ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ ЯРОСЛАВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ П.Г. ДЕМИДОВА

На правах рукописи

Овченков Николай Иванович

МОДЕЛИ И МЕТОДЫ ИНФОРМАЦИОННОГО УПРАВЛЕНИЯ ТРАНСПОРТНОЙ БЕЗОПАСНОСТЬЮ АЭРОПОРТА

Том 1

2.9.6 – «Аэронавигация и эксплуатация авиационной техники»
(технические науки)

Диссертация
на соискание ученой степени
доктора технических наук

Научный консультант:

доктор технических наук, доцент

Борзова Анжела Сергеевна

Москва – 2024

ОГЛАВЛЕНИЕ

Том 1

ВВЕДЕНИЕ 6

ГЛАВА 1 АНАЛИЗ ПРОБЛЕМ ОБЕСПЕЧЕНИЯ ТРАНСПОРТНОЙ БЕЗОПАСНОСТИ АЭРОПОРТОВ 20

1.1 Эволюция систем безопасности в гражданской авиации 20

1.2 Организация системы обеспечения безопасности аэропорта 25

1.3 Анализ проблем обеспечения и управления транспортной безопасностью аэропорта 31

1.4 Анализ угроз безопасности аэропортовой деятельности 37

1.5 Анализ проблем уязвимости аэропорта 46

1.6 Анализ проблем несанкционированного вмешательства персонала в производственную деятельность аэропорта 51

1.7 Обоснование научной задачи диссертационного исследования 63

Выводы к главе 1 70

ГЛАВА 2 ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ АЛГОРИТМИЧЕСКОЙ СОВМЕСТИМОСТИ ИНФОРМАЦИОННОГО МЕНЕДЖМЕНТА И ОПТИМАЛЬНОГО УПРАВЛЕНИЯ ТРАНСПОРТНОЙ БЕЗОПАСНОСТЬЮ АЭРОПОРТА 72

2.1 Управление как исключающая альтернатива обеспечению транспортной безопасности 72

2.2 Принципы информационного управления транспортной безопасностью 79

2.3 Интеллектуальное сопровождение процессов и процедур информационного управления безопасностью 86

2.4 Интеллектуальные технологии для решения задач информационного управления безопасностью 90

2.5 Краевые задачи теории поля для интеллектуального анализа безопасности 99

2.6 Нейронные сети как инструмент интеллектуального анализа 102

Выводы к главе 2 122

ГЛАВА 3 МЕТОДЫ РЕШЕНИЯ ПРОБЛЕМЫ «УПРАВЛЯЕМОСТЬ ТРАНСПОРТНОЙ БЕЗОПАСНОСТИ АЭРОПОРТА» НА ОСНОВЕ ИНФОРМАЦИОННО-УПРАВЛЯЮЩЕГО ПРОСТРАНСТВА 124

3.1 Концепция информационной управляемости транспортной безопасности аэропорта 124

3.2 Пространственно-ситуационный подход к управлению транспортной безопасностью 130

3.3. Информационно-управляющее пространство и его кластеризация . 137

3.4. Иерархия моделей эксплуатации информационно-управляющего пространства 151

3.5 Методы снижения негативного влияния персонала на транспортную безопасность аэропорта 157

3.6 Ситуационная модель управления несанкционированным вмешательством персонала 164

3.7 Конфликт интересов в системе управления безопасностью 168

Выводы к главе 3 173

ГЛАВА 4 МОДЕЛИРОВАНИЕ И ОПТИМИЗАЦИЯ ПРОСТРАНСТВА БЕЗОПАСНОСТИ АЭРОПОРТА 176

4.1 Уязвимость объекта транспортной инфраструктуры как критерий оптимизации информационного управления безопасностью 176

4.2 Моделирование пространства угроз безопасности аэропорта (стационарная задача) 183

4.3 Моделирования пространства уязвимостей аэропорта (нестационарная задача) 193

4.4. Нейросетевое ранжирование аэропортов по критерию уязвимость (экспериментальный шаблон)..... 200

Выводы к главе 4 216

ГЛАВА 5 НЕЙРОСЕТЕВЫЕ МОДЕЛИ ДЛЯ ПАРИРОВАНИЯ УГРОЗ НЕСАНКЦИОНИРОВАННОГО ВМЕШАТЕЛЬСТВА ПЕРСОНАЛА ТРАНСПОРТНОЙ БЕЗОПАСНОСТИ..... 218

5.1 Несанкционированное вмешательство персонала как фактор угрозы безопасности объекта защиты..... 218

5.2 Моделирование процедур минимизации несанкционированного вмешательства персонала 228

5.3 Информационное управление негативным влиянием персонала.... 241

5.4 Разработка нейросетевого классификатора персонала по критерию профессиональной готовности 251

5.5 Разработка автономных программных средств нейросетевой классификации персонала..... 264

Выводы к главе 5 292

ЗАКЛЮЧЕНИЕ 295

СПИСОК СОКРАЩЕНИЙ И УСЛОВНЫХ ОБОЗНАЧЕНИЙ 299

СПИСОК ЛИТЕРАТУРЫ 302

Том 2

ПРИЛОЖЕНИЕ А Моделирование угроз безопасности аэропорта в формате дифференциальных уравнений в частных производных для стационарной задачи (обязательное)

ПРИЛОЖЕНИЕ Б Моделирование угроз безопасности аэропорта в формате дифференциальных уравнений в частных производных для нестационарной задачи (обязательное)

ПРИЛОЖЕНИЕ В Нейросетевое ранжирование аэропортов (справочное)

ПРИЛОЖЕНИЕ Г Нейросетевая оценка уровня готовности персонала (справочное)

ВВЕДЕНИЕ

Актуальность работы. Современные транспортные системы занимают одно из ведущих мест в организационно-управленческой структуре государства, динамично развиваются и требуют постоянного внимания к решению возникающих специфических проблем. Одной из важнейших характеристик транспорта и критерием его существования является безопасность, поскольку отсутствие (снижение) приемлемого уровня таковой ставит под сомнение вопрос об эффективности предоставления транспортных услуг.

Общее понятие безопасности содержится в Федеральном законе «О безопасности» от 28.12.2010 № 390-ФЗ: «Безопасность – состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз». Безопасность – это многозначное понятие, которое характеризует низкий уровень риска для человека, общества или любых других субъектов, объектов или их систем. Безопасность – это состояние сложной системы, когда действие внешних и внутренних факторов не приводит к ухудшению состояния системы или невозможности ее функционирования [103].

Транспортная безопасность (ТБ) определяется в Федеральном законе «О транспортной безопасности» от 9 февраля 2007 года № 16-ФЗ как «состояние защищенности объектов транспортной инфраструктуры и транспортных средств от актов незаконного вмешательства (АНВ) в их деятельность» [156].

Авиационная безопасность (АБ) рассматривается как составная часть транспортной и в соответствии с Воздушным кодексом (ФЗ от 19 марта 1997 г. № 60-ФЗ) определяется как: «состояние защищенности авиации от незаконного вмешательства в деятельность в области авиации» [118; 154].

Гражданская авиация представляет собой многофункциональный, иерархический комплекс, обеспечивающий потребности страны в авиационных транспортных услугах. Становление и функциональное развитие гражданской авиации как системы проходит в рамках определенной нормативной базы, которая

постоянно совершенствуется. Как единая структура гражданская авиация с точки зрения системотехники относится к категории сложных систем. В силу своей специфики исследование сложных систем далеко не всегда завершается успешно, поэтому развитие гражданской авиации основано на всестороннем и глубоком исследовании процессов и процедур функционирования отрасли, выявлении соответствующих закономерностей, их обобщении и формализации в формате законов существования и динамики развития. Все это в полной мере относится к исследованию проблем безопасности гражданской авиации как отдельной предметной области [96; 151; 176]. Предметная область представляет собой, как правило, сложную систему, основным инструментом исследования которой является моделирование [22; 196; 236]. Возникает вопрос об идентификации предметной области исследования.

На сегодняшний день в гражданской авиации сформировано достаточно много устойчивых предметных областей, исследование которых предполагается в автономном режиме, т.е. в каждом направлении выявлено некоторое множество закономерностей, которые в своей совокупности выделяют и описывают границы этой предметной области.

Транспортная безопасность аэропорта понимается в рамках определения как некоторое состояние защищенности. Состояние – это некоторое отвлеченное понятие, обозначающее множество устойчивых значений переменных параметров объекта, т.е. транспортная безопасность как состояние представляет собой многопараметрическую характеристику объекта. В качестве объекта выбран аэропорт как наиболее сложная эксплуатационная единица в структуре гражданской авиации. Если говорить о состоянии объекта защиты, то его следует рассматривать как единую систему, относящуюся к категории сложных систем. С этих позиций актуальность темы диссертационного исследования не вызывает сомнений.

Методология диссертационного исследования. Исследование сложных систем возможно с помощью системотехники, квалиметрии, эвристического подхода, теории принятия решений и анализа уязвимости объекта защиты. На этой основе разработаны некоторые концепции: оценки уровня транспортной безопасности [96; 118], прогнозирования уровня мобилизационной готовности персонала [118; 193], уязвимости объектов транспортной инфраструктуры и транспортных средств [103; 118], которые, реализуя совокупность моделей и методов, приводят к понятиям обеспечение транспортной безопасности и управление транспортной безопасностью.

Обеспечение транспортной безопасности, т.е. защиты от АНВ, – это реализация определяемой государством системы правовых, экономических, организационных и иных мер в сфере транспортного комплекса, соответствующих угрозам совершения актов незаконного вмешательства [118].

Обеспечение авиационной (транспортной) безопасности следует рассматривать с двух сторон. Прежде всего, это некоторая деятельность, направленная на предотвращение факторов незаконного вмешательства в деятельность гражданской авиации. Во-вторых, обеспечение АБ (ТБ) можно рассматривать как результат указанной деятельности. Следует заметить, что абсолютный результат невозможен, можно только стремиться к достижению некоторого приемлемого состояния безопасности. В таком случае возникает понятие уровень авиационной (транспортной) безопасности, т.е. количественное отображение состояния защищенности объекта. Понятно, что эта величина динамически изменяется под воздействием угроз и принимаемых мер защиты объекта [118].

Управление транспортной безопасностью в рамках действующих систем рассматривается как управление системой обеспечения безопасности в аэропорту и осуществляется на основе централизованного руководства в целях: координации специально разрабатываемых в этом направлении мероприятий; координации кадровых, материальных, финансовых и других сил и средств на решение задач

обеспечения ТБ; контроля за реализацией принимаемых решений по проблемам обеспечения ТБ; организации взаимодействия с составными звеньями системы обеспечения ТБ; активного использования более гибких форм и методов руководства. В таком случае, говорить о прямом управлении транспортной безопасностью нельзя, поскольку в этой трактовке его просто нет.

Транспортная безопасность обеспечивается досмотром и предотвращением доступа в контролируемую зону аэропорта, охраной соответствующих объектов, реализацией мер противодействия АНВ. Обеспечение транспортной безопасности реализуется в рамках нормативного управления аэропортовой деятельностью, в результате которого обеспечивается приемлемый уровень безопасности. Проблема состоит в управлении транспортной безопасностью, т.е. состоянием объекта защиты. В любом случае, чтобы управлять чем-то, необходимо уметь это что-то измерять, оценивать и сопоставлять с нормативным значением. В случае несоответствия – принимать меры. В таком случае, применительно к транспортной безопасности, необходимо уметь измерять уровень безопасности, решить проблему единиц измерения и шкалы. Тогда можно говорить о реальном управлении.

Процедура управления представляет собой несколько этапов: первичная оценка безопасности, которая состоит в сравнении параметров ситуации в объекте защиты с нормативными требованиями, фиксирование по каждому параметру отклонений от нормативных значений, оценка степени несоответствия, формирование сигнала управления и включение исполнительных схем для ликвидации отклонений по каждому параметру. В современных системах реализовано только обеспечение транспортной безопасности, классического управления безопасностью нет.

Таким образом, главная проблема в области транспортной безопасности состоит в опосредованном регулировании уровня безопасности по принципу достаточности (приемлем – не приемлем), т.е. в гражданской авиации современные системы не обладают возможностью управлять транспортной безопасностью.

Подобных систем нет также в других отраслях промышленности. Например, одна из лучших, разработанная фирмой «Итерация», комплексная автоматизированная информационно-управляющая система (КАИУС-безопасность), ориентированная для работы с критически важными объектами, в перечне своих функций управление безопасностью не содержит.

Отсюда возникает новое понятие: управляемость транспортной безопасности аэропорта. Управляемость безопасности представляет собой способность системы защиты объекта устанавливать и поддерживать приемлемый уровень безопасности при всех изменениях внешних и внутренних угроз в заданном диапазоне.

Анализ понятий «безопасность личности», «единая безопасность» и «неделимая безопасность» применительно к гражданской авиации [128], дает несколько неожиданный и интересный результат. В авиационной транспортной системе фигурируют и используются несколько видов безопасности, каждая из которых имеет прямое отношение к безопасности личности, но парадокс состоит в том, что достижение приемлемого уровня, например, безопасности полетов, абсолютно не гарантирует приемлемого уровня безопасности личности, если, например, не удается достичь приемлемый уровень транспортной безопасности. В таком случае становится актуальным понятие «единая и неделимая безопасность». Предлагается ввести понятие «интегральная безопасность воздушного транспорта» – состояние авиационной транспортной системы, которое гарантирует приемлемый уровень безопасности личности в условиях реализации исчерпывающего перечня авиационных услуг и авиационных работ [128]. Переход к понятию интегральная безопасность в отдельных случаях дает возможность говорить о комплексной оценке безопасности, что позволяет выстраивать соответствующую систему управления безопасностью.

Важно отметить, что проблема управления безопасностью решается в рамках теории оптимального управления, тогда как обеспечение безопасности (теоретический аспект) реализуется с помощью теории управления организационными системами.

Решение проблемы управления транспортной безопасностью в рамках классической теории управления предполагает исследование некоторой математической модели. Формализованное представление модели достаточно проблематично, поскольку содержит множество параметров, имеющих различную физическую природу и относящихся к различным совокупностям, определяющим состояние среды.

Поскольку понятие интегральная безопасность в своем содержательном смысле базируется на всех этих совокупностях, возникает проблема идентификации понятия через некоторое пространство состояний гипотетической среды, отражающей эти совокупности, для чего можно воспользоваться аппаратом теории поля, т.е. безопасность личности отождествить с некоторым полем безопасности, и ввести гипотетические поля угроз и защиты. Тогда появляется триада гипотетических полей, результатом взаимодействия которых является интегральная безопасность, для решения вопроса о приемлемом уровне, которой необходимо разработать методологию оценочных процедур и решить проблемы формализации и моделирования. При этом, следует учитывать, что пространство – это форма существования материальных объектов и процессов, а поле – это обширное однородное пространство, связанное и сравнимое с протяженностью в пространстве.

Система безопасности должна быть готова к обнаружению и отражению любых угроз, т.е. система настраивается на гипотетические (потенциальные) угрозы. В действительности это означает, что система работает с двумя типами угроз: потенциальные и реализованные. При этом процедуры исследования реализованных угроз достаточно хорошо отработаны и понятны: главный принцип – не допустить повторения, а метод исследования – статистическое моделирование. Исследование потенциальных угроз предполагает новые подходы к математическому моделированию, тем более что они содержат класс неизвестных угроз.

Интеграция предполагает объединение на некоторой основе средств обеспечения безопасности, не только технических, с целью повышения их эффективности. Научная идея интеграции состоит в постепенном переходе от принципов нормативного управления процессами аэропортовой деятельности к автоматизированному [54; 63; 66; 79]. При этом транспортная безопасность аэропорта становится не только критерием эффективности аэропортовой деятельности, но и управляемым параметром.

Степень разработанности. Проведено комплексное научное исследование и анализ предметной области, связанной с транспортной безопасностью аэропорта, с целью выделения актуальных направлений применения методов и технологий информационного управления безопасностью. Исследованы краевые задачи теории поля как инструмент интеллектуальной формализации безопасности; исследованы нейронные сети как инструмент интеллектуального моделирования безопасности; исследованы интеллектуальные технологии для решения задач информационного управления безопасностью.

Обосновано и реализовано новое научное направление, связанное с разработкой информационно-управляющего пространства безопасности как интеллектуального центра сбора и обработки динамических данных о ситуации в объекте защиты: разработаны принципы функционирования интеллектуальных систем управления транспортной безопасностью, разработаны концепция и базовые принципы информационного управления безопасностью, разработана кластерная структура информационно-управляющего пространства безопасности.

Разработана методология информационного управления транспортной безопасностью аэропорта на основе моделей и методов моделирования пространства угроз и пространства уязвимостей в формате краевой задачи: разработана модель уязвимости критического элемента аэропорта, разработаны методы и алгоритмы оценки уязвимости, исследовано качество системы защиты объекта как результат оценки уязвимости, разработана модель пространства угроз

безопасности в формате дифференциальных уравнений в частных производных, проведено численное моделирование угроз безопасности в системе MATLAB.

Разработана методология интеллектуального управления транспортной безопасностью аэропорта на основе методов нейросетевого моделирования: разработана и исследована нейронная сеть для ранжирования аэропортов по критерию уязвимость (классификатор), разработан сеточный метод моделирования пространства угроз безопасности аэропорта, проведено численное моделирование пространства уязвимостей в системе MATLAB.

Разработана методология информационного управления негативным влиянием персонала сил обеспечения транспортной безопасности аэропорта в процессе выполнения профессиональной деятельности: разработана модель персонала в безопасности как субъекта сложной системы, разработано новое научное содержание понятия «человеческий фактор», разработана минимаксная модель человеческого фактора, исследовано несанкционированное вмешательство персонала как фактор угрозы безопасности, исследовано негативное влияние персонала как результат профессиональной ошибки, разработаны и исследованы нейросетевые модели (в системе MATLAB и автономно) классификатора персонала по критерию готовности к выполнению профессиональных функций.

Разработке автоматизированной системы управления транспортной безопасностью объекта транспортной инфраструктуры предшествует процесс решения ряда проблем и задач, основанный на научных подходах и методах, в результате реализации которых степень неопределенности в исследуемом объекте должна быть существенно понижена, для чего необходима разработка математической (или иной) модели, с приемлемой степенью адекватности способной описать реальные процессы, происходящие в объекте исследования, и реализация процедур моделирования.

Отмеченная проблема является на сегодняшний день одной из важнейших. Успешное развитие методов и средств автоматизации управления транспортной безопасностью в значительной степени зависит от информационной составляющей

и, если современные компьютерные технологии обработки информации развиваются достаточно успешно, то формализация и алгоритмизация процессов управления транспортной безопасностью представлены слабо и требуют серьезного развития.

В работе [88] представлен авторский анализ возможностей использования математических моделей при решении задач обеспечения АБ в гражданской авиации, где показано, что в прямой постановке задача математического моделирования не может быть решена в связи с непреодолимыми трудностями формализации. Для таких задач решение необходимо не получить, а принять. В основе такой модели лежит математическое представление моделируемых функций, а по входу модели (формализация) и по ее выходу (интерпретация результатов) используются эвристические процедуры. Наиболее адекватным в данном случае представляется математический аппарат теории поля, в частности, совокупность краевых задач, которые описываются системой дифференциальных уравнений в частных производных [6; 74; 124].

Транспортная безопасность, как состояние защищенности объекта, возникает в результате противостояния двух физически реализованных систем (системы угроз (опасностей) и системы защиты) и оценивается понятием уязвимость, которое отвечает на вопрос: в какой степени объект соответствует требованиям по безопасности [3; 52]. В таком случае, правомочно ввести понятие «качество защиты», которое понимается как степень соответствия характеристик системы защиты и требований к ней, и связать с понятием уязвимость. Безопасность обеспечивается, в том числе, совокупностью средств защиты, каждое из которых создает отдельный фрагмент защиты объекта, а все вместе формируют некоторую среду, которую можно представить, как пространство безопасности, характеризуемое параметром качество.

Основы теории транспортной безопасности исследуют закономерности автоматизированного управления соответствующими процедурами. Такие системы по определению являются интегрированными, откуда следует, что управление

является ситуационным, а анализ ситуации является комплексным, т.е. предполагает наличие некоторого единого центра управления, где сосредоточена основная информация о состоянии и параметрах управления. В первом приближении, это ситуационный центр на основе каких-то информационных технологий. Предложенный выше подход рассматривает исследуемые объекты, а это система угроз (опасностей), система защиты и система безопасности, в формате некоторых гипотетических полей. В таком случае, с учетом используемых моделей правомочно говорить о некотором информационно-управляющем пространстве, где совмещены все три исследуемых пространства (поля).

Транспортная безопасность отражает состояние объекта защиты. Проблема состоит в умении управлять безопасностью, т.е. этим состоянием. С этой целью система управления транспортной безопасностью осуществляет сбор и обработку соответствующей информации о динамике изменения параметров состояния исследуемого объекта. Система управления безопасностью включает большой объем информационных каналов, по которым циркулируют информационные массивы, отражающие ситуацию в объекте защиты и требующие соответствующей обработки. Практическая реализация системы основана на современных достижениях в области компьютерных технологий, которые можно применить в области безопасности, но главные трудности в процессе адаптации состоят в отсутствии или низком уровне математической формализации процессов управления безопасностью, что существенно осложняет алгоритмизацию.

Цель и задачи диссертационной работы.

Цель: повышение эффективности управления транспортной безопасностью аэропорта.

Задачи:

1. Анализ проблем транспортной безопасности аэропорта.
2. Разработка ситуационной модели безопасности аэропорта в формате взаимодействующих и противоборствующих пространств угроз и защиты.

3. Моделирование пространства угроз безопасности объекта в формате краевой задачи в виде дифференциальных уравнений в частных производных.

4. Ранжирование и классификация субъектов пространства защиты объекта на основе нейросетевой модели.

5. Разработка методов парирования негативного влияния человеческого фактора.

6. Разработка структуры системы и процедур информационного управления транспортной безопасностью аэропорта.

Положения, выносимые защиту:

– теоретическое обоснование методологии информационного управления транспортной безопасностью аэропорта, которое определяет основные направления совершенствования систем обеспечения безопасности в гражданской авиации;

– методы и средства формализации и алгоритмизации процессов управления транспортной безопасностью в условиях обработки больших информационных массивов;

– метод идентификации совокупности внешних и внутренних угроз безопасности аэропорта в виде гипотетического пространства в терминах теории поля и его формализация в формате краевой задачи с использованием дифференциальных уравнений в частных производных;

– модели, метод и процедуры моделирования пространства угроз безопасности аэропорта в формате краевой задачи и в формате нейронной сети;

– метод информационного управления транспортной безопасностью аэропорта с учетом негативного влияния несанкционированных действий авиационного персонала в процессе профессиональной деятельности;

– модель и процедуры ранжирования персонала по уровню квалификационной готовности к исполнению своих профессиональных функций на основе компетентностного подхода.

Степень достоверности. Достоверность и обоснованность полученных автором научных результатов основаны на адекватной постановке задач исследования и корректном использовании математического аппарата, известных теоретических положений, проверке и согласованности полученных и ранее известных результатов, численном моделировании разработанных объектов в системе MATLAB и в нейросетевом базисе.

Научная новизна. Научная новизна работы заключается в том, что впервые разработаны:

– базовые принципы и концепция информационного управления транспортной безопасностью;

– методы формализации угроз безопасности аэропорта в формате гипотетического пространства;

– методы моделирования пространства угроз безопасности аэропорта;

– модели и методы моделирования уязвимости аэропорта;

– методы сценарного управления безопасностью в формате информационных технологий;

– модель и методика нейросетевого управления уровнем транспортной безопасности аэропорта;

– новое содержание понятий «человеческий фактор» и «негативное влияние персонала» в транспортной безопасности и их теоретическое обоснование;

– модели и методы моделирования фактора «негативное влияние персонала».

Теоретическая и практическая значимость работы. Практическая значимость результатов исследования состоит:

– в получении численных результатов математического моделирования исследуемых объектов транспортной безопасности, что позволяет решать практические задачи информационного управления безопасностью;

– в разработке и исследовании экспериментальных вариантов нейронных сетей для целей безопасности и соответствующих методик, что обеспечивает

переход к автоматизированным технологиям информационного управления безопасностью и повышению эффективности управленческих процедур.

Теоретическая значимость работы, ее ценность состоит в решении актуальной проблемы управления транспортной безопасностью в гражданской авиации, имеющей важное государственное значение и связанной с разработкой адекватных моделей и методов формализации процессов, с использованием информационного управления безопасностью и современных информационных технологий ESM, PSIM, DATA MINING и других. Особую важность имеет теоретическая и практическая значимость работы, основанная на разработке основ теории транспортной безопасности и ее практических приложений для процессов информационного управления безопасностью.

Объект, предмет, гипотеза исследования.

Предметная область. Транспортная безопасность аэропорта.

Объект исследования. Система управления транспортной безопасностью аэропорта.

Предмет исследования. Модели и методы информационного управления транспортной безопасностью.

Проблема. Современные системы управления транспортной безопасностью объектов воздушного транспорта основаны на понятии обеспечения безопасности. В этом случае в системе реализуется нормативное управление, когда управляемый параметр (безопасность) в явном виде для управления не используется, а заменяется совокупностью нормативных документов, процессов и процедур, т.е. управление безопасностью можно рассматривать исключительно как вторичный процесс и результат. Тогда информационное управление, которое по сути является автоматизированным, должно быть оптимальным в соответствии с теорией оптимального управления [134]. Реализация такого управления требует разработки адекватных математических моделей и формальных решений по алгоритмизации процессов управления транспортной безопасностью. Проблема усугубляется тем, что понятия обеспечение и управление далеко не синонимы.

Идея. Информационное управление транспортной безопасностью на основе адекватных математических моделей пространства безопасности и адаптивных алгоритмов оптимизации параметров системы защиты лежит в основе нового эволюционного класса систем автоматизированного управления – интеллектуальные комплексы.

Гипотеза. Методология информационного управления транспортной безопасностью аэропорта, основанная на математическом моделировании в формате краевой задачи, понятии уязвимость (как характеристика объекта защиты) и нейросетевом моделировании, обеспечит приемлемый уровень безопасности.

Цель исследования. Повышение эффективности управления транспортной безопасностью аэропорта путем создания комплекса информационного управления на основе пространственно-ситуативного подхода, разработки адекватных моделей пространства безопасности и адаптивных алгоритмов оптимизации параметров системы защиты.

Публикации и апробация. Список публикаций автора по теме диссертации включает 38 научных трудов, в том числе 14 статей в рецензируемых научных журналах из перечня ВАК при Минобрнауки РФ (127 с.), 4 публикации в изданиях, индексированных в международных базах данных Web of Science и Scopus (31 с.), 20 публикаций в трудах международных и всероссийских конференций (80 с.).

Структура и объём диссертационной работы. Диссертация состоит из введения, пяти глав, заключения, списка сокращений и условных обозначений, списка литературы, приложений (в томе 2). Общий объем работы составляет 330 страниц текста. Диссертация содержит 8 таблиц, 105 рисунков. Список используемых источников состоит из 272 наименований.

ГЛАВА 1 АНАЛИЗ ПРОБЛЕМ ОБЕСПЕЧЕНИЯ ТРАНСПОРТНОЙ БЕЗОПАСНОСТИ АЭРОПОРТОВ

1.1 Эволюция систем безопасности в гражданской авиации

Вопросы безопасности на начальном этапе развития гражданской авиации, как правило, рассматривались с точки зрения безопасности полетов, поскольку не было серьёзной необходимости защищать объекты авиации от вмешательства в их деятельность. Мероприятия по защите назывались режимом обеспечения безопасности полетов и входили в состав понятия безопасность полетов. При этом на международном уровне вопросы безопасности рассматривались уже давно. Однако, с возникновением проблем в межгосударственных отношениях и появлением терроризма, вопросы, которые сейчас относятся к сфере авиационной безопасности, вышли на первое место и потребовали принятия решений на государственном и межгосударственном уровне.

В 1975 году появилось первое издание документа «Безопасность. Защита гражданской авиации от актов незаконного вмешательства». Приложение 17 к Чикагской конвенции ИКАО [147]. До сих пор данный документ переиздаётся и является основополагающим.

Постановление Правительства РФ от 30.07.1994 № 897 «О федеральной системе обеспечения защиты деятельности гражданской авиации от актов незаконного вмешательства» определило новое научное направление в области гражданской авиации.

В 1997 году вступил в силу федеральный закон от 19.03.1997 № 60-ФЗ «Воздушный кодекс РФ», в котором отдельная глава посвящена авиационной безопасности и введено понятие «Авиационная безопасность» [154].

Федеральный закон от 09.02.2007 № 16-ФЗ «О транспортной безопасности» вводит понятие «Транспортная безопасность» [156].

В 2019 году утверждены Национальные программы в области транспортной безопасности [198; 199; 200].

Эти даты можно считать ключевыми точками в развитии транспортной безопасности как научного направления. В промежутках между ними вышли в свет и вступили в силу достаточно много нормативных и регламентирующих документов различного уровня и статуса, которые определили цель и задачи развития транспортной безопасности как науки и этапы эволюционного развития (Рисунок 1.1).

Первый этап (1) связан с созданием и функционированием автономных систем. Главная задача таких систем состояла в обнаружении угроз. Принципы функционирования основаны на нормативно-правовом управлении, когда требования к алгоритмам функционирования заложены в совокупности нормативных документов, оборудование настроено на исполнение этих требований, а контроль осуществляется периодически по мере возникновения нестандартных ситуаций. Управления безопасностью, как такового, фактически нет.

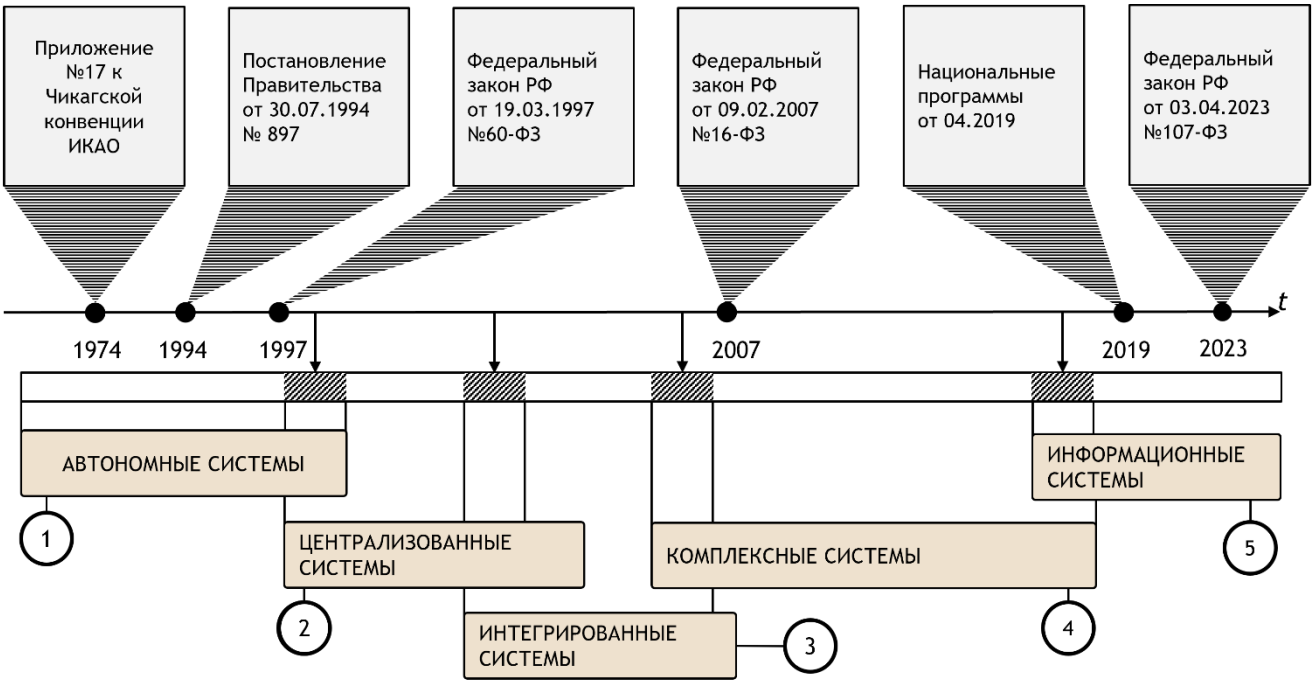


Рисунок 1.1 – Эволюция систем транспортной безопасности

Второй этап (2) связан с понятием централизованная обработка информации. С одной стороны, этап характеризуется заметным усложнениям требований к системам безопасности в связи с увеличением объема и изменением характера внешних угроз, с другой стороны, появлением новых возможностей в методологии и средствах обеспечения безопасности. Здесь впервые зарождается понятие интеграции систем, основанное не на элементной базе технических средств, а на стандартах и протоколах обработки информации. Появляется единая система обработки информации, объединяющая разнородные сигналы с последующей выдачей их в исполнительное звено. Управление безопасностью по-прежнему отсутствует, но появляются информационные каналы, объединяющие систему в единое целое.

Следует отметить, что границы этапов в достаточной степени размыты и характеризуются некоторым переходным периодом, который не поддается четкой классификации.

Третий этап (3) характеризуется появлением интегрированных систем. Этот важнейший этап связан с резким скачком в развитии аналитических возможностей систем транспортной безопасности. Интегрированные системы характеризуются развитыми средствами анализа событий; глубокой интеграцией, которая понимается как наличие единого информационного пространства; впервые появляется возможность и необходимость научного осмысления процессов в системе и создания некоторой методологии и основ теории транспортной безопасности. Система становится двухуровневой, где главным является уровень аналитики, включая процессы управления, и уровень аппаратно-технических средств, т.е. исполнительный уровень.

На данном этапе решена важнейшая задача, связанная с обнаружением угрозы, сбором и обработкой информации. Не менее важна задача ликвидации угрозы, которая предполагает четкое понимание в системе ответственности исполнителя за каждый фрагмент деятельности по отработке угрозы. Дальнейшее

развитие систем определяется именно этой задачей и, по сути, представляет собой методологию совершенствования интегрированных систем управления транспортной безопасностью.

Четвертый этап (4) характеризует комплексные системы, которые реализуют следующие функции:

- подтверждение данных;
- управление реагированием на инциденты;
- отчетность в реальном времени;
- управление уровнями безопасности;
- автоматизация обработки инцидентов;
- открытая платформа;

Пятый этап (5) определяется понятием информационное управление, которое на первоначальной стадии связано с понятием инцидентного управления.

Инцидентное управление ситуацией в объекте защиты основано на понятии инцидент безопасности. Инцидент безопасности – это событие, зафиксированное системой и свидетельствующее о нестандартной ситуации в объекте защиты и наличии негативных событий.

В последние годы успешно развивается новое направление в области систем безопасности, связанное с понятием информационное управление системами и комплексами безопасности. Платформой для интеграции и управления комплексами (Physical security information management – PSIM) называется категория программного обеспечения, предназначенная для интеграции несвязанных приложений.

На сегодняшний день доминирующей является концепция инцидентного управления. Можно назвать два объективных фактора, препятствующих широкому внедрению в практику информационного управления: это низкая доступность данных для интеллектуального анализа безопасности и отсутствие моделей защиты, включая сценарии и способы защиты. Для решения этих проблем

необходима «глубокая» интеграция средств защиты и применение технологий Date Mining, оперирующих с «Большими данными» (Big date).

Как уже было отмечено, начиная с третьего этапа (Рисунок 1.1) эволюционного развития систем транспортной безопасности все последующие этапы характеризуют системы, которые относятся к классу интегрированных систем безопасности, поэтому важно выделить базовые отличия интегрированных систем и определить принципы и направления их перспективного развития.

Проблемы управления транспортной безопасностью наиболее наглядно проявляются, если рассматривать в качестве объекта транспортной инфраструктуры аэропорт [103]:

- организационная проблема,
- проблема связана с процедурами оценки уровня транспортной безопасности,
- проблема определяется человеческим фактором,
- проблема кроется в понятии интегрированные системы,
- проблема связана с динамическим характером угроз.

Отсюда возникает новая проблема интеграции, а именно: соблюдение в динамике оптимального в смысле некоторых критериев баланса между комплексом технических средств обеспечения транспортной безопасности и человеческим фактором. При этом отдельной проблемой становится вопрос о критериях оптимизации (Рисунок 1.2).

Фактор времени в системах транспортной безопасности имеет определяющее значение, поскольку в таких системах речь идет о постоянном противостоянии объекта противоправной деятельности и системы защиты, даже в тех случаях, когда акт незаконного вмешательства (АНВ) в деятельность гражданской авиации отсутствует. При наличии АНВ особую значимость приобретают два временных фактора: время обнаружения и время ликвидации.

