ или его сотрудников либо у субъекта в целом, которые из личных или корыстных побуждений могут быть заинтересованы в получении информации, обрабатываемой в ОКИИ, либо нарушении его функционирования?											
3.	Имеется ли в ОКИИ информация, которая может заинтересовать иностранные спецслужбы?											
4.	Имеются ли в составе сотрудников субъекта КИИ люди, лояльность которых вызывает сомнение, неудовлетворенные условиями работы, оплаты, подлежащие увольнению?											
5.	Имеется ли в ОКИИ информация, которая может представлять интерес для криминальных элементов?											
6.	Имеются ли в составе сотрудников субъекта КИИ люди, увлекающиеся хакерством (составлением специальных программ взлома защиты компьютерных систем) или способные к этому?											
7.	Возможны ли катастрофические последствия или нарушение систем											

[1] Тип нарушителя «Хакеры или группировки хакеров» рассматривается для ОКИИ, имеющих подключение к внешним информационным системам или сетям

	обеспечения в результате нарушения работы ОКИИ?											
8.	Могут ли сотрудники субъекта КИИ устанавливать или запускать ПО, не входящее в перечень разрешенного?											
9.	Используется ли в ОКИИ несертифицированное программное обеспечение, разработанное на заказ внешними организациями?											
10.	Производится ли периодический выпуск и установка обновлений ПО в ОКИИ?											
11.	Разрабатывают ли сотрудники субъекта КИИ собственное прикладное ПО для внедрения в ОКИИ?											
12.	Имеются ли подрядные организации (контрагенты), сотрудники которых регулярно проводят техническое обслуживание, установку или настройку ПО, иное обслуживание и ремонтно-восстановительные работы серверов, АРМ и ТСПД?											
13.	Имеются ли сотрудники субъекта КИИ, которые проводят техническое обслуживание, установку или настройку ПО, иное обслуживание и ремонтно-восстановительные работы серверов, АРМ и сетевого оборудования?											
14.	Имеется ли доступ к сети Интернет или сетям общего пользования из ТСПД ОКИИ либо внешним ИС и ИТКС?											
15.	Имеет ли обслуживающий персонал (техники, уборщицы и т.д.), доступ в помещения, где расположены компоненты ОКИИ?											

ПРИЛОЖЕНИЕ 2.

Лист экспертного ранжирования свойств технологических и (или) информационных процессов ОКИИ

Тех./ инф. процесс	**Свойство процесса**	**Ранг**
Тех. процесс	точность	
	надежность	
	быстродействие	
	производительность	
	контролируемость	
	степень загрязнения окружающей среды	
	удобство обслуживания	
	технологическая трудоемкость	
	взрывобезопасность	
	уровень токсичности	
	энергоемкость	
	удобство управления	
	материалоемкость	
Инф. процесс	Достоверность	
	Полнота	
	Актуальность (своевременность)	
	Доступность	
	Конфиденциальность	
	Целостность	
	Управляемость	
	Эффективность	
	Масштабируемость	
	Надежность	

ПРИЛОЖЕНИЕ 3.

Опросная анкета оценки применяемых мер безопасности для уязвимых звеньев ОКИИ

Вопрос	**Ответ для верхнего уровня**	**Ответ для среднего уровня**	**Ответ для нижнего уровня**	**Индекс уязвимого звена**	**Наименование уязвимого звена / *компонент объектов воздействия***
Используются ли сотрудниками субъекта КИИИ отчуждаемые гибкие диски, жесткие диски, системы хранения данных СХД, флэш-карты?				УЗ 1	Отчуждаемые носители информации (флеш-накопители, оптические компакт-диски) *К.2.3 Устройство хранения данных* *К.2.3.1 Система хранения данных* *К.2.3.2 Съемный машинный носитель информации*
Используются ли в составе ОКИИ серверы и АРМ со средствами ввода информации?				УЗ 2	Средства ввода информации (клавиатуры, мыши, порты и др.) *К.2.1 Периферийное оборудование* *К.2.1.1Принтер* *К.2.1.2 Монитор* *К.2.1.3 Мышь* *К.2.1.4 Клавиатура* *К.2.1.5 Микрофон* *К.2.1.6 Веб-камера К.2.1.7 Другие периферийные устройства*
Используются ли сотрудниками субъекта КИИ дисководы и программные средства записи CD, DVD-дисков в ОКИИ?				УЗ 3	Дисководы оптических компакт-дисков *К.2.1.7 Другие периферийные устройства (IP-камеры и др.)*
Используется ли в ОКИИ множительная техника,				УЗ 4	Принтеры *К.2.1 Периферийное оборудование*

подключаемая к АРМ (принтеры, плоттеры и др.)?					*К.2.1.1Принтер*
Используются ли в составе ОКИИ средства отображения информации (мониторы, информационные дисплеи и др.)?				УЗ 5	Средства отображения информации (мониторы, информационные дисплеи и др.) *К.2.1 Периферийное оборудование* *К.2.1.2 Монитор*
Используются ли в составе ОКИИ средства обработки информации (ОЗУ, ЦП, контроллеры внешних устройств и др.)?				УЗ 6	Средства обработки информации (ОЗУ, ЦП, контроллеры внешних устройств и др.) *К.1 Программное обеспечение* *К.1.1Микропрограммное обеспечение* *К.1.1.1Прошивка (встроенная микропрограмма)*
Возможен ли неконтролируемый доступ к коммутационным элементам ТСПД (маршрутизаторы, коммутаторы, концентраторы и др.)?				УЗ 7	Коммутационные элементы сети, к которым имеется физический доступ *К.2.4 Программно-аппаратное средство защиты информации* *К.2.4.1 Система доверенной загрузки* *К.2.4.3Межсетевой экран* *К.2.4.4Средство обнаружения (предотвращения) вторжений* *К.2.4.5Другие средства защиты информации*
Отсутствуют специальные коробы для прокладки кабелей локальной сети?				УЗ 8	Кабели компьютерной сети на участках, где имеется к ним физический доступ *К.3.1Канал передачи данных* *К.3.1.1Проводной канал передачи данных*
Не обеспечивается физическая и криптографическ				УЗ 9	Незащищённые каналы связи и оборудование *К.2.4 Программно-*

ая защита каналов связи и оборудования за пределами КЗ?					*аппаратное средство защиты информации К.2.4.2Криптошлюз*
На объекте отсутствует система бесперебойного электропитания?				УЗ 10	Система электропитания *К.1.6.7Другие средства защиты информации*
Аппаратные СЗИ не применяются или применяются частично?				УЗ 11	Не применяются аппаратные СЗИ *К.2.5 Интерфейсы сервисного обслуживания устройства К.2.5.1Распаянные на плате интерфейсы*
Периодический выпуск и установка обновлений ПО технических средств не производится?				УЗ 12	Небезопасные технические средства *К.1.4 Инструментальное ПО К.1.4.1 ПО для разработки кода К.1.4.2 Средства тестирования и отладки*
Используются ли в составе ОКИИ серверы и рабочие станции с микросхемами базовой системы ввода/вывода?				УЗ 13	Микросхемы базовой системы ввода/вывода (BIOS/UEFI) *К.1.1.2 UEFI/BIOS К.2.2 Интерфейсы ввода/вывода К.2.2.1 Интерфейс подключения клавиатуры К.2.2.2 Интерфейс подключения мыши К.2.2.3 Интерфейс подключения монитора К.2.2.4 Интерфейс подключения проектора К.2.2.5 Интерфейс подключения аудиоустройства К.2.2.6 Интерфейс подключения принтера/сканнера/МФУ К.2.2.7 Датчики К.2.2.8 Сетевой интерфейс*
Периодический выпуск и установка				УЗ 14	Операционная система *К.1.2 Системное программное обеспечение*

обновлений ОС, серверов, АРМ, ПЛК и другого оборудования ОКИИ не производится?					*(ПО)* *К.1.2.4 Драйвер* *К.1.2.5 Утилита*
ОС ОКИИ не имеют сертификатов соответствия требованиям по защите информации?				УЗ 15	Недокументированная точка входа в ОС *К.1.2 Системное программное обеспечение (ПО)* *К.1.2.1 Операционная система* *К.1.2.2 Мобильная операционная система* *К.1.2.3 Программная оболочка* *К.1.2.6 Загрузчик операционной системы*
Используется ли сотрудниками субъекта КИИ или администраторам и ПО, не предназначенное для выполнение должностных обязанностей или запрещенное к использованию (нештатное программное обеспечение)?				УЗ 16	Нештатное дополнительное ПО *К.1.5 Прикладное ПО* *К.1.5.1 Клиент электронной почты* *К.1.5.2 Мессенджер* *К.1.5.3 Среда управления контейнеризацией* *К.1.5.4 Виртуальная машина* *К.1.5.6 Мобильное приложение* *К.1.5.7 Скрипт автоматизации* *К.1.5.8 Система мониторинга* *К.1.5.9 Клиент системы видеоконференцсвязи* *К.1.5.10 Клиент IP-телефонии* *К.1.5.11 Пакет офисного ПО* *К.1.5.12 ПО для проектирования и моделирования* *К.1.5.13 Система управления предприятием* *К.1.5.14 Контейнер* *К.1.5.15 Веб-браузер*
Имеются ли у пользователей				УЗ 17	Доступные файлы со служебной информацией

права локального администратора?					(системный журнал учетных записей пользователей и т.д.) *К.4.2Непривилегированные пользователи* *К.4.2.1Непривилегированный сотрудник*
Имеет ли ОКИИ доступ к сети Internet или Шлюз выхода в сеть Internet или сети общего пользования?				УЗ 18	Шлюз выхода в сеть Internet или сети общего пользования *К.1.3.3 Веб-сервер* *К.2.4.3Межсетевой экран*
Имеется ли взаимодействие ОКИИ с внешними ИС и сетями связи?				УЗ 19	Уязвимости протоколов межсетевого взаимодействия прикладного уровня *К.1.7 Веб-приложение* *К.1.7.1 Веб-сайт* *К.1.7.2 Веб-клиент* *К.1.7.3 Веб-интерфейс администрирования* *К.1.7.4 Другие примеры веб-приложений*
Развернуты ли в ТСПД общие сетевые ресурсы?				УЗ 20	Открытые общие сетевые ресурсы *К.3.1 Канал передачи данных* *К.3.1.1 Проводной канал передачи данных* *К.3.1.2 Беспроводной канал передачи данных*
Имеются ли у пользователей административные привилегии на уровне домена?				УЗ 21	Доступный системный реестр, системные папки *К.1.3.11 Система распределенного реестра*
В ОКИИ не применяются программные СЗИ, в том числе сертифицированные?				УЗ 22	Не применяются программные СЗИ на серверах, АРМ, контроллерах и другом оборудовании ОКИИ *К.1.6 Программное средство защиты информации* *К.1.6.1 Антивирусные средства* *К.1.6.2 Агент системы защиты*

					К.1.6.3 Межсетевой экран уровня приложений *К.1.6.4 ПО системы резервного копирования* *К.1.6.5 Средства разграничения и управления доступом* *К.1.6.6 Средства анализа защищенности* *К.1.6.7 Другие СЗИ*
Программно-аппаратный комплекс сетевых устройств не сертифицирован по требованиям безопасности?				УЗ 23	Сетевая операционная система, сетевые драйверы *К.1.2.7 Гипервизор* *К.1.3 Сервисное ПО* *К.1.3.1 Системные и сетевые службы* *К.1.3.2 Терминальный сервер* *К.1.3.3 Веб-сервер* *К.1.3.4 Система управления содержимым сайта (CMS)* *К.1.3.5 Файловый сервер* *К.1.3.6 Сервер электронной почты* *К.1.3.7 Сервер видеоконференцсвязи* *К.1.3.8 Сервер IP-телефонии* *К.1.3.9 DNS-сервер* *К.1.3.10 Сервер каталогов*
Какой стек протоколов используется для сетевого взаимодействия?				УЗ 24	Уязвимости сетевых протоколов (TCP/IP, Modbus TCP/RTU) *К.3.2 Протокол передачи данных* *К.3.2.1 Протоколы аутентификации* *К.3.2.2 Протоколы обмена данными* *К.3.2.3 Другие примеры протоколов*
Разрабатываются ли сотрудниками прикладные программы?				УЗ 25	Прикладное программное обеспечение *Программное обеспечение (программы)*
Используются ли в ТСПД ОКИИ облачные				УЗ 26	Незащищенная информация пользователя *Объекты файловой*

технологии обработки данных?					*системы*
В ОКИИ применяются СУБД?				УЗ 27	Базы данных и системы управления ими *К.1.5.5 Система управления базами данных (СУБД)*
Используются ли в составе ОКИИ серверы и АРМ с нелицензионным ПО?				УЗ 28	Нелицензионные программные продукты *К.1.5.11 Пакет офисного ПО* *К.1.5.12 ПО для проектирования и моделирования* *К.1.5.13 Система управления предприятием* *К.1.6.1 Антивирусные средства*
Отсутствуют ли средства контроля действий администраторов ОКИИ и администраторов ИБ?				УЗ 29	Процедура обхода администратором ОКИИ установленных правил и режимов безопасности *К.4.1 Привилегированные пользователи* *К.4.1.1 Администратор* *К.4.1.2 Разработчик* *К.4.1.3 Тестировщик* *К.4.1.4 Модератор* *К.4.1.5 Сотрудник технической поддержки*
Имеются ли процедуры обхода (невыполнения) пользователями сети установленных правил и режимов безопасности?				УЗ 30	Процедура обхода (невыполнения) пользователями сети установленных правил и режимов безопасности *К.4.2Непривилегированные пользователи* *К.4.2.1Непривилегированный сотрудник* *К.4.2.2Клиент организации*

ПРИЛОЖЕНИЕ 4.

