МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ,
СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М.А. Бонч-Бруевича»

На правах рукописи

Миняев Андрей Анатольевич

МЕТОДИКА ОЦЕНКИ ЭФФЕКТИВСНОСТИ СИСТЕМЫ ЗАЩИТЫ ТЕРРИТОРИАЛЬНО-РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

2.3.6 – Методы и системы защиты информации, информационная безопасность

Диссертация на соискание ученой степени
кандидата технических наук

Научный руководитель
кандидат технических наук , доцент
Красов Андрей Владимирович

Санкт-Петербург – 2021

СОДЕРЖАНИЕ

Введение

Актуальность темы исследования. Информационная безопасность в последние годы становится все более значимой и важной сферой национальной безопасности Российской Федерации, что отражено в Доктрине информационной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации 5 декабря 2016 г. № 646 [1]. В соответствии с Доктриной информационные технологии в настоящее время приобрели глобальный трансграничный характер и стали неотъемлемой частью всех сфер деятельности личности и, общества и государства. Расширение областей и сфер применения информационных технологий значительно расширяет перспективы развития новых информационных угроз. Зарубежные специальные службы расширяют свое влияние информационно-психологического воздействия, направленного на дестабилизацию внутриполитической и социальной ситуации в различных регионах мира и приводящего к подрыву суверенитета и нарушению территориальной целостности других государств. Средства массовой информации увеличивают объемы материалов, содержащих предвзятую оценку государственной политики Российской Федерации. Возрастают масштабы компьютерной преступности, прежде всего в кредитно-финансовой сфере. В сфере обороны страны, в области государственной и общественной безопасности, в экономической сфере, в области науки, технологий и образования, в области стратегической стабильности и равноправного стратегического партнерства наблюдаются государством определены стратегические цели для обеспечения эффективного состояния информационной безопасности [1].

Одновременно с ростом и развитием информационных технологий развиваются тактики, техники и способы реализации проведения атак, расширяется инструментарий для нарушения состояния информационной безопасности. На рисунке 1.1 представлен анализ роста утечек конфиденциальной информации за последние 15 лет.

Рисунок 1.1 – График утечек конфиденциальной информации из отчета экспертно-аналитического центра группы компаний InfoWatch[1]

Изменить ситуацию можно путем разработки новых подходов к обеспечению информационной безопасности, способных предоставить надежную защиту от современных угроз безопасности информации [56, 57].

Задача обеспечения информационной безопасности становится в последнее время наиболее актуальной. Актуальность данной задачи обусловлена, в первую очередь, с ростом утечек информации и компьютерных атак, отражаемых в статистических данных по совершению преступлений в сфере высоких технологий, приводимыми Генеральной прокуратурой Российской Федерации и ведущими международными и организациями Российской Федерации в сфере информационной безопасности, а также законодательными нововведениями. В соответствии со сводными отчетами[2] Генеральной прокуратуры Российской Федерации «рост криминальной активности с использованием интернета и современных коммуникационных устройств в 2017 году в России составил 37% и достиг 90 587 зафиксированных случаев по сравнению с 65 949 в 2016 году. Соответственно каждое двадцатое преступление от числа всех зарегистрированных

[1] https://www.infowatch.ru/analytics/reports
[2] https://genproc.gov.ru/stat/data/

в России преступлений квалифицируется как киберпреступление. Среди всех совершённых в 2017 году компьютерных преступлений лидируют нарушения статей 272 и 273 Уголовного Кодекса Российской Федерации (далее – УК РФ), предусматривающие ответственность за неправомерный доступ к компьютерной информации, а также создание, использование и распространение компьютерных «вирусов». Второе место в незаконной электронной деятельности по данным надзорного ведомства занимает мошенничество с использованием сервисов онлайн-платежей (статья 159.3 УК РФ). Количество таких правонарушений в первом полугодии 2018 г. возросло в 7 раз. За первое полугодие 2019 года правоохранительные органы зарегистрировали 117 640 (+46,8 %) преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации». В качестве другого примера можно привести результаты исследований экспертно - аналитического центра группы компании InfoWatch, в котором отражено зарегистрированное количество утечек информации в России и в мире за 2020 год, разделенное по следующим типам информации: персональные данные, коммерческая тайна, платежная информации, государственная тайна (рисунки 1.2, 1.3).

Рисунок 1.2 – Распределение утечек информации по типам данных из отчета экспертно-аналитического центра группы компаний InfoWatch[3]

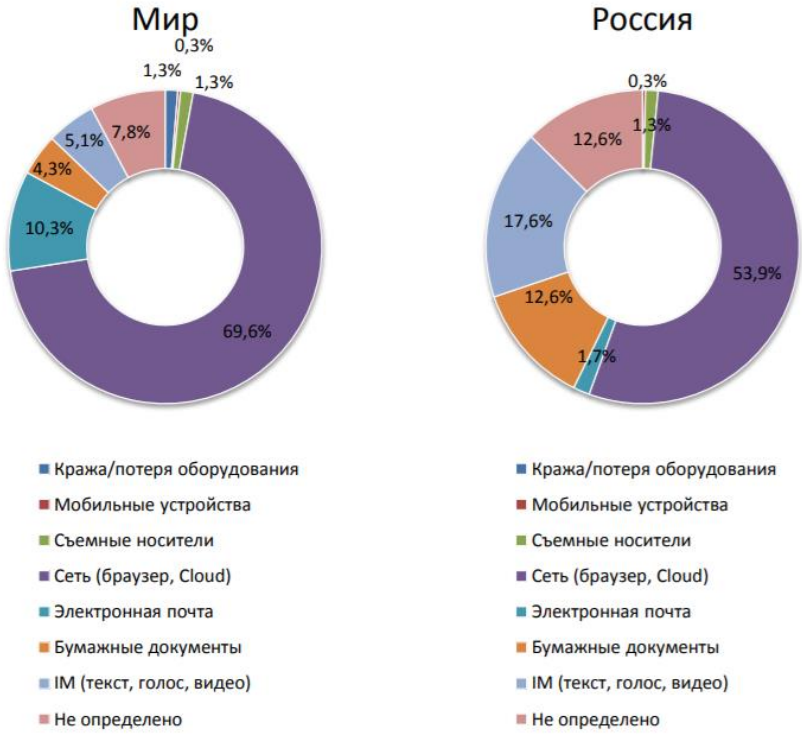


Рисунок 1.3 – Распределение утечек конфиденциальной информации по каналам из отчета экспертно-аналитического центра группы компаний InfoWatch[4]

[3] https://www.infowatch.ru/analytics/reports
[4] https://www.infowatch.ru/analytics/reports

Еще одним примером роста утечек информации являются ежегодные отчеты[5] «Hi-Tech Crime Trends» международной компании Group-IB, в котором говориться об активности так называемых проправительственных организаций, занимающихся киберпреступлениями (проведению атак) в интересах своих государств. Согласно отчету «Hi-Tech Crime Trends 2020-2021», отмечается увеличение роста кибератак с использованием шпионского программного обеспечения, шифровальщиков, бэкдоров, увеличение атак на банки и рост финансового мошенничества с использованием социальной инженерии. При этом мотив киберпреступников остается тем же – кража денег или информации, за которую можно получить финансовую прибыль.

Согласно аналитическим данных компании Positive Technologies, по итогам 3 квартала 2020 года отмечается рост количества инцидентов на 2,7 % по сравнению с предыдущим периодом, увеличение доли APT -атак с 63% до 70%, а также рост атак и использование шифровальщиков. На рисунке 1.4 представлен график роста количества инцидентов в 2019 и 2020 года, представленный компанией Positive Technologies.

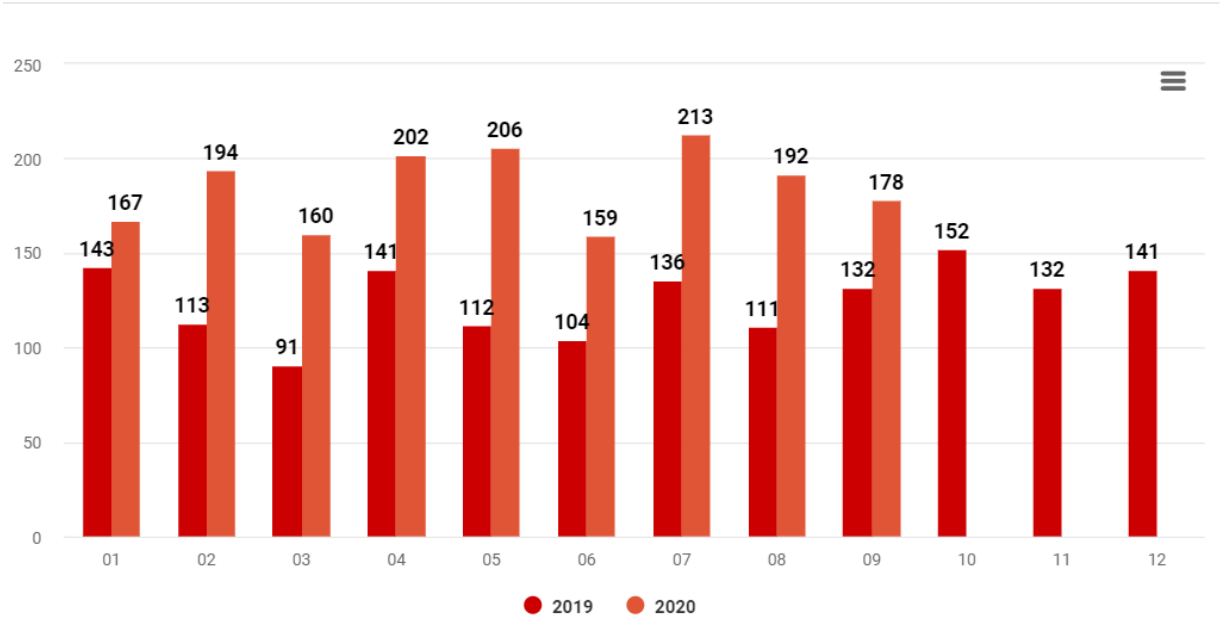


Рисунок 1.4 – График количества инцидентов в 2019 и 2020 годах[6]

[5] https://www.group-ib.ru/resources/threat-research/2018-report.html
[6] https://www.ptsecurity.com/ru-ru/research/analytics/

Для обеспечения информационной безопасности необходимо: определить цели и задачи информационной системы; исследовать бизнес-процессы в информационной системе (функциональные подсистемы, модули и их функции); определить всех пользователей информационной системы (далее – ИС); роли и полномочия пользователей в ИС (права доступа), перечень информационных технологий, обеспечивающих выполнение бизнес-процессов (ИТ-инфраструктура, программное обеспечение, в том числе средства защиты информации, модели и методы доступа пользователей в ИС и т.д.). Непосредственно в части информационной безопасности необходимо определить актуального нарушителя в ИС, определить перечень актуальных угроз безопасности информации (моделирование угроз безопасности информации), спроектировать и внедрить систему информационной безопасности (систему защиты информации), а также проводить на регулярной основе качественную оценку эффективности системы защиты информации. Одной из наиболее важной задачей из перечисленных является оценка эффективности системы защиты информации, качественное проведение которой влияет на уровень защищенности ИС от актуальных угроз безопасности информации.

Под эффективностью системы защиты информации понимается ее способность противостоять угрозам безопасности информации, т.е. эффективность системы защиты информации характеризует уровень защищенности информационной системы. Эффективность системы защиты информации зависит от множества взаимосвязанных между собой подсистем, модулей и элементов, как правило, оцениваемых совокупностью показателей (критерий). На сегодняшний день отсутствует общий подход к проведению оценки эффективности системы защиты информации, что влечет за собой ряд проблем, связанных с процедурами оценивания и определения уровня защищенности информационных систем. Недостатки известных методов и методик оценки эффективности систем защиты информации, связанных в том числе с выбором показателей, также приводят к недостаточно качественному оцениванию эффективности и уровня защищенности информационных систем. Все перечисленное может привести к возникновению

различных рисков для владельцев информационных систем, в том числе связанных с киберрисками.

В настоящее время бизнес-процессы большинства компаний строятся с учетом географии точек их присутствия. Примером могут быть компании, имеющие свои филиалы, представительства и подразделения на все территории страны присутствия и за ее пределами. Это относиться и к процессам государственного управления. Структура государственных органов власти распределена по все территории Российской Федерации, соответственно, их структурные элементы расположены в регионах и субъектах страны. В этой связи современные информационные системы в большинстве случаев представляют собой сложные географически-распределенные (территориально-распределенные) системы с своей ИТ-инфраструктурой, технологией обработки информации и информационными технологиями, реализующими бизнес-процессы или процессы государственного управления.

На основании вышеизложенного целью диссертационного исследования является повышение качества оценки эффективности систем защиты территориально-распределенных информационных систем за счет определения необходимых и достаточных показателей оценки с использованием перспективных технологий, позволяющих наиболее эффективно решать такие задачи, а именно: определение наилучших параметров работы адаптивных нечетких нейронных продукционных систем, как наиболее подходящих для решения таких задач, алгоритмов нечеткого вывода и применение технологий Data Science при обработке большого объема данных.

Степень разработанности темы. Проблемы информационной безопасности в информационных системах, в том числе оценки эффективности СЗИ, оценке соответствия СЗИ, отражены в работах Гвоздика Я.М., Десятова А.Д., Коломойцева В.С., Чемина А.А., Лившица И.И., Буйневича М.В., Зегжды Д.П., Ивашко А.М., Барабанова А.В., Дорофеева А.В., Маркова А.С., Цирлова В.Л., Герасименко В.А., Котенко И.В., Саенко И.Б., Юсупова Р.М., Молдовяна Н.А., Молдовяна А.А., Зикратова И.А., Кустова В.Н., Домарева В.В., Scott Barman, Brian Carrie, Lendver

K., D. Maclean, Norbert Wiener и др. [2-6, 66-68, 82-84]. В настоящей диссертационной работе также использованы результаты исследований, посвященных построению систем поддержки принятия решений в слабоструктурированных предметных областях, обработке трудно формализуемых и нечетких данных, ряда российских и зарубежных ученых: Л. Заде, Т. Саати, О.М. Полещука, Н.В. Хованова и др.

Работа Гвоздика Я.М. [2] посвящена оценке СЗИ автоматизированных систем. В качестве показателей (критериев) оценки выбраны функциональные требования и требования доверия к безопасности руководящего документа ФСТЭК России (Гостехкомиссии) «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий», а также ГОСТ Р ИСО/МЭК ТО 19791-2008. Модель и методика, предложенные автором в данной работе, предназначена для автоматизированных систем без привязки к классам, уровням защищенности и категориям значимости информационных систем, без учета актуальных угроз безопасности информации (далее – УБИ) в ИС и без учета технических решений по защите информации и специфики ИТ-инфраструктуры ИС, например, наиболее распространенных в настоящее время территориально – распределенных ИС (далее – ТРИС). В работе Десятова А.Д. [3] определены показатели (критерии) эффективности системы защиты информации распределенной информационной системы с учетом конфликтных взаимоотношений, разработаны модель и алгоритм оценки показателей эффективности вариантов построения системы защиты информации распределенной информационной системы органов внутренних дел. В работе не рассматривались в качестве показателей актуальные УБИ и требования по защите информации, предъявляемые к определенным типам, классам, уровням защищенности и категориям значимости ИС. В работе Коломойцева В.С. [4] для оценки эффективности СЗИ используется набор критериев, характеризующие задержки поиска угроз, вероятность их обнаружения и надежность системы по выполнению требуемых функций, при этом для эффективности не учитываются перечень требований по защите информации, что не позволяет учитывать оценку

соответствия ИС по требованиям защиты информации. В работе Чемина А.А. [5] сформированы базовые положения, описывающие оценку эффективности выполнения политик безопасности в зависимости от возникающих инцидентов и предложен метод расчета количественной оценки уровня защищенности ИС специального назначения. При этом в работе не учитываются такие обязательные показатели оценки эффективности, как: требования по ИБ, степень нейтрализации угроз безопасности информации, актуальных для ТРИС, а также показатели эффективности с точки зрения финансовых затрат на создание СЗИ ТРИС, не раскрыта степень детализации задачи оптимальности состава комплекса средств защиты информации при разработке СЗИ ИС специального назначения.

Существующие методы и методики определения (моделирования) актуальных угроз безопасности информации и оценки эффективности СЗИ не могут быть применены на всех этапах жизненного цикла ТРИС, не учитывают в совокупности такие показатели, как: ИТ-инфраструктура ТРИС, актуальные УБИ, требований по ИБ, перечень средств защиты информации и их стоимость, как важных показателей при выполнении таких задач. Одновременно с этим, для известных методов и методик моделирования УБИ и оценки эффективности СЗИ ТРИС остается цель – повышение эффективности с точки зрения определения количества актуальных УБИ, выполнения требований по ИБ, снижения стоимости затрат на создание СЗИ ТРИС, а также исключения ошибок экспертов. Для математического аппаратов существующих методов остается актуальной задача уменьшения среднеквадратической ошибки работы адаптивных нечетких нейронных продукционных систем.

На основании изложенного можно сделать вывод о необходимости совершенствования методов и методик оценки эффективности СЗИ, что подтверждает актуальность настоящего диссертационного исследования.

Объектом исследования являются угрозы безопасности и требования по защите информации.

Предметом исследования являются методы и методики моделирования актуальных угроз безопасности информации и оценки эффективности систем защиты информации.

Целью диссертационного исследования является повышение качества оценки эффективности систем защиты территориально-распределенных информационных систем за счет определения необходимых и достаточных показателей.

Для достижения поставленной цели необходимо выполнить следующие **задачи**:

1. Провести анализ ТРИС: определить основные бизнес-процессы; информацию, обрабатываемую в ТРИС; группы пользователей, имеющих доступ в ТРИС, их права и полномочия; выявить основные аспекты технологии обработки информации; исследовать ИТ-инфраструктуру ТРИС (информационные технологий и программное обеспечение, реализующее бизнес-процессы ТРИС); провести анализ атак и угроз безопасности информации в ТРИС, требований по защите информации в ТРИС; анализ СЗИ ТРИС; анализ существующих методов и методик моделирования УБИ и оценки эффективности СЗИ ТРИС.
2. Повысить качество определения актуальных угроз безопасности информации в ТРИС за счет определения необходимых и достаточных показателей, достижения наименьшей среднеквадратической ошибки работы методики, автоматизации процесса для исключения недостатков экспертных методов и применения технологий Data Science при обработке большого объема данных.
3. Повысить качество оценки эффективности СЗИ ТРИС за счет определения необходимых и достаточных показателей оценки, уменьшения значений среднеквадратической ошибки работы адаптивных нечетких нейронных продукционных систем по сравнению с известными методами, автоматизировать процесс для исключения недостатков экспертных методов.

4. Разработать методические рекомендации по оценке эффективности систем защиты ТРИС, позволяющие в автоматизированном режиме оценивать эффективность СЗИ на всех этапах жизненного цикла ТРИС с точки зрения нейтрализации актуальных УБИ, соответствия по требованиям ИБ, уменьшения финансовых затрат на создание СЗИ, за счет внесения изменений в алгоритмы известных методик.
5. Провести оценки эффективности предложенных методов и методик.

Научная задача диссертационного исследования состоит в том, чтобы повысить качество оценки эффективности СЗИ ТРИС, предложив автоматизированные методику определения актуальных УБИ и метод оценки эффективности СЗИ ТРИС, основанные на адаптивных нечетких нейронных продукционных систем, за счет определения необходимых и достаточных показателей и адаптации параметров таких систем.

Математическая запись поставленной задачи может быть представлена как:

найти наименьшее значение RMSE:

$$RMSE = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(y_i - \hat{y}_i)^2},$$

где $y_i, \hat{y}_i$ – наборы данных (обучения, проверки), N – число элементов в обучающей выборке, определив необходимые и достаточные показатели при определении актуальных УБИ, оценки эффективности СЗИ и наилучшие параметры адаптивных нечетких нейронных продукционных систем и алгоритмов нечеткого вывода.

Научная новизна результатов исследования заключается в следующем:

1. Предложенная методика определения актуальных угроз безопасности информации, в отличие от известных, в автоматизированном режиме определяет перечень актуальных УБИ, гипотетически исключая ошибки экспертов.
2. Предложенный метод оценки эффективности систем защиты информации, в отличие от известных, основан на теории адаптивных

нечетких нейронных продукционных системе и алгоритме нечеткого вывода Такаги-Сугено-Канга с применением технологий Data Science.

3. Разработанные методические рекомендации по оценке эффективности систем защиты информации в территориально-распределенных информационных системах, в отличие от известных, позволяют сократить количество не учтенных актуальных угроз безопасности информации, снизить финансовые затраты на создание системы защиты информации, применимы на всех этапах жизненного цикла систем, могут быть адаптированы под требования владельцев ТРИС. Использование рекомендаций не требует привлечения высококвалифицированных специалистов по информационной безопасности, тем самым исключает недостатки существующих методик, не требует больших вычислительных ресурсов, предлагает автоматизированный режим работы, что, в совокупности, повышает эффективность систем защиты информации в территориально-распределенных информационных системах.

Теоретическая и практическая значимости диссертационного исследования. Теоретическая ценность диссертационного исследования заключается ее вкладом в развитие теории и методов обеспечения информационной безопасности, а именно: определения необходимых и достаточных показателей определения актуальных УБИ и оценки эффективности СЗИ; расширении класса методов оценки эффективности СЗИ ТРИС в части адаптации регулятора адаптивной нечеткой нейронной продукционной системы, достигаемой применением нейрона с последовательным методом обучения; доказательством достижения наименьшей среднеквадратической ошибки работы ANFIS при применения алгоритма нечеткого вывода Такаги-Сугено-Канга для решения поставленной задачи; использования технологий Data Science при обработке большого объема данных при определении актуальных УБИ и оценки эффективности СЗИ в части очистки и преобразования наборов данных, выбора наиболее полезных и создание новых более репрезентативных признаков.

Практическая ценность работы заключается в следующих результатах:

1. Проведенный анализ ТРИС выявил основные бизнес-процессы, выполняемые системами; виды и категории информации; группы пользователей и методы доступа к ТРИС; аспекты технологий обработки информации и ИТ-инфраструктуры систем. Анализ атак и угроз безопасности информации в ТРИС, требований по защите информации, анализ СЗИ ТРИС, анализ существующих методов и методик моделирования УБИ и оценки эффективности СЗИ позволил использовать полученные результаты при определении необходимых и достаточных показателей моделирования УБИ и оценки эффективности СЗИ ТРИС.
2. Предложенная методика определения актуальных угроз безопасности информации позволяет определять на 5% больше актуальных УБИ, гипотетически исключая недостатки экспертов и минимизирует трудоемкость процесса и вычислительные ресурсы, в отличие от известных методик.
3. Предложенные метод и методические рекомендации по оценке эффективности СЗИ ТРИС позволяют проводить оценку эффективности СЗИ на основе необходимых и достаточных показателей, определенных в настоящем диссертационном исследовании, предоставляют владельцам ТРИС возможность оценивать эффективность СЗИ в реальном времени на всех этапах жизненного цикла существования ТРИС, гипотетически исключая ошибки экспертов, что, в свою очередь, позволяет своевременно вносить корректировки в проектные решения СЗИ для нейтрализации УБИ и выполнения требований по защите информации, учитывая финансовую составляющую при создании СЗИ. Показатели оценки эффективности могут быть изменены в зависимости от целей и потребностей владельца ТРИС в проведении оценки эффективности СЗИ ТРИС.
4. Разработанные в рамках диссертационного исследования программы для ЭВМ «Модель угроз и нарушителя» и «Оценка системы защиты

информации» автоматизируют процессы определения перечня актуальных УБИ и проведения оценки эффективности СЗИ.

Внедрение результатов. Результаты диссертации использованы при определении перечня актуальных угроз безопасности и проведении оценки эффективности систем защиты территориально-распределенных информационных систем в ЗАО «ДИДЖИТАЛ ДИЗАЙН», ООО «Рэйдикс» и ЗАО НПФ «УРАН» (Приложение В, Г, Д). Разработана программа для ЭВМ «Модель угроз и нарушителя» (Приложение А), реализующая предложенную методику определения актуальных угроз безопасности информации и автоматизирующее этот процесс. Разработана программа для ЭВМ «Оценка системы защиты информации» (Приложение Б), реализующая предложенный метод оценки эффективности СЗИ. Результаты работы были внедрены в учебный процесс СПбГУТ на старших курсах обучения бакалавров по направлению подготовки 10.03.01 «Информационная безопасность» по дисциплине «Методы оценки безопасности компьютерных систем» (рабочая программа дисциплины, регистрационный № 18.05/1185-Д) и магистров первого года обучения по направлению подготовки 10.04.01 «Информационная безопасность» по дисциплине «Сертификация средств защиты информации» (рабочая программа дисциплины, регистрационный № 20.05/330-Д) при чтении курсов лекций, проведении практических занятий и лабораторных работ (Приложение Е).

Методология и методы исследования. В работе использованы методы неявного перебора, теории вероятности и математической статистики, динамического программирования, теории адаптивных нечетких нейронных продукционных систем, алгоритмы нечеткого вывода.

Основные результаты, выносимые на защиту.

1. Методика определения актуальных угроз безопасности информации.
2. Метод оценки эффективности систем защиты информации.
3. Методические рекомендации по оценке эффективности систем защиты территориально-распределенных информационных систем.

Достоверность результатов. Достоверность результатов, выносимых на защиту диссертационного исследования, выводов научного характера подтверждаются математическим обоснованием результатов исследований, системным подходом к решению поставленных задач, обоснованием выбранных методов и показателей определения актуальных УБИ и оценки эффективности СЗИ, доказательствами и результатами экспериментальной проверки предложенных метода и методик, анализом работ существующих зарубежных и отечественных практик решения аналогичных задач, апробацией результатов работы на международных и российских конференциях, а также подтверждением о внедрении предложенных метода и методик в организациях и предприятиях.

Апробация работы. Результаты, полученные в рамках работы над диссертацией, представлялись и обсуждались на следующих конференциях:

IX и X Международная научно-техническая и научно-методическая конференции «Актуальные проблемы инфотелекоммуникаций в науке и образовании» (Россия, Санкт-Петербург, 2020 – 2021 гг.).

XII Международный конгресс по ультрасовременным системам телекоммуникаций и управления (THE 12TH INTERNATIONAL CONGRESS ON ULTRA MODERN TELECOMMUNICATIONS AND CONTROL SYSTEMS). Brno, Czech Republic, 5-7 октября 2020 г. Online.

X Международная научно-техническая конференция «Технологии разработки информационных систем» (Россия, г. Геленджик, 7-12 сентября 2020 г., online).

Всероссийская межведомственная научно-техническая конференция «НАУКА И АСУ — 2020» (Россия, г. Москва, 20 октября 2020 г., online).

XX Международная конференция «Распределенные компьютерные и телекоммуникационные сети: управление, вычисление, связь» (DCCN-2017, Москва, 25–29 сентября 2017 г.).

IV, V и VI Всероссийская конференция «Проблема комплексного обеспечения информационной безопасности и совершенствование

образовательных технологий подготовки специалистов силовых структур» (Россия, Санкт-Петербург, 2015-2017 гг.).

Диссертация выполнена при поддержке гранта для студентов вузов, расположенных на территории Санкт-Петербурга, аспирантов вузов, отраслевых и академических институтов, расположенных на территории Санкт-Петербурга (Россия, Санкт-Петербург, 2015 г.). Диплом № 15542 от 27.11.2015 г.

Подготовлено учебно-методическое пособие «Сертификация средств защиты информации» (Россия, Санкт-Петербург, СПбГУТ).

Публикации. По материалам диссертационной работы опубликовано 16 работ, в том числе 6 – в рецензируемых изданиях из перечня ВАК при Минобрнауки России («Наукоемкие технологии в космических исследованиях Земли», «Информатизация и связь», «Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1. Естественные и технические науки»), 2 – в изданиях, индексируемых в международной базе Scopus, получены 2 свидетельства о государственной регистрации программы для ЭВМ.

Соответствие паспорту специальности. Все результаты, выносимые на защиту, сопоставлены с пунктами 1, 3 и 10 паспорта искомой специальности «Методы и системы защиты информации, информационная безопасность»: «Теория и методология обеспечения информационной безопасности и защиты информации», «Методы, модели и средства выявления, идентификации и классификации угроз нарушения информационной безопасности объектов различного вида и класса» и «Модели и методы оценки эффективности систем (комплексов) обеспечения информационной безопасности объектов защиты», соответственно.

Личный вклад автора. В работе предложены методика определения актуальных угроз безопасности информации, метод и методические рекомендации по оценке эффективности систем защиты в территориально-распределенных информационных системах, разработаны программы для ЭВМ, реализующие предложенные методики и методы, положения работы были внедрены в учебный процесс СПбГУТ. Перечисленные результаты получены автором лично.

Глава 1. Анализ моделей и методов построения систем, атак и угроз безопасности информации, оценки эффективности систем защиты информации

1.1 Анализ моделей и методов построения информационных систем

Моделирование систем является одним из основных методов исследования во всех областях знаний и научно обоснованным методом оценок характеристик сложных систем. Под моделированием информационных систем понимается замещение существующей реальной ИС другой с целью получения информации о важных свойствах оригинальной ИС с помощью модели (объекта-модели) ИС [72]. Аналогично для моделирования атак и систем защиты ИС.

В основе моделирования лежит теория подобия, основная суть которой заключается в том, что абсолютное подобие может существовать только тогда, когда можно заменить один объект другим, точно таким же. В настоящее время существует следующая классификация видов моделирования систем, представленная на рисунке 1.5.

Рисунок 1.5 – Классификация видов моделирования систем

В соответствии с классификационными признаками модели делятся на полные, неполные и приближенные. В зависимости от характеристик в процессах ИС *S* модели делятся на: детерминированные и стохастические, статические и динамические, дискретные, непрерывные и дискретно-непрерывные. Детерминированное моделирование отображает процессы, в которых отсутствуют случайные воздействия. Стохастическое моделирование отображает вероятностные процессы и события. Статическое моделирование описывает поведение ИС в какой-либо момент времени. Динамическое – отражает поведение ИС во времени. Дискретное моделирование описывает процессы, которые являются дискретными, а непрерывное – непрерывные процессы в ИС. Дискретно-непрерывное моделирование используется при описании дискретных и непрерывных процессов [85].

Моделирование ИС *S* разделяют на мысленное и реальное.

Мысленное моделирование используется при моделировании объектов, которые либо нереализуемы в определенном интервале времени, либо существуют вне условий, возможных для их создания.

При наглядном моделировании формируются наглядные модели ИС, отображающие явления и процессы, протекающие в ИС. В гипотетическом моделировании закладывается гипотеза о закономерностях процессов в реальной ИС, которая отражает уровень знаний эксперта о ИС и базируется на причинно-следственных связях между входом и выходом изучаемой ИС. Такое моделирование используется, когда знаний об ИС недостаточно для построения формальных моделей.

Аналоговое моделирование использует аналогии различных уровней. Наилучшим уровнем является полная аналогия исследуемой ИС.

Макетирование применяется, когда протекающие в реальной ИС процессы не поддаются физическому моделированию. В основе макетов также лежат аналоги ИС, базирующиеся на причинно-следственных связях между явлениями и процессами ИС. Знаковое моделирование реализуется, если вводятся условные обозначения отдельных понятий, с помощью знаков отображается набор понятий –

отдельные цепочки из слов и предложений. Используя операции теории множеств, можно в отдельных символах дать описание какой-либо реальной ИС.

В языковом моделировании в основе лежит тезаурус, базирующийся из фиксированного набора входящих понятий.

Символическое моделирование – процесс создания логической ИС, которая замещает реальную и выражает основные свойства ее взаимосвязей с помощью определенной системы знаков или символов.

При математическом моделировании для исследования характеристик процесса функционирования ИС *S* математическими методами должна быть проведена формализация этого процесса, т.е. построена математическая модель. Математическое моделирование – процесс установления соответствия реальной ИС некоторого математического объекта – математической модели.

При аналитическом моделировании процессы функционирования элементов ИС записываются в виде некоторых функциональных соотношений (алгебраических, интегродифференциальных, конечно-разностных и т.д.) или логических условий. Аналитическая модель исследуется аналитическим, численным и качественным методами.

При имитационном моделировании алгоритм воспроизводит процесс функционирования ИС *S* во времени. При таком моделировании имитируются явления, составляющие процессы ИС, с сохранением логической структуры и последовательности протекания во времени.

Комбинированное (аналитико-имитационное) моделирование ИС объединяет достоинства аналитического и имитационного моделирования. При построении комбинированным методом ИС осуществляется декомпозиция процесса функционирования на подпроцессы. Для подпроцессов, где возможно, используются аналитические модели, для остальных – имитационные.

При реальном моделировании исследуются характеристики на реальной ИС либо ее частях. Такое моделирование проводится на системах, работающих в нормальных условиях, так и при организации специальных условий для оценки

интересующих характеристик. Реальное моделирование является наиболее эффективным, но его возможности с учетом исследуемой системы ограничены.

Натурное моделирование – исследование на реальной ИС с последующей обработкой результатов на основе теории подобия. При натурном моделировании используются такие разновидности экспериментов, как производственный эксперимент и комплексные испытания, обладающие высокой степенью достоверности.

При физическом моделировании ИС проводятся в среде функционирования, которая сохраняет природу явлений и обладает физическим подобием. Физическое моделирование может протекать в реальном и нереальном масштабах времени, а также без учета времени.

В настоящее время средством моделирования систем являются средства вычислительной техники (далее – СВТ). При моделировании систем необходимы следующие виды обеспечения.

При построении математической модели «каждая конкретная система *S* характеризуется набором свойств, отражающих поведение исследуемой модели и учитывающие условия ее взаимодействия с внешней средой *E*. Модель *S* можно представить в виде множества величин, описывающих процессы функционирования реальной системы и образующих следующие подмножества»:

Совокупность входных воздействий на систему:

$$\mathrm{x_i} \epsilon\, \mathrm{X}, \mathrm{i} = \overline{1, \mathrm{n_x}},$$

Совокупность воздействий внешней среды:

$$v_l \epsilon\, V, \mathrm{l} = \overline{1, n_{\mathrm{V}}},$$

Совокупность внутренних параметров системы:

$$h_k \epsilon\, H, \mathrm{k} = \overline{1, n_{\mathrm{H}}},$$

Совокупность выходных характеристик:

$$y_j \epsilon\, Y, \mathrm{j} = \overline{1, n_{\mathrm{Y}}},$$

Переменные $\mathrm{x_i}, v_l, h_k, y_j$ являются элементами непересекающихся подмножеств и содержат детерминированные и стохастические составляющие.

При моделировании системы S входные воздействия, воздействия внешней среды E и внутренние параметры системы являются независимыми (экзогенными) переменными, которые в векторной форме имеют вид:

$$\vec{x}(t) = (x_1(t), x_2(t), \dots, x_{nX}(t));$$
$$\vec{v}(t) = (v_1(t), v(t), \dots, v_{nV}(t));$$
$$\vec{h}(t) = (h_1(t), h_2(t), \dots, h_{nH}(t));$$

а выходные характеристики системы S являются зависимыми (эндогенными) переменными и векторной форме имеют вид

$$\vec{y}(t) = (y(t), y(t), \dots, y_{nY}(t));$$

Функционирование S описывается оператором F_s:

$$\vec{y}(t) = F_s(\vec{x}, \vec{v}, \vec{h}, t) \quad (1.1)$$

Зависимость (1.1) является законом функционирования системы S - F_s. F_s.

Алгоритм функционирования A_s – метод получения выходных характеристик с учетом входных воздействий $\vec{x}(t)$, воздействий внешней среды $\vec{v}(t)$ и собственных параметров системы $\vec{h}(t)$. Один и тоже закон функционирования F_s системы S может быть реализован разными способами – множеством различных алгоритмов функционирования A_s.

Соотношение (1.1) является математическим описанием системы моделирования S во времени t. Соответственно, математические модели такого вида являются динамическими.

Также (1.1) может быть задано различными способами: аналитически, графически, таблично и т.д. Такие соотношения могут быть получены через свойства системы S в конкретные моменты времени – состояния. Состояние S характеризуется векторами:

$$\vec{z}' = (z_1', z_2', \dots, z_k') \text{ и } z'' = (\vec{z}_1'', \vec{z}_2'', \dots, \vec{z}_k''),$$

где $z_1' = z_1(t'), z_2' = z_2(t'), \dots, z_k' = z_k(t')$ в момент $t' \epsilon\ (t_0, T)$; $z_1'' = z_1(t''), z_2'' = z_2(t''), \dots, z_k'' = z_k(t'')$ в момент $t'' \epsilon\ (t_0, T)$ и т.д., где $k = \overline{1, n_Z}$.

Состояние системы S в момент времени $t_0 \le t^* \le T$полностью определятся начальными условиями $\vec{z}^0 = (z_1^0, z_2^0, \dots, z_k^0)$, входными воздействиями $\vec{x}(t)$,

воздействиями внешней среды $\vec{v}(t)$ и внутренними параметрами $\vec{h}(t)$, которые имели место за промежуток времени $t^* - t_0$ с помощью двух векторных уравнений

$$z(t) = \Phi(\vec{z}^0, \vec{x}, \vec{v}, \vec{h}, t)$$
$$= F(\vec{z}, t)$$

Таким образом цепочка уравнений системы «вход – состояние - выход» определяет характеристики системы:

$$\vec{y}(t) = F\left[\Phi(\vec{z}^0, \vec{x}, \vec{v}, \vec{h}, t)\right]$$

Под математической моделью системы «понимается конечное подмножество переменных $\{\vec{x}(t), \vec{v}(t). \vec{h}(t)\}$ с математическими связями между ними и характеристиками $\vec{y}(t)$» [83].

Детерминированная модель (D - схема) описывается в общем виде

$$\vec{y}' = \vec{f}(\vec{y}, t);\ \vec{y}(t_0) = \vec{y}_0,$$

где $\vec{y}' = d\vec{y}/dt$, $\vec{y} = (y_1, y_2, \dots, y_n)$ и $\vec{f} = (f_1, f_2, \dots, f_n)$ - n – мерные векторы $f\left(\vec{y}, \vec{t}\right)$ – вектор-функция, определенная на некотором (n+1)-мерном $(\vec{y}, t)$ множестве и является непрерывной.

Дискретно-детерминированные модели F-схемы. В основе лежит теория автоматов, математическая модель – автомат, понятие которого варьируется в зависимости от характера системы.

Автомат задается F-схемой

$$F = \langle Z, X, Y, \varphi, \psi, z_0 \rangle,$$

которая функционирует в дискретном автоматном времени, где X- входные сигналы, Z - множество внутренних состояний системы, Y- выходные сигналы, начальное состояние z_0, $z_0 \epsilon\ Z$, функция перехода $\varphi(z, x)$, функция выхода $\psi(z, x)$.

Дискретно-стохастические модели (P-схемы). Модель построена на вероятностных автоматах – P-автомата.

Непрерывно-стохастические модели (Q-схемы). Системы массового обслуживания – Q-схемы (queueing system).

Сетевые модели (N-схемы) сети Петри. Для решения задач, связанных с формализованным описанием и анализом причинно-следственных связей в сложных системах. Самым распространенным формализмом, описывающим структуру и взаимодействие параллельных систем и процессов, являются сети Петри.

Сеть Петри (N-схема) задается следующим образом:

$$N = \langle B, D, I, O \rangle,$$

B – позиции, D – переходы, I – входная функция, O – выходная функция.

Для каждого перехода $d_j \epsilon\ D$ можно определить множество входных позиций перехода $I(d_j)$ и выходных позиций перехода $O(d_j)$ как

$$I(d_j) = \{b_i \epsilon B | I(b_i, d_j) = 1\},$$

$$O(d_j) = \{b_i \epsilon B | O(d_j, b_i) = 1\},$$

$$i = \overline{1,n};\ j = \overline{1,m}; n = |B|, m = |D|.$$

Аналогично для каждого перехода $b_i \epsilon B$ вводятся определения множества входных переходов позиции $I(b_i)$ и множества выходных переходов позиции $O(b_i)$.

Классификация методов построения моделей приведена на рисунке 1.6.

Рисунок 1.6 – Классификация методов построения моделей

Каждая модель и методы имеют свои преимущества и недостатки. Основными недостатками перечисленных моделей являются:

1. При моделировании не всегда существует возможность выявления новых качественных характеристик.
2. Любая модель минимизирует объяснения возможных явлений.
3. Статистические модели могут быть объективными только в пределах эмпирического множества построения модели.
4. Как правило, необходимых данных для настройки моделей не хватает.

На основании вышеизложенного можно сделать вывод о том, что существующие методы построения моделей имеют ряд своих недостатков, что, в свою очередь, доказывает необходимость их совершенствования.

1.2 Анализ ИТ - архитектуры и систем защиты информации

С ростом и развитием информационных технологий растет и сложность архитектуры ИС. Современные типовые ИС представляет собой клиент – серверные территориально-распределенные многопользовательские архитектуры. Программное обеспечение (как правило, прикладное программное обеспечение) предоставляет возможности функциональных модификаций на базе открытого программного интерфейса (API) с использованием распространенных языков программирования (таких как C#, TypeScript (платформа разработки Angular, среда разработки dotnet.core) и т.д.).

ИС обеспечивают принцип централизованного хранения, накопления и многократного использования данных. Для экономии ресурсов и обеспечения информационной безопасности на автоматизированных рабочих местах (далее – АРМ) пользователей хранение данных не осуществляется. Обработка осуществляется на стороне серверной части [65]. Для этого могут использоваться технологии терминального доступа. Такая технология может быть реализована в IT-инфраструктуре путем развертывания терминальной фермы RDS (Remote Desktop Services). При такой технологии рабочие профили пользователей хранятся на серверах терминальной фермы. Это упрощает организацию доступа пользователей к информационным ресурсам ИС, а также наиболее эффективно обеспечивает процессы информационной безопасности. Также технология обеспечивает процессы при удаленной работе пользователей [60].

Для ТРИС характерно размещение серверных компонент, сетевого оборудования и АРМ пользователей на всей территории страны и, возможно, за ее пределами. В этом случае такие ИС имеют сложную архитектуру с точки зрения расположения своих компонентов и технологий обработки информации. Соответственно, возникают и сложности с обеспечением информационной безопасности [82-84].

В состав типовой территориально-распределенной ИС входят следующие компоненты:

1. серверы, включающие:
- серверное оборудование;
- прикладные и специализированные программы, обеспечивающие обработку информации и ее представление в виде, необходимом для последующей автоматизированной обработки;
2. АРМ пользователей:
- типовые АРМ пользователя (стационарные ПК);
- мобильное АРМ: планшеты, мобильные телефоны.

Для обеспечения защиты информации, предаваемой по открытым каналам связи, используется криптографическая защита между площадками ИС [82].

На мобильных АРМ, расположенных за пределами локальной вычислительной сети ИС и осуществляющих информационный обмен с серверами ИС применяются средства криптографической защиты информации.

ИС взаимодействуют в другими ИС для обмена необходимой информации, для интеграции между собой.

Как и в большинстве территориально-распределенных системах присутствуют иные категории пользователей, не относящихся к работникам владельца ИС. К таким категориям пользователей относятся разработчики программного обеспечения (далее – ПО) и технических средств (далее – ТС) – лица, обеспечивающие разработку, поставку и внедрение программных, аппаратно-программных и аппаратных средств ИС. Обслуживающий персонал – лица, обеспечивающие штатное функционирование ТС ИС (работники эксплуатационных подразделений владельца ИС, осуществляющие обслуживание и техническое сопровождение инженерных систем и помещений, в которых размещается оборудование ИС) [88].

Рассмотрим объекты ТРИС, которые потенциально относятся к объектам защиты. В соответствии с руководящими документами и нормативными правовыми актами регуляторов Российской Федерации в области обеспечения информационной безопасности [22-27] к объектам защиты ТРИС относятся [83]:

- информация, обрабатываемые в ТРИС;

- ТС, предназначенные для обработки информации;
- системное и прикладное ПО;
- средства защиты информации (далее – СрЗИ);
- средства криптографической защиты информации (далее – СКЗИ);
- среда функционирования (далее – СФ) СКЗИ;
- информация, относящаяся к криптографической защите информации, включая ключевую, парольную и аутентифицирующую информацию СКЗИ;
- документы, дела, журналы, картотеки, издания, технические документы, видео-, кино- и фотоматериалы, рабочие материалы и т.п., в которых отражена защищаемая информация, относящаяся к ТРИС и их криптографической защите, включая документацию на СКЗИ и на технические и программные компоненты СФ;
- носители защищаемой информации, используемые в ТРИС в процессе криптографической защиты информации, носители ключевой, парольной и аутентифицирующей информации СКЗИ и порядок доступа к ним;
- используемые ТРИС каналы связи;
- помещения, в которых находятся ресурсы ТРИС, имеющие отношение к криптографической защите информации.

Типовая структурная схема комплекса технических средств ТРИС представлена на рисунке 1.7.

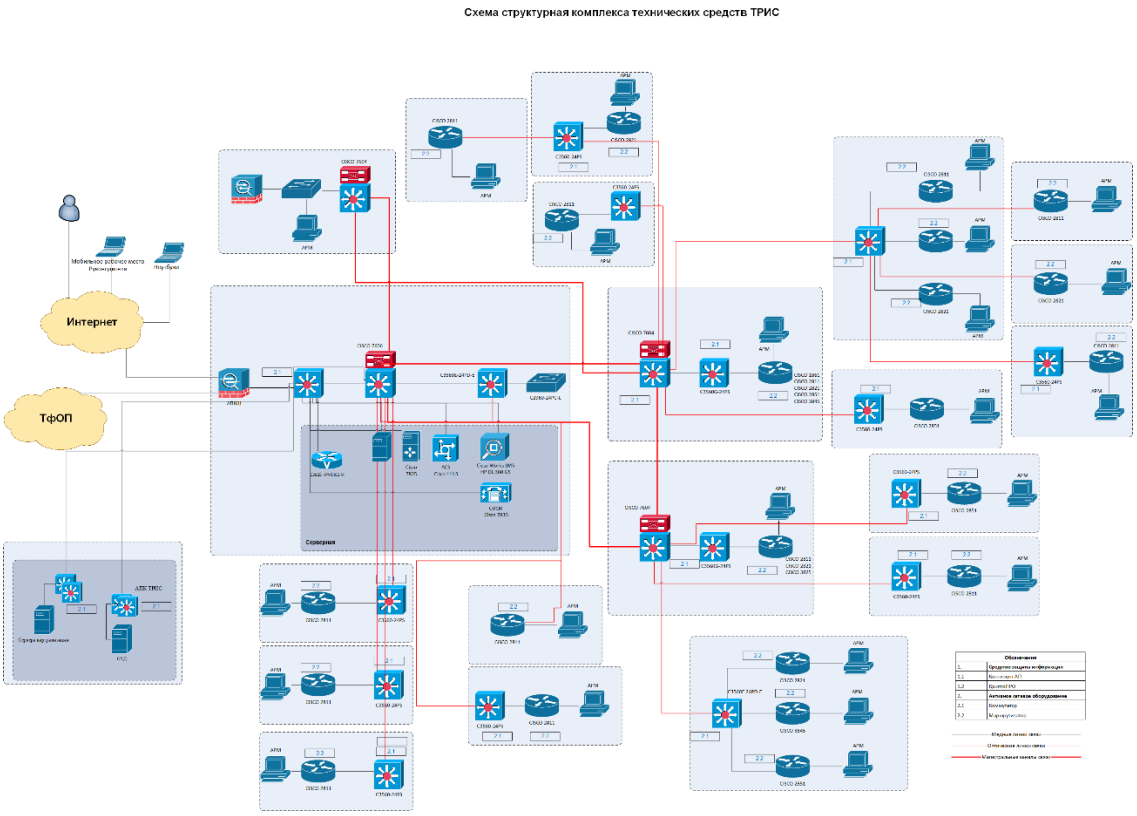


Рисунок 1.7 – Типовая структурная схема комплекса технических средств ТРИС

На основании вышеизложенного следует, что ТРИС имеют ряд своих аспектов ИТ-инфраструктуры, которые необходимо учитывать при моделировании УБИ и при формировании показателей оценки эффективности СЗИ. Ключевыми аспектами являются: географическая распределенность ИС, незащищенные сети передачи данных (каналы связи), клиент-серверные приложения, обработка информации в центрах обработки данных, облачные инфраструктуры (IaaS, SaaS, PaaS) [97-99]. Особое внимание необходимо уделять категориям нарушителей в ТРИС, которыми являются как внешние, так и внутренние группы нарушителей [80].