Каждый из этих факторов определяет возможности нарушителя реализовать соответствующие угрозы и причинить соответствующий ущерб.

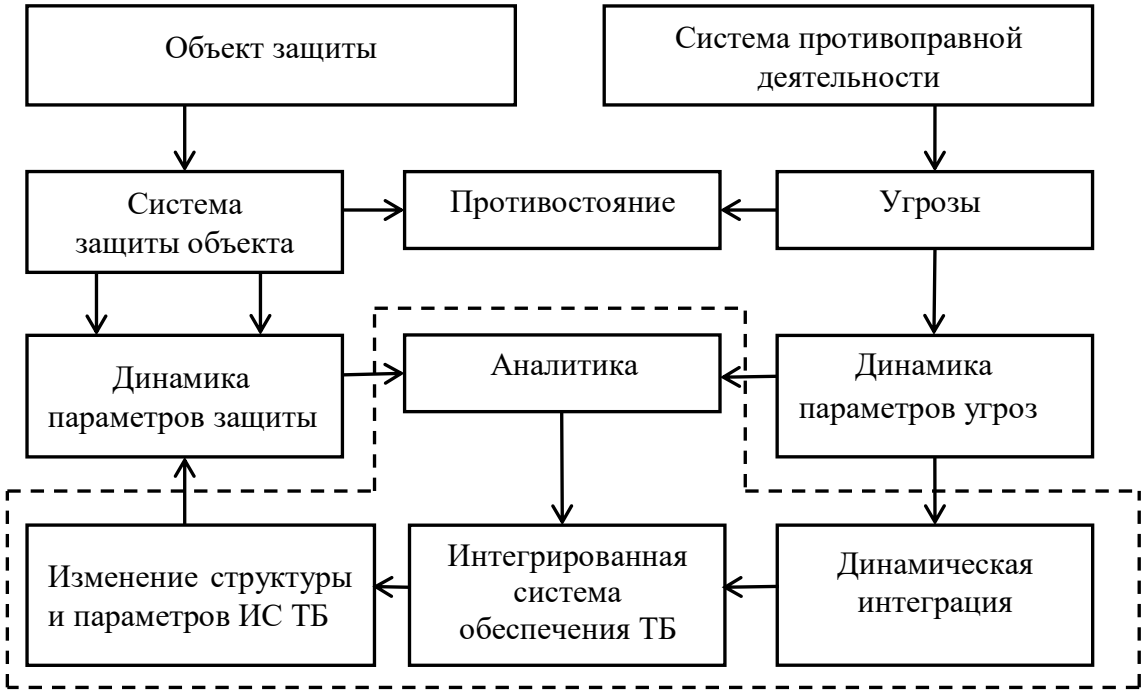


Рисунок 1.2 – К вопросу о динамике угроз

Динамическая интеграция средств обеспечения транспортной безопасности аэропорта интерпретирует интегрированную систему транспортной безопасности аэропорта как сложную систему, структура которой является динамической и адаптивной. Главным критерием оптимального управления техническими средствами защиты аэропорта от несанкционированного вмешательства в его деятельность является качество обеспечения такой защиты.

1.2 Организация системы обеспечения безопасности аэропорта

Основным критерием деятельности транспортного комплекса страны, в том числе гражданской авиации, является безопасность. Обеспечение безопасности объектов транспортной инфраструктуры представляет собой сложный, наукоемкий процесс, включающий совокупность методов и средств, отвечающих современным требованиям гражданского общества.

Становление и развитие систем обеспечения авиационной безопасности определено в стандартах и практике Международной организации гражданской авиации (ИКАО) [73; 139; 147; 165; 166; 167; 209], Федеральных законах РФ [154; 155; 156], Федеральных авиационных правилах (ФАП) [162; 164], Национальных программах [198; 199; 200] и других нормативных документах [40; 157; 158; 159; 160; 161; 163].

Каждое направление с точки зрения науки представляет собой достаточно сложную предметную область, исследование которой предполагает использование адекватного аппарата, математического, методологического, технического, с другой стороны, автономное исследование здесь недопустимо, поскольку безопасность требует комплексного подхода к исследованию. Это требует решения ряда сложных, научных проблем.

Системы обеспечения авиационной и транспортной безопасности включают в свой состав множество подсистем, включая подсистему нормативно-правового регулирования, которая представляет собой комплекс правовых и нормативных документов, утвержденных в установленном порядке и придающих им статус юридической нормы. На основе этих норм разрабатываются документы более низкого уровня, регламентирующие процессы по обеспечению безопасности. Проблема состоит в том, что подсистема не работает в режиме реального времени, более того, промежуток времени от начала выполнения процедуры до ее завершения в рамках такого управления может быть значительным. Такое управление, называемое нормативным, не может быть оптимальным, поскольку в данном случае трудно определить критерий оптимальности. Решение следует искать в области автоматизации процедур управления.

Человеческий фактор в гражданской авиации всегда квалифицируется как положительно, так и отрицательно. Если положительно, это значит, что персонал выполняет свои функции в полном соответствии с требованиями и установленными нормами, если нет, имеют место нарушения установленных правил, что, в конечном итоге, приводит к негативным событиям. Особенно важно

это для транспортной безопасности, где негативное событие по вине персонала может привести к трагическим последствиям.

Временной фактор один из важнейших в системе обеспечения безопасности. Процесс обеспечения безопасности всегда ограничен временными рамками, нарушение которых приводит если не к катастрофическим последствиям, то, в любом случае, к увеличению материальных потерь. Временной фактор в совокупности с человеческим еще более усугубляется тем, что приходится учитывать физиологические особенности человека и не всегда с положительным результатом.

Статистический анализ в транспортной безопасности достаточно редкое явление по причине единичности событий внутри и вне системы.

Весьма важен вопрос об управляемости системы обеспечения транспортной безопасности. Уровень управляемости определяется степенью интеграции технических средств и уровнем адаптивности управляющих элементов к изменению внешних условий. Управляемость определяется уровнем интеллекта управляющей системы, ее эффективностью в вопросах оценки своевременности и достоверности применяемой информации, уровнем контроля за исполнением регламентов, избыточностью или недостатком используемых данных. Отдельно стоит вопрос об оценке критичности негативного события и оценки своевременности сигналов о действиях служб безопасности. Вопрос о точности принимаемых и реализуемых решений фактически определяет точность функционирования системы обеспечения в комплексе и должен быть решен на этапе проектирования.

Уязвимость объектов защиты в современных системах обеспечения безопасности является критерием оптимальности управления безопасностью и определяет структуру технических средств защиты. Практически все модели процессов обеспечения безопасности основаны на понятии уязвимость. Уязвимость – это состояние объекта и системы обеспечения его транспортной

безопасности, допускающее возможность совершения акта незаконного вмешательства в его деятельность и реализации угроз объекту.

Главной тенденцией развития современных систем защиты становится решение задачи упреждения угроз безопасности. Задача тем более усложняется, что угрозы описываются на предполагаемом уровне, т.е. в гипотетическом формате. Тогда прогнозное моделирование процессов в системе становится достаточно сложным, а выбор методов прогнозирования приобретает первостепенное значение. С учетом трудностей формализации, прогнозные модели будут эвристическими.

Вопросы, связанные с перестройкой структуры, и адаптивность системы в контексте транспортной безопасности синонимы. Адаптивность систем обеспечения транспортной безопасности понимается как управляемость структуры технических средств по критерию уязвимость, что позволяет системе в автоматизированном режиме менять структуру при изменениях ситуации в объекте защиты.

Основным методом исследования систем транспортной безопасности является моделирование, что предполагает формализацию предметной области. В задачах, связанных с безопасностью, процедура формализации достаточно сложна и неопределенна, поскольку переменные в структуре математического описания плохо идентифицированы и неоднозначны. Это связано с тем, что вопросы безопасности решаются через анализ и исследование ситуации в объекте защиты, которая складывается под воздействием множества внешних и внутренних факторов, что переводит задачу в разряд многофакторных и многокритериальных. В этом случае переход от лингвистического описания к математической модели затруднен, а процедуры формализации становятся эвристическими. Вместе с тем, возможность структуризации процессов и процедур обеспечения безопасности остается безусловной, поскольку предполагается их алгоритмизация и компьютерная реализация. Оценочные процедуры связаны с квалиметрией.

Ситуацию в объекте транспортной инфраструктуры в отношении безопасности достаточно удобно рассматривать как результат взаимодействия или противостояния пространства угроз и пространства защиты, что формирует пространство безопасности. Эти пространства в виде некоторых параметров отражаются и используются в системе безопасности. Современные системы в высокой степени интегрированы, что означает наличие единого ситуационного центра управления. В таком случае, вполне закономерно появление информационно-управляющего пространства как источника параметров управления.

Если абстрагироваться от гражданской авиации как авиационной транспортной системы (АТС), наиболее важные процессы обеспечения безопасности можно исследовать на примере аэропорта, поскольку именно аэропорты являются наиболее уязвимой частью АТС [106; 107; 111]. Современный аэропорт – это сложнейшая многоэлементная эргатическая система, реализующая в своей производственной деятельности достаточно сложные алгоритмы и технологии в условиях большого скопления людей при внешних факторах, далеко не всегда благоприятствующих достижению целей функционирования.

Интеллектуальное содержание проблем обеспечения транспортной безопасности в современных структурах и системах гражданской авиации достигло такого уровня, что требует соответствующего уровня развития методологии решения этих вопросов, что предполагает успешное формирование основ теории транспортной безопасности.

За последние десять лет сделан серьезный шаг в этом направлении [103; 118]. Вместе с тем, все успехи здесь связаны с обеспечением безопасности. Дело в том, что существуют принципиальные отличия между понятием обеспечение безопасности и понятием управление безопасностью.

Обеспечение транспортной безопасности – деятельность (система мер), осуществляемая специально уполномоченными органами, службами,

подразделениями и авиационным персоналом, направленная на предотвращение террористических акций, захвата и/или угона воздушного судна и иных незаконных вмешательств в авиационную деятельность. (Модельный закон о безопасности на воздушном транспорте. Принят Межпарламентской Ассамблеей государств-участников СНГ, постановление от 31 октября 2007 года № 29-10).

Целями обеспечения безопасности на воздушном транспорте являются:

– защита жизни и здоровья граждан,

– функционирование ГА без авиационных и чрезвычайных событий,

– снижение негативного влияния авиационных и чрезвычайных происшествий на безопасность,

– повышение ответственности участников авиационной деятельности.

Задачами обеспечения безопасности являются:

– определение угроз безопасности на воздушном транспорте,

– защита от угроз,

– предотвращение авиационных и чрезвычайных происшествий,

– снижение тяжести последствий,

– предупреждение кризисных ситуаций,

– снижение негативного влияния на окружающую среду.

В последние годы наметилась вполне определенная тенденция рассматривать вопросы обеспечения транспортной безопасности с точки зрения оптимального управления её уровнем с последовательным решением задач идентификации, измерения, оценки и принятия решений, что определяет настоятельную необходимость перехода к проблеме формализации предметной области [104; 114; 117].

1.3 Анализ проблем обеспечения и управления транспортной безопасностью аэропорта

В настоящее время транспортная безопасность как научная область включает в себя набор научно-методических инструментов для решения проблем, которые можно отнести к категории слабо формализованных. Это определяется рядом парадоксов, которые возникают внутри системы транспортной безопасности и отражают существенную неопределенность при постановке задач. Формальное описание этих парадоксов представляет собой довольно сложную и многомерную проблему, которая требует использования сложных, часто эвристических, алгоритмов для ее решения.

Процесс обеспечения транспортной безопасности реализуется в строгом соответствии с требованиями к каждой процедуре, утвержденными в установленном порядке, т.е. представляет собой набор унифицированных алгоритмов, каждый из которых содержит исчерпывающий перечень элементов профессиональной деятельности персонала, достаточный для достижения целевой функции обеспечения безопасности. Любое отклонение от алгоритма может быть квалифицировано как незаконное вмешательство, которое в отдельных случаях может привести к катастрофическим последствиям.

Приемлемый уровень транспортной безопасности достигается в результате противостояния между системой безопасности (системой защиты объекта) и набором угроз безопасности, внешних и внутренних по отношению к системе. В этом случае результат можно считать положительным, когда достигнут консенсус между всеми типами безопасности. Противостояние угроз и системы защиты выявляет некоторые парадоксы безопасности.

Парадокс 1. Сотрудники подразделений транспортной безопасности.

Авиационный персонал, выполняя свою целевую функцию, осуществляет профессиональную деятельность по обеспечению безопасности, т.е. решает проблему достижения приемлемого уровня транспортной безопасности. С другой

стороны, персонал, являясь человеческим компонентом в эргатической системе обеспечения транспортной безопасности, в силу своей физиологии может допускать некоторые отклонения от установленного алгоритма деятельности, и не обязательно намеренно. Это приводит к возникновению парадокса двойственности, когда персонал одновременно выполняет положительные и отрицательные функции. В конечном счете, соотношение положительных и отрицательных аспектов в производственной деятельности персонала обеспечивает приемлемый уровень транспортной безопасности аэропорта [103]. Другими словами, персонал подразделения транспортной безопасности имеет основополагающее значение для обеспечения приемлемого уровня безопасности, который реализует процедуры, с другой стороны, этот же персонал является источником угрозы безопасности охраняемого объекта из-за ошибок, вынужденных или случайных, без которых наша деятельность невозможна.

Человеческий фактор в строгом определении является не фактором, а гораздо более сложной и многогранной категорией, которая относится к сложным системам и обладает целевой функциональностью, не поддающейся строгому математическому описанию. Для изучения парадокса вводится новое понятие «кадровая угроза», под которым понимается состояние неадекватности профессиональной готовности оператора и параметров ситуации в системе безопасности, определяемое максимальным уровнем профессиональных параметров индивида, допускающим возникновение негативного события. Возникает новая ситуация, когда нужно не минимизировать человеческий фактор, а стремиться регулировать негативное влияние персонала авиационной организации на процедуры производственной деятельности, рассматривая это влияние как угрозу безопасности объекта. В этом случае меняются подходы к решению проблемы и методы исследования [119].

Решение заключается в разработке системы для минимизации вмешательства персонала подразделения транспортной безопасности в процедуры ее обеспечения, основанной на изучении причин и характера ошибок со стороны персонала и

разработке автоматизированной системы контроля несанкционированного вмешательства. Предлагается исследовать негативное влияние персонала авиационной организации на процедуры обеспечения транспортной безопасности и управления ими. Необходимо свести к минимуму ту часть человеческого фактора, которая представляет угрозу для производственной деятельности и является несанкционированным вмешательством. В этом случае существуют соответствующие структурно-логические модели и методы их исследования, которые выявляют негативное влияние персонала авиационной организации. Результат исследования, представленный в некотором количественном эквиваленте, можно рассматривать как параметр для управления уровнем негативного влияния, т.е. угроза со стороны ЧФ становится управляемой [251].

Парадокс 2. Неделимость безопасности.

Безопасность на воздушном транспорте – довольно сложная категория, где транспортная безопасность является лишь одним из элементов среди многих других, различных видов безопасности. Эти виды безопасности исследуются независимо, например, безопасность полетов, экологическая безопасность, промышленная безопасность и т.д. Парадокс заключается в том, что приемлемый уровень одного типа безопасности не означает, что приемлемый уровень в целом достигнут, поскольку низкий (неприемлемый) уровень, например, безопасности полетов, может привести к катастрофе.

Здесь появляется концепция интегральной безопасности и концепция личной безопасности, с которыми необходимо сочетать основные положения концепции информационного управления транспортной безопасностью [128].

Парадокс 3. Большие данные.

В процессе обеспечения транспортной безопасности обрабатываются очень большие объемы информации, поступающей от множества датчиков и других источников. Сегодня существует довольно много различных технологий, предназначенных для работы с большими объемами данных (BIG DATA, DATA MINING, DATA SCIENCE), а также PSIM – специальные системы управления

физической безопасностью. Парадокс заключается в том, что эти современные инструменты, обладающие обширными вычислительными возможностями, не могут быть использованы в области транспортной безопасности из-за практического отсутствия формальных описаний процедур и алгоритмов предметной области. Решение заключается в разработке соответствующих процедур и алгоритмов. Одной из таких систем является программный комплекс «Electronika Security Manager (ESM)» как многофункциональная технологическая платформа [103]. Более современный вариант этой системы, реализующий технологию PSIM (ESM-PSIM) представлен в работе [105].

Парадокс 4. Угрозы безопасности.

Транспортная безопасность объекта строится в результате противодействия определенному набору угроз, внешних и внутренних по отношению к объекту. Парадокс угроз заключается в том, что они не проявляются до тех пор, пока не будет установлен факт их физической реализации, когда становится возможным идентифицировать угрозы и осуществлять контрмеры. Однако, очевидно, что наиболее важной является превентивная функция системы безопасности, реализация которой возможна, когда создано формальное представление угроз в виде их гипотетического распределения по топологии объекта безопасности, что отражается в информационно-управляющем пространстве безопасности (аналогия теории поля). Решение предлагается искать в виде краевой задачи для уравнения в частных производных. Математический аппарат теории краевых задач довольно обширен и хорошо представлен в литературе [23; 35; 38; 123; 197; 232]. Это могут быть краевые задачи для линейного уравнения, для гиперболических и параболических уравнений, трехмерного уравнения Лапласа, задачи Дирихле, Неймана, уравнение Пуассона и другие. Представленный класс задач является исчерпывающим для моделирования гипотетических полей безопасности, но каждый тип уравнения может быть соотнесен только с определенным типом угрозы. В этом случае отдельные результаты решения задачи моделирования должны быть проанализированы вместе, и общее решение должно быть принято с

использованием определенных эвристических алгоритмов в рамках теории принятия решений. Необходимо согласиться с тем, что эвристическая процедура может обеспечить только качественный результат, который далек от реальной картины взаимодействия полей, но вполне достаточен для целей обеспечения транспортной безопасности. Проблема относится к классу плохо формализуемых и слабо структурируемых. Результат моделирования представляет собой определенное распределение интенсивности угроз по топологии объекта транспортной инфраструктуры, что позволяет выявить экстремальные точки воздействия и включить их в список приоритетов для мониторинга ситуации.

Парадокс 5. Процедуры оценки.

Обеспечение приемлемого уровня безопасности и, что особенно важно, управление им, невозможно без процедур оценки, которые реализуются в основном экспертными методами. Парадокс заключается в том, что в большинстве случаев результат довольно далек от реальных оценок, с которыми приходится мириться из-за отсутствия лучших инструментов. При индивидуальной оценке достоверность оценки определяется уровнем компетентности эксперта, который проявляется в его интуиции. Часто интуитивная оценка может противоречить инструментальной, но именно эта оценка принимается в качестве результата. При переходе на массовые оценки, особенно при оценке профессиональной готовности персонала, все это не работает. Решение заключается в использовании нейронных сетей в режиме классификации персонала, что может отражать некоторые интуитивные идеи эксперта [38; 97; 126; 169; 182].

Рассмотренные парадоксы не исчерпывают всех парадоксальных ситуаций, возникающих в системе обеспечения транспортной безопасности в гражданской авиации, но они определяют основные проблемы, подлежащие решению при создании автоматизированных систем управления уровнем транспортной безопасности. Современные системы постепенно становятся информационными. Мощные вычислительные платформы, которые работают с большими объемами данных и используют передовое программное обеспечение и математику, уже

созданы и используются. Однако, основной проблемой при использовании таких систем в области транспортной безопасности является отсутствие достаточного набора разработанных алгоритмов и процедур, которые формализованы и описывают процессы в системах управления безопасностью. Представленные подходы к решению проблем достаточно универсальны и позволяют получить некоторый формализованный аппарат для использования современных информационных технологий в обеспечении транспортной безопасности.

Предлагаемые подходы не лишены некоторых недостатков. Почти все задачи, которые необходимы для обеспечения приемлемого уровня транспортной безопасности и, более того, ее управления, являются достаточно сложными, что определяется их характеристиками, перечисленными ниже.

Неопределенность – транспортная безопасность достигается в результате противодействия угроз и систем защиты. Несмотря на то, что список возможных угроз безопасности задан, их параметры не могут быть точно определены до тех пор, пока угроза не будет реализована. Следовательно, в постановке задачи существует значительная неопределенность.

Многокритериальность – безопасность определяется многими факторами, часто различной физической природы. Интеграция таких факторов практически невозможна. Многие факторы взаимозависимы. Все это приводит к значительной нелинейности решаемых задач.

Формализуемость – исходные данные для постановки задач в области транспортной безопасности заметно ограничены. Формализованные зависимости между параметрами процессов безопасности не могут быть описаны. В этой ситуации практически невозможно получить точное математическое представление исследуемых процессов. Следовательно, процедуры формализации должны быть дополнены некоторыми эвристическими решениями.

Структурируемость – как важный элемент алгоритмизации довольно сложна. В тех случаях, когда используется эвристический подход, связанный с теорией

принятия решений, результат решения не может быть получен, он должен быть принят при выполнении определенных условий.

Несмотря на отмеченные трудности, предлагаемый подход обеспечивает решение поставленных задач, которые приходится решать через понятие гомеостаза.

1.4 Анализ угроз безопасности аэропортовой деятельности

Гомеостаз следует рассматривать как одну из функциональных характеристик динамичных систем, гармонизирующих стабильное поведение системы в условиях неустойчивости внешней и внутренней среды.

Системы обеспечения безопасности по определению являются динамичными, т.е. изменяют свои параметры и структуру при условии воздействия внешней и внутренней среды. Воздействие как термин следует понимать, как любое действие, направленной на объект с целью повлиять на него, вызвать изменения. Причиной воздействия внешней среды может быть множество факторов, определяемых понятием угрозы. Внутренние факторы определяются в большинстве случаев понятием конфликт интересов, т.е. конфликт является важнейшей частью понятия безопасность. Конфликтные ситуации возникают при несовпадении целей элементов системы или несовпадении этих целей с целевым функционалом всей системы. Кроме того, обеспечение безопасности включает элементы управления, а любое управление всегда есть насилие, противоречит динамическому развитию системы и усиливает конфликтную ситуацию. С другой стороны, конфликт в данном случае неизбежен и определяет прогрессивный фактор развития ситуации при условии, что конфликт разрешен до такого момента развития, когда нет возврата в исходную точку возникновения конфликта.

Обеспечение безопасности с точки зрения системотехники представляет собой системное взаимодействие некоторых процессов, в результате чего возникает безопасная ситуация в объекте защиты. При этом ситуация должна

сохранять безопасное состояние в условиях проявления внешних и внутренних угроз, что соответствует понятию гомеостаз безопасности. Схема гомеостатической системы безопасности представлена на рисунке 1.3.

Важнейшим элементом схемы является системное взаимодействие процессов обеспечения безопасности, с учетом угроз и парадоксов, результатом чего становится безопасное состояние объекта защиты. Характер взаимодействия определяется конфликтом интересов в системе. Аналитическое исследование конфликта в большинстве случаев не дает решения, необходимо моделирование.

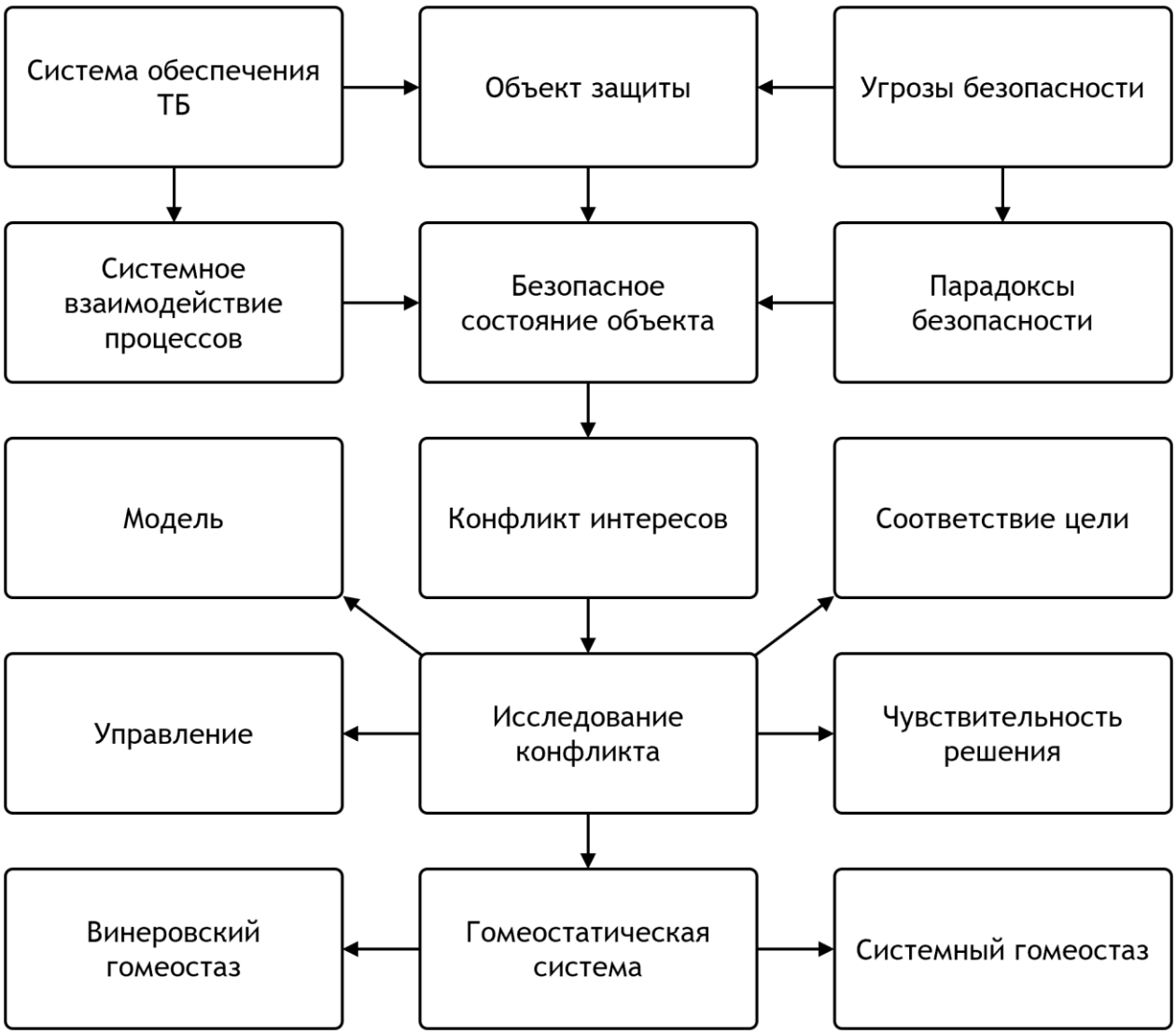


Рисунок 1.3 – Схема гомеостатической системы безопасности

Гомеостатическая система безопасности образуется путем установления функциональных связей между элементами.

Винеровский гомеостаз есть такое системное взаимодействие процессов, при котором система возвращается к некоторому устойчивому состоянию после возмущений, вызванных внешними факторами.

Системный гомеостаз – возвращение к необратимому процессу развития после флуктуации или выбор нового направления.

Конфликт представляет собой нарушение гомеостаза, следствием чего может быть: восстановление гомеостаза (прекращение конфликта), изменение гомеостаза (взаимодействие систем), прекращение гомеостаза (разрушение части системы). Структурно-логическая модель гомеостаза безопасности представлена на рисунке 1.4.

Рисунок 1.4 – Структурно-логическая модель гомеостаза безопасности

Возникновение и формирование гомеостаза безопасности определяется взаимодействием внутрисистемных процессов, которые проявляются как воздействия внешней и внутренней среды в формате угроз и конфликтов. Безопасное состояние объекта определяется гомеостазом безопасности, достижение которого возможно при условии выполнения следующих процедур (процессов): идентификация параметрических и структурных отклонений, мониторинг отклонений параметров и структуры, коррекция параметров и структуры в рамках общей коррекции взаимодействующих процессов. В таком случае, гомеостаз выступает как цель обеспечения безопасного состояния объекта защиты и как критерий (уровень безопасности объекта приемлем – неприемлем) достижения этого уровня.

Работа системы защиты объекта транспортной инфраструктуры выстраивается в соответствии с перечнем предполагаемых угроз безопасности. Если угроза реализуется, т.е. защита не сработала удовлетворительно, то анализ этих событий имеет несколько академический интерес, поскольку можно говорить только о ликвидации последствий негативного события. Главная задача системы защиты – предотвратить негативное событие. В таком случае приходится иметь дело с предполагаемыми угрозами. Гипотетичность угроз вызывает определенные трудности в их исследовании в связи с достаточным уровнем неопределенности при лингвистическом описании. Основой для модели угроз (Рисунок 1.5) является модель субъекта противоправной деятельности (СППД) [193].

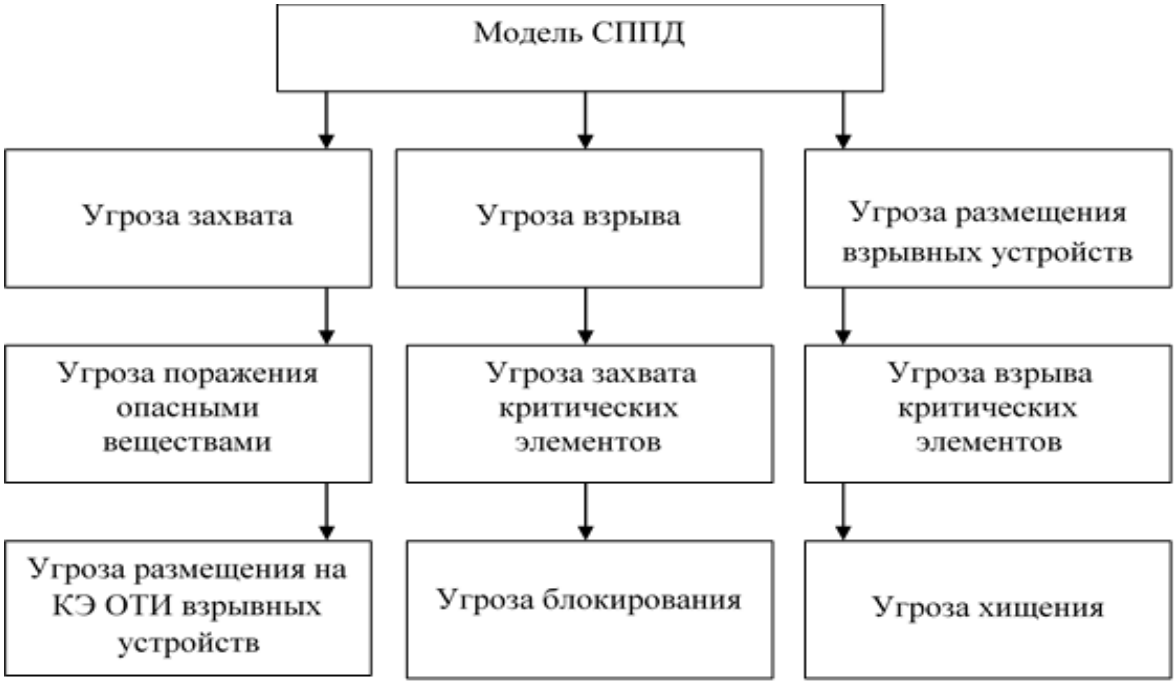


Рисунок 1.5 – Модель угроз безопасности авиапредприятия

Анализ угроз необходим для определения методов и процедур их формализации, предполагающих дальнейшее использование формализованного представления угроз в качестве критерия оптимизации процессов информационного управления транспортной безопасностью. Предполагается, что результат анализа может быть представлен в количественном формате.

Ниже рассмотрены некоторые подходы к количественной оценке угроз реализации актов незаконного вмешательства в деятельность объектов гражданской авиации. В работах [33; 34] авторы исходят из определения угрозы АНВ как намерения нарушителя осуществить акт незаконного вмешательства в деятельность объекта гражданской авиации.

Предлагается количественный показатель степени угрозы j-го (j=1,2,…y) АНВ (B_j) в деятельность i-го объекта ГА на временном интервале $T = t+\Delta t$ в виде вероятности W_i начала исполнения угрозы на этом временном интервале.

Степень угрозы j-го АНВ i-му объекту ГА определяется содержанием и значениями ряда факторов $f_{ij\Phi} \in F$ $(\Phi = 1,2 \ldots \Phi)$, которые способствуют началу реализации этого АНВ:

$$W_i\left(B_j\right)_T^{y2p} = W_T^{y2p}\left(f_{ij\phi} \in F\right) \tag{1.1}$$

где F – множество известных фактов.

Оценить указанные факторы можно с помощью количественной оценки системы из присутствия на интервале времени Т. Такая задача может быть решена только экспертными методами. Результаты экспертизы после соответствующей обработки авторы предлагают изучить в следующем виде:

$$W_i\left(в_j\right)_T^{y2p} = \sum_{\hat{0}}^{0} W\left(f_{ij\phi}\right)_T - \sum_{\alpha_1\beta} W\left(f_{ijp} \cap f_{ij\beta}\right)_T + \sum_{\alpha_1\beta_1\gamma} W(f_{ij\alpha} \cap f_{ij\beta} \cap f_{ij\gamma})_T - \ldots$$
$$\ldots + (-1)^{\phi-1} W(f_{ij1} \cap f_{ij2} \cap \ldots \cap f_{ij\hat{0}})_T \tag{1.2}$$

или в конечном варианте:

$$W_i\left(в_j\right)_T^{y2p} = 1 - \prod_{\hat{0}-1}^{0}\left(1 - W\left(f_{ij\varphi}\right)_T\right) \tag{1.3}$$

Анализ показывает [118], что предложенный подход дает весьма ограниченные возможности представления полученных оценок в качестве критерия оптимизации.

В работах [103; 124; 250] рассмотрен вариант вероятностного анализа угроз безопасности в виде сложной системы «авиационная безопасность – субъект противоправной деятельности» (АБ-СППД).

Достаточно часто при исследовании угроз безопасности применяют сеточное моделирование, в том числе с формализацией в виде дифференциальных уравнений в частных производных. Решение в этом случае может быть получено численными методами, например, методом Зейделя (см. 4.1).

Задача моделирования пространства угроз безопасности возникла при решении проблемы разработки требований к системе защиты объекта в соответствии с уровнем угроз.

Процесс распространения угрозы для распределенных объектов может рассматриваться как процесс диффузии. Тогда математической моделью распространения угрозы будет уравнение диффузии. Решение уравнения диффузии – это нахождение зависимости концентрации вещества (или иных объектов) от пространственных координат и времени, причем задан коэффициент (в общем случае также зависящий от пространственных координат и времени), характеризующий проницаемость среды для диффузии [39; 254]:

$$\frac{\partial}{\partial x}\left(\sigma(x,y)\frac{\partial u}{\partial x}\right)+\frac{\partial}{\partial y}\left(\sigma(x,y)\frac{\partial u}{\partial y}\right)=f(x,y),\quad (x,y)\in D, \tag{1.4}$$

где u - уровень угрозы, $\sigma(x,y)$ – проницаемость угрозы, $f(x,y)$ – плотность распределения источников опасности.

Правая часть $f(x,y)$ уравнения означает некоторые источники угрозы. На начальных этапах исследования ограничимся рассмотрением точечных источников угроз. Возможно пространственное распределение источников угроз с некоторой плотностью.

По аналогии с другими процессами диффузии введем понятия «проницаемость среды» и «плотность распределения источников угроз». Проницаемость среды характеризует некое препятствие среды распространению угроз. Будем считать, что плотность источников угроз носит относительный характер, определенный по некоторой шкале угроз. Привязка этих значений к конкретным угрозам представляет самостоятельную задачу.

Таким образом, уровень угрозы в конкретной точке пространства будет определяться расположением источника угрозы относительно этой точки, значением угрозы и проницаемостью среды для угрозы.

В своих работах [120; 125; 127; 129; 130; 136; 137; 259] автор представил анализ возможностей использования математических моделей при решении задач обеспечения АБ и показал, что в прямой постановке задача не может быть решена в связи с непреодолимыми трудностями формализации. Для таких задач решение необходимо не получить, а принять. Предлагается модель, которую автор назвал

эвристической. В основе модели лежит математическое представление моделируемых функций, а по входу модели (формализация) и по ее выходу (интерпретация результатов) используются эвристические процедуры. Модель может быть названа математической в достаточной степени условно. Целый ряд серьезных обстоятельств автор намеренно не принимает во внимание, в частности, функция проницаемости представлена в модели далеко неадекватно, без учета скачков и разрывов на границе области. Автора это обстоятельство устраивает, поскольку проницаемость введена в модель с одной целью: показать принципиальную возможность регулирования уровня опасности.