Результаты оценки актуальности угроз БИ, обрабатываемой в ОКИИ - промышленная АСУ ТП в соответствии с методикой ФСТЭК РФ

УБИ.005: Угроза внедрения вредоносного кода в BIOS	
Негативные последствия	НК, НЦ, НД
Источник угрозы	Внутренней нарушитель с высоким потенциалом
Объект воздействия	Микропрограммное и аппаратное обеспечение BIOS/UEFI
Сценарий	Внедрение нарушителем в дискредитируемую автоматизированную систему вредоносного кода, который может быть в дальнейшем запущен «вручную» пользователями, автоматически при выполнении определённого условия (наступления определённой даты, входа пользователя в систему и т.п.) или с использованием аутентификационных данных, заданных «по умолчанию», а также возможность несанкционированного внедрения нарушителем некоторых собственных данных для обработки в дискредитируемую автоматизированную систему, фактически осуществив незаконное использование чужих вычислительных ресурсов и блокирование работы устройства при выполнении определенных команд
Способ реализации	Использование уязвимостей программного обеспечения; Слабость мер антивирусной защиты и разграничения доступа; Работа дискредитируемого пользователя с файлами, поступающими из недоверенных источников; Наличие у нарушителя привилегий установки программного обеспечения
УБИ.067: Угроза неправомерного ознакомления с защищаемой информацией	
Негативные последствия	НК
Источник угрозы	Внутренний нарушитель (Н1)
Объект воздействия	АРМ пользователей (аппаратное обеспечение, объекты файловой системы)

Сценарий	Неправомерное случайное или преднамеренное ознакомление пользователя с информацией, которая для него не предназначена, и дальнейшее её использование для достижения своих или заданных ему другими лицами (организациями) деструктивных целей. Реализация данной угрозы не подразумевает установку и использование нарушителем специального вредоносного программного обеспечения. При этом ознакомление может быть проведено путём просмотра информации с экранов мониторов других пользователей, с отпечатанных документов, путём подслушивания разговоров и др.
Способ реализации	Использование уязвимостей средств контроля доступа, ошибок в параметрах конфигурации данных средств или отсутствие указанных средств
УБИ.071: Угроза несанкционированного восстановления удалённой защищаемой информации	
Негативные последствия	НК
Источник угрозы	Внешний нарушитель (H1), Внутренний нарушитель (H1)
Объект воздействия	Машинный носитель информации
Сценарий	Осуществление прямого доступа (доступа с уровней архитектуры более низких по отношению к уровню операционной системы) к данным, хранящимся на машинном носителе информации, или восстановление данных по считанной с машинного носителя остаточной информации
Способ реализации	Слабости механизма удаления информации с машинных носителей – информация, удалённая с машинного носителя, в большинстве случаев может быть восстановлена. Технологические особенности машинного носителя информации не приводят к гарантированному уничтожению информации при получении команды на стирание данных;
УБИ.089: Угроза несанкционированного редактирования реестра	
Негативные последствия	НК, НЦ, НД
Источник угрозы	Внешний нарушитель (H1), Внутренний нарушитель (H1)
Объект воздействия	АРМ пользователей (системное программное обеспечение, использующее реестр)
Сценарий	Внесение нарушителем изменений в используемый дискредитируемым приложением реестр, которые влияют на функционирование отдельных сервисов приложения или приложения в целом. При этом под реестром понимается не только реестр операционной системы Microsoft Windows, а любой реестр, используемый приложением. Изменение реестра может быть как этапом при осуществлении другого деструктивного воздействия, так и основной целью

Способ реализации	Использование слабостей механизма контроля доступа, заключающихся в присвоении реализующим его программам слишком высоких привилегий при работе с реестром. Получение нарушителем прав на работу с программой редактирования реестра.
УБИ.090: Угроза несанкционированного создания учётной записи пользователя	
Негативные последствия	НК, НЦ, НД
Источник угрозы	Внешний нарушитель (H1), Внутренний нарушитель (H1)
Объект воздействия	АРМ пользователей (системное ПО)
Сценарий	Создание нарушителем в системе дополнительной учётной записи пользователя и её дальнейшее использование в собственных неправомерных
Способ реализации	Использование слабостей механизмов разграничения доступа к защищаемой информации. Наличие прав на запуск специализированных программ для редактирования файлов, содержащих сведения о пользователях системы (при удалённом доступе) или штатных средств управления доступом из состава операционной системы (при локальном доступе)
УБИ.093: Угроза несанкционированного управления буфером	
Негативные последствия	НК, НЦ, НД
Источник угрозы	Внешний нарушитель (H1), Внутренний нарушитель (H1)
Объект воздействия	АРМ пользователей (системное ПО, прикладное ПО, сетевое ПО)
Сценарий	Осуществление нарушителем несанкционированного доступа к данным, содержащимся в буфере обмена, в интересах ознакомления с хранящейся там информацией или осуществление деструктивного программного воздействия на систему (например, переполнение буфера для выполнения произвольного вредоносного кода)
Способ реализации	Использование слабостей в механизме разграничения доступа к буферу обмена, а также слабости в механизмах проверки вводимых данных. Осуществление нарушителем успешного несанкционированного доступа к сегменту оперативной памяти дискредитируемого объекта, в котором расположен буфер обмена
УБИ.145: Угроза пропуска проверки целостности программного обеспечения	
Негативные последствия	НЦ, НД
Источник	Внешний нарушитель (H1), Внутренний нарушитель (H1)

угрозы	
Объект воздействия	АРМ пользователей (системное ПО, прикладное ПО, сетевое ПО)
Сценарий	Внедрение нарушителем в дискредитируемую систему вредоносного программного обеспечения путём обманного перенаправления запросов пользователя или его программ на собственный сетевой ресурс, содержащий вредоносное программное обеспечение, для его «ручной» или «автоматической» загрузки с последующей установкой в дискредитируемую систему от имени пользователя или его программ. Использование обманных техник одного из следующих методов: «ручного метода» – нарушитель, используя обманные механизмы, убеждает пользователя перейти по ссылке на сетевой ресурс нарушителя, что приводит к запуску вредоносного кода на компьютере пользователя; «автоматического метода» – нарушитель осуществляет деструктивное воздействие переадресацию функции автоматического обновления дискредитируемой программы на собственный вредоносный сервер
Способ реализации	Использование слабостей механизмов проверки целостности файлов программного обеспечения и/или проверки подлинности источника их получения
УБИ.113: Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники	
Негативные последствия	НЦ, НД
Источник угрозы	Внешний нарушитель (Н1), Внутренний нарушитель (Н1)
Объект воздействия	АРМ пользователей (системное ПО, аппаратное обеспечение)
Сценарий	Сброс пользователем (нарушителем) состояния оперативной памяти (обнуление памяти) путём случайного или намеренного осуществления перезагрузки отдельных устройств, блоков или системы в целом. Реализация данной угрозы возможна как аппаратным способом (нажатием кнопки), так и программным (локально или удалённо)
Способ реализации	Свойство оперативной памяти обнулять своё состояние при выключении и перезагрузке. Наличие в системе открытых сессий работы пользователей; Наличие у нарушителя прав в системе (или физической возможности) на осуществление форсированной перезагрузки
УБИ.124: Угроза подделки записей журнала регистрации событий	
Негативные последствия	НЦ
Источник угрозы	Внешний нарушитель (Н1), Внутренний нарушитель (Н1)

Объект воздействия	АРМ пользователей (системное ПО)
Сценарий	Внесение нарушителем изменений в журналы регистрации событий безопасности дискредитируемой системы (удаление компрометирующих нарушителя записей или подделка записей о непроизошедших событиях) для введения в заблуждение её администраторов или сокрытия следов реализации других угроз
Способ реализации	Технология ведения журналов регистрации событий безопасности предполагает возможность их редактирования, и нарушитель обладает необходимыми для этого привилегиями, или технология ведения журналов регистрации событий безопасности не предполагает возможность их редактирования, но нарушитель обладает привилегиями, необходимыми для осуществления записи в файлы журналов, а также специальными программными средствами, способными обрабатывать файлы журналов используемого в дискредитируемой системе формата
УБИ.157: Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	
Негативные последствия	НЦ НД
Источник угрозы	Внешний нарушитель (Н1)
Объект воздействия	АРМ пользователей (носитель информации, аппаратное обеспечение)
Сценарий	Умышленное выведение из строя внешним нарушителем средств хранения, обработки и (или) ввода/вывода/передачи информации, что может привести к нарушению доступности, а в некоторых случаях и целостности защищаемой информации
Способ реализации	Использование слабостей мер контроля физического доступа к средствам хранения, обработки и (или) ввода/вывода/передачи информации. Получение нарушителем физического доступа к носителям информации (внешним, съёмным и внутренним накопителям), средствам обработки информации (процессору, контроллерам устройств и т.п.) и средствам ввода/вывода информации (клавиатура и т.п.)
УБИ.160: Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации	
Негативные последствия	НК, НД
Источник угрозы	Внешний нарушитель (Н1)
Объект воздействия	АРМ пользователей (носитель информации, аппаратное обеспечение)

Сценарий	Осуществление внешним нарушителем кражи компьютера (и подключённых к нему устройств), USB-накопителей, оптических дисков или других средств хранения, обработки, ввода/вывода/передачи информации
Способ реализации	Слабости мер контроля физического доступа к средствам хранения, обработки и (или) ввода/вывода/передачи информации. Наличие у нарушителя физического доступа к носителям информации (внешним, съёмным и внутренним накопителям), средствам обработки информации (процессору, контроллерам устройств и т.п.) и средствам ввода/вывода информации (клавиатура и т.п.)
УБИ.179: Угроза несанкционированной модификации защищаемой информации	
Негативные последствия	НЦ
Источник угрозы	Внешний нарушитель (H1), Внутренний нарушитель (H1)
Объект воздействия	АРМ пользователей (объекты файловой системы)
Сценарий	Нарушение целостности защищаемой информации путём осуществления нарушителем деструктивного физического воздействия на машинный носитель информации или деструктивного программного воздействия (в т.ч. изменение отдельных бит или полное затирание информации) на данные, хранящиеся на нём
Способ реализации	Получение нарушителем системных прав на запись данных или физического доступа к машинному носителю информации на расстояние, достаточное для оказания эффективного деструктивного воздействия
УБИ.031: Угроза использования механизмов авторизации для повышения привилегий	
Негативные последствия	НК
Источник	Внешний нарушитель (H1), Внутренний нарушитель (H1)
Объект воздействия	АРМ пользователей (системное ПО, прикладное ПО, сетевое ПО)
Сценарий	Получение нарушителем доступа к данным и функциям, предназначенным для учётных записей с более высокими, чем у нарушителя привилегиями, за счёт ошибок в параметрах настройки средств разграничения доступа. При этом нарушитель для повышения своих привилегий не осуществляет деструктивное программное воздействие на систему, а лишь использует существующие ошибки
Способ реализации	Использование слабостей мер разграничения доступа к программам и файлам. Наличие у нарушителя каких-либо привилегий в системе

ПРИЛОЖЕНИЕ 5.

Результаты оценки угроз БИ ОКИИ - промышленной АСУ ТП, полученные с применением АС «МУИБ»

Идентификатор	Верхний уровень	Средний уровень	Полевой уровень
УБИ.001	Угроза не определена	Угроза не определена	Угроза не определена
УБИ.002	Угроза не определена	Угроза не определена	Угроза не определена
УБИ.003	Угроза не определена	Угроза не определена	Угроза не определена
УБИ.004	Угроза не определена	Угроза не определена	Угроза не определена
УБИ.005	Актуально	Актуально	Актуально
УБИ.006	Неактуально	Неактуально	Неактуально
УБИ.007	Неактуально	Неактуально	Неактуально
УБИ.008	Неактуально	Неактуально	Неактуально
УБИ.009	Неактуально	Неактуально	Неактуально
УБИ.010	Неактуально	Неактуально	Неактуально
УБИ.011	Неактуально	Неактуально	Неактуально
УБИ.012	Неактуально	Неактуально	Неактуально
УБИ.013	Неактуально	Неактуально	Неактуально
УБИ.014	Неактуально	Неактуально	Неактуально
УБИ.015	Неактуально	Неактуально	Неактуально
УБИ.016	Неактуально	Неактуально	Неактуально
УБИ.017	Угроза не определена	Угроза не определена	Угроза не определена
УБИ.018	Неактуально	Неактуально	Неактуально
УБИ.019	Угроза не определена	Угроза не определена	Угроза не определена
УБИ.020	Неактуально	Неактуально	Неактуально
УБИ.021	Угроза не определена	Угроза не определена	Угроза не определена
УБИ.022	Неактуально	Неактуально	Неактуально
УБИ.023	Неактуально	Неактуально	Актуально
УБИ.024	Угроза не определена	Угроза не определена	Угроза не определена
УБИ.025	Неактуально	Неактуально	Неактуально
УБИ.026	Угроза не определена	Угроза не определена	Угроза не определена
УБИ.027	Угроза не определена	Угроза не определена	Актуально
УБИ.028	Неактуально	Неактуально	Неактуально
УБИ.029	Неактуально	Неактуально	Неактуально
УБИ.030	Неактуально	Неактуально	Неактуально
УБИ.031	Актуально	Неактуально	Неактуально
УБИ.032	Неактуально	Неактуально	Неактуально
УБИ.033	Неактуально	Неактуально	Неактуально
УБИ.034	Неактуально	Неактуально	Неактуально
УБИ.035	Неактуально	Неактуально	Неактуально
УБИ.036	Неактуально	Неактуально	Неактуально
УБИ.037	Неактуально	Неактуально	Неактуально
УБИ.038	Неактуально	Неактуально	Неактуально
УБИ.039	Неактуально	Неактуально	Неактуально