1.3 Анализ моделей угроз безопасности информации и атак на информационные системы

Статические модели угроз безопасности информации включают в себя описание выявленных УБИ, анализ исходной защищенности ИС, описание

возможных нарушителей, оценку реализуемости и опасности угроз, перечень актуальных угроз безопасности информации в ИС. Разрабатываются экспертами владельцев ИС с учетом назначения, условий и особенностей функционирования ИС.

Статические модели УБИ имеют следующие недостатки [90, 91]:

- недостатки экспертных методов (экспертных оценок);
- разрабатываются на текущее состояние ИС, в этой связи возникают сложности в постоянной актуализации таких моделей УБИ в конкретные определенный момент времени – проблема поддержки в актуальном состоянии модели УБИ;
- не учитывают все необходимые показатели при определении перечня актуальных УБИ, а именно: изменения в модели рисков (негативных последствий от реализации УБИ); изменение условий эксплуатации объектов воздействия (элементы архитектуры ИС, обрабатывающие защищаемую информацию); версионность СПО, ППО; динамично развивающиеся способы реализации, тактик и техник атак;
- не рациональное использование множества известных баз данных УБИ, уязвимостей, тактик и техник атак (MITRE ATT&CK, CVE, CWE, OSVDB, NVD, Secunia и т.д.);
- как следствие, некачественная оценка эффективности СЗИ (уровня защищенности ИС).

В соответствии с ГОСТ [40] «компьютерная атака - целенаправленное несанкционированное воздействие на информацию, на ресурс автоматизированной информационной системы или получение несанкционированного доступа к ним с применением программных или программно-аппаратных средств». Под объектом атаки (цель атаки) понимается элемент ТРИС. В настоящее время существует множество моделей атак, методов и средств моделирования атак. Нарушитель – «любое лицо, преднамеренно использующее уязвимости технических и нетехнических мер и средств контроля и управления безопасностью с целью

захвата или компрометации информационных систем и сетей, или снижения доступности ресурсов информационной системы и сетевых ресурсов для законных пользователей».

Основные модели атак на информационные системы представлены на рисунке 1.8 [66].

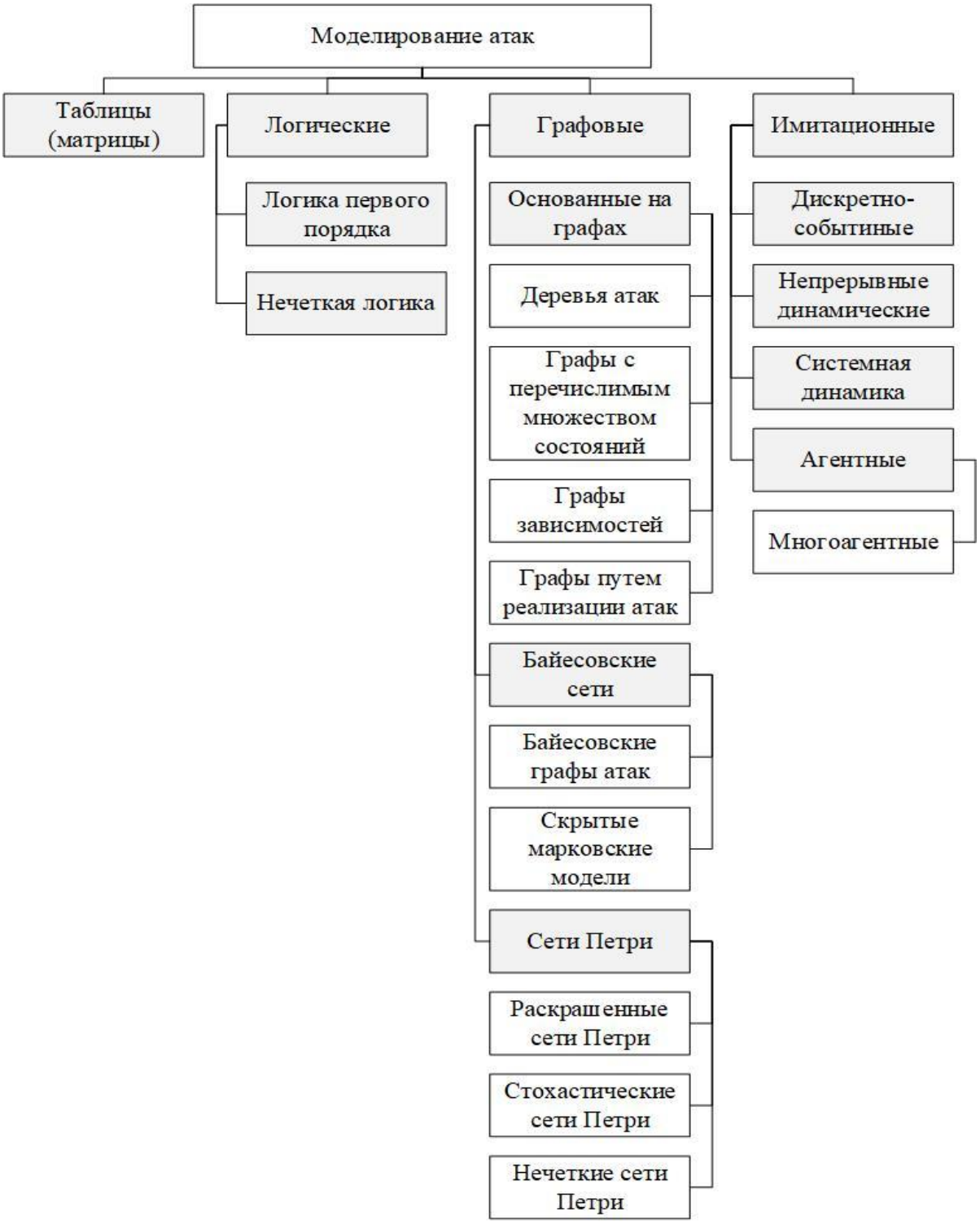


Рисунок 1.8 – Модели атак на информационные системы

Преимущества и недостатки основных моделей атак представлены в таблице 1.1.

Таблица 1.1 – Преимущества и недостатки моделей атак

№ п/п	Модель	Преимущества	Недостатки
1.	Табличные (матричные)	Наиболее простые	Сложна при моделировании циклических атак, большого количества связей между инцидентами или действиями нарушителя
2.	Логические	Обработка инцидентов и использование языков представления знаний о предметной области. Учитывает случаи неопределенности входных данных о моделируемых атаках	Использование ППО, обеспечивающее механизмы логического вывода; Требует значительных вычислительных ресурсов
3.	Графовые	Предназначены для решения большего числа задач, таких как «анализ инцидентов, обнаружения атак, оценка эффективности СЗИ, определение мер по ИБ, минимизация рисков и ресурсов для обеспечения ИБ	Масштабируемость, связанная с формированием графа для ТРИС с большим числом элементов
4.	Графовые на деревьях атак	Наглядность, масштабируемость, адаптируемость, универсальность	Сложны при моделировании циклических атак; Отсутствие динамического моделирования
5.	Байесовские графы	Наглядность, масштабируемость, адаптируемость, универсальность. учитывает случаи неопределенности входных данных об атаках	Сложны при моделировании циклических атак; Отсутствие динамического моделирования

Таблица 1.1. Продолжение

6.	Сети Петри	Удобство моделирования динамических и параллельных процессов, способны отражать вероятностные процессы, использование временных параметров, простота изучения и использования, наличие большого количества инструментальных средств, возможность использования для анализа различных аспектов ИБ исследуемой ТРИС	Неспособность описывать поведение нарушителя и цели атаки
7.	Имитационные	Позволяют моделировать поведенческие характеристики нарушителя и цели атаки. Удобны для моделирования распределенных атак, имеют широкий спектр инструментальных средств	Требуют больших вычислительных ресурсов

Модели атак имеют ряд общих недостатков, а именно:

- сложность моделирования;
- требуют вычислительных ресурсов;
- требуют привлечения высококвалифицированных специалистов в области ИБ;
- ошибки экспертных методов (экспертных оценок).

На основании проведенного анализа можно сделать вывод о необходимости совершенствования и разработки новых методик определения актуальных УБИ (моделирования УБИ), исключающих недостатки существующих.

1.4 Анализ международных стандартов в области обеспечения безопасности информации

В современном мире сложилась большая нормативная база стандартов и лучших практик по информационной безопасности [89]. Существуют множество

нормативных документов, но начать стоит с серии стандартов ISO 27x [41, 45-48, 102, 103] Международной Организации по Стандартизации (International Organization for Standardization, ISO) и Международной Электротехнической Комиссии (International Electrotechnical Commission, IEC). Серия стандартов содержит лучшие практики и рекомендации по создания, развитию и поддержанию системы менеджмента информационной безопасности (далее – СМИБ) [104]. Перечень стандартов и неутвержденных проектов стандартов на сегодняшний день серии 27x представлен в таблице 1.2.

Таблица 1.2 – Перечень стандартов серии 27x

Номер стандарта ISO	**Номер соответствующего стандарта ГОСТ**	**Наименование стандарта**
ISO/IEC27000	ГОСТ Р ИСО/МЭК 27000-2012	«Информационные технологии - Методы обеспечения безопасности - Системы менеджмента информационной безопасности - Определения и основные принципы»
ISO/IEC 27001	ГОСТ Р ИСО/МЭК 27001-2006	«Информационные технологии - Методы обеспечения безопасности - Системы менеджмента информационной безопасности - Требования. Вторая редакция 01.10.2013»
ISO/IEC 27002	ГОСТ Р ИСО/МЭК 27002-2012	«Информационные технологии - Методы обеспечения безопасности - Практические правила управления информационной безопасностью. Вторая редакция 01.10.2013»
ISO/IEC 27003	ГОСТ Р ИСО/МЭК 27003-2012	«Информационные технологии - Методы обеспечения безопасности - Руководство по внедрению системы управления информационной безопасностью»
ISO/IEC 27004	ГОСТ Р ИСО/МЭК 27004-2011	«Информационные технологии - Методы обеспечения безопасности - Системы менеджмента информационной безопасности – Измерение»
ISO/IEC 27005	ГОСТ Р ИСО/МЭК 27005-2010	«Информационные технологии - Методы обеспечения безопасности - Управление рисками информационной безопасности. Вторая редакция, 2011»
ISO/IEC 27006	ГОСТ Р ИСО/МЭК 27006-2008	«Информационные технологии - Методы обеспечения безопасности - Требования к органам аудита и сертификации систем управления информационной безопасностью»
ISO/IEC 27007	ГОСТ Р ИСО/МЭК 27007-2014	«Информационные технологии - Методы обеспечения безопасности - Руководство по аудиту Систем менеджмента информационной безопасности»

Таблица 1.2. Продолжение

ISO/IEC 27008	ГОСТ Р 56045-2014/ISO/IEC TR 27008:2011	«Информационные технологии - Методы обеспечения безопасности - Руководство для аудиторов по механизмам контроля СМИБ»
ISO/IEC 27010		«Информационные технологии - Методы обеспечения безопасности - Управление информационной безопасностью при коммуникациях между секторами»
ISO/IEC 27011	ГОСТ Р ИСО/МЭК 27011-2012	«Информационные технологии - Методы обеспечения безопасности - Руководство по управлению информационной безопасностью для телекоммуникаций»
ISO/IEC 27013	ГОСТ Р ИСО/МЭК 27013-2014	«Информационные технологии - Методы обеспечения безопасности - Руководство по интегрированному внедрению ISO/IEC 20000-1 и ISO/IEC 27001»
ISO/IEC 27014		«Информационные технологии - Методы обеспечения безопасности - Базовая структура управления информационной безопасностью»
ISO/IEC 27015		«Информационные технологии - Методы обеспечения безопасности - Руководство по внедрению систем управления информационной безопасностью в финансовом и страховом секторе»
ISO/IEC 27018		«Информационные технологии - Методы обеспечения безопасности - Практическое руководство по защите персонально идентифицируемой информации (далее – ПИИ) в публичных облаках, используемых для обработки ПИИ. Первая редакция, Август 2014 г.»
ISO/IEC 27031	ГОСТ Р ИСО/МЭК 27031-2012	«Информационные технологии - Методы обеспечения безопасности - Руководство по обеспечению готовности информационных и коммуникационных технологий к их использованию для управления непрерывностью бизнеса»
ISO/IEC 27032		«Информационные технологии - Методы обеспечения безопасности - Руководство по обеспечению кибербезопасности»

Таблица 1.2. Продолжение

ISO/IEC 27033	ГОСТ Р ИСО/МЭК 27033-1-2011 ГОСТ Р ИСО/МЭК 27033-3-2014	«Информационные технологии - Методы обеспечения безопасности - Сетевая безопасность - Основные концепции управления сетевой безопасностью. Информационные технологии - Методы обеспечения безопасности - Сетевая безопасность - Руководство по проектированию и внедрению системы обеспечения сетевой безопасности». «Информационные технологии - Методы обеспечения безопасности - Сетевая безопасность - Базовые сетевые сценарии - угрозы, методы проектирования и механизмы контроля». «Информационные технологии - Методы обеспечения безопасности - Сетевая безопасность - Обеспечение безопасности межсетевых взаимодействий при помощи шлюзов безопасности - угрозы, методы проектирования и механизмы контроля». «Информационные технологии - Методы обеспечения безопасности - Сетевая безопасность - Обеспечение безопасности Виртуальных Частных Сетей - угрозы, методы проектирования и механизмы контроля». «Информационные технологии - Методы обеспечения безопасности - Сетевая безопасность - Конвергенция в IP сетях». «Информационные технологии - Методы обеспечения безопасности - Сетевая безопасность - Руководство по обеспечению безопасности беспроводных сетей - Риски, методы проектирования и механизмы контроля. ISO 27033 заменяет известный международный стандарт сетевой безопасности ISO 18028, состоящий из пяти частей»
ISO/IEC 27034	ГОСТ Р ИСО/МЭК 27034-1-2014	«Информационные технологии - Методы обеспечения безопасности - Обзор и основные концепции в области обеспечения безопасности приложений». «Информационные технологии - Методы обеспечения безопасности - Безопасность приложений - Нормативная база организации (проект)». «Информационные технологии - Методы обеспечения безопасности - Процесс управления безопасностью приложений (проект)». «Информационные технологии - Методы обеспечения безопасности - Оценка безопасности приложений (проект)». «Информационные технологии - Методы обеспечения безопасности - Руководство по обеспечению безопасности конкретных приложений (проект)»

Таблица 1.2. Продолжение

ISO/IEC 27035		«Информационные технологии - Методы обеспечения безопасности - Управление инцидентами безопасности»
ISO/IEC 27036		«Информационные технологии - Методы обеспечения безопасности - Информационная безопасность при взаимодействии с поставщиками - Часть 1: Обзор и концепции». «Информационные технологии - Методы обеспечения безопасности - Руководство по взаимодействию с поставщиками - Часть 2: Требования». «Информационные технологии - Методы обеспечения безопасности - Информационная безопасность при взаимодействии с поставщиками - Часть 3: Руководящие указания по защите цепей поставки информационных и коммуникационных технологий»
ISO/IEC 27037	ГОСТ Р ИСО/МЭК 27037-2014	«Информационные технологии - Методы обеспечения безопасности - Руководство по идентификации, сбору и/или получению и обеспечению сохранности цифровых свидетельств»
ISO/IEC 27038	ГОСТ Р ИСО/МЭК 27038-2016	«Информационные технологии - Методы обеспечения безопасности - Требования и методы электронного цензурирования»
ISO/IEC 27040		«Информационные технологии - Методы обеспечения безопасности - Безопасность хранения данных»
ISO/IEC 27041		«Информационные технологии - Методы обеспечения безопасности - Руководство по предоставлению гарантий пригодности и адекватности метода расследования инцидента»
ISO/IEC 27042		«Информационные технологии - Методы обеспечения безопасности - Руководство по анализу и интерпретации цифровых свидетельств»

Перечисленные стандарты, в том числе, описывает методологию оценки рисков, как составной части при моделировании УБИ. При этом необходимо учитывать, что ущерб от реализации УБИ может быть прямым или непрямым. Прямой ущерб — это непосредственные и прогнозируемые потери предприятия от реализации УБИ, например утеря прав интеллектуальной собственности, судебные издержки и выплата штрафов и компенсаций (например, при утечке персональных данных действия предприятия или физического лица попадают под действия статьи 13.11 КоАП РФ.

В настоящей работе проведен анализ нормативной базы Национального института стандартов и технологий США (National Institute of Standards and Technology, NIST).

Таблица 1.3 – Перечень методологий риск-менеджмента

№ п/п	Наименование методологии	Краткое описание
1.	NIST SP 800-39 «Managing Information Security Risk: Organization, Mission, and Information System View»	Целью специальной публикации 800-39 является предоставление руководства для интегрированной общеорганизационной программы по управлению рисками информационной безопасности для организационных операций (т.е. миссии, функций, имиджа и репутации), активов организации, отдельных лиц, других организаций
2.	NIST SP 800-37 «Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy»	В документе описывается структура управления рисками (RMF) и даются рекомендации по применению RMF к ИС и организациям. RMF обеспечивает дисциплинированный, структурированный и гибкий процесс управления рисками безопасности и конфиденциальности, который включает категоризацию информационной безопасности; контролировать отбор, реализацию и оценку; системные и общие разрешения управления; и постоянный мониторинг
3.	NIST SP 800-30 «Guide for Conducting Risk Assessments»	«Руководство по проведению оценки рисков» сфокусирован на ИТ, ИБ и операционных рисках. Описывает подход к процессам подготовки и проведения оценки рисков, коммуницирования результатов оценки, а также дальнейшей поддержки процесса оценки
4.	NIST SP 800-137 «Information Security Continuous Monitoring (ISCM) for Federal Information systems and Organizations»	Цель руководства - помочь предприятию в разработке стратегии непрерывного мониторинга и реализации программы непрерывного мониторинга, обеспечивающей наглядность активов предприятия, осведомленность об угрозах и уязвимостях, а также представление об эффективности развернутых средств контроля безопасности

Раздел по управлению ИБ содержит серию стандартов, результаты анализа которых представлены в таблице 1.4.

Таблица 1.4 – Перечень стандартов CSRC по управлению ИБ

№ п/п	Наименование стандарта	Краткое описание
1.	SP 800-50 «Building an Information Technology Security Awareness and Training Program»	Специальная публикация NIST 800-50 «Создание программы повышения осведомленности и обучения в области безопасности информационных технологий» содержит руководство по созданию эффективной программы обеспечения безопасности информационных технологий и поддерживает требования, указанные в Федеральном законе об управлении информационной безопасностью (FISMA) 2002 г.
2.	SP 800-84 «Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities»	Документ призван помочь организациям в проектировании, разработке, проведении и оценке мероприятий по тестированию, обучению и упражнениям (TT & E), чтобы помочь персоналу в подготовке к неблагоприятным ситуациям, связанным с информационными технологиями. Мероприятия предназначены для обучения персонала, реализации планов ИТ и тестирования ИТ-систем, чтобы организация могла максимально использовать свои возможности для подготовки к бедствиям, реагирования на них, управления ими и восстановления после них, которые могут повлиять на ее миссию. В руководстве описывается проектирование, разработка, проведение и оценка мероприятий для отдельных организаций, в отличие от крупномасштабных мероприятий, в которых могут участвовать несколько организаций
3.	SP 800-100 «Information Security Handbook: A Guide for Managers»	В документе представлен широкий обзор элементов программы информационной безопасности, чтобы помочь менеджерам понять, как создать и реализовать программу информационной безопасности. Как правило, организация обращается к документу за обеспечение выбора и реализации соответствующих мер безопасности, демонстрацию эффективности удовлетворения своих заявленных требований безопасности
4.	SP 800-60 «Guide for Mapping Types of Information and Information Systems to Security Categories»	Раздел III закона об электронном правительстве «Федеральный закон об управлении информационной безопасностью (FISMA)»

Таблица 1.4. Продолжение

5.	SP 800-115 «Technical Guide to Information Security Testing and Assessment»	Цель этого документа - помочь организациям в планировании и проведении технических тестов и проверок информационной безопасности, анализе результатов и разработке стратегий смягчения последствий. Руководство содержит практические рекомендации по разработке, внедрению и сопровождению процессов и процедур тестирования и проверки технической информации. Данные могут использоваться для нескольких целей, таких как обнаружение уязвимостей в системе или сети и проверка соответствия политике или другим требованиям. Руководство не предназначено для представления всеобъемлющей программы тестирования и экспертизы информационной безопасности, а скорее представляет собой обзор ключевых элементов тестирования и экспертизы технической безопасности с акцентом на конкретные технические методы, преимущества и недостатки каждого из них и рекомендации по их использованию
6.	SP 800-34 Rev. 1 «Contingency Planning Guide for Federal Information Systems»	Документ помогает организациям в понимании цели, процесса и формата разработки планирования на случай непредвиденных обстоятельств ИС на основе практических руководств. Руководящий документ содержит справочную информацию о взаимосвязях между планированием действий в чрезвычайных ситуациях информационной системы и другими типами планов действий в чрезвычайных ситуациях, связанных с безопасностью и управлением в чрезвычайных ситуациях, организационной отказоустойчивостью и жизненным циклом разработки системы. Содержит руководство, помогающее персоналу оценить ИС и операции для определения требований и приоритетов планирования действий в чрезвычайных ситуациях
7.	SP 800-61 Rev. 2 «Computer Security Incident Handling Guide»	Документ помогает организациям создавать возможности реагирования на инциденты компьютерной безопасности и эффективно и результативно обрабатывать инциденты. Содержит рекомендации по обработке инцидентов, в частности, по анализу данных, связанных с инцидентами, и определению соответствующего ответа на каждый инцидент. Указания могут соблюдаться независимо от конкретных аппаратных платформ, операционных систем, протоколов или приложений

Международный подход к управлению информационными технологиями, разработанный Ассоциацией контроля и аудита систем (Information Systems Audit and Control Association - ISACA) и Институтом руководства ИТ (IT Governance Institute - ITGI), Control Objectives for Information and related Technology (COBIT). Актуальная на сегодняшний день редакция документа пятая (COBIT 5).

COBIT 5 является новым поколением рекомендаций ISACA по руководству предприятием и менеджменту ИТ.

С точки зрения ИБ COBIT 5 рассматривает некоторые вопросы. В частности, 2 из 37 процессов COBIT 5 имеют непосредственное отношение к ИБ:

1. APO13 Manage Security.
2. DSS05 Manage Security Services.

Часть процессов COBIT 5 можно использовать при внедрении процессов комплексной системы ИБ (например, СМИБ по ISO 27001). В частности:

- EDM03 Ensure Risk Optimization;
- APO09 Manage Service Agreements;
- APO12 Manage Risk;
- BAI04 Manage Availability and Capacity;
- BAI06 Manage Changes;
- BAI08 Manage Knowledge;
- BAI09 Manage Assets;
- BAI010 Manage Configuration;
- DSS02 Manage Service Requests and Incidents;
- DSS03 Manage Problems;
- DSS04 Manage Continuity.

Иная международная нормативная база в области информационной безопасности. Описание иных международных стандартов приведено в таблице 1.5.

Таблица 1.5 – Иная нормативная международная база в области ИБ

№ п/п	Наименование методологии	Краткое описание
1.	Методология FRAP (Facilitated Risk Analysis Process)	Методология является способом оценки рисков с фокусом только на самых критически важных активах. Качественный анализ проводится с помощью экспертной оценки
2.	Стандарт AS/NZS ISO 31000-2009	Документ ориентирован не только на ИТ-инфраструктурах, но и на бизнес-здоровье компании, предлагает более глобальный подход к управлению рисками

Таблица 1.5. Продолжение

3.	Методология OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)	Методология ориентирована на самостоятельную работу членов бизнес-подразделений. Она используется для масштабной оценки всех информационных систем и бизнес-процессов предприятия
4.	Методология FMEA (Failure Modes and Effect Analysis)	Методология предлагает проведение оценки системы защиты информации ИС с точки зрения её слабых мест для поиска ненадежных элементов
5.	Методология FAIR (Factor Analysis of Information Risk)	Методология представляет собой проприетарный фреймворк для проведения количественного анализа рисков, предлагающий модель построения системы управления рисками на основе экономически эффективного подхода, принятия информированных решений, сравнения мер управления рисками, финансовых показателей и точных риск-моделей
6.	Методология CRAMM (Central Computing and Telecommunications Agency Risk Analysis and Management Method)	Методология предлагает использование автоматизированных средств для управления рисками
7.	Концепция COSO ERM (Enterprise Risk Management)	Концепция описывает пути интеграции риск-менеджмента со стратегией и финансовой эффективностью деятельности предприятия и акцентирует внимание на важность их взаимосвязи. В документе описаны такие компоненты управления рисками, как стратегия и постановка целей, экономическая эффективность деятельности предприятия, анализ и пересмотр рисков, корпоративное управление и культура, а также информация, коммуникация и отчетность

Одним из наиболее важных документов является The General Data Protection Regulation (GDPR), Общий регламент защиты данных № 2016/679, утвержденный Европейским Парламентом и Советом Европейского Союза 27 апреля 2016 г. «Регламент предусматривает защиту физических лиц в отношении обработки персональных данных, являющейся фундаментальным правом (статья 8 (1) Хартии основных прав Европейского Союза (ЕС) и статья 16 (1) Договора о функционировании Европейского Союза (TFEU). В соответствии с документом принципы и правила защиты физических лиц при обращении с их личными данными должны, независимо от их национальности или места жительства, уважать их основные права и свободы, в частности их право на защиту персональных данных. Настоящий Регламент призван внести вклад в достижение свободы, безопасности и справедливости экономического союза, экономического и социального прогресса, укрепление и сближение экономик на внутреннем рынке,

а также на благосостояние людей. Регламент применяется при обработке персональных данных учреждениями, органами, организациями и агентствами Евросоюза».

Персональные данные в соответствии с Регламентом делятся на категории: «генетические данные» (genetic data), «биометрические данные» (biometric data), «данные о здоровье» (data concerning health).

Основными принципами, связанными с обработкой персональных данных, является правомерность обработки. «Обработка персональных данных, раскрывающих расовое или этническое происхождение, политические взгляды, религиозные или философские убеждения, сведения о членстве в профсоюзе, а также обработка генетических данных, биометрических данных для однозначной идентификации физического лица, данных касающихся здоровья, половой жизни или сексуальной ориентации физического лица, запрещена, за исключением предусмотренных Регламентом позиций».

1.5 Анализ требований по защите информации регуляторов Российской Федерации

Проведен анализ требований регуляторов Российской Федерации в области обеспечения безопасности информации в ИС.

Существует два вида нормативно-правовых и методических документов РФ в области защиты информации. Это документы, регулирующие правовые отношения и документы, непосредственно определяющие организационные и технические требования.

Документы, регулирующие правовые отношения в области защиты информации:

- Федеральные законы;
- Указы Президента РФ;
- Постановления Правительства РФ;

- Приказы Регуляторов в области защиты информации (ФСБ России, ФСТЭК России, Роскомнадзор).

К методическим документам ФСТЭК России по технической защите конфиденциальной информации относят [22-30]:

- «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)» (утв. Гостехкомиссией в 2002 г.).
- «Сборник временных методик оценки защищённости конфиденциальной информации от утечки по техническим каналам» (утв. Гостехкомиссией в 2001 г.).
- «Временная методика оценки защищенности основных технических средств и систем, предназначенных для обработки, хранения и передачи по линиям связи конфиденциальной информации».
- «Временная методика оценки защищенности конфиденциальной информации, обрабатываемой основными техническими средствами и системами от утечки за счет наводок на вспомогательные технические средства и системы».
- «Временная методика оценки защищенности помещений от утечки речевой конфиденциальной информации по акустическому и виброакустическому каналам».
- «Временная методика оценки защищенности помещений от утечки речевой конфиденциальной информации по каналам электроакустических преобразований во вспомогательных технических средствах и системах».

По результатам проведенного анализа можно сделать вывод о том, что для каждого типа ИС существую подмножества подсистем защиты информации (мер по защите информации), которые можно объединить в следующие:

- идентификацию и аутентификацию (далее – ИАФ);
- управление доступом (далее – УПД);

- ограничение программной среды (далее – ОПС);
- защиту машинных носителей информации (далее – ЗНИ);
- аудит безопасности (далее – АУД);
- антивирусную защиту (далее – АВЗ);
- предотвращение вторжений (компьютерных атак) (далее – СОВ);
- обеспечение целостности (далее – ОЦЛ);
- обеспечение доступности (далее – ОДТ);
- защиту технических средств и систем (далее – ЗТС);
- защиту информационной (автоматизированной) системы и ее компонентов (далее – ЗИС);
- реагирование на компьютерные инциденты (далее – ИНЦ);
- управление конфигурацией (далее – УКФ);
- управление обновлениями программного обеспечения (далее – ОПО);
- планирование мероприятий по обеспечению безопасности (далее – ПЛН);
- обеспечение действий в нештатных ситуациях (далее – ДНС);
- информирование и обучение персонала (далее – ИПО).

«Оценка эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности информации проводится оператором самостоятельно или с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Указанная оценка проводится не реже одного раза в три года».

В соответствии с законодательством РФ [7-28] в области обеспечения безопасности информации в ИС определим типы информационных систем:

- автоматизированные системы;
- автоматизированные системы, обрабатывающие сведения, составляющие государственную тайну;
- информационные системы общего пользования;

- информационные системы персональных данных;
- государственные информационные системы;
- автоматизированные системы управления технологическими процессами;
- критические информационные инфраструктуры.

Типы ИС и соответствующие им международные стандарты и НПА Регуляторов РФ по ИБ представлены на рисунке 1.9.

Типы информационных систем	Требования по ИБ	НМД Регуляторов РФ	Международные стандарты ИБ
Автоматизированные системы	РД АС от НСД	СТР-К	NIST (CSRC, FIPS, FRAP, OCTAVE, FMEA, FAIR, CRAMM), COBIT, ISO, DHS
Автоматизированные системы, обрабатывающие сведения, составляющие государственную тайну	РД АС от НСД, СТР	СТР	
Информационные системы общего пользования	Приказ ФСТЭК России № 489	СТР-К	NIST, COBIT, ISO, DHS
Информационные системы персональных данных	Приказ ФСТЭК России № 21 Приказ ФСБ России № 378	Базовая модель ФСТЭК Методика ФСТЭК МР ФСБ Приказы РКН Проект методики УБИ ФСТЭК 2020	NIST, COBIT, ISO, GDPR
Государственные информационные системы	Приказ ФСТЭК России № 17	Проект методки УБИ ФСТЭК 2020	NIST, COBIT, ISO
Критические информационные инфраструктуры	Приказ ФСТЭК России № 239	Базовая модель КСИИ ФСТЭК Методика УБИ КСИИ ФСТЭК Проект методики УБИ ФСТЭК 2020	NIST (CSF), COBIT, ISO

Рисунок 1.9 – Типы ИС и соответствующие им международные стандарты и НПА Регуляторов РФ по ИБ

В соответствии с НПА по ИБ определим свойства безопасности информации [61]:

- конфиденциальность;
- целостность;
- доступность;
- подлинность;

- неотказуемость;
- подотчетность;
- аутентичность;
- достоверность.

На основании проведенного анализа можно сделать вывод о том, что требования по ИБ НПА регуляторов в зависимости от типов ИС и их классов, уровней защищенности и категорий значимости можно объединить в единые подмножества. Также следует отметить, что одним из основных требований является определение актуальных УБИ и проведение оценки эффективности СЗИ в соответствии с уставленным законодательством порядком, что, в свою очередь, подтверждает актуальность совершенствования существующих методов и методик определения актуальных УБИ и оценки эффективности СЗИ.

1.6 Анализ методов и методик оценки эффективности систем защиты информации

В соответствии с ГОСТ [42] «эффективность системы защиты информации – степень соответствия результатов защиты информации цели защиты информации».

Для проведения оценки эффективности СЗИ необходимо определить показатели оценки, метод и методику оценки.

В качестве показателей оценки могут быть критерии из серии ГОСТ Р ИСО/МЭК 15408 [37-39], требования руководящих документов регуляторов [16-21], проектные решения на создание СЗИ ИС и иные.

Основными методами оценки эффективности системы защиты информации информационных систем [64, 67] являются:

- Статистический;
- Вероятностный;
- Частотный;
- Экспертный;
- Информационно-энтропийный;

– Многокритериальный (нейросетевой);
– Метод минимизации рисков;
– Матричный (формальный);
– Многоуровневый;
– Комбинаторный (оптимизационный).

При статистическом методе проводится обработка потенциальных угроз и их последствий. Показателем оценки эффективности является: угроза *i*-го типа возникает в среднем за период времени T_i.

При вероятностном методе определяется вероятность отказа системы от обработки информации в результате успешной реализации угроз. Суммарные средние потери рассчитываются по формуле:

$$R = \Sigma_{i=1}^{2^m} \Sigma_{j=1}^{2^m} P(\frac{\vec{\gamma}}{\vec{s}}) P(\vec{s}) \Pi(\vec{\gamma}, \vec{s}) + m,$$

где $P(\frac{\vec{\gamma}}{\vec{s}})$ - вероятность устранения, $P(\vec{s})$ - априорная вероятность состояния объекта контроля, $\Pi(\vec{\gamma}, \vec{s})$ - потери принятия решения s при состоянии объекта s, m – количество обнаруженных УБИ.

При частотном методе на основании анализа статического материала задается значение *S*, величина *V* выбирается равной от 1 до *max* возможной суммы ущерба, рассчитывается значение показателя R_i как функции параметров *V* и *S*. Показатель оценки эффективности: ожидаемый ущерб от i-й УБИ:

$$R_i = F(S, V),$$

где *S*– показатель частоты возникновения УБИ, *V* – условный показатель ущерба.

При экспертном методе определяется количество n и перечень параметров *i*, характеризующих СЗИ ТРИС. Задаются значения субъективных коэффициентов важности W_i каждой из характеристик G_i, назначенные экспертным путем. Рассчитывается значение параметра *SR*.

Показатель оценки эффективности: степень обеспечения безопасности *SR* системы *S* рассчитывается следующим образом:

$$SR_{(s,r)} = \frac{1}{n_{i-1}^{n}} W_i G_i$$

При информационно-энтропийном методе проводится аналитическое вычисление информационной энтропии системы, используя понятие свертки функции. При линейной зависимости эффективность интеграции подсистем в информационной плане считают удовлетворительной. В противном случае – неэффективной.

Показателем оценки эффективности подхода является величина информационной энтропии Шеннона:

$$\psi(t) = (\int_0^{\tau} S_n(t-\tau)...(\int_0^{\tau} S_3(\int_0^{\tau} S_1(\tau) S_2(t-\tau)dt)dt...)dt,$$

где $S_1 \dots S_n$ - значения информационных энтропий различный подсистем.

Нейросетевой метод (многокритериальная оценка). Принадлежность определенного уровня безопасности определяется на промежутке [0,1], показатели надежности являются функцией принадлежности:

$$\mu^{A}(x_i),$$

где x_i – элемент множества *X* – требований по безопасности информации, *A* – множество значений, определяющих выполнение требований по безопасности информации. Оценка эффективности СЗИ ТРИС производится по четко определенным показателям.

Нечеткие показатели СЗИ ТРИС в виде лингвистических переменных, таких как «высокая степень защищенности», «средняя степень защищенности» и «низкая степень защищенности»:

$$A = \sum_{i=1}^{n} \frac{\mu^{A}(x_i)}{x_i}$$

Метод минимизации рисков. Реализуется следующими шагами:

1. Фиксация рисков.
2. Индекс риска.
3. Проводится классификация рисков.

4. Определяются способы обработки рисков.

5. Рассчитываются показатели, характеризующие риски.

6. Рассчитываются показатели экономического эффекта от управления рисками.

Показателем оценки эффективности является показатель экономического эффекта от управления рисками. Рассчитывается по формуле, учитывающей:

M_0 - суммарные вероятные потери без обработки идентифицированных рисков, суммарные вероятные потери после обработки рисков M, суммарные фактические потери от проявления рисков $I_{\text{ф}}$, суммарные фактические расходы на обработку идентифицированных рисков ($H = H_{\text{ф}}$), суммарные фактические потери от проявления рисков $I_{\text{фн}}$, суммарные фактические расходы на обработку рисков $H_{\text{фн}}$.

$$E = (\sum_{i=1}^{N} M_{oi} - \sum_{i=1}^{N} M_i) - ((\sum_{i=1}^{N} I_{фi} + \sum_{i=1}^{N} H_{фi}) + (\sum_{j=1}^{K} I_{фнj} + \sum_{j=1}^{K} H_{фнj}))$$

Матричный метод (формальные модели защиты). Метод реализуется следующими шагами:

1. Определяются параметры.

2. Составляется трехмерная матрица отношений.

3. Преобразование матрицы отношений в двумерную таблицу.

4. Определяются качественные и количественные значения показателей.

Показателем оценки эффективности является состояние СЗИ ТРИС, описанное параметрами, например:

(*S, O, M*) – множества *S*-субъектов, *O* – объектов, *M* – прав доступа или (*O, H, M*), где *O* – основы и составные части системы (нормативно-правовая, организационная, техническая и т.д.), *H* – направления защиты, *M* – этапы создания СЗИ ТРИС.

Многоуровневый метод использует модель конечных состояний Белла Ла-Падулы и решетчатая модель Д. Деннинга. Состояние СЗИ ТРИС описывается

совокупностью уровней конфиденциальности и набора категорий конфиденциальности.

Также метод использует алгоритмы нечеткой логики [70, 71].

Комбинаторный (оптимизационный). В данном методе решается задача дискретного программирования вида: максимизировать $\sum_{j=1}^{n}(c_j x_j)$ при условиях:

$$\sum_{j=1}^{n} a_{ij} x_j \le b_i, i = \overline{1,m},$$

$$x_j \in \{0,1\}, j = \overline{1,n}$$

Преимущества и недостатки методов [64, 73] оценки эффективности СЗИ представлены в таблице 1.6.

Таблица 1.6 – Преимущества и недостатки методов оценки эффективности СЗИ

№ п/п	Метод оценки СЗИ ИС	Преимущества	Недостатки
1.	Статистический	Позволяет получать результаты в случаях, когда не известны параметры СЗИ и СФ, позволяет оценивать СЗИ ТРИС любой сложности	Результаты достоверны с определенной вероятностью, большой объем обработки статистических данных
2.	Вероятностный	Анализируется полный спектр УБИ, использование реалистичного подхода, взаимосвязи между элементами СЗИ ТРИС учитываются в явном виде	Сложность вычислений, невозможно обнаружить плавное изменение вероятностных характеристик наблюдений
3.	Частотный	Удобство реализации, графическое представление характеристик СЗИ ТРИС	Необходимость в большой статистической выборке

Таблица 1.6. Продолжение

4.	Экспертный	Использование метода в отсутствии статистических сведений. Быстрота получения результатов.	Человеческий фактор - достоверность результатов зависит от компетенций экспертов. Субъективность метода. Потребность в высококвалифицированных специалистах по ИБ. Недостаточная устойчивость
5.	Информационно-энтропийный	По характеру зависимости Ψ(t) удобно судить об эффективности СЗИ ТРИС. Если вид зависимости отличается от линейной, то можно сделать вывод о неэффективности СЗИ ИБ	Необходимость принятия пороговых значений для оценивания результатов вычислений или составление эталонных образов, что вызывает трудности в связи с ограниченностью и неполнотой результатов эксперимента. Не рассматривается стохастическая природа событий и явлений, которые возникают в процессе обеспечения ИБ
6.	Многокритериальный (нейросетевой)	Позволяет учитывать большое количество критериев оценки СЗИ ТРИС. Позволяет учитывать не только количественные, но и качественные показатели критериев оценки СЗИ ТРИС. Позволяет преодолевать неопределенности	Сложность выбора оптимальной структуры Отсутствие формализованных процедур выбора измеряемых параметров (показатели оценки СЗИ ТРИС). Требует больших вычислительных ресурсов
7.	Метод минимизации рисков	Отсутствие необходимости в точной и полной информации. Простота в части использования инструментальных средств проведения оценки эффективности СЗИ ТРИС	Сложность при проведении оценки рисков. Результат зависит от экспертной оценки рисков. Использование нескольких оптимизационных моделей
8.	Матричный (формальный)	Универсальный метод для проведения оперативной оценки эффективности СЗИ ТРИС. Требует минимальных вычислительных ресурсов	Не позволяет проводить оценку эффективности СЗИ ТРИС в условиях неопределенности, большого числа показателей оценки

Таблица 1.6. Продолжение

9.	Многоуровневый	Повышение объективности и корректности оценки эффективности СЗИ ТРИС, позволяет обрабатывать трудноформализуемые данные качественных характеристик и нечеткой информации	Сложность формирования уровней оценивания СЗИ ТРИС. Сложность проведения вычислений
10	Комбинаторный (оптимизационный)	Наиболее эффективный методом в оценке эффективности СЗИ ТРИС. Гибкость построения	Сложность проведения вычислений

Одновременно с этим существуют ряд проблем, связанных с выбором показателей оценки эффективности СЗИ, а именно:

совокупность показателей оценки эффективности СЗИ находятся в сложных взаимосвязях, неверный учет и определение которых приводят к некачественной оценке эффективности СЗИ;

излишний или недостаточный выбор показателей оценки эффективности СЗИ;

методики расчета количественных оценок эффективности СЗИ имеют свои недостатки, связанные в том числе с определением весов у показателей - в зависимости от модели рисков (модели угроз безопасности информации) у каждого показателя вес может меняться динамически, исходя из текущих в тот или иной момент времени протекающих бизнес-процессов, актуальности типов нарушителей и условий эксплуатации ИС (ИТ-инфраструктуры ИС);

субъективные оценки экспертов, гипотетически приводящие к некачественной оценке эффективности СЗИ;

качественных оценок недостаточно для определения эффективности СЗИ (уровня защищенности).

Проведенный анализ показал, что существующие методы оценки эффективности СЗИ имеют ряд своих недостатков, что обуславливает необходимость повышения качеств существующих методов.

1.7 Формулирование цели и задач диссертационного исследования

1.7.1 Цель диссертационного исследования

Определение перечня актуальных УБИ и оценка эффективности СЗИ являются неотъемлемой частью этапов жизненного цикла ТРИС. Специфика ИТ-инфраструктуры, сложность определения актуальных УБИ и нарушителя в ТРИС, выбор показателей, недостатки известных методов оценки эффективности СЗИ и, как следствие, недостаточная эффективность (уровень защищенности) СЗИ ТРИС приводит к рискам нанесения ущерба активам владельцев ТРИС. В связи с этим целью настоящей работы является повышение качества оценки эффективности СЗИ ТРИС за счет определения необходимых и достаточных показателей.

1.7.2 Постановка задач диссертационного исследования

В общем виде задачи в настоящем диссертационном исследовании может быть сформулированы следующим образом:

- повысить качество определения (моделирования) актуальных УБИ за счет определения необходимых и достаточных показателей и автоматизировать процесс для исключения гипотетических ошибок экспертов;
- повысить качество оценки эффективности СЗИ за счет определения необходимых и достаточных показателей, определения наилучших параметров работы адаптивных нечетких нейронных продукционных систем, алгоритмов нечеткого вывода и применения технологий Data Science при обработке большого объема данных;
- разработать методические рекомендации по оценке эффективности СЗИ ТРИС;
- провести оценку эффективности предложенных метода, методики рекомендаций.

Математически задачи можно формализовать следующим образом:

- выбрать наилучшие для решения поставленных задач математические модели и определить наилучший алгоритм нечеткого вывода;
- определить наилучшие параметры модели, позволяющие минимизировать среднеквадратическую ошибку (RMSE) по сравнению с известными методами и методиками.

Сложность решения перечисленных задач обуславливается недостаточной проработкой на текущий момент времени следующих подзадач:

- определение специфичных для ТРИС аспектов с точки зрения ИТ-инфраструктуры и СЗИ;
- недостатки существующих методик моделирования актуальных УБИ и, как следствие, некорректное определение актуальных УБИ в ТРИС;
- недостатки существующих методов оценки эффективности СЗИ, что может является результатом недостаточно эффективной СЗИ, приводящей к увеличению рисков нарушения конфиденциальности, целостности, доступности и иных свойств информации.

В настоящее время не в полной мере проработаны решения задач по определению перечня актуальных УБИ и оценки эффективности СЗИ. В частности, существующие решения в международной и российской практике имеют ряд своих недостатков, связанных с ошибками экспертов, высокой вычислительной сложностью и привлечения высококвалифицированных специалистов в области ИБ. Одновременно с этим, существующие методы и методики в качестве показателей используют недостаточно полные и рациональные, необходимые для наиболее эффективного и точного определения актуальных УБИ и оценки эффективности СЗИ. Перечисленные проблемы позволяют сделать вывод о том, что необходимо прорабатывать возможные решения обозначенные задачи с помощью научного подхода с применением математического аппарата, использования комплексного и системного подходов, комбинированных методов и перспективных в настоящее время технологий.

В этой связи, повышение качества оценки эффективности СЗИ, максимально исключающих недостатки существующих, является актуальной задачей.

Выводы

В соответствии с целью и задачами, определенными в настоящем диссертационном исследовании, в главе 1 проанализированы основные бизнес-процессы ИС/ТРИС, виды и категории обрабатываемой в ТРИС информации, группы пользователей и методы доступа в ТРИС, определены ключевые аспекты ИТ-инфраструктуры ТРИС и их СЗИ, произведен анализ моделей и методов моделирования ИС, моделей атак и УБИ, методов и методик оценки эффективности систем защиты информации ТРИС, а также анализ международных документов и документов регуляторов РФ в части обеспечения требований по ИБ.