Проблемы, связанные с неопределенностью в процедурах формирования пространства угроз безопасности, остаются как по входу системы, т.е. при идентификации исходных параметров, так и по выходу, т.е. при интерпретации результатов [56; 132].

Наряду с указанными выше проблемами математического моделирования пространства угроз безопасности аэропорта возникает еще одна проблема, связанная с особенностями выбранной модели угроз в формате краевой задачи. Как было показано в работе [135], уравнение диффузии является далеко не единственным, которое может быть выбрано в качестве модели, существует достаточно представительная линейка дифференциальных уравнений в частных производных, из которой может быть осуществлен выбор. Характер уравнения определяется порядком частных производных, числом независимых переменных, линейностью, однородностью, видами коэффициентов уравнения, стационарностью. Линейные дифференциальные уравнения в частных производных второго порядка делятся на три типа: эллиптические уравнения, если $B^2 - 4AC < 0$, параболические уравнения, если $B^2 - 4AC = 0$, гиперболического типа, если $B^2 - 4AC > 0$ [6].

Значения функции ищутся внутри некоторой области *S*, ограниченной поверхностью Г для трехмерных задач или линией Г для двумерных задач. На

границе задаются *граничные условия*, многие из которых могут быть представлены в виде

$$\left(\alpha u + \beta \frac{\partial u}{\partial n}\right)_{\Gamma} = f, \qquad (1.5)$$

где α и β – заданные функции точки границы Г;

f – известная функция, возможно, зависящая от решения u;

$\partial u/\partial n$ – производная искомой функции по нормали к границе Г.

Для нестационарных задач, описывающих процессы во времени, должны быть также заданы начальные условия $u_{|t=0} = \varphi$, описывающие состояние объекта в начальный момент времени.

Вопрос о выборе уравнения, адекватно описывающего гипотетическое поле защиты объекта транспортной инфраструктуры, остается открытым. Наиболее прогнозируемым вариантом является модель, включающая несколько типов уравнений, тогда прямое математическое моделирование невозможно и предлагается использовать физическое моделирование на основе гибридных сеточных моделей, которые представляют собой аналого-цифровой вычислительный комплекс (АЦВК) класса сетка-ЦВМ, сочетающий аналоговые возможности моделирующей сетки и цифровые преимущества компьютерной обработки информации.

Формируя модель защиты на основе угроз безопасности, необходимо учитывать следующие положения:

– кроме известных (прогнозируемых) угроз всегда существуют неизвестные, количество которых бесконечно,

– для известных угроз существует бесконечное количество способов их реализации,

– в любой момент времени возможно возникновение любого количества угроз, включая ранее неизвестные,

– любые меры защиты не исключают реализации актов незаконного вмешательства,

– для любого объекта существует модель нарушителя, против которой существующая система защиты неэффективна.

Таким образом, исследование угроз безопасности с учетом представленных положений всегда дает не точный, предполагаемый результат, даже если он цифровой, что переводит методологию моделирования в разряд эвристических технологий.

1.5 Анализ проблем уязвимости аэропорта

Уязвимость некоторого объекта транспортной безопасности определяется состоянием объекта защиты, которое сложилось в результате противодействия совокупности угроз безопасности и системы защиты, что характеризуется некоторым пространством угроз, которому противостоит некоторое пространство защиты, в результате чего образуется пространство безопасности аэропорта, соответствующее приемлемому уровню уязвимости (безопасности), поскольку абсолютной безопасности не существует. Состояние здесь понимается как отвлеченное понятие, обозначающее множество устойчивых значений переменных параметров объекта. Уровень безопасности – это степень защищенности транспортного комплекса, соответствующая степени угрозы совершения АНВ.

Пространство следует понимать, как форму существования материальных объектов и процессов, характеризующую структурность и протяженность материальной системы, и обладающее протяженностью. В таком случае, уязвимость выступает как критерий оптимизации процессов управления транспортной безопасностью. Понятие уязвимость определяется [156] степенью защищенности объектов транспортной инфраструктуры от несанкционированного вмешательства в их деятельность (Рисунок1.6).

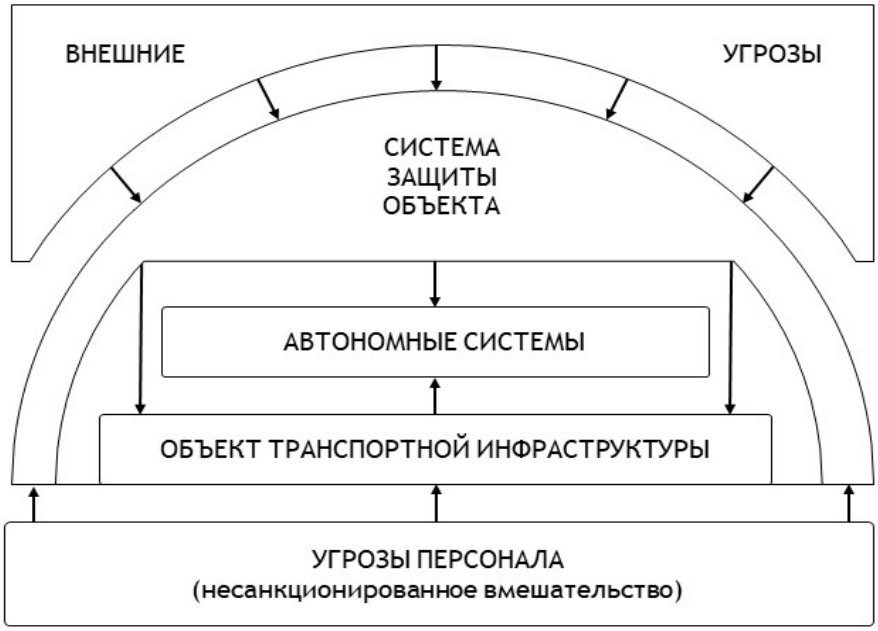


Рисунок 1.6 – К понятию уязвимость объекта транспортной инфраструктуры

Оценка уязвимости объектов транспортной инфраструктуры понимается как процесс определения степени защищенности ОТИ и ТС от угроз совершения актов незаконного вмешательства [131].

Порядок проведения оценки уязвимости [163] предполагает наличие определенных методик оценки, процедур оценки и параметров объекта, которые могут быть реализованы и получены только при идентификации объектов, по отношению к которым они применялись, т.е. требуется исследование объекта и его структуризация. При этом должны быть определены технические, технологические и эксплуатационные характеристики объекта, его критические элементы, потенциальные угрозы и способы их реализации, на основе чего разрабатывается система мер защиты (Рисунок 1.7).

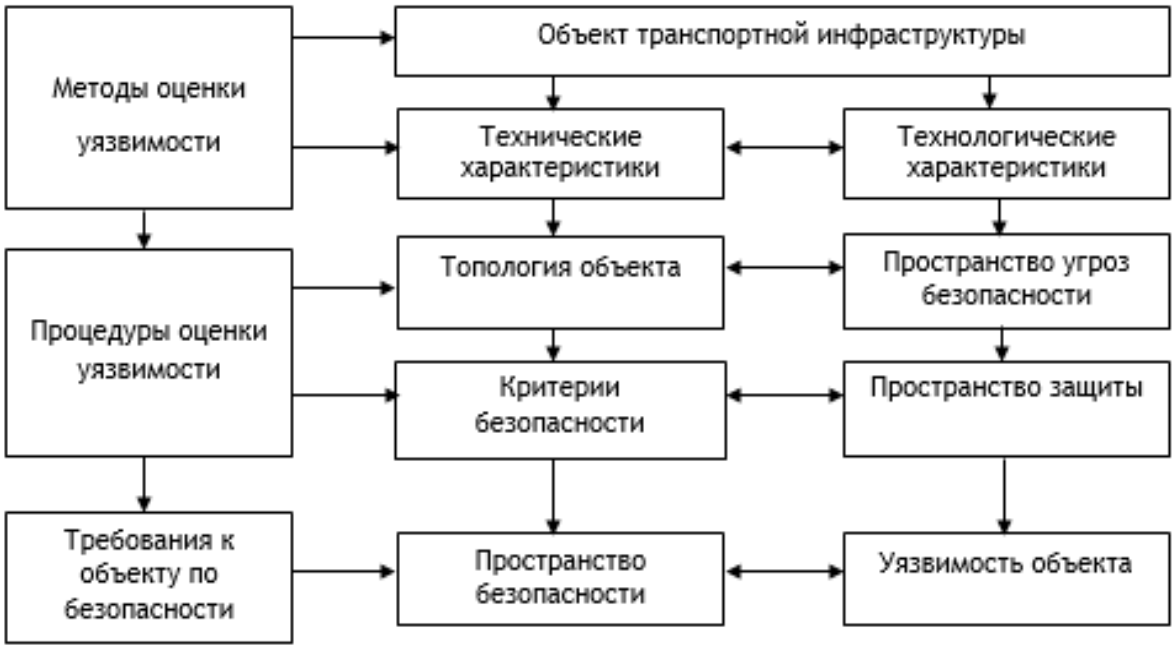


Рисунок 1.7 – Уязвимость как критерий безопасности

При оценке уязвимости используется модель нарушителя, рекомендованная Минтрансом России [163].

Примерная структура документа «Результаты оценки уязвимости ОТИ и ТС воздушного транспорта» состоит из следующих разделов:

1. Введение.
2. Результаты изучения технических и технологических характеристик ОТИ и ТС и порядка его функционирования.
3. Результаты обследования системы принятых на ОТИ и ТС мер по защите от АНВ.
4. Способы реализации потенциальных угроз совершения АНВ.
5. Рекомендации субъекту транспортной инфраструктуры в отношении мер, которые необходимо дополнительно включить в систему мер по обеспечению транспортной безопасности ОТИ и ТС.

Определяется перечень критических элементов ОТИ и анализируются потенциальные угрозы совершения АНВ в деятельности ОТИ с точки зрения определения наиболее вероятных из них применительно к критическим элементам.

В соответствии с введенными оценочными значениями определяются количественные показатели угроз, на основе чего определяются наиболее вероятные угрозы для каждого критического элемента (КЭ).

Модель нарушителя представляет собой совокупность качественных и количественных характеристик нарушителя и определяется по количественным показателям и статистическим данным. Для определения количественных значений показателей типов нарушителей на ОТИ вводятся оценочные значения.

Для определения способов реализации потенциальных угроз совершения акта незаконного вмешательства применительно к критическим элементам ОТИ проведено моделирование различных сценариев реализации угроз АНВ (Рисунки 1.8 и 1.9).

Рисунок 1.8 – Показатели модели нарушителя для КЭ

Оценка возможных последствий при реализации потенциальных угроз АНВ в деятельность ОТИ определялась для пессимистической концепции, предполагающей, что нарушители хорошо подготовлены и информированы, и способны нанести ущерб в наиболее неблагоприятных для объекта условиях о времени и месту.

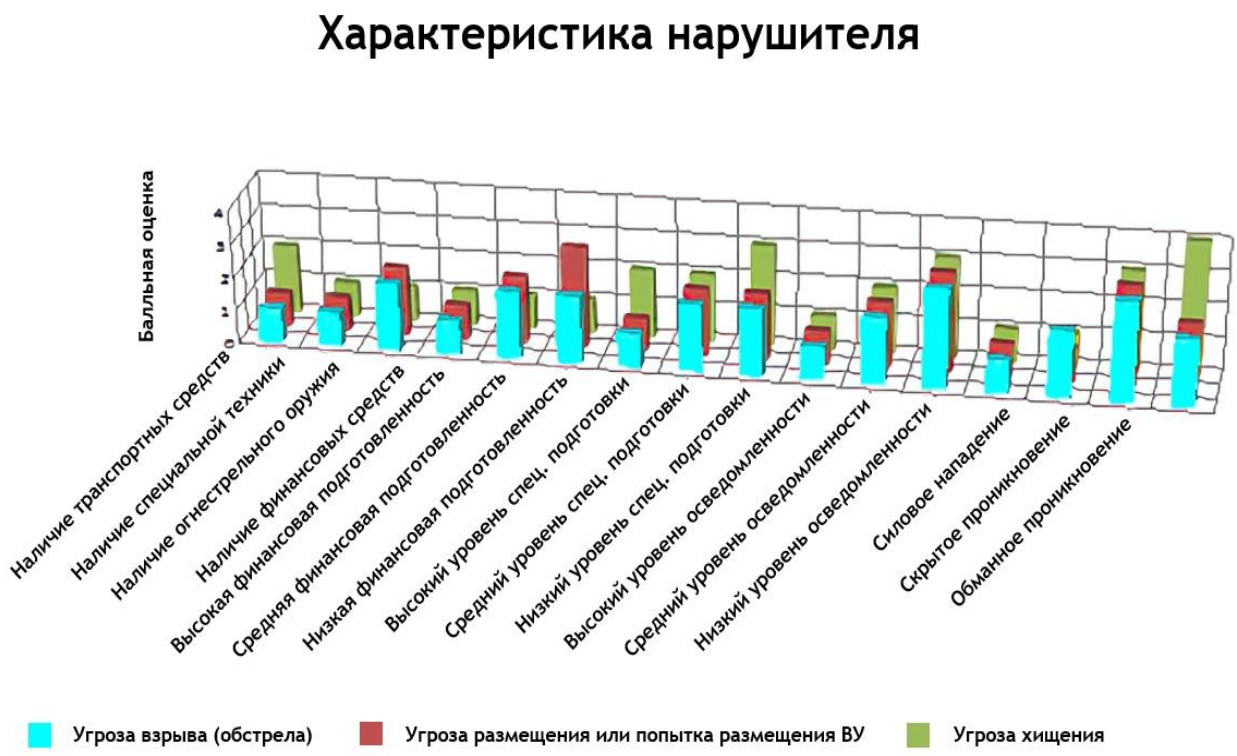


Рисунок 1.9 – Общие характеристики модели нарушителя для КЭ

При определении возможных последствий (ущерба) при реализации потенциальных угроз АНВ, оценивается шесть видов частных потерь: политические, людские, прямые финансовые, экономические, информационные, экологические.

Политические потери – потери, выражающиеся в снижении авторитета различных уровней власти и возникающей в связи с этим нестабильностью в обществе.

Под людскими потерями понимаются потери, выражающиеся в утрате жизни людей, а также их здоровья, квалифицированного присвоения любой группы инвалидности.

Финансовые потери заключаются в непосредственной утрате материальных ценностей в результате АНВ и других действий нарушителей.

Экономические потери в стоимостном выражении учитывают экономические потери, определяемые потерей связей с предприятиями-смежниками. В настоящее время методики, позволяющие достоверно количественно оценить экономические потери, отсутствуют.

Под экологическими потерями понимаются потери природных ресурсов, приводящие к ухудшению социально-гигиенических условий проживания населения. Для подсчета экологических потерь существуют достаточно строгие аналитические методики.

Информационные потери в результате действий нарушителей на ОТИ, в соответствии с обобщенным их пониманием, заключаются в утратах конфиденциальной информации и передовых технологий.

1.6 Анализ проблем несанкционированного вмешательства персонала в производственную деятельность аэропорта

Проблемы несанкционированного вмешательства персонала, обеспечивающего транспортную безопасность, в производственную деятельность аэропорта достаточно специфичны и в значительной мере связаны с вопросами адекватности алгоритмов профессиональной деятельности персонала и стандартных эксплуатационных процедур, в которых прописаны параметры функционирования аэропорта, соответствующие требованиям приемлемого уровня безопасности, достижение которого становится целью и условием профессиональной деятельности персонала. При этом на первый план выдвигаются вопросы оценки уровня профессиональной подготовки персонала.

Существуют различные подходы к оценке профессиональных качеств специалиста. Они основаны на процедурах формализации исходной модели специалиста. А также на совокупности тех факторов и характеристик, которые исследователь предполагает использовать в своей модели. Особенно важным является такое исследование в динамике [32; 57; 103].

Оценки человеческого фактора используются для принятия управленческих решений и могут быть приняты только тогда, когда с достаточной степень точности определены профессиональные требования к авиационным специалистам.

При этом необходимо иметь в виду следующие обстоятельства [103].

1. Необходимо учитывать конфликтность любого выбора.

2. Следует исключить многовариантность и неопределенность исходной информации.

3. Управленческие решения должны приниматься в динамике, поскольку часть профессиональных качеств должна присутствовать на начальном этапе профессиональной деятельности специалиста, а остальные характеристики должны формироваться в процессе трудовой деятельности и являются основой управления.

4. Необходимо учитывать определенную динамику самих требований. Изменение внешних и внутренних условий реализации производственной деятельности влечет за собой изменения в целях деятельности организации и заставляет менять характеристики производственного процесса.

5. Окончательное управленческое решение должно учитывать практически неизбежный субъективизм оценочных процедур, который может быть снижен только статистически.

6. Количество оценочных процедур должно быть достаточно велико не только с точки зрения статистической достоверности, но и для того, чтобы процесс управления носил плавный, монотонный характер, исключающий экстремальные, чаще всего необоснованные решения.

7. Вопрос о точности принятия управленческого решения сводится к проблеме определения допустимой нормы расхождения между требованиями и реальными характеристиками специалистов.

8. Методы и процедуры оценки профессиональных качеств специалистов требуют дальнейшего исследования на новой научной платформе, выключающей методы прогнозирования [103].

Разработан достаточно широкий математический аппарат методов прогнозирования: математическая подгонка полиномами, экстраполяция по элементарным функциям, экстраполяция с дисконтированием, функции с гибкой структурой, экстраполяция по огибающим кривым, авторегрессионные модели, парные и тождественные регрессии, компонентный анализ, многофакторный анализ, экстраполяция факторов [194; 195].

Использование экстраполяции в прогнозировании имеет в своей основе предположение о том, что рассматриваемый процесс представляет собой сочетание регулярной и случайной составляющих, при этом регулярная составляющая представляет собой гладкую функцию от аргумента (тренд, уровень, тенденция), а случайная составляющая считается некоррелированным случайным процессом с нулевым математическим ожиданием [193].

Процедура сглаживания направлена на линеаризацию случайных отклонений точек ряда от некоторой гладкой кривой тренда. Наиболее распространённой темой является линейное сглаживание [118]:

$$\begin{aligned} \tilde{y}_0 &= \frac{1}{3}(y_{-1} + y_0 + y_{+1}) \\ \tilde{y}_{-1} &= \frac{1}{6}(5y_{-1} + 2y_0 - y_{+1}) \\ \tilde{y}_{+1} &= \frac{1}{6}(-y_{-1} + 2y_0 + 5y_{+1}) \end{aligned} \qquad (1.6)$$

где y_0, $\tilde{y}_0$ – значение исходной и сглаженной функций в средней точке,

y_{-1}, $\tilde{y}_{-1}$ – значение исходной и сглаженной функций в левой от средней точки,

y_{+1}, $\tilde{y}_{+1}$ – значение исходной и сглаженной функций в правой от средней точки [118].

В качестве критерия, по которому можно судить о нецелесообразности повторного сглаживания, можно использовать выражение:

$$\max\{|y_i - \tilde{y}_i|\} \leq \varepsilon \tag{1.7}$$

В общем виде формула сглаживания для средней точки скользящей группы m=2p+1 точек имеет вид:

$$\tilde{y}_t = \frac{1}{m}\sum_{i=t-p}^{t+p} y_i \tag{1.8}$$

Задача о приближении ставится в общем случае следующим образом: данную функцию f(t) требуются приближённо заменить обобщённым полиномом

$$Q(x) = c_0\phi_0(x) + c_1\phi_1(x) + \cdots + c_m\phi_m(x) \tag{1.9}$$

так, чтобы отклонение в некотором смысле функции f(x) от Q(x) на заданном множестве X=$\{x\}$ было наименьшим.

Наиболее важными для практики являются степенный полиномы вида:

$$Q(x) = a_0 + a_1x + a_1x + a_2x + \cdots + a_mx^m \tag{1.10}$$

Применительно к ним можно сформулировать задачу интерполирования в следующем виде: для данной функции f(x) найти полином Q(x) возможно низшей степени m, принимающий в заданных точках x_i (i=1, 2, …, n) те же значения, что и f(x). Заданная система точек x_1, x_2, …, x_n называется узлами интерполирования, а полином Q(x) – интерполяционным полиномом.

Если n≤m, то можно положить m=n и определить коэффициенты разложения a_1 из системы уравнений:

$$\begin{cases} a_0 + a_1x_0 + \cdots + a_nx_0^n = y_0 \\ a_0 + a_1x_1 + \cdots + a_nx_1^n = y_1 \\ a_0 + a_1x_n + \cdots + a_nx_n^n = y_n \end{cases} \tag{1.11}$$

Определитель этой системы является определителем Вундермана [145]. Эта система имеет единственное решение. Этим решением будет интерполяционный полином Лагранжа:

$$L_n(x) = \sum_{i=0}^{n} \frac{(x-x_0)\dots(x-x_{i-1})(x-x_{i+1})\dots(x-x_n)}{(x_i-x_0)\dots(x_i-x_{i-1})(x_i-x_{i+1})\dots(x_i-x_n)} * y_i \quad (1.12)$$

Если $n < m$, то интерполяция невозможна, так как число узлов превосходит степень полинома и система становится некорректной. В этом случае переходят к приближенной интерполяции, как правило, к точечному квадратичному аппроксимированию [193].

Основная идея прогнозирования при помощи экстраполяции динамических рядов базируются на предположении сохранении закона изменения прогнозируемой переменой, выявленного на ретроспективном участке, на определенном интервале времени в будущем [194].

Метод движущейся средней предлагает в качестве дисконтирующей функции использовать единичную ступенчатую функцию вида

$$\omega(t_0) = \begin{cases} 1 \text{ для } t_0 - t_p \le t \le t_0 \\ 0 \text{ для } t < t_0 - t_p \end{cases} \quad (1.13)$$

где t_p – последний момент времени ретроспективного участка,

t_0 – момент времени начала ретроспекции.

Метод прогнозирования по огибающим направлен на преодоление ограниченности экстраполяции путем перехода на более высокий уровень агрегирования тенденций.

Основная цель метода – объединение частных тенденций, составляющих процесс, в единую общую. Огибающая дает возможность выявить общую тенденцию развития, оценить пределы её развития, характер приближения к этим пределам.

В задачах прогнозирования уровня развития специалиста прогнозируемой характеристикой *У* может выступать количество тех или иных качеств человека, соответствующее определенному уровню квалификации. Входными параметрами $X=\{x_1 \dots\dots x_n\}$ могут выступать некоторые технологические характеристики модели, Q_j – скорость изменения этих характеристик, *So* – некоторая аддитивная ошибка, возникающая в результате определения исходных данных. В этом случае

регрессионная модель состояния качества подготовки специалиста описывается уравнением регрессионного анализа

$$\tilde{y} = \sum_{j=1}^{n} Q_j x_j + S_0 \quad (1.14)$$

Под прогнозом развития специалиста понимается правдоподобная оценка возможных результатов и путей будущего развития способностей человека, а также требуемых для этого ресурсов [194].

Одним из подходов к решению данной проблемы является метод прогнозного графа, в основе которого лежит объединение методики экспертной оценки и методов сетевого планирования. Результатом работы является построение графа взаимосвязанных событий, или графа соподчиненности.

Обобщенную оценку качества работы в системе человек-техника можно представить функционалом:

$$W_{\sum} = \sum_{j=1}^{n} a_j \sum_{i=1}^{m_j} \beta_{ij} w_{ij} \text{ , где} \quad (1.15)$$

$$\sum a_j = 1,\ j = [1, n]; \quad , \sum \beta_{ij} = 1,\ i = [1, m_j], \quad (1.16)$$

n – число групп, объединяющих по какому-либо признаку критерии, выбранные для оценки деятельности человека в системе m_j – число критериев в j – группе, a_j – весовой коэффициент j-ой группы, β_{ij} - весовой коэффициент i-го критерия из j-ой группы, w_{ij} –балльная оценка i- го критерия из j- ой группы.

Использование метода статистического анализа предполагает предварительное накопление информации о значениях показателей $\{q_n\}$, характеризующих возможности специалистов [195].

К методам многофакторного анализа можно отнести метод группового учета аргументов МГУА [96]. Он представляет собой автоматизированный поиск оптимальной модели с помощью последовательного перебора генерируемых по определенным правилам усложняющихся моделей – претендентов, отбираемых по внешним критериям. Внешний критерий при усложнении моделей имеет минимум, что дает возможность найти единственную оптимальную модель. В качестве внешнего критерия обычно используется критерий регулярности следующего вида:

$$\Delta = \sqrt{\sum_{t=m+1}^{m+n} (y(t) - \overline{y}(t))^2 n^{-1}} \,, \qquad (1.17)$$

где n – число наблюдений обучающей выборки,

m – число наблюдений проверочной выборки,

$y\,(t)$ – табличные исходные значения входной переменной,

$\overline{y}\,(t)$ – значения, рассчитанные по модели, коэффициенты которой определялись по обучающей выборке наблюдений.

Алгоритм МГУА основывается на определении оптимальной по сложности модели из некоторого класса моделей. Наиболее часто исходное множество людей представлено в виде многочлена [118]

$$y = \sum_{i=1}^{l} a_i \prod_{k=1}^{m} x_k^{a(i,k)} \text{ , где} \qquad (1.18)$$

y – выходная, а x – входная переменные,

m – количество входных переменных,

ℓ – число слагаемых в модели,

i – 0,1,2 …

Заданы таблицы исходных данных $Y(n)$ и $X\,(m,\ n)$. Параметры i, l и a определяются в ходе моделирования.

Метод динамики средних оперирует понятием эшелона – группы специалистов, объединенных по определенному признаку. Понятие эшелона интерпретируется в зависимости от подхода к структуризации системы и в случае специалиста предполагает различные квалификационные уровни или место специалиста внутри одного квалификационного уровня. Специалисты в силу ряда причин могут переходить из одного эшелона в другой.

Пусть имеется сложная система S, состоящая из большого числа N однородных элементов, каждый из которых может случайным образом переходить из состояния в состояние. Предположим, что все потоки событий, переводящие систему S из одного состояния в другое – пуассоновские, тогда процесс, протекающий в системе, будет марковским. Если известны вероятности состояний одного элемента $P_1,\ P_2 \ldots P_n$, как

функции времени, то известны и средние численности состояний $m_1 \ldots\ldots m_n$ и их дисперсии $\sigma_1 \ldots\ldots \sigma_n$.

Метод динамики средних заключается в том, что вместо дифференциальных уравнений Колмогорова для вероятностей состояний составляют уравнения непосредственно для средних численностей состояний и интегрируют их при других начальных условиях, соответствующих начальным численностям состояний [118].

При переходе к управлению ТБ в современных системах безопасности ставится задача минимизации ЧФ и замены человеческого влияния на процессы обеспечения безопасности, во всех случаях, где это возможно, автоматизированными процедурами без участия человека.

Такой подход представляется автору неправомочным по следующим причинам.

1. Полностью автоматизированные системы безопасности представляются в некотором смысле утопией, поскольку любая автоматизация предполагает почти полную алгоритмизацию процедур, ее реализующих. В транспортной безопасности большинство процессов трудно поддаются формальному описанию и алгоритмизации, а решаемые задачи являются плохо формализуемыми и слабоструктурированными.

2. По мере развития и усложнения систем безопасности доля человеческого фактора в реализации процедур безопасности заметно увеличивается.

3. Дискредитация человека как самого слабого звена принципиально не правомочна, поскольку существует достаточно широкий класс задач, процессов, процедур, где человек (специалист), и только он, обладает существенными преимуществами по сравнению с техникой.

Иными словами, должен ставиться вопрос не о минимизации человеческого фактора, а о существенном изменении смысла и содержания понятия человеческий фактор.

Из понятия ЧФ можно вычленить личностный фактор (ЛФ), т.е. все, что связано с характеристиками человека. В этой части исследование ЧФ состоит в изучении достоинств и недостатков специалиста как участника производственного процесса с последующим ограничением степени его участия в соответствии с профессиональными возможностями.

Во второй части можно сконцентрировать то, что связано с техникой и ее взаимодействием со специалистом. Здесь вопрос ставится о взаимной адаптации параметров человека и техники к условиям и задачам, решаемым в рамках управления ТБ.

Хотелось бы обратить внимание на третий аспект, который в современных работах по человеческому фактору остается за рамками исследований. В процессе выполнения производственных операций персонал авиационных организаций достаточно часто выходит за рамки установленного алгоритма деятельности, руководствуясь совсем не обязательно какими-то негативными устремлениями. Часто наоборот: желая повысить эффективность своей работы, принимаются решения, которые при всей своей привлекательности могут привести к сугубо негативным результатам, вплоть до авиационного происшествия с катастрофическими последствиями. В этом случае персонал авиационной организации, принимающий участие в обеспечении транспортной безопасности, становится источником опасности и способен вывести ситуацию с объектом исследования из состояния равновесия, что проявляется, как минимум, через отклонения от требований по транспортной безопасности к объекту. В таком случае, появляется задача управления этими отклонениями с целью их минимизации, при этом параметром управления становится угроза (опасность) со стороны персонала авиационной организации в отношении безопасности объекта. На сегодняшний день эта задача становится наиболее актуальной и своевременной [112; 249; 256].

С точки зрения транспортной безопасности предлагается человеческий (личностный) фактор рассматривать как неизбежное зло, исключая полезную

составляющую, и все его негативные проявления отнести к категории угроз безопасности. Возникает новая ситуация, когда необходимо минимизировать не человеческий фактор как таковой, а ставится задача регулировать негативное влияние персонала авиационной организации на процедуры выполнения производственной деятельности, рассматривая это влияние как угрозу безопасности объекта.

Причины, определяющие фактор негативного влияния персонала, проявляются как расхождения, отклонения, несоответствия с алгоритмом деятельности. Дело в том, что в транспортной безопасности вся производственная деятельность строго регламентирована и узаконена в формате стандартных эксплуатационных процедур (СЭП). СЭП – это технология, правило или инструкция, разработанные уполномоченным должностным лицом для того, чтобы данная конкретная задача (процедура) выполнялась в соответствии с установленными требованиями по обеспечению транспортной безопасности и обеспечивала достижение поставленной задачи (процедуре) цели [103].

Угроза персонала – далеко не всегда потенциальное событие, достаточно часто эти угрозы реализуются, проявляясь как некоторые негативные результаты деятельности авиационного специалиста, что в пределе может быть АНВ и даже террористическим актом.

Угрозы со стороны персонала, осуществляющего профессиональную деятельность по обеспечению транспортной безопасности, рассматриваются в составе общей совокупности угроз безопасности аэропорта, как один из типов угроз. В действительности это не совсем так.

Внешние угрозы и их типы определяются моделью нарушителя. На основе этой модели для каждого типа угрозы разработаны соответствующие меры противодействия, включая деятельность персонала и совокупность соответствующих технических средств защиты объекта.

Угрозы персонала рассматриваются как некоторый побочный результат профессиональной деятельности специалиста по обеспечению транспортной

безопасности. Это означает, что выделить отдельную угрозу или как-то их классифицировать невозможно в принципе. По этой же причине нельзя исследовать угрозы персонала как потенциальные, т.е. нельзя для каждой угрозы заранее разработать аппарат противодействия. В этом главная трудность исследования угроз персонала, которая препятствует использованию математических моделей и других классических методов исследования [109; 134].

Риск имеет множество разнообразных определений, но всегда это есть сочетание вероятности и последствий наступления неблагоприятных событий. Риск – это характеристика ситуации, имеющей неопределенность. Риск – это вероятность возможной нежелательной потери чего-либо. Риск – это вероятность выхода опасного фактора из-под контроля и серьёзность последствий. Риск – это произведение вероятности на убыток.

В гражданской авиации риск всегда связан с понятиями опасность и безопасность. Опасность понимается как возможность возникновения обстоятельств, при которых материя, поле, энергия, информация или их сочетание могут таким образом повлиять на сложную систему, что приведет к ухудшению или невозможности ее функционирования и развития.

Безопасность – это отсутствие какого-либо риска, в случае реализации которого возникают негативные последствия в отношении кого-либо или чего-либо. Безопасность – это такое состояние сложной системы, когда действие внешних и внутренних факторов не приводит к ухудшению системы или невозможности ее функционирования и развития. Безопасность объекта – это условия, при которых действия или бездействия по отношению к объекту не влекут за собой негативных последствий [2; 14; 31; 36; 173].

Стохастическому подходу соответствует вероятностный риск, основанный на заданных априорных вероятностях исходов.

Ситуационному подходу соответствует ситуационный риск, который характеризует возможные отклонения реальной ситуации от ее оценки, недоучет слабо уловимых признаков и скрытых тенденций. Количественная мера

ситуационного риска вводится условно на основании некоторой системы ценностей.

Оперативному подходу соответствует оперативный риск, характеризующий способность к предвидению и умению навязать желаемый способ действий взаимодействующей системе.

Оценка риска – это процесс определения величины (меры) риска. Инженерный подход к оценке риска опирается на статистику опасностей и вероятностный анализ безопасности. Модельный подход исследует воздействие опасных факторов. Экспертный подход использует не расчетные данные, а экспертные оценки. Социологический подход исследует отношение к разным видам риска.

Управление риском понимается как совокупность действий, направленных на снижение уровня технологического риска, уменьшение потенциальных потерь и других негативных последствий нежелательных событий. Количественно риск может быть определен как частота реализации определенной опасности.

Существует традиционный подход к обеспечению безопасности, основанный на концепции «абсолютной безопасности» – ALAPA (настолько низко, насколько это достижимо практически). В настоящее время успешно развивается концепция «приемлемого» риска – ALARA (настолько низко, насколько это достижимо в пределах разумного).

Риск как мера опасности впервые представлен в документах ИКАО [147; 165] и ИПУ РАН. В работе [28] предложена методология НРБ (надежность, риски, безопасность) исчисления рисков как «меру опасности». Здесь применяется развернутая трактовка математической модели рисков в виде «риск – мера количества опасности» в состоянии системы, когда возможно возникновение случайного дискретного события, которое несет нежелательные последствия или ущерб. Рассматриваются интерпретации понятий в рамках концепций Fuzzy Sets of Fujita M. (Tails – far from medium) и Малинецкого Г.Г. (Hard Tails from Risk Theory – ИПУ РАН):

– оценка значимости риска нежелательных последствий прогнозируемых результатов определяется на основе проактивного метода с помощью матрицы рисков в виде единственного числа, отражающего экспертное значение сочетания чисел,

– приемлемость расчетного проактивного риска находится путем его сравнения с допустимым уровнем приемлемого риска так, что величина расхождения двух уровней используется для выработки управляющих воздействий с целью повышения уровня безопасности,

– управление риском и управление безопасностью осуществляется путем воздействия на систему через факторы и условия возникновения опасных событий при конкретных видах и факторах опасности и при выявленных угрозах,

– методы снижения рисков, основанные на управлении состоянием системы, включают способы уклонения от факторов опасности.

Проактивный метод управления безопасностью на основе управления рисками является основным для повышения уровня безопасности путем прогнозирования априорно возможных негативных последствий от каждого опасного фактора. Активный метод управления рисками применяется при исследовании негативных ситуаций для выявления скрытых угроз. Операции по управлению безопасностью путем управления рисками составляют цепь последовательных действий: «угроза – рисковое событие – прогноз сценария событий – опасное состояние – оценка риска – управляющее воздействие» [5; 10].

1.7 Обоснование научной задачи диссертационного исследования

Авиационная транспортная система в своем развитии накопила достаточно серьезный опыт в решении задач обеспечения транспортной безопасности, позволяющий выявить определенные закономерности развития систем транспортной безопасности. С другой стороны, этот же опыт показывает, что состояние проблемы обеспечения транспортной безопасности в гражданской

авиации далеко не всегда отвечает современным требованиям и требует для своего решения новых подходов и методов (Рисунок 1.10).