УБИ.040	Угроза не определена	Угроза не определена	Угроза не определена
УБИ.041	Угроза не определена	Угроза не определена	Угроза не определена
УБИ.042	Неактуально	Неактуально	Неактуально
УБИ.043	Неактуально	Неактуально	Неактуально
УБИ.044	Неактуально	Неактуально	Неактуально
УБИ.045	Неактуально	Неактуально	Неактуально
УБИ.046	Неактуально	Неактуально	Неактуально
УБИ.047	Неактуально	Неактуально	Неактуально
УБИ.048	Неактуально	Неактуально	Неактуально
УБИ.049	Неактуально	Неактуально	Неактуально
УБИ.050	Неактуально	Неактуально	Неактуально
УБИ.051	Неактуально	Неактуально	Неактуально
УБИ.052	Угроза не определена	Угроза не определена	Угроза не определена
УБИ.053	Неактуально	Неактуально	Неактуально
УБИ.054	Угроза не определена	Угроза не определена	Угроза не определена
УБИ.055	Неактуально	Неактуально	Неактуально
УБИ.056	Угроза не определена	Угроза не определена	Угроза не определена
УБИ.057	Неактуально	Неактуально	Неактуально
УБИ.058	Неактуально	Неактуально	Неактуально
УБИ.059	Неактуально	Неактуально	Неактуально
УБИ.060	Неактуально	Неактуально	Неактуально
УБИ.061	Неактуально	Неактуально	Неактуально
УБИ.062	Угроза не определена	Угроза не определена	Угроза не определена
УБИ.063	Неактуально	Неактуально	Неактуально
УБИ.064	Неактуально	Неактуально	Неактуально
УБИ.065	Актуально	Неактуально	Неактуально
УБИ.066	Угроза не определена	Угроза не определена	Угроза не определена
УБИ.067	Неактуально	Неактуально	Неактуально
УБИ.068	Неактуально	Неактуально	Неактуально
УБИ.069	Актуально	Неактуально	Актуально
УБИ.070	Неактуально	Неактуально	Неактуально
УБИ.071	Актуально	Неактуально	Неактуально
УБИ.072	Неактуально	Неактуально	Неактуально
УБИ.073	Неактуально	Неактуально	Неактуально
УБИ.074	Неактуально	Неактуально	Неактуально
УБИ.075	Неактуально	Неактуально	Неактуально
УБИ.076	Неактуально	Неактуально	Неактуально
УБИ.077	Неактуально	Неактуально	Неактуально
УБИ.078	Неактуально	Неактуально	Неактуально
УБИ.079	Неактуально	Неактуально	Неактуально
УБИ.080	Неактуально	Неактуально	Неактуально
УБИ.081	Неактуально	Неактуально	Неактуально
УБИ.082	Неактуально	Неактуально	Неактуально
УБИ.083	Угроза не определена	Угроза не определена	Угроза не определена
УБИ.084	Неактуально	Неактуально	Неактуально
УБИ.085	Неактуально	Неактуально	Неактуально
УБИ.086	Неактуально	Неактуально	Неактуально
УБИ.087	Угроза не определена	Угроза не определена	Угроза не определена
УБИ.088	Неактуально	Неактуально	Неактуально

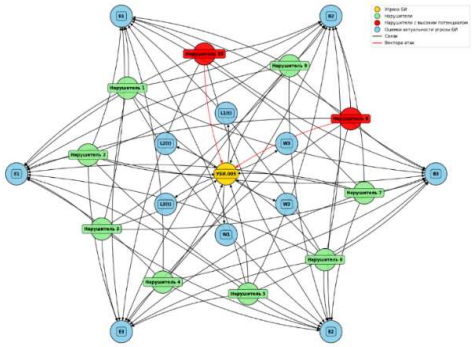
УБИ.089	Актуально	Неактуально	Неактуально
УБИ.090	Актуально	Неактуально	Неактуально
УБИ.091	Неактуально	Неактуально	Неактуально
УБИ.092	Неактуально	Неактуально	Неактуально
УБИ.093	Актуально	Неактуально	Неактуально
УБИ.094	Неактуально	Неактуально	Неактуально
УБИ.095	Неактуально	Неактуально	Неактуально
УБИ.096	Неактуально	Неактуально	Неактуально
УБИ.097	Неактуально	Неактуально	Неактуально
УБИ.098	Угроза не определена	Угроза не определена	Угроза не определена
УБИ.099	Угроза не определена	Угроза не определена	Актуально
УБИ.100	Актуально	Неактуально	Неактуально
УБИ.101	Неактуально	Неактуально	Неактуально
УБИ.102	Неактуально	Неактуально	Неактуально
УБИ.103	Угроза не определена	Угроза не определена	Угроза не определена
УБИ.104	Угроза не определена	Угроза не определена	Угроза не определена
УБИ.105	Неактуально	Неактуально	Неактуально
УБИ.106	Неактуально	Неактуально	Неактуально
УБИ.107	Угроза не определена	Угроза не определена	Актуально
УБИ.108	Неактуально	Неактуально	Неактуально
УБИ.109	Неактуально	Неактуально	Неактуально
УБИ.110	Неактуально	Неактуально	Неактуально
УБИ.111	Неактуально	Неактуально	Неактуально
УБИ.112	Неактуально	Неактуально	Неактуально
УБИ.113	Актуально	Неактуально	Неактуально
УБИ.114	Неактуально	Неактуально	Неактуально
УБИ.115	Неактуально	Неактуально	Неактуально
УБИ.116	Угроза не определена	Угроза не определена	Угроза не определена
УБИ.117	Неактуально	Неактуально	Неактуально
УБИ.118	Неактуально	Неактуально	Неактуально
УБИ.119	Неактуально	Неактуально	Неактуально
УБИ.120	Неактуально	Неактуально	Неактуально
УБИ.121	Угроза не определена	Угроза не определена	Угроза не определена
УБИ.122	Неактуально	Неактуально	Неактуально
УБИ.123	Неактуально	Неактуально	Неактуально
УБИ.124	Актуально	Неактуально	Неактуально
УБИ.125	Угроза не определена	Угроза не определена	Угроза не определена
УБИ.126	Угроза не определена	Угроза не определена	Угроза не определена
УБИ.127	Неактуально	Неактуально	Неактуально
УБИ.128	Угроза не определена	Угроза не определена	Угроза не определена
УБИ.129	Неактуально	Неактуально	Неактуально
УБИ.130	Угроза не определена	Угроза не определена	Угроза не определена
УБИ.131	Неактуально	Неактуально	Неактуально
УБИ.132	Неактуально	Неактуально	Неактуально
УБИ.133	Угроза не определена	Угроза не определена	Угроза не определена
УБИ.134	Неактуально	Неактуально	Неактуально
УБИ.135	Неактуально	Неактуально	Неактуально
УБИ.136	Неактуально	Неактуально	Неактуально
УБИ.137	Неактуально	Неактуально	Неактуально

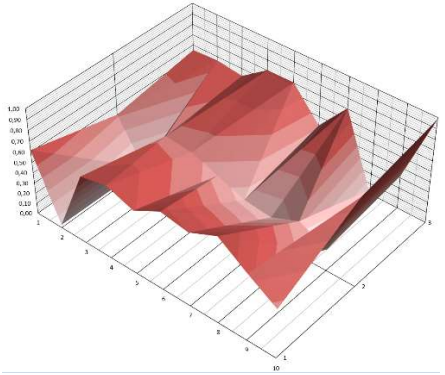
УБИ.138	Неактуально	Неактуально	Неактуально
УБИ.139	Неактуально	Неактуально	Неактуально
УБИ.140	Неактуально	Неактуально	Неактуально
УБИ.141	Неактуально	Неактуально	Неактуально
УБИ.142	Угроза не определена	Угроза не определена	Угроза не определена
УБИ.143	Неактуально	Неактуально	Неактуально
УБИ.144	Неактуально	Неактуально	Неактуально
УБИ.145	Актуально	Неактуально	Неактуально
УБИ.146	Неактуально	Неактуально	Неактуально
УБИ.147	Неактуально	Неактуально	Неактуально
УБИ.148	Угроза не определена	Угроза не определена	Угроза не определена
УБИ.149	Неактуально	Неактуально	Неактуально
УБИ.150	Неактуально	Неактуально	Неактуально
УБИ.151	Угроза не определена	Угроза не определена	Угроза не определена
УБИ.152	Актуально	Неактуально	Неактуально
УБИ.153	Неактуально	Неактуально	Неактуально
УБИ.154	Неактуально	Неактуально	Неактуально
УБИ.155	Неактуально	Неактуально	Неактуально
УБИ.156	Неактуально	Неактуально	Неактуально
УБИ.157	Актуально	Неактуально	Неактуально
УБИ.158	Неактуально	Неактуально	Неактуально
УБИ.159	Угроза не определена	Угроза не определена	Угроза не определена
УБИ.160	Актуально	Неактуально	Неактуально
УБИ.161	Неактуально	Неактуально	Неактуально
УБИ.162	Неактуально	Неактуально	Неактуально
УБИ.163	Неактуально	Неактуально	Неактуально
УБИ.164	Неактуально	Неактуально	Неактуально
УБИ.165	Неактуально	Неактуально	Неактуально
УБИ.166	Неактуально	Неактуально	Неактуально
УБИ.167	Неактуально	Неактуально	Неактуально
УБИ.168	Угроза не определена	Угроза не определена	Угроза не определена
УБИ.169	Неактуально	Неактуально	Неактуально
УБИ.170	Угроза не определена	Угроза не определена	Угроза не определена
УБИ.171	Угроза не определена	Угроза не определена	Угроза не определена
УБИ.172	Угроза не определена	Угроза не определена	Угроза не определена
УБИ.173	Угроза не определена	Угроза не определена	Угроза не определена
УБИ.174	Угроза не определена	Угроза не определена	Угроза не определена
УБИ.175	Угроза не определена	Угроза не определена	Угроза не определена
УБИ.176	Угроза не определена	Угроза не определена	Угроза не определена
УБИ.177	Неактуально	Неактуально	Неактуально
УБИ.178	Неактуально	Неактуально	Неактуально
УБИ.179	Актуально	Неактуально	Неактуально
УБИ.180	Угроза не определена	Угроза не определена	Угроза не определена
УБИ.181	Неактуально	Неактуально	Неактуально
УБИ.182	Неактуально	Неактуально	Неактуально
УБИ.183	Неактуально	Неактуально	Неактуально
УБИ.184	Неактуально	Актуально	Неактуально
УБИ.185	Неактуально	Неактуально	Неактуально
УБИ.186	Неактуально	Неактуально	Неактуально

УБИ.187	Неактуально	Неактуально	Неактуально
УБИ.188	Неактуально	Неактуально	Неактуально
УБИ.189	Неактуально	Неактуально	Неактуально
УБИ.190	Неактуально	Неактуально	Неактуально
УБИ.191	Неактуально	Неактуально	Неактуально
УБИ.192	Неактуально	Неактуально	Неактуально
УБИ.193	Неактуально	Неактуально	Неактуально
УБИ.194	Неактуально	Неактуально	Неактуально
УБИ.195	Неактуально	Неактуально	Неактуально
УБИ.196	Неактуально	Неактуально	Неактуально
УБИ.197	Неактуально	Неактуально	Неактуально
УБИ.198	Неактуально	Неактуально	Неактуально
УБИ.199	Неактуально	Неактуально	Неактуально
УБИ.200	Неактуально	Неактуально	Неактуально
УБИ.201	Неактуально	Неактуально	Неактуально
УБИ.202	Неактуально	Неактуально	Неактуально
УБИ.203	Неактуально	Неактуально	Неактуально
УБИ.204	Неактуально	Актуально	Неактуально
УБИ.205	Угроза не определена	Угроза не определена	Угроза не определена
УБИ.206	Неактуально	Актуально	Неактуально
УБИ.207	Неактуально	Актуально	Неактуально
УБИ.208	Угроза не определена	Актуально	Угроза не определена
УБИ.209	Неактуально	Актуально	Неактуально
УБИ.210	Неактуально	Неактуально	Неактуально
УБИ.211	Неактуально	Актуально	Неактуально
УБИ.212	Неактуально	Актуально	Неактуально
УБИ.213	Неактуально	Неактуально	Неактуально
УБИ.214	Неактуально	Неактуально	Неактуально
УБИ.215	Неактуально	Неактуально	Неактуально
УБИ.216	Неактуально	Неактуально	Неактуально
УБИ.217	Неактуально	Неактуально	Неактуально
УБИ.218	Неактуально	Неактуально	Неактуально
УБИ.219	Неактуально	Неактуально	Неактуально
УБИ.220	Неактуально	Неактуально	Неактуально
УБИ.221	Неактуально	Неактуально	Неактуально
УБИ.222	Неактуально	Неактуально	Неактуально

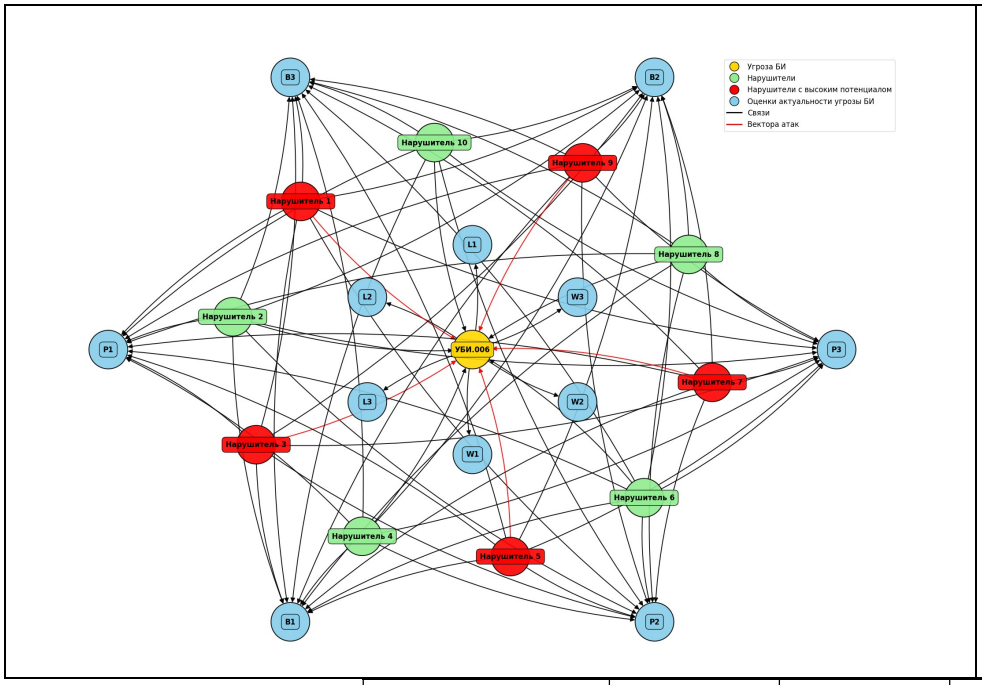
ПРИЛОЖЕНИЕ 6.