Ключевыми аспектами ИТ-инфраструктуры ТРИС являются: географическая распределенность ТРИС, незащищенные сети передачи данных (каналы связи), клиент-серверные приложения, обработка информации в центрах обработки данных, облачные инфраструктуры (IaaS, SaaS, PaaS). Перечисленные аспекты необходимо учитывать при определении перечня актуальных УБИ и оценке эффективности СЗИ ТРИС.

Существующие методики определения актуальных УБИ (моделирования УБИ) имеют свои недостатки. Основными их них являются:

1. При моделировании УБИ не всегда существует возможность выявления новых качественных характеристик.
2. Любая модель УБИ минимизирует объяснения возможных явлений.
3. Как правило, необходимых данных для настройки моделей не хватает.
4. Недостатки экспертных методов (экспертных оценок).
5. Модели УБИ разрабатываются на текущее состояние ИС, в этой связи возникают сложности в постоянной актуализации таких моделей УБИ.
6. Не учитывают все необходимые показатели при определении перечня актуальных УБИ.

7. Не рациональное использование множества известных баз данных УБИ, уязвимостей, тактик и техник атак (MITRE ATT&CK, CVE, CWE, OSVDB, NVD, Secunia и т.д.).
8. Как следствие, некачественная оценка эффективности СЗИ (уровня защищенности ИС).

Анализ методов и методик оценки эффективности СЗИ показал, что в настоящее время существуют недостатки оценки эффективности СЗИ, связанные с выбором показателей, сложная вычислительная нагрузка, недостатки экспертных оценок и необходимость привлечения высококвалифицированных специалистов в области ИБ. К другим недостаткам известных методов и методик оценки эффективности СЗИ можно отнести следующие:

1. Совокупность показателей оценки эффективности СЗИ находятся в сложных взаимосвязях.
2. Излишний или недостаточный выбор показателей оценки эффективности СЗИ.
3. Недостатки известных методик расчета количественных оценок эффективности СЗИ.
4. Субъективные оценки экспертов, гипотетически приводящие к некачественной оценке эффективности СЗИ.
5. Качественных оценок недостаточно для определения эффективности СЗИ (уровня защищенности).

Анализ требований показал, что в мире и в РФ имеется большое количество документов в области обеспечения ИБ, что не позволяет полноценно и качественно принять меры по ИБ в ТРИС. для каждого класса ТРИС существуют определенные требования по ИБ регуляторов. Так как ТРИС могут быть классифицированы как ИСПДн, КИИ, ГИС одновременно, то вызывает затруднение при проектировании СЗИ таких систем, ввиду предъявления требований ИБ для каждого типа и класса ТРИС. В этом случае возникает потребность в полноценном выборе мер по ИБ, учитывающих актуальные УБИ и нарушителя, архитектуру ТРИС, экономическую

составляющую при создании СЗИ ТРИС, а также учитывающие требования по защите информации регуляторов в области обеспечения безопасности информации.

В главе 1 сформулирована цель диссертационного исследования. Определены задачи, которые необходимо решить для достижения поставленной цели. Решение задач позволит повысить эффективность научных и практических основ оценки эффективности СЗИ.

Глава 2. Методика определения актуальных угроз безопасности информации

Для эффективного определения перечня актуальных УБИ необходимо последовательно выполнить следующие шаги:

1. Определить цели и задачи, выполняемые ИС (ТРИС).
2. Провести анализ бизнес-процессов, выполняемых ИС (ТРИС).
3. Провести анализ защищаемой информации, обрабатываемой в ИС (ТРИС).
4. Определить риски (киберриски) и негативные последствия при наступлении этих рисков (успешной реализации нарушителями УБИ).
5. Определить объекты воздействия УБИ в ИС (ТРИС) – элементы ТРИС (информационные активы).
6. Определить источники УБИ (актуальных нарушителей), оценить уровень их возможностей и мотивацию.
7. Определить перечень возможных УБИ в ИС (ТРИС) с учетом ИТ-инфраструктуры и технологии обработки информации.
8. Определить возможные способы и сценарии реализации УБИ в ИС (ТРИС) – тактики, техники и процедуры.
9. Определить итоговый перечень актуальных УБИ, для нейтрализации которых необходимо разработать СЗИ.

В главе 1 были перечислены основные сложности, проблемы и недостатки известных методик (методологий) определения актуальных УБИ, с учетом и на основании которых в настоящем диссертационном исследовании предлагаются решить задачу определения перечня актуальных УБИ.

2.1 Типы угроз безопасности информации

При формировании перечня УБИ следует рассматривать угрозы следующих типов:

- угрозы, не являющиеся атакой;
- угрозы, которые являются атаками.

В соответствии с п. 6.5 документа «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (Выписка), утвержденной приказом ФСТЭК России 15.02.2008, при обработке Информации в ТРИС возможна реализация следующих УБИ:

- угрозы утечки информации по техническим каналам;
- угрозы НСД к информации, обрабатываемым в ТРИС;
- угрозы специальных воздействий на ТРИС.

Угрозы утечки информации по техническим каналам включают в себя:

- угрозы утечки информации по акустическому каналу;
- угрозы утечки информации по визуально-оптическому каналу;
- угрозы утечки информации по каналу побочных электромагнитных излучений и наводок (ПЭМИН).

Возникновение угроз утечки акустической (речевой) информации [84], содержащейся непосредственно в произносимой речи пользователя ТРИС, невозможно в связи с отсутствием функций голосового ввода информации в ТРИС или функций воспроизведения информации акустическими средствами ТРИС.

Реализация угрозы утечки информации по визуально-оптическому каналу возможна за счет просмотра информации с помощью оптических (оптикоэлектронных) средств и без их использования с экранов дисплеев и других средств отображения СВТ, информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации, входящих в состав ТРИС.

Возникновение угрозы утечки информации по каналам ПЭМИН возможно за счет перехвата побочных (не связанных с прямым функциональным значением элементов ТРИС) информативных электромагнитных полей и электрических сигналов, возникающих при обработке ТС ТРИС [22].

Генерация информации, в том числе содержащей ПДн, и циркулирующей в ТС ТРИС в виде электрических информативных сигналов, обработка и передача указанных сигналов в электрических цепях ТС ТРИС сопровождается побочными электромагнитными излучениями, которые могут распространяться за пределы служебных помещений в зависимости от мощности излучений и с учетом размеров ТРИС.

Регистрация ПЭМИН может осуществляться с целью перехвата информации, циркулирующих в ТС обработки информации в составе ТРИС. Для регистрации ПЭМИН используется аппаратура в составе радиоприемных устройств и оконечных устройств восстановления информации.

Перехват ПЭМИН возможен с использованием электронных устройств перехвата информации, подключенных к каналам связи или ТС обработки информации в составе ТРИС.

Регистрация ПЭМИН может вестись с использованием аппаратуры следующих видов:

- стационарной аппаратуры, размещаемой в близлежащих строениях с неконтролируемым пребыванием посторонних лиц;
- портативной возимой аппаратуры, размещаемой в транспортных средствах, осуществляющих движение вблизи служебных помещений или при их парковке рядом с этими помещениями;
- портативной носимой аппаратуры – физическими лицами в непосредственной близости от ТРИС;
- автономной автоматической аппаратуры, скрытно устанавливаемой физическими лицами в непосредственной близости от ТРИС.

Каналы утечки информации, обусловленные наводками, образуются за счет соединительных линий ТС ТРИС, посторонних проводников.

Наводки электромагнитных излучений ТС ТРИС возникают при излучении элементами ТС ТРИС информативных сигналов при наличии емкостной, индуктивной или гальванической связей соединительных линий ТС ТРИС. В результате на случайных антеннах наводится информативный сигнал.

Прохождение информативных сигналов в цепи электропитания возможно при наличии емкостной, индуктивной или гальванической связей источника информативных сигналов в составе ТС ТРИС и цепей питания. Прохождение информативных сигналов в цепи заземления обусловлено наличием емкостной, индуктивной или гальванической связей источника информативных сигналов в составе аппаратуры ТС приема информации и цепей заземления.

Различные ТС ТРИС, их соединительные линии, а также линии электропитания, проводники и цепи заземления выполняют роль случайных сосредоточенных или распределенных антенн, при подключении к которым средств разведки возможен перехват наведённых информативных сигналов. Сосредоточенная случайная антенна представляет собой компактное ТС, подключённое к линии, выходящей за пределы КЗ ТРИС. К распределённым случайным антеннам относятся случайные антенны с распределёнными параметрами: кабели, провода, металлические трубы и другие токопроводящие коммуникации, выходящие за пределы КЗ ТРИС. Уровень наводимых в них сигналов в значительной степени зависит не только от мощности излучаемых сигналов, но и расстояния до них от ТС обработки информации.

Для съема информации с проводных линий могут быть использованы:

- средства съема сигналов, содержащих информацию, с цепей ТС ТРИС, линий связи и передачи данных, выходящих за пределы служебных помещений;
- средства съема наведенных информативных сигналов с цепей электропитания;

- средства съема наведенных информативных сигналов с шин заземления;
- средства съема наведенных информативных сигналов с проводящих инженерных коммуникаций.

Угрозы утечки могут быть реализованы как внутренними, так и внешними нарушителями, в том числе путем размещения закладочных устройств как в пределах КЗ, так и вне ее.

Угрозы НСД связаны с действиями нарушителей, имеющих доступ к ТРИС, включая пользователей ТРИС, реализующих угрозы непосредственно в ТРИС, а также нарушителей, не имеющих доступа к ТРИС, реализующих угрозы из внешних сетей связи общего пользования и (или) международного информационного обмена [106, 107].

Реализация угроз НСД к информации может приводить к следующим видам нарушения ее безопасности:

- нарушению конфиденциальности;
- нарушению целостности;
- нарушению доступности;
- нарушению подлинности;
- нарушению неотказуемости;
- нарушению подотчетности, аутентичности и достоверности.

2.2 Определение источников угроз безопасности информации

Определение источников УБИ (актуальных нарушителей) является сложной задачей. Связано это, прежде всего, с необходимостью в определении мотивации и оценки возможностей потенциальных нарушителей, а также в проведении анализа известных тактик, техник и процедур (способов и сценариев реализации УБИ). В этой связи для определения актуального нарушителя существует необходимость в привлечении экспертов, что для многих владельцев ИС (ТРИС) является затруднительным. К другой проблеме относится и отсутствие в настоящее время

единой методологии определения актуального нарушителя и УБИ, а также наличие различных баз данных УБИ, уязвимостей, тактик, техник и процедур (способов и сценариев реализации) УБИ.

В соответствии с МД ФСТЭК России [25] необходимо определить антропогенные источники УБИ в ИС (ТРИС), к которым относятся нарушители, осуществляющие реализацию УБИ путем несанкционированного доступа (далее – НСД) и (или) воздействия на информационные ресурсы и (или) компоненты систем и сетей (информационные активы ТРИС) – актуальные нарушители.

Для определения актуальных нарушителей в исследуемой ТРИС определим виды ущерба и возможные негативных последствий (далее – НП) от реализации УБИ для исследуемой ТРИС. Фрагмент результатов приведен в таблице 2.1

Таблица 2.1 – Виды ущербов и возможные НП

Обозначение	**Виды ущерба**	**Возможные типовые НП**
У1	Ущерб физическому лицу	Нанесение ущерба субъекту путем незаконной обработки его ПДн, в том числе нарушения прав на неприкосновенность частной жизни, личную и семейную тайны
У2	Ущерб юридическому лицу	Нарушение требований нормативных и методических документов в области информационной безопасности, влекущие за собой наложение санкций, например, в виде штрафов, предусмотренных кодексом об административных правонарушениях (далее – КоАП)
		Нарушение деловой репутации юридического лица
		Виды ущербов, связанных с эксплуатацией критических информационных инфраструктур, автоматизированных систем управления технологическими процессами
		Необходимость изменения (перестроения) бизнес-процессов, реализующих ТРИС Нанесение ущерба юридическому лицу путем утечки и незаконной обработки защищаемой информации в виде финансового ущерба

Для последующего формирования набора данных при определении перечня актуальных УБИ введем классификаторы ОВ, ДИ, СР следующим образом:

«Наименование ТРИС».«ОВ».«Аббревиатура, присвоенный ОВ»

«Наименование ТРИС».«СР».«Аббревиатура, присвоенный СР»

«Наименование ТРИС».«ДИ».«Аббревиатура, присвоенный ДИ»

Например,

ТРИС.ОВ.АСО – Активное сетевое оборудование, включающее в себя коммутаторы, маршрутизаторы, межсетевые экраны;

ТРИС.СР.ВПО – Внедрение вредоносного ПО (установка ПО, имеющего скрытый функционал для возможности реализации УБИ);

ТРИС.ДИ.КС – Командная строка – интерфейсы доступа SSH, Telnet, и т.д., используемые для взаимодействия с ОВ.

В соответствии с п. 4.3 МД ФСТЭК России [25] (далее – Методика ФСТЭК России) определим возможные объекты воздействия (далее – ОВ) в исследуемой ТРИС и доступные для них интерфейсы (далее – ДИ). Фрагмент результатов приведен в таблице 2.2.

Таблица 2.2 – Возможные ОВ для ТРИС и ДИ

№ п.п	ОВ	Обозначение ОВ	ДИ
1. Сетевой уровень			
1.1	Активное сетевое оборудование, включающее в себя коммутаторы, маршрутизаторы, межсетевые экраны	ТРИС.ОВ.АСО	Веб-интерфейс («Тонкий» клиент) – веб браузер «Яндекс», Internet Explorer для взаимодействия с ОВ (далее – ДИ.ВИ); Командная строка интерфейсы доступа SSH, Telnet, и т.д., используемые для взаимодействия с ОВ (далее – ДИ.КС); Физический доступ (далее – ДИ.ФД)
1.2	Линии связи (каналы передачи данных между компонентами ТРИС)	ТРИС.ОВ.КС	ДИ.ФД
2. Серверный уровень			
2.1	Кластер серверов;	ТРИС.ОВ 1.1	ДИ.ВИ; ДИ.КС; ДИ.ФД
3. Прикладной уровень			
3.1	ППО	ТРИС.ОВ 1.1	Программное обеспечение («Толстый» клиент) – устанавливаемый программный клиент для взаимодействия с ОВ (далее – ДИ.ПО)

№ п.п	ОВ	Обозначение ОВ	ДИ
4. Пользовательский уровень			
4.1	АРМ пользователя ТРИС	ТРИС.ОВ.АРМ	ДИ.ФД
4.2	Веб браузер «Яндекс», Internet Explorer	ТРИС.ОВ.ППО	ДИ.ФД

Определим ОВ (по уровням из таблицы 2.2.) исследуемой ТРИС, которые непосредственно участвуют в обработке защищаемой информации, и виды воздействия на ОВ исследуемой ТРИС, которые могут привести к НП. Результаты приведены в таблице 2.3.

Таблица 2.3 – Возможные ОВ и виды воздействия

НП	ОВ	Виды воздействия
У1 1. Нанесение ущерба субъекту путем незаконной обработки его ПДн, в том числе нарушения прав на неприкосновенность частной жизни, личную и семейную тайну	Серверный уровень Пользовательский уровень	Нарушение конфиденциальности, целостности, доступности, подлинности, неотказуемости, подотчетности, аутентичности и достоверности защищаемой информации
У2 1. Нарушение требований нормативных и методических документов в области информационной безопасности, влекущие за собой наложение санкций, например, в виде штрафов, предусмотренных КоАП 2. Нарушение деловой репутации юридическому лицу 4. Необходимость изменения (перестроения) бизнес-процессов, реализующих ТРИС 5. Виды ущербов, связанных с эксплуатацией критических информационных инфраструктур, автоматизированных систем управления технологическими процессами 6. Нанесение ущерба юридическому лицу путем утечки и незаконной обработки коммерческой тайны в виде финансового ущерба	Сетевой уровень Серверный уровень, прикладной уровень Пользовательский уровень	Нарушение конфиденциальности, целостности, доступности, подлинности, неотказуемости, подотчетности, аутентичности и достоверности защищаемой информации

Основными видами нарушителей, подлежащих оценке, являются:

- специальные службы иностранных государств;
- террористические, экстремистские группировки;
- преступные группы (криминальные структуры);
- отдельные физические лица (хакеры);
- конкурирующие организации;
- разработчики программных, программно-аппаратных средств;
- лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем;
- поставщики услуг связи, вычислительных услуг;
- лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ;
- лица, обеспечивающие функционирование систем и сетей или обеспечивающих систем оператора (администрация, охрана, уборщики и др.);
- авторизованные пользователи систем и сетей;
- системные администраторы и администраторы безопасности;
- бывшие (уволенные) работники (пользователи).

Нарушители признаются актуальными для систем и сетей, когда возможные цели реализации ими угроз безопасности информации могут привести к определенным для систем и сетей негативным последствиям и соответствующим рискам (видам ущерба).

В зависимости от уровня возможностей нарушители подразделяются на нарушителей, обладающих:

- базовыми возможностями по реализации угроз безопасности информации (Н1);
- базовыми повышенными возможностями по реализации угроз безопасности информации (Н2);
- средними возможностями по реализации угроз безопасности информации (Н3);

– высокими возможностями по реализации угроз безопасности информации (Н4).

В соответствии с Методикой ФСТЭК России определяем виды, категории и возможные цели потенциальных нарушителей в исследуемой ТРИС. Результаты приведены в таблице 2.4.

Таблица 2.4 – Виды, категории и возможные цели потенциальных нарушителей в исследуемой ТРИС

№ п/п	Вид нарушителя	Категория нарушителя	Возможные цели реализации угроз безопасности
1.	Преступные группы (криминальные структуры)	Внешний	Получение финансовой или иной материальной выгоды. Желание самореализации (подтверждение статуса)
2.	Отдельные физические лица (хакеры)	Внешний	Получение финансовой или иной материальной выгоды. Любопытство или желание самореализации (подтверждение статуса)
3.	Разработчики программных, программно-аппаратных средств	Внутренний	Непреднамеренные, неосторожные или неквалифицированные действия Финансовая выгода (например, осуществление и продление технической поддержки разработанного средства)
4.	Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	Внешний	Непреднамеренные, неосторожные или неквалифицированные действия
5.	Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	Внутренний	Непреднамеренные, неосторожные или неквалифицированные действия

Таблица 2.4. Продолжение

6.	Лица, обеспечивающие функционирование ТРИС (охрана, уборщики и т.д.)	Внутренний	Непреднамеренные, неосторожные или неквалифицированные действия. Материальная выгода (кража оборудования)
7.	Авторизованные пользователи ТРИС	Внутренний	Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия. Непреднамеренные, неосторожные или неквалифицированные действия
8.	Системные администраторы и администраторы безопасности	Внутренний	Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия. Непреднамеренные, неосторожные или неквалифицированные действия
9.	Бывшие работники (пользователи)	Внешний	Любопытство или желание самореализации (подтверждение статуса) Месть за ранее совершенные действия

На основании определенного актуального нарушителя в соответствии с МД ФСБ России «Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности» (утвержденным руководством 8 Цента ФСБ России 31 марта 2015 г. № 149/7/2/6-432 (далее – Методика ФСБ России)) [23] определяются классы СКЗИ, необходимые для защиты информации [32]. Приведем сопоставление видов нарушителей в соответствии с Методикой ФСТЭК России на соответствие видам нарушителей по Методике ФСБ России. Результаты проведенного сопоставления представлены в таблице 2.5.

Таблица 2.5 – Уровни возможностей нарушителей по реализации УБИ

Тип нарушителя (Методика ФСТЭК России)	**Уровень возможностей нарушителей**	**Возможности нарушителей по реализации угроз безопасности информации**	**Тип нарушителя (Методика ФСБ России)**
Н1	Нарушитель, обладающий базовыми возможностями	Имеет возможность при реализации угроз безопасности информации использовать только известные уязвимости, скрипты и инструменты. Имеет возможность использовать средства реализации угроз (инструменты), свободно распространяемые в сети «Интернет» и разработанные другими лицами, имеет минимальные знания механизмов их функционирования, доставки и выполнения вредоносного программного обеспечения, эксплойтов. Обладает базовыми компьютерными знаниями и навыками на уровне пользователя. Имеет возможность реализации угроз за счет физических воздействий на технические средства обработки и хранения информации, линий связи и обеспечивающие системы систем и сетей при наличии физического доступа к ним. Таким образом, нарушители с базовыми возможностями имеют возможность реализовывать только известные угрозы, направленные на известные (документированные) уязвимости, с использованием общедоступных инструментов	Н1, Н2

Таблица 2.5. Продолжение

Н2	Нарушитель, обладающий базовыми повышенными возможностями	Обладает всеми возможностями нарушителей с базовыми возможностями. Имеет возможность использовать средства реализации угроз (инструменты), свободно распространяемые в сети «Интернет» и разработанные другими лицами, однако хорошо владеет этими средствами и инструментами, понимает, как они работают и может вносить изменения в их функционирование для повышения эффективности реализации угроз. Оснащен и владеет фреймворками и наборами средств, инструментов для реализации угроз безопасности информации и использования уязвимостей. Имеет навыки самостоятельного планирования и реализации сценариев угроз безопасности информации. Обладает практическими знаниями операционных систем, а также защитных механизмов, применяемых в программном обеспечении, программно-аппаратных средствах. Таким образом, нарушители с базовыми повышенными возможностями имеют возможность реализовывать угрозы, в том числе направленные на неизвестные уязвимости, с использованием специально созданных для этого инструментов, свободно распространяемых в сети «Интернет». Не имеют возможностей реализации угроз на физически изолированные сегменты ТРИС	Н3

Таблица 2.5. Продолжение

Н3	Нарушитель, обладающий средними возможностями	Обладает всеми возможностями нарушителей с базовыми повышенными возможностями. Имеет возможность приобретать информацию об уязвимостях, размещаемую на специализированных платных ресурсах (биржах уязвимостей). Имеет возможность приобретать дорогостоящие средства и инструменты для реализации угроз, размещаемые на специализированных платных ресурсах (биржах уязвимостей). Имеет возможность самостоятельно разрабатывать средства (инструменты), необходимые для реализации угроз (атак), реализовывать угрозы с использованием данных средств. Имеет возможность получения доступа к встраиваемому программному обеспечению аппаратных платформ, системному и прикладному программному обеспечению, телекоммуникационному оборудованию и другим программно-аппаратным средствам для проведения их анализа. Обладает знаниями и практическими навыками проведения анализа программного кода для получения информации об уязвимостях. Обладает высокими знаниями и практическими навыками о функционировании сетей и систем, операционных систем, а также имеет глубокое понимание защитных механизмов, применяемых в программном обеспечении, программно-аппаратных средствах. Имеет возможность реализовывать угрозы безопасности информации в составе группы лиц. Таким образом, нарушители со средними возможностями имеют возможность реализовывать угрозы, в том числе на выявленные ими неизвестные уязвимости, с использованием самостоятельно разработанных для этого инструментов. Не имеют возможностей реализации угроз на физически изолированные сегменты ТРИС	Н4, Н5

Нарушитель, обладающий высокими возможности категории Н4 (Н6 в соответствии с Методикой ФСБ России) в настоящей работе не рассматривается из-за отсутствия актуальности для исследуемой ТРИС.

Далее экспертным путем проведем оценку возможных целей нарушителей и НП для владельца исследуемой ТРИС. Результаты оценки представлены в таблице 2.6.

Таблица 2.6 – Оценка возможных целей нарушителей и НП для владельца исследуемой ТРИС

Вид нарушителя	**Возможные цели нарушителя**		**НП**
	Физическое лицо	**Юридическое лицо**	
Преступные группы (криминальные структуры)	+ (получение финансовой выгоды за счет хищения и продажи ПДн)	+ (получение финансовой выгоды за счет использования вычислительных мощностей серверов ТРИС не по целевому назначению)	У1.1 У2.3 У2.5 У2.6
Отдельные физические лица (хакеры)	+ (желание самореализоваться)	+ (получение финансовой выгоды за счет кражи коммерческой тайны, ПДн)	У1.1 У2.5 У2.6
Разработчики программных, программно-аппаратных средств	-	-	-
Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	-	-	-
Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	-	-	-

Таблица 2.6. Продолжение

Лица, обеспечивающие функционирование ТРИС (охрана, уборщики и т.д.)	-	-	-
Авторизованные пользователи ТРИС	+ (непреднамеренные, неосторожные или неквалифицированные действия)	+ (желание самореализоваться)	У1.1 У2.2 У2.3 У2.4 У2.5 У2.6
Системные администраторы и администраторы безопасности	-	-	-
Бывшие работники (пользователи)	+ (желание самореализоваться)	+ (месть за ранее совершенные действия)	У1.1 У2.2 У2.3 У2.4 У2.5 У2.6

Разработчики программных, программно-аппаратных средств, лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем, лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ, лица, обеспечивающие функционирование ТРИС (охрана, уборщики и т.д.) условно для исследуемой ТРИС считаются не актуальными из-за наличия факторов, которые снижают уровень мотивации для реализации поставленных ими целей.

Экспертным путем определяются виды, категории и уровни возможностей нарушителей, а также виды ущербов и НП, что и является результатом определения актуального нарушителя для исследуемой ТРИС. Перечень актуальных нарушителей для исследуемой ТРИС представлен в таблице 2.7.

Таблица 2.7 – Перечень актуальных нарушителей для исследуемой ТРИС

№ п/п	Виды ущерба и возможные НП	Виды нарушителя	Категория нарушителя	Уровень возможностей нарушителя
1	У1 1. Нанесение ущерба субъекту путем незаконной обработки его ПДн, в том числе нарушения прав на неприкосновенность частной жизни, личную и семейную тайну	Преступные группы (криминальные структуры)	Внешний	Н2
		Отдельные физические лица (хакеры)	Внешний	Н1
		Авторизованные пользователи ТРИС	Внутренний	Н1
		Бывшие работники (пользователи)	Внешний	Н1
2	У2 1. Нарушение требований нормативных и методических документов в области информационной безопасности, влекущие за собой наложение санкций, например, в виде штрафов, предусмотренных КоАП 2. Нарушение деловой репутации юридическому лицу 4. Необходимость изменения (перестроения) бизнес-процессов, реализующих ТРИС 5. Виды ущербов, связанных с эксплуатацией критических информационных инфраструктур, автоматизированных систем управления технологическими процессами 6. Нанесение ущерба юридическому лицу путем утечки и незаконной обработки коммерческой тайны в виде финансового ущерба	Преступные группы (криминальные структуры)	Внешний	Н2
		Бывшие работники (пользователи)	Внешний	Н1
		Отдельные физические лица (хакеры)	Внешний	Н1
		Авторизованные пользователи ТРИС	Внутренний	Н1

В соответствии с положениями приказа ФСБ России №378 от 10 июля 2014 г. «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» и на основании определенного в настоящей Модели угроз уровня возможности нарушителя для обеспечения безопасности ПДн посредством применения СКЗИ [32] необходимо использовать следующий классы:

- за пределами КЗ – класс КС1 в соответствии с подпунктом «в» пункта 10 приказа ФСБ России № 378: проведение атаки, находясь вне пространства, в пределах которого осуществляется контроль за пребыванием и действиями лиц и (или) транспортных средств;
- в пределах КЗ – класс КС3 в соответствии с подпунктом «а» пункта 11 приказа ФСБ России № 378: проведение атаки при нахождении в пределах контролируемой зоны; и подпунктом «а» пункта 12 приказа ФСБ России № 378: физический доступ к СВТ, на которых реализованы СКЗИ и СФ.

2.3 Перечень возможных угроз безопасности информации

Для определенных типов актуальных нарушителей определяются следующие способы реализации (далее – СР) УБИ [22]:

1. Угрозы утечки информации по техническим каналам могут быть реализованы посредством:
   - «просмотра информации с помощью оптических (оптикоэлектронных) средств с экранов дисплеев и других средств отображения, СВТ, информационно-вычислительных комплексов, ТС

обработки графической, видео- и буквенно-цифровой информации, входящих в состав ТРИС»;

– «перехвата ПЭМИН, излучаемых СВТ в составе ТРИС при обработке информации в ТРИС, специальными техническим средствами радио-, радиотехнической разведки, размещенными как на территории КЗ ТРИС, так и за её пределами»;

– «перехвата ПЭМИН, возникающих при обработке информации в ТРИС, с использованием электронных устройств перехвата информации, подключенных к каналам связи или ТС обработки информации ТРИС».

2. Угрозы НСД к информации могут быть реализованы посредством:
   – воздействия на ТС ТРИС в ходе загрузки ОС;
   – прямого доступа к ПО или ТС ТРИС после загрузки ОС;
   – удаленного доступа к ПО или ТС ТРИС;
   – прямого или удаленного воздействия на объекты виртуальной среды ТРИС и информацию, хранимую в виртуальном пространстве ТРИС.
3. Угрозы специальных воздействий на ТРИС могут быть реализованы посредством:
   – механического воздействия;
   – химического воздействия;
   – акустического воздействия;
   – биологического воздействия;
   – радиационного воздействия;
   – термического воздействия;
   – электромагнитного воздействия:
   – электрическими импульсами;
   – электромагнитными излучениями;
   – магнитным полем.

При определении способа реализации УБИ подразумевалось, что угрозы могут быть реализованы непосредственно за счет доступа к компонентам ТРИС и (или) информации или косвенно за счет создания условий и (или) средств, обеспечивающих такой доступ.

Способы реализации УБИ, которые могут быть использованы нарушителями в соответствии с [22, 25], для исследуемой ТРИС являются следующие:

- Внедрение вредоносного ПО (установка ПО, имеющего скрытый функционал для возможности реализации УБИ):
- Внедрение вредоносного кода в веб-приложение (использование SQL, XSRF, XSS, CRLF инъекций, для реализации УБИ);
- Использование ошибок проектирования;
- Модификация, копирование, удаление конфигурационных и иных файлов;
- Использование вредоносных плагинов веб-браузера (установка расширений браузера для реализации УБИ);
- Использование уязвимостей ППО;
- Прослушивание линий связи (возможность прослушивания линий связи при помощи программного анализатора/приёмника пакетов либо установки аппаратного анализатора/приёмника пакетов);
- Использование уязвимостей СПО.

Таким образом, в таблице 2.8 приведен фрагмент сопоставления видов нарушителей, описания интерфейсов ОВ, доступных для использования нарушителями, и возможных СР УБИ.

Таблица 2.8 – Фрагмент сопоставления видов нарушителей, описания интерфейсов ОВ, доступных для использования нарушителями, и возможных СР УБИ

ОВ	**Вид нарушителя**		
	Преступные группы (криминальные структуры)	**Отдельные физические лица (хакеры), Бывшие (уволенные) работники (пользователи)**	**Авторизованные пользователи ТРИС**
ТРИС.ОВ.КС	-	-	ТРИС.ДИ.ФД
	-	-	ТРИС.СР.МИТМ
ТРИС.ОВ.АСО	ТРИС.ДИ.ВИ ТРИС.ДИ.КС	ТРИС.ДИ.ВИ ТРИС.ДИ.КС	ТРИС.ДИ.ВИ ТРИС.ДИ.КС
	ТРИС.СР.ВПО ТРИС.СР.ВК ТРИС.СР.УЗК ТРИС.СР.МУК ТРИС.СР.ВПБ ТРИС.СР.УСПО	ТРИС.СР.ВПО ТРИС.СР.ВК ТРИС.СР.УЗК ТРИС.СР.МУК ТРИС.СР.ВПБ ТРИС.СР.УСПО	ТРИС.СР.ВПО ТРИС.СР.ВК ТРИС.СР.УЗК ТРИС.СР.МУК ТРИС.СР.ВПБ ТРИС.СР.УППО ТРИС.СР.УСПО
ТРИС.ОВ.СП	-	-	ТРИС.ДИ.КС
	-	-	ТРИС.СР.ВПО ТРИС.СР.УЗК ТРИС.СР.МУК ТРИС.СР.УППО ТРИС.СР.УСПО

В соответствии с положениями п. 5.3.3. Методики ФСТЭК России [25] УБИ возможна при условии наличия актуального нарушителя, ОВ, СР УБИ и НВ в случае успешной реализации УБИ:

$$УБИi = [Н; ОВ; СР\ УБИ; СрЗИ; НП],$$

где,

УБИi – i угроза безопасности информации из Банка данных угроз ФСТЭК России (далее – БДУ);

Н – актуальный нарушитель;

ОВ – объект воздействия;

СР УБИ – способ реализации УБИ;

СрЗИ – средство защиты информации, предназначенное для нейтрализации УБИ;

НП – негативные последствия.

На основании вышеизложенного, результатов главы 1 и БДУ ФСТЭК России определен перечень УБИ для исследуемой ТРИС, а также определена их возможность. Фрагмент перечня возможных УБИ в исследуемой ТРИС представлен в таблице 2.9.

Таблица 2.9 – Перечень возможных УБИ в исследуемой ТРИС

№ УБИ из БДУ	Наименование УБИ	Вид нарушителя	ОВ	СР УБИ	НП	Возможность УБИ
004	Угроза аппаратного сброса пароля BIOS	Авторизованные пользователи ТРИС	ТРИС.ОВ.СП	-	У2	Невозможна
006	Угроза внедрения кода или данных	Отдельные физические лица (хакеры), Бывшие (уволенные) работники (пользователи), Преступные группы (криминальные структуры)	ТРИС.ОВ.СП ТРИС.ОВ.АРМ ТРИС.ОВ.ППО ТРИС.ОВ.АСО	СР.ВПО СР.ВК СР.УЗК СР.МУК СР.ВПБ СР.УППО СР.УСПО СР.МИТМ	У1, У2	Возможна
007	Угроза воздействия на программы с высокими привилегиями	Преступные группы (криминальные структуры)	ТРИС.ОВ.СП ТРИС.ОВ.АСО, ТРИС.ОВ.КС	СР.ВПО СР.ВК СР.УЗК СР.МУК СР.ВПБ СР.УППО	У1, У2	Возможна
008	Угроза восстановления и/или повторного использования аутентификационной информации	Отдельные физические лица (хакеры), Бывшие (уволенные) работники (пользователи); Авторизованные пользователи ТРИС	ТРИС.ОВ.СП ТРИС.ОВ.АРМ ТРИС.ОВ.АСО	СР.ВПО СР.ВК СР.УЗК СР.МУК СР.ВПБ СР.УППО	У1, У2	Возможна
009	Угроза восстановления предыдущей уязвимой версии BIOS	Авторизованные пользователи ТРИС	ТРИС.ОВ.СП	-	У2	Невозможна
010	Угроза выхода процесса за пределы виртуальной машины	Преступные группы (криминальные структуры)	ТРИС.ОВ.СП ТРИС.ОВ.АСО ТРИС.ОВ.МН	СР.ВПО СР.ВК СР.УЗК СР.МУК СР.ВПБ СР.УППО	У1, У2	Возможна

В соответствии с положениями п. 5.3.4 Методики ФСТЭК России [25], актуальность возможных УБИ определяется наличием сценариев их реализации.

Для исследуемой ТРИС определен набор возможных сценариев реализации УБИ (тактик, техник и процедур). В таблице 2.10 приведен фрагмент перечня сценариев реализации возможных УБИ.

Таблица 2.10 – Фрагмент перечня сценариев реализации возможных УБИ

№ п/п	№ УБИ из БДУ ФСТЭК России	Наименование УБИ	Сценарий реализации УБИ
1.	006	Угроза внедрения кода или данных	T1.3, T1.4, T1.5, T1.9, T1.11, T1.12, T1.16, T2.3, T2.5, T2.7, T2.8, T2.10, T2.11, T2.12, T3.1, T3.6, T3.7, T3.8, T3.9, T3.10, T3.14, T3.15, T3.16, T4.1, T4.5, T4.7, T5.1, T5.2, T5.3, T5.4, T5.6, T5.8, T5.9, T5.10, T5.11, T6.1, T6.2, T6.4, T6.5, T6.6, T6.8, T6.9, T7.1, T7.3, T7.4, T7.6, T7.8, T7.10, T7.11, T7.12, T7.13, T7.15, T7.16, T7.17, T7.18, T7.20, T7.21, T7.23, T7.24, T7.25, T7.26, T8.1, T8.2, T8.4, T8.5, T8.6, T8.8, T9.1 T9.3, T9.4, T9.5, T9.7, T9.9, T9.12, T9.13, T10.1, T10.2, T10.3, T10.4, T10.5, T10.6, T10.8. T10.10, T10.11
2.	007	Угроза воздействия на программы с высокими привилегиями	T1.3, T1.4, T1.5, T1.9, T1.11, T1.12, T1.16, T2.3, T2.5, T2.7, T2.8, T2.10, T2.11, T2.12, T3.1, T3.6, T3.7, T3.8, T3.9, T3.10, T3.14, T3.15, T3.16, T4.1, T4.5, T4.7, T5.1, T5.2, T5.3, T5.4, T5.6, T5.8, T5.9, T5.10, T5.11, T6.1, T6.2, T6.4, T6.5, T6.6, T6.8, T6.9
3.	008	Угроза восстановления и/или повторного использования аутентификационной информации	T1.3, T1.4, T1.5, T1.9, T1.11, T1.12, T1.16, T2.3, T2.5, T2.7, T2.8, T2.10, T2.11, T2.12

Для ряда возможных УБИ при определении сценариев реализации (тактик, техник и процедуры) также использовалась международная база данных MITRE ATT&CK, ввиду отсутствия единой базы данных и не достаточного наполнения информацией об известных тактиках, техниках и процедурах (способов и сценариев реализации УБИ).

С помощью навигатора, предоставляемого ресурсом MITRE ATT&CK (https://mitre-attack.github.io/attack-navigator/enterprise/), составим модель атак, состоящей из тактик и техник потенциального нарушителя для исследуемой ТРИС, архитектура которой была приведена в главе 1 настоящего диссертационного исследования, в виде матрицы.

Составим матрицу тактик и техник атак (в качестве элементов матрицы – уникальные идентификаторы). Идентификаторы используются присвоенные MITRE ATT&CK. Матрица представлена в таблице 2.11.

Таблица 2.11 – Матрица тактик и техник атак MITRE ATT&CK

TA0001	TA0002	TA0003	TA0004	TA0005	TA0006	TA0007	TA0008	TA0009	TA0011	TA0010	TA0040
T1189	T1155	T1156	T1134	T1134	T1098	T1087	T1155	T1123	T1043	T1020	T1531
T1190	T1191	T1015	T1015	T1527	T1139	T1010	T1527	T1119	T1092	T1002	T1485
T1133	T1059	T1098	T1182	T1009	T1110	T1217	T1017	T1115	T1090	T1022	T1486
T1200	T1223	T1182	T1103	T1197	T1522	T1538	T1175	T1530	T1094	T1030	T1491
T1191	T1175	T1103	T1138	T1088	T1003	T1526	T1210	T1213	T1024	T1048	T1488
T1193	T1196	T1138	T1088	T1146	T1503	T1482	T1534	T1005	T1132	T1041	T1487
T1192	T1173	T1131	T1038	T1191	T1081	T1083	T1037	T1039	T1001	T1011	T1499
T1194	T1106	T1197	T1157	T1116	T1214	T1046	T1075	T1025	T1172	T1052	T1495
T1195	T1129	T1067	T1514	T1500	T1212	T1135	T1097	T1074	T1483	T1029	T1490
T1199	T1203	T1176	T1519	T1223	T1187	T1040	T1076	T1114	T1008	T1537	T1498
T1078	T1061	T1042	T1068	T1109	T1179	T1201	T1105	T1056	T1188		T1496
	T1118	T1109	T1181	T1122	T1056	T1120	T1021	T1185	T1104		T1494
	T1152	T1122	T1044	T1090	T1141	T1069	T1091	T1113	T1026		T1489
	T1168	T1136	T1179	T1196	T1208	T1057	T1051	T1125	T1079		T1492
	T1177	T1038	T1183	T1207	T1142	T1012	T1184		T1205		T1529
	T1170	T1157	T1160	T1140	T1171	T1018	T1080		T1219		T1493
	T1086	T1519	T1050	T1089	T1040	T1063	T1072		T1105		
	T1121	T1133	T1502	T1038	T1174	T1518	T1506		T1071		
	T1117	T1044	T1034	T1073	T1145	T1082	T1077		T1032		
	T1085	T1158	T1150	T1480	T1167	T1016	T1028		T1095		
	T1053	T1179	T1013	T1211	T1528	T1049			T1065		
	T1064	T1062	T1504	T1181	T1539	T1033			T1102		
	T1035	T1183	T1055	T1222	T1111	T1007					
	T1218	T1525	T1053	T1107		T1124					
	T1216	T1215	T1058	T1006		T1497					
	T1153	T1159	T1166	T1144							
	T1151	T1160	T1178	T1484							
	T1072	T1152	T1165	T1158							
	T1154	T1161	T1169	T1147							
	T1127	T1168	T1206	T1143							
	T1204	T1162	T1078	T1148							
	T1047	T1037	T1100	T1183							
	T1028	T1177		T1054							
	T1220	T1031		T1066							
		T1128		T1070							
		T1050		T1202							
		T1137		T1130							
		T1034		T1118							
		T1150		T1152							
		T1205		T1149							
		T1013		T1036							
		T1504		T1112							
		T1163		T1170							
		T1164		T1126							
		T1108		T1096							
		T1060		T1027							
		T1053		T1502							
		T1180		T1150							
		T1101		T1205							
		T1505		T1186							
		T1058		T1093							
		T1166		T1055							
		T1023		T1108							
		T1198		T1121							
		T1165		T1117							
		T1019		T1536							
		T1501		T1014							
		T1209		T1085							
		T1154		T1064							
		T1078		T1218							

Таблица 2.11. Продолжение

		T1100		T1216							
		T1084		T1198							
		T1004		T1045							
				T1151							
				T1221							
				T1099							
				T1127							
				T1535							
				T1078							
				T1497							
				T1102							
				T1506							
				T1220							

На основе проведенного анализа в настоящей работе в качестве предметной онтологии предлагается принимать модель атак на ИС концептуальную модель [93], включающую тактики и техники атак MITRE ATT&CK. Сформированная модель атак имеет иерархическую структуру, состоящую из трех уровней:

1. Уровень модели атак (подготовка атак (PRE_ATT), атаки на предприятие (ENT_ATT), атаки на мобильные устройства (MOB_ATT)).
2. Уровень тактик атак.
3. Уровень техник атак.

Структура модели представлена на рисунке 2.1.

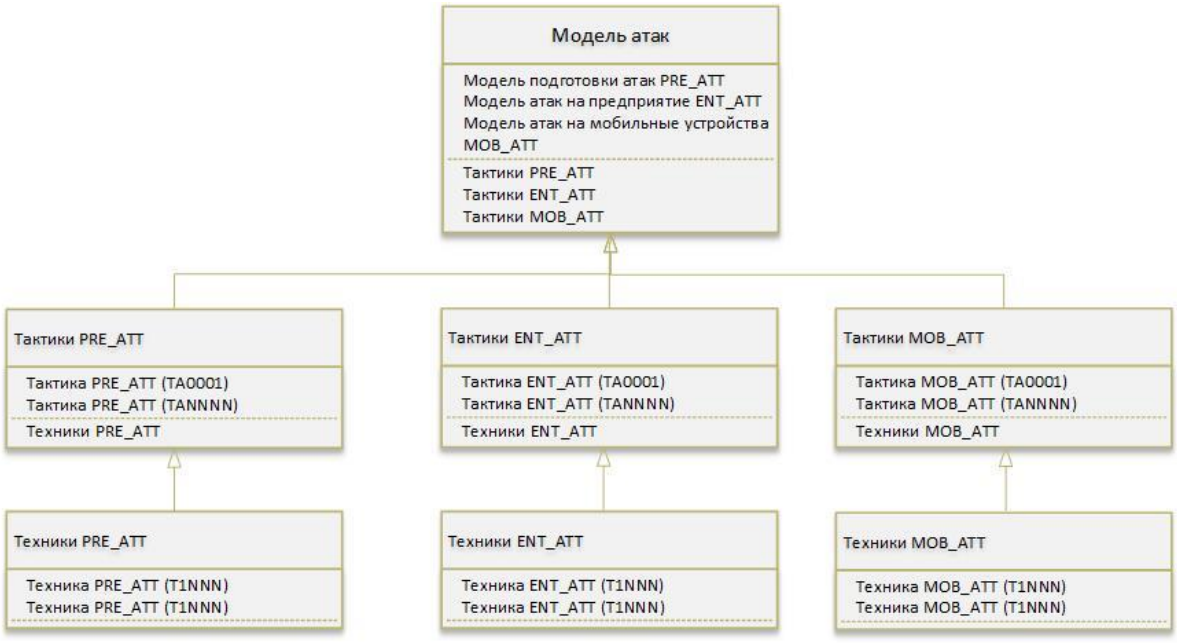


Рисунок 2.1 – Структура модели атак

Обобщенная схема модели атак представлена на рисунке 2.2.

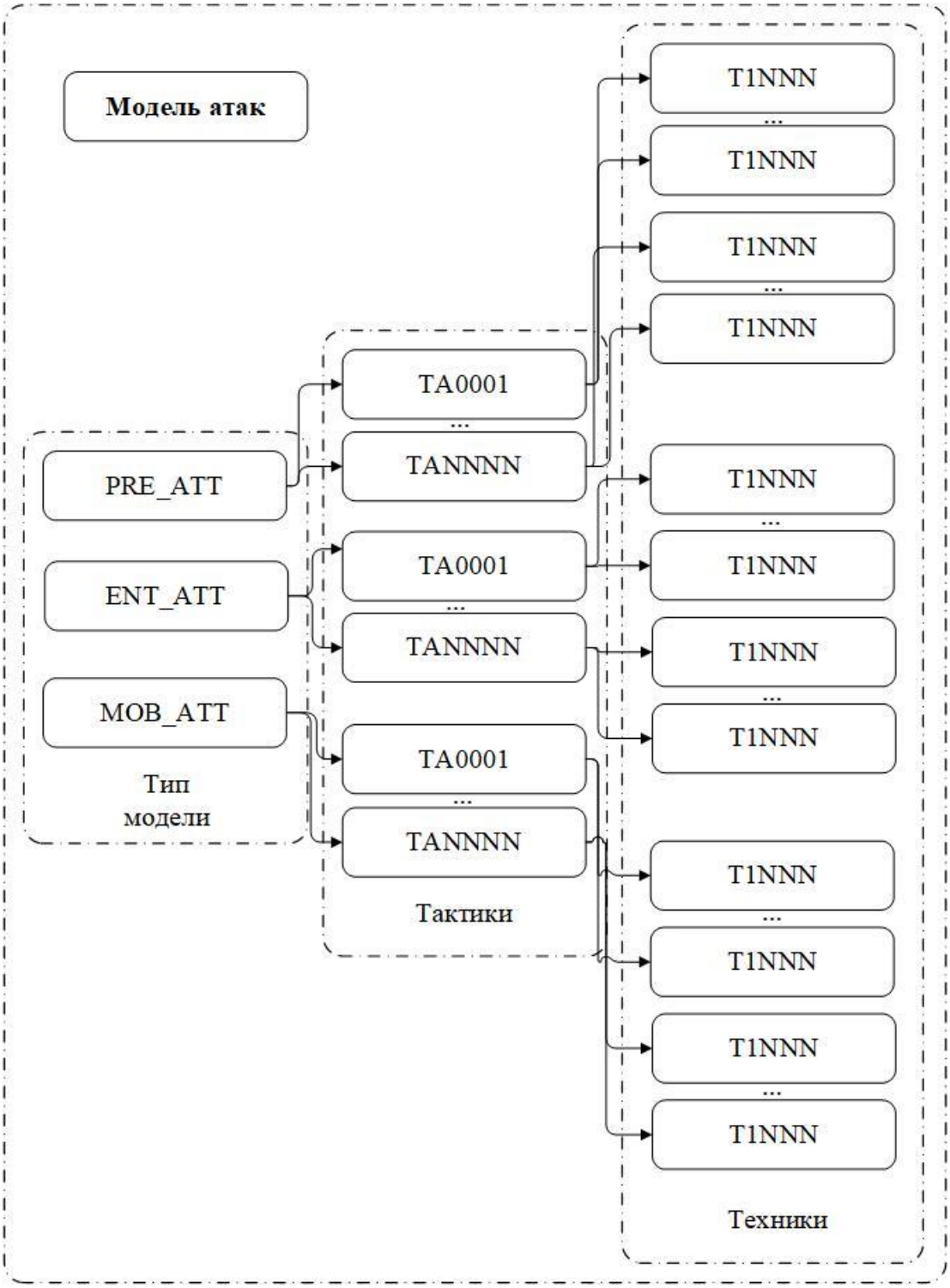


Рисунок 2.2 – Обобщенная схема модели атак

В результате формируется итоговый набор данных с учетом экспертных оценок и статических моделей УБИ на основе БДУ ФСТЭК России (MITRE ATT&CK), включающий в себя определенного для исследуемой ТРИС актуального нарушителя, объектов воздействия с версиями ПО (элементов или

информационных активов ТРИС), а также возможных тактик, техник и способов реализации, характерных для актуального нарушителя в исследуемой ТРИС.