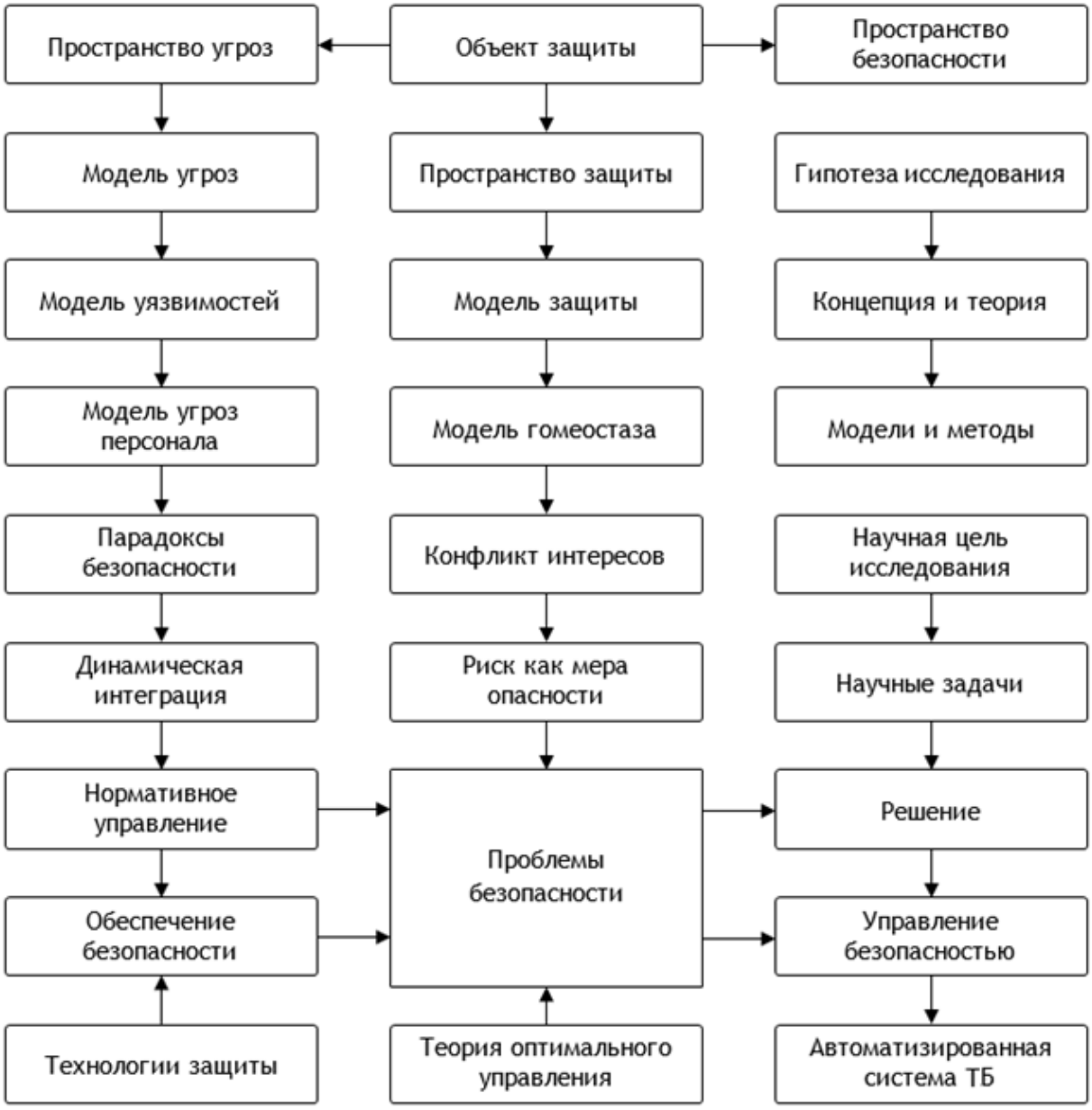


Рисунок 1.10 – Постановка научной задачи диссертационного исследования

При всем многообразии существующих здесь проблем можно выделить одну, без решения которой дальнейшее развитие систем безопасности становится весьма проблематичным.

Проблема. Современные системы управления транспортной безопасностью основаны на понятии обеспечение безопасности. В этом случае в системе реализуется нормативное управление, когда управляемый параметр (безопасность) в явном виде для управления не используется, а заменяется совокупностью нормативных документов, процессов и процедур, т.е. управление безопасностью можно рассматривать исключительно как вторичный процесс и результат. С другой стороны, информационное управление, которое, по сути, является автоматизированным, должно быть оптимальным в соответствии с принципом максимума Л. Понтрягина [93]. Реализация такого управления требует разработки адекватных математических моделей и формальных решений по алгоритмизации процессов управления транспортной безопасностью. Проблема усугубляется тем, что понятия обеспечение и управление безопасностью далеко не синонимы.

В таком случае решение проблем следует искать в рамках информационного управления.

Идея. Информационное управление транспортной безопасностью на основе адекватных математических моделей пространства безопасности и адаптивных алгоритмов оптимизации параметров системы защиты лежит в основе нового эволюционного класса систем автоматизированного управления – интеллектуальные комплексы.

Для реализации идеи в рамках данной работы выдвигается следующая гипотеза.

Гипотеза. Методология информационного управления транспортной безопасностью аэропорта, основанная на математическом моделировании в формате краевой задачи, понятии уязвимость и нейросетевом моделировании, обеспечит приемлемый уровень безопасности.

Методология предполагает следующие цель и задачи.

Цель исследования. Повышение уровня транспортной безопасности аэропорта путем создания системы информационного управления параметрами и процедурами на основе ситуационной модели объекта.

Задачи исследования.

1. Разработка ситуационной модели безопасности аэропорта в формате взаимодействующих и противоборствующих пространств угроз и защиты.
2. Моделирование пространства угроз безопасности объекта в формате краевой задачи в виде дифференциальных уравнений в частных производных.
3. Ранжирование и классификация субъектов пространства защиты объекта на основе нейросетевой модели.
4. Разработка методов парирования негативного влияния человеческого фактора.
5. Разработка структуры системы и процедур информационного управления транспортной безопасностью аэропорта.

В последние годы появилось достаточно много программно-компьютерных средств, реализующих новые, современные технологии обработки информации, такие как PSIM, BIG DATA, DATA MINING и другие, которые обладают исключительными возможностями для оперирования с большими массивами данных. Практическое использование указанных технологий в рамках информационного управления безопасностью осложняется тем, что в транспортной безопасности слабо развиты научные исследования по формализации и алгоритмизации процедур обеспечения безопасности, т.е. существует разрыв между низким уровнем математической постановки задач моделирования безопасности и высоким уровнем программно-технических средств решения этих задач. Иными словами, уровень развития теории транспортной безопасности не соответствует уровню требований, которые предъявляются со стороны авиационной транспортной системы.

Таким образом, в работе исследуются две научные проблемы безопасности: проблема управляемости и проблема алгоритмизации.

Структура диссертационного исследования представлена в таблице 1.1.

Таблица 1.1 – Структура диссертационного исследования

№	Основные понятия	Гл. 1	Гл. 2	Гл. 3	Гл. 4	Гл. 5
1	Транспортная безопасность	+	+	+	+	+
2	Авиационная безопасность	+	+	+	+	+
3	Безопасность полетов	+	–	–	–	–
4	Незаконное вмешательство	+	+	+	+	+
5	Объект транспортной инфраструктуры	+	+	–	–	–
6	Обеспечение ТБ	+	–	+	+	+
7	Управление ТБ	+	+	+	+	+
8	Теория ТБ	+	+	+	+	+
9	Гипотеза	+	–	–	–	–
11	Концепция	–	+	–	–	+
12	Предметная область	+	–	–	–	–
13	Эвристические модели	–	–	+	+	+
14	Физические модели	–	+	–	–	–
15	Математические модели	–	+	+	+	+
16	Квалиметрия	+	–	–	+	+
17	Эвристический подход	+	+	–	–	–
18	Теория принятия решений	+	+	–	+	+
19	Ситуационное управление	+	–	+	–	+
20	Уровень ТБ	+	+	+	–	+
21	Динамическая интеграция	+	–	–	–	–
22	Адаптивная система защиты	+	–	–	+	–
23	Уязвимость	+	–	+	+	–
24	Человеческий фактор	+	–	–	–	+

Продолжение таблицы 1.1

№	Основные понятия	Гл. 1	Гл. 2	Гл. 3	Гл. 4	Гл. 5
25	Личностный фактор	+	–	–	–	+
26	Авиационный персонал	+	–	–	–	+
27	Персонал сил обеспечения транспортной безопасности	–	–	–	–	+
28	Оценочный подход	–	+	+	–	+
29	Организационно-нормативное управление	+	–	–	–	–
30	Автоматизированная система управления	+	+	+	+	+
31	Обнаружение – отражение – ликвидация	–	–	–	+	+
32	Оптимальное управление	+	+	+	–	–
33	Критерий управления	+	+	+	–	–
34	Состояние (ситуация) объекта	+	+	+	–	–
35	Пространство угроз	+	–	+	+	–
36	Пространство защиты	+	–	+	–	–
37	Пространство безопасности	+	–	+	–	–
38	Единая и неделимая безопасность	+	–	–	–	–
39	Интегральная безопасность	+	–	–	–	–
40	Триада гипотетических полей	+	+	+	–	–
41	Приемлемый уровень безопасности	–	+	+	+	+
42	Математическая формализация	+	+	+	+	+
43	Краевые задачи	+	+	–	+	–
44	Система дифференциальных уравнений в частных производных	–	+	–	+	–

Продолжение таблицы 1.1

№	Основные понятия	Гл. 1	Гл. 2	Гл. 3	Гл. 4	Гл. 5
45	Качество защиты	–	+	–	–	+
46	Потенциальные угрозы	+	–	–	–	–
47	Информационно-управляющее пространство	+	+	+	–	–
48	Информационное управление ТБ	+	+	+	+	+
49	Ситуационная модель безопасности	–	+	+	–	+
50	Адаптивная перестройка структуры	–	+	–	–	+
51	Нейросетевое моделирование	–	+	+	+	+
52	Парирование негативного влияния персонала	–	–	–	–	+
53	Лингвистическое описание	+	+	–	–	–
54	Многофакторность		+	+	–	–
55	Многокритериальность	+	+	+	–	–
56	Акт незаконного вмешательства	+	+	+	+	+
57	Эволюция систем АБ	+	–	–	–	–
58	Автономные системы ТБ	+	–	–	–	–
59	Централизованная обработка информации в ТБ	+	–	–	–	–
60	Интегрированная система ТБ	+	–	+	–	–
61	Комплексная система ТБ	+	–	–	–	–
62	Инцидентное управление ТБ	+	–	+	–	–
63	Системные параметры интеграции	–	–	+	–	–
64	PSIM	+	–	+	–	+
65	Date Mining	–	–	+	–	+
66	Big Date	–	+	+	–	+

Продолжение таблицы 1.1

№	Основные понятия	Гл. 1	Гл. 2	Гл. 3	Гл. 4	Гл. 5
67	Многокритериальное управление ТБ	–	+	+	–	–
68	Субъект противоправной деятельности	+	–	+	–	–
69	Слабо структурированная задача	+	+	–	+	–
70	Плохо формализованная задача	+	+	–	+	–
71	Угроза персонала ТБ	–	+	–	–	+
72	Несанкционированное вмешательство	–	–	–	–	+
73	Противоправные действия	–	–	+	–	+
74	Управляемость	–	–	+	–	–
75	Открытая платформа	–	–	–	+	–
76	Единая информационная среда	+	–	+	–	–

Выводы к главе 1

1. В действующих системах транспортной безопасности реализована концепция обеспечения безопасности в терминах теории управления организационными структурами, т.е. информационный менеджмент. Результаты анализа проблем обеспечения безопасности дают основания утверждать, что современные системы далеко не всегда отвечают требованиям по эффективности, надежности и адаптивности. Требуется информационное управление в терминах теории оптимального управления, т.е. главная научная проблема, проблема управляемости, состоит в обосновании и реализации корректного перехода от обеспечения транспортной безопасности к информационному управлению безопасностью. Проблема усугубляется слабой проработанность алгоритмического и модельного ряда процедур информационного управления безопасностью.

2. Разработана гипотеза исследования, предполагающая решение проблем на основе методологии интеллектуального управления безопасностью с

применением компьютерных технологий PSIM, Data Mining, Big Data, краевых задач теории поля и нейросетевых моделей.

3. Предложено формировать интеллектуальное управление транспортной безопасностью на базе информационно-управляющего пространства, построенного с использованием трех гипотетических пространств: пространства угроз, пространства защиты и пространства безопасности.

4. Установлено, что информационное управление транспортной безопасностью является многокритериальным. Критериями оптимальности управления являются угрозы безопасности, уязвимость объекта транспортной инфраструктуры и уровень готовности персонала к выполнению производственной деятельности.

5. Предложено рассматривать персонал сил транспортной безопасности как источник угрозы в части, касающейся незаконного вмешательства персонала в производственную деятельность по управлению транспортной безопасностью.

ГЛАВА 2 ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ АЛГОРИТМИЧЕСКОЙ СОВМЕСТИМОСТИ ИНФОРМАЦИОННОГО МЕНЕДЖМЕНТА И ОПТИМАЛЬНОГО УПРАВЛЕНИЯ ТРАНСПОРТНОЙ БЕЗОПАСНОСТЬЮ АЭРОПОРТА

2.1 Управление как исключающая альтернатива обеспечению транспортной безопасности

Современные системы транспортной безопасности построены на принципе обеспечения безопасности. Это означает, что объект защиты рассматривается как сложная система, управление которой осуществляется на основе анализа ситуации, сложившейся в объекте под влиянием внешних условий. При этом параметр управления, безопасность, в явном виде не используется. Обеспечение осуществляется в рамках нормативного управления, когда безопасность нормируется, утверждаются нормативные документы и процедуры, а безопасность оценивается как степень соответствия требованиям, заложенным в эти документы. Обеспечение реализуется в соответствии с теорией управления организационными системами.

С другой стороны, для управления необходимо измерять параметры безопасности, их анализировать, сравнивать с эталоном и, при появлении несоответствий, принимать управляющие решения. Не зависимо от того, какой тип управления используется, принимаемые решения должны быть оптимальными в смысле некоторого или некоторых критериев. Отсюда, появляются две задачи: обеспечение оптимальности управления в условиях многокритериальности и снижение уровня многокритериальности, которая существенно усложняет задачу. Таким образом, управление безопасностью рассматривается как альтернатива обеспечению и реализуется в рамках теории оптимального управления.

Управление – это организованное воздействие на какую-либо систему с целью достижения желаемых результатов. Управлять безопасностью это значит

осознанно переводить объект из одного состояния (опасное) в другое (менее опасное). Управление безопасностью – это система сбора и обработки входной информации об угрозах для безопасности с упреждением во времени (прогнозирование), зависящим от необходимого времени на реализацию контрмер. Включает: систему оценки риска эксплуатации объекта на текущий момент времени при прогнозируемых угрозах; критерий принятия решения (решающее правило) для лица, принимающего решения; управляющие воздействия, влияющие на безопасность. Задача принятия решения направлена определение наилучшего (оптимального) способа действий для достижения поставленной цели.

Анализ предполагает исследование трех критериев оптимизации процессов управления транспортной безопасностью: угрозы безопасности объекта защиты, уязвимость объекта защиты и авиационный персонал, рассматриваемый с точки зрения его негативного вмешательства в процедуры управления.

Угрозы безопасности объекта защиты представляют собой любое внешнее или внутреннее вмешательство в производственную деятельность авиапредприятия, приводящее к нарушению установленных алгоритмов обеспечения безопасности. Проблема угроз с точки зрения критерия оптимизации заключается в некоторой неопределенности их идентификации и формального представления. Если угроза реализована, то ее исследование возможно статистически, что дает эффект только при накоплении определенного набора данных. С точки зрения оптимизации управления такой эффект минимален. Если угрозы рассматривать как потенциальные, что и необходимо делать, исследование таких угроз резко усложняется из-за проблем формализации.

Понятие уязвимость определяется степенью защищенности объектов транспортной инфраструктуры от несанкционированного вмешательства. Проблемы связаны с несовершенством методологии оценки уязвимости, трудностями формализации и адаптации математического аппарата для исследования. В большинстве случаев приходится использовать эвристический подход.

Стратегия национальной безопасности РФ вводит понятие безопасность личности, под которой понимается такое состояние и условия жизни личности, при которых реализуются ее права и свободы, прежде всего, право на жизнь и личную неприкосновенность [128].

В международно-правовой сфере широко используются понятия «единой» и «неделимой» безопасности, которые связаны с обеспечением государственной безопасности [128].

Эти понятия дают несколько неожиданный эффект при их использовании в транспортной безопасности.

Существует достаточно много типов безопасности (Рисунок 2.1), каждый из которых имеет прямое отношение к безопасности личности, но парадокс состоит в том, что достижение приемлемого уровня одной их них не гарантирует такого же результата для другой [128]. Например, приемлемый уровень безопасности полетов, абсолютно не гарантирует приемлемого уровня безопасности личности, если, например, не удается достичь приемлемого уровня транспортной безопасности.

Предлагается ввести новое понятие «интегральная безопасность воздушного транспорта» – это такое состояние авиационной транспортной системы, которое гарантирует приемлемый уровень безопасности личности в условиях реализации исчерпывающего перечня авиационных услуг и авиационных работ.

Безопасность личности можно отождествить с некоторым полем безопасности. В таком случае правомочно ввести гипотетические поля угроз и защиты. Тогда появляется триада гипотетических полей, результатом взаимодействия которых является интегральная безопасность.

Такая интерпретация интегральной безопасности нам представляется вполне правомочной, поскольку само понятие безопасность является гипотетическим и все исследования в области безопасности осуществляются на уровне умозрительных представлений [128].

<table>
<tr><td colspan="3">Безопасность</td></tr>
<tr><td colspan="3">Транспортная безопасность</td></tr>
<tr><td colspan="3">Безопасность воздушного транспорта</td></tr>
<tr><td colspan="2">Безопасность полетов</td><td>Авиационная безопасность</td></tr>
<tr><td>Техногенная безопасность</td><td>Производственная безопасность</td><td>Промышленная безопасность</td></tr>
<tr><td>Информационная безопасность</td><td>Экологическая безопасность</td><td>Экономическая безопасность</td></tr>
<tr><td colspan="2">Единство безопасности</td><td>Неделимость безопасности</td></tr>
<tr><td colspan="3">Интегральная безопасность воздушного транспорта</td></tr>
<tr><td colspan="3">Безопасность личности</td></tr>
</table>

Рисунок 2.1 – К вопросу об интеграции типов безопасности воздушного транспорта

Основная тенденция совершенствования и развития систем управления транспортной безопасностью в гражданской авиации как альтернатива обеспечению связана с понятием автоматизированная система управления. Понятие определяется двумя ключевыми словами: управление и автоматизированная система.

В предыдущих разделах показано как современные системы транспортной безопасностью постепенно переходят от обеспечения безопасности к управлению её уровнем с целью достижения приемлемого значения.

Вопросы автоматизации решаются с применением современных достижений в области компьютерных систем, более того, успехи в развитии методов и процедур автоматизации определяются достижениями в сфере компьютерных технологий.

Задачи, связанные с исследованием транспортной безопасности, можно отнести к классу плохо формализуемых и слабо структурированных.

Если плохо формализуемая и слабо структурированная задача решается с помощью математического моделирования, то точность решения зависит от качества и объема дополнительной информации, которая может быть получена и адекватно адаптирована с параметрами модели. В простейших случаях это могут быть некоторые эвристические алгоритмы, в более сложных случаях требуется разработка информационно-управляющих систем. В рамках транспортной безопасности такие системы представляют собой мощные компьютерные комплексы обработки больших объемов информации, разработанные на базе современных компьютерных технологий ESM, ESM-PSIM, DATA MINING и других. Главной проблемой внедрения таких комплексов является практическое отсутствие формализованных алгоритмов и процедур, соответствующих процессам обеспечения и управления транспортной безопасностью конкретного объекта защиты, поскольку указанные комплексы в значительной степени унифицированы и разрабатываются для определенных классов решаемых задач.

В этих условиях предлагается решать указанную задачу с помощью информационно-управляющего пространства (ИУП), рассматриваемого как некоторый интерфейс или адаптер между противоборствующими пространствами. Информационно-управляющее пространство представляет собой дальнейшее развитие центров (систем) обработки информации и решает задачи по формированию адекватной модели управления транспортной безопасностью и управляющих сигналов для исполнительных элементов.

Современный этап в развитии автоматизированных систем безопасности характеризуется серьезной проблемой, которую следует считать, прежде всего, научной. Современные компьютерные системы развиваются ускоренными темпами и предлагают широкие возможности для решения практических задач в различных областях, в том числе в сфере безопасности, за счет внедрения эффективных технологий типа BIG DATA, DATA MINING, PSIM. Эти технологии позволяют реализовать информационное управление, когда речь идет об обработке и анализе больших массивов информации, что обеспечивает высокую

эффективность и оптимальность управленческих процедур, а в области безопасности повышает её уровень. Однако, использование указанных технологий предполагает развитую систему постановки задач, включающую методологию формализации предметной области, адаптированный математический аппарат и определенную совокупность адекватных моделей.

На сегодня, всего этого в области транспортной безопасности практически нет, т.е. уровень развития основ теории и методологии безопасности значительно отстает от уровня разработанных компьютерных технологий, что серьезно осложняет совершенствование и развитие автоматизированных систем транспортной безопасности на базе информационного управления.

Решение указанной задачи основано на методах системотехники, теории оптимального управления, теории краевых задач, теории принятия решений, методах математического моделирования, квалиметрии, эвристическом и компетентностном подходах (Рисунок 2.2) и находится в сфере создания методологии формализации, моделирования и алгоритмизации.

Безопасность здесь понимается как транспортная и основана на понятии безопасность личности.

Пространство безопасностей рассматривается как гипотетическое понятие, введенное для упрощения методологии исследования.

Формализация представлена как направление в решении плохо формализуемых и слабо структурируемых задач.

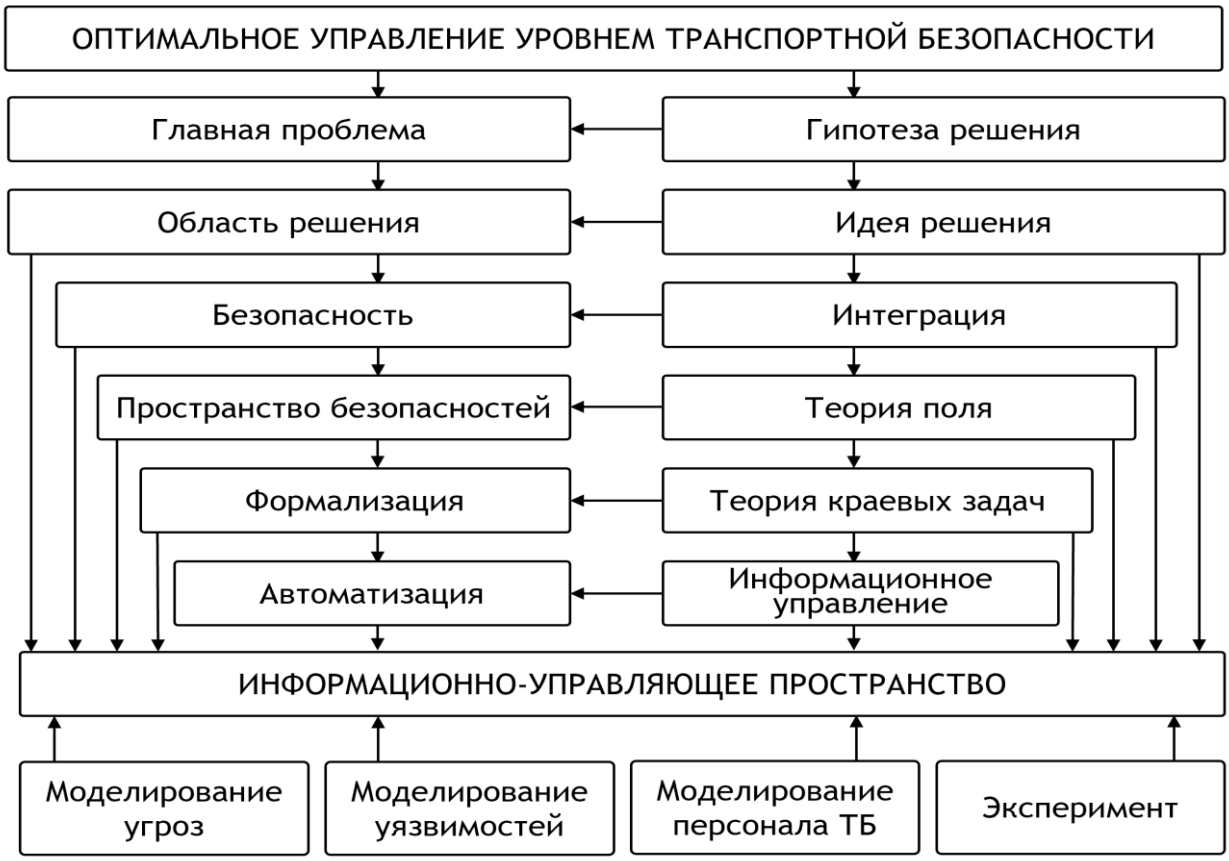


Рисунок 2.2 – Концепция информационного управления транспортной безопасностью

Автоматизация рассматривается как основа интеллектуального управления безопасностью.

Каждому направлению исследований соответствует некоторая специфическая методология.

Гипотеза решения предполагает успешный результат при условии гармонизации проблем развития компьютерной и алгоритмической составляющих управления безопасностью.

Идея решения состоит в разработке информационно-управляющего пространства как совокупности основ теории, методологии, методов, моделей, алгоритмов и процедур, определяющих интеллектуальное управление безопасностью.

Интеграция является системной основой управления, на базе которой построены модели процессов и процедур безопасности.

Теория поля – теоретическая основа структуризации безопасности.

Теория краевых задач – теоретическая основа моделирования процессов безопасности.

Информационное управление включает совокупность типов управлений безопасностью, оперирующих с большими массивами информации.

На базе основных направлений и соответствующих методологий формируется информационно-управляющее пространство.

Предлагаемая концепция включает логическую последовательность научных задач, представленных в формате лингвистических постановок, решение которых, в конечном итоге, обеспечивает условия реализации информационного управления уровнем транспортной безопасности на основе формирования информационно-управляющего пространства.

2.2 Принципы информационного управления транспортной безопасностью

Интеллектуальные системы управления транспортной безопасностью (ИСУ ТБ) основаны на понятии интеллектуальный анализ информации о ситуации в объекте защиты. ИСУ ТБ являются развитием класса интегрированных систем, что предполагает адаптацию и развитие принципов управления, которые положены в основу более ранних классов в структуре эволюционного развития. При этом основные процессы и процедуры управления безопасностью должны быть сохранены на основе комплексного подхода.

Комплексный подход заключается в реализации системы управления с учетом требований нормативных документов; результатов оценки уязвимости; в использовании высокоэффективных инновационных систем безопасности; в интеграции систем безопасности в единый автоматизированный комплекс; в наличии открытых документированных средств интеграции.

Анализ [62; 71; 76; 82; 189] процессов и процедур обеспечения безопасности показывает чрезвычайную сложность этих задач. С другой стороны, анализ современной нормативной базы в области транспортной безопасности [64; 90; 102; 188] говорит о заметном возрастании уровня требований к системам безопасности. Все это ставит задачу совершенствования и развития систем безопасности, но, при этом, абсолютно понятно, что современные подходы и методы практически исчерпали свои возможности. Требуются новые, оригинальные подходы и методы. Автор провел достаточное глубокое исследование указанных проблем, результаты которого изложены в работах [108; 110; 115; 116; 130; 133; 202; 248]. На основании этих исследований появилась авторская концепция, предлагающая исследовать проблемы транспортной безопасности с помощью краевых задач теории поля [123; 125; 135; 137].

Краевая задача формулируется в формате дифференциальных уравнений, где ставится цель получения решения в заданной области при заданных дополнительных ограничениях в точках границы [29; 38; 39; 258].

Краевая задача для линейного уравнения n-го порядка имеет вид

$$L(y) = f(x), \quad U\mu(y) = \gamma\mu, \ \mu = 1,2,\ldots, m, \tag{2.1}$$

где $L(y) = \sum_{v=0}^{n} f_v(x) y^{(v)}$.

Краевая задача для уравнения параболического типа состоит в нахождении функции $u(x, t) \in C^2(Q_\infty) \cap C^1(\overline{Q}_\infty)$, $\text{grad}_x u \in C(\overline{Q}_\infty)$, удовлетворяющей уравнению

$$\rho \frac{\partial u}{\partial t} = \text{div}\,(p\ \text{grad}\ u) - qu + F(x, t), \quad (x, t) \in Q_\infty, \tag{2.2}$$

Для уравнений эллиптического типа известны следующие краевые задачи: трехмерное уравнение Лапласа, внутренняя и внешняя задача Дирихле, внутренняя и внешняя задача Неймана, уравнение Пуассона [38].

Математический аппарат теории краевых задач содержит практически исчерпывающий перечень математических моделей для формального представления различных физических процессов, в том числе в теории транспортной безопасности.

Управление в таких сложных системах, как система управления транспортной безопасностью, может быть оптимальным, ситуационным или адаптивным (Рисунок 2.3).

Теория оптимального управления основана на принципе максимума Л. Понтрягина [8; 49; 67; 93; 94].

Рисунок 2.3 – Принципы информационного управления транспортной безопасностью

В общем виде задача оптимального управления в транспортной безопасности состоит в следующем. Управляемый объект, в данном случае, это транспортная безопасность как сложная система. Деятельность по обеспечению безопасности на некотором интервале времени, определяемом целью исследования, рассматривается как движение системы. Параметры движения изменяются под

влиянием управляющих элементов, определенным образом влияющих на управляемый объект. Параметры влияния определяются на основе изучения параметров объекта, тем самым формируется функция «движения» объекта. Для реализации оптимального управления необходимо иметь закон движения объекта, описывающий его динамические свойства.

Тогда изменения управляющих параметров будут контролировать состояние управляемого объекта в допустимых или необходимых пределах. Закон движения может иметь вид:

$$\frac{dx^i}{dt} = f^i(x^1, \ldots, x^n, u^1, \ldots, u^r), \tag{2.3}$$

где $i = 1,..., n$,

а управление объектом как функция времени

$$u^j = u^j(t), \tag{2.4}$$

где $j = 1,..., r$,

определяется параметрами в каждый момент времени. Если начальное $(x^1_0,..., x^n_0)$ и конечное $(x^1_1,..., x^n_1)$ состояния объекта заданы, то цель управления достигается, если найдётся момент времени $t_1 > t_0$, когда решение $(x^1(t),..., x^n(t))$ задачи

$$\frac{dx^i}{dt} = f^i(x^1,..., x^n, u^1(t),..., u^r(t)) \tag{2.5}$$

где $x^i(t_0) = x^i_0$, $i = 1, ..., n$, удовлетворяет условию $x^i(t_1) = x^i_1$.

Качество управления можно оценить значением функционала

$$J(u) = \int_{t_0}^{t_1} f^0(x^1(t), \ldots, x^n(t), u^1(t), \ldots, u^r(t))dt, \tag{2.6}$$

где $f^0(x^1, \ldots, x^n, u^1, \ldots, u^r)$ – заданная функция.

Задача оптимального управления состоит в отыскании такого реализующего цель управления, для которого указанный функционал принимает наименьшее возможное значение. Функционал качества имеет для задач транспортной безопасности определяющее значение, поскольку, учитывая неопределенность в исходных условиях и некоторую неадекватность формализации, является основным критерием оптимального управления.

Ситуационное управление осуществляется на основе оценки и анализа ситуации в системе, и представляет собой формирование целесообразного поведения управляемой системы на основе измерения, оценки и анализа ситуации, сложившейся внутри системы [6; 25; 46; 48, 89; 143]. Ситуационное управление представляет собой методологию управления сложными слабо структурированными объектами на основе интуиции и опыта лица, принимающего решение (ЛПР). На основе управляющих решений устанавливают соответствие между решениями и параметрами ситуаций.

Реализация управления может состоять из следующих этапов:

– получение информации о динамике ситуации. Основные требования к системе сбора и анализа информации: надежность, секретность, авторизация изменений, средства первичного анализа и др.;

– прогноз развития ситуации. Прогноз развития ситуации лежит в основе ситуационной управления и предполагает исследование динамики управляемых параметров с помощью методов математического моделирования, статистического анализа, методов искусственного интеллекта, включая нейросетевые технологии и т.д.;

– выработка управляющих воздействий. Реализуется ЛПР на основе интуиции и опыта и с использованием информации от системы поддержки принятия решений.

Адаптивное управление рассматривается как совокупность методов, позволяющих изменять параметры или структуру объекта. Адаптивные системы делятся на самонастраивающиеся, самоорганизующиеся, поисковые, системы

с эталонной моделью, системы с идентификатором, системы с настраиваемой моделью, системы с сигнальной адаптацией, системы с параметрической адаптацией. Адаптивное управление особенно актуально в автоматизированных системах управления [45; 49; 59].

На основе вышеизложенного можно сформулировать некоторые принципы управления в сложных системах транспортной безопасности:

– **Эволюционность.** Управление в области транспортной безопасности в своем развитии прошло путь от организационно-нормативного управления до автоматизированных систем управления со всеми соответствующими промежуточными этапами, причем отдельные элементы различных типов управлений не потеряли свою актуальность и сегодня. Эти элементы должны быть идентифицированы, исследованы и встроены в структуру современных систем управления.

– **Обоснованность.** Объект управления в транспортной безопасности относится к категории сложных систем и управляется в соответствии с законами системотехники. Решение задачи управления предполагает разработку некоторой методологии на основе теории, а при ее отсутствии серьезное обоснование, в том числе математическое, принимаемых решений.

– **Дуальность.** Управление в транспортной безопасности имеет единую цель, направленную на достижение приемлемого уровня безопасности, однако, методы достижения этой цели решают две функционально разные задачи, связанные, одна непосредственно с уровнем безопасности, вторая с ним же, но через управление авиационным персоналом, т.е. через человеческий фактор. Причем обе задачи требуют разработки принципиально разных методологий.

– **Конфликтность.** Во всех эргатических системах все процедуры, особенно процедуры управления, связаны с конфликтными ситуациями. Конфликт неизбежен, что определяется природой человека, но перед началом разработки и реализации управления необходимо найти решение конфликта. Конфликт ликвидировать невозможно, но решение конфликта снижает уровень

противостояния, взаимных претензий, что, в свою очередь, снижает многокритериальность решаемой задачи и упрощает процедуры управления.

– **Оптимальность-эвристичность.** Оптимальность управления предполагает удовлетворение некоторой совокупности критериев оптимизации, однако, не зависимо от физической природы этих критериев, возникают сложности, связанные с существенной неопределенностью в описании объекта управления, в результате чего решаемая задача становится плохо формализуемой, а адекватность модели управления в этом случае трудно обеспечить. Кроме того, количественные измерения в данном случае являются экспертными. Приемлемая альтернатива связана с использованием эвристического подхода.

– **Системность-ситуативность.** Управление сложной системой предполагает наличие системотехнического подхода, который реализуется в формате ситуационного управления. Объект управляется через идентификацию и исследование ситуации в сложной системе с использованием методов системотехники.

– **Адаптивность-интегрируемость.** Адаптивность управления в транспортной безопасности понимается как возможность перестройки структуры объекта и системы управления в соответствии с динамикой параметров внешней и внутренней среды. Принцип адаптивности реализуется в интегрированных системах обеспечения транспортной безопасности.

– **Безопасность-интегральность.** Принцип безопасности в гражданской авиации связан с понятием безопасность личности. Реализация этого принципа становится возможной, если согласиться с принципом интегральности безопасности, когда последняя рассматривается как совокупность элементов, функционально и по физической природе различных, но структурно и по смыслу связанных между собой, и рассматриваемых в комплексе.

– **Уязвимость-качество.** Оба принципа достаточно близки по физическому смыслу, что дает возможность выбора в задачах оптимизации, когда они выступают в качестве критериев, т.е. критерием оптимизации управления

может быть уязвимость, но количественная оценка критерия возможна через качество, с использованием методов квалиметрии.

– **Структурируемость-алгоритмизируемость.** С учетом существенной неопределенности в постановке задачи и определении исходных параметров при моделировании транспортной безопасности уровень структурируемости должен быть достаточно высок, что достигается применением структурно-логических моделей. Тогда алгоритмизируемость при переходе к автоматизированной системе управления вполне достижима.

– **Динамичность-прогнозируемость.** Задачи, решаемые в части управления авиационным персоналом, связаны с динамическим характером исследуемых факторов, что заставляет дополнить алгоритмы управления прогнозными моделями.

2.3 Интеллектуальное сопровождение процессов и процедур информационного управления безопасностью

Системы обеспечения транспортной безопасности выстраиваются на основе ситуационного подхода, предполагающего постоянный мониторинг состояния объекта защиты и управления этим состоянием с целью достижения приемлемого уровня безопасности.

Ситуационный анализ независимо от области применения достаточно сложный процесс, требующий адекватных теоретических обоснований. Ситуационный анализ в области транспортной безопасности реализуется в условиях интеллектуального и информационного управления уровнем безопасности. Интеллектуальное управление предполагает формирование критерия (критериев) управления на основе глубокого математического анализа ситуации в объекте защиты с использованием формальных моделей.

Информационное управление также основано на анализе ситуации, но предполагает сбор и соответствующую обработку больших информационных

массивов. Объединение этих двух принципиальных подходов в рамках единой системы автоматизированного управления транспортной безопасностью требует решения целого ряда методологических проблем (Рисунок 2.4).