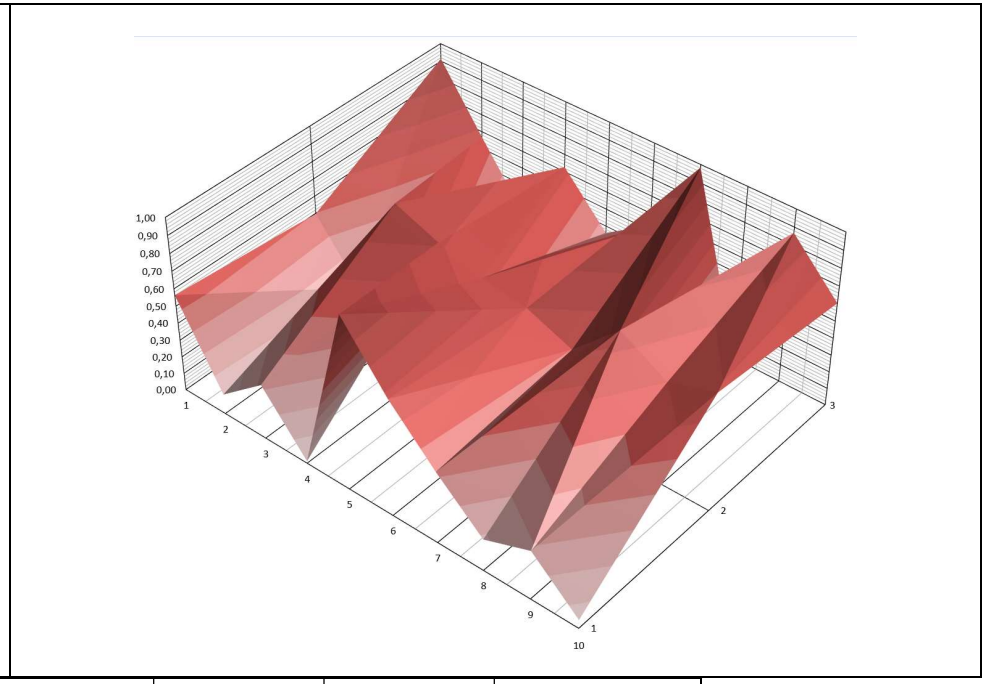
Описание оценок угроз БИ, полученных с применением АС «МУИБ»



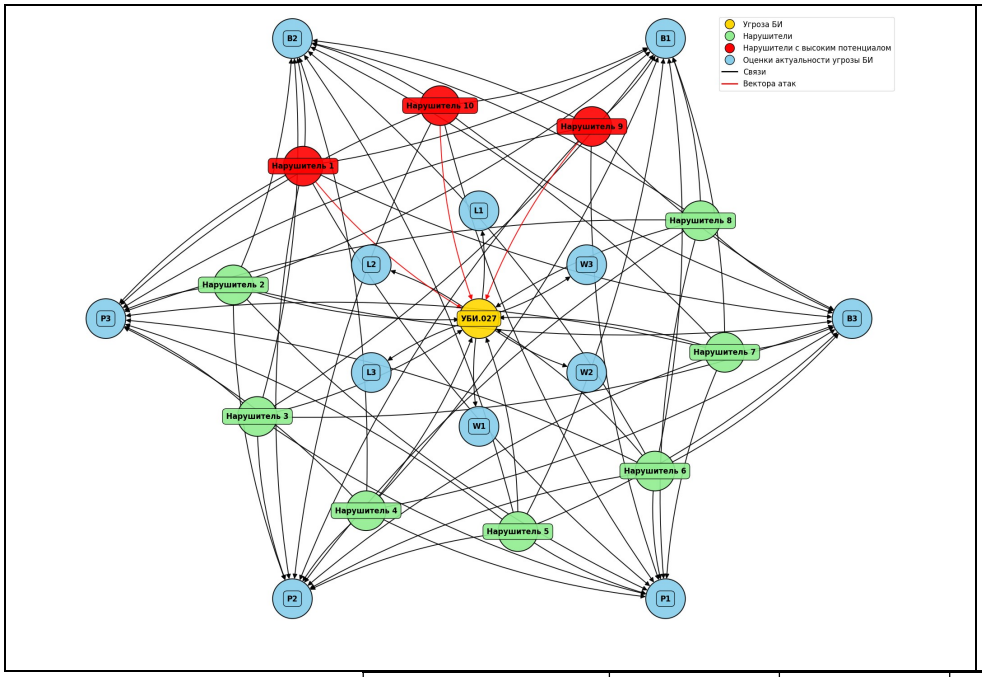


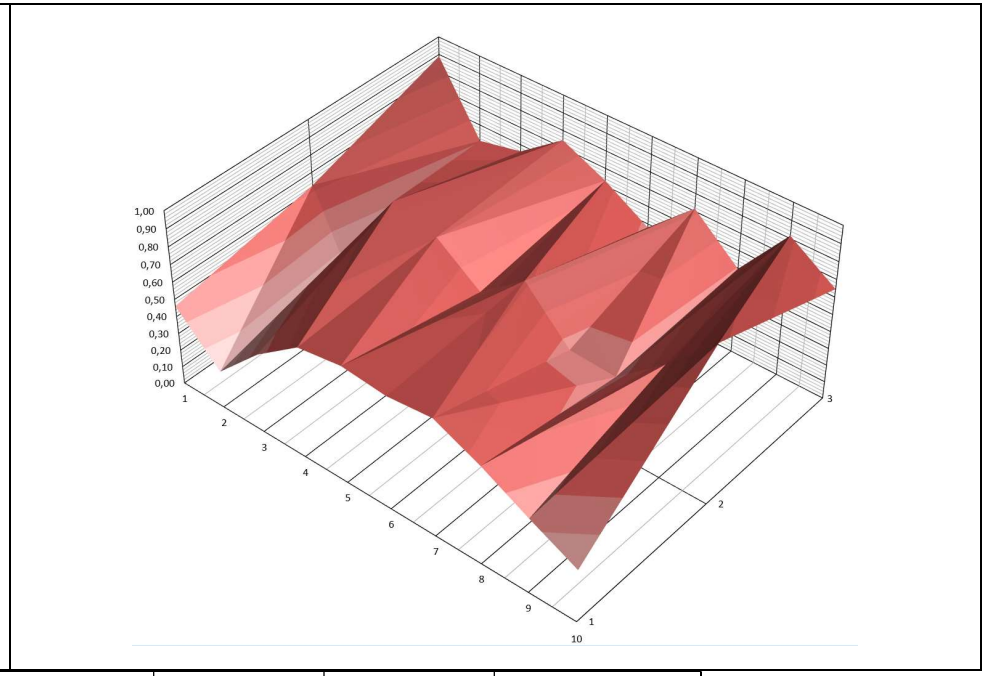
Оценка актуальности УБИ.005	Уровень 1	Уровень 2	Уровень 3	Уровень 1	Уровень 2	Уровень 3
	Оценки опасности реализации УБИ			Оценки защищенности УЗ		
	L1	L2	L3	W1	W2	W3
	0,037482	0,000907	0,180262	0,454545	0,636364	0,636364
	Потенциал			Оценки актуальности		
	P1	P2	P3	B1	B2	B3
Нарушитель 1	0,48	0,52	0,57	0,85	0,53	0,73
Нарушитель 2	0,30	0,10	0,13	0,17	0,07	0,59
Нарушитель 3	0,53	0,50	0,52	0,76	0,52	0,87
Нарушитель 4	0,50	0,52	0,57	0,84	0,53	0,76
Нарушитель 5	0,55	0,53	0,50	0,73	0,58	0,92
Нарушитель 6	0,30	0,50	0,48	0,74	0,56	0,37
Нарушитель 7	0,55	0,40	0,45	0,65	0,39	0,95
Нарушитель 8	0,25	0,50	0,52	**0,80**	0,55	0,23
Нарушитель 9	0,45	0,55	0,40	0,58	0,65	0,76
Нарушитель 10	0,48	0,58	0,53	0,50	**0,87**	**0,86**



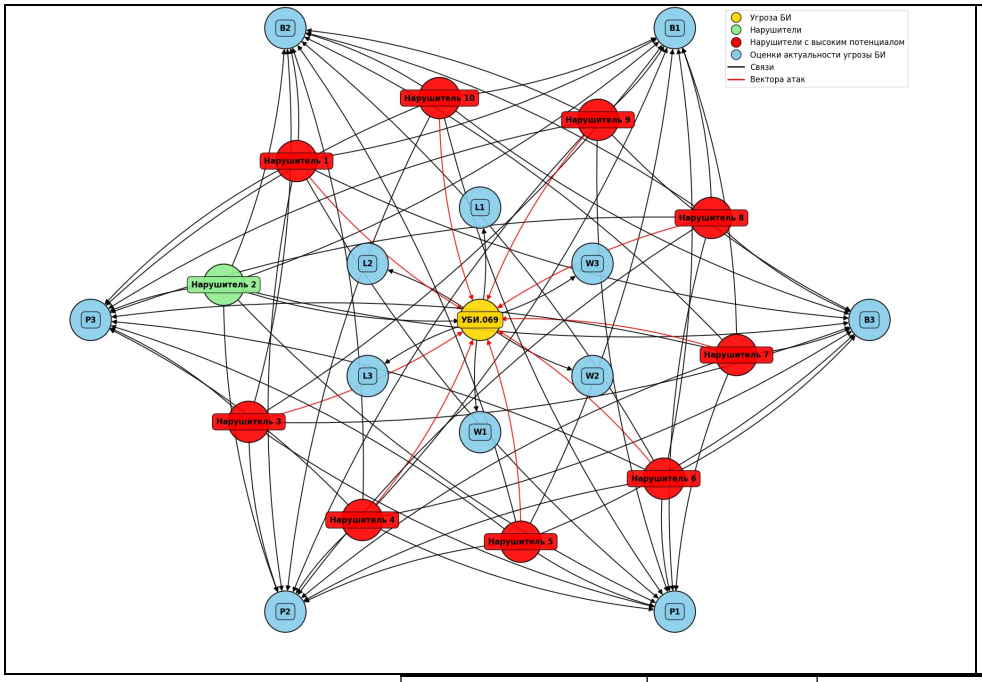


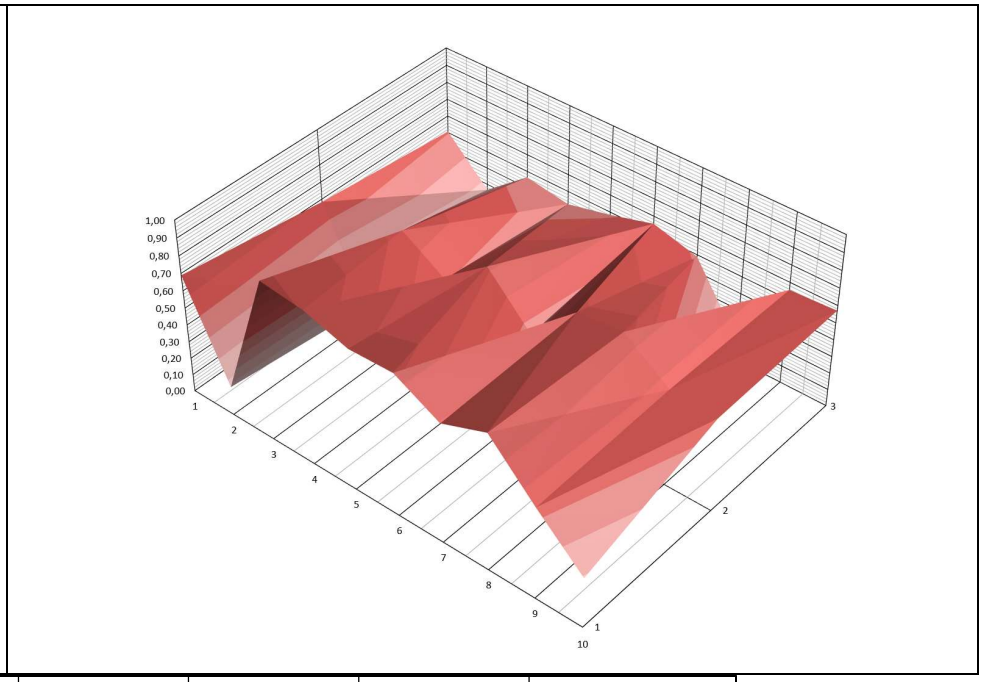
Оценка актуальности УБИ.006	Уровень 1	Уровень 2	Уровень 3	Уровень 1	Уровень 2	Уровень 3
	Оценки опасности реализации УБИ			Оценки защищенности УЗ		
	L1	L2	L3	W1	W2	W3
	0,02690134	0,51022574	0,02418976	0,454545	0,636364	0,637354
	Потенциал			Оценки актуальности		
	P1	P2	P3	B1	B2	B3
Нарушитель 1	0,48	0,52	0,57	0,56	0,50	0,91
Нарушитель 2	0,30	0,10	0,13	0,12	0,18	0,57
Нарушитель 3	0,53	0,50	0,52	0,32	0,81	0,24
Нарушитель 4	0,50	0,52	0,57	0,01	0,71	0,63
Нарушитель 5	0,55	0,53	0,50	1,00	0,64	0,36
Нарушитель 6	0,30	0,50	0,48	0,68	0,60	0,53
Нарушитель 7	0,55	0,40	0,45	0,42	0,50	0,98
Нарушитель 8	0,18	0,50	0,52	0,19	0,75	0,00
Нарушитель 9	0,45	0,55	0,40	0,29	0,60	0,87
Нарушитель 10	0,48	0,58	0,53	0,05	0,69	0,60