По результатам проведенного исследования можно сказать о том, что существующие методологии в большинстве своем имеют существенные недостатки, а именно: большой объем данных, отсутствие документации, отсутствие автоматизированных средств определения актуальных УБИ, необходимость в высокой квалификации специалистов по информационной безопасности.

В связи с вышесказанным в настоящей главе были поставлены следующие задачи:

1. Подготовка набора данных для определения перечня актуальных УБИ на основании известных баз данных УБИ и уязвимостей, а также разработанных ранее статических моделей угроз для ТРИС.
2. Анализ сформированного набора данных.
3. Форматирование набора данных для последующей автоматизированной обработки.
4. Выбор и сравнение качества работы нескольких моделей, определение наилучшей.
5. Определение параметров в наилучшей модели.
6. Проверка модели.
7. Разработка программы определения актуальных УБИ для ЭВМ «Модель угроз и нарушителя».
8. Итоговое представление результатов работы.

2.4 Методика определения актуальных угроз безопасности информации

2.4.1 Подготовка набора данных для определения актуальных угроз безопасности информации

Для преставления набора данных для автоматизированной обработки и разработки программного обеспечения использовался язык программирования Python 3 и технологии Data Science [74].

Сложностью определения актуальных УБИ для исследуемой ТРИС является обработка большого объема данных [58], необходимого при определении перечня актуальных УБИ, а именно: данные из БДУ ФСТЭК России и (или) зарубежных баз данных и знаний, сложность использования методических документов регуляторов РФ в области обеспечения безопасности информации.

В данной работе набор данных был сформирован на основании данных из БДУ ФСТЭК России и на основании ранее разработанных моделей угроз подобных ТРИС, описанной выше.

На рисунках 2.3 и 2.4 представлены графики анализа данных БДУ ФСТЭК России.

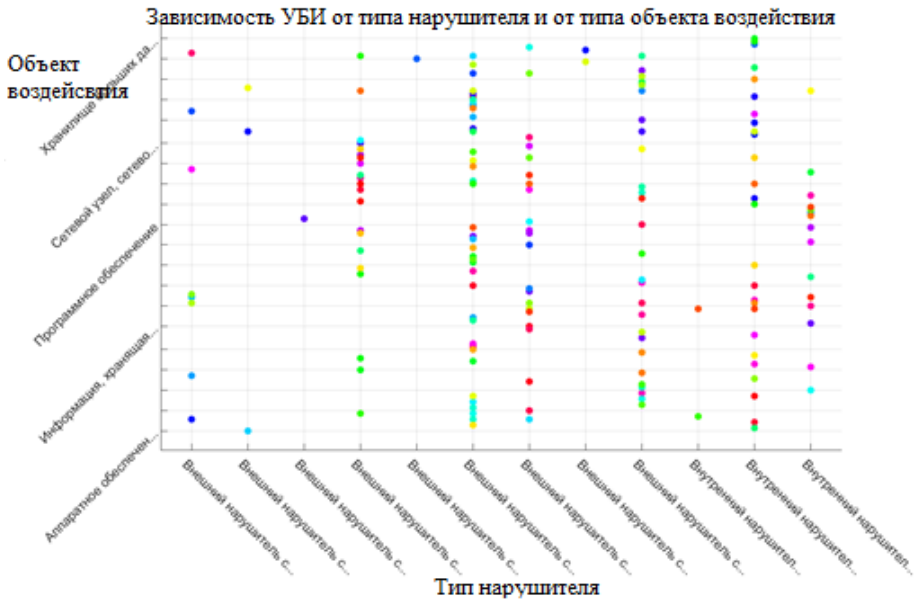


Рисунок 2.3 – Зависимость УБИ от типа нарушителя и от типа объекта воздействия

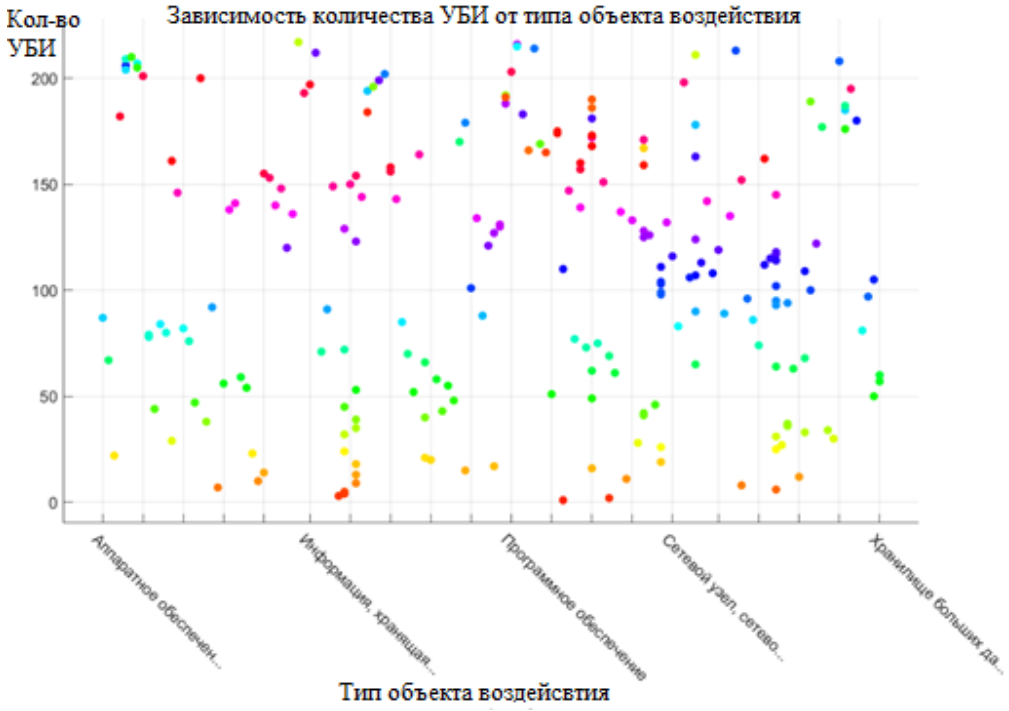


Рисунок 2.4 – Зависимость количества УБИ от типа объекта воздействия

Также был проведен анализ уязвимостей БДУ ФСТЭК России. На рисунке 2.5 представлен график зависимости количества уязвимостей от производителя.

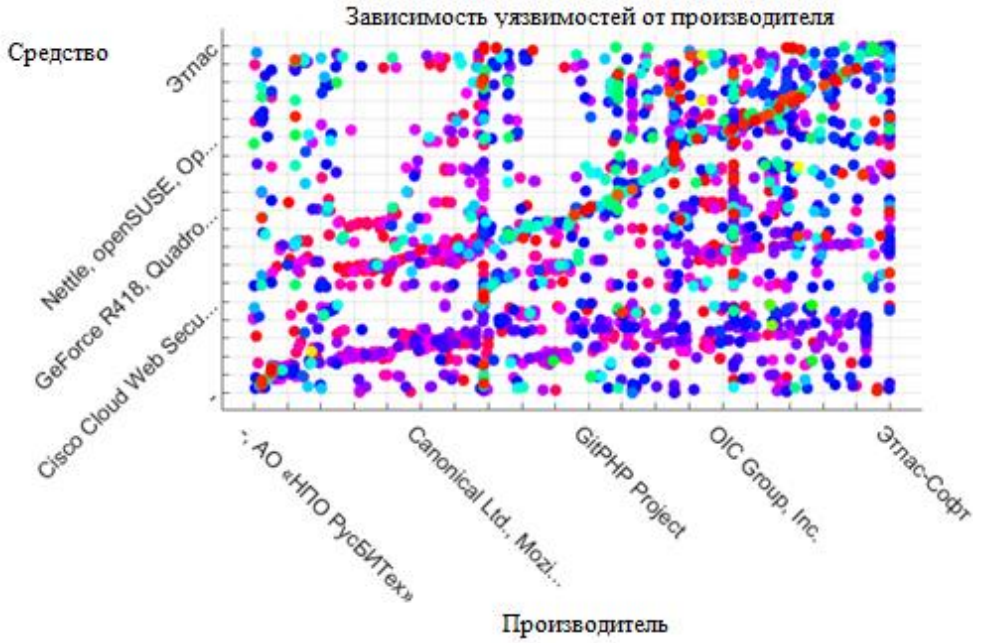


Рисунок 2.5 – График зависимости уязвимостей от производителя

Как видно из графиков информация имеет большой объем, что вызывает трудоемкость в процессе определения актуальных УБИ [92]. Экспертный подход определения актуальных УБИ влечет за собой ошибки, связанные с человеческим фактором, такие как: личное мнение эксперта, разрозненность и несогласованность мнений, трудоемкость. Методические документы регуляторов РФ определяют подход и этапы определения актуальных УБИ, при этом ошибки экспертов и трудоемкость не учитываются [58, 78, 79, 81].

В соответствии с МД регуляторов РФ актуальность УБИ определяется в зависимости от актуального нарушителя в ТРИС, перечнем потенциальных УБИ и уязвимостей в ИТ-инфраструктуре ТРИС, а также возможными последствиями от реализации УБИ. В этой связи набора данных был сформирован из сведений базы данных угроз ФСТЭК России, моделей УБИ ТРИС и технических решений исследуемой ТРИС.

2.4.2 Преобразование набора данных

На рисунках 2.6 и 2.7 представлены наборы данных dataframe БДУ ФСТЭК России до конвертации данных.

```
In [5]: r_bdu = pd.read_excel('thrlist (8).xlsx')
        r_bdu
```

Out[5]:

	Общая информация	Unnamed: 1	Unnamed: 2	Unnamed: 3	Unnamed: 4	Последствия	Unnamed: 6	Unnamed: 7	Дополните
0	Идентификатор УБИ	Наименование УБИ	Описание	Источник угрозы (характеристика и потенциал на...	Объект воздействия	Нарушение конфиденциальности	Нарушение целостности	Нарушение доступности	Дата вклю угрозы
1	1	Угроза автоматического распространения вредоно...	Угроза заключается в возможности внедрения и з...	Внешний нарушитель со средним потенциалом, Вну...	Ресурсные центры грид-системы	1	1	1	2015-00
		Угроза агрегирования	Угроза	Внешний					

Рисунок 2.6 – Dataframe УБИ БДУ ФСТЭК России до конвертации

```
In [9]: r_vul = pd.read_excel('vullist.xlsx')
        r_vul
```

Out[9]:

	Описание уязвимостей	Unnamed: 1	Unnamed: 2	Unnamed: 3	Unnamed: 4	Unnamed: 5	Unnamed: 6	Unnamed: 7	Unnam
0	Общая информация	NaN	NaN	NaN	NaN	NaN	NaN	NaN	
1	Идентификатор	Наименование уязвимости	Описание уязвимости	Вендор ПО	Название ПО	Версия ПО	Тип ПО	Наименование ОС и тип аппаратной платформы	уязви
2	BDU:2014-00001	Уязвимость микропрограммного обеспечения прогр...	Микропрограммное обеспечение модуля 140NOE7711...	Schneider Electric	Микропрограммное обеспечение программируемого ...	4.6 (Микропрограммное обеспечение программируе...	ПО программно-аппаратного средства АСУ ТП	Schneider Electric Микропрограммное обеспечени...	Уязви архите
3	BDU:2014-00002	Уязвимость микропрограммного обеспечения маршр...	Скрипт «/scgi-bin/platform.cgi» микропрограммн...	D-Link Corp.	Микропрограммное обеспечение маршрутизатора D–...	1.02b11 (Микропрограммное обеспечение маршрути...	ПО сетевого программно-аппаратного средства	D-Link Corp. Микропрограммное обеспечение марш...	Уязви

Рисунок 2.7 – Dataframe уязвимостей БДУ ФСТЭК России до конвертации

Для подготовки итогового набора данных в предложенной методике определения актуальных УБИ использовались БДУ ФСТЭК России, MITRE ATT&CK, статические модели УБИ ТРИС, а также экспертные оценки при определении актуальных нарушителей. Сформированный dataframe представляет собой матрицу (табличная форма), для которой требуется преобразование для последующей автоматизированной обработки.

Итоговый фрагмент набора при автоматизированной обработке представлен на рисунке 2.8.

```
In [20]: r_bdu = pd.read_excel('C:\\Users\\minyaev.a\\Desktop\\python\\MUiN\\dataset_UBI.xlsx')
         r_bdu
```

Out[20]:

	Hacker	Target	TTP
0	Специальные службы иностранных государств	Мобильное устройство (аппаратное устройство) н...	T3.1\nT7.4\n\nT1204\nT1399
1	Террористические, экстремистские группировки	Средство защиты информации\n\n12.4 (Cisco IOS)...	T6.1\nT7.21\n\nT1562\nT1056
2	Преступные группы (криминальные структуры)	Виртуальная машина VMWare\n\n6.5 (VMWare Works...	T1.3\nT1.4\n\nT1592.004\nT1205
3	Отдельные физические лица (хакеры)	узлы хранилища больших данных	T1595.001: Scanning IP Blocks
4	Конкурирующие организации	Метаданные	T1595.002: Vulnerability Scanning
5	Разработчики программных, программно- аппаратн...	Вычислительные узлы суперкомпьютера	T1592.004: Client Configurations
6	Лица, обеспечивающие поставку программных, про...	Облачная система, Облачная инфраструктура, обл...	T1592.003: Firmware
7	Поставщики вычислительных услуг, услуг связи	Гипервизор	T1592.001: Hardware
8	Лица, привлекаемые для установки, настройки, ...	Узлы грид-системы	T1592.002: Software
9	Лица, обеспечивающие функционирование АС ОЗ БР...	Хранилище больших данных	T1589.001: Credentials
10	Авторизованные пользователи АС ОЗ БР	Мобильное устройство	T1589.002: Email Addresses

Рисунок 2.8 – Итоговый фрагмент набора данных для определения перечня актуальных УБИ

Для подготовки автоматизированной обработки данных необходимо выполнить конвертацию данных [58, 77]. Код на языке программирования Python

3 для преобразования данных dataframe (конвертирование данных) представлен ниже:

```
train = pd.read_csv('threats.csv', encoding='utf-8')
df = pd.get_dummies(train)
# Преобразование строковых данных
for col in list(df.columns):
   # Выбор колонок для преобразования
   if ('ft²' in col or 'kBtu' in col or 'Metric Tons CO2e' in col or 'kWh' in
      col or 'therms' in col or 'gal' in col or 'Score' in col):
      # Конвертация
      df[col] = df[col].astype(float)
```

По результатам преобразования данных dataframe необходимо определить модель для реализации методики, повысить его эффективность по отношению к известным за счет определения и адаптации наилучших параметров системы.

На основании сформированного итогового набора данных для определения актуальных УБИ необходимо определить модель [94], наиболее подходящую для решения поставленной задачи.

2.4.3 Выбор модели определения актуальных угроз безопасности информации

Было проведено исследование адаптивных нечетких нейронных продукционных систем ANFIS (adaptive neuro-fuzzy inference system) с применением алгоритмов нечеткого вывода Сугено-Такаги, Такаги-Сугено-Канга, Ванга-Менделя и Мамдани [86, 87]. Отмечено, что зависимость погрешности от количества правил при проверке на тестовой выборке меньше у сети ANFIS с алгоритмом нечеткого вывода Такаги-Сугено-Канга. В этой связи для определения актуальных УБИ была выбрана адаптивная нечеткая нейронная продукционная система ANFIS [95], основанная на нечеткой системе вывода Такаги-Сугено-Канга (далее – TSK).

Алгоритм ее работы заключается в реализации нечеткой продукционной модели, основанной на правилах типа:

$$R_i : IFx_i ISA_{i1} AND...ANDx_j ISA_{ij} AND...ANDx_{im} ISA_{im}, THEN$$

$$y = c_{i0} + \sum_{j=1}^{m} c_{ij} x_j), j = 1,...,n$$

Для этого была сформирована база правил для определения актуальных УБИ. Пример заполнения базы правил на основании сформированного в данной работе набора данных приведен в таблице 2.11.

Таблица 2.11 – Фрагмент базы правил методики определения актуальных УБИ

№ п/п	**ЕСЛИ (IF)**			**ТО (THEN)**
	Тип нарушителя (источник воздействия)	**ИТ – инфраструктура (объект воздействия, версия ПО)**	**Сценарий реализации (тактики, техники и процедуры)**	
1	Внешний нарушитель с низким потенциалом, Внутренний нарушитель с низким потенциалом	Виртуальная машина VMWare 6.5 (VMWare Workstation), от 7.0.0 до 7.1.4 включительно (VMWare Workstation)	T1.3 T1.4 T1592.004 T1205	Угроза несанкционированного доступа к защищаемым виртуальным машинам со стороны других виртуальных машин (УБИ.079)
2	Внешний нарушитель с высоким потенциалом	Мобильное устройство (аппаратное устройство) на базе iOS (Android), до 10.3.3 включительно (iOS)	T3.1 T7.4 T1204 T1399	Угроза контроля вредоносной программой списка приложений, запущенных на мобильном устройстве (УБИ.196)
…				

Таблица 2.11. Продолжение

N	Внешний нарушитель со средним потенциалом, Внутренний нарушитель со средним потенциалом	Средство защиты информации 12.4 (Cisco IOS), 12.4 (Cisco IOS), 15.0 (Cisco IOS), 15.0 (Cisco IOS), 15.1 (Cisco IOS), 15.1 (Cisco IOS), 12.2 (Cisco IOS), 12.2 (Cisco IOS), 15.2 (Cisco IOS), 15.2 (Cisco IOS)	Т6.1 Т7.21 Т1562 Т1056	Угроза несанкционированного воздействия на средство защиты информации (УБИ.187)

Количество правил n для случая определения актуальных УБИ на основе БДУ ФСТЭК России равно 222. Для определения уязвимостей на основе БДУ ФСТЭК России оно будет составлять n=30321. Правила представлены в таблице 2.11 как единое, фактически оно представляет множество правил, состоящих отдельно по типу нарушителя, типу СрЗИ (например, SecretNet, Dallas Lock и т.д.) и по воздействию. Набор данных был сформирован уже с учетом этих нюансов. Объект воздействия – совокупность данных из БДУ ФСТЭК России и данных об ИТ-инфраструктуре ИС, взятых из моделей УБИ и проектных решений по СЗИ.

Конечный результат определения актуальности УБИ рассчитывается по совокупности показателей методики определения актуальных УБИ, описанных в разделе 2.3 настоящей работы.

ANFIS базируется на следующих положениях [76]:

– входные переменные являются четкими;

– функции принадлежности (далее – ФП) определены функцией Гаусса:

$$\mu_{A_{ij}}(x_j) = \exp(-\frac{1}{2}(\frac{x_j - a_{ij}}{b_{ij}})^2)$$

где x_j – входные сети a_{ij}, b_{ij} - настраиваемые параметры ФП.

– нечеткая импликация Ларсена – нечеткое произведение;

– Т-норма – нечеткое произведение;

– композиция не производится;

– метод дефаззификации – метод центроида.

Функциональная зависимость после дефаззификации для получения выходной переменно принимает следующий вид [75, 76]:

$$y^{'} = \frac{\Sigma_{i}^{n}((c_{i0} + \Sigma_{j=1}^{m} c_{ij} x_j)\Pi_{j}^{m} \mu_{A_{ij}}(x_j^{'}))}{\Sigma_{i=1}^{n} \Pi_{j}^{m} \mu_{A_{ij}}(x_j^{'})} = \frac{\Sigma_{i}^{n}((c_{i0} + \Sigma_{j=1}^{m} c_{ij} x_j))\Pi_{j}^{m} \exp\left[-(\frac{x_j^{'} - a_{ij}}{b_{ij}})^2\right]}{\Sigma_{i=1}^{n} \Pi_{j}^{m} \exp\left[-(\frac{x_j^{'} - a_{ij}}{b_{ij}})^2\right]} \quad (2.1)$$

Выражение 2.1 лежит в основе сети ANFIS с применением алгоритма TSK, которая включает в себя пять слоев:

Первый слой выполняет фаззификацию входных четких переменных:

$$x_j^{'}(j = 1,...,n).$$

Элементы второго слоя вычисляют значения степеней ФП $\mu_{A_{ij}}\left[x_j^{'}\right]$, заданных функциями Гаусса с параметрами a_{ij}, b_{ij} .

Третий слой генерирует значения функций $(c_{j0} + \Sigma_{j=1}^{m} c_{ij} x_j^{'})$, которые перемножаются на результаты вычислений элементами второго слоя.

Первый элемент слоя 4 необходим для активизации заключений правил в соответствии со значениями, агрегированных в 3 слое, степеней принадлежности предпосылок правил. Второй элемент четвертого слоя производит дополнительные вычисления для последующей дефаззификации результата работы сети ANFIS.

Данный слой состоит из одного нормализующего элемента и производит дефаззификацию результатов работы сети ANFIS.

ANFIS TSK содержит 2 параметрических слоя (слой 1 и 3). Настраиваемыми в процессе обучения сети ANFIS параметрами являются:

– в 1 слое – нелинейные параметры a_{ij}, b_{ij} ФП фаззификатора;

– в 3 слое – параметры c_{i0} и c_{ij} линейных функций $(c_{j0} + \Sigma_{j=1}^{m} c_{ij} x_j^{'})$ из заключений базы правил.

При наличии n правил и m-входных переменных число параметров 1 слоя равно $2nm$, а 2 – $n(m+1)$. Суммарное общее число настраиваемых параметров равно $n(3m+1)$.

На следующем шаге предложенного метода рассчитываются параметры c_{i0} и c_{ij} с линейных функций при условии фиксированных значений параметров a_{ij}, b_{ij} . Параметры c_{i0} и c_{ij} находятся путем решения системы линейных уравнений.

Выходную переменную из выражения 2.1 представляем в следующем виде:

$$y^{'} = \sum_{i=1}^{n} w_i^{'}(c_{i0} + \sum_{j=1}^{m} c_{ij} x_j),$$

где

$$w_i^{'} = \frac{\Pi_{j=1}^{m} \mu_{A_{ij}}(x_j^{'})}{\sum_{i=1}^{n} \Pi_j^m \mu_{A_{ij}}(x_j^{'})} = \frac{\Pi_j^m \exp\left[-(\frac{x_j^{'} - a_{ij}}{b_{ij}})^2\right]}{\sum_{i=1}^{n} \Pi_j^m \exp\left[-(\frac{x_j^{'} - a_{ij}}{b_{ij}})^2\right]} = const$$

Алгоритм обучения сети ANFIS с применением алгоритма TSK.

При K обучающих примерах $x_1^{(k)}, x_2^{(k)}, ..., x_m^{(k)}, y^{(k)}$, где $k=1,...,K$ и замене значений выходных переменных $y'^{(k)}$ значениями эталонных переменных $y^{(k)}$, получим систему из K линейных уравнений вида:

$$\begin{bmatrix} w_1^{'(1)} & w_1^{'(1)}x_1^{(1)} & \dots & w_1^{'(1)}x_m^{(1)} & \dots & w_n^{'(1)} & w_n^{'(1)}x_1^{(1)} & \dots & w_n^{'(1)}x_m^{(1)} \\ w_1^{'(2)} & w_1^{'(2)}x_1^{(2)} & \dots & w_1^{'(2)}x_m^{(2)} & \dots & w_n^{'(2)} & w_n^{'(2)}x_1^{(2)} & \dots & w_n^{'(2)}x_m^{(2)} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ w_1^{'(k)} & w_1^{'(k)}x_1^{(k)} & \dots & w_1^{'(k)}x_m^{(k)} & \dots & w_n^{'(k)} & w_n^{'(k)}x_1^{(k)} & \dots & w_n^{'(k)}x_m^{(k)} \end{bmatrix} x \begin{bmatrix} c_{10} \\ \dots \\ c_{1m} \\ \dots \\ c_{n0} \\ \dots \\ c_{nm} \end{bmatrix} = \begin{bmatrix} y^{(1)} \\ y^{(2)} \\ \dots \\ y^{(k)} \end{bmatrix} \quad (2.2)$$

где $w_i^{'(k)}$ агрегированная степень истинности предпосылок по i -му правилу при предъявлении k -го входного вектора $(x_1^{(k)}, x_2^{(k)}, ..., x_m^{(k)})$.

Таким образом, 2.2 в сокращенном виде:

$$W \times c = y$$

Матрица W имеет размерность равной $K \times (m+1)n$, при этом количество строк k значительно больше количества столбцов: $K \times (m+1)n$. Решение этой системы уравнений можно провести за один шаг при помощи псевдоинверсии матрицы W:

$$c = W^{+} y = (W^{T} \bullet W)^{-1} W^{T} y$$

После определения линейных параметров ij фиксируем и рассчитываем фактические выходные сигналы сети для всех примеров, для чего используем линейную зависимость:

$$y^{'} = \begin{bmatrix} y^{(1)} \\ y^{(2)} \\ \dots \\ y^{(k)} \end{bmatrix} = W \bullet c$$

определяем вектор ошибок:

$$e = y^{'} - y$$

производим уточнение параметры:

$$a_{ij}^{(k)}(t+1) = a_{ij}^{(k)}(t) - C \frac{dE^{(k)}(t)}{da_{ij}^{(k)}}$$

$$b_{ij}^{(k)}(t+1) = b_{ij}^{(k)}(t) - C \frac{dE^{(k)}(t)}{db_{ij}^{(k)}}$$

Структура нечеткой нейронной продукционной сети ANFIS с применением алгоритма TSK представлена на рисунке 2.8.

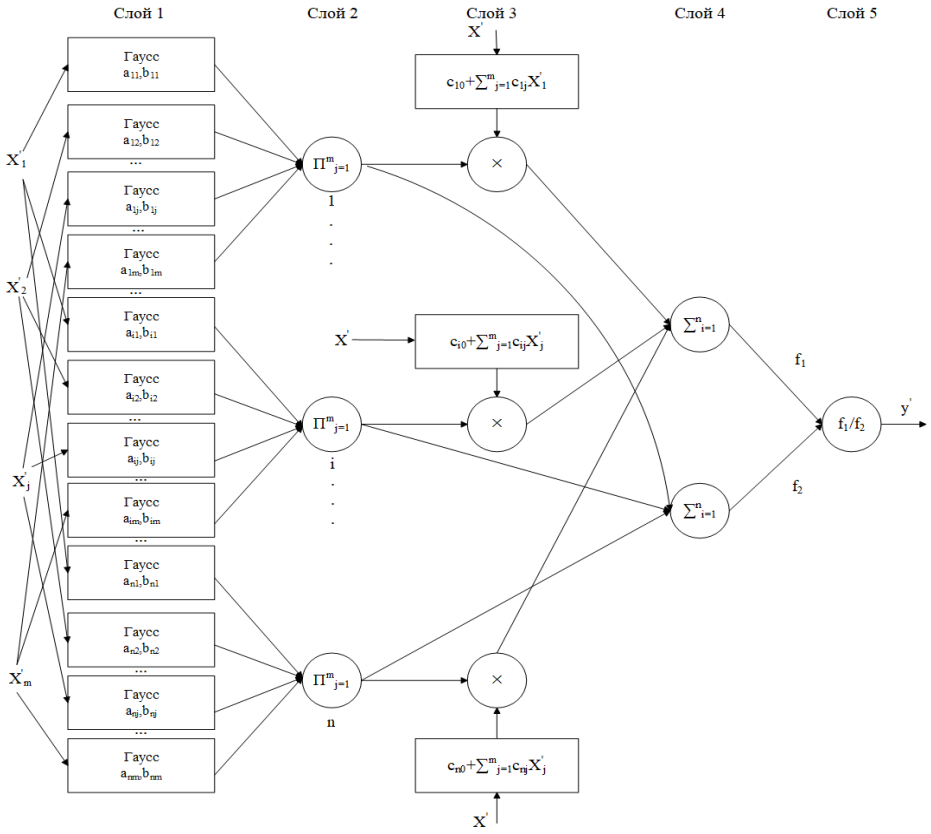


Рисунок 2.8 – Сеть ANFIS с применением алгоритма TSK

Для проведения вычислений и определения актуальных УБИ в данной работе было разработана программа для ЭВМ «Модель угроз и нарушителя» (Приложение А) на языке программирования Python 3, а также расчеты были проведены в среде MATLAB для сравнения и иллюстрации исследований.

2.4.4 Определение параметров в наилучшей модели

При первоначальных исходных данных и параметров сети ANFIS ошибка обучения сети составляла 3,6-3,7. В ходе проведения экспериментов было установлено, что при определенных параметрах сети ANFIS, очистки и преобразования набора исходных данных ошибка обучения уменьшается.

На рисунках 2.9 – 2.11 представлены настройки сети ANFIS в среде MATLAB.

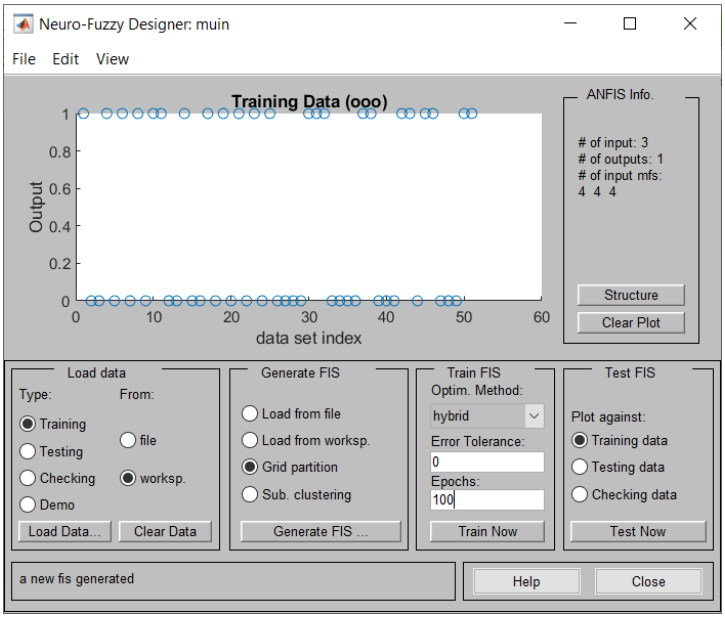


Рисунок 2.9 – Настройки ANFIS в среде MATLAB и распределение обучающих данных

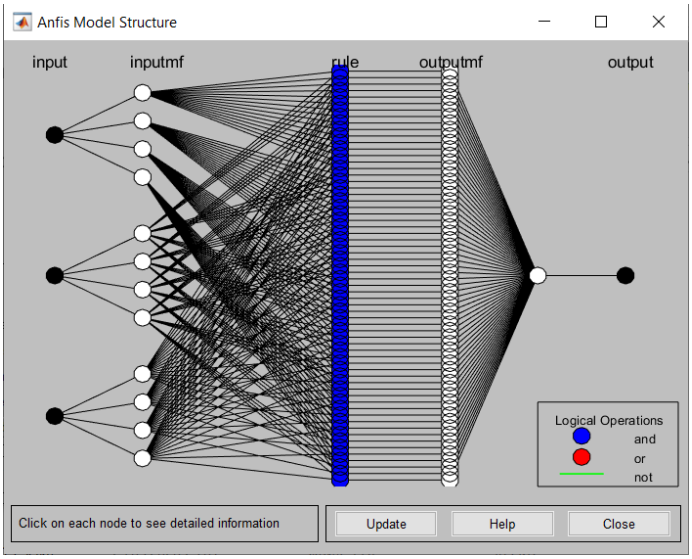


Рисунок 2.10 – Структура сети ANFIS

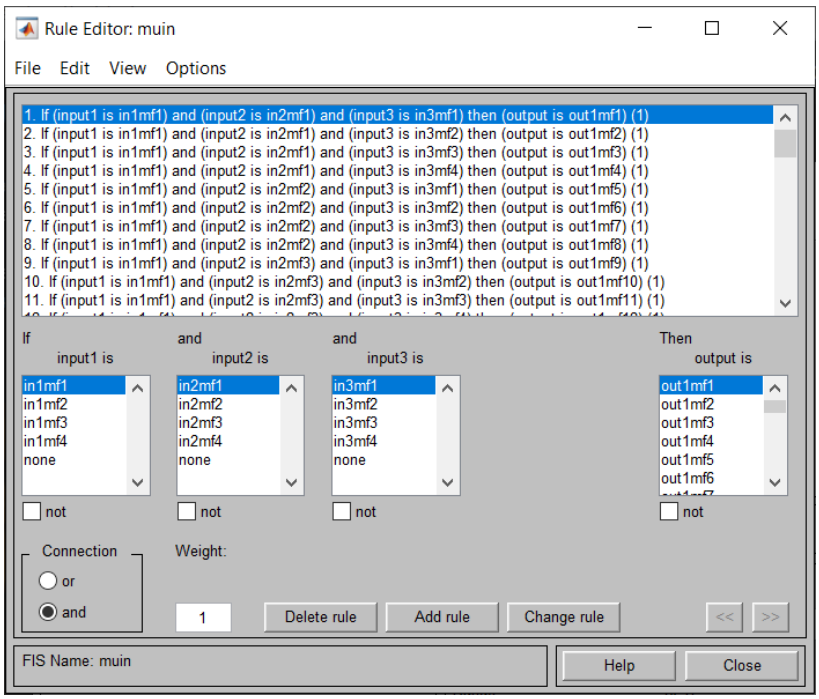


Рисунок 2.11 – Правила сети ANFIS

В результате проведения обучения сети ANFIS с параметрами, указанными на рисунках 2.9-2.11, при сформированном наборе данных ошибка обучения сети достигала значений в диапазоне 0,012-0,023, что является наилучшим результатом работы метода по сравнению с существующими.

Фрагмент текста программы для ЭВМ «Модель угроз и нарушителя» на языке программирования Python 3 для создания и обучения сети представлен ниже:

```
class ANFIS:
    def __init__(self, X, Y, memFunction):
        self.X = np.array(copy.copy(X))
        self.Y = np.array(copy.copy(Y))
        self.Xlen = len(self.X)
        self.memClass = copy.deepcopy(memFunction)
        self.memFuncs = self.memClass.MFList
        self.memFuncsByVariable = [[x for x in range(len(self.memFuncs[z]))] for z in range(len(self.memFuncs))]
        self.rules = np.array(list(itertools.product(*self.memFuncsByVariable)))
        self.consequents = np.empty(self.Y.ndim * len(self.rules) * (self.X.shape[1] + 1))
        self.consequents.fill(0)
        self.errors = np.empty(0)
```

```
        self.memFuncsHomo = all(len(i)==len(self.memFuncsByVariable[0]) for i in self.memFuncsByVariable)
        self.trainingType = 'Not trained yet'

    def LSE(self, A, B, initialGamma = 1000.):
        coeffMat = A
        rhsMat = B
        S = np.eye(coeffMat.shape[1])*initialGamma
        x = np.zeros((coeffMat.shape[1],1)) # need to correct for multi-dim B
        for i in range(len(coeffMat[:,0])):
            a = coeffMat[i,:]
            b = np.array(rhsMat[i])
            S = S - (np.array(np.dot(np.dot(np.dot(S,np.matrix(a).transpose()),np.matrix(a)),S)))/(1+(np.dot(np.dot(S,a),a)))
            x = x + (np.dot(S,np.dot(np.matrix(a).transpose(),(np.matrix(b)-np.dot(np.matrix(a),x)))))
        return x

    def trainHybridJangOffLine(self, epochs=5, tolerance=1e-5, initialGamma=1000, k=0.01):

        self.trainingType = 'trainHybridJangOffLine'
        convergence = False
        epoch = 1

        while (epoch < epochs) and (convergence is not True):

            #4 слой
            [layerFour, wSum, w] = forwardHalfPass(self, self.X)

            #5 слой
            layerFive = np.array(self.LSE(layerFour,self.Y,initialGamma))
            self.consequents = layerFive
            layerFive = np.dot(layerFour,layerFive)

            #ошибка
            error = np.sum((self.Y-layerFive.T)**2)
            print('current error: '+ str(error))
            average_error = np.average(np.absolute(self.Y-layerFive.T))
            self.errors = np.append(self.errors,error)

            if len(self.errors) != 0:
                if self.errors[len(self.errors)-1] < tolerance:
```

```
                convergence = True

            # подтверждение распространения
            if convergence is not True:
                cols = range(len(self.X[0,:]))
                dE_dAlpha = list(backprop(self, colX, cols, wSum, w, layerFive) for colX
in range(self.X.shape[1]))


            if len(self.errors) >= 4:
                if (self.errors[-4] > self.errors[-3] > self.errors[-2] > self.errors[-1]):
                    k = k * 1.1

            if len(self.errors) >= 5:
                if (self.errors[-1] < self.errors[-2]) and (self.errors[-3] < self.errors[-2]) and
(self.errors[-3] < self.errors[-4]) and (self.errors[-5] > self.errors[-4]):
                    k = k * 0.9
```

Фрагмент кода описывает слои нейронной сети, а также ошибку обучения сети. За счет адаптации параметров сети в настоящей работе удалось достичь наименьшей RMSE, в отличие от известных методов и методик определения актуальных УБИ.

2.5 Оценка эффективности методики определения актуальных угроз безопасности информации

В настоящей главе предложена методика определения актуальных УБИ в ТРИС, эффективность которой, по сравнению с известными методиками, достигается следующими показателями: количество определяемых актуальных УБИ в ТРИС увеличилось на 5%, снижение финансовых затрат на закупку СрЗИ от 15 до 30%.

В работе были проведены эксперименты сравнительного анализа работы предложенной методики и известных методов классификации для решения подобных задач. В качестве сравнительной характеристики использовалась точность определения актуальных УБИ в ТРИС (точность классификации). Результаты работы методов оценивались экспертным путем для каждого из экспериментов.

Результаты сравнительного анализа приведены в таблице 2.12.

Таблица 2.12 – Результаты сравнительного анализа

	Наивный Байес	Предложенный метод на основе ANFIS
Точность определения актуальных УБИ в ТРИС (%)	66,8	85,4

На рисунке 2.12 приведен график сравнительного анализа методов для решения поставленной задачи в диссертационном исследовании.

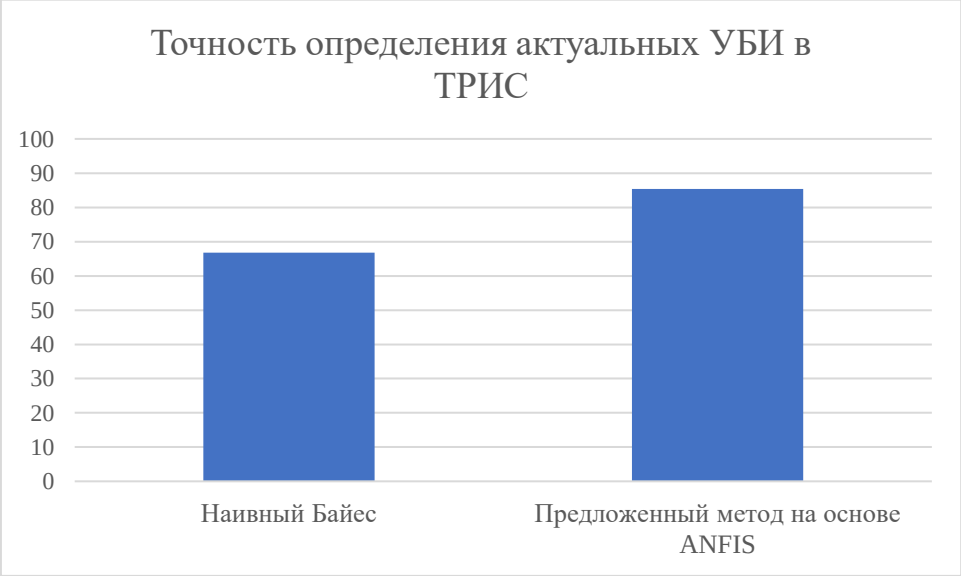


Рисунок 2.12 – График сравнительного анализа методов для решения поставленной задачи

Таким образом, для заданных условий задачи (сформированного набора данных после очистки, преобразования, выбора наиболее полезных и созданных новых более репрезентативных признаков) и определенных в работе показателей определения актуальных УБИ предложенная методика является наилучшей по сравнению с существующими.

Анализ оценки эффективности предложенной методики определения актуальных УБИ представлен в таблице 2.13.

Таблица 2.13 – Анализ оценки эффективности предложенной методики определения актуальных УБИ

Показатель	Известные методики	Предложенная методика
RMSE	0,017 – 0,068	0,012-0,023
Определение количества актуальных УБИ	~ 71	~ 76
Стоимость СЗИ	снижение до 15%	снижение до 30%

Среднеквадратичная ошибка предложенной методики вычисляется по формуле:

$$RMSE = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(y_i - \hat{y}_i)^2},$$

где $y_i, \hat{y}_i$ – наборы данных (обучения, проверки), N – число элементов в обучающей выборке.

Графики сравнения RMSE известных и предложенного метода на заданном интервале представлены на рисунке 2.13.

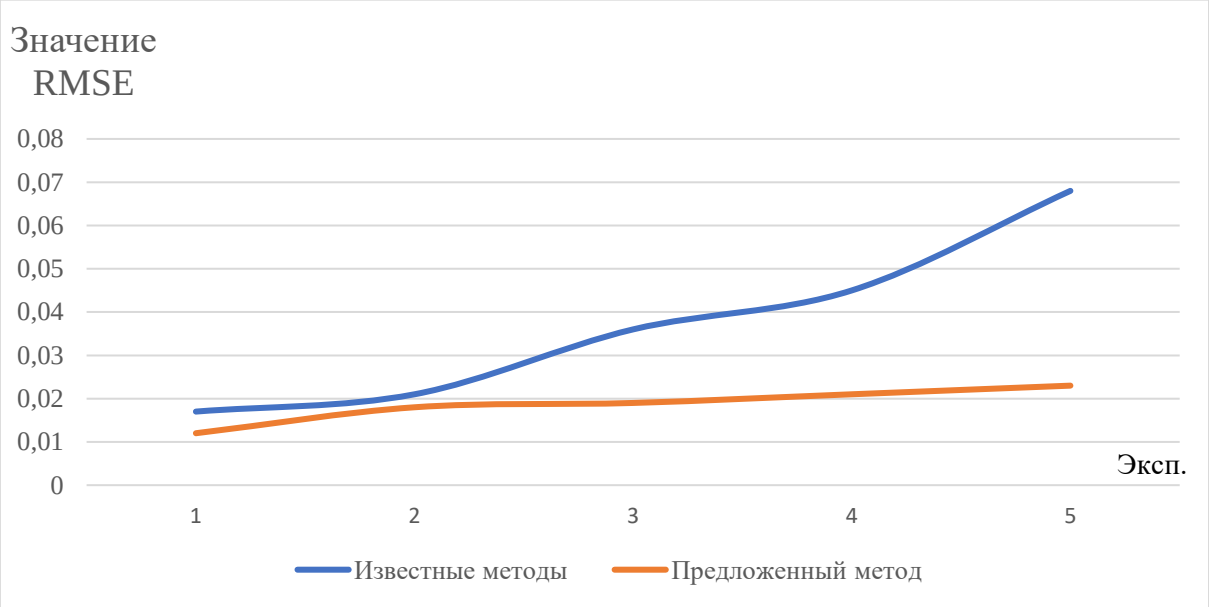


Рисунок 2.13 – График сравнения RMSE известных и предложенного метода на заданном интервале

RMSE достигает значения в диапазоне 0,012-0,023, что является локальным минимумом на заданном интервале и позволяет доказать выполнение поставленной в настоящем диссертационном исследовании задачи.

Выводы

Предложена методика определения актуальных угроз безопасности информации, основанная на теории адаптивных нечетких нейронных продукционных систем и алгоритмах нечеткого вывода, в отличии от известных, использует определенные в настоящей работе необходимые и достаточные показатели, автоматизирована и гипотетически исключает ошибки экспертов. Увеличивает количество определяемых актуальных угроз безопасности информации на 5%, снижает финансовые затраты на закупку средств защиты информации от 15% до 30% по сравнению с известными методиками. Учитывает необходимые и достаточные показатели: уровень мотивации и возможности нарушителей в ТРИС (источник УБИ, актуальный нарушитель), ИТ-инфраструктуру ТРИС (объекты воздействия), перечень существующих СрЗИ в ТРИС, тактики, техники и способы реализации (процедуры) атак. Методика отличается от известных следующим:

- процесс полностью автоматизирован;
- отсутствует необходимость привлечения высококвалифицированных специалистов в области ИБ;
- минимизирует недостатки экспертных оценок;
- предложенная методика позволяет определять перечень актуальных УБИ в ИС различных типов и классов;
- позволяет выполнять требования регуляторов в области обеспечения безопасности информации, учитывает БДУ ФСТЭК России;
- может быть адаптирована для работы с международными базами данных УБИ (MITRE CVE, OSVDB, NVD, Secunia);

- использованием перспективных научных исследований в области адаптивных нечетких нейронных продукционных систем, алгоритмов нечеткого вывода и технологий Data Science при обработке большого объема данных для определения актуальных УБИ.