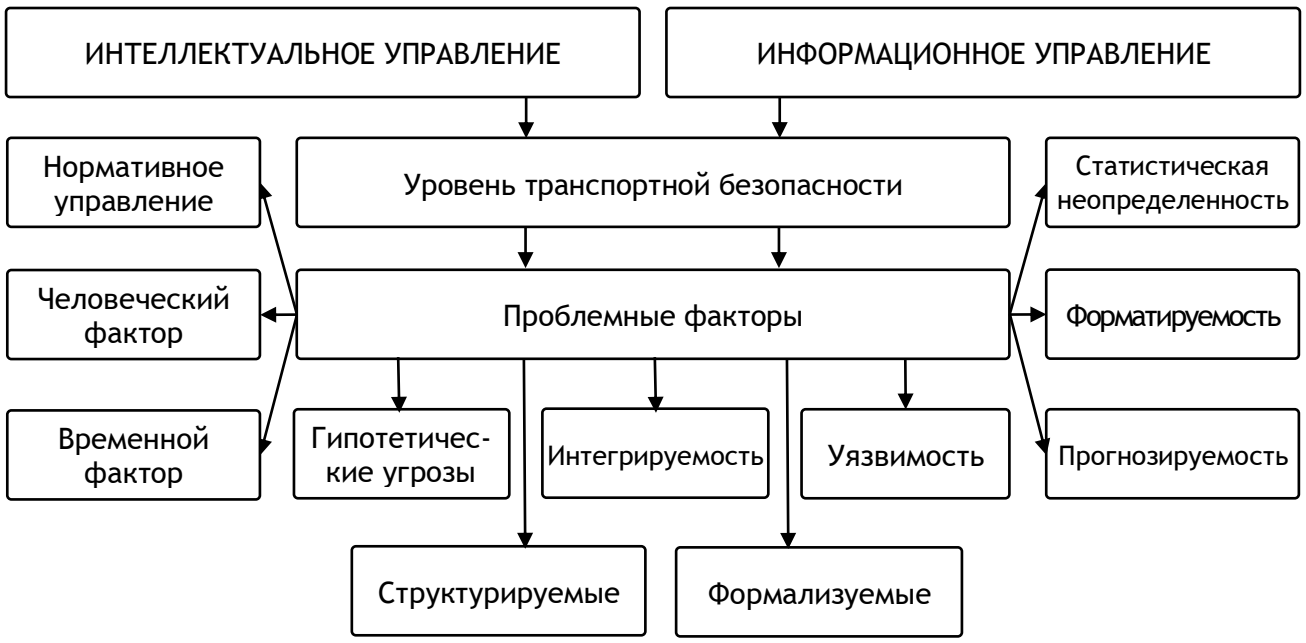


Рисунок 2.4 – Методологические проблемы управления транспортной безопасностью

Государственное регулирование деятельности в области гражданской авиации осуществляется в рамках нормативно-правового управления. Здесь можно выделить несколько слабых позиций: совокупность требований, изложенных в нормативных документах, при любой степени их детализации, содержит некоторую неопределенность, связанную с отсутствием количественных эквивалентов и неадекватностью лингвистических описаний; оценка соответствия всегда экспертная со всеми негативными последствиями, присущими этому методу; достаточно ощутимый временной разрыв между точкой фиксации несоответствия и точкой ликвидации последствий [52; 72].

Человеческий фактор в области безопасности, тем более в области транспортной безопасности, является одним из важнейших элементов системы. Достаточно глубокие исследования человеческого фактора в безопасности

показывают его негативное влияние на параметры безопасности [68]. В современных системах транспортной безопасности ставится задача максимального снижения роли человеческого фактора за счет замены человеческой компоненты системы на программно-технические элементы. Понятно, что это не самое оптимальное решение. При переходе к информационному управлению безопасностью в такой формулировке данная задача даже не рассматривается. Требуются кардинально иные подходы, пересматривающие само понятие человеческий фактор и предлагающие более эффективные методы минимизации негативного влияния человеческого фактора.

Деятельность любой сложной системы, а система транспортной безопасности относится именно к этому классу, выстраивается, в том числе, на основе статистического анализа результатов предыдущей деятельности. Понятно, что для анализа необходима достаточно представительная выборка [68; 73; 102]. События, которые фиксируются в рамках действующих систем обеспечения транспортной безопасности, относятся к разряду единичных. Вопрос о форме представления информации, циркулирующей в системе обеспечения транспортной безопасности, на сегодняшний день остается открытым. Дело в том, что в системе присутствуют различные элементы, имеющие принципиально отличные физические параметры и различную физическую природу. Их значимость в структуре системы далеко не одинакова, но их присутствие требует определенной унификации параметров в обработке информации.

Целевая функция управления в качестве критериев управления включает ряд параметров, определяемых физикой процессов объекта управления. В таком случае, в основе управления лежит математическая модель, формально описывающая ситуацию в исследуемом объекте. С точки зрения безопасности ситуация представляет собой динамику противостояния совокупности угроз безопасности объекта и системы защиты объекта. Поскольку первичным здесь является комплекс угроз безопасности, исходная модель должна отображать пространство этих угроз. Предполагается, что система безопасности должна быть

готова к обнаружению и отражению любых угроз, т.е. система настраивается на гипотетические (потенциальные) угрозы. В действительности это означает, что система работает с двумя типами угроз: потенциальные и реализованные, при этом должен быть обеспечен одинаковый результат [68]. Процедуры исследования реализованных угроз достаточно хорошо отработаны и понятны: главный принцип не допустить повторения. Что касается гипотетических угроз, то здесь единственный путь – моделирование.

Понятия интегральная безопасность, интегрированные системы безопасности достаточно хорошо определены и широко используются. Интеллектуальные системы также являются интегрированными, однако, в них понятие интегрируемость переходит на более высокий уровень и связано с интеграцией на уровне информационных процессов и процессов интеллектуального анализа.

Уязвимость объектов транспортной инфраструктуры, пожалуй, самое прогрессивное понятие последних лет, введенное в области транспортной безопасности [118; 131]. Дело в том, что это оценочное понятие, оно дает возможность получить ответ на вопрос о готовности системы защиты объекта противостоять потенциальным угрозам. Существует принципиальная возможность довести эти оценки до цифрового (количественного) формата и достаточно понятно, как это сделать, а это уже ключевой шаг к интеллектуальным системам.

На том уровне автоматизации, который реализован в современных системах обеспечения транспортной безопасности, остается главным целевой функционал: обнаружение-ликвидация угрозы. Понятно, что в конечном итоге сколь угодно эффективное совершенствование системы в этом направлении столкнется с некоторым пределом, связанным с несовершенством методологии. Понятно также, что перспектива – в смене функционала, а именно: упреждение. В таком случае прогнозные процедуры приобретают первостепенное значение. Методы прогнозирования достаточно хорошо известны, остается решить вопрос об используемых моделях [15; 44; 85].

Структурируемость – одна из важнейших проблем на пути автоматизации управленческих процедур. Достаточно важно это понятие на системном (структурном и алгоритмическом) уровне. Еще более важно обеспечить эффективное структурирование процедур моделирования, поскольку автоматизация управления выстраивается на основе использования математических или иных моделей, тем более, если речь идет об оптимальном управлении.

Задача формализации обусловлена и инициирована современным состоянием проблемы обеспечения транспортной безопасности на основе нормативного принципа управления, который не предполагает измерения уровня безопасности в количественном эквиваленте, что решает задачу обеспечения транспортной безопасности без оценки оптимальности принимаемых решений и оценки эффективности используемых средств обеспечения. При этом остается открытой проблема измеримости требований и субъективности оценок [12; 13].

2.4 Интеллектуальные технологии для решения задач информационного управления безопасностью

В последние годы успешно развивается новое направление в области систем безопасности, связанное с понятием информационное управление безопасностью (Рисунок 2.5).

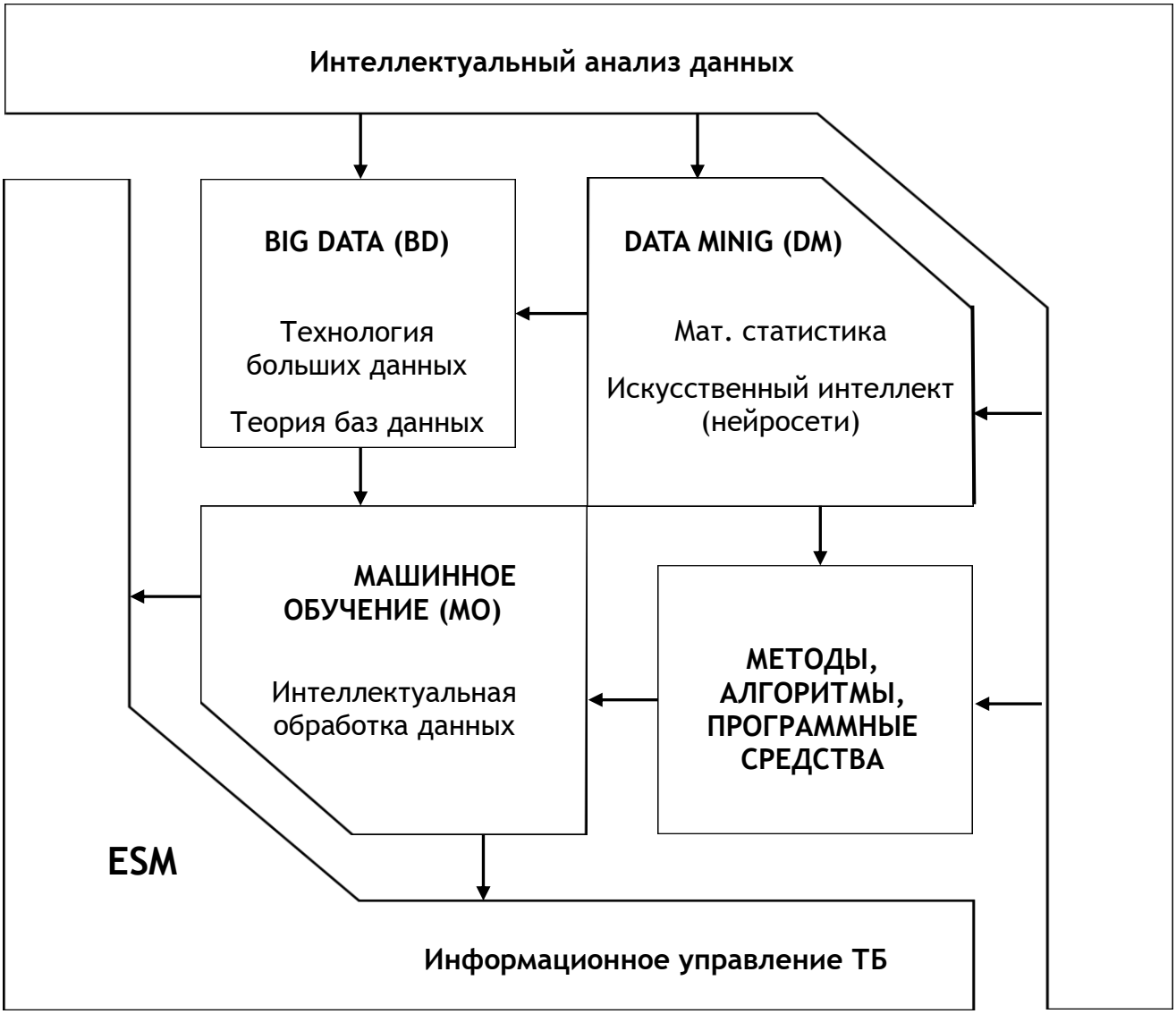


Рисунок 2.5 – Интеллектуальные технологии в задачах информационного управления транспортной безопасностью

Информационное управление предполагает реализацию следующих функций:

– интеграция разнородных систем различных производителей, являющихся источником информации об угрозах;

– анализ тревожных событий с целью определения типа угрозы и степени ее влияния на безопасность и назначение приоритета реагирования;

– верификация – предоставление оператору всесторонней информации об инциденте с целью выполнения правильной оценки;

– реагирование – предоставление оператору пошаговых инструкций и автоматизация процесса реагирования на инцидент;

– отчетность – сбор и консолидация данных об инциденте, автоматизация формирования отчетов;

– расследование – системное отслеживание адекватной реакции каждого оператора на каждый инцидент.

Информационное управление проектируется на основе модели защиты объекта, решающей задачу максимально быстро идентифицировать угрозу безопасности и ликвидировать ее, минимизировав ущерб. Модель включает два компонента: модель угроз и сценарии защиты.

Первым шагом в этом направлении является технология ESM (Electronika Security Manager) – один из первых отечественных программных продуктов, который можно рассматривать как технологию для решения задач управления безопасностью объекта защиты.

В ESM заложены возможности, которые позволяют эффективно интегрировать организационные мероприятия в единый комплекс системы безопасности (Рисунок 2.6) [103]:

1. Анализ и сопоставление данных о событиях и тревогах (инцидентах безопасности) с целью выявления реальной ситуации и их приоритетов.

2. Автоматизация операционных (эксплуатационных) процедур – пошаговых инструкций оператора, на основе лучших практик и политик организаций.

3. Контроль выполнения оперативных процедур и вычисление времени реагирования.

4. Генерация событий по действиям или отсутствию действий оператора.

Главной отличительной характеристикой инцидентного управления является передача значительной части процедур, связанных с обеспечением безопасности,

от человека-оператора автоматизированному комплексу технических средств, при этом в системе реализуется диалоговый режим.

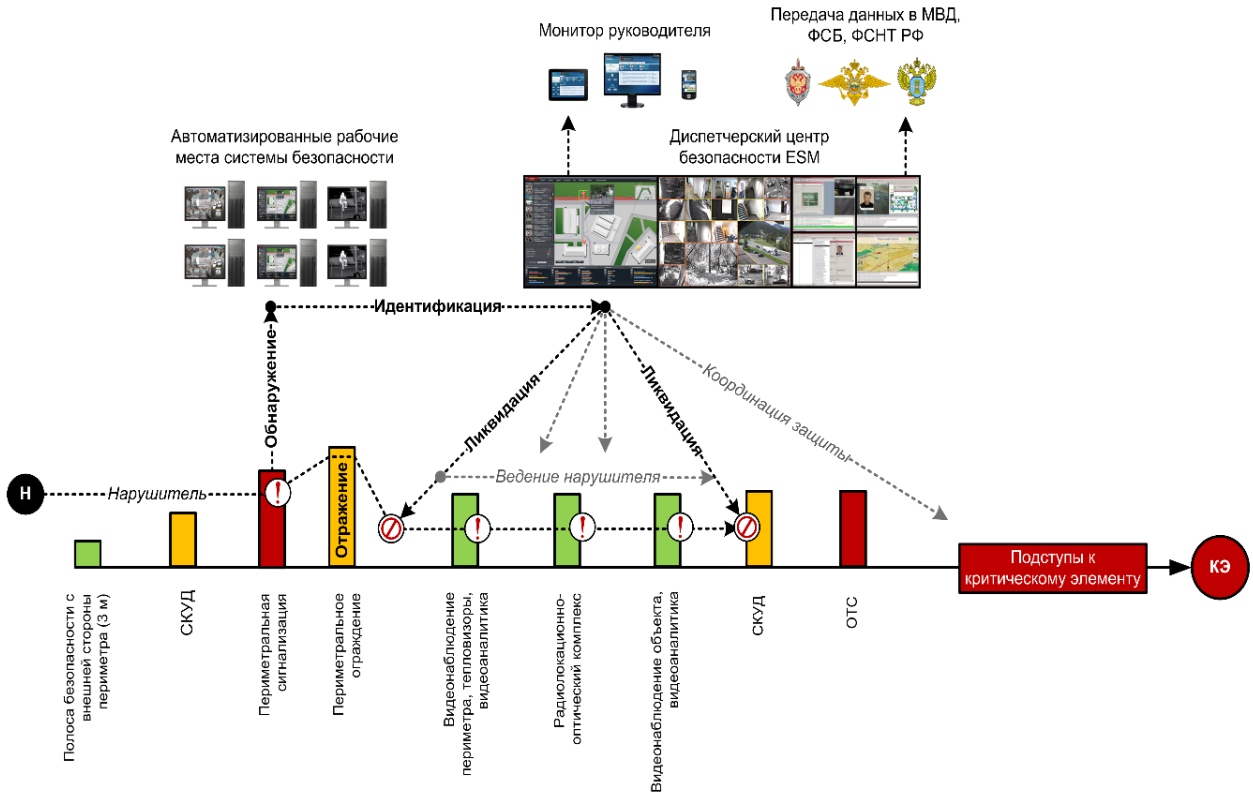


Рисунок 2.6 – Типовой сценарий работы комплекса ESM

На сегодняшний день доминирующей является концепция инцидентного управления. Можно назвать два объективных фактора, препятствующих широкому внедрению в практику информационного управления: это низкая доступность данных для интеллектуального анализа и отсутствие моделей защиты, включая сценарии и способы защиты. Для решение этих проблем необходима «глубокая» интеграция средств защиты и применение технологий Data Mining, оперирующих с «Большими данными» (Big data).

Следующий шаг на пути информационного управления безопасностью – это технология PSIM. Концепция информационного управления безопасностью принципиально отличается от традиционных, в том числе от инцидентного управления. Концепция PSIM – это управление через информацию и, прежде всего,

это автоматизированный анализ данных. Сбор данных с чрезвычайно большого количества систем и средств безопасности порождает огромные массивы информации. Это значит, что с оператора снимается большой объем профессиональных обязанностей, а оставшиеся серьезно трансформируются. В таком случае, инцидентное управление становится некоторым подмножеством множества функций систем информационного управления.

Платформой для интеграции и управления комплексами безопасности (Physical security information management – PSIM) называется категория программного обеспечения, предназначенная для управления через единый пользовательский интерфейс.

PSIM (управление информацией о физической безопасности) – это программная платформа, которая собирает и обрабатывает информацию от устройств обеспечения безопасности и других систем и формирует их в единое информационное пространство. Главное достоинство PSIM заключается в возможности глубокой интеграции, чем характеризуются комплексные системы безопасности. PSIM предлагает уникальные возможности интеллектуального решения вопросов управления безопасностью. И, наконец, PSIM обеспечивает активное управление событиями для повышение операционной эффективности, в том числе включает пошаговые планы действий. Указанные преимущества позволяют осуществлять централизованное управлении и использовать технологию на критических объектах с повышенными требованиями безопасности. Иными словами, PSIM – это класс программных средств, которые предоставляют платформу для интеграции функциональных приложений и технических средств безопасности, а также управления ими через единый пользовательский интерфейс [103; 105].

Достаточно близко к понятию ССОИ (система сбора и обработки информации), но это не так. Обратимся к нормативной базе.

ГОСТ Р 52860-2007. Технические средства физической защиты (ТСФЗ). «5.4.1. ССОИ предназначена для приема, обработки, отображения и регистрации

информации, поступающей от СО (средства охраны), а также для формирования команд управления и контроля работоспособности ТСФЗ».

ГОСТ Р 53195.1-2008. Безопасность функциональная связанных с безопасностью зданий и сооружений систем. «3.11. Комплексная система безопасности (КСБ). Система безопасности, одновременно выполняющая несколько функций безопасности, снижающих риски, обусловленные несколькими видами и/или источниками опасностей».

Отсюда ССОИ – это система/подсистема верхнего уровня КСБ.

Выделяется шесть функций у систем класса PSIM: сбор данных, верификация, анализ, поддержка процессов, отчеты и контроль. Здесь появляются две новых функции – автоматический анализ данных и поддержка процессов.

Концепция PSIM – это «управление через информацию». Здесь акценты перенесены с управления техническими средствами и системами КСБ на процессы управления безопасностью. Следует заметить, что PSIM – это первый шаг на пути к информационному управлению, когда инцидентное управление, характерное для ESM, становится лишь особым режимом функционирования систем класса PSIM (Рисунок 2.7).

Отечественная разработка ESM-PSIM [105] реализует следующие функции:

– интеграция технических решений в единой информационной среде;

– сценарный механизм обнаружения угроз, определение достоверности событий и критичности ситуации;

– активизация пошаговых инструкций;

– координация сил реагирования, своевременное оповещение;

– контроль работы операторов, анализ эффективности;

– сбор доказательной базы и автоматическое формирование отчетов.

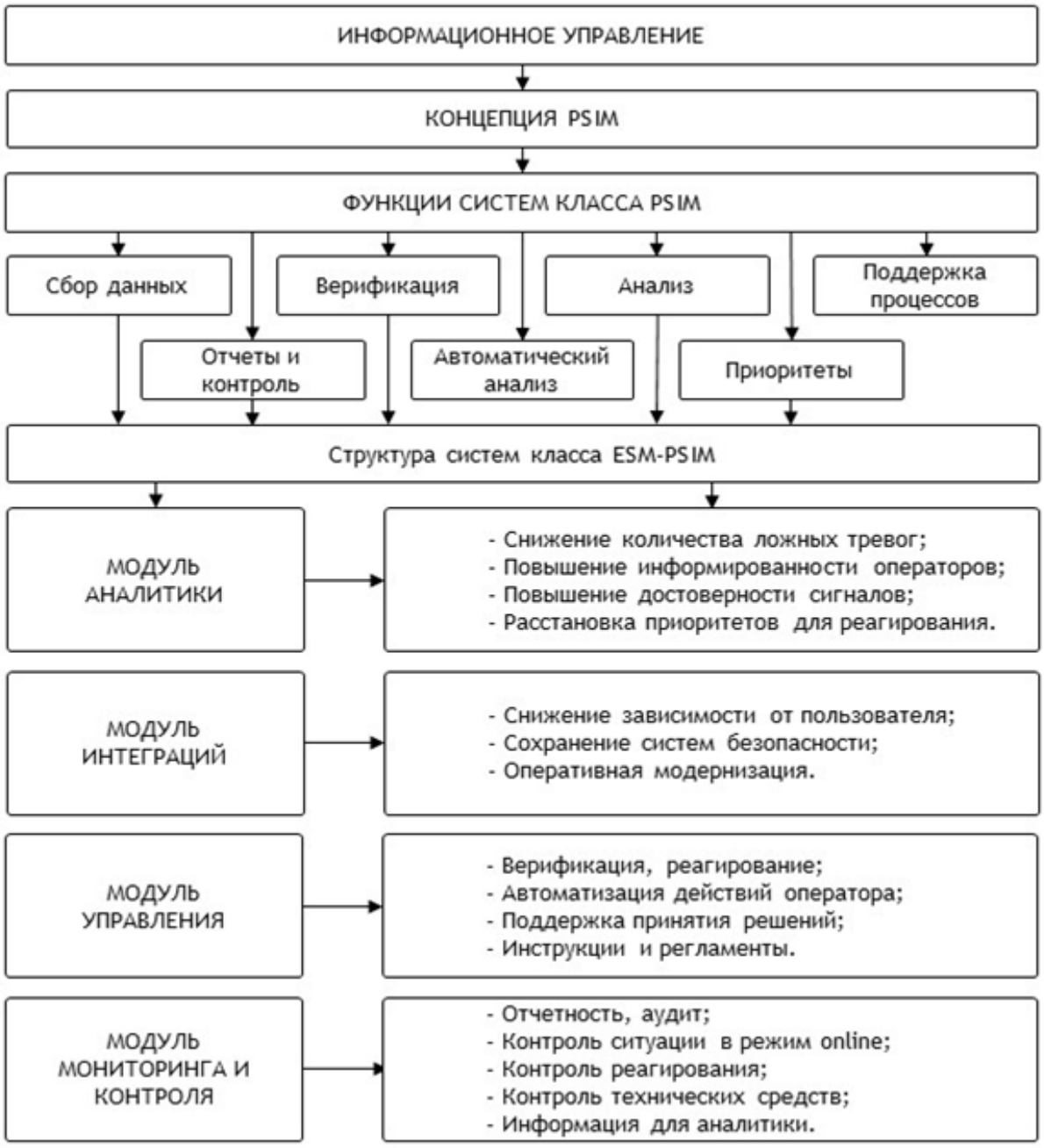


Рисунок 2.7 – Концепция PSIM

ESM-PSIM имеет модульную структуру и решает следующие задачи:

1. Модуль интеграции (сбор информации)

– снижение зависимости от конкретного производителя;

– сохранение действующих систем безопасности;

– оперативная модернизация комплекса.

2. Модуль аналитики (аналитика, верификация угроз)

– снижение количества ложных тревог;

– повышение информированности операторов;

– повышение достоверности сигналов;

– расстановка приоритетов для реагирования.

3. Модуль управления (верификация угроз, реагирование)

– автоматизация действий оператора;

– обеспечение поддержки принятия решений в случае внештатной ситуации;

– выполнение инструкций и регламентов авиапредприятия на 100%.

4. Модуль мониторинга и контроля (отчетность, аудит)

– контроль ситуации на объекте в режиме online (выполнение инструкций по реагированию, перемещение сотрудников через точки доступа, изменение состояния технических средств);

– предоставление информации для расследования и аналитики событий.

Принципиальное отличие современных PSIM-систем от традиционных систем мониторинга и управления состоит в процессной направленности не только и не столько в части реагирования, сколько в минимизации рисков, предсказании и профилактике происшествий и нарушений. Главное в концепции PSIM – переход от практики узконаправленного инцидентного управления к полноформатному информационному менеджменту.

Технология Data Mining основана на трех понятиях: математическая статистика (кластерный анализ, регрессионный анализ и т.д.), искусственный интеллект (нейронные сети), машинное обучение (интеллектуальная обработка данных). Технология применяется для решения следующих классов задач: обнаружение отклонений, обучение ассоциациям, кластеризация, классификация, регрессия, подведение итогов. Data Mining (интеллектуальный анализ данных) – это технология выявления взаимосвязей внутри больших баз данных [103; 229] (Рисунок 2.8).

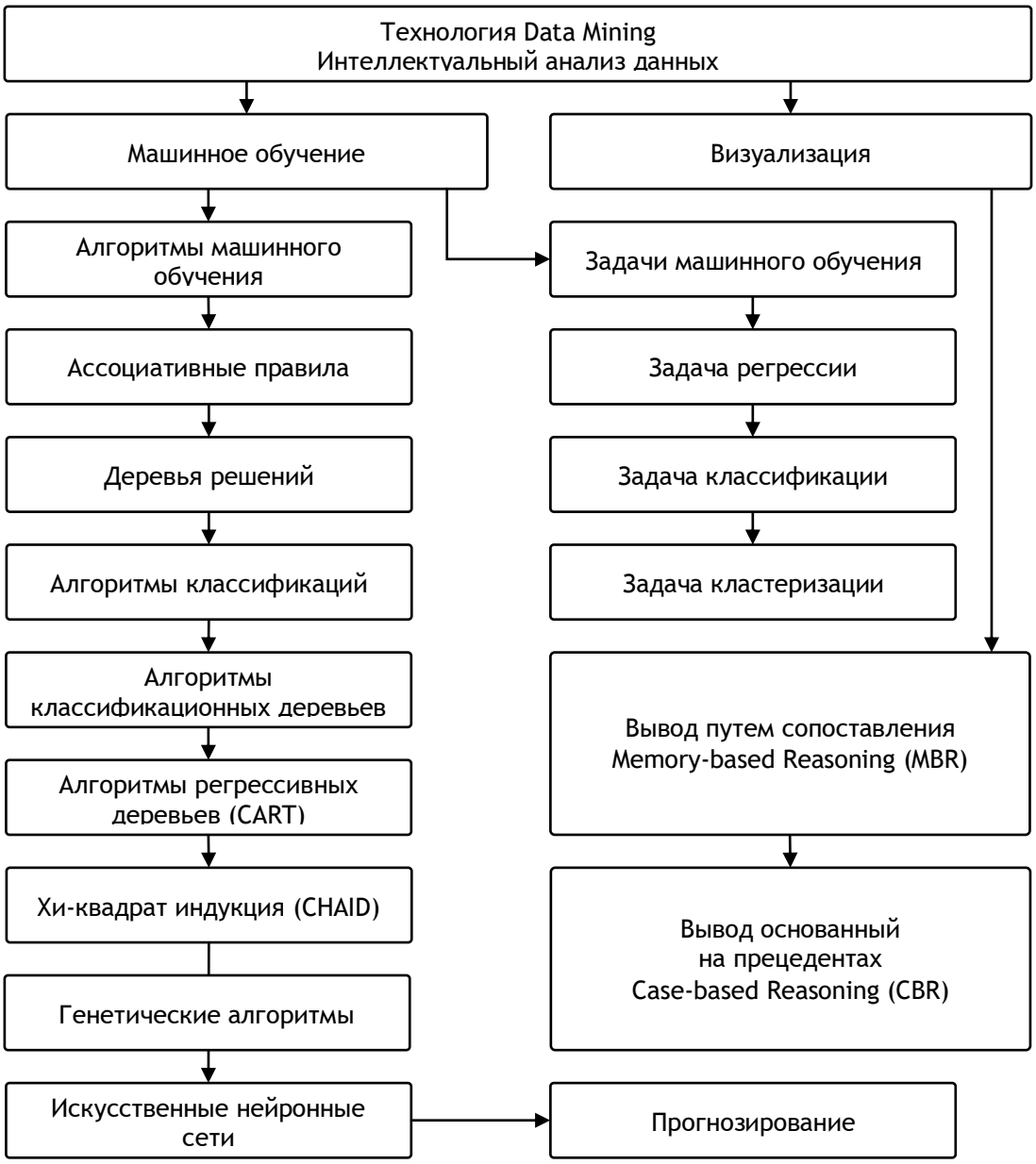


Рисунок 2.8 – Концепция Data Mining

В основе большинства инструментов Data Mining лежат две технологии: машинное обучение и визуализация, которые реализуется в виде следующих алгоритмов: ассоциативные правила, деревья решений и алгоритмы классификации, алгоритмы классификационных или регрессионных деревьев, хи-квадрат индукция, искусственные нейронные сети, прогнозирование, генетические

алгоритмы, вывод путем сопоставления или вывод, основанный на прецедентах, кластерный анализ.

Можно выделить обобщенные задачи машинного обучения.

Задача регрессии – приближение неизвестной целевой зависимости на некотором множестве данных.

Задача классификации – распределение некоторого множества объектов по заданному множеству групп (классов).

Задача кластеризации – разделение некоторого множества объектов на непересекающиеся группы (кластеры) таким образом, чтобы каждая группа состояла из схожих объектов, а объекты разных кластеров существенно отличались.

2.5 Краевые задачи теории поля для интеллектуального анализа безопасности

Краевая задача (задача для дифференциальных уравнений в частных производных) – задача получения решения дифференциального уравнения в частных производных в заданной области при заданных ограничениях на решение в точках границы.

Аналитическое решение краевых задач возможно в достаточно редких случаях с использованием приближенных методов. Наиболее простыми представляются метод конечных разностей и метод конечных элементов [38,39].

Рассмотрим уравнение Пуассона в неоднородной области D, ограниченной поверхностью S

$$\frac{\partial}{\partial x}\left(\sigma\frac{\partial\varphi}{\partial x}\right)+\frac{\partial}{\partial y}\left(\sigma\frac{\partial\varphi}{\partial y}\right)+\frac{\partial}{\partial z}\left(\sigma\frac{\partial\varphi}{\partial z}\right)=Q, \qquad (2.7)$$

где на части границы S_2 заданы условия второго рода, а на части границы S_3 – условия третьего рода, причем в этих условиях поток, направленный внутрь границы, запишем в виде

$$q = \sigma \operatorname{grad} \varphi \bullet \mathbf{n}, \tag{2.8}$$

где $\bullet$ обозначает скалярное произведение, $\mathbf{n}$ – нормальный единичный вектор, направленный наружу к границе.

Для данной задачи минимизируется функционал

$$F = \int_D \left\{ 0.5\sigma \left(\operatorname{grad} \varphi \right)^2 - Q\varphi \right\} dv - \int_{S_2, S_3} \left(q\varphi \right) ds. \tag{2.9}$$

Представляя функционал суммой функционалов, относящихся к отдельным конечным элемента, получаем [38]

$$F = \sum_{i=1}^{m} F_i^{(e)} = \sum_{i=1}^{m} \left[\int_D \left\{ 0.5\sigma \boldsymbol{\Phi}_i^{(e)\mathrm{T}} \left(\frac{\partial \mathbf{N}_i^{(e)}}{\partial \chi} \right)^{\mathrm{T}} \frac{\partial \mathbf{N}_i^{(e)}}{\partial \chi} \boldsymbol{\Phi}_i^{(e)} - Q \mathbf{N}_i^{(e)\mathrm{T}} \boldsymbol{\Phi}_i^{(e)} \right\} dv - \int_{S_2, S_3} \left(q \mathbf{N}_i^{(e)\mathrm{T}} \boldsymbol{\Phi}_i^{(e)} \right) ds \right] \tag{2.10}$$

где χ и m – координатный вектор и число элементов, соответственно.

После вычисления интеграла выражение (2.10) может быть записано в виде

$$F = \sum_{i=1}^{m} \left(0.5 \boldsymbol{\Phi}_i^{(e)\mathrm{T}} \mathbf{K}_i^{(e)} \boldsymbol{\Phi}_i^{(e)} - \boldsymbol{\Phi}_i^{(e)\mathrm{T}} \mathbf{f}_i^{(e)} \right),$$

или

$$F = 0.5 \mathbf{X}^{\mathrm{T}} \mathbf{K} \boldsymbol{\Phi} - \mathbf{X}^{\mathrm{T}} \mathbf{f}, \tag{2.11}$$

где $\mathbf{K}_i^{(e)}$, $\mathbf{K}$, $\mathbf{f}_i^{(e)}$ и f, соответственно, матрица жесткости и вектор нагрузки, соответствующие i-му элементу и полученные *ансамблированием* [38], т.е. суммированием с учетом топологического расположения элементов.

Условие минимизации функционала F получается приравниванием нулевому вектору производной F относительно вектора $\boldsymbol{\Phi}$.

$$\frac{\partial F}{\partial \boldsymbol{\Phi}} = \sum_{i=1}^{m} \left\{ \frac{\partial F_i^{(e)}}{\partial \boldsymbol{\Phi}} \mathbf{K}_i^e \left(\frac{\partial F_i^{(e)}}{\partial \boldsymbol{\Phi}} \right)^{\mathrm{T}} \right\} \boldsymbol{\Phi} - \mathbf{f} = \mathbf{0},$$

или

$$\frac{\partial F}{\partial \boldsymbol{\Phi}} = \mathbf{K} \boldsymbol{\Phi} - \mathbf{f} = \mathbf{0},$$

что приводит к системе линейных алгебраических уравнений

$$\mathbf{K} \boldsymbol{\Phi} = \mathbf{f}, \tag{2.12}$$

из решения которой определяется неизвестный вектор узловых значений $\mathbf{\Phi}$, используя который вычисляются значения функции φ в любой точке области.

Проблемы решения краевых задач численными методами достаточно серьезны. Некоторые из них решаются при использовании электрических моделей.

Современная теория электрического моделирования краевых задач объединяет достаточно большое число разнообразных методов, которые объединяются в следующие три основные группы: методы непрерывного времени, методы дискретного представления времени и методы квазианалогий [4; 71].

Метод «непрерывное пространство и время». Сущность метода сводится к замене параметров элементов пространства сосредоточенными электрическими параметрами, из которых образуются схемы замещения.

Электрическое моделирование исходного уровня сводится к решению совокупности уравнений Кирхгофа для всех узловых точек электрической сетки, каждое из которых имеет вид:

$$\frac{U_{x-1.y.z}}{R_1}+\frac{U_{x+1.y.z}}{R_2}+\frac{U_{x.y+1.z}}{R_3}+\frac{U_{x.y-1.z}}{R_4}+$$
$$+\frac{U_{x.y.z+1}}{R_5}+\frac{U_{x.y.z-1}}{R_6}-U_{x.y.z}\sum_{i=1}^{6}\frac{1}{R_i}=C\frac{dU_{x.y.z}}{dt}, \qquad (2.13)$$

где x, y, z – координаты узловой точки, для которой составлено данное уравнение;

R_1 – R_6 – электрическое сопротивление ветвей;

C – емкость узловой точки.

Решение исходного уравнения заключается в отыскании значений потенциалов узловых точек при заданных граничных и начальных условиях.

Метод «дискретное пространство – дискретное время». Пространство разбивается на отдельные элементы, каждый из которых моделируется электрической схемой замещения.