Оценка актуальности УБИ.027	Уровень 1	Уровень 2	Уровень 3	Уровень 1	Уровень 2	Уровень 3
	Оценки опасности реализации УБИ			Оценки защищенности УЗ		
	L1	L2	L3	W1	W2	W3
	0,04478545	0,10697372	0,13476033	0,454545	0,636364	0,637354
	Потенциал			Оценки актуальности		
	P1	P2	P3	B1	B2	B3
Нарушитель 1	0,48	0,52	0,57	0,46	0,63	0,89
Нарушитель 2	0,30	0,10	0,13	0,21	0,08	**0,51**
Нарушитель 3	0,53	0,50	0,52	0,46	0,78	0,56
Нарушитель 4	0,50	0,52	0,57	0,64	0,70	0,74
Нарушитель 5	0,55	0,53	0,50	0,68	0,52	0,63
Нарушитель 6	0,30	0,50	0,48	0,66	0,72	0,48
Нарушитель 7	0,55	0,40	0,45	0,68	0,46	0,72
Нарушитель 8	0,25	0,50	0,52	0,57	0,45	0,50
Нарушитель 9	0,45	0,55	0,40	0,43	0,66	0,82
Нарушитель 10	0,48	0,58	0,53	0,31	0,92	0,65





Оценка актуальности УБИ.069	Уровень 1	Уровень 2	Уровень 3	Уровень 1	Уровень 2	Уровень 3
	Оценки опасности реализации УБИ			Оценки защищенности УЗ		
	L1	L2	L3	W1	W2	W3
	0,06274103	0,10088888	0,03922812	0,454545	0,636364	0,637354
	Потенциал			Оценки актуальности		
	P1	P2	P3	B1	B2	B3
Нарушитель 1	0,48	0,52	0,57	**0,69**	**0,58**	**0,51**
Нарушитель 2	0,30	0,10	0,13	0,17	0,08	0,27
Нарушитель 3	0,53	0,50	0,52	**0,92**	**0,67**	0,46
Нарушитель 4	0,50	0,52	0,57	**0,90**	**0,51**	0,42
Нарушитель 5	0,55	0,53	0,50	**0,82**	**0,72**	0,48
Нарушитель 6	0,30	0,50	0,48	**0,83**	0,46	**0,56**
Нарушитель 7	0,55	0,40	0,45	**0,70**	**0,72**	0,49
Нарушитель 8	0,25	0,50	0,52	**0,80**	**0,75**	0,11
Нарушитель 9	0,45	0,55	0,40	**0,53**	**0,56**	**0,56**
Нарушитель 10	0,48	0,58	0,53	0,29	**0,55**	**0,57**

ПРИЛОЖЕНИЕ 7.

Листинг программы

Модуль определения потенциала нарушителя БИ для трёх экспертов

```
using System;
using System.Collections.Generic;
using System.Linq;

namespace ThreatPotentialAssessment
{
    public class Program
    {
        public static void Main(string[] args)
        {
            // Входные данные: матрицы идентификаторов угроз от экспертов (10x10)

               Matrix1(10, 10), // Матрица эксперта 1
               Matrix2(10, 10), // Матрица эксперта 2
               Matrix3(10, 10) // Матрица эксперта 3
            };
            Console.WriteLine("=== Анализ согласованности экспертов ===");
            // Преобразование матриц угроз в ранжировки
            List<List<int>> expertRankings =
ConvertThreatMatricesToRankings(threatMatrices);

            // Расчет коэффициента конкордации
            double w = CalculateKendallsW(expertRankings);
            Console.WriteLine($"Коэффициент конкордации: {w:F4}");
            // Проверка значимости коэффициента
            int n = expertRankings[0].Count; // количество объектов (10)
            int m = expertRankings.Count; // количество экспертов (3)
            double chiSquare = m * (n - 1) * w;
            double criticalValue = 16.919; // Для α=0.05 и df=9 (n-1=10-1=9)
            Console.WriteLine($"\nХи-квадрат: {chiSquare:F2}");
            Console.WriteLine($"Критическое значение (α=0.05, df={n-1}):
{criticalValue:F3}");
            if (chiSquare > criticalValue)
            {
                Console.WriteLine("Заключение: мнения экспертов согласованы
(коэффициент значим).");
            }
            else
            {
                Console.WriteLine("Заключение: мнения экспертов НЕ согласованы
(коэффициент не значим).");
                Console.WriteLine("Рекомендация: провести повторный опрос
экспертов.");
                return;
            }
            // Если эксперты согласованы, продолжаем расчет потенциалов
```

```
            Console.WriteLine("\n=== Расчет потенциалов нарушителей ===");
            // Расчет потенциалов для каждого эксперта
            List<List<double>> expertPotentials =
CalculateExpertPotentials(threatMatrices);
            Console.WriteLine("\nПотенциалы нарушителей по каждому эксперту:");
            for (int i = 0; i < expertPotentials.Count; i++)
            {
                Console.Write($"Эксперт {i+1}: ");
                foreach (var potential in expertPotentials[i])
                {
                    Console.Write($"{potential:F2} ");
                }
                Console.WriteLine();
            }
            // Расчет обобщенных потенциалов
            List<double> generalPotentials =
CalculateGeneralPotentials(expertPotentials);
            Console.WriteLine("\nОбобщенные потенциалы нарушителей:");
            for (int i = 0; i < generalPotentials.Count; i++)
            {
                Console.WriteLine($"Нарушитель {i + 1}:
{generalPotentials[i]:F2}");
            }

            // Расчет средних потенциалов по уровням ОКИИ
            List<int> levelsDistribution = new List<int> { 3, 4, 3 };
            List<double> levelAverages = CalculateLevelAverages(generalPotentials,
levelsDistribution);
            Console.WriteLine("\n=== Средние потенциалы по уровням ОКИИ ===");
            for (int i = 0; i < levelAverages.Count; i++)
            {
                Console.WriteLine($"Уровень {i + 1}: {levelAverages[i]:F2}");
            }
        }
       // Метод для преобразования матриц угроз в ранжировки
        public static List<List<int>>
ConvertThreatMatricesToRankings(List<List<List<int>>> threatMatrices)
        {
            matrix (int rows, int cols)
            List<List<int>> rankings = new List<List<int>>();
            foreach (var matrix in threatMatrices)
            {
                List<int> sums = new List<int>();
                int columns = matrix[0].Count;
                // Вычисление суммы угроз для каждого нарушителя
                for (int j = 0; j < columns; j++)
                {
                    int sum = 0;
                    for (int i = 0; i < matrix.Count; i++)
                    {
                        sum += matrix[i][j];
                    }
                    sums.Add(sum);
                }
                List<int> ranking = new List<int>();
                var sorted = sums.Select((x, i) => new KeyValuePair<int, int>(x,
i))
                                 .OrderByDescending(x => x.Key)
                                 .ToList();
                int currentRank = 1;
                int prevValue = sorted[0].Key;
                ranking.Add(currentRank);
```

```
                for (int i = 1; i < sorted.Count; i++)
                {
                    if (sorted[i].Key == prevValue)
                    {
                        ranking.Add(currentRank);
                    }
                    else
                    {
                        currentRank = i + 1;
                        ranking.Add(currentRank);
                        prevValue = sorted[i].Key;
                    }
                }
                List<int> finalRanking = new List<int>(new int[columns]);
                for (int i = 0; i < sorted.Count; i++)
                {
                    finalRanking[sorted[i].Value] = ranking[i];
                }
                rankings.Add(finalRanking);
            }
            return rankings;
        }
        // Расчет коэффициента конкордации Кендалла-Смитта
        public static double CalculateKendallsW(List<List<int>> expertRankings)
        {
            int m = expertRankings.Count; // Количество экспертов
            int n = expertRankings[0].Count; // Количество объектов

            // Сумма рангов для каждого объекта
            List<int> rankSums = new List<int>(new int[n]);
            foreach (var ranking in expertRankings)
            {
                for (int i = 0; i < n; i++)
                {
                    rankSums[i] += ranking[i];
                }
            }
            // Средняя сумма рангов
            double meanRankSum = rankSums.Average();
            // Вычисляем S - сумму квадратов отклонений
            double S = 0;
            foreach (var sum in rankSums)
            {
                S += Math.Pow(sum - meanRankSum, 2);
            }
            // Коэффициент конкордации
            double W = 12 * S / (Math.Pow(m, 2) * (Math.Pow(n, 3) - n));
            return W;
        }
        // Расчет потенциалов нарушителей для каждого эксперта
        public static List<List<double>>
CalculateExpertPotentials(List<List<List<int>>> matrices)
        {
            List<List<double>> expertPotentials = new List<List<double>>();
            foreach (var matrix in matrices)
            {
                List<double> potentials = new List<double>();
                int columns = matrix[0].Count; // Количество нарушителей

                for (int j = 0; j < columns; j++)
                {
                    double sum = 0;
```

```
                    int rows = matrix.Count; // Количество способов реализации
угроз

                    for (int i = 0; i < rows; i++)
                    {
                        sum += matrix[i][j];
                    }
                    potentials.Add(sum / rows);
                }

                expertPotentials.Add(potentials);
            }
            return expertPotentials;
        }
        // Расчет обобщенных потенциалов нарушителей
        public static List<double> CalculateGeneralPotentials(List<List<double>>
expertPotentials)
        {
            List<double> generalPotentials = new List<double>();
            int violatorsCount = expertPotentials[0].Count;
            for (int j = 0; j < violatorsCount; j++)
            {
                double sum = 0;
                int expertsCount = expertPotentials.Count;

                for (int i = 0; i < expertsCount; i++)
                {
                    sum += expertPotentials[i][j];
                }
                generalPotentials.Add(sum / expertsCount);
            }
            return generalPotentials;
        }
        // Расчет средних потенциалов по уровням ОКИИ
        public static List<double> CalculateLevelAverages(List<double>
generalPotentials, List<int> levelsDistribution)
        {
            List<double> levelAverages = new List<double>();
            int currentIndex = 0;

            foreach (int count in levelsDistribution)
            {
                if (count == 0) continue;

                double sum = 0;
                for (int i = 0; i < count; i++)
                {
                    if (currentIndex < generalPotentials.Count)
                    {
                        sum += generalPotentials[currentIndex];
                        currentIndex++;
                    }
                }
                levelAverages.Add(sum / count);
            }
            return levelAverages;
        }
    }
}
```