Материалы главы 2 были представлены в материалах международных и российских научно-технических конференциях и опубликованы в изданиях, включенных в перечень ВАК при Минобрнауки России [58]. Результатом работы, проведенной в главе 2, является разработанное автором программа для ЭВМ «Модель угроз и нарушителя», номер регистрации 2020617876 от 15.07.2020 г., копия свидетельства о регистрации программы для ЭВМ представлена в приложении А.

Глава 3. Метод оценки эффективности систем защиты информации

При оценке эффективности СЗИ необходимо учитывать условия неопределенности и неточные данные по текущему уровню защищенности ИС, которые могут привести к некорректным результатам. Для снижения таких рисков необходимо использовать методы искусственного интеллекта. Методы искусственного интеллекта делятся на две группы: слабые (weak methods) и сильные (strong methods) [89, 94]. Слабые методы используют логику, математическую вероятность, машинное обучение и т.д. и могут быть применены для решения большого ряда проблем и задач. В сильных методах учитываются знания о конкретной проблеме и задаче. При этом сильные методы зависят от слабых, т.к. система, обладающая знаниями, зависит от методологии обработки и преобразования этих знаний. К слабым методам относят нечеткую логику, нейронные сети и генетические алгоритмы. Генетические алгоритмы используются для поиска оптимальных решений. Для оценки эффективности СЗИ целесообразно использовать нечеткую логику и нейронные сети. Различия этих технологий в том, что нейронные сети работают по принципу «черного ящика», который отражает проблему с учетом полной неизвестности, в наличии имеются только наблюдения. В нечеткой логике проблемы и задачи известны в виде экспертных знаний, опыта и понимания процесса, т.е. по принципу «белого ящика». В случае «белого ящика» исследователь составляет базу правил, на основе которой работает система. Для решения задачи проведения оценки эффективности СЗИ, для которой имеются экспертные знания, целесообразно использовать нечеткую логику. Исходя и перечисленных ранее в настоящей работе недостатков технологий, наиболее рационально использовать в качестве основы метода оценки эффективности СЗИ нечеткие нейронные продукционные системы вывода ANFIS, которые являются гибридными сетями, объединяющими принципы нейронных сетей и нечеткой логики.

До момента проведения оценки эффективности СЗИ должны быть выполнены шаги по определению актуальных УБИ и классификации ИС,

формированию требований по ИБ и проектированию СЗИ. На основании методических документов ФСТЭК России и ФСБ России, БДУ ФСТЭК России (MITRE ATT&CK), а также на основании статических моделей угроз безопасности информации типовых ТРИС был сформирован перечень возможных УБИ. Сформирован набор данных и решена задача по очистке и преобразованию большого объема данных для определения перечня актуальных угроз безопасности информации с помощью технологий Data Science. На основании адаптивных нечетких нейронных продукционных систем вывода автором была предложена методика определения актуальных УБИ, описанная в главе 2 настоящего диссертационного исследования.

При формировании требований по защите информации для ИС на основании приказов ФСТЭК России были определены требования по защите информации для различных типов и классов ИС [96]. В качестве примера в данной работе предлагается рассмотреть территориально-распределенную ИС, являющуюся одновременно информационной системой обработки персональных данных 4 уровня защищенности, 3 класса защищенности государственной информационной системой, системой, обрабатывающей конфиденциальную информацию класса 1 Г. Пример был выбран, как наиболее распространенный в существующих ИС [105].

При разработке СЗИ для ТРИС учитывались такие факторы, как использование сертифицированных по требованиям безопасности информации средств защиты в соответствии с п. 11 Приказа № 17 ФСТЭК России от 11.02.2013 г. [17, 101].

3.1. Определение показателей оценки эффективности систем защиты информации

Для оценки эффективности СЗИ необходимо определить необходимые и достаточные показатели [51, 59]. Показатели оценки эффективности СЗИ являются характеристиками для оценки. В настоящей работе для достижения эффективности СЗИ (необходимого уровня защищенности) предлагается использовать некоторый

уровень достижения заданных владельцами ТРИС характеристик, т.е. квантиля заданного уровня гарантии безопасности информации [53, 53]. Таким образом, устанавливается пороговое значение, при котором эффективность СЗИ достигается. Данное пороговое значение суммарно формируется из пороговых значений определенных показателей достижения необходимого уровня защищенности СЗИ, при этом для каждого показателя может быть предусмотрен определенный вес, устанавливаемый также владельцем ТРИС, исходя из НП при наступлении определенных рисков (киберрисков).

В настоящем диссертационном исследовании полагается, что оценка эффективности СЗИ [42, 43] достигается путем создания СЗИ, способной максимально нейтрализовать актуальные УБИ, выполнить требования по защите информации, предъявляемые к ТРИС на основании требований регуляторов в области обеспечения безопасности информации, а также позволяющей максимально сократить финансовые затраты на создание СЗИ [44, 49]. В связи с этим показателями оценки предлагается считать следующими:

- перечень актуальных УБИ;
- перечень требований по ИБ с учетом классификации конкретной ИС;
- перечень СрЗИ, который формируется по результатам разработки СЗИ ТРИС и их стоимость (информация от производителей/вендоров).

Необходимость и достаточность определяется следующим образом:

если из посылки A следует заключение B, то A достаточно для B или B необходимо при A:

$$((A \to B)\,\&\,(B \to A) = (A \sim B)$$

Таким образом, *эффективность СЗИ* достигается при следующих необходимых условиях: нейтрализации УБИ, выполнении требований по ИБ и наименьшей стоимости СрЗИ из предлагаемых вариантов. Нейтрализация УБИ в ТРИС, выполнение требований по ИБ и наименьшая стоимость СрЗИ из предлагаемых вариантов является необходимым и достаточным условием достижения *эффективности СЗИ*.

В таблице 3.1 представлены варианты достижения эффективности СЗИ при необходимых достаточных значениях показателей (квантилей).

Таблица 3.1 – Варианты достижения эффективности СЗИ

Нейтрализация УБИ (X)	**Выполнение требований по ИБ (Y)**	**Наименьшая стоимость СрЗИ (Z)**	**Эффективность СЗИ (S)**
1	1	1	1
1	1	0	0
1	0	1	0
0	1	1	0
1	0	0	0
0	1	0	0
0	0	1	0
0	0	0	0

То есть,

$$X \,\&\, Y \,\&\, Z = S\,,$$

$$\neg X \,\&\, Y \,\&\, Z = \neg S \text{ и т.д.}$$

В таблице 3.1 приведен пример достижения эффективности СЗИ при максимальной гарантии уровня защищенности СЗИ. Как было указано ранее, необходимый уровень гарантии определяется владельцем ТРИС самостоятельно, исходя из НП при возникновении рисков (киберрисков). Это же является обязательным условием работы предложенного метода оценки эффективности СЗИ.

Исходя из определений эффективности СЗИ, МД и НПА регуляторов в области ИБ, а также результатов проведенного в настоящей работе анализа ТРИС, можно сделать вывод о том, что перечисленные показатели являются необходимыми и достаточными для полноценной и наиболее достоверной оценки эффективности СЗИ [60].

3.2. Формирование требований по защите информации

На основании исходных данных, результатов информационного обследования ТРИС, НПА РФ в области обеспечения безопасности информации и требований ФСТЭК России [22, 25] в настоящем диссертационном исследовании предлагается определить требования по ИБ в совокупности. Требования по ИБ, предъявляемые к исследуемой ТРИС представлены таблице 3.2.

Таблица 3.2 – Требования по ИБ для исследуемой ТРИС

№ п/п	Условное обозначение	Функции подсистемы	Соответствие функции для АС	
			ИСПДн (4 УЗ)	ГИС (К3)
Идентификация и аутентификация субъектов доступа и объектов доступа				
1	ИАФ.1	Идентификация и аутентификация пользователей и инициируемых ими процессов	+	+
2	ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	+	+
3	ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации	+	+
4	ИАФ.5	Защита аутентификационной информации при передаче	+	+
5	ИАФ.6	Идентификация и аутентификация внешних пользователей	+	+
Управление доступом субъектов доступа к объектам доступа				
6	УПД.1	Управление учетными записями пользователей, в том числе внешних пользователей	+	+
7	УПД.2	Реализация дискреционного, мандатного, ролевого или иного метода разграничения доступа, типов (чтение, запись, выполнение и т.д.) и правил разграничения доступа	+	+
8	УПД.3	Управление информационными потоками между устройствами, сегментами Системы, а также между подсистемами Системы	+	+
9	УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование Системы	+	+

Таблица 3.2. Продолжение

10	УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	+	+
11	УПД.6	Ограничение неуспешных попыток входа в Систему	+	+
12	УПД.10	Блокирование сеанса доступа в Систему после установленного времени бездействия (неактивности) пользователя или по его запросу	-	+
13	УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации	-	+
14	УПД.13	Реализация защищенного удаленного доступа через внешние информационно-телекоммуникационные сети	+	+
15	УПД.14	Регламентация и контроль использования в Системе технологий беспроводного доступа	+	+
16	УПД.15	Регламентация и контроль использования в Системе мобильных технических средств	+	+
17	УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)	+	+
Ограничение программной среды				
18	ОПС.3	Установка (инсталляция) только разрешенного к использованию ПО и (или) его компонентов	-	+
Защита машинных носителей информации				
19	ЗНИ.1	Учет машинных носителей информации	-	+
20	ЗНИ.2	Управление доступом к машинным носителям информации	-	+
21	ЗНИ.8	Уничтожение (стирание) или обезличивание информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания	-	+
Регистрация событий безопасности				
22	РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения	+	+
23	РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	+	+
24	РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения	+	+

Таблица 3.2. Продолжение

25	РСБ.4	Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации	-	+
26	РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них	-	+
27	РСБ.6	Генерирование временных меток и (или) синхронизация системного времени в Системе	-	+
28	РСБ.7	Защита информации о событиях безопасности	+	+
Антивирусная защита				
29	АВЗ.1	Реализация антивирусной защиты	+	+
30	АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	+	+
Контроль (анализ) защищенности информации				
31	АНЗ.1	Выявление, анализ уязвимостей Системы и оперативное устранение выявленных уязвимостей	-	+
32	АНЗ.2	Контроль установки обновлений ПО, включая ПО от СрЗИ	+	+
33	АНЗ.3	Контроль работоспособности, параметров настройки и правильности функционирования ПО и СрЗИ	-	+
34	АНЗ.4	Контроль состава ТС, ПО и СрЗИ	-	+
35	АНЗ.5	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа и полномочий пользователей	-	+
Обеспечение целостности информационной системы и информации				
36	ОЦЛ.3	Обеспечение возможности восстановления ПО, включая ПО СрЗИ, при возникновении нештатных ситуаций	-	+
Защита среды виртуализации				
37	ЗСВ.1	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре	+	+
38	ЗСВ.2	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре	+	+
39	ЗСВ.3	Регистрация событий безопасности	-	+
40	ЗСВ.9	Реализация и управление антивирусной защитой в виртуальной инфраструктуре	-	+

Таблица 3.2. Продолжение

41	ЗСВ.10	Разбиение виртуальной инфраструктуры на сегменты для обработки информации отдельным пользователем и (или) группой пользователей	-	+
Защита технических средств				
42	ЗТС.2	Организация КЗ, в пределах которой постоянно размещаются стационарные ТС, обрабатывающие информацию, и СрЗИ, а также средства обеспечения функционирования	-	+
43	ЗТС.3	Контроль и управление физическим доступом к ТС, СрЗИ, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены для исключения НСД к ним	+	+
44	ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр	+	+
Защита информационной системы, ее средств, систем связи и передачи данных				
45	ЗИС.3	Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы КЗ	+	+
46	ЗИС.5	Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств	-	+
47	ЗИС.20	Защита беспроводных соединений, применяемых в Системе	-	+
48	ЗИС.30	Защита мобильных ТС, применяемых в Системе	-	+

Представленный в качестве примера в таблице 3.2 перечень требований по защите информации подготовлен на основании НПА ФСТЭК России [22, 25] и сформирован для четвертого уровня защищенности ИСПДн и третьего класса защищенности ГИС. Для предлагаемого в настоящем диссертационном исследовании метода оценки эффективности СЗИ для каждого типа и класса, уровня защищенности, категории значимости ТРИС формируются аналогичные перечни требований по защите информации.

3.3. Подготовка и преобразование набора данных метода

На основании сформированного перечня требований по ИБ, перечня актуальных УБИ, перечня СрЗИ и их стоимости был подготовлен набор данных для метода оценки эффективности СЗИ. С помощью технологий Data Science были выполнены следующие шаги:

- очистка и преобразование подготовленного набора данных;
- выбор наиболее полезных признаков и создание новых более репрезентативных;
- сравнение качества работы нескольких моделей;
- определение параметров в наилучшей модели ANFIS;
- проверка модели на тестовой выборке;
- интерпретация результатов;
- итоговое представление результатов выполнения задачи.

Ввиду того, что в наборе данных присутствует лишняя информация, что увеличивает вычислительные ресурсы и усложняет процесс обработки информации, а значит может повлиять на результаты метода оценки эффективности СЗИ, в качестве первого шага была произведена чистка данных. Фрагмент dataframe до его преобразования представлен на рисунке 3.1.

	Описание уязвимостей	Unnamed: 1	Unnamed: 2	Unnamed: 3	Unnamed: 4	Unnamed: 5	Unnamed: 6	Unnamed: 7	Unnam
0	Общая информация	NaN	NaN	NaN	NaN	NaN	NaN	NaN	
1	Идентификатор	Наименование уязвимости	Описание уязвимости	Вендор ПО	Название ПО	Версия ПО	Тип ПО	Наименование ОС и тип аппаратной платформы	уязви
2	BDU:2014-00001	Уязвимость микропрограммного обеспечения прогр...	Микропрограммное обеспечение модуля 140NOE7711...	Schneider Electric	Микропрограммное обеспечение программируемого ...	4.6 (Микропрограммное обеспечение программируе...	ПО программно-аппаратного средства АСУ ТП	Schneider Electric Микропрограммное обеспечени...	Уязви архите
3	BDU:2014-00002	Уязвимость микропрограммного обеспечения маршр...	Скрипт «/scgi-bin/platform.cgi» микропрограммн...	D-Link Corp.	Микропрограммное обеспечение маршрутизатора D–...	1.02b11 (Микропрограммное обеспечение маршрути...	ПО сетевого программно-аппаратного средства	D-Link Corp. Микропрограммное обеспечение марш...	Уязви
4	BDU:2014-00003	Уязвимость браузера Opera, позволяющая злоумыш...	Браузер Opera содержит уязвимость, связанную с...	Opera Software ASA	Opera	до 11.65 включительно (Opera)	Прикладное ПО информационных систем	Apple Inc. Mac OS X (64-bit, PowerPC);\r\nMicr...	Уязви архите
...	...	...	...	...	...	...	...	...	
26924	BDU:2020-02509	Уязвимость компонента Outside In Filters набор...	Уязвимость компонента Outside In Filters набор...	Oracle Corp.	Outside In Technology	8.5.4 (Outside In Technology)	Прикладное ПО информационных систем	NaN	Уязви архите

Рисунок 3.1 – Фрагмент набора данных dataframe

Фрагмент кода на языке программирования Python 3 для преобразования набора данных представлен ниже:

```
r_vul = pd.read_excel('vullist.xlsx')
r_vul
…
plt.style.use('fivethirtyeight')
df.reset_index().pivot('name','type_of_hacker').plt.hist(df, bins = 100, edgecolor = 'k'),
plt.xlabel('Тип нарушителя'), plt.ylabel('Количество угроз'),
plt.title('Угрозы безопасности информации')
```

Преобразование строковых данных:

```
# Преобразование строковых данных
for col in list(df.columns):
    #Выбор колонок для преобразования
    if ('ft²' in col or 'kBtu' in col or 'Metric Tons CO2e' in col or 'kWh' in
        col or 'therms' in col or 'gal' in col or 'Score' in col):
```

```
# Конвертация
df[col] = df[col].astype(float)
```

В ходе работы были определены ключевые составляющие набора данных:

1. Перечень актуальных УБИ с признаками нейтрализации/не нейтрализации.
2. Перечень требований по ИБ с признаками соответствия: соответствует, в целом соответствует, частично соответствует, не соответствует.
3. Наименование СрЗИ, его версия, версии обновлений (патчей).
4. Стоимость СрЗИ от производителя (спецификации вендоров).

На основании определения ключевых составляющих были отсечены лишние данные из набора.

Признаки, являющиеся изначально числовыми, интерпретированы как *object*. В этой связи такие признаки были конвертированы в числа – тип *float*. Далее производится замена значения «Not Available» в dataframe на «не число» (np.nan — «not a number»). Это позволит изменить тип числовых признаков на *float.* В dataframe нейтрализуем пропуски и выбросы.

Производим предварительный анализ данных (Exploratory Data Analysis — EDA), на его основании определяем закономерности, аномалии или связи между признаками. Необходимо определить признаки и значения признаков, имеющие основное влияние на целевой признак. Оцениваем влияние значений категориальных признаков на целевой — *density plot*.

Для численного оценивания степени влияния признаков в настоящей работе был использован коэффициент корреляции Пирсона. Мера степени и положительности линейных связей между двумя переменными. Значение «+1» означает идеальную пропорциональность между значениями признаков и, соответственно, «-1» аналогично, но с отрицательным коэффициентом.

Рассчитываем величину корреляции:

```
correlations_data = data.corr()[‘score’].sort_values()
```

Выбор признаков – процесс выбора наиболее релевантных признаков. Из dataframe удаляются признаки, чтобы модель уделила больше внимания и ресурсов первостепенным признакам. Таким образом, это чистка набора данных, при которой остаются только наиболее важные для данной задачи данные.

Создание новых признаков – процесс, при котором на основе имеющихся данных конструируются новые признаки. Затем определяются коллинеарные признаки.

После выполнения чистки данных и предварительного анализа оставлены только полезные признаки. Следующим шагом перед началом обучения системы ANFIS является определение показателя, по которому можно понять, есть ли положительный результат от алгоритма или нет.

До расчета вышеописанного критерия, необходимо разделить выборку на обучающую и тестовую:

1. Обучающая выборка – набор данных, который подается на вход системы ANFIS в процессе обучения вместе с ответами, с целью обучить систему ANFIS обнаруживать связь между этими признаками и правильным ответом.
2. Тестовая выборка используется для проверки системы ANFIS. Система не получает целевой признак на вход и, более того, должна предсказать его величину, используя значения остальных признаков. Эти предсказания потом сравниваются с реальными ответами.

Фрагменты dataframe после его преобразования представлен на рисунках 3.2 и 3.3, соответственно.

	Unnamed: 0	mum_UBI	name	description	type_of_hacker	target
0	0	2	The threat of aggregation of data transmitted ...	The threat lies in the possibility of the viol...	enternal	Network traffic
1	1	3	The threat of analyzing cryptographic algorith...	The threat lies in the possibility of identify...	external and enternal	Metadata, system software
2	2	4	BIOS hardware reset password threat	The threat lies in the possibility of resettin...	external and enternal	BIOS / UEFI firmware and hardware
3	3	5	Threat of introducing malicious code into the ...	This threat is caused by the vulnerabilities o...	enternal	BIOS / UEFI firmware and hardware
4	4	6	Threat of automatic distribution of malicious ...	The threat lies in the possibility of introduc...	external	Grid system resource centers
5	5	7	The threat of aggregation of data transmitted ...	The threat lies in the possibility of the viol...	enternal	Network traffic
6	6	8	The threat of analyzing cryptographic algorith...	The threat lies in the possibility of identify...	external and enternal	Metadata, system software
7	7	9	BIOS hardware reset password threat	The threat lies in the possibility of resettin...	external and enternal	BIOS / UEFI firmware and hardware
8	8	10	Threat of introducing malicious code into the ...	This threat is caused by the vulnerabilities o...	enternal	BIOS / UEFI firmware and hardware
9	9	11	Threat of automatic distribution of malicious ...	The threat lies in the possibility of introduc...	external	Grid system resource centers
10	10	12	The threat of aggregation of data transmitted ...	The threat lies in the possibility of the viol...	enternal	Network traffic

Рисунок 3.2 – Фрагмент dataframe

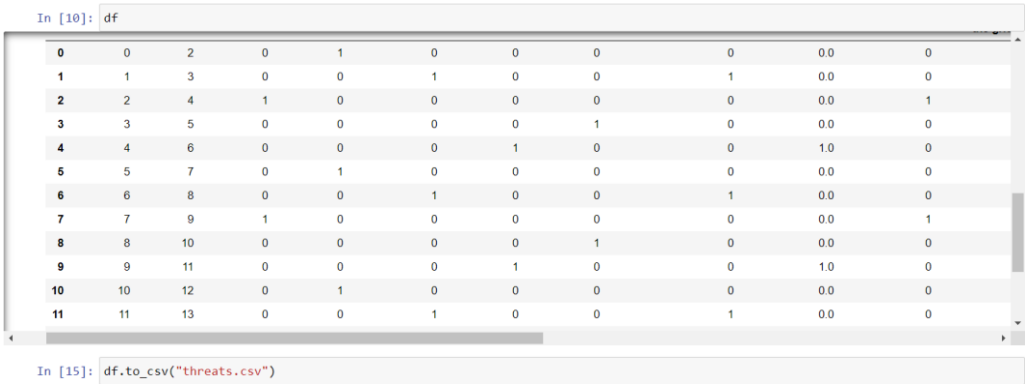


Рисунок 3.3 – Фрагмент dataframe после преобразования

На основании сформированного набора данных, включающего в себя перечни требований по ИБ, актуальных УБИ, перечня СрЗИ и их стоимости, с помощью технологий Data Science произведено его преобразование и форматирование, позволившее собрать только необходимые и достаточные данные для метода оценки эффективности СЗИ, что, в свою очередь, уменьшает сложность вычислительного процесса и количество ошибок экспертных оценок, тем самым повышая эффективность предлагаемого метода.

3.4. Метод оценки эффективности систем защиты информации

В настоящее время существуют большое число гибридных нейро-нечетких моделей, отличающихся архитектурой и возможностями [69]. В данной работе был проведен анализ моделей и на его основе определены основные их свойства, такие как:

- возможность автоматизированного формирования набора решающих правил;
- применение различных обучения модели;
- изменение структуры модели;
- хранение в системе данных в процессе параметрической оптимизации или обучения новым правилам.

Описание области применения нейро-нечетких моделей представлены в таблице 3.3.

Таблица 3.3 – Область применения нейро-нечетких моделей

Модель	**Описание области применения**
ANFIS	– настраиваемые параметры в первом и последнем скрытом слое; – структура базы правил должна быть известна заранее (тип и количество ФП для каждой переменной); – обучение в два этапа: – параметры первого слоя фиксированы, МНК используется для оценки параметров второго слоя, – параметры второго слоя фиксированы, параметры первого слоя оценивается алгоритмом обратного распространения ошибки (RMSE)
NEFCON	– лингвистические нечеткие модели; – возможность индуцирования и оптимизации базы правил
NEFCLASS	– структура базы правил может меняться; – возможность оптимизации базы правил
FALCON	– обучение в два этапа: – обучение без учителя; – параметрическая оптимизация (метод градиентного спуска)
FUN	– алгоритм перестройки связей и изменения параметров ФП носит случайный характер

При проведении анализа моделей были сделаны выводы о применении типов моделей для спектра решаемых задач. Результаты анализа представлены в таблице 3.4.

Таблица 3.4 – Спектр решаемых задач в зависимости типа модели

Модель	Спектр задач
NEFPROX, NEFCLASS	Интеллектуальная обработка и анализ данных
NEFCLASS	Задачи классификации Задачи принятие решений
ANFIS, NEFPROX, FBF	Аппроксимация нелинейных зависимостей
NEFCON, ARIC, GARIC, ANFIS, FUN, AMN	Интеллектуальное управление
NNDFR, ANFIS	Моделирование
FAM, NEFPROX	Прогнозирование

На основании результатов проведенного анализа, представленных в таблице 3.4, можно сделать вывод о том, что для решения задач проведения оценки эффективности СЗИ целесообразно использовать ANFIS.

Для разработки метода были проанализированы ANFIS с алгоритмами нечеткого вывода Такаги-Сугено-Канга, Такаги-Канга, Мамдани и Ванга-Менделя. Выбор связан с тем, что сети ANFIS предназначены, в том числе, для решения задач оценивания. Вывод систем соответствует набору нечетких правил «если-то» (if-then), которые имеют способность к обучению аппроксимированию нелинейных функций.

Алгоритм работы сети ANFIS с алгоритмом нечеткого вывода Такаги-Сугено-Канга (TSK) в предлагаемом методе заключается в реализации нечеткой продукционной модели, основанной на правилах типа [50, 76]:

$$R_i : IFx_i ISA_{i1} AND...ANDx_j ISA_{ij} AND...ANDx_{im} ISA_{im}, THEN \quad (3.1)$$

$$y = c_{i0} + \sum_{j=1}^{m} c_{ij} x_j,\ j = 1,...,n$$

На основании показателей и требований по защите информации, определенных ранее, а также на основании перечня актуальных УБИ и ИТ-инфраструктуры ТРИС была сформирована база правил, фрагмент которой приведен в таблице 3.5.

Таблица 3.5 – Фрагмент базы правил для оценки эффективности СЗИ

№	ЕСЛИ (IF)			ТО (THEN)
	Требование по защите информации (мера)	УБИ	Стоимость СЗИ	
1	ИАФ.3 С	УБИ.001 Н	Min	Эффективность СЗИ достигается
2	ИАФ.4 НС	УБИ.002 НН	Max	Эффективность СЗИ не достигается
…				
N	УПД.2 ЦС	УБИ.003 НН	Min	Эффективность СЗИ не достигается

где терм-множествами лингвистических переменных [68] являются следующие:

С – соответствует, ЦС – в целом соответствует, ЧС – частично соответствует, Н – не соответствует, Н – УБИ нейтрализована, НН – УБИ не нейтрализована, min – цена СЗИ минимальная, max – цена СЗИ максимальная. Оценка эффективности Д – достигается, НД – не достигается. Количественные значения лингвистических переменных приведены в таблице 3.6.

Таблица 3.6 – Количественные значения лингвистических переменных

№ п/п	Обозначение переменной	Наименование	Значение
1	С	Соответствует	1
2	ЦС	в целом соответствует	0,7
3	ЧС	частично соответствует	0,3
4	Н	не соответствует	0
5	УБИ Н	УБИ нейтрализована	1
6	УБИ НН	УБИ не нейтрализована	0
7	Д	Достигается	1
8	НД	не достигается	0

Стоимость СрЗИ [31] определяется на основе данных производителей (вендоров) средств защиты информации (прайс-литы). Пример прайс-листа (по состоянию на 2015 г.[7]) приведен в таблице 3.7.

Таблица 3.7 – Пример прайс-листа СЗИ

№ п/п	Наименование СЗИ	Стоимость (руб.)
1	Аккорд Win 32	12 589
2	Блокхост-сеть К	5 800
3	Dallas Lock 8.0-K	7000
4	Secret Net 7	7425
5	ПАК «Соболь» 3.0	10 350
6	ПАК СЗИ НСД «Аккорд-АПМДЗ»	14 030
7	АПК «БЛОКХОСТ-АМДЗ»	12 600

Таким образом база правил для реализации метода оценки эффективности СЗИ имеет следующий вид:

[7] https://www.securitycode.ru/upload/iblock/5a5/analiz-rinka-szi-nsd-2012-2014.pdf

R_1 : *ИАФ*.1(*С*) *ANDУБИ*.001(*Н*) *ANDCOST*(*MIN*)*THENEVALSZI*(*Д*)

R_2 : *ИАФ*.1(*С*) *ANDУБИ*.001(*Н*) *ANDCOST*(*MAX*)*THENEVALSZI*(*Д*)

R_3 : *ИАФ*.1(*С*) *ANDУБИ*.001(*НН*) *ANDCOST*(*MIN*)*THENEVALSZI*(*НД*)

R_4 : *ИАФ*.1(*С*) *ANDУБИ*.001(*НН*) *ANDCOST*(*MAX*)*THENEVALSZI*(*НД*)

R_5 : *ИАФ*.1(*ЦС*) *ANDУБИ*.001(*Н*) *ANDCOST*(*MIN*)*THENEVALSZI*(*Д*)

R_6 : *ИАФ*.1(*ЦС*) *ANDУБИ*.001(*Н*) *ANDCOST*(*MAX*)*THENEVALSZI*(*Д*)

R_7 : *ИАФ*.1(*ЦС*) *ANDУБИ*.001(*НН*) *ANDCOST*(*MIN*)*THENEVALSZI*(*НД*)

R_8 : *ИАФ*.1(*ЦС*) *ANDУБИ*.001(*НН*) *ANDCOST*(*MAX*)*THENEVALSZI*(*НД*)

R_9 : *ИАФ*.1(*ЧС*) *ANDУБИ*.001(*Н*) *ANDCOST*(*MIN*)*THENEVALSZI*(*Д*)

R_{10} : *ИАФ*.1(*ЧС*) *ANDУБИ*.001(*Н*) *ANDCOST*(*MAX*)*THENEVALSZI*(*НД*)

R_{11} : *ИАФ*.1(*ЧС*) *ANDУБИ*.001(*НН*) *ANDCOST*(*MIN*)*THENEVALSZI*(*НД*)

R_{12} : *ИАФ*.1(*ЧС*) *ANDУБИ*.001(*НН*) *ANDCOST*(*MAX*)*THENEVALSZI*(*НД*)

R_{13} : *ИАФ*.1(*Н*) *ANDУБИ*.001(*Н*) *ANDCOST*(*MIN*)*THENEVALSZI*(*Д*)

R_{14} : *ИАФ*.1(*Н*) *ANDУБИ*.001(*Н*) *ANDCOST*(*MAX*)*THENEVALSZI*(*НД*)

R_{15} : *ИАФ*.1(*Н*) *ANDУБИ*.001(*НН*) *ANDCOST*(*MIN*)*THENEVALSZI*(*НД*)

R_{16} : *ИАФ*.1(*Н*) *ANDУБИ*.001(*НН*) *ANDCOST*(*MAX*)*THENEVALSZI*(*НД*)

...

R_k : *ИАФ*.3(*С*) *ANDУБИ*.001(*Н*) *ANDCOST*(*MIN*)*THENEVALSZI*(*Д*)

...

R_l : *ИАФ*.4(*НС*) *ANDУБИ*.002(*НН*) *ANDCOST*(*MAX*)*THENEVALSZI*(*НД*)

...

R_n : *УПД*.2(*ЦС*) *ANDУБИ*.003(*НН*) *ANDCOST*(*MIN*)*THENEVALSZI*(*НД*)

Правила в общем виде имеют вид:

R_m : "*REG_NUM*"(*С*) *ANDУБИ*."*BDU_NUM*"(*Н*) *ANDCOST*(*MIN*)*THENEVALSZI*(*Д*)

R_{m+1} : "*REG_NUM*"(*С*) *ANDУБИ*."*BDU_NUM*"(*Н*) *ANDCOST*(*MAX*)*THENEVALSZI*(*Д*)

R_{m+2} : "*REG_NUM*"(*С*) *ANDУБИ*."*BDU_NUM*"(*НН*) *ANDCOST*(*MIN*)*THENEVALSZI*(*НД*)

R_{m+3} : "*REG_NUM*"(*С*) *ANDУБИ*."*BDU_NUM*"(*НН*) *ANDCOST*(*MAX*)*THENEVALSZI*(*НД*)

R_{m+4} : "*REG_NUM*"(*ЦС*) *ANDУБИ*."*BDU_NUM*"(*Н*) *ANDCOST*(*MIN*)*THENEVALSZI*(*Д*)

R_{m+5} : "*REG_NUM*"(*ЦС*) *ANDУБИ*."*BDU_NUM*"(*Н*) *ANDCOST*(*MAX*)*THENEVALSZI*(*Д*)

R_{m+6} : "*REG_NUM*"(*ЦС*) *ANDУБИ*."BDU_NUM"(*НН*) *ANDCOST*(*MIN*)*THENEVALSZI*(*НД*)

R_{m+7} : "*REG_NUM*"(*ЦС*) *ANDУБИ*."*BDU_NUM*"(*НН*) *ANDCOST*(*MAX*)*THENEVALSZI*(*НД*)

R_{m+8} : "*REG_NUM*"(*ЧС*) *ANDУБИ*."*BDU_NUM*"(*Н*) *ANDCOST*(*MIN*)*THENEVALSZI*(*Д*)

R_{m+9} : "*REG_NUM*"(*ЧС*) *ANDУБИ*."*BDU_NUM*"(*Н*) *ANDCOST*(*MAX*)*THENEVALSZI*(*НД*)

R_{m+10} : "*REG_NUM*"(*ЧС*) *ANDУБИ*."*BDU_NUM*"(*НН*) *ANDCOST*(*MIN*)*THENEVALSZI*(*НД*)

R_{m+11} : "*REG_NUM*"(*ЧС*) *ANDУБИ*."*BDU_NUM*"(*НН*) *ANDCOST*(*MAX*)*THENEVALSZI*(*НД*)

R_{m+12} : "*REG_NUM*"(*Н*) *ANDУБИ*."*BDU_NUM*"(*Н*) *ANDCOST*(*MIN*)*THENEVALSZI*(*Д*)

R_{m+13} : "*REG_NUM*"(*Н*) *ANDУБИ*."*BDU_NUM*"(*Н*) *ANDCOST*(*MAX*)*THENEVALSZI*(*НД*)

R_{m+14} : "*REG_NUM*"(*Н*) *ANDУБИ*."*BDU_NUM*"(*НН*) *ANDCOST*(*MIN*)*THENEVALSZI*(*НД*)

R_{m+15} : "*REG_NUM*"(*Н*) *ANDУБИ*."*BDU_NUM*"(*НН*) *ANDCOST*(*MAX*)*THENEVALSZI*(*НД*)

где, «REG_NUM» - идентификатор меры из требований по ИБ (требований приказов ФСТЭК России), «BDU_NUM» - идентификатор УБИ (БДУ ФСТЭК России), «COST» - стоимость СрЗИ [31].

Правила R_3, R_7, R_{11} совпадают по результатам выводов о не достижении необходимой эффективности СЗИ, т.е. при одинаковых значениях показателей «BDU_NUM» и «COST», значения терм-множеств «С», «ЦС» и «ЧС» показателя «REG_NUM» не имеют разницы. Связано это с проведенными экспертными оценками при формировании базы правил, а именно – для значений показателей «BDU_NUM» и «COST» значение оценки соответствия требованию по ИБ при условии «ЧС» и выше является равнозначными.

В работе был проведен анализ большого объема данных, таких как решения по ИТ-инфраструктуре, статических моделей УБИ, систем защиты информации ТРИС. С помощью технологий Data Science был сформирован набор данных для реализации метода. Фрагмент набора данных для реализации метода приведен в таблице 3.8.

Таблица 3.8 – Фрагмент набора данных для реализации метода

Условное обозначение	**Наименование меры**	**СрЗИ**	**УБИ**	**Признак соответствия**	**Значение**	**Стоимость**	**Эффективность СЗИ**
ИАФ.1	Идентификация и аутентификация пользователей и инициируемых ими процессов	Secret Net LSP ВВ ОС	001 Н 003 Н	С ЦС ЧС Н	1 0,7 0,3 0	7500 30000	Д НД
ИАФ.2	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных	Secret Net LSP ВВ ОС	123 НН 113 НН	С ЦС ЧС Н	1 0,7 0,3 0	7500 30000	Д НД

В таблице 3.8 выделены цветом и подчеркнуты значения, при которых оценка эффективности СЗИ достигается.

Система ANFIS в предлагаемом методе базируется на следующих положениях:

– входные переменные являются четкими;

– ФП определены функцией Гаусса:

$$\mu_{A_{ij}}(x_j) = \exp(-\frac{1}{2}(\frac{x_j - a_{ij}}{b_{ij}})^2)$$

где x_j – входные сети a_{ij}, b_{ij} - настраиваемые параметры ФП.

– нечеткая импликация Ларсена – нечеткое произведение;

– Т-норма – нечеткое произведение;

– композиция не производится;

– метод дефаззификации – метод центроида.

Функциональная зависимость после дефаззификации для получения выходной переменно принимает следующий вид [87]:

$$y' = \frac{\Sigma_i^n((c_{i0} + \Sigma_{j=1}^m c_{ij} x_j)\Pi_j^m \mu_{A_{ij}}(x_j'))}{\Sigma_{i=1}^n \Pi_j^m \mu_{A_{ij}}(x_j')} = \frac{\Sigma_i^n((c_{i0} + \Sigma_{j=1}^m c_{ij} x_j))\Pi_j^m \exp\left[-(\frac{x_j' - a_{ij}}{b_{ij}})^2\right]}{\Sigma_{i=1}^n \Pi_j^m \exp\left[-(\frac{x_j' - a_{ij}}{b_{ij}})^2\right]} \quad (3.2)$$

Выражение 3.2 лежит в основе сети ANFIS с применением алгоритма TSK, которая включает в себя пять слоев.

ANFIS TSK содержит два параметрических слоя (слой 1 и 3). Настраиваемыми в процессе обучения сети ANFIS параметрами являются:

– ФП фаззификатора;

– параметры c_{i0} и c_{ij} линейных функций $(c_{j0} + \Sigma_{j=1}^m c_{ij} x_j')$ из заключений базы правил.

Общее число настраиваемых параметров равно $n(3m+1)$.

На следующем шаге в предлагаемом методе рассчитываются параметры c_{i0} и c_{ij} с линейных функций при условии фиксированных значений параметров a_{ij}, b_{ij}. Параметры c_{i0} и c_{ij} находятся путем решения системы линейных уравнений.

Выходную переменную из выражения (3.2) представляем в следующем виде:

$$y^{'} = \sum_{i=1}^{n} w_i^{'}(c_{i0} + \sum \sum_{j=1}^{m} c_{ij} x_j),$$

где

$$w_i^{'} = \frac{\Pi_{j=1}^{m} \mu_{A_{ij}}(x_j^{'})}{\sum_{i=1}^{n} \Pi_j^m \mu_{A_{ij}}(x_j^{'})} = \frac{\Pi_j^m \exp\left[-(\frac{x_j^{'} - a_{ij}}{b_{ij}})^2\right]}{\sum_{i=1}^{n} \Pi_j^m \exp\left[-(\frac{x_j^{'} - a_{ij}}{b_{ij}})^2\right]} = const$$

При K обучающих примерах $x_1^{(k)}, x_2^{(k)}, ..., x_m^{(k)}, y^{(k)}$, где $k=1,...,K$ и замене значений выходных переменных $y^{'(k)}$ значениями эталонных переменных $y^{(k)}$, получим систему из K линейных уравнений вида:

$$\begin{bmatrix} w_1^{'(1)} & w_1^{'(1)}x_1^{(1)} & \dots & w_1^{'(1)}x_m^{(1)} & \dots & w_n^{'(1)} & w_n^{'(1)}x_1^{(1)} & \dots & w_n^{'(1)}x_m^{(1)} \\ w_1^{'(2)} & w_1^{'(2)}x_1^{(2)} & \dots & w_1^{'(2)}x_m^{(2)} & \dots & w_n^{'(2)} & w_n^{'(2)}x_1^{(2)} & \dots & w_n^{'(2)}x_m^{(2)} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ w_1^{'(k)} & w_1^{'(k)}x_1^{(k)} & \dots & w_1^{'(k)}x_m^{(k)} & \dots & w_n^{'(k)} & w_n^{'(k)}x_1^{(k)} & \dots & w_n^{'(k)}x_m^{(k)} \end{bmatrix} x \begin{bmatrix} c_{10} \\ \dots \\ c_{1m} \\ \dots \\ c_{n0} \\ \dots \\ c_{nm} \end{bmatrix} = \begin{bmatrix} y^{(1)} \\ y^{(2)} \\ \dots \\ y^{(k)} \end{bmatrix} \quad (3.3)$$

где $w_i^{'(k)}$ агрегированная степень истинности предпосылок по i -му правилу при предъявлении k -го входного вектора $(x_1^{(k)}, x_2^{(k)}, ..., x_m^{(k)})$.

Соответственно, 3.3 в сокращенном виде:

$$W \times c = y$$

Размерность матрицы W равна $K \times (m+1)n$, при этом, как правило, количество строк k значительно больше количества столбцов: $K \times (m+1)n$. Решение этой системы уравнений можно провести за один шаг при помощи псевдоинверсии матрицы W:

$$c = W^{+} y = (W^T \bullet W)^{-1} W^T y$$

После определения линейных параметров ij фиксируем и рассчитываем фактические выходные сигналы сети для всех примеров, для чего используем линейную зависимость:

$$y' = \begin{bmatrix} y^{(1)} \\ y^{(2)} \\ \dots \\ y^{(k)} \end{bmatrix} = W \bullet c$$

определяем вектор ошибок:

$$e = y' - y$$

Среднеквадратичная ошибка (RMSE) вычисляется следующим образом:

$$RMSE = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(y_i - \hat{y}_i)^2},$$

где $y_i, \hat{y}_i$ - наборы данных (обучения, проверки), N – число элементов в обучающей выборке.

Производим уточнение параметры:

$$a_{ij}^{(k)}(t+1) = a_{ij}^{(k)}(t) - C\frac{dE^{(k)}(t)}{da_{ij}^{(k)}}$$

$$b_{ij}^{(k)}(t+1) = b_{ij}^{(k)}(t) - C\frac{dE^{(k)}(t)}{db_{ij}^{(k)}}$$

По результатам уточнения нелинейных параметров процесс адаптации нейрона запускается до тех пор, пока не достигнет повторения результатов. Таким образом, алгоритм является гибридным. Особенность заключается в разделении этапов обучения. Такой алгоритм является наиболее эффективным, что и позволило достичь наилучшего результата в настоящем диссертационном исследовании.

Структура нечеткой нейронной продукционной сети ANFIS с применением алгоритма TSK представлена на рисунке 3.4.

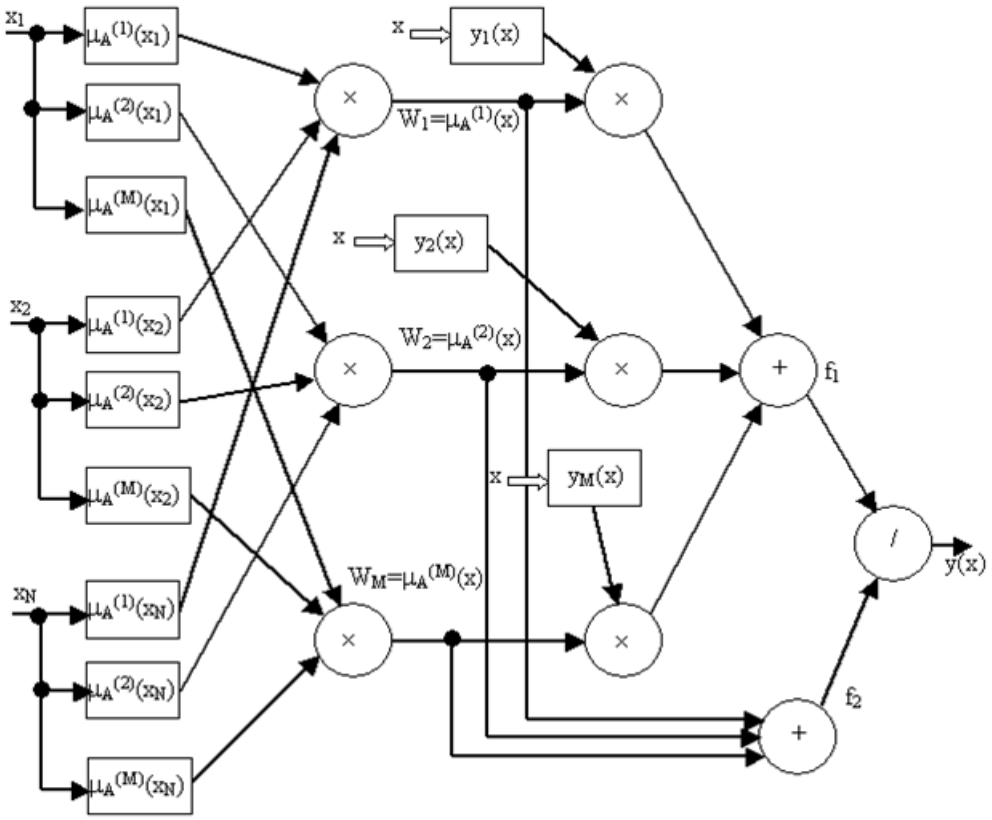


Рисунок 3.4 – Сеть ANFIS с применением алгоритма TSK

Реализация предложенного метода для наглядности и сравнения выполнена в среде MATLAB, а также разработана программа для ЭВМ «Оценка системы защиты информации» на языке программирования Python 3. Настройки модели ANFIS и структура сети с наилучшими параметрами, дающими минимальную среднеквадратичную ошибку RMSE в диапазоне 0,012-0,017, представлены на рисунках 3.5 и 3.6, соответственно.