Таким образом, моделирование пространства угроз безопасности аэропорта принципиально возможно с помощью дифференциальных уравнений в частных

производных в формате краевой задачи. Если абстрагироваться от тех проблем, которые при этом возникают, краевые задачи в зависимости от состояния правой части дифференциального уравнения представляют собой совокупность различных уравнений эллиптического, гиперболического или параболического типа, при этом они образуют некоторый класс задач: задача Дирихле, задача Неймана, задача Стефана и другие [123; 125; 126; 129].

Представленный класс задач является исчерпывающим для моделирования псевдополей безопасности, но при этом каждый тип уравнения может быть соотнесен только с определенным типом угрозы из всей совокупности.

Анализ применимости численных методов с использованием нейрокомпьютеров показывает их достаточную привлекательность для моделирования угроз безопасности аэропорта, но при этом требования к вычислительной системе весьма велики, поэтому используется распараллеливание вычислительного процесса, мелкозернистый (массивный) параллелизм. В этом случае нейрокомпьютер представляет собой массивно-параллельную вычислительную систему, в которой процессорные элементы являются технической моделью нейронов. Альтернативным вариантом решения такого класса задач является бессеточный метод, основанный на использовании сетей радиальных базисных функций (РБФ-сеть), где основная сложность связана с определением параметров и весов радиальных базовых функций [201; 232].

2.6 Нейронные сети как инструмент интеллектуального анализа

Особый интерес для решения проблем безопасности представляют нейрокомпьютеры и нейронные сети [65,79]. Для решения сложных, плохо формализуемых и слабоструктурированных задач в качестве инструмента решения широко применяются искусственные нейронные сети, которые способны к обучению и обобщению. При этом обучение сводится к настройке параметров сети,

а обобщение означает способность сети распознавать ситуации, на которых сеть не обучалась (Рисунок 2.9).

Рисунок 2.9 – К понятию нейронных сетей

Модель искусственного нейрона [38]:

$$y = f(s) = f\left(\sum_{i=1}^{n} w_i x_i + w_0\right), \tag{2.14}$$

где y – выходной сигнал нейрона, x_i – входные сигналы, $f(s)$ – функция активации, w_i – синаптический вес (весовой коэффициент), w_0 – смещение (порог).

Адаптивный сумматор осуществляет взвешенное суммирование входов по формуле (2.14). Часто взвешенную сумму записывают в форме

$$s = \sum_{i=0}^{n} w_i x_i \,, \tag{2.15}$$

где $x_0 = 1$.

Тогда произведение $w_0 x_0$ представляет собой смещение.

Нейроны входят в состав нейронных сетей. Выход i-го нейрона с учетом (2.15) записывается в виде

$$y_i = f_i(s_i) = f_i\left(\sum_{j=0}^{n} w_{ij} x_j\right), \tag{2.16}$$

где индекс i является номером нейрона, индекс j – номером входа нейрона, вес w_{ij} – это вес, соответствующий входу j нейрона i.

Простейшей функцией активации является *линейная функция*

$$f(s) = s.$$

Первыми в нейронных сетях стали применяться пороговые функции, например, смещенная пороговая функция активации (дискретная функция Хевисайда)

$$f(s) = \begin{cases} 0, & \text{если } s < 0, \\ 1, & \text{если } s \geq 0. \end{cases} \tag{2.17}$$

или антисимметричная пороговая функция

$$f(s) = \begin{cases} -1, & \text{если } s < 0, \\ 1, & \text{если } s \geq 0. \end{cases} \tag{2.18}$$

Однако, все достоинства нейронных сетей проявляются при использовании нелинейных функций активации, например, сигмоидальной функции. Нейронные сети классифицируются по различным признакам (Рисунок 2.10):

1. По типу обрабатываемой информации:

– аналоговые сети: используют информацию в непрерывной форме, аппаратно реализуются с помощью аналоговых схем;

– цифровые сети: оперируют с информацией, представленной в цифровом виде, аппаратно реализуются с помощью цифровых схем.

2. По способу решения задач.

3. По количеству слоев выделяют однослойные и многослойные сети. Первым слоем считается распределительный слой, который не производит никакой обработки, а только передает входные сигналы на обрабатывающий слой.

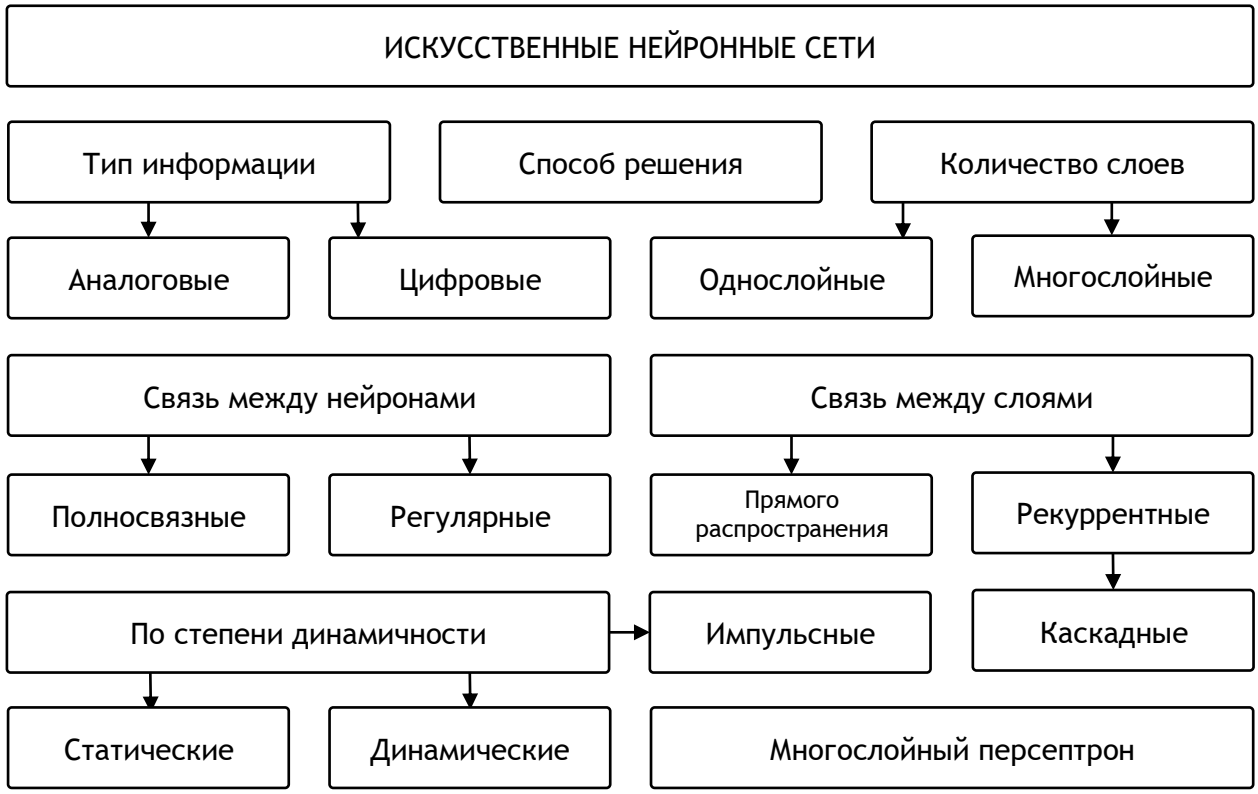


Рисунок 2.10 – Классификация нейронных сетей

Выход y_i нейрона номер i формируется по формуле (2.16), где индекс i является номером нейрона, индекс j – номером входа нейрона, вес w_{ij} – это вес, соответствующий входу j нейрона i. В матричной форме работа сети описывается следующим образом:

$$\mathbf{y} = \mathbf{f}\left(\mathbf{W}\mathbf{x}\right), \tag{2.19}$$

где $\mathbf{y}=[y_1\ y_2\ \ldots\ldots y_m]^{\mathrm{T}}$ – вектор выходов сети, $\mathbf{f}=[f_1\ f_2\ldots\ f_m]^{\mathrm{T}}$ – вектор-функция активации (как правило, все нейроны одного слоя имеют одинаковую функцию активации), $\mathbf{x}=[x_1\ x_2\ \ldots\ldots x_n]^{\mathrm{T}}$ – вектор входов сети, $\mathbf{W}$ – матрица синаптических весов, имеющая вид

$$\mathbf{W}=\begin{bmatrix} w_{11} & w_{12} & \cdots & w_{1n} \\ w_{21} & w_{22} & \cdots & w_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ w_{m1} & w_{m2} & \cdots & w_{mn} \end{bmatrix}. \qquad (2.20)$$

Матрица является прямоугольной ($m\neq n$). Строки матрицы представляют собой веса соответствующих нейронов.

Многослойная сеть содержит M слоев, среди которых выделяют первый слой, *промежуточные* (*скрытые*) слои и выходной слой. Номер слоя отображается на рисунке верхним индексом. Слои содержат, как правило, разное количество нейронов $N^{(i)}$, $i=1,2,\cdots,M$. Матрицы $\mathbf{W}^{(i)}$, $i=1,2,\cdots,M$ – это матрицы весов соответствующих слоев.

Вектор выхода первого слоя $\mathbf{y}^{(1)}=\mathbf{f}_1\left(\mathbf{W}^{(1)}\mathbf{x}\right)$ является входом второго слоя, выход второго слоя $\mathbf{y}^{(2)}=\mathbf{f}_2\left(\mathbf{W}^{(2)}\mathbf{y}^{(1)}\right)$ является входом третьего слоя и т. д. выход $\mathbf{y}^{(M)}$ слоя M является выходом сети.

4. По характеру связей между слоями многослойной сети выделяют:

– сети прямого распространения (Feed Forward Networks), в таких сетях информация перемещается от входа к выходу;

– рекуррентные сети (Recurrent Network), в таких сетях имеются обратные связи между слоями сети;

– каскадные сети (Cascade-Forward Networks), имеющие в каждом слое синаптические связи не только от предыдущего слоя, но и от входов сети.

5. По характеру связей между нейронами выделяют:

– полносвязные сети, где каждый нейрон одного слоя связан с каждым нейроном следующего слоя;

– регулярные сети, где нейроны в слое и между слоями связаны в соответствии с регулярным шаблоном, например, клеточные нейронные сети (cellular neural network).

6. По степени динамичности выделяют:

– статические сети, не имеющие обратных связей и временны́х задержек;

– динамические (темпоральные, временны́е) сети – это рекуррентные сети и сети прямого распространения, на входы которых подаются сигналы с разными временны́ми задержками;

– импульсные сети, воспроизводящие импульсный характер взаимодействия нейронов головного мозга.

Многослойный персептрон – это многослойная нейронная сеть, в которой входные сигналы распространяются по сети в прямом направлении от слоя к слою, а функции активации являются сигмоидальными. Такие сети способны осуществлять любое отображение входных векторов в выходные, то есть нейронная сеть может быть представлена как некоторая многомерная функция $F:\mathbf{x}\to\mathbf{y}$, где $\mathbf{x}$ – входной вектор, $\mathbf{y}$ – выходной вектор.

Схема обработки информации в полносвязной многослойной сети, содержащую *M* слоев, выглядит так:

$$\mathbf{x}\to\mathbf{W}^{(1)}\xrightarrow{\mathbf{s}^{(1)}}\mathbf{f}_1\left(\mathbf{s}^{(1)}\right)\xrightarrow{\mathbf{y}^{(1)}}\ldots\xrightarrow{\mathbf{y}^{(M-2)}}\mathbf{W}^{(M-1)}\xrightarrow{\mathbf{s}^{(M-1)}}\mathbf{f}_{M-1}\left(\mathbf{s}^{(M-1)}\right)\xrightarrow{\mathbf{y}^{(M-1)}}$$
$$\xrightarrow{\mathbf{y}^{(M-1)}}\mathbf{W}^{(M)}\xrightarrow{\mathbf{s}^{(M)}}\mathbf{f}_M\left(\mathbf{s}^{(M)}\right)\to\mathbf{y}^{(M)}$$

где $\mathbf{x}$ – вектор входа; $\mathbf{W}^{(i)}$ – матрица весов слоя i; $\mathbf{s}^{(i)}$ – вектор выходов адаптивных сумматоров слоя i; $\mathbf{y}^{(i)}=\mathbf{f}_i\left(\mathbf{s}^{(i)}\right)$ – вектор выхода слоя i; $\mathbf{f}_i$ – вектор-функция активации слоя i. Отметим, что функция активация может быть различной у разных слоев, например, зачастую выходной слой имеет линейную

функцию активации, а все остальные – логистическую. Первый слой называется входным. Слой M называется выходным, остальные слои – скрытыми или промежуточными. Часто используют фиктивный входной слой, число нейронов которого равно размерности входного вектора $\mathbf{X}$. В такой трактовке входной слой не производит никакой обработки, а только распределяет информацию.

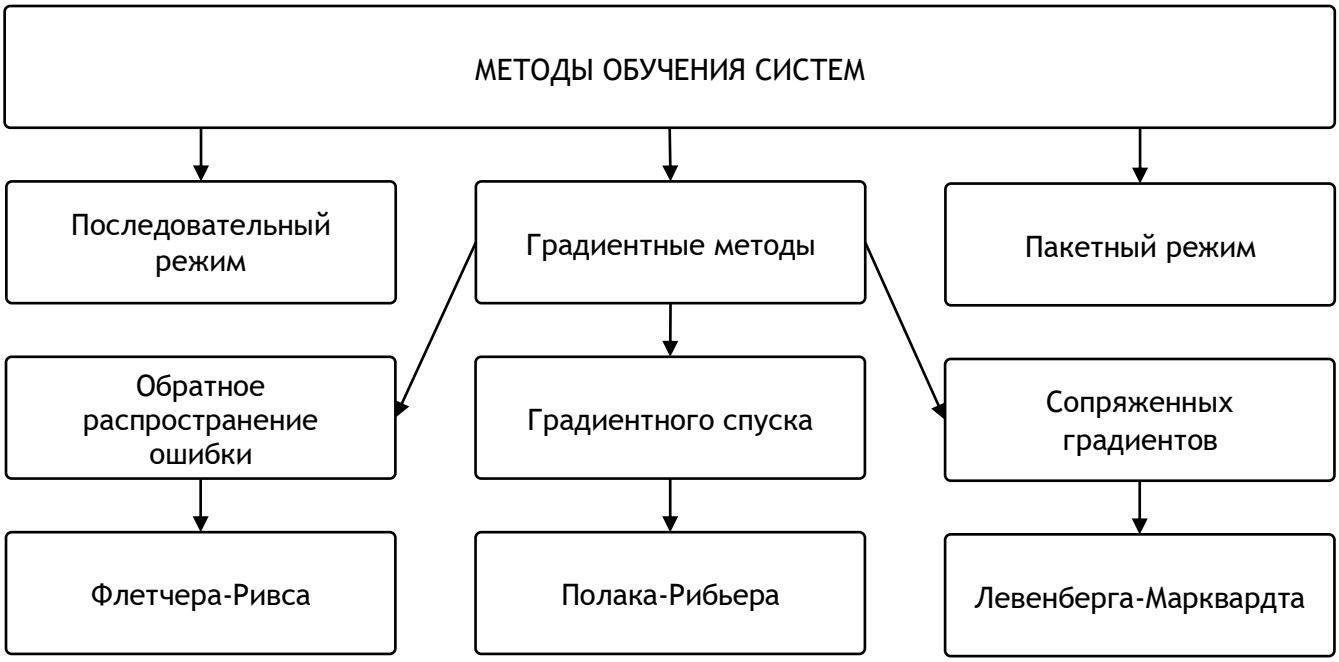


Рисунок 2.11 – Методы обучения нейронных сетей

При использовании последовательного режима (Рисунок 2.11) обучения настройка весов и смещений производится после подачи каждого вектора обучающей выборки, и функционал ошибки сети рассчитывается по формуле

$$E = \frac{1}{2}\sum_{i=1}^{N^{(M)}} e_i^2 = \frac{1}{2}\sum_{i=1}^{N^{(M)}} \left(y_i^{(M)} - t_i \right)^2, \qquad (2.21)$$

где $N^{(M)}$ – число нейронов выходного слоя, M – число слоев, $\mathbf{e} = \left[e_i \right]$ – вектор ошибок на выходе сети, $e_i = y_i^{(M)} - t_i$ – ошибка на выходе i, $\mathbf{y} = \left[y_i^M \right]$ – выходной вектор сети, $\mathbf{t} = \left[t_i \right]$ – вектор целей.

Коэффициент $1/2$ введен для упрощения последующего анализа.

В пакетном режиме обучения настройка весов производится после предъявления сети множества векторов, функционал ошибки имеет вид

$$E = \frac{1}{2}\sum_{q=1}^{Q}\sum_{i=1}^{N^{(M)}}\left(e_i^{(q)}\right)^2 = \frac{1}{2}\sum_{q=1}^{Q}\sum_{i=1}^{N^{(M)}}\left(y_i^{(qM)} - t_i^{(q)}\right)^2, \qquad (2.22)$$

где Q – объем (количество примеров) обучающей выборки, q – номер обучающего примера, $e_i^{(q)} = y_i^{(qM)} - t_i^{(q)}$ – ошибка на выходе i при подаче на вход примера q, $y_i^{(qM)}$ – i-ый выход выходного слоя M для входного примера q, $t_i^{(q)}$ – i-е значение вектора цели для входного примера q.

Пакетный режим обучения является частным случаем при объеме обучающей выборки $Q=1$. Правило функционирования слоя m ($m=1,2,\ldots,M$) описывается формулой:

$$y_k^{(qm)} = f_m\left(\sum_{l=0}^{N^{(m-1)}} w_{kl}^{(m)} y_l^{(q,m-1)}\right), \quad k=1,2,\ldots,\ldots N^{(m)}, \quad m=1,2,\ldots,M. \qquad (2.23)$$

В формуле учтено, что входным вектором слоя m является выходной вектор слоя $m-1$. Входом первого слоя является входной вектор, т. е. формально $\mathbf{y}^{(0)} = \mathbf{x}$. Будем считать, что сеть является полносвязной, т.е. каждый выход слоя $(m-1)$ связан с каждым входом слоя m. Индекс $l=0$ соответствует смещению. Смещение будем рассматривать как единичный вход, соединенный весом $w_{k0}^{(m)}$. Вес w_{ij} – это вес, соответствующий входу j нейрона i.

При обучении многослойных сетей чаще всего используют градиентные методы обучения, требующие вычисления производных функционала ошибки по параметрам сети. Например, в алгоритме градиентного спуска элементы матрицы весов w_{ij} корректируются по формуле

$$w_{ij}^{(k)} = w_{ij}^{(k-1)} - \eta \frac{\partial E^{(k-1)}}{\partial w_{ij}^{(k-1)}}, \quad (2.24)$$

где k – номер цикла обучения, η – числовой коэффициент (скорость обучения), E – функционал ошибки, $\frac{\partial E^{(k-1)}}{\partial w_{ij}^{(k-1)}}$ – компонент градиента функционала ошибки по вектору весов.

Но, функционал ошибки и его производные по весам можно вычислить только для выходного слоя. Алгоритм обратного распространения ошибки (Error Back Propagation) позволяет вычислить эти производные для всех слоев сети, начиная с выходного слоя. Алгоритм обратного распространения ошибки используется в сочетании с различными стратегиями оптимизации, что приводит к различным методам обучения сетей.

При использовании метода обратного распространения ошибки обучение сети производится по следующему алгоритму.

1. Инициализация. Весам сети присваиваются малые случайные значения.
2. Проход вперед. На вход сети подается входной вектор (или несколько входных векторов в пакетном режиме обучения), рассчитываются выходные векторы скрытых слоев и выходного слоя. Рассчитывается функционал ошибки E. Если $E > \varepsilon$, где ε – заданная величина, то – на шаг 3, иначе – на конец алгоритма (шаг 5).
3. Проход назад. Двигаясь от выходного слоя, рассчитываются производные вида $\frac{\partial E}{\partial w_{ij}}$ (компоненты градиента функционала ошибки по весам и смещениям сети) и корректируются веса сети.
4. Переход на шаг 2.
5. Конец алгоритма.

В процессе обучения модели возможны недообучение и переобучение. Недообучение (underfitting) возникает, когда модель слишком простая, чтобы выявить закономерности в данных. Переобучение (overfitting) возникает, когда

модель слишком сложна относительно объема и зашумленности обучающих данных. Причем недообученность и переобученность модели можно обнаружить только при испытании на новых примерах, не участвовавших в обучении. Если нет никаких предположений о данных, то невозможно выбрать модель, априорно гарантирующую лучшую работу. Единственный способ узнать, какая модель лучше – оценить некоторое множество моделей на определенных данных.

Можно выделить несколько основных проблем машинного обучения, свойственных обучению нейронных сетей [182]:

– Недостаточный размер обучающих данных, т.е. требуются большие объемы обучающих данных.

– Нерепрезентативные обучающие данные. Обучающие данные могут быть нерепрезентативными из-за недостатков построения выборки. Явление нерепрезентативности выборки называется смещением выборки.

– Данные плохого качества, содержащие ошибки, пропуски данных, выбросы.

– Несущественные признаки, затрудняющие обучение.

Рассмотрим кратко основные понятия, связанные с архитектурой и обучением нейронных сетей, предназначенных для решения задач классификации, т. е. отнесения объекта к одному из известных классов.

Нейронные сети относятся к такой обширной области, как машинное обучение [234; 241; 273]. Машинное обучение изучает методы построения алгоритмов, способных обучаться, т. е. улучшать свое поведение в процессе работы. В отличие от других моделей машинного обучения нейронные сети позволяют эффективно строить сложные нелинейные зависимости, более точно описывающие наборы данных. В отличие от экспертных систем, основанных на логическом выводе, нейронные сети не требуют построения баз знаний, которые зачастую невозможно построить из-за отсутствия информации в явном виде.

Такой подход особенно важен для классификации аэропортов по параметру уязвимость. Количественные оценки уязвимости получают экспертным путем, т.е.

они отражают субъективное мнение эксперта. Уязвимость, по сути, представляет собой оценку соответствия требованиям. При этом понятно, что в такой предметной области как транспортная безопасность требования не могут быть сформулированы точно, всегда есть некоторый разброс в описаниях явлений и отсутствие полноты в описании субъектов. Полученные оценки уязвимости весьма приблизительно отражают степень безопасности объекта защиты, т.е. степень неопределенности в самой постановке задачи достаточно велика. Поэтому принимать решение о безопасности объекта защиты в такие условия весьма проблематично. Именно здесь нейронные сети дают весьма привлекательные возможности. Высокая степень неопределенности по входу в значительной степени снижается за счет процедур обучения нейронной сети, но, с другой стороны, повышаются требования к системе обучения.

Нейронные сети обладают и рядом свойств, вызывающих проблемы при их применении. К таким свойствам относится отсутствие строгой теории по выбору структуры сети, что зачастую требует больших объемов экспериментальной работы с сетями разной структуры. Недостатком сетей является сложность обучения сетей. В случае обучения с учителем необходимы примеры для обучения и тестирования сети. При этом, как правило, успешное обучение не гарантировано, что требует экспериментов с сетью. Сеть представляет собой "черный ящик", то есть с помощью сети нельзя объяснить, почему получился тот или иной результат.

Функция f называется функцией активации. В нейронных сетях наиболее распространенными являются сигмоидальные функции активации – гладкие, монотонно возрастающие дифференцируемые ограниченные функции.

В искусственных нейронах получили распространение разновидности сигмоидальных функций – униполярная логистическая функция активации (асимметричная или смещённая логистическая функция), описываемая выражением

$$f(s)=\frac{1}{1+e^{-s}}, \qquad (2.25)$$

и антисимметричная логистическая функция (биполярная логистическая функция), описываемая выражением

$$f(s)=\frac{1-e^{-s}}{1+e^{-s}}. \tag{2.26}$$

Широко используют в качестве функции активации гиперболический тангенс

$$\mathrm{th}(s)=\frac{e^{s}-e^{-s}}{e^{s}+e^{-s}}. \tag{2.27}$$

При решении на нейронной сети задач классификации для выходного слоя сети удобна конкурирующая функция активации с мягким максимумом – функция SoftMax

$$f(s_i)=\frac{e^{s_i}}{\sum_{j=1}^{n} e^{s_j}}, \tag{2.28}$$

где $f(s_i)$ – выход i-го нейрона, s_i – взвешенная сумма i-го нейрона, n – число нейронов выходного слоя.

При обучении многослойных сетей, как правило, используют *градиентные методы обучения*. Градиентные методы основаны на том, что в малой окрестности локального минимума гладкий функционал ошибки хорошо аппроксимируется суммой первых трёх слагаемых его разложения по формуле Тейлора:

$$E(\mathbf{w}+\Delta\mathbf{w})=E(\mathbf{w})+\left[\mathbf{g}(\mathbf{w})\right]^{\mathrm{T}}\Delta\mathbf{w}+\frac{1}{2}\Delta\mathbf{w}^{\mathrm{T}}\mathbf{H}(\mathbf{w})\Delta\mathbf{w}, \tag{2.29}$$

где $\mathbf{w}$ – вектор всех весов сети, $\Delta\mathbf{w}$ – вектор коррекции весов,

$$\mathbf{g}(\mathbf{w})=\mathrm{grad}\,E=\nabla E=\left[\frac{\partial E(\mathbf{w})}{\partial w_1}\ \frac{\partial E(\mathbf{w})}{\partial w_2}\ldots\frac{\partial E(\mathbf{w})}{\partial w_n}\right]^{\mathrm{T}} \tag{2.30}$$

– вектор градиента функционала ошибки по весам,

$$\mathbf{H}(\mathbf{w}^*)=\begin{bmatrix}\frac{\partial^2 E(\mathbf{w}^*)}{\partial w_1\partial w_1} & \frac{\partial^2 E(\mathbf{w}^*)}{\partial w_1\partial w_2} & \cdots & \frac{\partial^2 E(\mathbf{w}^*)}{\partial w_1\partial w_n}\\ \cdots & \cdots & \cdots & \cdots\\ \frac{\partial^2 E(\mathbf{w}^*)}{\partial w_n\partial w_1} & \frac{\partial^2 E(\mathbf{w}^*)}{\partial w_n\partial w_2} & \cdots & \frac{\partial^2 E(\mathbf{w}^*)}{\partial w_n\partial w_n}\end{bmatrix}. \tag{2.31}$$

Типичным алгоритмом первого порядка обучения нейронных сетей является метод градиентного спуска, при использовании которого вектор весов корректируется в направлении вектора антиградиента функционала ошибки

$$w_{ij}^{(k)} = w_{ij}^{(k-1)} - \eta \frac{\partial E^{(k-1)}}{\partial w_{ij}^{(k-1)}}, \tag{2.32}$$

где k – номер цикла обучения, η – числовой коэффициент (скорость обучения), E – функционал ошибки, $\frac{\partial E^{(k-1)}}{\partial w_{ij}^{(k-1)}}$ – компонент градиента функционала ошибки по вектору весов.

Метод сопряженных градиентов (*Conjugate-Gradient Method*) [38] применяется при решении систем линейных алгебраических уравнений вида

$$\mathbf{Ax} = \mathbf{b},$$

где $\mathbf{A}$ – матрица размером $n \times n$, $\mathbf{b}$ – вектор-столбец размером $n \times 1$.

Решение системы эквивалентно минимизации квадратичного функционала

$$f(\mathbf{x}) = \frac{1}{2}\mathbf{x}^{\mathrm{T}}\mathbf{A}\mathbf{x} - \mathbf{b}^{\mathrm{T}}\mathbf{x} + c, \tag{2.33}$$

где c – скаляр.

Причем при отсутствии погрешностей вычислений решение может быть найдено не более чем за n шагов.

В малой окрестности точки локального минимума функционал ошибки нейронной сети хорошо аппроксимируется квадратичным функционалом. Между функционалами существует прямая аналогия: вектору $\mathbf{x}$ соответствует вектор $\mathbf{p}$ изменения весов сети, вектору $\mathbf{b}$ соответствует вектор градиента $\mathbf{g}$, а матрице $\mathbf{A}$ – Гессиан $\mathbf{H}$ (в точке локального минимума Гессиан положительно определен). Поэтому, метод сопряженных градиентов может быть применен для минимизации функционала ошибки сети, то есть для обучения сети. Это будет метод второго порядка, так как Гессиан содержит вторые производные функционала ошибки. А так как функционал ошибки только приближенно можно рассматривать как

квадратичный, то даже в отсутствии ошибок вычислений метод становится итерационным.

В варианте метода сопряженных градиентов, используемом для обучения нейронных сетей, вектор направления поиска минимума $\mathbf{p}_k$ выбирается таким образом, чтобы направление было сопряжено со всеми предыдущими направлениями $\mathbf{p}_0, \mathbf{p}_1, \ldots, \mathbf{p}_{k-1}$. Векторы $\mathbf{p}_i$ и $\mathbf{p}_j$ называются сопряженными (сопряженными относительно матрицы $\mathbf{A}$), если $\left(\mathbf{A}\mathbf{p}_i, \mathbf{p}_j\right) = 0$. Вектор, удовлетворяющий указанным условиям, может быть построен по выражению

$$\mathbf{p}_k = -\mathbf{g}_{k-1} + \beta_k \mathbf{p}_{k-1},$$

где $\mathbf{g}_{k-1} = \mathbf{g}\left(\mathbf{w}_{k-1}\right)$ – вектор градиента, β_k – коэффициент, вычисляемый в каждой итерации обучения. Принимают $\mathbf{p}_0 = -\mathbf{g}_0$, где $\mathbf{g}_0 = \mathbf{g}\left(\mathbf{w}_0\right)$, $\mathbf{w}_0$ – начальное значение вектора весов.

Вектор $\mathbf{p}_1$ вычисляется по формуле градиентного спуска. На последующих итерациях используются специальные формулы. В общем виде вычисления коэффициента β_k требует знания Гессиана. Однако, известно несколько способов вычисления коэффициента β_k, не требующих знания Гессиана, наиболее популярными при обучении нейронных сетей являются два:

– *формула Флетчера-Ривса* (*Fletcher R., Reeves C. M.*) [38]

$$\beta_k = \frac{\mathbf{g}_{k-1}^{\mathrm{T}} \mathbf{g}_{k-1}}{\mathbf{g}_{k-2}^{\mathrm{T}} \mathbf{g}_{k-2}} = \frac{\left(\mathbf{g}_{k-1}, \mathbf{g}_{k-1}\right)}{\left(\mathbf{g}_{k-2}, \mathbf{g}_{k-2}\right)}, \tag{2.34}$$

– *формула Полака-Рибьера* (*Polak E., Ribiere G.)* [18]

$$\beta_k = \frac{\left(\mathbf{g}_{k-1} - \mathbf{g}_{k-2}\right)^{\mathrm{T}} \mathbf{g}_{k-1}}{\mathbf{g}_{k-2}^{\mathrm{T}} \mathbf{g}_{k-2}} = \frac{\left(\mathbf{g}_{k-1} - \mathbf{g}_{k-2}, \mathbf{g}_{k-1}\right)}{\left(\mathbf{g}_{k-2}, \mathbf{g}_{k-2}\right)}. \tag{2.35}$$

При минимизации квадратичного функционала формулы Флетчера-Ривса и Полака-Рибьера эквивалентны. Из-за приближенного характера формулы и неточности вычисления нового приближения вектора весов сопряженность направлений поиска постепенно теряется. Это приводит к снижению скорости

сходимости метода. Формула Полака-Рибьера позволяет алгоритму выйти из этой ситуации. Можно дать следующее качественное объяснение такому свойству формулы Полака-Рибьера [38]. Обучение "застопорится", если $\mathbf{g}_{k-1} \approx \mathbf{g}_{k-2}$. Но, тогда коэффициент $\beta_k \approx 0$ и новое направление поиска становится равным антиградиенту. Это означает *рестарт процедуры обучения*: направление минимизации из точки полученного решения выбирается по алгоритму скорейшего спуска, а на последующих итерациях применяется метод сопряженных градиентов. Считается, что возникли проблемы со сходимостью, если число итераций обучения превысило число настраиваемых параметров сети. Рестарт процедуры обучения реализован во всех алгоритмах сопряженных градиентов.

Изменение вектора весов производится по выбранному направлению

$$\mathbf{w}^{(k)} = \mathbf{w}^{(k-1)} + \eta_k \mathbf{p}_k . \qquad (2.36)$$

Коэффициент η_k находится как решение задачи одномерной оптимизации. Часто применяется аппроксимация функционала ошибки по направлению $\mathbf{p}_k$ с последующим расчетом минимума полученной функции одной переменной η. Одномерная оптимизация может занять много времени, так как требует многократного вычисления вектора весов, выхода сети и функционала ошибки. В [38] предложен *масштабируемый алгоритм сопряженных градиентов* (*scaled conjugate gradient algorithm*), в котором для одномерной оптимизации используется одномерная форма алгоритма Левенберга-Марквардта.

Алгоритм метода сопряженных градиентов строится следующим образом (в алгоритме не отражены рестарты, при каждом рестарте алгоритм повторяется).

На *"нулевой" итерации* выполняются подготовительные действия:

1. Полагается $k = 0$.

2. Задается начальное приближение вектора весов $\mathbf{w}^{(0)}$ и, используя алгоритм обратного распространения ошибки, вычисляется вектор градиента $\mathbf{g}_0$.

3. В качестве направления движения выбирается $\mathbf{p}_1 = -\mathbf{g}_0$.

На первой и следующих итерациях ($k = 1, 2, \cdots$) выполняются следующие действия:

4. Вычисляется номер текущей итерации $k = k + 1$.

5. С использованием одномерной оптимизации вычисляется коэффициент η_k.

6. Находится новое приближение вектора весов

$$\mathbf{w}^{(k)} = \mathbf{w}^{(k-1)} + \eta_k \mathbf{p}_k.$$

7. Вычисляются выход сети и функционал ошибки $E(\mathbf{w}_k)$.

8. Проверяется условие окончания процесса обучения $E(\mathbf{w}_k) \le \varepsilon$, где ε – малая величина. Если условие выполняется, то алгоритм завершен (переход на шаг 14), иначе – переход на следующий шаг алгоритма.

9. Используя алгоритм обратного распространения ошибки, вычисляется вектор градиента $\mathbf{g}_k$.

10. Вычисляется коэффициент β_{k+1}.

11. Определяется новое направление движения

12. $\mathbf{p}_{k+1} = -\mathbf{g}_k + \beta_{k+1}\mathbf{p}_k$

13. Переход на шаг 4.

14. Конец алгоритма.

Метод сопряженных градиентов имеет сходимость, близкую к линейной, и работает значительно быстрее метода градиентного спуска, метод уступает методу Левенберга-Марквардта, но значительно менее требователен к памяти. Особо следует отметить, что в сетях глубокого обучения из-за очень большого числа весов, как правило, применяют более простые методы первого порядка.

Широко используемым при обучении нейронных сетей, не содержащих большого числа слоев, является метод Левенберга-Марквардта. В этом методе матрица Гессе аппроксимируется с помощью матрицы Якоби. В методе Левенберга-Марквардта функционал ошибки представляется в виде

$$E(\mathbf{w}) = \frac{1}{2}\sum_{i=1}^{M}\left[e_i(\mathbf{w})\right]^2 = \frac{1}{2}(\mathbf{e},\mathbf{e}) = \frac{1}{2}\mathbf{e}^{\mathrm{T}}\mathbf{e}, \tag{2.37}$$

где $e_i = y_i(\mathbf{w}) - t_i$, $y_i(w)$ – выход сети, t_i – целевое значение, M описан ниже, $\mathbf{e}$ – вектор ошибок сети, T – символ транспонирования,

$$\mathbf{e}(\mathbf{w}) = \begin{bmatrix} e_1(\mathbf{w}) \\ e_2(\mathbf{w}) \\ \ldots \\ e_M(\mathbf{w}) \end{bmatrix}. \tag{2.38}$$

В формуле использован один индекс ошибки. В случае пакетного обучения функционал ошибки вычисляется как сумма квадратов ошибок по всем выходам сети и по всем обучающим примерам. Тогда для применения метода Левенберга-Марквардта необходимо последовательно пронумеровать ошибки по всем примерам и выходам сети. В этом случае $M = Q \cdot N$, где Q – количество примеров обучающей выборки, N – число нейронов выходного слоя. Например, вектор ошибок сети можно представить в виде

$$\mathbf{e} = \left[\underline{e_1^{(1)}\, e_2^{(1)} \ldots e_N^{(1)}} \,\vdots\, \underline{e_1^{(2)}\, e_2^{(2)} \ldots e_N^{(2)}} \,\vdots\, \ldots \,\vdots\, \underline{e_1^{(Q)}\, e_2^{(Q)} \ldots e_N^{(Q)}}\right]^{\mathrm{T}},$$

где $e_i^{(q)}$ – ошибка нейрона i выходного слоя ($i = \overline{1, N}$, N – число нейронов в выходном слое) на примере q ($q = \overline{1, Q}$).