Модуль оценки актуальности угроз БИ

```
using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.Linq;
using System.Text;
using System.Threading.Tasks;
using System.Windows.Forms;
using System.Net;
using System.IO;
namespace APCsMT
{
    public partial class Form2 : Form
    {
        public Form2()
        {
            Program.f2 = this;
            InitializeComponent();
            this.StartPosition = FormStartPosition.Manual;
            Size s = SystemInformation.PrimaryMonitorSize;
            this.Location = new Point(0, 0); угол
        }
        Label[] lbs2;//массив Label'ов коэффициентов опасности реализации УБИ
        int w = 13;// количество нарушителей
       public int[] arraytip = new int[13]; // массив типов нарушителей
       public double[] arrayvubi1 = new double[13]; //верхний уровень ОКИИ
        public double[] arrayvubi2 = new double[13]; //средний уровень ОКИИ
        public double[] arrayvubi3 = new double[13]; //полевой уровень ОКИИ
        private void button4_Click(object sender, EventArgs e)
        {
            lbs2 = new Label[] { label11, label12, label13, label14, label15,
label16, label17, label18, label19, label20, label21, label22, label23 };
            for (int i = 0; i < w; i++)
            {
                lbs2[i].Text = Program.f6.array2[i].ToString("0.00");
            }
        }
        private void button5_Click(object sender, EventArgs e)
        {
           // Загрузка БДУ с сайта ФСТЭК РФ
            WebClient webClient = new WebClient();
            webClient.DownloadProgressChanged += (o, args) => progressBar1.Value =
args.ProgressPercentage;
            webClient.DownloadFileCompleted += (o, args) => progressBar1.Value =
100; // статус загрузки БДУ
            string link = @"https://bdu.fstec.ru/files/documents/thrlist.xlsx";
            string downloadFileName = System.IO.Path.GetFileName("thrlist.xls");
            webClient.DownloadFileAsync(new Uri(link), @"d:\" + downloadFileName);
            string filename = downloadFileName;
            Form5 f = new Form5();
            f.ShowDialog();
        }
        private void button2_Click(object sender, EventArgs e)
        {
            button3.PerformClick();
            int RC = dataGridView2.RowCount;
            double z;
            string ubi = "УБИ ";
```

```
            for (int j = 2; j < RC; j++)
            {
                for (int i = 0; i < 3; i++)
                {
                    dataGridView1.Rows.Add();
                    dataGridView1.Rows[j - 1].Cells[0].Value = ubi + (j -
1).ToString();
                    z = Convert.ToDouble(dataGridView2.Rows[j].Cells[i +
2].Value);

                    if (z == 0.000)
                    {
                        dataGridView1.Rows[j - 1].Cells[i + 1].Value = "Угроза не
определена";
                        dataGridView1.Rows[j - 1].Cells[i + 1].Style.BackColor =
Color.YellowGreen;

                    }
                    else if (z < 0.499)
                    {
                        dataGridView1.Rows[j - 1].Cells[i + 1].Value =
"Неактуально";
                        dataGridView1.Rows[j - 1].Cells[i + 1].Style.BackColor =
Color.Green;

                    }
                    else
                    {
                        dataGridView1.Rows[j - 1].Cells[i + 1].Value =
"Актуально";
                        dataGridView1.Rows[j - 1].Cells[i + 1].Style.BackColor =
Color.Red;
                    }
                }
            }
        }
        private void releaseObject(object obj)
        {
            try
            {
                System.Runtime.InteropServices.Marshal.ReleaseComObject(obj);
                obj = null;
            }
            catch (Exception ex)
            {
                obj = null;
                MessageBox.Show("Unable to release the object " + ex.ToString());
            }
            finally
            {
                GC.Collect();
            }
        }
        private void button3_Click(object sender, EventArgs e)
        {
            string str;
            int rCnt;
            int cCnt;
            arraytip = new int[];
            dataGridView2.Visible = true;
            string exePath = AppDomain.CurrentDomain.BaseDirectory;//path to exe
file
```

```
            string filename = Path.Combine(exePath, "Help\\thrlist.xlsx");


            Microsoft.Office.Interop.Excel.Application ExcelApp = new
Microsoft.Office.Interop.Excel.Application();
            Microsoft.Office.Interop.Excel._Workbook ExcelWorkBook;
            Microsoft.Office.Interop.Excel.Worksheet ExcelWorkSheet;
            Microsoft.Office.Interop.Excel.Range ExcelRange;
ExcelWorkBook = ExcelApp.Workbooks.Open(filename, 0, true, 5, "", "", true,
Microsoft.Office.Interop.Excel.XlPlatform.xlWindows, "\t", false,
                false, 0, true, 1, 0);
            ExcelWorkSheet =
(Microsoft.Office.Interop.Excel.Worksheet)ExcelWorkBook.Worksheets.get_Item(1);
            ExcelRange = ExcelWorkSheet.UsedRange;
            for (rCnt = 1; rCnt <= ExcelRange.Rows.Count; rCnt++)
            {
                dataGridView2.Rows.Add(1);
                for (cCnt = 1; cCnt <= 5; cCnt++)
                {
                    str = (string)(ExcelRange.Cells[rCnt, cCnt] as
Microsoft.Office.Interop.Excel.Range).Text; // преобразование типа string и double
в плоский текст
                    dataGridView2.Rows[rCnt - 1].Cells[cCnt - 1].Value = str;
                }
            }
            ocenka_UBI("Носитель информации");
            ocenka_UBI("Микропрограммное и аппаратное обеспечение BIOS/UEFI");
            ocenka_UBI("Аппаратное обеспечение"); ocenka_UBI("Сервер");
ocenka_UBI("Средство вычислительной техники");
            ocenka_UBI("Аппаратное устройство"); ocenka_UBI("(аппаратное
устройство)");
            ocenka_UBI("Сетевой узел"); ocenka_UBI("Сетевое оборудование");
            ocenka_UBI("Каналы связи (передачи) данных");
            ocenka_UBI("Ресурсные центры грид-системы");
            ocenka_UBI("Информационная система"); ocenka_UBI("Инфраструктура
информационных систем");
            ocenka_UBI("Средство защиты информации"); ocenka_UBI("Средства защиты
информации");
            ocenka_UBI("Микропрограммное обеспечение BIOS/UEFI");
            ocenka_UBI("Объекты файловой системы"); ocenka_UBI("Объект файловой
системы");
            ocenka_UBI("Прикладное программное обеспечение");
ocenka_UBI("Программное обеспечение"); ocenka_UBI("программное обеспечение");
            ocenka_UBI("Метаданные"); ocenka_UBI("Информационные ресурсы");
            ocenka_UBI("Сетевой трафик"); ocenka_UBI("Вычислительный узел
суперкомпьютера"); ocenka_UBI("Вычислительные узлы суперкомпьютера");
            ocenka_UBI("Реестр"); ocenka_UBI("Технические средства воздушного
кондиционирования");
            ocenka_UBI("Объекты файловой системы"); ocenka_UBI("Хранилище больших
данных");
            ocenka_UBI("Система управления доступом"); ocenka_UBI("Система
хранения данных суперкомпьютера");
            ocenka_UBI("Сетевое программное обеспечение");
            ocenka_UBI("Рабочая станция"); ocenka_UBI("Аппаратное средство");
            ocenka_UBI("Машинный носитель информации"); ocenka_UBI("Виртуальная
машина"); ocenka_UBI("Мобильное устройство"); ocenka_UBI("Виртуальные устройства
хранения");
            ocenka_UBI("Узлы грид-системы"); ocenka_UBI("Облачная
инфраструктура"); ocenka_UBI("Гипервизор"); ocenka_UBI("Грид-система");
            ocenka_UBI("Программное обеспечение (программы)");
ocenka_UBI("Системное программное обеспечение"); ocenka_UBI("Облачная система");
            ExcelWorkBook.Close(true, null, null);
```

```
            ExcelApp.Quit();
            releaseObject(ExcelWorkSheet);
            releaseObject(ExcelWorkBook);
            releaseObject(ExcelApp);
           }
         public void ocenka_UBI (string uz)
        {
            string str1;
            string str2;
            string str3;
            int rCnt;
            int cCnt;
            int step=1;
            int RC = dataGridView2.RowCount;
            int CC = dataGridView2.ColumnCount;
            string[,] arrayactual = new string[RC, CC]; // массив актуальных угроз
            arrayactual = new string[RC, CC];
            string exePath = AppDomain.CurrentDomain.BaseDirectory;//path to exe
file
            string filename = Path.Combine(exePath, "Help\\thrlist.xlsx");
            if (uz == "Носитель информации")
            step = 0;
            else if (uz == "Микропрограммное и аппаратное обеспечение BIOS/UEFI")
            step = 1;
            else if (uz == "Аппаратное обеспечение" || uz == "Сервер" || uz ==
"Средство вычислительной техники")
                step = 2;
            else if (uz == "Аппаратное устройство" || uz == "(аппаратное
устройство)")
                step = 3;
            else if (uz == "Сетевой узел" || uz == "Сетевое оборудование")
                step = 4;
            else if (uz == "Каналы связи (передачи) данных")
                step = 5;
            else if (uz == "Ресурсные центры грид-системы")
                step = 6;
            else if (uz == "Информационная система" || uz == "Инфраструктура
информационных систем")
                step = 7;
            else if (uz == "Средство защиты информации" || uz == "Средства защиты
информации")
                step = 8;
            else if (uz == "Системное программное обеспечение" || uz ==
"Информационные ресурсы")
                step = 9;
            else if (uz == "Микропрограммное обеспечение BIOS/UEFI")
                step = 10;
            else if (uz == "Объекты файловой системы" || uz == "Объект файловой
системы")
                step = 11;
            else if (uz == "Прикладное программное обеспечение" || uz ==
"Системное программное обеспечение" || uz == "Программное обеспечение" || uz ==
"программное обеспечение")
                step = 12;
            else if (uz == "Метаданные" || uz == "Программное обеспечение
(программы)")
                step = 13;
            else if (uz == "Сетевой трафик" || uz == "Вычислительный узел
суперкомпьютера" || uz == "Вычислительные узлы суперкомпьютера")
                step = 14;
            else if (uz == "Реестр" || uz == "Технические средства воздушного
кондиционирования")
```

```
                step = 15;
            else if (uz == "Объекты файловой системы" || uz == "Хранилище больших
данных")
                step = 16;
            else if (uz == "Система управления доступом" ||  uz == "Система
хранения данных суперкомпьютера")
                step = 17;
            else if (uz == "Сетевое программное обеспечение" || uz == "Облачная
система")
                step = 18;
            else if (uz == "Сетевой узел" || uz == "Рабочая станция" || uz ==
"Аппаратное средство")
                step = 19;
            else if (uz == "Машинный носитель информации" || uz == "Виртуальная
машина" || uz == "Мобильное устройство" || uz == "Виртуальные устройства
хранения")
                step = 20;
            else if (uz == "Узлы грид-системы" || uz == "Облачная инфраструктура"
|| uz == "Гипервизор" || uz == "Грид - система")
                step = 21;

            Microsoft.Office.Interop.Excel.Application ExcelApp = new
Microsoft.Office.Interop.Excel.Application();
            Microsoft.Office.Interop.Excel._Workbook ExcelWorkBook;
            Microsoft.Office.Interop.Excel.Worksheet ExcelWorkSheet;
            Microsoft.Office.Interop.Excel.Range ExcelRange;
            ExcelWorkBook = ExcelApp.Workbooks.Open(filename, 0, true, 5, "", "",
true, Microsoft.Office.Interop.Excel.XlPlatform.xlWindows, "\t", false,
                false, 0, true, 1, 0);
            ExcelWorkSheet =
(Microsoft.Office.Interop.Excel.Worksheet)ExcelWorkBook.Worksheets.get_Item(1);

            ExcelRange = ExcelWorkSheet.UsedRange;
            for (rCnt = 1; rCnt <= ExcelRange.Rows.Count; rCnt++) // цикл проверки
БДУ ФСТЭК на предмет внешних и внутренних нарушителей их потенциалов и объектов
воздействия (объект воздействия соотносится с уязвимыми звеньями)
            {
                for (cCnt = 5; cCnt <= 5; cCnt++)
                {
                    if (dataGridView2.Rows[rCnt - 1].Cells[cCnt -
1].Value.ToString().Contains(uz) ) // объект воздействия
                    {
                        for (int i = 0; i < w; i++)
                        {
                            //Только для внешних нарушителей

                                if (dataGridView2.Rows[rCnt - 1].Cells[cCnt -
2].Value.ToString() == "Внешний нарушитель с низким потенциалом" && arraytip[i] ==
1)
                                {
                                    if (Program.f6.array2[i] >= 0.01 &&
Program.f6.array2[i] <= 0.3)
                                {
                                    arrayvubi1[i] = Program.f6.array2[i] *
Program.f7.arrayoz1[step];
                                    arrayvubi2[i] = Program.f6.array2[i] *
Program.f7.arrayoz2[step];
                                    arrayvubi3[i] = Program.f6.array2[i] *
Program.f7.arrayoz3[step];
                                    }
                                    else
                                        {
```

```
                                        arrayvubi1[i] = 0 *
Program.f7.arrayoz1[step];
                                         arrayvubi2[i] = 0 *
Program.f7.arrayoz2[step];
                                         arrayvubi3[i] = 0 *
Program.f7.arrayoz3[step];
                                    }
                                }
                                else if (dataGridView2.Rows[rCnt -
1].Cells[cCnt - 2].Value.ToString() == "Внешний нарушитель со средним потенциалом"
&& arraytip[i] == 1)
                                if (Program.f6.array2[i] > 0.3 &&
Program.f6.array2[i] <= 0.6)
                            {
                                arrayvubi1[i] = Program.f6.array2[i] *
Program.f7.arrayoz1[step];
                                arrayvubi2[i] = Program.f6.array2[i] *
Program.f7.arrayoz2[step];
                                arrayvubi3[i] = Program.f6.array2[i] *
Program.f7.arrayoz3[step];
                                }
                                else
                                    {
                                        arrayvubi1[i] = 0 *
Program.f7.arrayoz1[step];
                                         arrayvubi2[i] = 0 *
Program.f7.arrayoz2[step];
                                         arrayvubi3[i] = 0 *
Program.f7.arrayoz3[step];
                                    }

                                else if (dataGridView2.Rows[rCnt -
1].Cells[cCnt - 2].Value.ToString() == "Внешний нарушитель с высоким потенциалом"
&& arraytip[i] == 1)
                                if (Program.f6.array2[i] > 0.6)
                            {
                                arrayvubi1[i] = Program.f6.array2[i] *
Program.f7.arrayoz1[step];
                                arrayvubi2[i] = Program.f6.array2[i] *
Program.f7.arrayoz2[step];
                                arrayvubi3[i] = Program.f6.array2[i] *
Program.f7.arrayoz3[step];
                                }
                                else
                                    {
                                        arrayvubi1[i] = 0 *
Program.f7.arrayoz1[step];
                                         arrayvubi2[i] = 0 *
Program.f7.arrayoz2[step];
                                         arrayvubi3[i] = 0 *
Program.f7.arrayoz3[step];
                                    }
//Только для внутренних нарушителей
                            else if (dataGridView2.Rows[rCnt - 1].Cells[cCnt -
2].Value.ToString() == "Внутренний нарушитель с низким потенциалом" && arraytip[i]
== 0)
                                if (Program.f6.array2[i] >= 0.01 &&
Program.f6.array2[i] <= 0.3)
                            {
                                arrayvubi1[i] = Program.f6.array2[i] *
Program.f7.arrayoz1[step];
```

```
                                    arrayvubi2[i] = Program.f6.array2[i] *
Program.f7.arrayoz2[step];
                                    arrayvubi3[i] = Program.f6.array2[i] *
Program.f7.arrayoz3[step];
                                    }
                                    else
                                        {
                                            arrayvubi1[i] = 0 *
Program.f7.arrayoz1[step];
                                             arrayvubi2[i] = 0 *
Program.f7.arrayoz2[step];
                                             arrayvubi3[i] = 0 *
Program.f7.arrayoz3[step];
                                        }
                                else if (dataGridView2.Rows[rCnt - 1].Cells[cCnt -
2].Value.ToString() == "Внутренний нарушитель со средним потенциалом" &&
arraytip[i] == 0)
                                    if (Program.f6.array2[i] > 0.3 &&
Program.f6.array2[i] <= 0.6)
                                {
                                    arrayvubi1[i] = Program.f6.array2[i] *
Program.f7.arrayoz1[step];
                                    arrayvubi2[i] = Program.f6.array2[i] *
Program.f7.arrayoz2[step];
                                    arrayvubi3[i] = Program.f6.array2[i] *
Program.f7.arrayoz3[step];
                                }
                                    else
                                    {
                                        arrayvubi1[i] = 0 *
Program.f7.arrayoz1[step];
                                        arrayvubi2[i] = 0 *
Program.f7.arrayoz2[step];
                                        arrayvubi3[i] = 0 *
Program.f7.arrayoz3[step];
                                    }
                                else if (dataGridView2.Rows[rCnt - 1].Cells[cCnt -
2].Value.ToString() == "Внутренний нарушитель с высоким потенциалом" &&
arraytip[i] == 0)
                                    if (Program.f6.array2[i] > 0.6)
                                {
                                    arrayvubi1[i] = Program.f6.array2[i] *
Program.f7.arrayoz1[step];
                                    arrayvubi2[i] = Program.f6.array2[i] *
Program.f7.arrayoz2[step];
                                    arrayvubi3[i] = Program.f6.array2[i] *
Program.f7.arrayoz3[step];
                                }
                                    else
                                    {
                                        arrayvubi1[i] = 0 *
Program.f7.arrayoz1[step];
                                        arrayvubi2[i] = 0 *
Program.f7.arrayoz2[step];
                                        arrayvubi3[i] = 0 *
Program.f7.arrayoz3[step];
                                    }
                                //Для внешних нарушителей с высоким потенциалом
                               else if (dataGridView2.Rows[rCnt - 1].Cells[cCnt -
2].Value.ToString() == "Внешний нарушитель с высоким потенциалом; Внутренний
нарушитель с низким потенциалом" && Program.f6.array2[i] >= 0.1)
```

```
                                    if (Program.f6.array2[i] <= 0.3 &
Program.f6.array2[i] > 0.6)
                                {
                                    arrayvubi1[i] = Program.f6.array2[i] *
Program.f7.arrayoz1[step];
                                    arrayvubi2[i] = Program.f6.array2[i] *
Program.f7.arrayoz2[step];
                                    arrayvubi3[i] = Program.f6.array2[i] *
Program.f7.arrayoz3[step];
                                }
                                    else
                                    {
                                        arrayvubi1[i] = 0 *
Program.f7.arrayoz1[step];
                                        arrayvubi2[i] = 0 *
Program.f7.arrayoz2[step];
                                        arrayvubi3[i] = 0 *
Program.f7.arrayoz3[step];
                                    }
                                else if (dataGridView2.Rows[rCnt - 1].Cells[cCnt -
2].Value.ToString() == "Внешний нарушитель с высоким потенциалом; Внутренний
нарушитель со средним потенциалом" && Program.f6.array2[i] >= 0.3)
                                    if (Program.f6.array2[i] <= 1)
                                {
                                    arrayvubi1[i] = Program.f6.array2[i] *
Program.f7.arrayoz1[step];
                                    arrayvubi2[i] = Program.f6.array2[i] *
Program.f7.arrayoz2[step];
                                    arrayvubi3[i] = Program.f6.array2[i] *
Program.f7.arrayoz3[step];
                                }
                                    else
                                    {
                                        arrayvubi1[i] = 0 *
Program.f7.arrayoz1[step];
                                        arrayvubi2[i] = 0 *
Program.f7.arrayoz2[step];
                                        arrayvubi3[i] = 0 *
Program.f7.arrayoz3[step];
                                    }
                                //Для внешних нарушителей с низким потенциалом
                                else if (dataGridView2.Rows[rCnt - 1].Cells[cCnt -
2].Value.ToString() == "Внешний нарушитель с низким потенциалом; Внутренний
нарушитель с низким потенциалом" && Program.f6.array2[i] >= 0.1)
                                    if (Program.f6.array2[i] <= 0.3)
                                {
                                    arrayvubi1[i] = Program.f6.array2[i] *
Program.f7.arrayoz1[step];
                                    arrayvubi2[i] = Program.f6.array2[i] *
Program.f7.arrayoz2[step];
                                    arrayvubi3[i] = Program.f6.array2[i] *
Program.f7.arrayoz3[step];
                                }
                                    else
                                    {
                                        arrayvubi1[i] = 0 *
Program.f7.arrayoz1[step];
                                        arrayvubi2[i] = 0 *
Program.f7.arrayoz2[step];
                                        arrayvubi3[i] = 0 *
Program.f7.arrayoz3[step];
                                    }
```

```
                                else if (dataGridView2.Rows[rCnt - 1].Cells[cCnt -
2].Value.ToString() == " Внешний нарушитель с низким потенциалом; Внутренний
нарушитель с низким потенциалом; Внешний нарушитель со средним потенциалом;
Внутренний нарушитель со средним потенциалом" && Program.f6.array2[i] >= 0.1)
                                    if (Program.f6.array2[i] <= 0.6)
                                {
                                    arrayvubi1[i] = Program.f6.array2[i] *
Program.f7.arrayoz1[step];
                                    arrayvubi2[i] = Program.f6.array2[i] *
Program.f7.arrayoz2[step];
                                    arrayvubi3[i] = Program.f6.array2[i] *
Program.f7.arrayoz3[step];
                                }
                                    else
                                    {
                                        arrayvubi1[i] = 0 *
Program.f7.arrayoz1[step];
                                        arrayvubi2[i] = 0 *
Program.f7.arrayoz2[step];
                                        arrayvubi3[i] = 0 *
Program.f7.arrayoz3[step];
                                    }
                                //Для внешних нарушителей со средним потенциалом
                                else if (dataGridView2.Rows[rCnt - 1].Cells[cCnt -
2].Value.ToString() == "Внешний нарушитель со средним потенциалом; Внутренний
нарушитель со средним потенциалом" && Program.f6.array2[i] > 0.3)
                                    if (Program.f6.array2[i] <= 0.6)
                                {
                                    arrayvubi1[i] = Program.f6.array2[i] *
Program.f7.arrayoz1[step];
                                    arrayvubi2[i] = Program.f6.array2[i] *
Program.f7.arrayoz2[step];
                                    arrayvubi3[i] = Program.f6.array2[i] *
Program.f7.arrayoz3[step];
                                }
                                    else
                                    {
                                        arrayvubi1[i] = 0 *
Program.f7.arrayoz1[step];
                                        arrayvubi2[i] = 0 *
Program.f7.arrayoz2[step];
                                        arrayvubi3[i] = 0 *
Program.f7.arrayoz3[step];
                                    }
                                else if (dataGridView2.Rows[rCnt - 1].Cells[cCnt -
2].Value.ToString() == "Внешний нарушитель со средним потенциалом; Внутренний
нарушитель с низким потенциалом" && Program.f6.array2[i] >= 0.1)
                                    if (Program.f6.array2[i] <= 0.6)
                                {
                                    arrayvubi1[i] = Program.f6.array2[i] *
Program.f7.arrayoz1[step];
                                    arrayvubi2[i] = Program.f6.array2[i] *
Program.f7.arrayoz2[step];
                                    arrayvubi3[i] = Program.f6.array2[i] *
Program.f7.arrayoz3[step];
                                }
                                    else
                                    {
                                        arrayvubi1[i] = 0 *
Program.f7.arrayoz1[step];
                                        arrayvubi2[i] = 0 *
Program.f7.arrayoz2[step];
```

```
                                        arrayvubi3[i] = 0 *
Program.f7.arrayoz3[step];
                                    }
                                        else
                                         {
                                             arrayvubi1[i] = 0 *
Program.f7.arrayoz1[step];
                                             arrayvubi2[i] = 0 *
Program.f7.arrayoz2[step];
                                             arrayvubi3[i] = 0 *
Program.f7.arrayoz3[step];
                                          }
                            }
                                double db1 = arrayvubi1.Max<double>();
                                str1 = db1.ToString("0.000");
                                dataGridView2.Rows[rCnt - 1].Cells[cCnt - 1].Value =
str1;

                                double db2 = arrayvubi2.Max<double>();
                                str2 = db2.ToString("0.000");
                                dataGridView2.Rows[rCnt - 1].Cells[cCnt - 2].Value =
str2;

                                double db3 = arrayvubi3.Max<double>();
                                str3 = db3.ToString("0.000");
                                dataGridView2.Rows[rCnt - 1].Cells[cCnt - 3].Value =
str3;
                            }
                        }
                    }
            }
             private void button6_Click(object sender, EventArgs e)
             {
                 button3.PerformClick();
                 int RC = dataGridView2.RowCount;
                 double z;
                 string ubi = "УБИ ";
                 for (int j = 2; j < RC; j++)
                 {
                     for (int i = 0; i < 3; i++)
                     {
                         dataGridView1.Rows.Add();
                         dataGridView1.Rows[j - 1].Cells[0].Value = ubi + (j -
1).ToString();
                         z = Convert.ToDouble(dataGridView2.Rows[j].Cells[i +
2].Value);

                         if (z == 0.000)
                         {
                             dataGridView1.Rows[j - 1].Cells[i + 1].Value = "Угроза не
определена";
                             dataGridView1.Rows[j - 1].Cells[i + 1].Style.BackColor =
Color.YellowGreen;

                         }
                         else if (z < 0.499)
                         {
                             dataGridView1.Rows[j - 1].Cells[i + 1].Value =
"Неактуально";
                             dataGridView1.Rows[j - 1].Cells[i + 1].Style.BackColor =
Color.Green;
```

```
                    }
                    else
                    {
                        dataGridView1.Rows[j - 1].Cells[i + 1].Value =
"Актуально";
                        dataGridView1.Rows[j - 1].Cells[i + 1].Style.BackColor =
Color.Red;
                    }
                }
            }
            Microsoft.Office.Interop.Excel.Application ExcelApp1 = new
Microsoft.Office.Interop.Excel.Application();
            Microsoft.Office.Interop.Excel.Workbook ExcelWorkBook1;
            Microsoft.Office.Interop.Excel.Worksheet ExcelWorkSheet1;
            ExcelWorkBook1 =
ExcelApp1.Workbooks.Add(System.Reflection.Missing.Value);
            ExcelWorkSheet1 =
(Microsoft.Office.Interop.Excel.Worksheet)ExcelWorkBook1.Worksheets.get_Item(1);
            Microsoft.Office.Interop.Excel.Range _excelCells1 =
(Microsoft.Office.Interop.Excel.Range)ExcelWorkSheet1.get_Range("A1", "D1").Cells;
            _excelCells1.Merge(Type.Missing
            ExcelApp1.Cells[1, 1] = "Оценка актуальности угроз БИ ОКИИ";
            ExcelApp1.Cells[1, 1].Font.Size = 16;
            ExcelApp1.Cells[1, 1].Font.Name = "Aharoni";
            ExcelApp1.Cells[1, 1].Font.Color = Color.Red;
            for (int j = 1; j < RC; j++)
            {
                for (int i = 0; i <= 3; i++)
                {
                    if (dataGridView1.Rows[j - 1].Cells[i].Value ==
"Неактуально")
                    {
                        ExcelApp1.Cells[j + 1, i + 1] =
dataGridView1.Rows[j].Cells[i].Value;
                        ExcelApp1.Cells[j, i + 1].Interior.Color = Color.Green;
                    }
                    else if (dataGridView1.Rows[j - 1].Cells[i].Value ==
"Актуально")
                    {
                        ExcelApp1.Cells[j + 1, i + 1] =
dataGridView1.Rows[j].Cells[i].Value;
                        ExcelApp1.Cells[j, i + 1].Interior.Color = Color.Red;
                    }
                    else if (dataGridView1.Rows[j - 1].Cells[i].Value == "Угроза
не определена")
                    {
                        ExcelApp1.Cells[j + 1, i + 1] =
dataGridView1.Rows[j].Cells[i].Value;
                        ExcelApp1.Cells[j, i + 1].Interior.Color =
Color.YellowGreen;
                    }
                    else
                    { ExcelApp1.Cells[j + 1, i + 1] =
dataGridView1.Rows[j].Cells[i].Value; }
                }
            }
            ExcelApp1.Visible = true;
            ExcelApp1.UserControl = true;
            ExcelWorkSheet1.Columns.WrapText = true;
            ExcelApp1.Columns.AutoFit
            ExcelApp1.Columns.HorizontalAlignment =
Microsoft.Office.Interop.Excel.Constants.xlCenter;
```

```
        }
        private void button7_Click(object sender, EventArgs e)
        {
            button3.PerformClick();
            int RC = dataGridView2.RowCount;
            double z;
            string ubi = "УБИ ";
            for (int j = 2; j < RC; j++)
            {
                for (int i = 0; i < 3; i++)
                {
                    dataGridView1.Rows.Add();
                    dataGridView1.Rows[j - 1].Cells[0].Value = ubi + (j -
1).ToString();
                    z = Convert.ToDouble(dataGridView2.Rows[j].Cells[i +
2].Value);
                    if (z == 0.000)
                    {
                        dataGridView1.Rows[j - 1].Cells[i + 1].Value = "Угроза не
определена";
                        dataGridView1.Rows[j - 1].Cells[i + 1].Style.BackColor =
Color.YellowGreen;

                    }
                    else if (z < 0.499)
                    {
                        dataGridView1.Rows[j - 1].Cells[i + 1].Value =
"Неактуально";
                        dataGridView1.Rows[j - 1].Cells[i + 1].Style.BackColor =
Color.Green;

                    }
                    else
                    {
                        dataGridView1.Rows[j - 1].Cells[i + 1].Value =
"Актуально";
                        dataGridView1.Rows[j - 1].Cells[i + 1].Style.BackColor =
Color.Red;
                    }
                }
            }
            Microsoft.Office.Interop.Excel.Application ExcelApp1 = new
Microsoft.Office.Interop.Excel.Application();
            Microsoft.Office.Interop.Excel.Workbook ExcelWorkBook1;
            Microsoft.Office.Interop.Excel.Worksheet ExcelWorkSheet1;
                        ExcelWorkBook1 =
ExcelApp1.Workbooks.Add(System.Reflection.Missing.Value);
                        ExcelWorkSheet1 =
(Microsoft.Office.Interop.Excel.Worksheet)ExcelWorkBook1.Worksheets.get_Item(1);
            string str1 = " ";
            string str2  = " ";
            string str3  = " ";
            ExcelApp1.Cells[1, 2] = "Актуальные угрозы БИ ОКИИ";
            ExcelApp1.Cells[1, 2].Font.Size = 16;
            ExcelApp1.Cells[1, 2].Font.Name = "Aharoni";
            ExcelApp1.Cells[1, 2].Font.Color = Color.Red;
            ExcelApp1.Cells[2, 1] = "Верхний уровень ОКИИ";
            ExcelApp1.Cells[3, 1] = "Средний уровень ОКИИ";
            ExcelApp1.Cells[4, 1] = "Полевой уровень ОКИИ";
            ExcelApp1.Cells[1, 2].Interior.Color = Color.Khaki;
            ExcelApp1.Cells[1, 1].Interior.Color = Color.LemonChiffon;
            ExcelApp1.Cells[2, 1].Interior.Color = Color.Gray;
```

```
            ExcelApp1.Cells[3, 1].Interior.Color = Color.Gray;
            ExcelApp1.Cells[4, 1].Interior.Color = Color.Gray;
            for (int j = 1; j < RC; j++)
            {
                for (int i = 0; i <= 3; i++)
                {
                        if (dataGridView1.Rows[j - 1].Cells[i].Value ==
"Актуально" && i==1)
                    {
                        str1 = str1 + (j - 1).ToString() + "; ";
                        ExcelApp1.Cells[2, 2] = str1;
                    }
                    else if (dataGridView1.Rows[j - 1].Cells[i].Value ==
"Актуально" && i == 2)
                    {
                        str2 = str2 + (j - 1).ToString() + "; ";
                        ExcelApp1.Cells[3, 2] = str2;
                    }
                    else if (dataGridView1.Rows[j - 1].Cells[i].Value ==
"Актуально" && i == 3)
                    {
                        str3 = str3 + (j - 1).ToString() + "; ";
                        ExcelApp1.Cells[4, 2] = str3;
                    }
                    else
                    { ExcelApp1.Cells[6, i + 1] = "  "; }
                }
            }
                         ExcelApp1.Visible = true;
            ExcelApp1.UserControl = true;
          //  ExcelWorkSheet1.Columns.WrapText = true;
            ExcelApp1.Columns.AutoFit();
        }
               }
           }
```