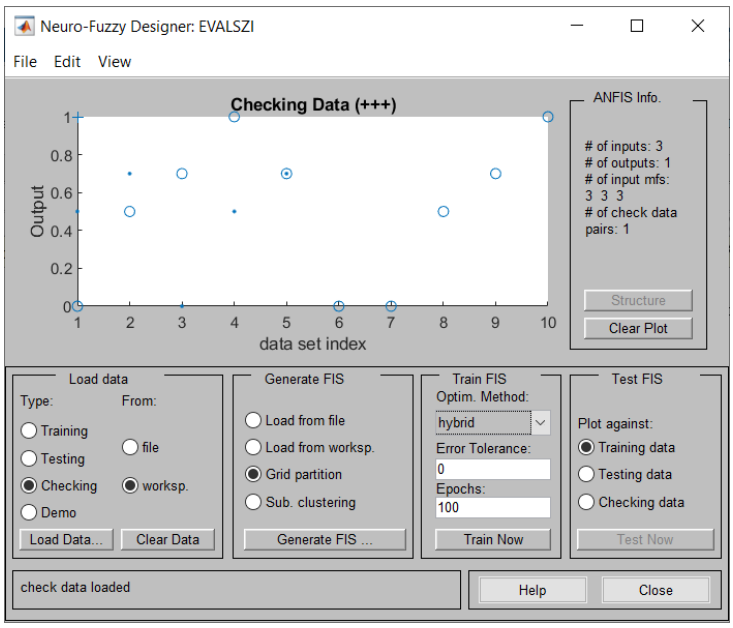


Рисунок 3.5 – Настройки сети ANFIS

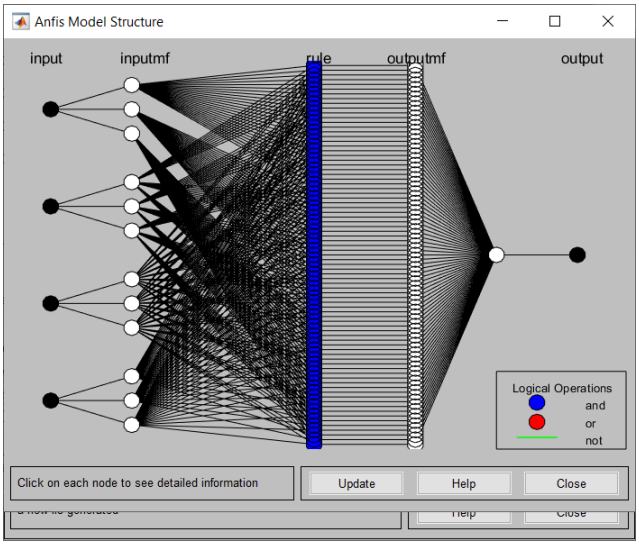
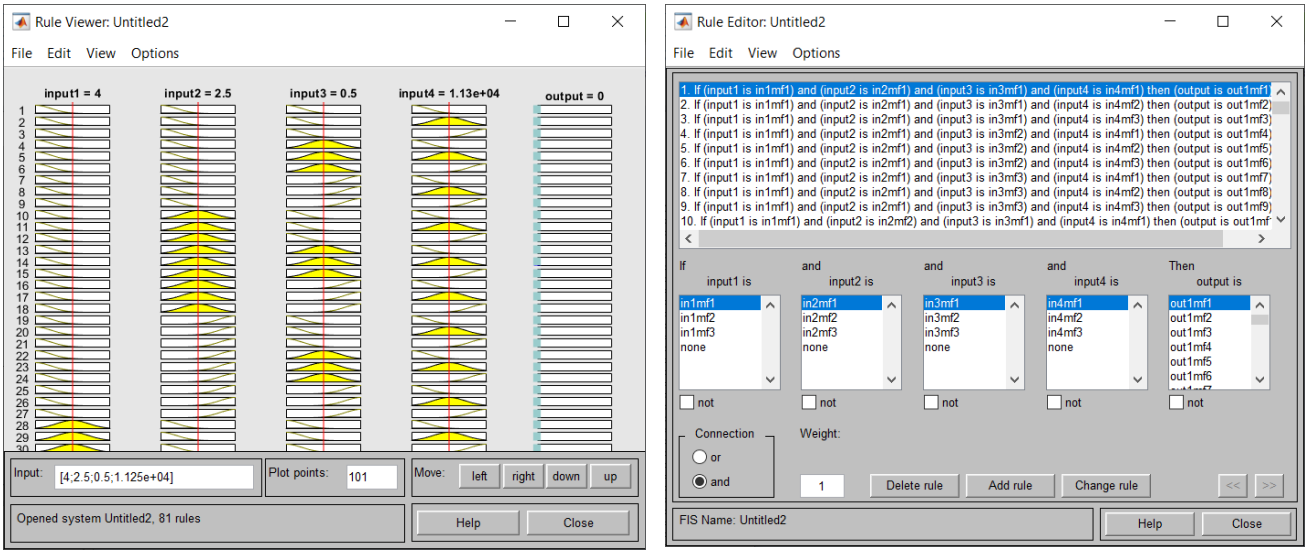


Рисунок 3.6 – Структура сети ANFIS

База правил для работы сети ANFIS представлены на рисунке 3.7 а) и б).



а) б)

Рисунок 3.7 – Правила сети ANFIS

Для системы ANFIS были исследованы пять моделей с различными параметрами, такими как: количество эпох работы сети, алгоритмы ошибки, количество нейронов для следующих алгоритмов работы: Такаги-Сугено-Канга, Такаги-Канга, Мамдани и Ванга-Менделя. Установлено, что наилучшим алгоритмом для решения задач оценки является алгоритм нечеткого вывода Такаги-Сугено-Канга. Связано это с тем, что процесс дефаззификации для ANFIS с таким алгоритмом более эффективен по сравнению с алгоритмами нечеткого вывода Такаги-Канга, Мамдани и Ванга-Менделя, поскольку использует взвешенную сумму нескольких точек данных, а не вычисляет центроид двумерной области, и ориентирован на точность.

Результаты экспериментов представлены в таблице 3.9.

Таблица 3.9 – Результаты экспериментов работы ANFIS

Исследуемый тип нечеткой сети ANFIS	**Эксперимент**	**RMSE**	**RMSE после обучения**	**Среднее значение RMSE**
ANFIS с алгоритмом Такаги-Сугено-Канга	tse1	0,014	0,007	0,014
	tse2	0,012	0,005	
	tse3	0,017	0,011	
	tse4	0,015	0,009	
	tse5	0,014	0,008	

ANFIS с алгоритмом Такаги-Сугено-Канга с параметрами, представленными на рисунках 3.5 и 3.6, и экспериментом tse2 является наилучшей для проведения оценки эффективности СЗИ.

Ниже представлен фрагмент кода программы для ЭВМ «Оценка системы защиты информации» (Приложение Б) на языке программирования Python 3, реализующего предложенный метод оценки эффективности СЗИ:

```
class Ui_MainWindow(object):
    def setupUi(self, MainWindow):
        if MainWindow.objectName():
            MainWindow.setObjectName(u”MainWindow”)
        MainWindow.resize(297, 402)
        self.action = Qaction(MainWindow)
        self.action.setObjectName(u”action”)
        self.action_2 = Qaction(MainWindow)
        self.action_2.setObjectName(u”action_2”)
        self.action_3 = Qaction(MainWindow)
        self.action_3.setObjectName(u”action_3”)
        self.action_4 = Qaction(MainWindow)
        self.action_4.setObjectName(u”action_4”)
        self.centralwidget = Qwidget(MainWindow)
        self.centralwidget.setObjectName(u”centralwidget”)
        self.verticalLayoutWidget = Qwidget(self.centralwidget)
        self.verticalLayoutWidget.setObjectName(u”verticalLayoutWidget”)
        self.verticalLayoutWidget.setGeometry(Qrect(10, 20, 141, 330))
        self.verticalLayout = QVBoxLayout(self.verticalLayoutWidget)
        self.verticalLayout.setObjectName(u”verticalLayout”)
        self.verticalLayout.setContentsMargins(0, 0, 0, 0)
        self.label = Qlabel(self.verticalLayoutWidget)
        self.label.setObjectName(u”label”)
```

```
self.verticalLayout.addWidget(self.label)

self.checkBox = QcheckBox(self.verticalLayoutWidget)
self.checkBox.setObjectName(u"133olumn133x")

self.verticalLayout.addWidget(self.checkBox)

self.checkBox_2 = QcheckBox(self.verticalLayoutWidget)
self.checkBox_2.setObjectName(u"133olumn133x_2")

self.verticalLayout.addWidget(self.checkBox_2)

self.checkBox_3 = QcheckBox(self.verticalLayoutWidget)
self.checkBox_3.setObjectName(u"133olumn133x_3")

self.verticalLayout.addWidget(self.checkBox_3)

self.checkBox_4 = QcheckBox(self.verticalLayoutWidget)
self.checkBox_4.setObjectName(u"133olumn133x_4")

self.verticalLayout.addWidget(self.checkBox_4)

self.label_2 = Qlabel(self.verticalLayoutWidget)
self.label_2.setObjectName(u"label_2")

self.verticalLayout.addWidget(self.label_2)

self.radioButton = QradioButton(self.verticalLayoutWidget)
self.radioButton.setObjectName(u"radioButton")
```

```
self.verticalLayout.addWidget(self.radioButton)

self.radioButton_2 = QradioButton(self.verticalLayoutWidget)
self.radioButton_2.setObjectName(u"radioButton_2")

self.verticalLayout.addWidget(self.radioButton_2)

self.label_3 = Qlabel(self.verticalLayoutWidget)
self.label_3.setObjectName(u"label_3")

self.verticalLayout.addWidget(self.label_3)

self.radioButton_4 = QradioButton(self.verticalLayoutWidget)
self.radioButton_4.setObjectName(u"radioButton_4")

self.verticalLayout.addWidget(self.radioButton_4)

self.radioButton_3 = QradioButton(self.verticalLayoutWidget)
self.radioButton_3.setObjectName(u"radioButton_3")

self.verticalLayout.addWidget(self.radioButton_3)

self.radioButton_5 = QradioButton(self.verticalLayoutWidget)
self.radioButton_5.setObjectName(u"radioButton_5")

self.verticalLayout.addWidget(self.radioButton_5)

self.pushButton = QpushButton(self.verticalLayoutWidget)
self.pushButton.setObjectName(u"pushButton")
```

```
self.verticalLayout.addWidget(self.pushButton)

self.listView = QlistView(self.centralwidget)
self.listView.setObjectName(u”listView”)
self.listView.setGeometry(Qrect(160, 40, 81, 61))
self.label_4 = Qlabel(self.centralwidget)
self.label_4.setObjectName(u”label_4”)
self.label_4.setGeometry(Qrect(160, 20, 61, 16))
MainWindow.setCentralWidget(self.centralwidget)
self.menubar = QmenuBar(MainWindow)
self.menubar.setObjectName(u”menubar”)
self.menubar.setGeometry(Qrect(0, 0, 297, 26))
self.menuFile = Qmenu(self.menubar)
self.menuFile.setObjectName(u”menuFile”)
self.menu = Qmenu(self.menubar)
self.menu.setObjectName(u”menu”)
MainWindow.setMenuBar(self.menubar)
self.statusbar = QstatusBar(MainWindow)
self.statusbar.setObjectName(u”statusbar”)
MainWindow.setStatusBar(self.statusbar)

self.menubar.addAction(self.menuFile.menuAction())
self.menubar.addAction(self.menu.menuAction())
self.menuFile.addAction(self.action)
self.menuFile.addAction(self.action_2)
self.menuFile.addAction(self.action_3)
self.menuFile.addAction(self.action_4)

self.retranslateUi(MainWindow)
```

```
        QmetaObject.connectSlotsByName(MainWindow)
    # setupUi
```

Описание пользовательского интерфейса программы (возможности действий пользователя):

```
    def retranslateUi(self, MainWindow):
        MainWindow.setWindowTitle(QcoreApplication.translate("MainWindow",
u"MainWindow", None))
        self.action.setText(QcoreApplication.translate("MainWindow",
u"\u041a\u043b\u0430\u0441\u0441\u0438\u0444\u0438\u043a\u0430\u0446\u0438\u
044f", None))
        self.action_2.setText(QcoreApplication.translate("MainWindow",
u"\u041d\u0430\u0440\u0443\u0448\u0438\u0442\u0435\u043b\u044c", None))
        self.action_3.setText(QcoreApplication.translate("MainWindow",
u"\u0421\u0432\u0435\u0434\u0435\u043d\u0438\u044f \u043e
\u0441\u0438\u0441\u0442\u0435\u043c\u0435", None))
        self.action_4.setText(QcoreApplication.translate("MainWindow",
u"\u0412\u044b\u0445\u043e\u0434", None))
        self.label.setText(QcoreApplication.translate("MainWindow",
u"\u0422\u0438\u043f \u041f\u0414\u043d", None))
        self.checkBox.setText(QcoreApplication.translate("MainWindow",
u"\u041e\u0431\u0449\u0435\u0434\u043e\u0441\u0442\u0443\u043f\u043d\u044b\u0
435", None))
        self.checkBox_2.setText(QcoreApplication.translate("MainWindow",
u"\u0421\u043f\u0435\u0446\u0438\u0430\u043b\u044c\u043d\u044b\u0435", None))
        self.checkBox_3.setText(QcoreApplication.translate("MainWindow",
u"\u0411\u0438\u043e\u043c\u0435\u0442\u0440\u0438\u0447\u0435\u0441\u043a\u0
438\u0435", None))
```

```
            self.checkBox_4.setText(QcoreApplication.translate("MainWindow",
u"\u0418\u043d\u044b\u0435", None))
            self.label_2.setText(QcoreApplication.translate("MainWindow",
u"\u043a\u043e\u043b\u0438\u0447\u0435\u0441\u0442\u0432\u043e
\u041f\u0414\u043d", None))
            self.radioButton.setText(QcoreApplication.translate("MainWindow",
u"\u041c\u0435\u043d\u0435\u0435 100 000", None))
            self.radioButton_2.setText(QcoreApplication.translate("MainWindow",
u"\u0411\u043e\u043b\u0435\u0435 10 000", None))
            self.label_3.setText(QcoreApplication.translate("MainWindow",
u"\u0422\u0438\u043f \u0443\u0440\u043e\u0437 ", None))
            self.radioButton_4.setText(QcoreApplication.translate("MainWindow",  u"1
\u0442\u0438\u043f \u0446\u0433\u0440\u043e\u0437", None))
            self.radioButton_3.setText(QcoreApplication.translate("MainWindow",  u"2
\u0442\u0438\u043f \u0443\u0433\u0440\u043e\u0437", None))
            self.radioButton_5.setText(QcoreApplication.translate("MainWindow",  u"3
\u0442\u0438\u043f \u0443\u0433\u0440\u043e\u0437", None))
            self.pushButton.setText(QcoreApplication.translate("MainWindow",
u"\u041a\u043b\u0430\u0441\u0441\u0438\u0444\u0438\u0446\u0438\u0440\u043e\u
0432\u0430\u0442\u044c", None))
            self.label_4.setText(QcoreApplication.translate("MainWindow",
u"\u0423\u0417 \u0418\u0421\u041f\u0414\u041d", None))
            self.menuFile.setTitle(QcoreApplication.translate("MainWindow",
u"\u0424\u0430\u0439\u043b", None))
            self.menu.setTitle(QcoreApplication.translate("MainWindow",
u"\u0421\u043f\u0440\u0430\u0432\u043a\u0430", None))

        class mainForm(Qwindow, Ui_MainWindow):
          def __init__(self, parent=None, *args, **kwargs):
            Qwindow.__init__(self)
```

```
        self.setupUi(self)
```

Описание адаптированной системы ANFIS с алгоритмом нечеткого вывода TSK:

```
class ANFIS:


    def __init__(self, X, Y, memFunction):
        self.X = np.array(copy.copy(X))
        self.Y = np.array(copy.copy(Y))
        self.Xlen = len(self.X)
        self.memClass = copy.deepcopy(memFunction)
        self.memFuncs = self.memClass.MFList
        self.memFuncsByVariable = [[x for x in range(len(self.memFuncs[z]))] for z
in range(len(self.memFuncs))]
        self.rules = np.array(list(itertools.product(*self.memFuncsByVariable)))
        self.consequents = np.empty(self.Y.ndim * len(self.rules) * (self.X.shape[1]
+ 1))
        self.consequents.fill(0)
        self.errors = np.empty(0)
        self.memFuncsHomo = all(len(i)==len(self.memFuncsByVariable[0]) for i in
self.memFuncsByVariable)
        self.trainingType = 'Not trained yet'


    def LSE(self, A, B, initialGamma = 1000.):
        coeffMat = A
        rhsMat = B
        S = np.eye(coeffMat.shape[1])*initialGamma
        x = np.zeros((coeffMat.shape[1],1)) # need to correct for multi-dim B
        for i in range(len(coeffMat[:,0])):
            a = coeffMat[i,:]
            b = np.array(rhsMat[i])
```

```
S = S – (np.array(np.dot(np.dot(np.dot(S,np.matrix(a).transpose()),np.matrix(a)),S)))/(1+(np.dot(np.dot(S,a),a)))
x = x + (np.dot(S,np.dot(np.matrix(a).transpose(),(np.matrix(b)-np.dot(np.matrix(a),x)))))
return x
```

Процесс обучения системы ANFIS предлагаемого метода:

```
def trainHybridJangOffLine(self, epochs=5, tolerance=1e-5, initialGamma=1000, k=0.01):

    self.trainingType = 'trainHybridJangOffLine'
    convergence = False
    epoch = 1

    while (epoch < epochs) and (convergence is not True):
      #слой 4
      [layerFour, wSum, w] = forwardHalfPass(self, self.X)

      #слой 5
      layerFive = np.array(self.LSE(layerFour,self.Y,initialGamma))
      self.consequents = layerFive
      layerFive = np.dot(layerFour,layerFive)
```

Описание RMSE обучения системы ANFIS:

```
      #ошибка
      error = np.sum((self.Y-layerFive.T)**2)
      print('current error: '+ str(error))
      average_error = np.average(np.absolute(self.Y-layerFive.T))
      self.errors = np.append(self.errors,error)
```

```
if len(self.errors) != 0:
    if self.errors[len(self.errors)-1] < tolerance:
        convergence = True
```

Описание обратного распространения ошибки работы системы ANFIS предлагаемого метода:

```
# обратное распространение
if convergence is not True:
    cols = range(len(self.X[0,:]))
    dE_dAlpha = list(backprop(self, colX, cols, wSum, w, layerFive) for colX in range(self.X.shape[1]))


if len(self.errors) >= 4:
    if (self.errors[-4] > self.errors[-3] > self.errors[-2] > self.errors[-1]):
        k = k * 1.1

if len(self.errors) >= 5:
    if (self.errors[-1] < self.errors[-2]) and (self.errors[-3] < self.errors[-2]) and (self.errors[-3] < self.errors[-4]) and (self.errors[-5] > self.errors[-4]):
        k = k * 0.9
```

Описание обработки переменных с различным числом MF:

```
t = []
for x in range(len(dE_dAlpha)):
    for y in range(len(dE_dAlpha[x])):
        for z in range(len(dE_dAlpha[x][y])):
            t.append(dE_dAlpha[x][y][z])

eta = k / np.abs(np.sum(t))
```

```
            if(np.isinf(eta)):
               eta = k
```

Описание кода обработки переменных с различным числом MF:

```
            dAlpha = copy.deepcopy(dE_dAlpha)
            if not(self.memFuncsHomo):
               for x in range(len(dE_dAlpha)):
                  for y in range(len(dE_dAlpha[x])):
                     for z in range(len(dE_dAlpha[x][y])):
                        dAlpha[x][y][z] = -eta * dE_dAlpha[x][y][z]
            else:
               dAlpha = -eta * np.array(dE_dAlpha)


            for varsWithMemFuncs in range(len(self.memFuncs)):
               for MFs in range(len(self.memFuncsByVariable[varsWithMemFuncs])):
                  paramList = sorted(self.memFuncs[varsWithMemFuncs][MFs][1])
                  for param in range(len(paramList)):
                     self.memFuncs[varsWithMemFuncs][MFs][1][paramList[param]] = self.memFuncs[varsWithMemFuncs][MFs][1][paramList[param]] + dAlpha[varsWithMemFuncs][MFs][param]
            epoch = epoch + 1


            self.fittedValues = predict(self,self.X)
            self.residuals = self.Y – self.fittedValues[:,0]

            return self.fittedValues
```

Описание кода сообщений работы программы для ЭВМ:

```
    def plotErrors(self):
        if self.trainingType == 'Сеть еще не обучена':
            print(self.trainingType)
        else:
            import matplotlib.pyplot as plt
            plt.plot(range(len(self.errors)),self.errors,’ro’, label=’errors’)
            plt.ylabel(‘error’)
            plt.xlabel(‘epoch’)
            plt.show()
```

Построение графиков:

```
    def plotMF(self, x, inputVar):
        import matplotlib.pyplot as plt
        from skfuzzy import gaussmf, gbellmf, sigmf

        for mf in range(len(self.memFuncs[inputVar])):
            if self.memFuncs[inputVar][mf][0] == ‘gaussmf’:
                y = gaussmf(x,**self.memClass.MFList[inputVar][mf][1])
            elif self.memFuncs[inputVar][mf][0] == ‘gbellmf’:
                y = gbellmf(x,**self.memClass.MFList[inputVar][mf][1])
            elif self.memFuncs[inputVar][mf][0] == ‘sigmf’:
                y = sigmf(x,**self.memClass.MFList[inputVar][mf][1])

            plt.plot(x,y,’r’)

        plt.show()

    def plotResults(self):
        if self.trainingType == 'Сеть еще не обучена':
            print(self.trainingType)
```

```
            else:
                import matplotlib.pyplot as plt
                plt.plot(range(len(self.fittedValues)),self.fittedValues,'r', label='trained')
                plt.plot(range(len(self.Y)),self.Y,'b', label='original')
                plt.legend(loc='upper left')
                plt.show()

        def forwardHalfPass(ANFISObj, Xs):
            layerFour = np.empty(0,)
            wSum = []
        Описание слоев нейронной сети:
            for pattern in range(len(Xs[:,0])):
                #слой 1
                layerOne = ANFISObj.memClass.evaluateMF(Xs[pattern,:])

                #слой 2
                miAlloc = [[layerOne[x][ANFISObj.rules[row][x]] for x in
range(len(ANFISObj.rules[0]))] for row in range(len(ANFISObj.rules))]
                layerTwo = np.array([np.product(x) for x in miAlloc]).T
                if pattern == 0:
                    w = layerTwo
                else:
                    w = np.vstack((w,layerTwo))

                #слой 3
                wSum.append(np.sum(layerTwo))
                if pattern == 0:
                    wNormalized = layerTwo/wSum[pattern]
                else:
                    wNormalized = np.vstack((wNormalized,layerTwo/wSum[pattern]))
```

```
            #подготовка к четвертому слою
            layerThree = layerTwo/wSum[pattern]
            rowHolder = np.concatenate([x*np.append(Xs[pattern,:],1) for x in
layerThree])
            layerFour = np.append(layerFour,rowHolder)

        w = w.T
        wNormalized = wNormalized.T

        layerFour = np.array(np.array_split(layerFour,pattern + 1))

        return layerFour, wSum, w


    def backprop(ANFISObj, 144olumn, columns, theWSum, theW, theLayerFive):

        paramGrp = [0]* len(ANFISObj.memFuncs[144olumn])
        for MF in range(len(ANFISObj.memFuncs[144olumn])):

            parameters = np.empty(len(ANFISObj.memFuncs[144olumn][MF][1]))
            timesThru = 0
            for alpha in sorted(ANFISObj.memFuncs[144olumn][MF][1].keys()):

                bucket3 = np.empty(len(ANFISObj.X))
                for rowX in range(len(ANFISObj.X)):
                    varToTest = ANFISObj.X[rowX,144olumn]
                    tmpRow = np.empty(len(ANFISObj.memFuncs))
                    tmpRow.fill(varToTest)
```

```
bucket2 = np.empty(ANFISObj.Y.ndim)
for colY in range(ANFISObj.Y.ndim):

    rulesWithAlpha = np.array(np.where(ANFISObj.rules[:,145olumn]==MF))[0]
    adjCols = np.delete(columns,145olumn)

    senSit = mfDerivs.partial_dMF(ANFISObj.X[rowX,145olumn],ANFISObj.memFuncs[145olumn][MF],alpha)
    # выдает d_rule вывод / параметр в MF
    dW_dAplha = senSit * np.array([np.prod([ANFISObj.memClass.evaluateMF(tmpRow)[c][ANFISObj.rules[r][c]] for c in adjCols]) for r in rulesWithAlpha])

    bucket1 = np.empty(len(ANFISObj.rules[:,0]))
    for consequent in range(len(ANFISObj.rules[:,0])):
        fConsequent = np.dot(np.append(ANFISObj.X[rowX,:],1.),ANFISObj.consequents[((ANFISObj.X.shape[1] + 1) * consequent))((ANFISObj.X.shape[1] + 1) * consequent) + (ANFISObj.X.shape[1] + 1)),colY])
        acum = 0
        if consequent in rulesWithAlpha:
            acum = dW_dAplha[np.where(rulesWithAlpha==consequent)] * theWSum[rowX]

        acum = acum – theW[consequent,rowX] * np.sum(dW_dAplha)
        acum = acum / theWSum[rowX]**2
        bucket1[consequent] = fConsequent * acum
```

```
                sum1 = np.sum(bucket1)

                if ANFISObj.Y.ndim == 1:
                    bucket2[colY] = sum1 * (ANFISObj.Y[rowX]-
theLayerFive[rowX,colY])*(-2)
                else:
                    bucket2[colY] = sum1 * (ANFISObj.Y[rowX,colY]-
theLayerFive[rowX,colY])*(-2)

                sum2 = np.sum(bucket2)
                bucket3[rowX] = sum2

            sum3 = np.sum(bucket3)
            parameters[timesThru] = sum3
            timesThru = timesThru + 1

        paramGrp[MF] = parameters

    return paramGrp


def predict(ANFISObj, varsToTest):

    [layerFour, wSum, w] = forwardHalfPass(ANFISObj, varsToTest)

    #слой 5
    layerFive = np.dot(layerFour,ANFISObj.consequents)

    return layerFive
```

Описание кода программы тестовой и обучающей выборки:

```
train = pd.read_csv('threats.csv', encoding='utf-8')
df = pd.get_dummies(train)
Преобразование строковых данных:
for col in list(df.columns):
    # Выбор колонок для преобразования
    if ('ft²' in col or 'kBtu' in col or 'Metric Tons CO2e' in col or 'kWh' in
        col or 'therms' in col or 'gal' in col or 'Score' in col):
        # Конвертация
        df[col] = df[col].astype(float)


def main():
    app = QguiApplication(sys.argv)
    main = mainForm()
    main.show()
    sys.exit(app.exec_)


main()
```

Фрагмент кода описывает пользовательский интерфейс, функциональные возможности программы для ЭВМ, слои адаптированной нейронной сети, а также алгоритм обратного распространения ошибки работы системы ANFIS предлагаемого метода. За счет адаптации параметров сети в настоящей работе удалось достичь наименьшей RMSE в отличии от известных методов оценки эффективности СЗИ.

Итоговая оценка эффективности СЗИ [57] рассчитывается по формуле:

$$W = \frac{\sum_{j=1}^{m} X_j}{m} \quad (3.4),$$

где X_j – выполнение требований одного из показателей оценки эффективности СЗИ, $j = 1, m$;

m – перечень показателей.

$$0 \le W \le 1$$

С учетом важности выполнения требований оценка эффективности СЗИ рассчитывается следующим образом:

$$W = \sum_{j=1}^{m} x_j a_j ,$$

$$0 \le W \le 1, \text{ где}$$

a_j – коэффициент важности требования, $0 \le a \le 1$, $\sum_{j=1}^{m} a_j = 1$.

3.5. Оценка эффективности предложенного метода

Для определения эффективности предложенного метода необходимо рассмотреть следующие аспекты нечеткой системы логического вывода. Нечеткая система логического вывода представляла собой систему, которая отображает входные данные в выходные посредством трех основных этапов:

- фаззификаця;
- логический вывод;
- дефаззификация.

Рассмотрены только фиксированные функции принадлежности, которые были выбраны произвольно для моделирования оценки эффективности СЗИ, структура правил которых по предопределена интерпретацией экспертом характеристик переменных в модели. В определенных ситуациях моделирования систем невозможно различить, как должны выглядеть функции членства, просто имея набор данных. Анализируя и адаптируя набор данных (dataframe) для проведения оценки, невозможно определить функции членства. Нейро-адаптивные методы обучения предоставляют методы нечеткого моделирования, позволяющие проанализировать информацию о наборах данных (dataframe). Метод вычисляет параметры функции принадлежности, позволяющие системе нечеткого вывода отслеживать данные ввода-вывода. Структура сети аналогична нейронной сети и может использоваться для интерпретации входов-выходов, что позволяет отображать входные данные из dataframe с помощью функций принадлежности и

связанных параметров и затем, на основе выходных функций принадлежности и связанных параметров, для вывода. Параметры, связанные с функциями принадлежности, адаптируются в процессе обучения системы. Вычисление и адаптация параметров упрощается вектором градиента. Вектор градиента обеспечивает меру того, насколько хорошо система нечеткого вывода моделирует входные и выходные данные для данных параметров. После того, как получен вектор градиента, применяется процедура оптимизации для настройки параметров. Указанная процедура предназначена уменьшить меру ошибки. RMSE определяется суммой квадратов разности между фактическим и желаемым выходом.

Таким образом, необходимость использования ANFIS, а также ее эффективность для оценки СЗИ, становится очевидной.

Следующим шагом при проведении оценки эффективности самого метода, основанного на ANFIS, является определение алгоритма нечеткого вывода. На основании исследований и проведенных экспериментов, результаты которых представлены в главе 3.4 (таблица 3.8), можно сделать вывод о том, что ANFIS с алгоритмом нечеткого вывода Такаги-Сугено-Канга является наилучшей для решения задачи проведения оценки эффективности СЗИ.

Качество предложенного метода оценки эффективности СЗИ, по сравнению с известными методами, достигается следующими показателями: эффективность СЗИ достигает 97%, финансовые затраты могут достигать уменьшения стоимости создаваемой СЗИ до 30%.

Поставленную в диссертационном исследовании задачу по повышению качества оценки эффективности СЗИ ТРИС можно решать с помощью методов классификации, использующих различные математические аппараты и подходы реализации. Однако, эффективность методов зависит от конкретной решаемой задачи. В работе был проведен сравнительный анализ методов решения поставленной задачи и в качестве оценки эффективности предложенного метода задача была решена с помощью методов, сравнительный анализ которых приведен в таблице 3.10.

Таблица 3.10 – Сравнительный анализ методов для решения поставленной задачи

Метод	Преимущества	Недостатки
Метод Байеса (Naïve Bayes, NB)	Быстродействие метода; Поддержка инкрементного обучения; Простая реализация алгоритма; Интерпретируемость результатов работы алгоритма	Относительно низкое качество классификации; Неспособность учитывать зависимость результата классификации от сочетания признаков
Метод k ближайших соседей (k Nearest Neighbors, KNN)	Простота реализации; Проработанная теоретическая база; Адаптация под нужную задачу выбором метрики или ядра; Интерпретируемость	Недостаточная производительность в реальных задачах; Трудность в наборе подходящих весов и определением, какие признаки необходимы для классификации; Зависимость от выбранной метрики расстояния между примерами
Метод опорных векторов (Support Vector Machine, SVM)	Более уверенная классификация; Эквивалентен двухслойной нейронной сети – простота реализации	Невозможность калибровки вероятности попадания в определенный класс; Подходит только для решения задач с двумя классами; Параметры модели сложно интерпретировать; Не описаны общие методы построения ядер и спрямляющих пространств, наиболее подходящих для конкретной задачи; Нет отбора признаков; Неустойчивость к шуму
Метод деревьев решений (Decision Trees, DT)	Высокая производительность обучения и прогнозирования; Не требует подготовки данных; Способен работать как с категориальными, так и с интервальными переменными; Использует модель «белого ящика»; Позволяет работать с большим объёмом информации без специальных подготовительных процедур	Проблема получения оптимального дерева решений; Проблема переобучения; проблема XOR, чётности или мультиплексарности

В работе были проведены эксперименты сравнительного анализа работы предложенного метода и методов, описанных в таблице 3.10. В качестве сравнительной характеристики использовалась точность определения достигаемости/не достигаемости эффективности СЗИ ТРИС (точность классификации). Результаты работы методов оценивались экспертным путем для каждого из экспериментов.

Результаты сравнительного анализа приведены в таблице 3.11.

Таблица 3.11 – Результаты сравнительного анализа

	Наивный Байес	Метод k-ближайших соседей	Деревья решений	Логистическая регрессия	Предложенный метод на основе ANFIS
Точность оценки эффективности СЗИ ТРИС (%)	86,8	70,3	92,2	93,7	97

На рисунке 3.8 приведен график сравнительного анализа методов для решения поставленной задачи в диссертационном исследовании.

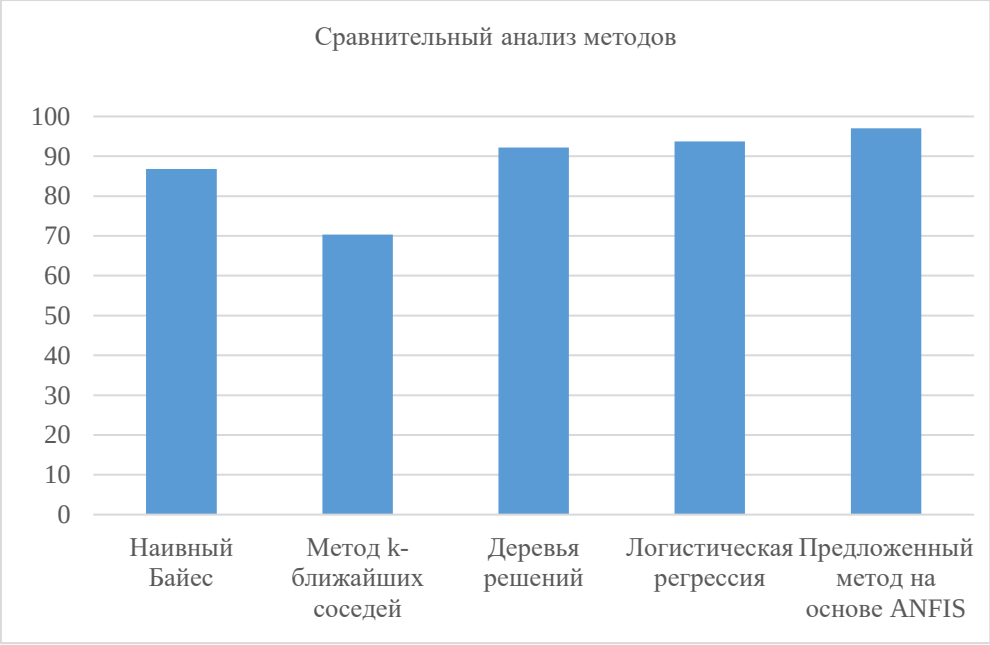


Рисунок 3.8 – График сравнительного анализа методов для решения поставленной задачи

Таким образом, для заданных условий задачи (сформированного набора данных после очистки, преобразования, выбора наиболее полезных и созданных новых более репрезентативных признаков) и определенных в работе показателей

оценки эффективности СЗИ предложенный метод является наилучшим по сравнению с известными.

Анализ оценки эффективности предложенного метода представлен в таблице 3.12.

Таблица 3.12 – Анализ оценки эффективности предложенного метода

Показатель	**Известные методы**	**Предложенный метод**
RMSE	0,021 – 0,213	0,012 – 0,017
Эффективность СЗИ	85,7 %	97 %
Стоимость СЗИ	снижение до 15%	снижение до 30%

Среднеквадратичная ошибка предложенного метода, вычисляемая по формуле:

$$RMSE = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(y_i - \hat{y}_i)^2},$$

где $y_i, \hat{y}_i$ – наборы данных (обучения, проверки), N – число элементов в обучающей выборке.

Графики сравнения RMSE известных и предложенного метода на заданном интервале представлены на рисунке 3.9.

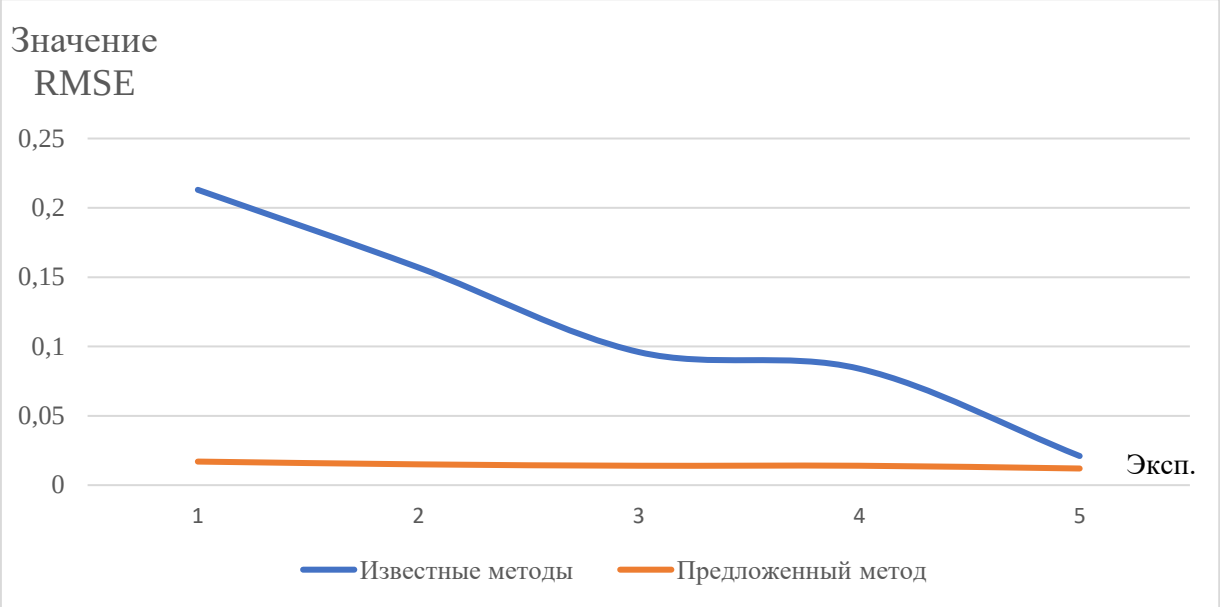


Рисунок 3.9 – График сравнения RMSE известных и предложенного метода на заданном интервале

RMSE достигает значения в диапазоне 0,012-0,017, что является локальным минимумом на заданном интервале и позволяет доказать выполнение поставленной в настоящем диссертационном исследовании задачи.

Выводы

В главе 3 определены необходимые и достаточные показатели, предложен метод оценки эффективности систем защиты информации, основанный на адаптивной нечеткой нейронной продукционной системе и алгоритме нечеткого вывода Такаги-Сугено-Канга, в отличии от известных, позволяет достигать меньшего значения среднеквадратической ошибки работы системы, таким образом повышает эффективность СЗИ (уровень защищенности) до 97%, что на 15% выше по сравнению с известными, финансовые затраты на создание системы защиты информации позволяют достигать уменьшения стоимости до 30%. Предложенный метод предоставляет возможность владельцам ИС автоматически оценивать эффективность СЗИ в режиме реального времени на всех этапах жизненного цикла

системы, что позволяет своевременно внести корректировки в проектные решения СЗИ для нейтрализации актуальных УБИ и выполнения требований по защите информации, учитывая финансовую составляющую. Также необходимо отметить, что показатели оценки эффективности для предложенного метода могут быть изменены в зависимости от целей и потребностей владельца системы в проведении оценки эффективности СЗИ.

Предложенный метод имеет следующие отличительные особенности и преимуществу в отличии от известных:

- предложенные показатели оценки эффективности СЗИ позволяют наиболее точно проводить оценку;
- не требует привлечения высоко квалифицированных специалистов в области ИБ;
- использует минимальные вычислительные ресурсы;
- позволяет оценить финансовые затраты на создание СЗИ;
- позволяет своевременно вносить корректировки в проектные решения по СЗИ: на этапе проектирования, внедрения и эксплуатации СЗИ;
- учитывает требования регуляторов РФ в области обеспечения безопасности информации;
- может быть адаптирован в зависимости от целей владельце систем при проведении оценки эффективности СЗИ.

С научной точки зрения предложенный метод использует современные и перспективные для решения подобных задач методы, практики и технологии.

Материалы главы 3 были представлены международных и российских научно-технических конференциях и опубликованы в изданиях, включенных в перечень ВАК при Минобрнауки России [56, 57, 60].

Результатом работы, проведенной в главе 3, является разработанная автором программа для ЭВМ «Оценка системы защиты информации», номер регистрации 2020664343 от 11.11.2020 г., копия свидетельства о регистрации программы для ЭВМ представлена в приложении Б.

Положения главы 3 настоящего диссертационного исследования были внедрены в учебный процесс курсов «Методы оценки безопасности компьютерных систем» и «Сертификация средств защиты информации» в СПбГУТ.

По результатам главы 3 подготовлено учебно-методическое пособие «Сертификация средств защиты информации» (Россия, Санкт-Петербург, СПбГУТ).

Глава 4. Методические рекомендации по оценке эффективности систем защиты территориально-распределенных информационных систем

В качестве исследуемой системы была выбрана ТРИС, являющаяся одновременно информационной системой обработки персональных данных 4 уровня защищенности [105] и государственной информационной системой 3 класса защищенности, а также автоматизированной системой, обрабатывающей конфиденциальную (коммерческую тайну) информацию класса 1 Г.

В настоящей работе предлагаются методические рекомендации по оценке эффективности СЗИ ТРИС, включающие в себя следующие шаги:

1. Обследование ТРИС в части: определения бизнес-процессов; информации, обрабатываемой системой; групп пользователей, их прав и полномочий; технологии обработки информации; ИТ-инфраструктуры, а также существующей СЗИ.
2. Определение перечня актуальных УБИ в соответствии с методическими документами регуляторов и на основании БДУ ФСТЭК России (MITRE ATT&CK), а также предложенной в настоящем диссертационном исследовании методики определения актуальных УБИ.
3. Формирование перечня требований по защите информации.
4. Подготовка набора данных для оценки эффективности СЗИ ТРИС, включающий в себя: перечень актуальных УБИ в ТРИС, перечень требований по защите информации, перечень возможных к использованию средств защиты информации в СЗИ ТРИС и их стоимость.
5. Проводятся экспертные оценки соответствия ТРИС по требованиям информационной безопасности.
6. Производиться оценка эффективности СЗИ на основании предложенного и описанного в работе метода оценки эффективности

СЗИ и реализованного с помощью программы для ЭВМ «Оценка системы защиты информации».

7. Внесение корректировок в технические решения по СЗИ ТРИС.

На основании требований по защите информации регуляторов были сформированы требования для исследуемой ТРИС. Перечень требований приведен в таблице 3.2 главы 3 настоящего диссертационного исследования.

Для формирования данных с помощью технологий Data Science был сформирован набор, составленный на описанной выше информации. Фрагменты набора данных и его преобразования представлены в главе 3.

4.1. Формы оценки соответствия систем защиты по требованиям безопасности информации

Формы оценки соответствия систем защиты информации по требованиям безопасности информации регламентируются Федеральным Законом «О техническом регулировании» (от 27.12.2002 г. № 184-ФЗ). Указанный закон регулирует отношения, возникающие при:

- разработке, принятии, применении и исполнении обязательных требований к продукции, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации;
- разработке, принятии, применении и исполнении на добровольной основе требований к продукции, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнению работ или оказанию услуг;
- оценке соответствия требованиям;
- при определении прав и обязанностей участников регулируемых отношений в сфере технического регулирования.

Основными определениями закона являются следующие:

- оценка соответствия требованиям — прямое или косвенное определение соблюдения требований, предъявляемых к объекту;
- подтверждение соответствия — документальное удостоверение соответствия продукции или иных объектов, процессов требованиям технических регламентов, положениям стандартов, сводов правил или условиям договоров.

Проведение оценки соответствия и оценки эффективности систем защиты информации информационных систем является обязательным для информационных систем обработки персональных данных, государственных информационных систем, автоматизированных систем управлениями технологическими процессами, критических информационных инфраструктур в соответствии с НПА ФСТЭК России[8].

Отдельно рассмотрим понятие аттестации объектов информатизации. В Российской Федерации аттестация объектов информатизации (ОИ) применяется для оценки соответствия требованиям систем защиты объектов информатизации и подтверждения их соответствия по требованиям безопасности информации. Под объектами информатизации, аттестуемыми по требованиям безопасности информации, понимаются автоматизированные системы различного уровня и назначения, системы связи, отображения и размножения вместе с помещениями, в которых они установлены, предназначенные для обработки и передачи информации, подлежащей защите, а также сами помещения, предназначенные для ведения конфиденциальных переговоров. Такими объектами являются:

---

[8]Приказ ФСТЭК России от 11 февраля 2013 г. №17 «Об утверждении требований о защите информации, не содержащей государственную тайну, содержащейся в государственных информационных системах».

Приказ ФСТЭК России от 18 февраля 2013 года №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

Приказ ФСТЭК России №31 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».

Приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

- автоматизированные системы;
- выделенные и защищаемые помещения;
- средства изготовления и размножения секретных документов.

Аттестация проводится в порядке, установленном в:

- Положение по аттестации объектов информатизации по требованиям безопасности информации (утверждено Гостехкомиссией РФ 25.11.1994).
- Порядок организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну (утвержден приказом ФСТЭК России от 29 апреля 2021 г. № 77).
- ГОСТ РО 0043-003-2012 «Аттестация объектов информатизации. Общие положения».
- ГОСТ РО 0043-004-2013 «Защита информации. Аттестация объектов информатизации. Программа и методики аттестационных испытаний».

Обязательным проведение аттестации является для информационных систем, обрабатывающих сведения, составляющие государственную тайну, государственных и муниципальных информационных систем, информационных систем управления производством, используемых организациями оборонно-промышленного комплекса. В остальных случаях аттестация ИС носит добровольный характер.

Существует также формы оценки соответствия ИС в форме декларации соответствия и формах приемки СЗИ ИС, установленных ФЗ № 184. Такие формы оценки, как правило, не достаточно полно отражают реальную оценку СЗИ ИС, ввиду субъективных точек зрения членов комиссии и недостатков экспертного метода.

В настоящей работе предлагаются методические рекомендации по оценке эффективности системы защиты территориально-распределенных информационных систем и не затрагивает вопросы проведения аттестации ОИ. Под

оценкой эффективности понимается следующее: эффективность СЗИ достигается путем создания СЗИ, способной максимально нейтрализовать актуальные УБИ, выполнить требования по защите информации, предъявляемые к ИС на основании требований регуляторов в области обеспечения безопасности информации, а также позволяющей максимально минимизировать финансовые затраты на создание СЗИ [59]. Для оценки применяются показатели, описанные в разделе 3.1. настоящей работы.

4.2. Алгоритм проведения оценки эффективности систем защиты территориально-распределенных информационных систем

Алгоритм проведения оценки эффективности СЗИ ТРИС состоит из следующих шагов:

1. Подготовка набора данных для проведения оценки эффективности СЗИ, состоящего из:
    - перечня актуальных УБИ в ТРИС (результаты программы для ЭВМ «Модель угроз и нарушителя»);
    - перечня требований по ИБ;
    - перечня СрЗИ, используемых в ТРИС, и их стоимости (информация от производителей).
2. Анализ, форматирование и конвертация набора данных. Подготовка файла для программы для ЭВМ «Оценка системы защиты информации» (глава 3 настоящей диссертации).
3. Формирование базы правил для проведения оценки эффективности СЗИ ТРИС (глава 3 настоящей диссертации).
4. Проведение оценки эффективности СЗИ ТРИС (глава 3 настоящей диссертации).
5. Оформление результатов проведения оценки эффективности СЗИ ТРИС. Внесение корректировок в проектные решения по СЗИ ТРИС, при необходимости.

Блок-схемы жизненного цикла создания СЗИ и проведения оценки эффективности СЗИ ТРИС представлены на рисунках 4.1 и 4.2, соответственно.