Последовательно пронумеровав элементы вектора, получим нужное представление. Будем также использовать единый вектор весов, последовательно пронумеровав веса, начиная с первого слоя.

В k-й итерации вектор весов корректируется по формуле

$$\mathbf{w}^{(k)} = \mathbf{w}^{(k-1)} + \Delta\mathbf{w}^{(k)}, \tag{2.39}$$

где вектор поправки $\Delta\mathbf{w}^{(k)}$ определяется из

$$\left(\mathbf{J}_{k-1}^{\mathrm{T}}\mathbf{J}_{k-1} + \mu_k\mathbf{E}\right)\Delta\mathbf{w}^{(k)} = -\mathbf{g}_{k-1},$$

где

$$\mathbf{J} = \begin{bmatrix} \frac{\partial e_1}{\partial w_1} & \frac{\partial e_1}{\partial w_2} & \cdots & \frac{\partial e_1}{\partial w_n} \\ \frac{\partial e_2}{\partial w_1} & \frac{\partial e_2}{\partial w_2} & \cdots & \frac{\partial e_2}{\partial w_n} \\ \cdots & \cdots & \cdots & \cdots \\ \frac{\partial e_M}{\partial w_1} & \frac{\partial e_M}{\partial w_2} & \cdots & \frac{\partial e_M}{\partial w_n} \end{bmatrix} \tag{2.40}$$

– матрица Якоби, μ – параметр регуляризации (параметр Левенберга-Марквардта), $\mathbf{g} = \mathbf{J}^{\mathrm{T}}\mathbf{e}$ – вектор градиента.

Нижние индексы у векторов и матриц означают, что они вычисляются по значению вектора весов, полученному на предыдущем шаге обучения. Причем параметр регуляризации изменяется на каждом шаге обучения.

Ошибка сети характеризуется *функцией потерь*, или *функцией издержек* (Loss Function). Функция потери – это неотрицательное число, характеризующее качество работы сети. При обучении с учителем применяется *квадратичная функция потерь* (Рисунок 2.12):

$$L(e_i) = (y_i - t_i)^2,$$

где e_i – ошибка i-го выхода, y_i – значение выходного сигнала, t_i -целевое значение.

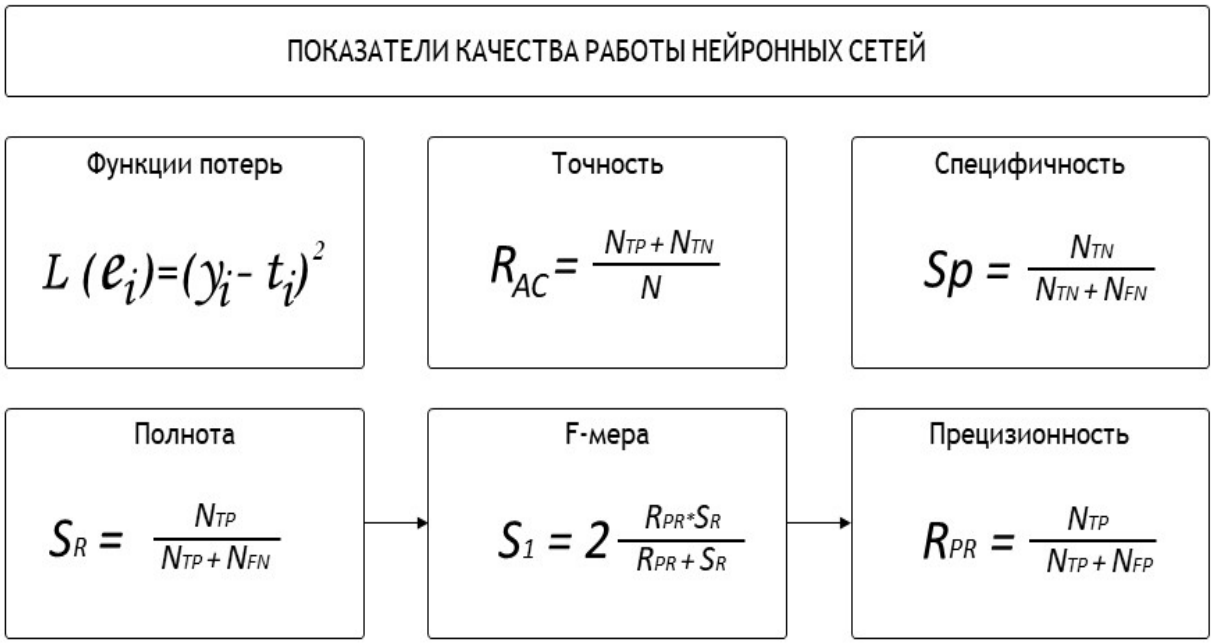


Рисунок 2.12 – Показатели качества сетей

Можно задать различный вес прецезионности и полноте, использовав меру

$$F_\beta = \left(\beta^2 + 1\right)\frac{R_{PR} * S_R}{\beta^2 R_{PR} + S_R}.$$

если $0<\beta<1$, то приоритет отдается прецезионности, если $\beta>1$, то приоритет отдается полноте. При $\beta=1$ получается мера F_1.

Применение нейросетей в решении задач управления безопасностью характеризуется как минимум двумя проблемными областями: все, что связано с машинным обучением (МО), а также с областью DATA MINING. Отличительной особенностью методов МО является то, что они способны решать широкий спектр задач без явного кодирования алгоритма решения. Сложность работы в сфере DATAMINING обусловлена неточностью, противоречивостью, разнородностью и неполнотой данных, которые при этом могут иметь гигантские объемы. Методы МО имеют преимущество в тех случаях, когда отсутствует четко формализованный

алгоритм решения в виду высокой вариативности решения или допускается неопределенность поведения модели.

Искусственный интеллект (ИИ), в частности машинное и глубокое обучение, значительно продвинул исследования в области интеллектуальных систем (ITS) благодаря способности распознавать и классифицировать шаблоны в больших наборах данных. Алгоритмы ИИ успешно применяются для решения основных проблем и задач ITS, в том числе зондирования, прогнозирования, восприятия, обнаружения и принятия решений. Однако, современные модели ИИ, особенно глубокие нейронные сети (DNN), страдают от недостатка интерпретируемости. Внутренняя структура DNN изначально не предназначена для предоставления информации об их внутреннем механизме работы. Это препятствует использованию и принятию этих моделей «черных ящиков» в системах, критически важных для безопасности (ITS). ITS включают в себя решения о жизни и смерти, доверяя такие важные решения системе, которая не может объяснить или оправдать себя, что представляет очевидную опасность, поэтому объяснимость и этичность ИИ становятся предметом пристального внимания в задачах интеллектуального транспорта.

Решение проблемы объяснимости ИИ связано с решением следующих задач:

– интерпретируемость глубоких нейронных сетей,

– интерпретируемость глубокого обучения с подкреплением, обучение с обратным подкреплением,

– интерпретируемые методы для моделей обучения под наблюдением и без учителя,

– компромисс между интерпретируемостью и точностью,

– показатели интерпретируемости и оценки.

Принципы реализуемости указанных задач заключаются в следующем:

1. Системы ИИ должны предоставлять сопутствующие доказательства или обоснования для всех своих результатов.

2. Системы должны предоставлять объяснения, которые являются значимыми или понятными для отдельных пользователей.

3. Объяснения правильно отражают процесс системы для генерирования выходных данных.

4. Система работает только в условиях, для которых она была разработана, или когда система достигает достаточной уверенности в своем выходе.

Указанные подходы должны быть реализованы в рамках информационного управления безопасностью.

Выводы к главе 2

1. Разработаны принципы интеллектуального управления транспортной безопасностью, основанные на оптимальном, ситуационном и адаптивном подходах к управлению и определяющие важнейшие процессы и процедуры управления.

2. На основе глубокого анализа проблем интеллектуального и информационного управления транспортной безопасностью установлено, что широкому внедрению такого управления в практику авиационных систем безопасности препятствует отсутствие серьезного математического обоснования и исследования процессов управления безопасностью, что существенно ограничивает возможности формализации и алгоритмизации, что в свою очередь, снижает эффективность автоматизированного управления.

3. Интеллектуальное и информационное управление безопасностью в части, касающейся аппаратно–программного обеспечения, базируется на современных достижениях компьютерных систем, основанных на технологиях ESM, PSIM, Data Mining.

4. ESM (Electronika Security Manager) представляет собой аппаратно–программный комплекс, реализующий принципы глубокой интеграции и инцидентного управления.

5. PSIM (система управления физической безопасностью) является программной платформой и предлагает уникальные возможности интеллектуального решения вопросов управления безопасностью через информацию.

6. Data Mining (интеллектуальный анализ данных) включает математическую статистику, искусственный интеллект и машинное обучение, обеспечивающие выявление скрытых взаимосвязей внутри больших бах данных.

7. Доказано, что эффективное управление безопасностью на основе интеллектуальных технологий возможно при наличии адаптивных моделей ситуации в объекте защиты, в качестве которых предложены и исследованы математические модели в формате дифференциальных уравнений в частных производных.

8. Показано, что в гражданской авиации исследование проблем безопасности дает максимальный эффект при использовании искусственных нейронных сетей.

ГЛАВА 3 МЕТОДЫ РЕШЕНИЯ ПРОБЛЕМЫ «УПРАВЛЯЕМОСТЬ ТРАНСПОРТНОЙ БЕЗОПАСНОСТИ АЭРОПОРТА» НА ОСНОВЕ ИНФОРМАЦИОННО-УПРАВЛЯЮЩЕГО ПРОСТРАНСТВА

3.1 Концепция информационной управляемости транспортной безопасности аэропорта

Одним из главных критериев эффективной деятельности гражданской авиации является безопасность, в рамках которой транспортная (авиационная) безопасность занимает не последнее место.

Транспортная (авиационная) безопасность – состояние защищённости объектов транспортной инфраструктуры и транспортных средств от актов незаконного вмешательства. ФЗ №16 от 9 февраля 2007

Состояние защищенности объекта. Требования. Оценка выполняемости. Соответствие требованиям.

Уровень безопасности. Приемлемый уровень. Измеряемость безопасности. Управление уровнем. Автоматизация.

Обеспечение безопасности. Нормативное управление. Теория управления организационными системами.

Управление безопасностью. Оптимальное управление. Теория оптимального управления.

Действующие системы обеспечения транспортной безопасности не обладают возможностью оперативно ей управлять.

Современные компьютерные технологии обладают существенными возможностями для решения задач управления безопасностью, но их применение ограничено значительной неопределенностью в постановке задач управления безопасностью, методологическими проблемами математической формализации, сложностью алгоритмизации процессов управления и явным недостатком количества и качества моделей управления в безопасности.

Транспортная безопасность - это состояние защищенности объекта, которое достигается через оценку соответствия требований к безопасности объекта и реальной ситуации на объекте. Этот процесс называется обеспечением безопасности и осуществляется в рамках нормативного управления на основе теории управления организационными структурами [21].

Нормативное управление не предполагает измерения безопасности, а ограничивается процедурой соответствия требованиям. Если ввести понятие уровень безопасности, то процедура соответствия не отвечает на этот вопрос, тем более если это приемлемый уровень. В таком случае необходимо измерение безопасности и управление ей. Такое управления называется оптимальным и реализуется в соответствии с теорией оптимального управления.

Все это обуславливает две проблемы в рамках исследования транспортной безопасности в гражданской авиации: проблема управляемости транспортной безопасностью аэропорта и проблема алгоритмизации процедур управления.

Решение проблем управляемости безопасности, формализации и алгоритмизации на базе теории оптимального управления и пространственно-ситуативного подхода состоит в разработке комплекса информационного управления транспортной безопасностью на основе адекватных математических моделей пространства безопасности и адаптивных алгоритмов оптимизации параметров системы защиты.

Информационное управление по отношению к транспортной безопасности реализует две функции: нормативное управление и оптимальное управление, причем, если нормативное управления достаточно хорошо разработано и реализовано, то оптимальное управление рассматривается как решение отмеченных проблем.

Проблема 1: Управляемость безопасности. Действующие системы транспортной безопасности основаны на понятии обеспечение безопасности, когда реализуется организационно-нормативный принцип управления (менеджмент),

предполагающий оценку безопасности через соответствие требованиям. Нормативное управление основано на теории управления организационными структурами, что не соответствует современным требованиям к транспортной безопасности объектов гражданской авиации. Альтернативой является оптимальное управление, что предполагает измерение уровня безопасности, его оценку, формирование приемлемого уровня и автоматизированную ликвидацию возникающих отклонений. Проблема усугубляется тем, что понятия обеспечение и управление далеко не синонимы и корректный переход от обеспечения к управлению безопасностью требует серьезного научного обоснования.

Проблема 2: Формализация и алгоритмизация. Методом решения проблемы управляемости безопасности является математическое моделирование, которое предполагает разработку адекватных моделей. Формирование математических моделей в предметной области транспортная безопасность, существенно осложняется методологическими проблемами формализации, на что влияет неопределенность и неоднозначность математического представления объектов и субъектов безопасности, нестабильность и нелинейность процессов безопасности, некоторая ограниченность применения известного математического аппарата для задач безопасности. Проблемы формализации инициируют проблемы алгоритмизации, возникающие при использовании классических методов построение алгоритмов.

Информационное управление представляет собой процесс выработки и реализации управленческих решений в ситуации, когда управляющее воздействие носит неявный, косвенный характер и объекту управления представляется информация о ситуации (информационная картина), ориентируясь на которую объект выбирает линию своего поведения (реакции) (Рисунок 3.1).

Информационное управление принципиально отличается от понятия информационный менеджмент. Информационный менеджмент использует информационные методы и технологии для поддержки организационного

управления [16; 21]. Информационное управление более формализовано и основано на информационных моделях и информационном моделировании. Парадигма информационного управления: «создание и использование информационных моделей для построения полностью формализованных технологий управления, анализ которых может быть выполнен человеком или компьютером. Главным свойством информационного управления является жесткая привязка к информационным управленческим моделям и обязательная интеграция последних в технологии управления.

Информационное управление транспортной безопасностью обладает свойством дуальности и основано на двух понятиях: обеспечение и собственно управление, действующих совместно (Рисунок 3.1).

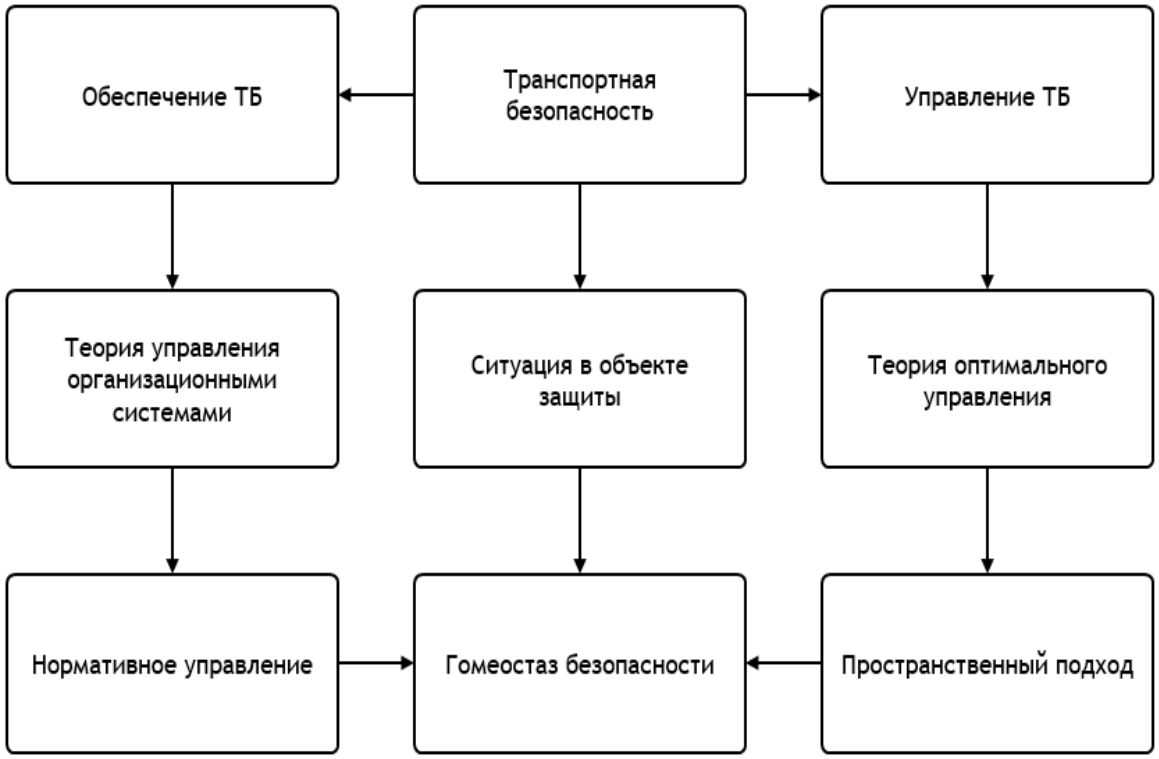


Рисунок 3.1 – Дуальность информационного управления

Гомеостаз безопасности понимается как некоторое устойчивое состояние объекта защиты (ситуация), когда пространство защиты обеспечивает поддержания приемлемого уровня безопасности.

Применение информационных моделей в управлении дает следующие преимущества:

– превращает технологию информационного управления в формализованную сложную систему с возможностью системного анализа,

– создает возможность логического анализа для сложных систем управления и при больших объемах управленческой информации,

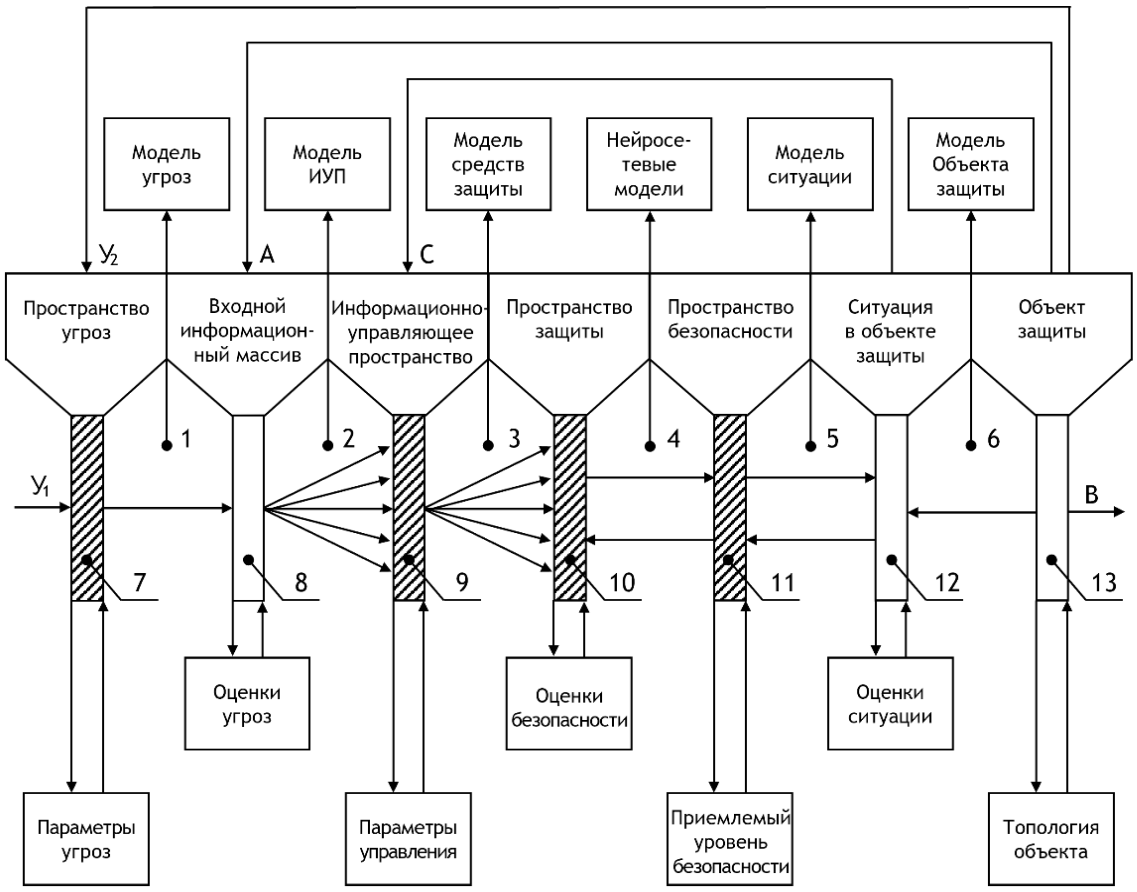
– осуществляет объектный (ресурсы, данные, результаты) и процессуальный (процессы, соответствие целям) анализы,

– создает возможность проводить ситуационный анализ, проводить формальный анализ рисков и строить прогнозы на основе объектных критериев.

Концепция основана на пространственно-ситуативном подходе и включает следующие пространства (Рисунок 3.2): пространство угроз (7), информационно-управляющее пространство (9), пространство защиты (10), пространство безопасности (11).

Пространство угроз (7) включает весь перечень потенциальных угроз, идентифицированных в аэропорту и определенных соответствующим приказом Росавиации. Формальное представление угроз в виде некоторой математической модели (1) достаточно затруднительно ввиду существенной неопределенности в описании угроз и их оценок, поэтому модель строится в рамках эвристического подхода с учетом топологии объекта защиты (13), отраженной в соответствующей модели объекта защиты (6).

На этой основе формируется входной информационный массив (8), включающий теоретические и практические (измеренные) данные по входным воздействиям на объект защиты.



A - информация по структуре и топологии объекта защиты (аэропорт);
B - выходные данные по транспортной безопасности;
C - информация по ситуации в объекте защиты;
$У_1$ - угрозы безопасности аэропорта;
$У_2$ - угрозы от несанкционированного вмешательства персонала.

Рисунок 3.2 – Структурно-логическая модель информационного управления транспортной безопасностью аэропорта (концепция)

Информационно-управляющее пространство (9) (ИУП) представляет собой центр, в котором концентрируется информация об объекте защиты, его топологии, оценки ситуации в объекте, методы обработки информационных массивов, реальные оценки безопасности и другие характеристические элементы. Модель ИУП (2) определяет методы и процедуры его формирования. ИУП формирует параметры управления для пространства защиты (10), которое включает средства защиты объекта. Пространство защиты формирует оценки безопасности как сигнал

управления для средств защиты. Средства защиты на основе соответствующей модели (3), выполняют совокупность действий по парированию угроз, осуществляют мониторинг безопасности и изменяют ситуацию (12) в объекте защиты (13). Эти процедуры выполняются в реальном масштабе времени с целью поддержания транспортной безопасности на приемлемом уровне.

3.2 Пространственно-ситуационный подход к управлению транспортной безопасностью

Информационное управление безопасностью основано на понятиях пространство безопасности и ситуация в структуре объекта защиты (состояние объекта), которые формируют понятие пространственно-ситуативный подход (Рисунок 3.3).

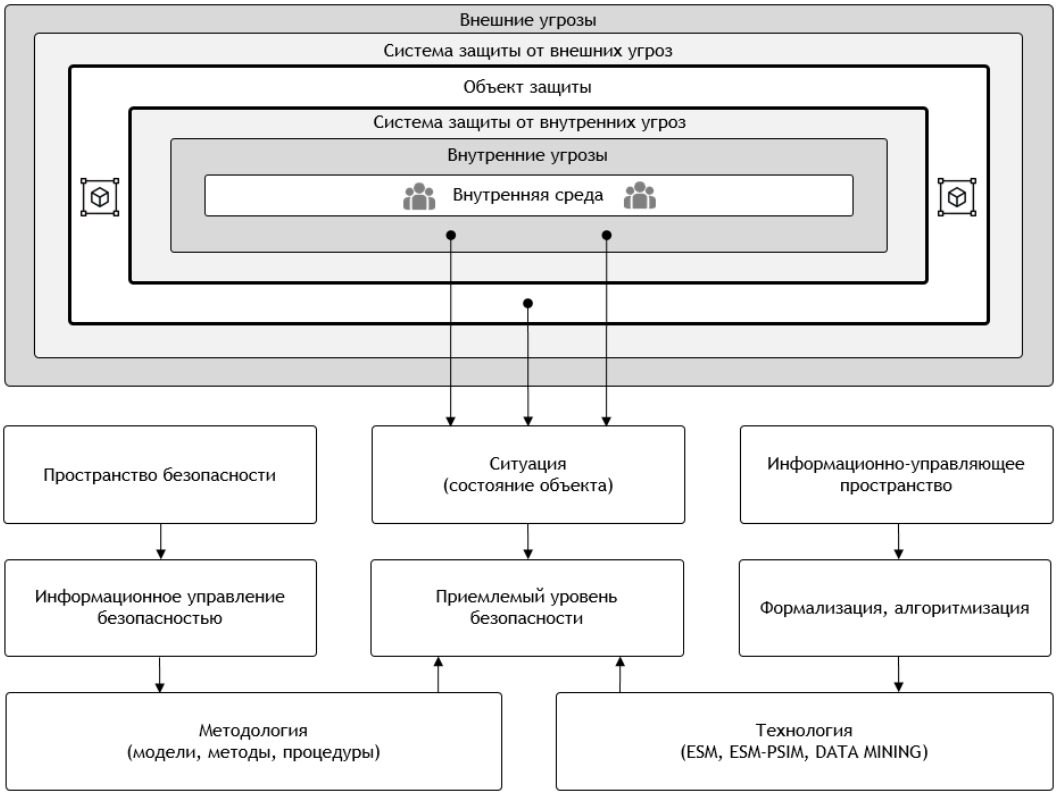


Рисунок 3.3 – Пространственно-ситуативный подход к информационному управлению безопасностью

Методология **обеспечения безопасности** ориентирована на теорию организационных систем и представляет собой нормативный тип управления. В рамках данной методологии результат формируется за счет удовлетворения совокупности определенных требований по безопасности, прописанных в нормативных документах, их оценки (уязвимость) применительно к объектам защиты, констатации факта приемлемости уровня безопасности и, если это условие не выполняется, подключения механизма защиты объекта, представляющего собой систему ликвидации или парирования угроз. Результат здесь понимается как состояние (ситуация) объекта защиты. Ситуация обозначает множество устойчивых значений переменных параметров объекта (Рисунок 3.4).

Рисунок 3.4 – Структура информационного менеджмента безопасности

Совокупность угроз безопасности или факторы нестабильности (2) концентрируются вокруг некоторой организационной структуры, в данном случае аэропорт, параметры которой отражаются в пространстве безопасности (5).

Организационная структура (5) изменяется под воздействием этих факторов, которые по отношению к структуре могут быть внешними (3) и внутренними (1). Термин «изменяется» здесь следует понимать как изменения в структуре системы защиты, внесенные на основании решения ЛПР (А).

Нормативное управление можно рассматривать как косвенное регулирование уровня безопасности объекта в соответствии с требованиями нормативных документов. В этом случае необходимо выстраивать определенную организационную структуру и управлять именно ей в соответствии с теорией управления организационными системами.

Организационная структура представляет собой целостную систему, состоящую из совокупности упорядоченных уровней управления, которая организует процесс коммуникации между ними с целью обеспечения приемлемого уровня безопасности в условиях взаимодействия с внешней и внутренней средой (Рисунок 3.4). Таким образом, обеспечение безопасности может быть квалифицировано как информационный менеджмент.

Корректировка параметров защиты возникает при появлении рассогласования между характеристиками организационной структуры (6) и критериальными требованиями (4), задаваемыми ЛПР. Иными словами, ЛПР задают требования к организационной структуре в форме критериев и их параметров (4,7), мониторинг характеристик (6), выявляет реальные параметры (9) этих критериев, которые сопоставляются в квалиметрической матрице (10), где роисходит преобразование указанных параметров в показатели качества и осуществляются процедуры квалиметрической оптимизации (13). Результат оптимизации используется в виде оценочных значений.

Идея квалиметрической оптимизации состоит в том, что векторные величины путем использования квалиметрических преобразований трансформируются в скалярные параметры, относящиеся к понятию качество [55; 116; 186].

Если критерии оптимизации выражены через скалярные величины, вопрос о переходе к качеству решается достаточно просто: можно поставить в соответствие

значение критерия и уровень качества, приняв единую шкалу измерения критериев и определив шкалу оценки уровня качества. Если критерии векторные, а их параметры скалярные величины, квалиметрическая оптимизация (Рисунок 3.5) состоит в процедуре вычисления минимального, максимального и среднего значений качества (КС-процедура).

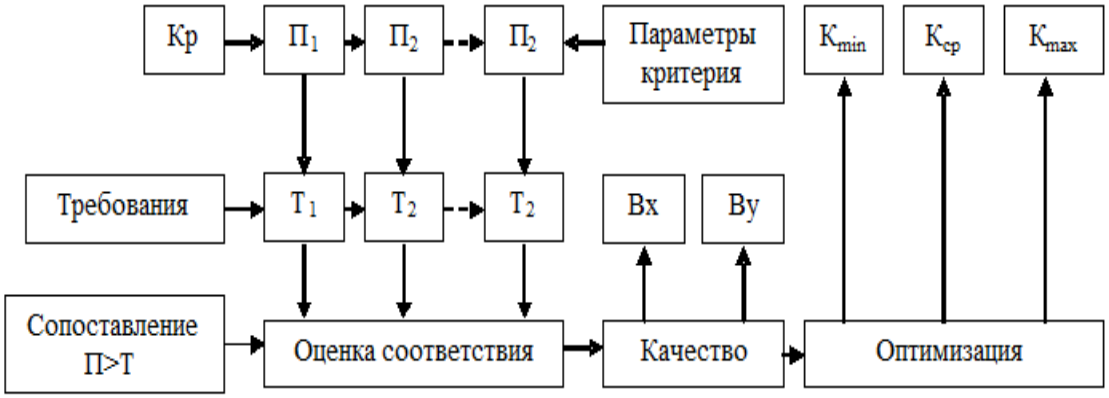


Рисунок 3.5 – К вопросу о квалиметрической оптимизации

Если критерии и их параметры векторные, то каждый из векторов однозначно определяется соответствующими параметрами: А и В. Тогда для перехода к параметру «качество» по отношению к каждому вектору правомочно провести КС-процедуру и использовать квалиметрическую матрицу (Рисунок 3.6).

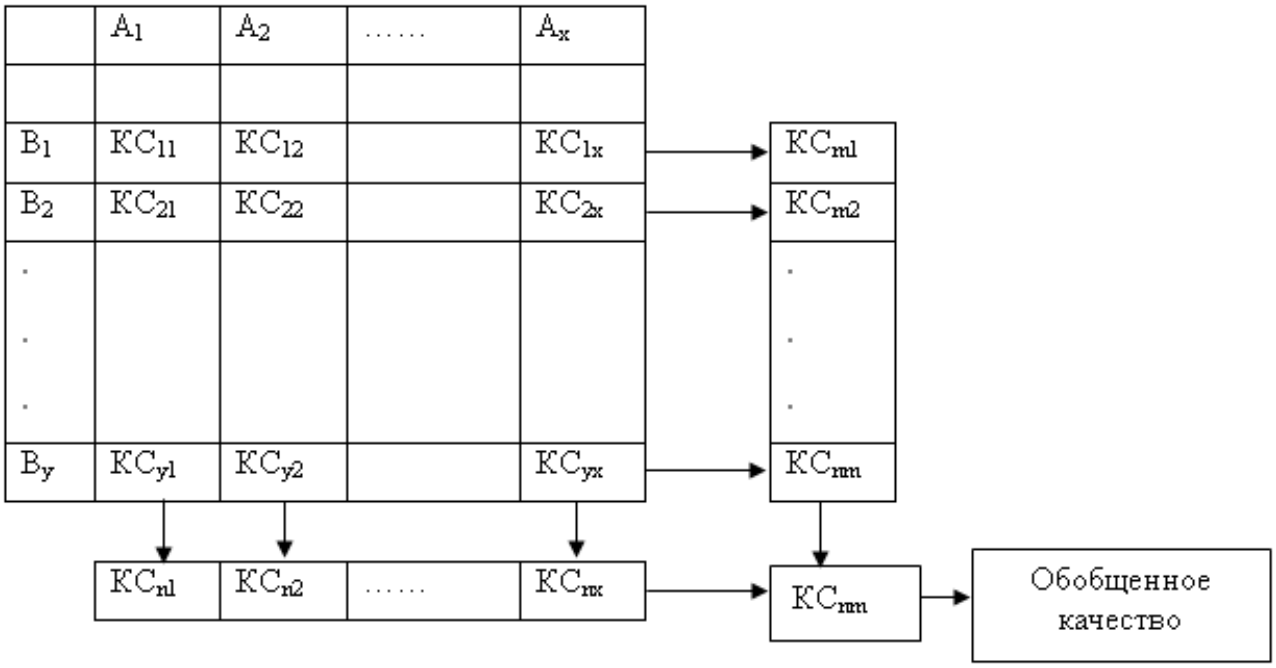


Рисунок 3.6 – Квалиметрическая матрица

Квалиметрическая процедура реализует идею перехода от векторного представления критерия оптимизации к скалярному представлению этого критерия в виде уровня качества. На основе квалиметрической матрицы строятся процедуры обеспечения транспортной безопасности. Управление в терминах информационного менеджмента осуществляется путем принятия соответствующих решений некоторой иерархией управляющих лиц: А – высший уровень иерархии управления, В – средний уровень и С – нижний уровень иерархии (Рисунок 3.4).

Методология **управления безопасностью** ориентирована на теорию оптимального управления. Такое управление предполагает постоянный или периодический мониторинг безопасности, при этом устанавливаются определенные единицы измерения. В подавляющем большинстве случаев это баллы, поскольку измерение уровня безопасности осуществляется экспертными методами. Устанавливается нормативное значение безопасности, т.е. выбирается приемлемый уровень, который поддерживается во времени, для чего существует соответствующая система коррекции. Информационное управление строится в соответствии с пространственным подходом.

С точки зрения системотехники исследуемый объект относится к категории сложных систем и включает в свой состав следующие элементы (категории): объект защиты, совокупность угроз, система защиты, безопасность как понятие, управление как процесс, определенный объем информации, внешняя среда, внутренняя среда. Эти категории определяют содержание и параметры процессов обеспечения и управления транспортной безопасностью. Каждую из этих категорий можно отобразить в форме некоторого пространства. Пространство понимается как форма существования материальных объектов и процессов. Пространство характеризует структурность и протяженность материальных систем (Рисунок 3.7).

Рисунок 3.7 – Структура информационного управления безопасностью

Ориентация информационного управления на пространственный подход позволяет использовать для исследования математическое моделирование, которое предполагает определенную формализацию. С учетом серьезной неопределенности в описании указанных выше категорий задача моделирования становится плохо формализуемой и слабо структурируемой. В таком случае приходится искать такие модели, которые при всех сложностях дадут приемлемый результат. Представление элементов управляющей структуры в форме некоторых пространств дает возможность решить эту задачу с приемлемой точностью.

Понятие угрозы является исходным при анализе безопасности. В приложении к транспортной безопасности необходимо исследовать четыре типа угроз: реализованные (акт незаконного вмешательства совершен), потенциальные (АНВ предполагается, но тип его известен), неизвестные (новые, не описанные и не объявленные ранее), несанкционированное вмешательство персонала. Угрозы, даже если они единичные, следует рассматривать в приложении к некоторому множеству объектов защиты, т.е. они обладают свойством протяженности и могут быть представлены в форме пространства. Такое представление упрощает формализацию и позволяет использовать более адекватные модели.

Пространство защиты однозначно определяется системой защиты, которая формируется в противовес всем типам угроз. С другой стороны, пространство защиты предназначено для обеспечения безопасности объекта защиты, который обладает определенной топологией. Выбор модели ограничен методологией исследования угроз.

Сопоставление этих двух пространств в динамике позволяет определить параметры пространства безопасности, которое формируется под воздействием управляющих сигналов в системе защиты.

Указанные пространства формируют совокупность данных (информационные массивы), отражающие состояние объекта защиты с точки зрения безопасности. Вся информация поступает в информационно-управляющий центр (пространство), в котором после ситуационного анализа вырабатываются

управляющие сигналы. Таким образом достигается определенная цикличность управления. Здесь как критерий оптимальности управления выступает гомеостаз безопасности.

Информационные массивы, как структурные, так и ситуативные, образуют пространства угроз, пространство защиты и, как итог, пространство безопасности. Они отражаются в формате информационно-управляющего пространства, где концентрируются в виде соответствующих параметров этого пространства, измерение и анализ которых лежит в основе принятия решений по управлению пространством защиты, что в свою очередь, управляет уровнем транспортной безопасности объекта защиты. Здесь решается главная задача информационного управления, а именно: формируются соответствующие модели и алгоритмы управления, реализация которых в цифровом формате представляет собой управляющее воздействие и передается на исполнительные системы. Задача решается поэтапно, путем внедрения на соответствующих этапах технологий ESM, PSIM и BIG DATE.