Модуль построения графа актуальных угроз БИ

```
import matplotlib.pyplot as plt
from matplotlib.lines import Line2D
G = nx.DiGraph()
central_node = "УБИ"
G.add_node(central_node)
levels = ["L1(t)", "L2(t)", "L3(t)", "W1", "W2", "W3"]
G.add_nodes_from(levels)
for level in levels:
    G.add_edge(central_node, level)
data = {
    "Нарушитель 1": {"E1", "E2", "E3", "B1", "B2", "B3":},
    "Нарушитель 2": {"E1", "E2", "E3", "B1", "B2", "B3":},
    "Нарушитель 3": {"E1", "E2", "E3", "B1", "B2", "B3":},
    "Нарушитель 4": {"E1", "E2", "E3", "B1", "B2", "B3":},
    "Нарушитель 5": {"E1", "E2", "E3", "B1", "B2", "B3":},
    "Нарушитель 6": {"E1", "E2", "E3", "B1", "B2", "B3":},
    "Нарушитель 7": {"E1", "E2", "E3", "B1", "B2", "B3":},
    "Нарушитель 8": {"E1", "E2", "E3", "B1", "B2", "B3":},
    "Нарушитель 9": {"E1", "E2", "E3", "B1", "B2", "B3":},
    "Нарушитель 10": {"E1", "E2", "E3", "B1", "B2", "B3":},
}
for violator, metrics in data.items():
    G.add_node(violator)
```

```
    G.add_edge(violator, central_node)
    for metric, value in metrics.items():
        G.add_node(metric)
        G.add_edge(violator, metric)
red_violators = []
node_colors = []
for node in G.nodes():
    if node.startswith("Нарушитель"):
        high_b = any(data.get(node, {}).get(b_metric, 0) > 0.8 for b_metric in
["B1", "B2", "B3"])
        if high_b:
            red_violators.append(node)
            node_colors.append("red")
        else:
            node_colors.append("lightgreen")
    elif node == central_node:
        node_colors.append("gold")
    else:
        node_colors.append("skyblue")
# Цвета рёбер
edge_colors = [
    "red" if (u in red_violators and v == central_node) or (v in red_violators and
u == central_node)
    else "black"
    for u, v in G.edges()
]
plt.figure(figsize=(20, 15))
pos = nx.shell_layout(G, nlist=[
    [central_node],
    levels,
    list(data.keys()),
    list({metric for violator in data.values() for metric in violator})
])
nx.draw(
    G,
    pos,
    with_labels=False,
    node_size=4000,
    node_shape="o",
    node_color=node_colors,
    edgecolors="black",
    linewidths=1.5,
    edge_color=edge_colors,
    arrows=True,
    arrowsize=15,
    arrowstyle='-|>',
    width=1.5,
    alpha=0.9,
    connectionstyle='arc3,rad=0.1'
)
for node, (x, y) in pos.items():
    plt.text(x, y, node,
             fontsize=12,
             fontweight='bold',
             ha='center',
             va='center',
             bbox=dict(facecolor=node_colors[list(G.nodes()).index(node)],
                       edgecolor='black',
                       boxstyle='round,pad=0.5',
                       alpha=0.9))
legend_elements = [
    Line2D([0], [0], marker='o', color='w', label='Угроза БИ',
```

```
           markerfacecolor='gold', markersize=15, markeredgecolor='black'),
    Line2D([0], [0], marker='o', color='w', label='Нарушители',
           markerfacecolor='lightgreen', markersize=15, markeredgecolor='black'),
    Line2D([0], [0], marker='o', color='w', label='Нарушители с высоким
потенциалом',
           markerfacecolor='red', markersize=15, markeredgecolor='black'),
    Line2D([0], [0], marker='o', color='w', label='Оценки актуальности угрозы БИ',
           markerfacecolor='skyblue', markersize=15, markeredgecolor='black'),
    Line2D([0], [0], color='black', lw=2, label='Связи'),
    Line2D([0], [0], color='red', lw=2, label='Вектора атак')
]
plt.legend(handles=legend_elements, loc='upper right', fontsize=12,
bbox_to_anchor=(1.3, 1))
plt.title("Нарушители → Оценка актуальности УБИ.5 (красные нарушители → красные
связи)",
          size=18, pad=20)
plt.tight_layout()
plt.show()
```