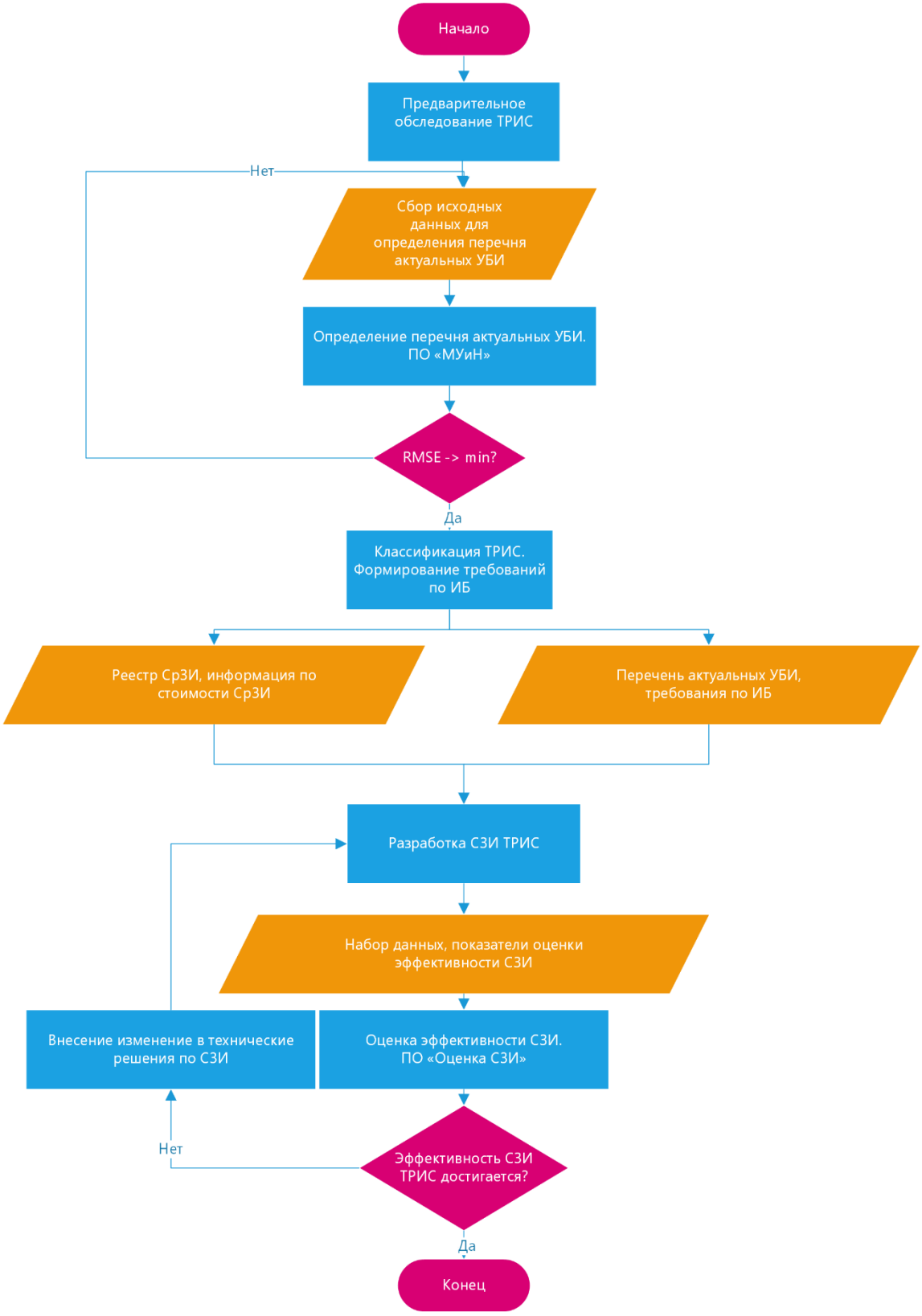


Рисунок 4.1 – Блок-схема жизненного цикла создания СЗИ ТРИС

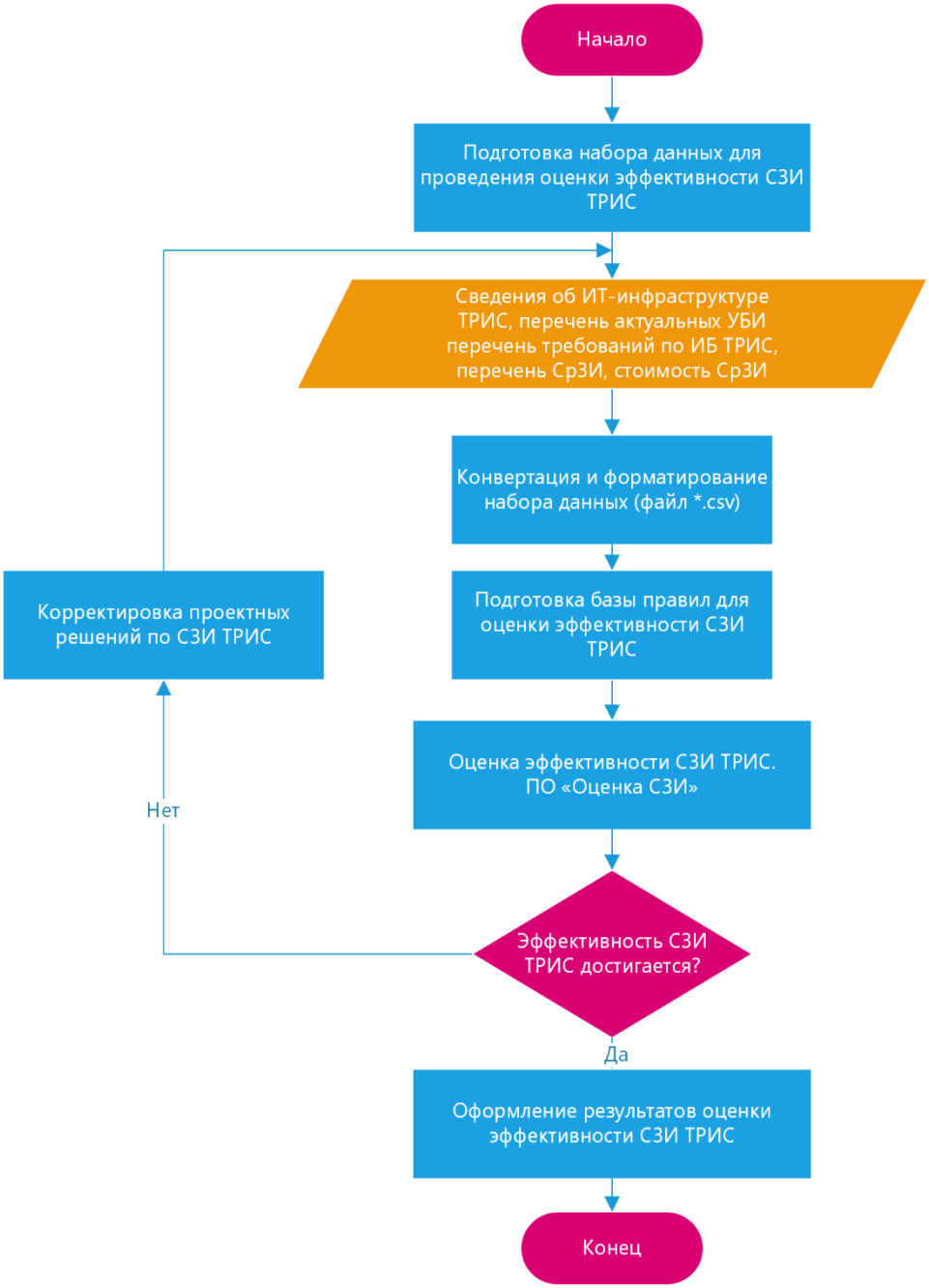


Рисунок 4.2 – Блок-схема проведения оценки эффективности СЗИ ТРИС

Представленные блок-схемы алгоритма методических рекомендаций по оценке эффективности СЗИ ТРИС наиболее полно и достаточно описывают шаги проведения работ по оценке, позволяющие проводить такие работы на всех этапах жизненного цикла существования ТРИС.

4.3. Методические рекомендации по оценке эффективности систем защиты территориально-распределенных информационных систем

Проведение оценки эффективности предлагается выполнять в соответствии с методическими рекомендациями, состоящими из следующих шагов [60, 61]:

1. Проводится обследование ТРИС, по результатам которого формируется протокол, включающий в себя описание бизнес-процессов; перечень информации, обрабатываемой системой; описание групп пользователей, их прав и полномочий; описание технологии обработки информации; описание ИТ-инфраструктуры, а также существующей СЗИ.
2. Определение перечня актуальных УБИ в соответствии с методическими документами регуляторов и на основании БДУ ФСТЭК России (MITRE ATT&CK, CVE, CWE, OSVDB, NVD, Secunia). Определяется тип и класс, уровень и (или) класс защищенности, категория значимости ТРИС. Перечень актуальных УБИ формируются на основе предложенной в настоящем диссертационном исследовании методики определения актуальных УБИ с использованием разработанной программы для ЭВМ «Модель угроз и нарушителя».
3. Формируется перечень требований по защите информации на основании классификации, перечня актуальных УБИ и требований по защите информации, устанавливаемых регуляторами РФ.
4. Формируется набор данных, включающий в себя: ИТ-инфраструктуру ТРИС, перечень актуальных УБИ в ТРИС, перечень требований по защите информации, перечень возможных к использованию средств защиты информации в СЗИ ТРИС, их стоимость. С помощью технологий Data Science набор данных очищается и преобразуется.

5. Проводятся и учитываются экспертные оценки соответствия ТРИС по требованиям информационной безопасности (терм-множества лингвистических переменных).
6. На основании предложенного метода оценки эффективности СЗИ производиться оценка эффективности (уровень защищенности) СЗИ ТРИС (программа для ЭВМ «Оценка системы защиты информации).
7. На основании результатов оценки эффективности СЗИ ТРИС при необходимости вносятся корректировки в проектные решения по защите информации.

Структурная схема проведения оценки эффективности СЗИ ТРИС представлена на рисунке 4.3 [55, 60].

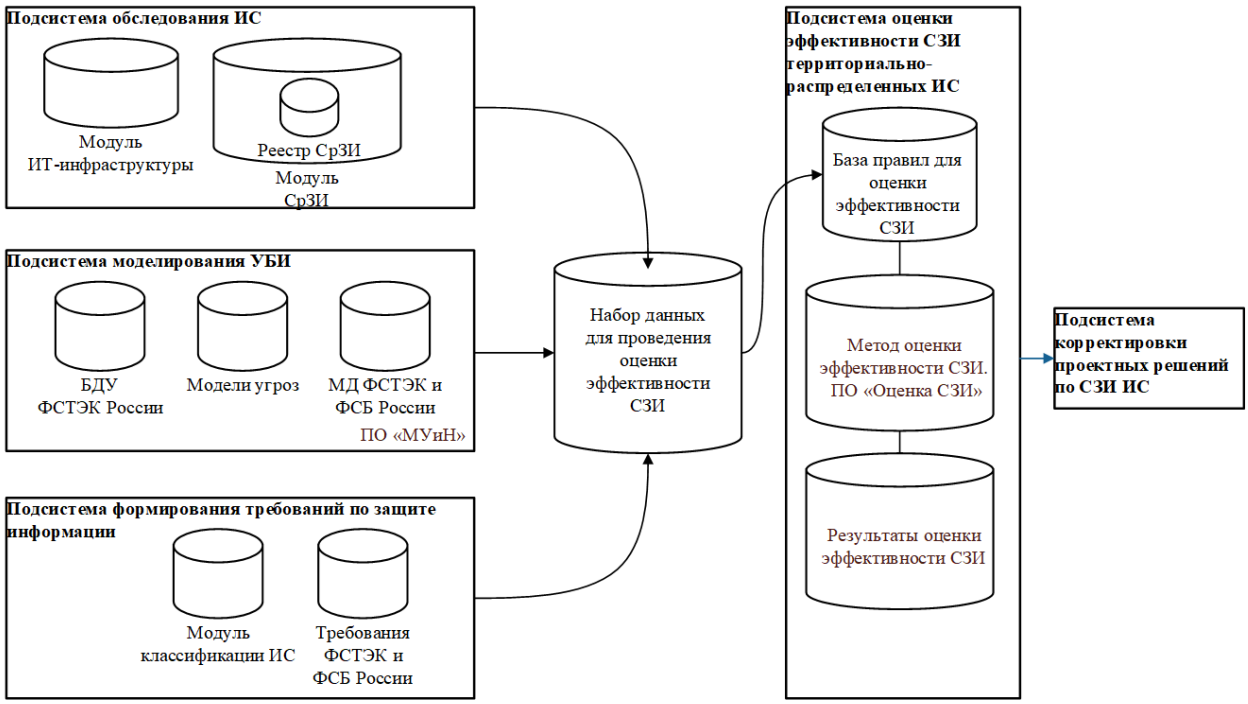


Рисунок 4.3 – Структурная схема проведения оценки эффективности СЗИ ТРИС

Процесс проведении оценки эффективности состоит из пяти подсистем:

1. Подсистема обследования ИС.
2. Подсистема моделирования УБИ.
3. Подсистема формирования требований по защите информации.

4. Подсистема оценки эффективности СЗИ ТРИС.
5. Подсистема корректировки проектных решений по СЗИ ТРИС.

Такое разбиение на подсистемы обусловлено независимостью друг от друга каждой из них, что, в свою очередь, позволяет вносить корректировки [63] в процессе проведения оценки эффективности СЗИ ТРИС без внесения изменений в смежные подсистемы.

4.4. Реализация методики оценки эффективности системы защиты информации территориально-распределенных информационных систем

На основании предложенной методики оценки эффективности системы защиты информации территориально-распределенных информационных систем была проведена оценка эффективности СЗИ ТРИС ЗАО «ДИДЖИТАЛ ДИЗАЙН».

По результатам обследования определены ключевые аспекты ИТ-инфраструктуры ТРИС ЗАО «ДИДЖИТАЛ ДИЗАЙН» (далее – Система).

Система реализована в формате клиент-серверной архитектуры. Система предоставляет возможности функциональных модификаций на базе открытого программного интерфейса (API) с использованием распространенных языков программирования (C#, TypeScript (платформа разработки Angular, среда разработки dotnet.core)).

Система обеспечивает принцип централизованного хранения, накопления и многократного использования данных. На АРМ пользователей хранение данных не осуществляется.

В состав информационной инфраструктуры Системы входят:

1. серверы, включающие:

– серверное оборудование;
– прикладные и специализированные программы, обеспечивающие обработку информации и ее представление в виде, необходимом для последующей автоматизированной обработки;

2. АРМ пользователей:
– типовые АРМ пользователя;
– АРМ руководителя (мобильное АРМ): используется руководителями высшего звена (мобильное устройство).

Серверные компоненты Системы размещены в среде виртуализации. Аппаратно-программный комплекс виртуализации Системы состоит из 5 серверов виртуализации на основе ПО Vmware, работающих под управлением сервера vCenter, сети хранения данных SAN в составе коммутаторов и 3 систем хранения данных, 2 оптических коммутаторов ядра сети и 1 коммутатора управления.

В среде виртуализации Системы развёрнуты 20 виртуальных серверов, в числе которых:

– 2 сервера OpenVPN для подключения удаленных пользователей из сети общего пользования «Интернет»;
– серверы приложений;
– сервер СУБД;
– серверы балансировщика нагрузки Load Balancer;
– терминальные серверы;
– сервер для онлайн просмотра;
– серверы для веб-просмотра;
– серверы синхронизации для мобильного АРМ;
– менеджмент-сервер.

Системы хранения данных, входящие в сеть хранения данных, включают:

– 2 скоростных хранилища – для хранения файлов виртуальных машин;
– 1 медленное хранилище – для Backup файлов виртуальных машин.

Резервное копирование данных Системы выполняется посредством возможностей ПО MS SQL и Veeam Backup & Replication (не сертифицирован в Системе сертификации средств защиты информации ФСТЭК России [39-41]), время хранения резервных копий не регламентировано.

Доступ к Системе для выполнения функций по администрированию компонентов ИТ-инфраструктуры осуществляется с АРМ администраторов Системы, расположенных в пределах КЗ Системы.

КЗ Системы включает в себя пространства (территория, здания, помещения), в которых размещаются компоненты Системы и исключено неконтролируемое пребывание посетителей, а также посторонних транспортных средств.

Информационный обмен между серверами и клиентскими рабочими местами обеспечивается с использованием ресурсов вычислительных сетей Системы и организаций пользователей Системы посредством технологий Ethernet и Fibre Channel. Также присутствует возможность удалённой работы с объектом информатизации с использованием рабочих мест за пределами локальной вычислительной сети Системы через OpenVPN сервер [100].

Структурная схема СЗИ ТРИС ЗАО «ДИДЖИТАЛ ДИЗАЙН» представлена на рисунке 4.4.

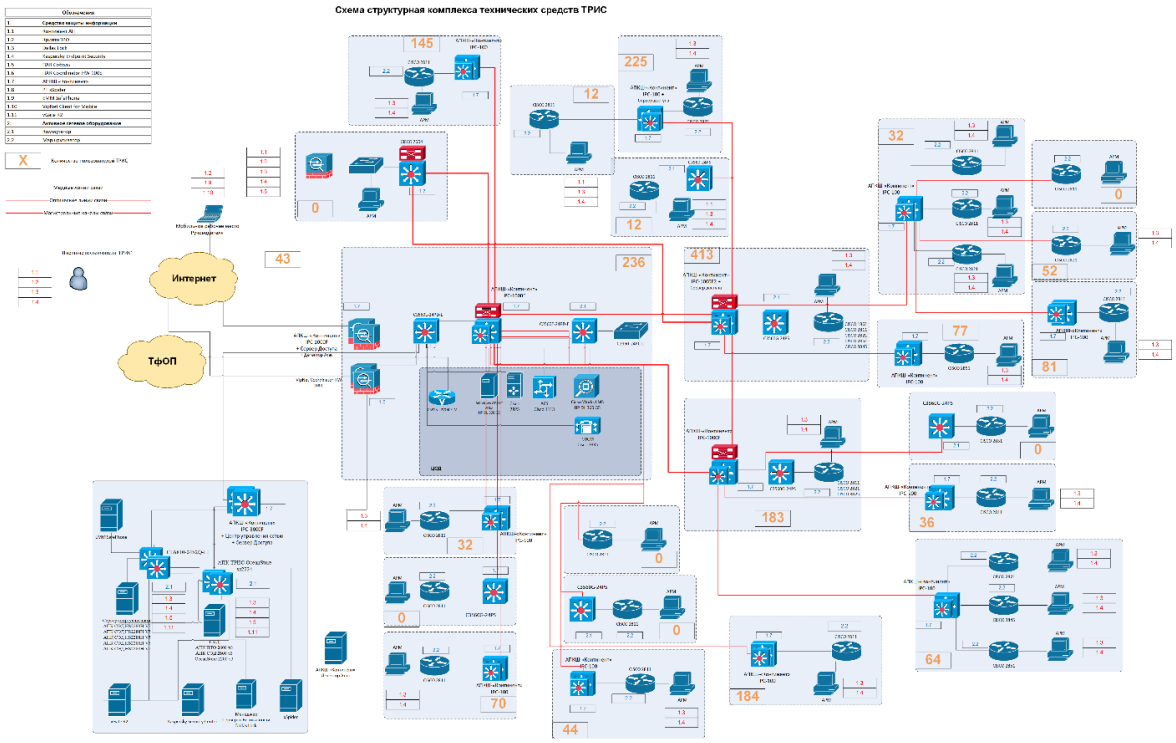


Рисунок 4.4 – Структурная схема СЗИ ТРИС ЗАО «ДИДЖИТАЛ ДИЗАЙН»

К объектам защиты ТРИС ЗАО «ДИДЖИТАЛ ДИЗАЙН» относятся:

– ПДн, обрабатываемые в ТРИС;

- ТС, предназначенные для обработки информации (в том числе средства вычислительной техники, машинные носители информации, средства и системы связи и передачи данных, ТС обработки буквенно-цифровой, графической, видео- и речевой информации);
- системное и прикладное ПО;
- СрЗИ;
- СКЗИ;
- среда функционирования СКЗИ (далее – СФ);
- информация, относящаяся к криптографической защите информации, в том числе ПДн, включая ключевую, парольную и аутентифицирующую информацию СКЗИ;
- документы, дела, журналы, картотеки, издания, технические документы, видео-, кино- и фотоматериалы, рабочие материалы и т.п., в которых отражена защищаемая информация, относящаяся к ИСПДн и их криптографической защите, включая документацию на СКЗИ и на технические и программные компоненты СФ;
- носители защищаемой информации, используемые в ТРИС в процессе криптографической защиты информации, носители ключевой, парольной и аутентифицирующей информации СКЗИ и порядок доступа к ним;
- используемые ТРИС каналы (линии) связи, включая кабельные системы;
- помещения, в которых находятся ресурсы ТРИС, имеющие отношение к криптографической защите информации.

В ТРИС обрабатываются следующие категории информации:

- ПДн;
- служебная информация;
- технические параметры ТРИС, конфигурационные файлы и файлы настроек системного и прикладного ПО ТРИС, включая ПО СрЗИ.

В соответствии с алгоритмом предложенной методики было проведено обследование Системы, по результатам которого разработана модель угроз безопасности с помощью предложенной методики определения актуальных УБИ, реализованной с помощью программы для ЭВМ «Модель угроз и нарушителя». Результаты показали увеличение актуальных УБИ на 5 % в отличие от существующей модели угроз в ТРИС ЗАО «ДИДЖИТАЛ ДИЗАЙН».

На рисунке 4.5 представлен интерфейс разработанной в настоящем диссертационном исследовании программы для ЭВМ «Модель угроз и нарушителя».

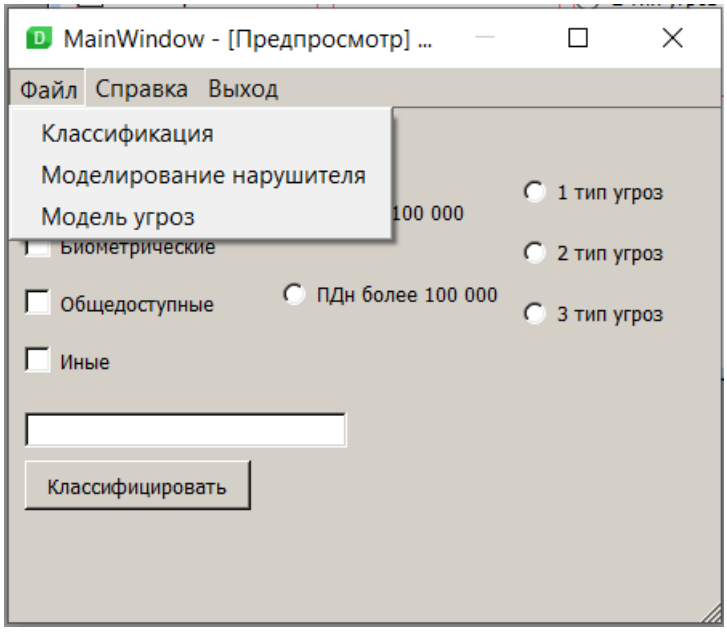


Рисунок 4.5 – Интерфейс программы для ЭВМ «Модель угроз и нарушителя»

Перечень сформированных актуальных УБИ приведен в таблице 4.1.

Таблица 4.1 – Перечень сформированных актуальных УБИ в ТРИС ЗАО «ДИДЖИТАЛ ДИЗАЙН»

№ п./п.	№ УБИ БДУ	Угроза безопасности информации
1.	003	Угроза анализа криптографических алгоритмов и их реализации
2.	067	Угроза неправомерного ознакомления с защищаемой информацией
3.	004	Угроза аппаратного сброса пароля BIOS
4.	005	Угроза внедрения вредоносного кода в BIOS
5.	045	Угроза нарушения изоляции среды исполнения BIOS
6.	123	Угроза подбора пароля BIOS
7.	129	Угроза подмены резервной копии программного обеспечения BIOS
8.	144	Угроза программного сброса пароля BIOS
9.	006	Угроза внедрения кода или данных
10.	007	Угроза воздействия на программы с высокими привилегиями
11.	008	Угроза восстановления и/или повторного использования аутентификационной информации
12.	012	Угроза деструктивного изменения конфигурации/среды окружения программ
13.	015	Угроза доступа к защищаемым файлам с использованием обходного пути
14.	022	Угроза избыточного выделения оперативной памяти
15.	023	Угроза изменения компонентов системы
16.	025	Угроза изменения системных и глобальных переменных
17.	027	Угроза искажения вводимой и выводимой на периферийные устройства информации
18.	028	Угроза использования альтернативных путей доступа к ресурсам
19.	030	Угроза использования информации идентификации/аутентификации, заданной по умолчанию
20.	031	Угроза использования механизмов авторизации для повышения привилегий
21.	032	Угроза использования поддельных цифровых подписей BIOS
22.	037	Угроза исследования приложения через отчёты об ошибках
23.	033	Угроза использования слабостей кодирования входных данных
24.	063	Угроза некорректного использования функционала программного и аппаратного обеспечения

Таблица 4.1. Продолжение

25.	034	Угроза использования слабостей протоколов сетевого/локального обмена данными
26.	068	Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением
27.	071	Угроза несанкционированного восстановления удалённой защищаемой информации
28.	074	Угроза несанкционированного доступа к аутентификационной информации
29.	086	Угроза несанкционированного изменения аутентификационной информации
30.	039	Угроза исчерпания запаса ключей, необходимых для обновления BIOS
31.	088	Угроза несанкционированного копирования защищаемой информации
32.	089	Угроза несанкционированного редактирования реестра
33.	090	Угроза несанкционированного создания учётной записи пользователя
34.	093	Угроза несанкционированного управления буфером
35.	044	Угроза нарушения изоляции пользовательских данных внутри виртуальной машины
36.	094	Угроза несанкционированного управления синхронизацией и состоянием
37.	201	Угроза утечки пользовательских данных при использовании функций автоматического заполнения аутентификационной информации в браузере
38.	102	Угроза опосредованного управления группой программ через совместно используемые данные
39.	109	Угроза перебора всех настроек и параметров приложения
40.	049	Угроза нарушения целостности данных кеша
41.	115	Угроза перехвата вводимой и выводимой на периферийные устройства информации
42.	117	Угроза перехвата привилегированного потока
43.	118	Угроза перехвата привилегированного процесса
44.	051	Угроза невозможности восстановления сессии работы на ПЭВМ при выводе из промежуточных состояний питания
45.	121	Угроза повреждения системного реестра
46.	122	Угроза повышения привилегий
47.	124	Угроза подделки записей журнала регистрации событий
48.	143	Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации
49.	145	Угроза пропуска проверки целостности программного обеспечения
50.	149	Угроза сбоя обработки специальным образом изменённых файлов

Таблица 4.1. Продолжение

51.	152	Угроза удаления аутентификационной информации
52.	178	Угроза несанкционированного использования системных и сетевых утилит
53.	059	Угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов
54.	179	Угроза несанкционированной модификации защищаемой информации
55.	187	Угроза несанкционированного воздействия на средство защиты информации
56.	061	Угроза некорректного задания структуры данных транзакции
57.	189	Угроза маскирования действий вредоносного кода
58.	062	Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера
59.	192	Угроза использования уязвимых версий программного обеспечения
60.	193	Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика
61.	195	Угроза удаленного запуска вредоносного кода в обход механизмов защиты операционной системы
62.	198	Угроза скрытной регистрации вредоносной программой учетных записей администраторов
63.	212	Угроза перехвата управления информационной системой
64.	016	Угроза доступа к локальным файлам сервера при помощи URL
65.	041	Угроза межсайтового скриптинга
66.	017	Угроза доступа/перехвата/изменения HTTP cookies
67.	019	Угроза заражения DNS-кеша
68.	167	Угроза заражения компьютера (мобильного устройства) при посещении неблагонадежных сайтов
69.	072	Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS
70.	042	Угроза межсайтовой подделки запроса
71.	111	Угроза передачи данных по скрытым каналам
72.	159	Угроза «форсированного веб-браузинга»
73.	174	Угроза «фарминга»
74.	186	Угроза внедрения вредоносного кода через рекламу, сервисы и контент
75.	069	Угроза неправомерных действий в каналах связи
76.	073	Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети

Таблица 4.1. Продолжение

77.	075	Угроза несанкционированного доступа к виртуальным каналам передачи
78.	098	Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб
79.	103	Угроза определения типов объектов защиты
80.	026	Угроза искажения XML-схемы
81.	104	Угроза определения топологии вычислительной сети
82.	016	Угроза перехвата данных, передаваемых по вычислительной сети
83.	128	Угроза подмены доверенного пользователя
84.	130	Угроза подмены содержимого сетевых ресурсов
85.	131	Угроза подмены субъекта сетевого доступа
86.	132	Угроза получения предварительной информации об объекте защиты
87.	087	Угроза несанкционированного использования привилегированных функций BIOS
88.	140	Угроза приведения системы в состояние «отказ в обслуживании»
89.	168	Угроза «кражи» учётной записи доступа к сетевым сервисам
90.	190	Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети «Интернет»
91.	010	Угроза выхода процесса за пределы виртуальной машины
92.	046	Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия
93.	092	Угроза несанкционированного удалённого внеполосного доступа к аппаратным средствам
94.	092	Угроза нарушения технологии обработки информации путём несанкционированного внесения изменений в образы виртуальных машин
95.	076	Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети
96.	077	Угроза несанкционированного доступа к данным за пределами зарезервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение
97.	095	Угроза несанкционированного управления указателями
98.	078	Угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети
99.	079	Угроза несанкционированного доступа к защищаемым виртуальным машинам со стороны других виртуальных машин
100.	084	Угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети

Таблица 4.1. Продолжение

101.	119	Угроза перехвата управления гипервизором
102.	099	Угроза обнаружения хостов
103.	120	Угроза перехвата управления средой виртуализации
104.	100	Угроза обхода некорректно настроенных механизмов аутентификации
105.	184	Угроза агрегирования данных, обрабатываемых с помощью мобильного устройства
106.	194	Угроза несанкционированного использования привилегированных функций мобильного устройства
107.	196	Угроза контроля вредоносной программой списка приложений, запущенных на мобильном устройстве
108.	199	Угроза перехвата управления мобильного устройства при использовании виртуальных голосовых ассистентов
109.	108	Угроза ошибки обновления гипервизора
110.	200	Угроза хищения информации с мобильного устройства при использовании виртуальных голосовых ассистентов
111.	202	Угроза несанкционированной установки приложений на мобильные устройства
112.	208	Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники
113.	113	Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники
114.	114	Угроза переполнения целочисленных переменных
115.	127	Угроза подмены действия пользователя путём обмана
116.	133	Угроза получения сведений о владельце беспроводного устройства
117.	153	Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов
118.	155	Угроза утраты вычислительных ресурсов
119.	162	Угроза эксплуатации цифровой подписи программного кода
120.	163	Угроза перехвата исключения/сигнала из привилегированного блока функций
121.	170	Угроза неправомерного шифрования информации
122.	171	Угроза скрытного включения вычислительного устройства в состав бот-сети
123.	172	Угроза распространения «почтовых червей»
124.	175	Угроза «фишинга»
125.	176	Угроза нарушения технологического/производственного процесса из-за временных задержек, вносимых средством защиты
126.	181	Угроза перехвата одноразовых паролей в режиме реального времени

Таблица 4.1. Продолжение

127.	182	Угроза физического устаревания аппаратных компонентов
128.	185	Угроза несанкционированного изменения параметров настройки средств защиты информации
129.	188	Угроза подмены программного обеспечения

По результатам обследования Системы, определения перечня актуальных УБИ и классификации Системы были сформированы требования по защите информации к ТРИС ЗАО «ДИДЖИТАЛ ДИЗАЙН». Перечень требований представлен в таблице 3.2 раздела 3.2 настоящей работы.

На основании результатов обследования, определения перечня актуальных УБИ в ТРИС, сформированных требования по защите информации и ГОСТ серии 34 были разработаны проектные решения по защите информации в Системе [62].

В качестве реализации СЗИ Системы далее описаны подсистемы защиты среды виртуализации и регистрации событий безопасности. Подсистема защиты среды виртуализации реализует следующие функции:

- «Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации»;
- «Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин»;
- «Регистрация событий безопасности в виртуальной инфраструктуре;
- Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных»;
- «Контроль целостности виртуальной инфраструктуры и ее конфигурации»;
- «Резервное копирование данных, резервирование ТС, ПО виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры»;

– «Реализация и управление антивирусной защитой в виртуальной инфраструктуре»;
– «Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки персональных данных отдельным пользователем и (или) группой пользователей».

В качестве подсистемы защиты среды виртуализации используется сертифицированное СрЗИ vGate R2.

СрЗИ vGate R2 обеспечивает реализацию всех функций подсистемы защиты среды виртуализации, защиту от специфических угроз виртуализации, позволяет контролировать действия администраторов виртуальной инфраструктуры и осуществляет фильтрацию трафика на уровне гипервизора.

В состав ПО vGate R2 входят сервер авторизации и консоль управления СрЗИ, которые устанавливаются на АРМ Администратора ИБ.

На рисунке 4.6 представлена логическая схема подсистемы защиты среды виртуализации, реализованная с применением СрЗИ vGate R2.

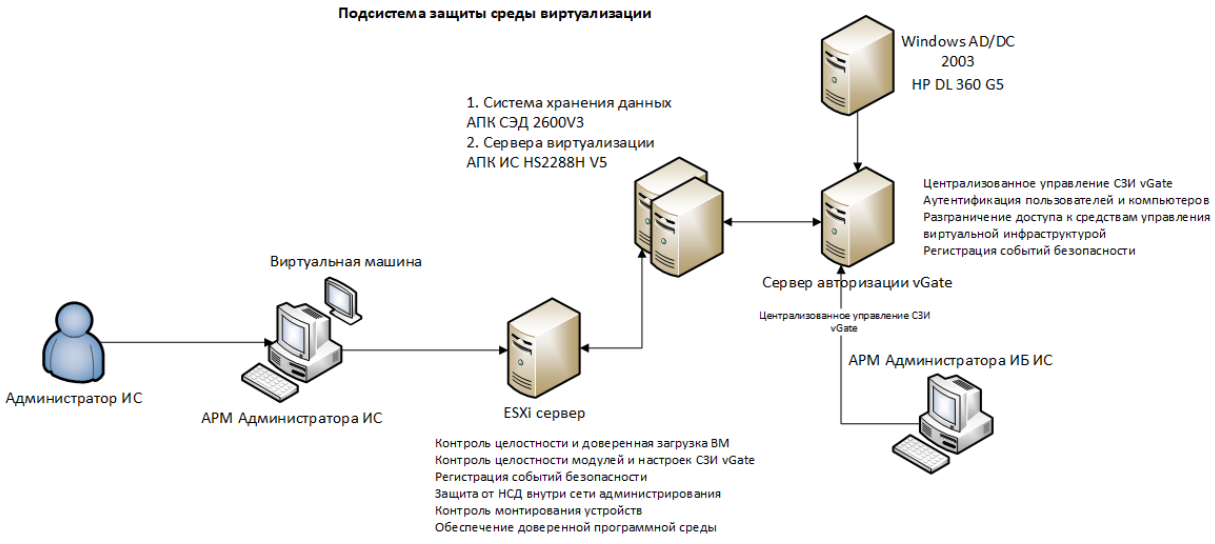


Рисунок 4.6 – Логическая схема подсистемы защиты среды виртуализации Системы

Подсистема регистрации событий безопасности предназначена для реализации следующих функций:

- Определение событий безопасности, подлежащих регистрации, и сроков их хранения;
- Определение состава и содержания информации о событиях безопасности, подлежащих регистрации;
- Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения;
- Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них;
- Защита информации о событиях безопасности.

Средствами обеспечения функций подсистемы регистрации событий безопасности являются журналы безопасности СрЗИ Dallas Lock 8.0-K, комплект ПО «Kaspersky Endpoint Security для бизнеса Стандартный» в составе компонентов «Kaspersky Endpoint Security 11» (KES) и Kaspersky Security Center 10 (KSC) и СрЗИ ЕММ SafePhone, в которых содержится информация о действиях пользователей, начиная с момента их входа в ОС, об ошибках, связанных с доступом к тем или иным объектам доступа, в том числе к тем, доступ приложений к которым запрещен.

СрЗИ «Dallas Lock 8.0-K содержит следующие журналы:

- Журнал входов.
- Журнал управления учетными записями.
- Журнал ресурсов.
- Журнал печати.
- Журнал управления политиками.
- Журнал процессов.
- Журнал пакетов МЭ.
- Журнал соединений МЭ.
- Журнал событий ОС.

– Журнал трафика.

– Журнал контроля приложений.

В каждом журнале фиксируются дата, время, имя пользователя, операция, результат и прочие параметры. Возможно упорядочивание элементов списков журнала по необходимому значению.

На рисунке 4.7 представлена логическая схема подсистемы регистрации событий безопасности, реализованная с применением СрЗИ от НСД Dallas Lock 8.0-K.

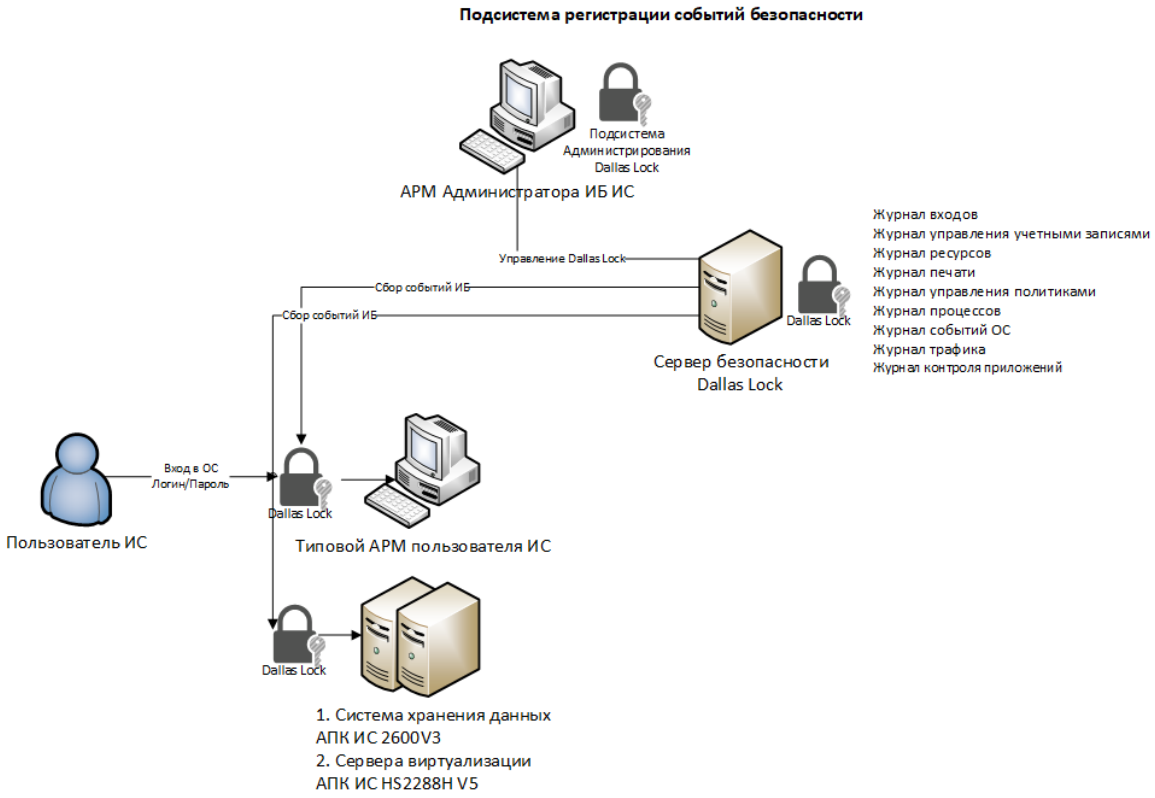


Рисунок 4.7 – Логическая схема подсистемы регистрации событий безопасности Системы

Полный перечень подсистем и функций по защите информации в исследуемой в настоящей диссертационной работе Системы приведен в таблице 4.2.

Таблица 4.2 – Подсистемы и функции по защите информации в Системе

Подсистема	Функции	СрЗИ
Подсистема идентификации и аутентификации субъектов доступа и объектов доступа	Идентификация и аутентификация пользователей, являющихся работниками ТРИС	Dallas Lock 8.0-K, EMM SafePhone, организационные меры с помощью встроенных возможностей (далее – ВВ) ОС и АСО
	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	
	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации	
	Защита обратной связи при вводе аутентификационной информации	
	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных	
Подсистема управления доступом субъектов доступа к объектам доступа	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей	Dallas Lock 8.0-K, организационные меры с помощью ВВ ОС
	Реализация дискреционного или ролевого метода доступа, типов (чтение, запись, выполнение) и правил разграничения доступа	АПКШ «Континент», «Континент – АП» Dallas Lock 8.0-K, встроенные средства прикладного ПО ТРИС, EMM SafePhone
	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами ТРИС, а также между информационными подсистемами	АПКШ «Континент», «Континент – АП»
	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование ТРИС	АПКШ «Континент», «Континент – АП», Dallas Lock 8.0-K
	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование ТРИС	Организационные меры с помощью ВВ ОС, Dallas Lock 8.0-K, EMM SafePhone
	Ограничение неуспешных попыток входа в ОС АРМ ТРИС	Организационные меры с помощью ВВ ОС, Dallas Lock 8.0-K, EMM SafePhone

Таблица 4.2. Продолжение

	Блокирование сеанса доступа в ТРИС после установленного времени бездействия (неактивности) пользователя или по его запросу	Организационные меры с помощью ВВ ОС
	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации	Организационные меры с помощью ВВ ОС, Dallas Lock 8.0-K, EMM SafePhone
	Регламентация и контроль использования в ТРИС технологий беспроводного доступа	АПКШ «Континент», «Континент – АП», организационные меры
	Реализация защищённого удалённого доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети	АПКШ «Континент», «Континент – АП», ViPNet Client Mobile 2, ПАК ViPNet Coordinator HW 4
	Регламентация и контроль использования в ТРИС мобильных ТС	Организационные меры, EMM SafePhone
	Обеспечение доверенной загрузки средств вычислительной техники	ПАК «Соболь», организационные меры
Подсистема ограничения программной среды	Обеспечение возможности установки только разрешенного к использованию ПО	Организационные меры с помощью ВВ ОС, Dallas Lock 8.0-K, vGate R2, EMM SafePhone
Подсистема защиты МН	Учет МН	Организационные меры
	Управление доступом к МН	
	Контроль перемещения МН за пределы КЗ ТРИС	
	Контроль подключения МН	Dallas Lock 8.0-K
Подсистема регистрации событий безопасности	Определение событий безопасности, подлежащих регистрации, и сроков их хранения	Организационные меры, Dallas Lock 8.0-K
	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	

Таблица 4.2. Продолжение

	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения	Журналы безопасности: – KSC и KES, – Dallas Lock 8.0-K, – EMM SafePhone
	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них	Журналы безопасности: – KES, – Dallas Lock 8.0-K, – EMM SafePhone
	Защита информации о событиях безопасности	Журналы безопасности: – KES, – Dallas Lock 8.0-K, – EMM SafePhone
Подсистема антивирусной защиты	Антивирусная защита АРМ и серверов ТРИС и съемных МН	– KES, – KSC
	Обновление БД признаков вредоносных компьютерных программ (вирусов)	
Подсистема защиты ТРИС, ее средств, систем связи и передачи данных	Разделение в ТРИС функций по управлению (администрированию) ТРИС, управлению (администрированию) СЗИ ТРИС, функций по обработке информации и иных функций ТРИС	Организационные меры
	Защита архивных файлов, параметров настройки СрЗИ и ПО и иных данных, не подлежащих изменению в процессе обработки информации	ВВ системы резервного копирования

Таблица 4.2. Продолжение

	Криптографическая защита данных, передаваемых по каналам связи	– АПКШ «Континент», – «Континент – АП», ViPNet Client Mobile 2, ПАК ViPNet Coordinator HW 4
	Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов	
	Разбиение ТРИС на сегменты и обеспечение защиты периметров сегментов ТРИС	
	Защита беспроводных соединений, применяемых в ТРИС	
Подсистема обнаружения вторжений	Обнаружение вторжений	АПКШ «Континент»: компонент «Детектор атак»
	Обновление базы решающих правил	
Подсистема анализа защищенности	Выявление, анализ уязвимостей информационной системы	ПО Xspider 7.8 Professional Edition
	Контроль установки обновлений ПО, включая обновление ПО СрЗИ	ПО Xspider 7.8 Professional Edition, ПО Windows Server Update Services (WSUS)
	Контроль работоспособности, параметров настройки и правильности функционирования ПО и СрЗИ	Организационные меры
	Контроль состава ТС, ПО и СрЗИ	Организационные меры
	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в ТРИС	ПО Xspider 7.8 Professional Edition, организационные меры

Таблица 4.2. Продолжение

Подсистема защиты ТС	Наличие организованной контролируемой зоны, в пределах которой постоянно размещаются стационарные ТС, обрабатывающие информацию, и СрЗИ	Реализация подсистемы защиты ТС организуется Эксплуатирующей организацией
	Возможность контроля и управления физическим доступом к ТС, СрЗИ, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, СрЗИ и средствам обеспечения функционирования ИС, в помещения и сооружения, в которых они установлены	
	Размещение устройств вывода информации АРМ и серверов ТРИС (мониторов, печатающих устройств) в помещениях, в которых они установлены, таким образом, чтобы была исключена возможность просмотра посторонними лицами текстовой и графической видовой информации	
Подсистема управления конфигурацией ИС и подсистемы информационной безопасности	Определение лиц, которым разрешены действия по внесению изменений в конфигурацию ТРИС и СЗИ	Реализация подсистемы управления конфигурацией ТРИС и СЗИ организуется Эксплуатирующей организацией, Dallas Lock 8.0-K
	Управление изменениями конфигурации ТРИС и подсистемы информационной безопасности	
	Анализ потенциального воздействия планируемых изменений в конфигурации ТРИС и СЗИ на обеспечение защиты информации и согласование изменений в конфигурации ТРИС с должностным лицом (работником ЗАО «ДИДЖИТАЛ ДИЗАЙН»), ответственным за обеспечение безопасности информации	
	Документирование информации (данных) об изменениях в конфигурации ТРИС и подсистемы информационной безопасности	
Подсистема обеспечения целостности ТРИС и информации	Контроль целостности ПО, включая ПО СрЗИ (СКЗИ)	Dallas Lock 8.0-K, Средства резервного копирования MS SQL, EMM SafePhone
	Контроль целостности информации, содержащихся в БД ТРИС	
	Обеспечение возможности восстановления ПО, включая ПО СрЗИ, при возникновении нештатных ситуаций	
Подсистема обеспечения доступности информации	Контроль безотказного функционирования ТС, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование	Организационные меры (просмотр журналов СрЗИ)

Таблица 4.2. Продолжение

	Использование отказоустойчивых ТС	Кластеры СрЗИ, АСО, резервирование каналов передачи информации организуется Эксплуатирующей организацией
	Резервирование ТС, ПО, каналов передачи информации, средств обеспечения функционирования ТРИС	
	Периодическое резервное копирование информации на резервные МН	Организуется Эксплуатирующей организацией
	Обеспечение возможности восстановления информации с резервных МН (резервных копий) в течение установленного временного интервала	Организуется Эксплуатирующей организацией
Подсистема выявления инцидентов и реагирования на них	Определение лиц, ответственных за выявление инцидентов и реагирование на них	Dallas Lock 8.0-K, Организационные меры
	Обнаружение, идентификация и регистрация инцидентов	
	Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в ТРИС пользователями и администраторами	
	Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий	
	Принятие мер по устранению последствий инцидентов	
	Планирование и принятие мер по предотвращению повторного возникновения инцидентов	

Таблица 4.2. Продолжение

Подсистема защиты среды виртуализации	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации	Резервное копирование среды виртуализации организуется Эксплуатирующей организацией, vGate R2, KES, KSC
	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин	
	Регистрация событий безопасности в виртуальной инфраструктуре	
	Реализация и управление антивирусной защитой в виртуальной инфраструктуре	
	Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки персональных данных отдельным пользователем и (или) группой пользователей	
	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных	
	Контроль целостности виртуальной инфраструктуры и ее конфигурации	
	Резервное копирование данных, резервирование ТС, ПО виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры	
Подсистема обеспечения сетевой безопасности	Реализация функции межсетевого экранирования в точках взаимодействия ТРИС между собой	Dallas Lock 8.0-K, АПКШ «Континент», «Континент – АП», EMM SafePhone
	Защита АСО и сетевой инфраструктуры ТРИС	
Подсистема централизованного управления средствами защиты информации	Управление СрЗИ	Серверы управления СрЗИ, KSC, Dallas Lock 8.0-K,ПО WSUS, EMM SafePhone
	Администрирование СрЗИ	
	Управление обновлениями ПО СрЗИ	
	Распространение исправлений ПО	
	Получение исправлений и иных обновлений безопасности ПО для централизованной установки на серверы и АРМ	

С помощью программы для ЭВМ «Оценка системы защиты информации», реализующей предложенный в настоящем диссертационном исследовании метод оценки эффективности СЗИ ТРИС, проводиться оценка эффективности проектных решений по защите информации Системы.