ПРИЛОЖЕНИЕ 8.

Акты о внедрении результатов диссертационной работы

АО ЦКБА

УТВЕРЖДАЮ
Генеральный директор
_____ А.В. Хомяков
«__» 04 2025 г.

АКТ
об использовании программы для ЭВМ

Регистрационный номер — Свидетельство № 2022611043
Заявка № 2022610172 от 11.01.2022г.

Название «Моделирование угроз информационной безопасности АСУ ТП»

Автор: Чернов Д.В.

Программа для ЭВМ используется в процессах формирования моделей угроз информационной безопасности объектов критической информационной инфраструктуры, что подтверждается Моделью угроз безопасности информации при ее обработке в АО ЦКБА (утверждена приказом № 472 от 24.05.2023г.).

Заместитель генерального директора по ЭБиР — М.В. Алямовский

С началом использования программы для ЭВМ ознакомлен

Автор

«30» 04 2025 г. — Д.В. Чернов

УТВЕРЖДАЮ
Проректор по учебной работе
_____ В.В. Котов
«30» 06 2025 г.

АКТ
внедрения результатов диссертации на соискание
ученой степени кандидата технических наук в учебный процесс

Комиссия Тульского государственного университета в составе:

Сычугов А.А. – председатель комиссии, заведующий кафедрой «Информационная безопасность», доктор технических наук;

– Токарев В.Л. – член комиссии, профессор кафедры «Информационная безопасность», доктор технических наук;

– Борзенкова С.Ю. – член комиссии, кандидат технических наук

рассмотрела результаты работы и материалы диссертации Чернова Д.В. на соискание ученой степени кандидата технических наук на тему «Методы и алгоритмы моделирования угроз безопасности объектов критической информационной инфраструктуры с применением аппарата экспертных оценок» и результаты их внедрения в учебный процесс кафедры «Информационная безопасность».

Комиссия констатирует, что теоретические результаты исследований включены в конспект лекций по дисциплинам «Безопасность операционных систем», «Защита от атак из сети Internet», использованы в методических указаниях по практическим и лабораторным занятиям по этим дисциплинам. Эффективность внедрения заключается в приобретении студентами знаний по перспективным направлениям развития науки и техники.

Председатель комиссии А.А. Сычугов

Члены комиссии В.Л. Токарев

С.Ю. Борзенкова

MK SERVICE

Общество с ограниченной ответственностью
"МК Сервис"
ИНН 7104075892 КПП 710401001
ОГРН 1177154016632
300013, РФ, г. Тула, ул. Московская, д. 17, оф. 16
Тел.: +7 (4872) 73-00-35

Исх. № 352 от 05.05.2025 г.

УТВЕРЖДАЮ
Директор
ООО «МК Сервис»
Каверин М.В.
«__» _____ 2025 г.

АКТ

об использовании результатов диссертационной работы на соискание ученой степени кандидата технических наук Чернова Дениса Владимировича

«Методы и алгоритмы моделирования угроз безопасности объектов критической информационной инфраструктуры с применением аппарата экспертных оценок»

Комиссия ООО «МК Сервис» подтверждает, что результаты диссертационной работы на соискание ученой степени кандидата технических наук Чернова Д.В., а именно:

1. Метод количественной оценки степени опасности реализации угроз БИ ОКИИ потенциальными нарушителями ИБ с использованием оценок вероятностей реализации угроз БИ и ущерба от их реализации;
2. Алгоритм определения уязвимых звеньев ОКИИ и оценки их защищенности;
3. Алгоритм экспертной оценки степени опасности реализации угроз БИ ОКИИ;
4. Автоматизированная система моделирования угроз БИ ОКИИ.

внедрены и используются в процессах выполнения мероприятий по обеспечению информационной безопасности объектов критической информационной инфраструктуры.

Председатель комиссии:

Ведущий специалист
по информационной безопасности — Лысенко М.Ю.

Члены комиссии:

Специалист по информационной безопасности — Зотов А.Р.

Специалист по информационной безопасности — Кривец Ю.А.

БД Безопасность
DATABASE SECURITY

Общество с ограниченной ответственностью
«БД Безопасность»
ИНН 7104526200 КПП 710401001
ОГРН 1147154036182
300013, г. Тула, ул. Московская, д.17, оф.20
Тел. (4872) 73-00-35

№ 71 от «05» мая 2025 г.

Акт о внедрении результатов
диссертационного исследования
Чернова Дениса Владимировича
«Методы и алгоритмы моделирования угроз безопасности объектов критической информационной инфраструктуры с применением аппарата экспертных оценок»

Настоящий Акт составлен в том, что результаты диссертационной работы, а именно:

- Метод определения потенциала нарушителя информационной безопасности объектов критической информационной инфраструктуры (ИБ ОКИИ) на основе вычисления матриц идентификаторов угроз безопасности информации (БИ);
- Алгоритм определения уязвимых звеньев ОКИИ и оценки уровня их защищенности;
- Алгоритм экспертной оценки степени опасности реализации угроз БИ для ОКИИ.

используются в работе аттестационной комиссии ООО «БД Безопасность», в целях выполнения комплексных проектов в области ИБ ОКИИ. Использование результатов диссертационного исследования способствует повышению качества разрабатываемой организационно-распорядительной документации объектов информатизации в части моделирования угроз информационной безопасности, а также формированию моделей нарушителей информационной безопасности объектов КИИ.

Директор
ООО «БД Безопасность» М.В. Каверин

КОМПЛЕКСЫ СИСТЕМЫ И СЕТИ

№ 3556 от «14» апреля 2025 г.

УТВЕРЖДАЮ
Директор
ООО «Комплексы системы и сети»
Жильцов Е.А.
«14» 04 2025г.

АКТ
о внедрении результатов
диссертационной работы на соискание степени кандидата технических наук Чернова Д.В.
«Методы и алгоритмы моделирования угроз безопасности объектов критической информационной инфраструктуры с применением аппарата экспертных оценок»

Настоящим сообщается, что результаты диссертационной работы «Методы и алгоритмы моделирования угроз безопасности объектов критической информационной инфраструктуры с применением аппарата экспертных оценок», внедрены и использованы в виде рекомендаций при выполнении мероприятий по моделированию угроз ИБ ОКИИ.

Результатом внедрения работы Чернова Д.В. в деятельность ООО «Комплексы системы и сети» стало увеличение эффективности моделирования угроз БИ ОКИИ с 2,88 до 7,66 (более чем в 2,6 раз) суммарного числа выявленных актуальных угроз и предложенных мер защиты в час.

Руководитель отдела А.Ф. Ташлыкова

ПРИЛОЖЕНИЕ 9.

Полученные свидетельства об интеллектуальной собственности

РОССИЙСКАЯ ФЕДЕРАЦИЯ

RU2022611043

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

ГОСУДАРСТВЕННАЯ РЕГИСТРАЦИЯ ПРОГРАММЫ ДЛЯ ЭВМ

Номер регистрации (свидетельства):
2022611043
Дата регистрации: **18.01.2022**
Номер и дата поступления заявки:
2022610172 11.01.2022
Дата публикации и номер бюллетеня:
18.01.2022 Бюл. № 1
Контактные реквизиты:
нет

Автор(ы):
Чернов Денис Владимирович (RU),
Сычугов Алексей Алексеевич (RU)
Правообладатель(и):
Федеральное государственное бюджетное образовательное учреждение высшего образования «Тульский государственный университет» (ТулГУ) (RU)

Название программы для ЭВМ:
Моделирование угроз информационной безопасности АСУ ТП

Реферат:
Программа предназначена для определения актуальных угроз информационной безопасности АСУ ТП на основе информации о потенциальных нарушителях информационной безопасности и технологических процессах, выполняющихся в автоматизированных системах. Программа повышает защищенность промышленных систем автоматизации производственных процессов и позволяет поддерживать актуальность сведений о возможных угрозах и потенциальных нарушителях информационной безопасности, что позволяет снизить расходы, связанные с их проектированием и эксплуатацией. Область применения: обеспечение информационной безопасности автоматизированных систем управления технологическими процессами. Функциональные возможности программы: определение потенциалов нарушителей информационной безопасности АСУ ТП, построение модели угроз информационной безопасности АСУ ТП. Тип ЭВМ: IBM PC-совмест. ПК на базе процессора Intel Pentium II и выше. ОС: Windows XP и выше.

Язык программирования: C Sharp (C#)

Объем программы для ЭВМ: 499 КБ

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2022611043

Моделирование угроз информационной безопасности АСУ ТП

Правообладатель: ***Федеральное государственное бюджетное образовательное учреждение высшего образования «Тульский государственный университет» (ТулГУ) (RU)***

Авторы: ***Чернов Денис Владимирович (RU), Сычугов Алексей Алексеевич (RU)***

Заявка № **2022610172**
Дата поступления **11 января 2022 г.**
Дата государственной регистрации
в Реестре программ для ЭВМ ***18 января 2022 г.***

Руководитель Федеральной службы по интеллектуальной собственности

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат 0x75699C0008AEB78543BD83DF819A6CD1
Владелец **Ивлиев Григорий Петрович**
Действителен с 24.12.2021 по 24.12.2022

Г.П. Ивлиев