На рисунке 4.8 представлен интерфейс разработанной в настоящем диссертационном исследовании программы для ЭВМ «Оценка системы защиты информации».

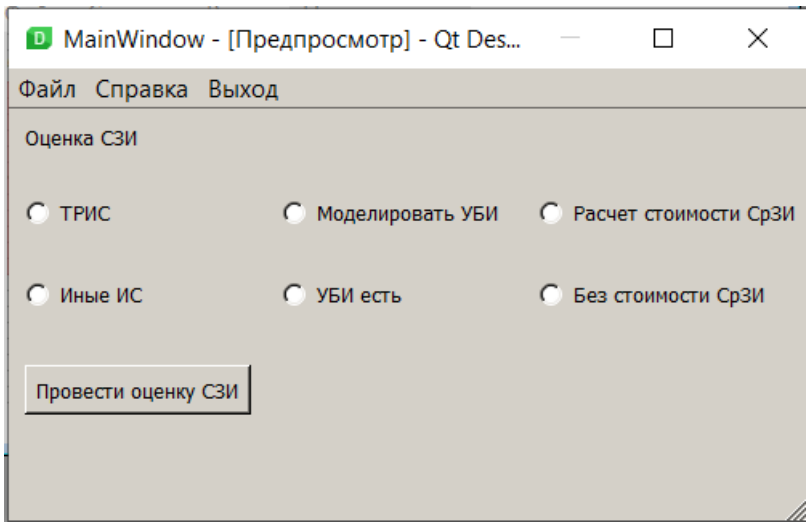


Рисунок 4.8 – Интерфейс программы для ЭВМ «Оценка системы защиты информации»

Фактически, оценка эффективности выполнялась следующим образом:

1. Формирование перечня актуальных ЦБИ выполнялось с помощью подготовки набора данных и с помощью программы для ЭВМ «Модель угроз и нарушителя», по результатам чего был сформирован перечень актуальных УБИ.
2. Проектирование СЗИ выполнялось экспертами по ИБ в соответствии с ГОСТ сери 34. В рамках настоящего диссертационного исследования не рассматривается отдельно и не является научным результатом.
3. Формирование набора данных для оценки эффективности СЗИ, получение экспертных оценок по выполнению требований по ИБ.
4. С помощью программы для ЭВМ «Оценка системы защиты информации» проведена оценка эффективности СЗИ исследуемой ТРИС.

Экспертным путем определяются оценки соответствия по требованиям ИБ. Результаты по 5 группам требований представлены в таблице 4.3.

Таблица 4.3 – Оценки экспертов по выполнению требований по ИБ

Эксперты	Оценки					
	ИАФ.3	УПД.4	РСБ.1	ЗТС.4	ЗИС.5	Итоговая оценка
Эксперт 1	0,7	1	1	1	0,7	0,88
Эксперт 2	1	1	1	0,5	0,5	0,8
Эксперт 3	0,5	0,7	1	0,7	0,5	0,68
Эксперт 4	0,7	1	1	0,7	0,5	0,78
Эксперт 5	0,7	0,7	1	0,7	0,7	0,76
	0,72	0,88	1	0,72	0,58	**0,78**

То есть,

$$A = \begin{bmatrix} 0,7 & 1 & 1 & 1 & 0,7 \\ 1 & 1 & 1 & 0,5 & 0,5 \\ 0,5 & 0,7 & 1 & 0,7 & 0,5 \\ 0,7 & 1 & 1 & 0,7 & 0,5 \\ 0,7 & 0,7 & 1 & 0,7 & 0,7 \end{bmatrix} = \begin{bmatrix} 0,88 \\ 0,8 \\ 0,68 \\ 0,78 \\ 0,76 \end{bmatrix} = 0,78$$

На основании результатов определения перечня актуальных УБИ и предполагаемых технических решений СЗИ ТРИС итоговая оценка эффективности СЗИ исследуемой ТРИС для перечня из 5 УБИ, 5 требований по ИБ и 5 СрЗИ рассчитывается следующим образом в соответствии с формулой 3.4:

$$W = (\frac{1+0+1+1+0}{5} + \frac{0,72+0,88+1+0,72+0,58}{5} + \frac{1+0+0+0+1}{5}) / 3 =$$
$$= (0,6+0,78+0,4) / 3 = 0,59$$

Для исследуемой ТРИС условно допустимым значением о достижении эффективности СЗИ, считается 0,85. Значение рассчитано, исходя из определенных рисков (киберрисков) в компании. Таким образом, текущая эффективность СЗИ (уровень защищенности системы) не соответствует заявленной владельцем ТРИС, т.е. эффективность СЗИ не достигается при условленной приемлемой для владельца ТРИС значения (квантиля). Результаты проведенной оценки были проанализированы и даны рекомендации по достижению приемлемого уровня защищенности исследуемой ТРИС.

Результаты проведенной оценки показали не эффективность предлагаемых решений по защите информации, а именно:

1. Проектные решения не учитывают нейтрализацию всех актуальных УБИ в Системе.
2. Эффективность СЗИ Системы можно повысить за счет уменьшения стоимости планируемых к закупке СрЗИ.

Для нейтрализации УБИ.121, УБИ.122, УБИ.124 в существующей СЗИ ТРИС не предусмотрены меры по защите информации, для части СрЗИ возможно уменьшение стоимости.

Результаты проведения оценки эффективности СЗИ Системы позволяют внести корректировки в проектные решения по СЗИ Системы на раннем этапе, что позволяет предотвратить возможные риски утечки данных и сэкономить финансовые затраты на создание СЗИ.

Следует отметить, что предложенные методика определения актуальных УБИ и метод оценки эффективности СЗИ предполагают установление владельцем ТРИС пороговых значений (квантилей) при определении актуальности УБИ и достижения необходимого уровня защищенности ТРИС.

Практическая реализация результатов настоящего диссертационного исследования в ЗАО «ДИДЖИТАЛ ДИЗАЙН» доказывает эффективность предложенной методики определения актуальных УБИ, метода и методических рекомендаций по оценке эффективности СЗИ ТРИС, что, в свою очередь, подтверждает выполнение поставленных в настоящей работе целей.

4.5. Оценка эффективности предложенных методических рекомендаций

Для оценки эффективности предложенных методических рекомендаций необходимо учитывать порядок проведения оценки с точки зрения требований ФСТЭК России [17-21], а также исходя из определения оценки эффективности и

требований владельцев ТРИС, описанных в настоящем диссертационном исследовании в разделе 4.1.

Под оценкой эффективности понимается следующее: эффективность СЗИ достигается путем создания СЗИ, способной максимально нейтрализовать актуальные УБИ в ТРИС, выполнить требования по защите информации, предъявляемые к ТРИС на основании требований регуляторов в области обеспечения безопасности информации, а также позволяющей снизить финансовые затраты на создание СЗИ.

Одной из форм оценки соответствия является аттестация ОИ. В соответствии с [36] аттестация ОИ делится на документальную проверку и инструментальный контроль. В связи с тем, что государственные информационное системы подлежат обязательной аттестации и с тем, что в данной диссертационном исследовании рассматриваются такие системы, в том числе, то выполнение требований ФСТЭК России является обязательным, как и условия нейтрализации актуальных УБИ в ТРИС. Одновременно с этим, в соответствии с требованиями регуляторов РФ по ИБ [17-21, 33-35] и требованиями владельцев ИС [59] показатели оценки финансовых затрат являются также обязательным. По условиям задачи, поставленных в настоящей работе, методика оценка эффективности СЗИ ТРИС должна быть применимой на всех этапах жизненного цикла ИС для своевременной возможности внесения изменений в проектные решения по защите информации. Предложенные показатели, методические рекомендации, а также предложенные в настоящей работе методики определения актуальных УБИ и метода оценки эффективности СЗИ позволяют проводить оценку эффективности СЗИ на всех этапах жизненного цикла ТРИС. В этой связи, поставленная в настоящем диссертационном исследовании цель по повышению качества оценки эффективности СЗИ ТРИС достигнута.

Выводы

Разработанные в главе 4 методические рекомендации по оценке эффективности систем защиты информации в территориально-распределенных информационных системах, в отличии от известных, позволяют владельцам ТРИС в режиме реального времени оценивать эффективность СЗИ, снижать финансовые затраты на создание систем защиты информации от 15 до 30%, сократить количество не учтенных актуальных угроз безопасности информации на 5%. Использование методических рекомендаций не требует привлечения высококвалифицированных специалистов по информационной безопасности, больших вычислительных ресурсов, эффективность систем защиты информации в территориально-распределенных информационных системах может достигать до 97%.

Предложенные методические рекомендации позволяют:

- учитывать все аспекты процесса проведения оценки эффективности СЗИ ТРИС;
- минимизировать проведение лишних и ненужных шагов оценки;
- учитывать при проведении оценки требования регуляторов РФ в области обеспечения безопасности информации;
- могут быть адаптированы под условия проведения оценки владельцев ТРИС;
- процесс автоматизирован, исключает недостатки экспертных методов, не требует привлечения высококвалифицированных специалистов в области ИБ.

Материалы главы 4 были представлены в материалах международных и российских научно-технических конференциях и опубликованы в изданиях, включенных в перечень ВАК при Минобрнауки России [59-61], а также в изданиях Scopus [54, 55]. Статья «Метод и методика оценки эффективности системы защиты

территориально-распределенных информационных систем» опубликована в издании, включенном в перечень ВАК при Минобрнауки России, без соавторства.

Заключение и выводы по работе

Поставленная в диссертационном исследовании цель по повышению качества оценки эффективности систем защиты информации территориально-распределенных информационных систем за счет определения необходимых и достаточных показателей **достигнута**.

Для достижения цели были поставлены и выполнены задачи, получены научные результаты, составляющие следующие итоги исследования:

1. Проведен анализ ТРИС: определены основные бизнес-процессы; информация, обрабатываемая в ТРИС; группы пользователей, имеющих доступ в ТРИС, их права и полномочия; выявлены основные аспекты технологии обработки информации; исследована ИТ-инфраструктура ТРИС (информационные технологий и программное обеспечение, реализующее бизнес-процессы ТРИС); проведен анализ атак и угроз безопасности информации в ТРИС, требований по защите информации в ТРИС; проведен анализ СЗИ ТРИС; анализ существующих методов и методик моделирования УБИ и оценки эффективности СЗИ ТРИС.

2. Предложена методика определения актуальных угроз безопасности информации, в отличие от известных, позволяющая в автоматизированном режиме формировать перечень актуальных УБИ, гипотетически исключая ошибки экспертов. Позволяющая определять большее количество актуальных УБИ, минимизировать трудоемкость процесса и вычислительные ресурсы.

3. Предложен метод оценки эффективности систем защиты информации, в отличие от известных, основанный на теории адаптивных нечетких нейронных продукционных системах и алгоритме нечеткого вывода Такаги-Сугено-Канга с применением технологий Data Science. Метод позволяет проводить оценку эффективности СЗИ на основе необходимых и достаточных показателей, определенных в настоящем диссертационном исследовании. RMSE работы системы ANFIS достигает наименьшего значения, что позволяет утверждать об эффективности работы метода и о достижении поставленной задачи.

4. Разработаны методические рекомендации по оценке эффективности систем защиты информации в территориально-распределенных информационных системах, в отличие от известных, позволяющие владельцам ТРИС в режиме реального времени выполнять оценку эффективности СЗИ, снижать финансовые затраты на создание системы защиты информации от 15 до 30%, сокращать количество не учтенных актуальных угроз безопасности информации на 5%. Использование методических рекомендаций не требует привлечения высококвалифицированных специалистов по информационной безопасности, больших вычислительных ресурсов, эффективность систем защиты информации в территориально-распределенных информационных системах достигает до 97%.

Разработанные методические рекомендации позволяют:

- учитывать все аспекты процесса проведения оценки эффективности СЗИ ТРИС;
- минимизировать проведение лишних и ненужных шагов оценки;
- учитывать при проведении оценки требования регуляторов РФ в области обеспечения безопасности информации;
- могут быть адаптированы под условия проведения оценки владельцев ТРИС;
- процесс автоматизирован, исключает недостатки экспертных методов, не требует привлечения высококвалифицированных специалистов в области ИБ.

5. Проведена оценка эффективности предложенных методики и метода.

Доказано, что предложенные методика и метод обладают большей эффективностью для решения задач, связанных с определением перечня актуальных УБИ и оценки эффективности СЗИ за счет определения необходимых и достаточных показателе. Определены наилучшие параметры работы адаптивной нечеткой нейронной продукционной системы с алгоритмом нечеткого вывода. Применены технологии Data Science при обработке большого объема данных.

Эффективность предложенных методики и метода подтверждается:

- достоверными результатами определения перечня актуальных угроз безопасности информации и достижения эффективности СЗИ;
- использованием минимальных вычислительных ресурсов;
- отсутствием необходимости привлечения высококвалифицированных специалистов в области ИБ;
- возможностью адаптации под конкретные цели владельцев ИС при проведении оценки эффективности СЗИ: выбором показателей, путем изменения параметров работы сети ANFIS и выбора алгоритма нечеткого вывода.

Все результаты, выносимые на защиту, являются новыми и подтверждаются актами об использовании результатов диссертационной работы (Приложение В, Г, Д, Е).

Основные результаты диссертационного исследования опубликованы в 16 печатных трудах, среди которых:

- 6 статей, опубликованных в изданиях, рекомендованных ВАК при Минобрнауки России, две из них без соавторства.
- 2 статьи, опубликованные в изданиях, входящих в перечень Scopus.
- Программа для ЭВМ «Модель угроз и нарушителя», номер регистрации 2020617876 от 15.07.2020 г. (Приложение А).
- программа для ЭВМ «Оценка системы защиты информации», номер регистрации 2020664343 от 11.11.2020 г. (Приложение Б).
- 6 статей, опубликованных в изданиях, входящих в перечень РИНЦ РФ.
- конкурс грантов для студентов вузов, расположенных на территории Санкт-Петербурга, аспирантов вузов, отраслевых и академических институтов, расположенных на территории Санкт-Петербурга (Диплом № 15542 от 27.11.2015 г.).
- Учебно-методическое пособие «Сертификация средств защиты информации» (Россия, Санкт-Петербург, СПбГУТ).
- тезисы докладов.

Сформулированы рекомендации по использованию результатов работы для выполнения производственных задач и в научных исследованиях. Предложенная методика определения актуальных угроз безопасности информации может использоваться при оценке рисков для активов организаций в соответствии с ИСО/МЭК серии 27х и иных стандартов по управлению рисками. Предложенный метод оценки эффективности СЗИ может использоваться для проведения аудита информационной безопасности в организациях и предприятиях на соответствие стандартам ИСО/МЭК серии 27х, а также при проведении аудита качества системы менеджмента в организациях на соответствие стандарту ИСО 9001. Разработанные методические рекомендации по оценке эффективности СЗИ ТРИС могут быть использованы для оценки соответствия в организациях подходам к управлению информационными технологиями COBIT 5, а также для управления жизненным циклом информационных систем с точки зрения проведения оценки состояния ИТ-инфраструктуры, парка АРМ, документации и т.д.

Дальнейшие научные исследования по теме диссертационного исследования целесообразно продолжить в следующих направлениях:

- в исследовании адаптивных нечетких нейронных продукционных систем, алгоритмов нечеткого вывода Такаги-Сугено-Канга, Такаги-Канга, Мамдани и Ванга-Менделя. Изменение параметров работы систем, уменьшения значений RMSE;
- в выборе показателей оценки эффективности СЗИ;
- в разработке и повышении качеств известных методов определения актуальных уязвимостей в ТРИС;
- в разработке и повышении качеств известных методов определения актуальных нарушителей в ТРИС;
- в разработке автоматизированных средств проектирования СЗИ ТРИС.

Все результаты, выносимые на защиту, сопоставлены с пунктами 1, 3 и 10 паспорта искомой специальности – «Методы и системы защиты информации, информационная безопасность»: «Теория и методология обеспечения

информационной безопасности и защиты информации», «Методы, модели и средства выявления, идентификации и классификации угроз нарушения информационной безопасности объектов различного вида и класса» и «Модели и методы оценки эффективности систем (комплексов) обеспечения информационной безопасности объектов защиты», соответственно.

Список сокращений и обозначений

АРМ	–	автоматизированное рабочее место
АСО	–	активное сетевое оборудование
АСУ ТП	–	автоматизированная система управления технологическими процессами
БДУ	–	банк данных угроз безопасности информации ФСТЭК России
ВАК	–	высшая аттестационная комиссия при Министерстве науки и высшего образования Российской Федерации
ВВ	–	внутренние возможности
ГИС	–	государственная информационная система
ИС	–	информационная система
ИСПДн	–	информационная система персональных данных
ИНС	–	искусственная нейронная сеть
ИТ	–	информационная технология
КЗ	–	контролируемая зона
КИИ	–	критическая информационная инфраструктура
МД	–	методический документ
МИО	–	международный информационный обмен
МН	–	машинный носитель
МЭДО	–	межведомственный электронный документооборот
НДВ	–	недекларированные возможности
НИР	–	научно-исследовательская работа
НП	–	негативные последствия
НСД	–	несанкционированный доступ
ОВ	–	объект воздействия
ОС	–	операционная система
ПАК	–	программно-аппаратный комплекс
СУБД	–	система управления базами данных

ПДн – персональные данные

ПО – программное обеспечение

РФ – Российская Федерация

СКЗИ – средство криптографической защиты информации

СЗИ – система защиты информации

СрЗИ – средство защиты информации

СУИБ – система управления информационной безопасностью

СФ – среда функционирования

ТЗ – техническое задание

ТС – технические средства

ТРИС – территориально-распределенная информационная система

УБИ – угроза безопасности информации

УИД – уникальный идентификатор

ФСБ – Федеральная служба безопасности Российской Федерации России

ФСО – Федеральная служба охраны Российской Федерации России

ФСТЭК – Федеральная служба по техническому и экспортному контролю России

BIOS – Basic Input/Output System (базовая система ввода/вывода)

CVE – Common Vulnerabilities and Exposures

CWE – Common Weakness Enumeration

DMZ – Demilitarized Zone

DMA – Direct Memory Access

IaaS – Infrastructure-as-a-Service

IDM – Identity management

IDS – Intrusion Detection System

IEC – International Electrotechnical Commission

IPS – Intrusion Prevention System

ISO – International Organization for Standardization

OWA – Outlook Web App

OWASP – Open Web Application Security Project

PaaS – Platform-as-a-Service

SaaS – Software-as-a-Service

SCRM – Social Customer Relationship Management

SIEM – Security Information and Event Management

SMB – Server Message Block

SSH – Secure Shell

Список используемой литературы

1. Доктрина информационной безопасности Российской Федерации, утверждена Указом Президента Российской Федерации 5 декабря 2016 г. № 646. – 2016. – 16 С.
2. Гвоздик Я.М. Модель и методика оценки систем защиты информации автоматизированных систем: дисс. канд. техн. наук: 05.13.19 / СПИИРАН. – Санкт-Петербург. – 2011. – 137 С.
3. Десятов А.Д. Моделирование процессов защиты информации в распределенных информационных системах органов внутренних дел: дисс. канд. техн. наук: 05.13.18 / Воронежский институт МВД России. – Воронеж. – 2006. – 134 С.
4. Коломойцев В.С. Модели и методы оценки эффективности систем защиты информации и обоснование выбора их комплектации.: дисс. канд. техн. наук: 05.13.19 / Университет ИТМО. – Санкт-Петербург. – 2018. – 175 С.
5. Чемин А.А. Разработка методов оценки эффективности систем защиты информации в распределенных информационных системах специального назначения: дисс. канд. техн. наук: 05.13.19 / ФГОУ «Московский государственный институт электроники и математики» (Технический университет). – Москва. – 2009. – 211 С.
6. Лившиц И.И. Модели и методы аудита информационной безопасности интегрированных систем управления сложными промышленными объектами: дисс. доктора техн. Наук: 05.13.19 / СПИИРАН. – Санкт-Петербург. – 2018. – 407 С.
7. Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
8. Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»;
9. Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
10. Федеральный закон Российской Федерации от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
11. Указ Президента Российской Федерации от 17.03.2008 №351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

12. Постановление Правительства Российской Федерации 11 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
13. Постановление Правительства Российской Федерации 8 февраля 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений (с изменениями от 13 апреля 2019 г.).
14. Приказ Министерства связи и массовых коммуникаций Российской Федерации и Федеральной службы охраны Российской Федерации от 27 мая 2015 года № 186/258 «Об утверждении Требований к организационно-техническому взаимодействию государственных органов и государственных организаций посредством обмена документами в электронном виде».
15. Приказ Федеральной службы безопасности Российской Федерации от 10 июля 2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».
16. Приказ ФСО России от 7 сентября 2016 г. № 443 «Об утверждении положения о Российском государственном сегменте информационно-телекоммуникационной сети «Интернет».
17. Приказ ФСТЭК России от 11 февраля 2013 г. №17 «Об утверждении требований о защите информации, не содержащей государственную тайну, содержащейся в государственных информационных системах».
18. Приказ ФСТЭК России от 14 марта 2014 г. №31 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».
19. Приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

20. Приказ ФСТЭК России от 31 августа 2010 г. № 489 «Об утверждении требований по защите информации, содержащейся в информационных системах общего пользования».
21. Приказ ФСТЭК России от 18 февраля 2013 года №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
22. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (Выписка) (утв. ФСТЭК России 15.02.2008).
23. Методический документ ФСБ России «Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности» (утв. руководством 8 Центра ФСБ России от 31 марта 2015 г. № 149/7/2/6-432).
24. Методический документ ФСТЭК России «Меры защиты информации в государственных информационных системах» (утв. приказом ФСТЭК России 11 февраля 2014 г.).
25. Методический документ ФСТЭК России «Методика оценки угроз безопасности информации» (утв. приказом ФСТЭК России 05 февраля 2021 г.).
26. Руководящий документ Гостехкомиссии России «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации».
27. Руководящий документ Гостехкомиссии России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации».
28. Руководящий документ Гостехкомиссии России «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации».
29. Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий (выписка), (утв. приказом ФСТЭК России от 02 июня 2020 г. № 76).

30. Положение о сертификации средств защиты информации по требованиям безопасности информации, утвержденное приказом Гостехкомиссии России от 03.04.2018 №55.
31. Государственный реестр сертифицированных средств защиты информации в системе сертификации средств защиты информации по требованиям безопасности информации № РОСС RU.ООО1.О1БИОО.
32. Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденное приказом ФСБ России от 09.02.2005 № 66.
33. ГОСТ 34.601-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания».
34. ГОСТ Р 51583-2014. Национальный стандарт Российской Федерации. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения.
35. ГОСТ Р 51583-2014. «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения».
36. Положение по аттестации объектов информатизации по требованиям безопасности информации, утвержденное приказом Гостехкомиссии России от 25.11.1994.
37. ГОСТ Р ИСО/МЭК 15408-1-2012 «Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Введение и общая модель».
38. ГОСТ Р ИСО/МЭК 15408-2-2013 «Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Функциональные компоненты безопасности».
39. ГОСТ Р ИСО/МЭК 15408-3-2013 «Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Компоненты доверия к безопасности».
40. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.
41. ГОСТ Р ИСО/МЭК 27033-1-2011: Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции.
42. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения.
43. СТО БР ИББС-1.2-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской

системы Российской Федерации требованиям СТО БР ИББС-1.0-2014». М.: Стандарт Банка России. – 2014. – С. 101.

44. СТО БР ИББС-1.1-2007 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Аудит информационной безопасности СТО БР ИББС-1.1-2007». М.: Стандарт Банка России. – 2007. – С. 14.
45. NIST SP 800-25, Federal Agency Use of Public Key Technology for Digital Signatures and Authentication. – October 2000. [Электронный ресурс] – Режим доступа к рес.: http://csrc.nist.gov/publications/nistir/ir7497/nistir-7497.pdf (дата обращения: 18.03.21).
46. NIST SP 800-30, Risk Management Guide for Information Technology Systems. – January 2002. [Электронный ресурс] – Режим доступа к рес.: http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol2-Rev1.pdf (дата обращения: 11.02.21).
47. CRAMM (CCTA Risk Analysis and Management Method) [Электронный ресурс]. URL: http://rm-inv.enisa.europa.eu/methods/m_cramm.html (дата обращения 13.01.21).
48. Standard: Department of Defense Trusted Computer System Evaliation Criteria, TCSEC, DoD 5200.28-STD, December 26, 1985. P. 116. [Электронный ресурс] – Режим доступа к рес.: http://csrc.nist.gov/publications/history/dod85.pdf (дата обращения: 14.07.21).
49. Шон Харрис. «CISSP All-in-One Exam Guide» / McGraw-Hill Osborne Media. – 2005. – С 875.
50. Саати Т. Принятие решений. Метод анализа иерархий. М.: Радио и связь. – 1993. – 278 С.
51. Петренко С.А., Симонов С.В. Экономически оправданная безопасность. М.: Изд. ДМК. – 2003. – 218 С.
52. Зегжда Д.П., Ивашко А.М. Как построить защищенную информационную систему. СПб.: НПО «Мир и семья-95». – 1997. – 312 С.
53. Барабанов А.В., Дорофеев А.В., Марков А.С., Цирлов В.Л. Семь безопасных информационных технологий / под ред. А.С. Маркова.- М.: ДМК Пресс. – 2017. – 224 С.: ил.
54. I.I. Livshitz, D.V. Yurkin, A.A. Minyaev. Formation of the Instantaneous Information Security Audit Concept // Communications in Computer and Information Science. – 2016, Vol. 678. – pp. 314-324.
55. Minyaev A. Andrey, Krasov V. Andrey, Saharov V. Dmitriy. The Method and Methodology of efficiency assessment of protection system of distributed information systems. Institute of Electrical and Electronics Engineers – 2020, pp. 291-295.

56. Миняев А.А, Будько М.Ю. Метод оценки эффективности системы защиты персональных данных // Информатизация и связь. – 2016. № 2. – С. 85-87.
57. Миняев А.А., Будько М.Ю. Метод оценки эффективности системы защиты информации территориально распределенных информационных систем // Информатизация и связь. – 2017. № 3. – С. 119-121.
58. **Миняев А.А.** Моделирование угроз безопасности информации в территориально-распределенных информационных системах // Наукоемкие технологии в космических исследованиях Земли. – 2021. № 2. – С 52-65.
59. **Миняев А.А.** Метод и методика оценки эффективности системы защиты территориально-распределенных информационных систем // Информатизация и связь. – 2020. № 6. – С. 29-36.
60. Миняев А.А., Красов А.В. Методика оценки эффективности системы защиты информации территориально-распределенных информационных систем// Вестник СПГУТД. № 3. – 2020. – С. 26-32.
61. Миняев А.А., Красов А.В., Сахаров Д.В. Метод оценки эффективности системы защиты информации территориально-распределенных информационных систем персональных данных // Вестник СПГУТД. № 1. – 2020. – С. 29-33.
62. Миняев А.А. Разработка системы защиты информации территориально-распределенных информационных систем // X Юбилейная Международная научно-техническая и научно-методическая конференция «Актуальные проблемы инфотелекоммуникаций в науке и образовании»: Сборник научных статей. – 2021. – С. 597-600.
63. Миняев А.А., Будько М.Ю. Методика оценки эффективности системы защиты персональных данных информационной системы // Проблема комплексного обеспечения информационной безопасности и совершенствование образовательных технологий подготовки специалистов силовых структур: Межвузовский сборник трудов VI Всероссийской научно-технической конференции (ИКВО НИУ ИТМО, 10 декабря 2015 г.). – 2016. – С. 43-45.
64. Маслова Н.А. Методы оценки эффективности систем защиты информационных систем // Искусственный интеллект, 2008, С. 253-264.
65. Десницкий В.А., Сахаров Д.В., Чечулин А.А., Ушаков И.А., Захарова Т.Е, Защита информации в центрах обработки данных, Санкт-Петербург. – 2019.
66. Котенко Д.И., Котенко И.В., Саенко И.Б. Методика итерационного моделирования атак в больших компьютерных сетях // Труды СПИИРАН. – 2012. Вып. 4 (23). ISSN 2078-9599. – С. 50-79.

67. Росс Г.В. Моделирование производственных и социально-экономических систем и использованием аппарата комбинаторной математики. – М.: Мир, – 2001. – 176 С.
68. Заде, Л. Понятие лингвистической переменной и его применение к принятию приближенных решений [Текст] / Л. Заде, под ред. Н.Н. Моисеева, С.А. Орловского; пер. с англ. – М.: Мир. – 1976. – 168 С.
69. Ярушкина, Н. Г. Основы теории нечетких и гибридных систем: Учебное пособие. – М.: Финансы и статистика. – 2004. – 320 С.
70. Круглов В.В., Дли М.И., Годунов Р.Ю. Нечеткая логика и искусственные нейронные сети. – М.: Физматлит. – 2001. – 224 С.
71. Круглов В.В. Искусственные нейронные сети. Теория и практика / В.В. Круглов, В.В. Борисов.- М.: Горячая линия – Телеком. – 2002. – 382 С.
72. Б.Я. Советов, С.А. Яковлев. Моделирование систем: учеб. для вузов – 3-е изд., перераб. И доп. – М.: Высш. шк., – 2001. – 343 с.: ил.
73. Власенко В.Д. Динамическое и стохастическое программирование. Хабаровск: Изд-во Тихоокеан. гос. ун-та, – 2008. – 35 С.
74. А.А. Барсегян, М.С. Куприянов, В.В. Степаненко, И.И. Холод. Методы и модели анализа данных: OLAP и Data Mining. – СПб.: БХВ-Петербург. – 2004, – 336 С.
75. С. Осовский. Нейронные сети для обработки информации / Пер. с польского И.Д. Рудинского. – М.: Финансы и статистика, – 2002. – 344 С.: ил.
76. Хижняков Ю.Н. Алгоритмы нечеткого, нейронного, нейро-нечеткого управления в системах реального времени. Пермь: ПНИПУ, – 2013. – 160 С.
77. Люгер, Д.Ф. Искусственный интеллект: стратегии и методы решения сложных проблем, 4-е издание. – Издательский дом Вильямс. - 2003. - 864 С.
78. Попов, Э.В. Экспертные системы: Решение неформализованных задач в диалоге с ЭВМ. - М.: Наука. – 1987. – 288 С.
79. Адлер, Ю.П. Планирование эксперимента при поиске оптимальных условий. – Рипол Классик. – 1976. – 279 С.
80. Шепитько Г. Е. Комплексная система защиты информации на предприятии. Часть1. Учебное пособие / Г. Е. Шепитько, А. А. Локтев, Г. Н. Гудов. – М.: МФЮА, – 2008, – 127 С.
81. Романовская А.М., Мендзин М.В. Динамическое программирование. Омск: Омский институт (филиал) РГТЭУ, – 2010. – 58 С.
82. Барабанов А.В., Дорофеев А.В., Марков А.С., Цирлов В.Л. Семь безопасных информационных технологий / под ред. А.С. Маркова.- М.: ДМК Пресс, – 2017. – 224 с.: ил.
83. Юсупов Р. М. Наука и национальная безопасность // 2-е издание, переработанное и дополненное. - СПб.: Наука, – 2011. – 369 С.

84. Ярочкин В.И. Информационная безопасность. Учебник для вузов. – Академический проект, Мир, Серия: Gaudeamus Ось-98, – 2008, – 544 С.
85. Карманов, В.Г. Математическое программирование. – М.: Наука. – 1980. – 256 С.
86. Рутковская, Д., Рутковский, Л., Пилиньский, М. Нейронные сети, генетические алгоритмы и нечеткие системы. – М.: Горячая линия-Телеком. – 2003. – 384 С.
87. Штовба С. Д. Fuzzy Logic Toolbox. Введение в теорию нечётких множеств. URL: http://matlab.exponenta.ru/fuzzylogic/book1/ (дата обращения: 17.05.21).
88. Андрианов В.И., Красов А.В., Липатников В.А. Инновационное управление рисками информационной безопасности. Санкт-Петербург: СПбГУТ, – 2012. – 396 с.
89. Бухарин В.В., Липатников В.А., Сахаров Д.В. Метод управления информационной безопасностью организации на основе процессного подхода // Информационные системы и технологии. – 2013. № 3 (77). – С. 102-109.
90. Mead, N., Shull, F., Vemuru, K., & Villadsen, O. A. Hybrid Threat Modeling Method. CMU/SEI-2018-TN-002. Software Engineering Institute, Carnegie Mellon University. – 2018. [http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=516617]. (date of access 15.06.21).
91. Khan, R.; McLaughlin, K.; Laverty, D.; & Sezer, Sakir. STRIDE-based Threat Modeling for Cyber-Physical Systems. In Proceedings of the 2017 IEEE PES Innovative Smart Grid Technologies Conference Europe. – 2017. DOI 10.1109/ISGTEurope.2017.8260283. (date of access 15.06.21).
92. Nataliya Shevchenko, Timothy A. Chick, Paige O'Riordan, Thomas Patrick Scanlon, PhD, & Carol Woody, PhD. Threat modelling: A summary of available methods. Carnegie Mellon University Software Engineering Institute, – 2018, – pp. 1-24.
93. Yue Li, Teng Zhang, Xue Li, and Ting Li. A Model of APT attack Defense Based On Cyber Threat Detection, Communications in Computer and Information Science, Cyber Security,15th International Annual Conference, CNCERT. – 2018, – pp. 122-134.
94. X. Cao and N. Z. Gong. Mitigating Evasion Attacks to Deep Neural Networks via Region-based Classification. Proceedings of the 2017 Annual Computer Security Applications Conference (ACSAC). ACM, – 2017, – pp. 278–287.
95. P. Mohassel and Y. Zhang. SecureML: A System for Scalable PrivacyPreserving Machine Learning. Proceedings of the 2017 IEEE Symposium on Security and Privacy (S&P). IEEE, – 2017, – pp. 19–38.

96. **Миняев А.А.** Метод оценки эффективности системы защиты информации территориально-распределенных информационных систем персональных данных. // IX Международная научно-техническая и научно-методическая конференция «Актуальные проблемы инфотелекоммуникаций в науке и образовании»: Сборник научных статей, СПбГУТ, – 2020. – С. 716-719.
97. Kuznetsov I.A., Lipatnikov V.A., Sakharov D.V. Integrated structure management with safety status forecasting // Telecommunication. – 2016. No. 3. – pp. 28-36.
98. Pronosa A.A., Vitkova L.A., Chechulin A.A., Kotenko I.V., Sakharov D.V. Methodology for disseminating information channels analysis in social networks // Vestnik of Saint Petersburg University. Applied Mathematics. Computer Science. Control Processes, – 2018. Vol. 14. iss. 4. – pp. 362-377.
99. Agrawal, A.; Ahmed, C. M.; & Chang, E. Poster: Physics-Based Attack Detection for an Insider Threat Model in a Cyber-Physical System. In Proceedings of the 2018 on Asia Conference on Computer and Communications Security, – 2018, DOI 10.1145/3196494.3201587, – pp. 821-823.
100. Ковцур М.М., Миняев А.А., Потемкин П.А., Хамза Д.Д. Обеспечение информационной безопасности Web-приложений с использованием машинного обучения. // IX Международная научно-техническая и научно-методическая конференция «Актуальные проблемы инфотелекоммуникаций в науке и образовании»: Сборник научных статей, СПбГУТ, – 2020. – С. 597-601.
101. Миняев А.А., Юркин Д.В., Ковцур М.М., Ахрамеева К.А. Сертификация средств защиты информации: учебное пособие. СПбГУТ. – СПб., – 2020. – 80 С.
102. Standard: ISO/IEC 27001 - Titles: The Information Security Standard. Renamed in 2007. [Электронный ресурс] – Режим доступа к рес.: http://www.itgovernance.co.uk/iso27001.aspx (дата обращения: 02.08.21).
103. ISO/IEC 13335-1: 2004 Information technology — Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management (IDT). [Электронный ресурс] – Режим доступа к рес.: http://www.iso27001security.com/html/others.html (дата обращения: 02.08.21).
104. Галатенко В.А. Стандарты информационной безопасности. Под ред. академика В.Б. Бетелина. – М.: ИНТУИТ.РУ, – 2004, – 328 С.
105. Minyaev A.A., Livshitz I.I., Yurkin D.V. Method of assessment of efficiency of the system of protection of personal data // Распределенные компьютерные и телекоммуникационные сети: управление, вычисление, связь (DCCN-2017, Москва, 25–29 сентября 2017 г.), – 2017. – С. 552-555.

106. Владыко А.Г. Оценка уровня защищенности информационной системы на основе мягких вычислений. – СПб.: Северо-Западный государственный заочный технический университет, – 2011, – 40 С.

107. Буйневич М.В., Покусов В.В., Израилов К.Е. Модель угроз информационно-технического взаимодействия в интегрированной системе защиты информации // Информатизация и связь, – 2021, № 4. – С. 66-73.

Приложение А

Сведения о регистрации программы для ЭВМ «Модель угроз и нарушителя»

21.10.2020 ПрЭВМ №2020617876

РОССИЙСКАЯ ФЕДЕРАЦИЯ

RU 2020617876

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ
(12) **ГОСУДАРСТВЕННАЯ РЕГИСТРАЦИЯ ПРОГРАММЫ ДЛЯ ЭВМ**

Номер регистрации (свидетельства): **2020617876** Дата регистрации: **15.07.2020** Номер и дата поступления заявки: **2020616749 29.06.2020** Дата публикации: **15.07.2020**	Авторы: **Красов Андрей Владимирович (RU), Миняев Андрей Анатольевич (RU), Пешков Андрей Иванович (RU)** Правообладатель: **Федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича» (СПбГУТ) (RU)**

Название программы для ЭВМ:
«Модель угроз и нарушителя»

Реферат:
Программа предназначена для автоматизации процесса определения актуального нарушителя и моделирования угроз безопасности информации для информационных систем и позволяет классифицировать информационную систему и рассчитывать её исходную защищенность от потенциального нарушителя, а также определять актуальные угрозы безопасности информации. Программа может применяться для защиты информации учреждений и организаций. Программа обеспечивает выполнение следующих функций: ввод исходных данных для классификации информационной системы; ввод информации для расчета исходной защищенности; определение потенциального нарушителя; определение перечня актуальных угроз безопасности информации. Тип ЭВМ: процессоры с тактовой частотой не ниже 1,2 ГГц ОС: Windows X SP3/Vista/7/8/10 и выше.

Язык программирования: VBA

Объем программы для ЭВМ: 27,7 Кб

Приложение Б

Сведения о регистрации программы для ЭВМ «Оценка системы защиты информации»

03.12.2020 ПрЭВМ №2020664343

РОССИЙСКАЯ ФЕДЕРАЦИЯ

RU 2020664343

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ
(12) **ГОСУДАРСТВЕННАЯ РЕГИСТРАЦИЯ ПРОГРАММЫ ДЛЯ ЭВМ**

Номер регистрации (свидетельства): **2020664343** Дата регистрации: **11.11.2020** Номер и дата поступления заявки: **2020663630 03.11.2020** Дата публикации: **11.11.2020**	Авторы: **Красов Андрей Иванович (RU), Миняев Андрей Анатольевич (RU), Пешков Андрей Иванович (RU), Ушаков Игорь Александрович (RU)** Правообладатель: **Федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича» (RU)**

Название программы для ЭВМ:
«Оценка систем защиты информации»

Реферат:
Программа предназначена для определения оценки эффективности систем защиты информации информационных систем. Область применения связана с государственными информационными системами, объектами критической информационной инфраструктуры, информационными системами, обрабатывающими конфиденциальную информацию. Обладает функциональными возможностями определения класса, категории значимости, уровня защищенности информационной системы.

Язык программирования: Python 3

Объем программы для ЭВМ: 74 КБ

Приложение В

Копия Акта использования результатов исследования в ЗАО «ДИДЖИТАЛ ДИЗАЙН»

DIGITAL DESIGN
мы делаем мир разумнее!

УТВЕРЖДАЮ
Генеральный директор
ЗАО «ДИДЖИТАЛ ДИЗАЙН»
к.т.н., Лившиц Д.Е.
_____
«__» февраля 2021 г.

АКТ

об использовании результатов диссертационной работы
Миняева Андрея Анатольевича на тему:
«Методика оценки эффективности системы защиты территориально-распределенных информационных систем»

Комиссия в составе: председателя комиссии-генерального директора ЗАО «ДИДЖИТАЛ ДИЗАЙН», к.т.н. Лившица Д.Е., руководителя направления системной интеграции Лучко Д.С., руководителя юридического отдела Матисовой А. Л., составила настоящий Акт том, что результаты диссертационной работы Миняева Андрея Анатольевича, а именно:

1. Методика определения актуальных угроз безопасности информации;
2. Метод оценки эффективности системы защиты информации;
3. Методические рекомендации по оценке эффективности системы защиты территориально-распределенных информационных систем.

используются в ЗАО «ДИДЖИТАЛ ДИЗАЙН» при организации работ по защите информации в информационных системах Общества.

Комиссия отмечает практическую значимость и новизну полученных в работе результатов.

Председатель комиссии: Лившиц Д.Е.

Члены комиссии: Лучко Д.С.
Матисова А.Л.

199178, Санкт-Петербург
наб. реки Смоленки, 33
+7 (812) 346-58-33
+7 (812) 346-58-34

115230, Москва
Варшавское шоссе, 36,
стр. 8, подъезд 5
+7 (499) 788-74-94
+7 (499) 788-74-95

www.digdes.ru
info@digdes.ru

Приложение Г

Копия Акта использования результатов исследования в ООО «Рэйдикс»

199178, Санкт-Петербург, ВО, наб. реки Смоленки, д.33
Телефон: +7 (812) 622 16 80
www.raidix.ru
info@raidix.com

УТВЕРЖДАЮ

Генеральный директор
ООО «Рэйдикс»
Федоров А.Р.

«02» февраля 2021 г.

АКТ
об использовании результатов диссертационной работы
Миняева Андрея Анатольевича
«Методика оценки эффективности системы защиты территориально-распределенных информационных систем»

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

1. Методика определения актуальных угроз безопасности информации;
2. Метод оценки эффективности системы защиты информации;
3. Методические рекомендации по оценке эффективности системы защиты территориально-распределенных информационных систем.

используются в ООО «Рэйдикс» при проведении работ по обеспечению безопасности информации в территориально-распределенной информационной системе организации.

Председатель комиссии: Федоров А.Р.

Члены комиссии: Разумовский С.Г.

Платонов С.М.

Приложение Д

Копия Акта использования результатов исследования в ЗАО НПФ «УРАН»

ЗАО НПФ «УРАН»

198099, Россия, Санкт-Петербург, Промышленная ул., д.5, оф.416

www.uran-spb.ruinfo@uran-spb.ru (812) 335-09-75

«УТВЕРЖДАЮ»
Генеральный директор
ЗАО НПФ «УРАН»
Лучко С.С.
«4» февраля 2021 г.

АКТ

об использовании результатов диссертационной работы
Миняева Андрея Анатольевича на тему:
«Методика оценки эффективности системы защиты территориально-распределенных информационных систем»

Комиссия в составе:

- председателя комиссии – генерального директора, Лучко С. С.;
- руководителя направления оптики, Черепова В. Е.;
- руководителя направления координатно-измерительных машин, Абрамова А.А.

составила настоящий Акт том, что результаты диссертационной работы Миняева Андрея Анатольевича, а именно:

1. методика определения угроз безопасности информации;
2. метод оценки эффективности системы защиты информации;
3. методические рекомендации по оценке эффективности системы защиты территориально-распределенных информационных систем.

используются в ЗАО НПФ «УРАН» при организации мероприятий по защите информации в информационных системах общества.

Комиссия отмечает практическую значимость и новизну полученных в работе результатов.

Председатель комиссии: Лучко С. С.

Члены комиссии: Черепов В. Е.
Абрамов А.А.

Приложение Е

Копия Акта использования результатов исследования в «Санкт-Петербургском государственном университете телекоммуникаций им. проф. М.А. Бонч-Бруевича»

МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА» (СПбГУТ)

Санкт-Петербург

УТВЕРЖДАЮ
Первый проректор - проректор по учебной работе
д.т.н., проф. Г. М. Машков
«19» 03 2021 г.

Акт

об использовании результатов диссертационной работы
Миняева Андрея Анатольевича
«Методика оценки эффективности системы защиты территориально-распределенных информационных систем» в учебном процессе университета

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

- методика определения актуальных угроз безопасности информации;
- метод оценки эффективности системы защиты информации;
- методические рекомендации по оценке эффективности системы защиты территориально-распределенных информационных систем

используются кафедрой защищенные системы связи федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича» в учебном процессе на старших курсах обучения бакалавров по направлению подготовки 10.03.01 «Информационная безопасность» по дисциплине «Методы оценки безопасности компьютерных систем» (рабочая программа дисциплины, регистрационный № 18.05/1185-Д) и магистров первого года обучения по направлению подготовки 10.04.01 «Информационная безопасность» по дисциплине «Сертификация средств защиты информации» (рабочая программа

дисциплины, регистрационный № 20.05/330-Д) при чтении курсов лекций, проведении практических занятий и лабораторных работ.

Председатель комиссии:

заведующий кафедрой ЗСС,
к.т.н., доцент — Красов Андрей Владимирович

Члены комиссии:

учёный секретарь кафедры ЗСС,
к.т.н., доцент — Кушнир Дмитрий Викторович

старший преподаватель
кафедры ЗСС, к.т.н. — Ушаков Игорь Александрович

старший преподаватель
кафедры ЗСС — Гельфанд Артем Максимович