3.3. Информационно-управляющее пространство и его кластеризация

Исследование системы управления транспортной безопасностью в значительной степени отличается от алгоритмов исследования обычных систем в связи с наличием нефункциональных связей между элементами и значительными неопределенностями со стороны внешнего периметра, что исключает применение комплексной модели. Приходится системное представление информационно-управляющего пространства структурировать, имея в виду его представление в форме функционально независимых моделей с последующим их автономным исследованием.

На первом этапе такого исследования целесообразно использовать технологию функционального моделирования, алгоритмические и программные средства которой в настоящее время достаточно хорошо отработаны. Из всего

многообразия известных технологий наиболее распространены методологии IDEF, ARIS и UML. IDEF (Icam Definition) использует метод структурного анализа и проектирования SADT (Structure Analysis and Technique). По отношению к объекту модель воспроизводит действия и связи между ними. Соответствует ГОСТ (Рекомендации по стандартизации «Методология функционального моделирования»). ARIS (Architecture of Integrated Information System) включает инструментальную систему графического моделирования организационной и функциональной структур и структуру данных объекта исследования. Наибольший интерес для задач безопасности представляет язык моделирования UML (Unified Modeling Language), включающий CASE-средства компьютерной поддержки. UML-модель дает полное представление о динамических, статических и структурных аспектах объекта [57].

Имея результаты моделирования с использованием UML-модели, можно говорить о некоторых контурах интеллектуально-стратегического управления безопасностью, поскольку именно здесь впервые появляются значения параметров управления и определяются направления развития пространства безопасности, т.е. появляется ситуация, динамику которой требуется исследовать. Для этих целей нужна модель динамики развития ситуации – сценарная модель развития. Такие модели могут быть аналитическими и имитационными. Аналитические модели в формате дифференциальных уравнений в частных производных рассмотрены выше. Эти модели позволяют определить ситуацию в некоторые моменты времени. С учетом неопределенности, неполной и неточной входной информации в этом случае можно говорить о приближенном решении с использованием эвристических методов. Ниже представлена сценарная модель безопасности с учетом модельных представлений Германа Канна [42; 57].

Ситуация с безопасностью в рамках объекта защиты описывается некоторым конечным множеством $W=\{w_0, w_l, \ldots, w_m\}$ состояний. W_o – начальное состояние, w_i – текущее состояние, $i = l, \ldots m$. $p: W \rightarrow W$ отображает воздействие, которое переводит систему из состояния в состояние. $P(w_i)$ – некоторое промежуточное

состояние, в котором находится система после воздействия. $D=(d_{ij})$ – матрица весов, которая определяет меру различия между состояниями. D_{ij} можно вычислить на основе текущих показателей (как расстояние Махаланобиса) [42] или экспертным путем [12; 84].

Сценарная модель развития системы безопасности строится в виде взвешенного ориентированного графа G=(Z,P,D). Свойства графа и алгоритм построения сценарной модели представлены в работах [118; 144; 192].

Рассмотренный алгоритмический аппарат достаточно легко трансформируется в программное отображение и согласуется с кластерной структурой информационно-управляющего пространства, в рамках которой формируются управляющие сигналы.

В условиях информационного управления безопасностью, информационно-управляющее пространство становится важнейшим элементом системы, в котором отображается информация по результатам мониторинга ситуации в объекте, формируются критерии и параметры управления безопасностью и вырабатываются сигналы управления.

На первых этапах формирования информационно-управляющего пространства его следует рассматривать как некоторый виртуальный объект, не имеющий физических параметров, и только потом, когда методология формирования пространства будет отработана, можно говорить о моделях информационно-управляющего пространства. В таком случае, на первом шаге следует определить некоторые основные понятия, определяющие базовую структуру информационного управления безопасностью (Рисунок 3.8).

Информационно-управляющее пространство (ИУП) представляет собой единый глобальный центр управления транспортной безопасностью, в котором сосредоточены основные модели сценариев и методов защиты объекта транспортной инфраструктуры, осуществляется интеллектуальный анализ больших объемов входной информации по ситуации в объекте, принимаются решения и вырабатываются управляющие команды для исполнительных

элементов. ИУП обладает свойством дуальности. С одной стороны, его можно рассматривать как виртуальный объект, где в обобщенном виде сосредоточены наши сиюминутные представления о сути явлений и процессов в объекте защиты под действием внешних и внутренних угроз безопасности. С другой стороны, это реальный программно-технический комплекс, обеспечивающий защиту объекта за счет своих исполнительных механизмов, который характеризуется функциональными моделями и конкретными алгоритмами деятельности.

Рисунок 3.8 – К понятию информационно-управляющего пространства

Задача комплексной оценки приводит к использованию аппарата теории векторной оптимизации и принятия решений, где вместо единственного критерия

оптимальности *f(y)* варианта решения *y* рассматривается вектор критериев оптимальности

$$f(y) = (f^1(y), f^2(y), ..., f^N(y)). \quad (3.1)$$

Идея состоит в том, чтобы осуществить переход к целостному учету влияния многих критериев на эффективность различных вариантов решений (способ учета неопределенности). Известно достаточно много методов принятия многокритериальных решений: метод весовых коэффициентов, множество Эджворта-Парето, оценка векторов, STEM, MAUT, ELECTRE, AHP, ПРИНН и другие [1; 27; 50; 61; 68].

Подход AHP (Analytic Hierarchi Pricess) основан на сравнении каждой пары критериев по определенной шкале. В результате задаются коэффициенты учета сравнительной значимости критериев

$$c_{ij}, \quad i, j = 1,...,n \quad c_{ii} = 1 \quad i = 1,...,n \quad (3.2)$$

На их основе рассчитывается собственный вектор каждого критерия

$$k_i = \sqrt[n]{d_i} \quad i = 1,...,n, \quad d_i = \prod_{j=1}^{n} c_{ij} \quad i = 1,...,n \quad (3.3)$$

и его весовой коэффициент в линейной свертке

$$\alpha_i = \frac{k_i}{\sum_{i=1}^{n} k_i}, \quad i = 1,...,n. \quad (3.4)$$

Метод ПРИНН использует модель принятия решений, содержащую три множества: допустимых вариантов решений ***Y***, неопределенностей ***X*** и допустимых способов учета неопределенности ***S*** и функцию обобщенных потерь ***f(x,y),*** выступающую в качестве локального обобщенного критерия оптимальности:

$$f(x, y) = \sum_{i=1}^{n} x_i f_i(y), \quad (3.5)$$

где x_i – неопределенные «весовые коэффициенты» критериев.

При нескольких обоснованных постулатах способы учета неопределенности задаются «функцией построения» $G(t)$:

– Для $X=\{x_i\}_{i=1,\ldots,N}$

$$F(X,y)=G^{-1}\left(\frac{1}{N}\sum_{i=1}^{N}G(f(x_i,y))\right) \quad . \tag{3.6}$$

– Для X – области конечномерного Евклидова пространства

$$F(X,y)=G^{-1}\left(\frac{1}{S_X}\int_{x\in X}G(f(x,y))dx\right) \quad , \tag{3.7}$$

где S_X – мера области X.

Если порождающая функция имеет простейший вид $G(t)=t$, тогда

$$F(X,y)=\frac{1}{N}\sum_{i=1}^{N}f(x_i,y) \quad , \tag{3.8}$$

что соответствует принципу Лапласа.

Пусть требуется получить комплексную оценку решений, описываемых двумя критериями $f^1(e)$, $f^2(y)$. Введем линейную свертку этих критериев с неопределенными весовыми коэффициентами x^1, x^2:

$$f(x^1,x^2,y)=x^1f^1(y)+x^2f^2(y), \tag{3.9}$$

удовлетворяющими известным условиям нормировки:

$$x^1+x^2=1,\_\_x^1>=0,\_\_x^2>=0. \tag{3.10}$$

Формула для расчета обобщенных потерь:

$$F(X,y)=\frac{1}{1}\int_0^1(x^1f^1(y)+(1-x^1)f^2(y))dx^1=\frac{f^1(y)+f^2(y)}{2}. \tag{3.11}$$

В случае двухкритериальной оценки эффективности решения y, при котором критерий f^1 является более значимым, чем f^2 добавляется неопределенность:

$$F(X,y)=\frac{1}{\frac{1}{2}}\int_{\frac{1}{2}}^1(x^1f^1(y)+(1-x^1)f^2(y))dx^1=\frac{3f^1(y)+f^2(y)}{4}. \tag{3.12}$$

Полученные оптимальные оценки лежат в основе кластеризации.

Известно множество алгоритмов кластеризации. Большинство из них предполагает сравнение объектов между собой на базе некоторой меры близости, которая принципиально отличает алгоритмы друг от друга. К таким мерам относятся: евклидово расстояние, квадрат евклидова расстояния, расстояние городских кварталов (манхэттенское расстояние), расстояние Чебышева, степенное расстояние и некоторые другие.

Мера близости – величина, имеющая предел и возрастающая с увеличением близости объектов:

– *Евклидово расстояние*

$$D(x,y)=\sqrt{\sum_i (x_i-y_i)^2} \tag{3.13}$$

– *Квадрат евклидова расстояния*:

$$D(x,y)=\sum_i (x_i-y_i)^2 \tag{3.14}$$

– *Манхэттенское расстояние:*

$$D(x,y)=\sum_i |\,x_i-y_i\,| \tag{3.15}$$

– *Расстояние Чебышева*:

$$D(x,y)=\max\left|x_i-y_i\right| \tag{3.16}$$

– *Степенное расстояние*:

$$D(x,y)=\sum_i \left(\left|x_i-y_i\right|^p\right)^{\frac{1}{\gamma}} \tag{3.17}$$

В данной работе для целей кластеризации используется методология нейросетевого моделирования.

Оптимальное управление уровнем транспортной безопасности возможно при условии решения проблемы отставания уровня развития методологии безопасности от уровня разработанных компьютерных технологий. Логично предположить, что решение проблемы находится в сфере формализации предметной области и разработки адекватных моделей соответствующих

процессов и структур. С учетом методологических сложностей в описании и формализации предметной области, которая относится к категории сложных систем, комплексное решение задачи весьма затруднено, а в некоторых случаях практически невозможно, поэтому предлагается последовательное решение задачи в рамках единой структуры, для чего формируются отдельные области (домены) и соответствующие им идеи (Рисунок 3.9).

Формирование информационного содержания доменов осуществляется на основе некоторых критериев и на различных уровнях обобщения. Самый высокий уровень обобщения относится к идеологии и соответствует критерию теория. Здесь каждый домен (безопасность, пространство безопасности, формализация, автоматизация) включает некоторую совокупность информационных массивов, описывающих предметную область безопасности и параметры управления ее уровнем. Внутри домена информация однородна по смысловому содержанию и направленности выходных параметров, т.е. доменная структура, является векторной.

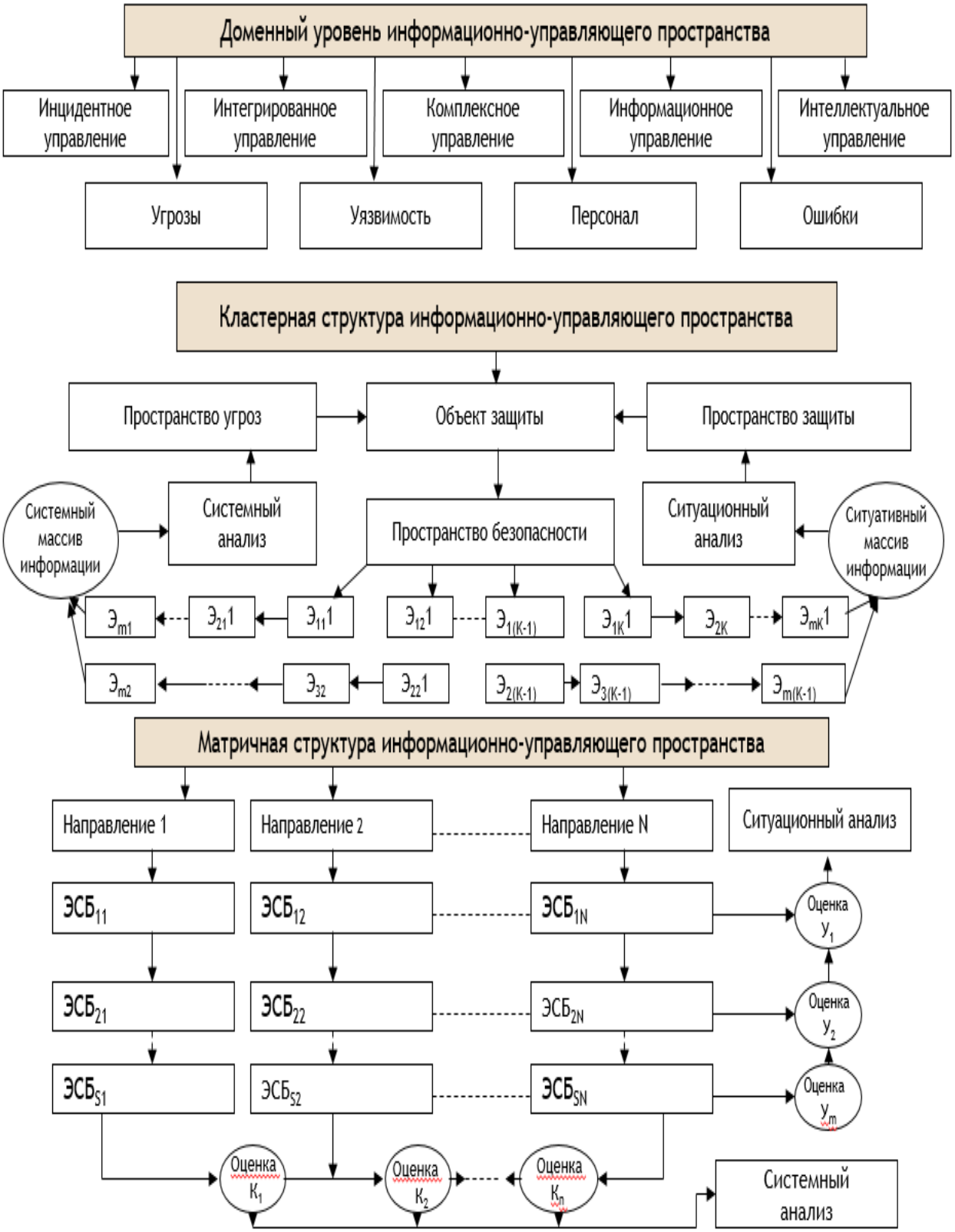


Рисунок 3.9 Базовая структура информационно-управляющего пространства

Первый домен, соответствующий критерию теория, связан с понятием безопасность. Идея решения состоит в интерпретации понятия безопасность, которую предлагается рассматривать как интегральную, основанную на понятии безопасность личности.

Второй домен вводит понятие гипотетическое поле безопасности. Предлагается безопасность объекта рассматривать как некоторое пространство безопасности, формируемое пространством угроз и пространством защиты. В таком случае, можно предположить, что эти пространства, при некоторых допущениях, находятся в сфере влияния теории поля.

Третий домен относится к области формализации. Для информационного управления чрезвычайно важны оценочные процедуры для безопасности, поскольку предполагается, что в его основе лежит интеллектуальный анализ информации. В таком случае, на первый план выдвигаются модели сценариев и модели методов защиты объекта, что на первое место ставит процедуры формализации. Системная сложность предметной области классифицирует решаемые задачи как плохо формализуемые и слабо структурированные. Идея решения находится в области теории краевых задач. При всей их привлекательности придется согласиться с тем, что адекватной модели получить и в этом случае не удастся, что предполагает использование на отдельных этапах алгоритма решения эвристических процедур.

Домен автоматизации включает вопросы гармонизации процедур обеспечения транспортной безопасности с технологическими процедурами информационного управления безопасностью. Идея состоит в том, что инцидентное управление переводится в информационное управление безопасностью с применением современных компьютерных технологий.

Следующий доменный уровень относится к методологии и соответствует критерию тип управления. Здесь выделяется пять доменов, каждый из которых соответствует одному из типов управления: инцидентное, интегрированное, комплексное, информационное и интеллектуальное (Рисунок 3.9).

На этом уровне можно говорить о векторном пересечении доменов, поскольку в реальных системах транспортной безопасности применяется совмещенное управление, например: инцидентное совместно с интеллектуальным.

Далее следует функциональный уровень доменов, который соответствует критерию параметр. Это четыре домена: угрозы, уязвимость, персонал, ошибки.

Домен угрозы концентрирует информацию об угрозах объекту защиты, включая внешние и внутренние источники, оценки параметров этих угроз, методы их идентификации, методы формализации, методы моделирования и другую аналогичную информацию. Идея решения здесь состоит в интерпретации понятия безопасность, которую предлагается рассматривать как интегральную, основанную на понятии безопасность личности. Вводится понятие гипотетическое поле безопасности. Предлагается безопасность объекта рассматривать как некоторое пространство безопасности, формируемое пространством угроз и пространством защиты. В таком случае, можно предположить, что эти пространства, при некоторых допущениях, находятся в сфере влияния теории поля. На выходе домена формируется информационный массив, достаточный для полной идентификации угроз.

Домен уязвимость относится к области формализации. Для информационного управления чрезвычайно важны оценочные процедуры для безопасности, поскольку предполагается, что в его основе лежит интеллектуальный анализ информации.

В таком случае, на первый план выдвигаются модели сценариев и модели методов защиты объекта, что на первое место ставит процедуры формализации.

Системная сложность предметной области классифицирует решаемые задачи как плохо формализуемые и слабо структурированные. Идея решения находится в области теории краевых задач, для чего необходим переход от краевых задач в терминах угроз к краевым задачам в терминах уязвимостей. Однако, при всей привлекательности такого перехода придется согласиться с тем, что адекватной

модели получить и в этом случае не удастся, что предполагает использование на отдельных этапах алгоритма решения эвристических процедур.

Домен персонал обобщает оперативную информацию, связанную с профессиональной деятельностью специалистов, обеспечивающих транспортную безопасность. Здесь выделяется часть угроз безопасности, исходящая от несанкционированных действий авиаспециалиста в рамках выполнения стандартных эксплуатационных процедур. Решение проблем внутри этого домена связано с идентификацией угроз персонала, их формализацией и моделированием, распределением угроз по топологии объекта защиты и масштабированием, что дает в качестве результата динамические параметры угроз для формирования коэффициентов в дифференциальных уравнениях в частных производных.

Домен ошибки детализирует домен персонал, выделяя из него те угрозы, которые связаны с ошибками персонала. Здесь формируются алгоритмы управления безопасностью, парирующие ошибки персонала.

Доменный уровень можно рассматривать как некоторую предметную область, в которой сосредоточены важные теоретические положения, определяющие научную основу информационного управления безопасностью. Доменная структура предполагает разновекторную функциональную направленность, которая комплексируется при переходе к информационно-управляющему пространству.

Последующая структуризация информационно-управляющего пространства связана с кластеризацией, т.е. на следующем уровне доменное представление структуры заменяется кластерным. Кластеры формируются внутри доменов, при этом теряется векторная направленность информационных массивов и повышается эффективность управляющих алгоритмов. Кластеры связаны с физическим смыслом обрабатываемой информации, формируются вне границ доменов, но должны удовлетворять методологическим и технологическим требованиям критериев обработки, т.е. системным и ситуационным критериям.

Группа системных кластеров объединяет методы и алгоритмы обработки информационных массивов, группа ситуационных кластеров включает в свой состав оценочные процедуры и алгоритмы. Например, домен угроз включает как минимум два кластера – моделирования угроз и оценки угроз. Кластер моделирования угроз включает модели и результаты моделирования угроз безопасности объекта транспортной инфраструктуры. Здесь решается задача оптимизации управления безопасностью по критерию угроз. Кластер моделирования уязвимостей решает аналогичные задачи применительно к понятию уязвимость. Кластер моделирования персонала транспортной безопасности исследует негативное влияние персонала ТБ на процедуры управления безопасностью с целью их оптимизации по критерию персонал.

Кластер эксперимент включает программно-технические решения, разработанные для практической реализации методологии информационного управления безопасностью.

В каждом кластере концентрируется информация, необходимая для управления безопасностью по направлению, образуя при этом пересекающиеся множества данных. Анализ информационного массива состоит из двух частей: системный и ситуационный анализ. Системный анализ включает все, что относится к системотехническому управлению и обеспечивает управление структурами и элементами, реализуя их перестройку.

Ситуационный анализ состоит в исследовании параметров процесса управления и обеспечивает реакцию системы на неблагоприятные внешние воздействия в направлении защиты объекта.

Ситуация исследуется с точки зрения противодействия опасностям, после чего реализуется режим обеспечения безопасности за счет активизации соответствующих элементов структуры системы защиты. Структура ИУП включает определенные направления деятельности, соответствующие типам управления безопасностью и критериям оценки этой деятельности.

В зоне безопасности аэропорта присутствуют три материальных кластера: субъект противоправной деятельности (СППД), система защиты аэропорта и аэропорт как физически реализованный объект. Материальность здесь следует понимать в прямой постановке, т.е. каждый из кластеров реализуется в форме физического объекта. В результате противостояния этих кластеров образуется пространство безопасности аэропорта.

Обеспечение этого пространства осуществляется путем анализа параметров кластеров и оценки результатов противостояния. Оценка может быть положительной, если АНВ не состоялся и цели АНВ не достигнуты, и отрицательной, если АНВ реализован и имеет место факт сбоя в системе защиты аэропорта. В любом случае результат может быть исследован, и могут быть разработаны соответствующие мероприятия, но только после совершения АНВ.

Вместе с тем, эти же кластеры можно представить, как не материальные объекты: пространство угроз, пространство защиты, пространство безопасности объекта, которое возникает как результат гипотетического взаимодействия указанных выше пространств.

Формально анализ приводится к исследованию линейной матрицы, где столбцы ассоциируются с направлениями (виды деятельности), а строки с критериями (угрозы, уязвимость и т.д.).

Промежуточный результат анализа состоит в получении количественных значений параметров управления безопасностью, а конечный результат представляет собой оценку качества выполнения управленческих операций (или эффективности управления).

Таким образом, структура информационно-управляющего пространства представлена на трех уровнях. Доменный уровень отражает основные направления и функциональные границы информационных массивов, однородных по смысловому содержанию. Кластерный уровень формирует предметные области математического моделирования, однородные с точки зрения методологии и различающиеся по функциональным признакам. Матричная структура относится к

функциональному уровню и включает структурированную совокупность процедурных решений по управлению транспортной безопасностью аэропорта.

По каждому факту принятия решения по управлению принимается соответствующая комплексная оценка, при этом возможны два вида: оперативная и стратегическая. Оценка формируется на основе теории векторной оптимизации и принятия решений, поскольку от единственного критерия оптимизации переходят к вектору критериев [17].

3.4. Иерархия моделей эксплуатации информационно-управляющего пространства

Информационно-управляющее пространство (ИУП) в той или иной форме отображает адекватную модель управления транспортной безопасностью объекта защиты. Форма модели определяется свойством дуальности ИУП, т.е. модель или соответствует некоторым виртуальным представлениям реальных процессов, или представляет собой некоторую функциональную структуру из элементов пространства и связей между ними.

Алгоритм реализации ИУП состоит из следующих этапов:

- ЛИНГВИСТИЧЕСКАЯ МОДЕЛЬ,
- ВИРТУАЛЬНАЯ МОДЕЛЬ,
- СТРУКТУРНО-ЛОГИЧЕСКАЯ МОДЕЛЬ,
- ФУНКЦИОНАЛЬНАЯ МОДЕЛЬ,
- МОДЕЛЬ УГРОЗ ПЕРСОНАЛА БЕЗОПАСНОСТИ,
- ИСПОЛНИТЕЛЬНАЯ СИСТЕМА.

Лингвистическая модель

Лингвистическая модель представляет собой умозрительное представление на текущий момент времени о ИУП, составленное в описательной форме. Модель рассмотрена в предыдущих разделах и включает следующие элементы:

- обеспечение безопасности,

- гомеостаз безопасности,
- управление безопасностью,
- угрозы безопасности,
- уязвимость объекта безопасности,
- персонал транспортной безопасности,
- риск как мера опасности,
- информационное управление безопасностью,
- интеллектуальное сопровождение и технологии,
- краевые задачи теории поля,
- нейронные сети.

Указанные элементы в совокупности с их параметрами и связями между ними дают исходное представление об информационно-управляющем пространстве.

Виртуальная модель

Виртуальная модель с функциональной точки зрения рассмотрена в предыдущих разделах и представлена на рисунке 3.10.

Виртуальная модель отражает целевой функционал информационно-управляющего пространства. С одной стороны, здесь сосредоточены информационные массивы, соответствующие различным аспектам безопасности, с другой – различные аспекты идеологии, теории, методологии и технологий, предназначенные для обработки этой информации на основе системного и ситуативного анализа.

Рисунок 3.10 – Виртуальная модель информационно-управляющего пространства

Виртуальная модель отображает воображаемое (мысленное) представление разработчика о функциях информационно-управляющего пространства. Конечная цель для разработчика состоит в создании реально действующей системы ИУП, отрабатывающей свой целевой функционал по управлению транспортной безопасностью.

Структурно-логическая модель

Структурно-логическая модель представляет собой важнейший этап перехода от умозрительных представлений об ИУП к реально действующей системе (Рисунок 3.11).

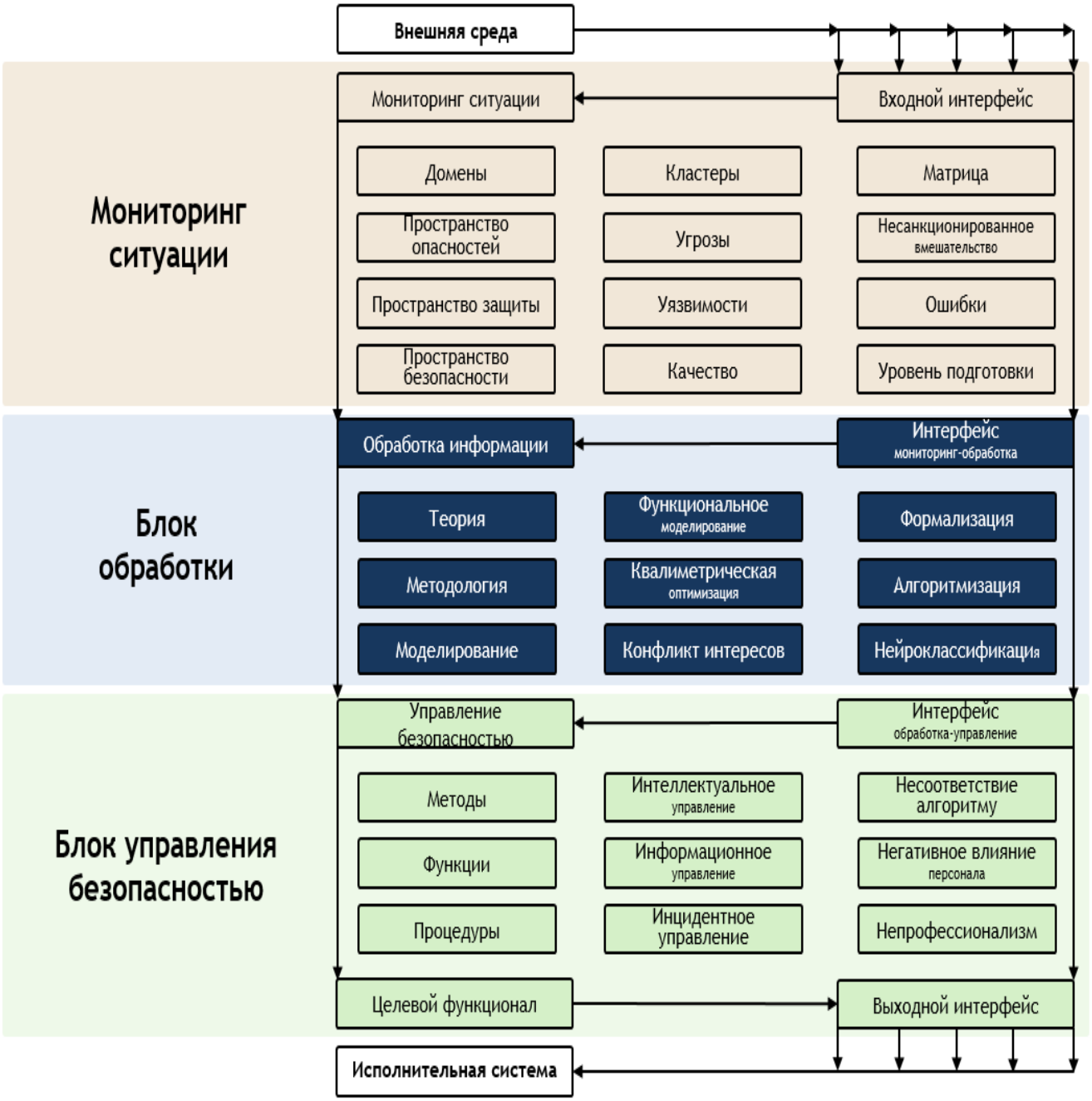


Рисунок 3.11 – Структурно-логическая модель информационно-управляющего пространства

Модель имеет блочную структуру: мониторинг ситуации, обработка информации, управление безопасностью и блок целевого функционала. По входу система связана с внешней средой через соответствующий входной интерфейс, который должен обеспечить: по входу, работу с большими объемами информации, а по выходу первичную структуризацию этой информации в соответствии с принятыми критериями структуризации – домены, кластеры, матрица. По выходу ИУП через выходной интерфейс связано с исполнительной системой.

В блоке «мониторинг ситуации» формируются локальные массивы информации, отражающие соответствующие пространства, критерии и их параметры, отдельные процедуры. Интерфейс блока обеспечивает переход к обработке информации.

Блок обработки включает элементы теории, методологию и модели обработки информации в целях управления безопасностью, методы, алгоритмы и процедуры этой обработки. Фактически в блоке решается важнейшая задача управления безопасностью, а именно: формализация и разработка алгоритмов обработки больших объемов информации. Интерфейс адаптирует результаты решения к процедурам управления.

Блок управления безопасностью объединяет методы, функции и процедуры в различных режимах информационного управления, включая интеллектуальное, информационное и инцидентное, с учетом соответствующих негативных воздействий. Выходной интерфейс обеспечивает адаптивный переход к исполнительной системе.

Исполнительная система включает средства обеспечения управляющих сигналов.

Функциональная модель (фрагмент)

Функциональная модель включает множество локальных моделей, отображающих отдельные функции системы управления безопасностью по направлениям деятельности.

На рисунке 3.12, как один из возможных вариантов, представлена локальная функциональная модель процесса обработки единичной ошибки.

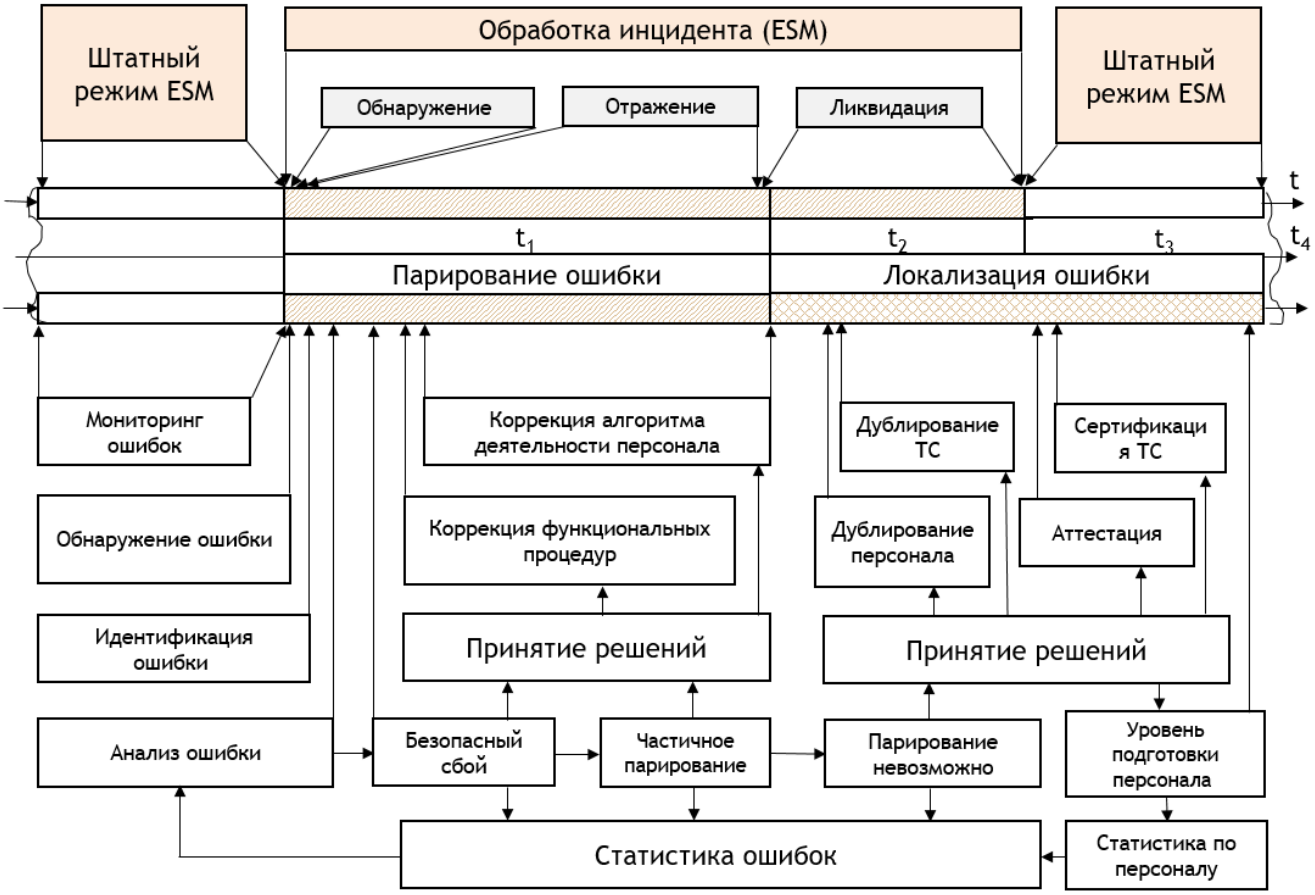


Рисунок 3.12 – Функциональная модель процесса обработки единичной ошибки

Таким образом, реализуется постепенный переход к реальной компьютерной системе, отрабатывающей управляющие сигналы. Тем самым решается одна из проблем, отмеченная как научная задача диссертационной работы: разработка методологии формализации и алгоритмизации информационных массивов управления транспортной безопасностью.

При переходе и использовании функциональной модели следует иметь в виду, что субъект противоправной деятельности (СППД) включает представительную совокупность угроз, имеющих различную физическую природу, существенную неопределенность в описании характеристических и целевых

функций и, как результат, характеризуется непреодолимыми трудностями математической формализации.

3.5 Методы снижения негативного влияния персонала на транспортную безопасность аэропорта

Угрозы со стороны персонала, осуществляющего профессиональную деятельность по обеспечению транспортной безопасности, рассматриваются в составе общей совокупности угроз безопасности аэропорта, как один из типов угроз. В действительности это не совсем так. Внешние угрозы и их типы определяются моделью нарушителя. На основе этой модели для каждого типа угрозы разработаны соответствующие меры противодействия, включая деятельность персонала и совокупность соответствующих технических средств защиты объекта. Угрозы персонала рассматриваются как некоторый побочный результат профессиональной деятельности специалиста по обеспечению транспортной безопасности. Это означает, что выделить отдельную угрозу или как-то их классифицировать невозможно в принципе. По этой же причине нельзя исследовать угрозы персонала как потенциальные, т.е. нельзя для каждой угрозы заранее разработать аппарат противодействия. В этом главная трудность исследования угроз персонала, которая препятствует использованию математических моделей и других классических методов исследования.

Объекты исследования необходимо разделить на материальные и нематериальные. Здесь имеется в виду, что в зоне безопасности аэропорта присутствуют материальные кластеры: СППД, система защиты и аэропорт как физический объект. В результате их противостояния образуется пространство безопасности аэропорта. Обеспечение этого пространства на данном этапе осуществляется путем анализа параметров кластеров и оценки результатов противостояния. Оценка может быть положительной, если АНВ не состоялся и цели АНВ не достигнуты, и отрицательной, если АНВ реализован и имеет место

факт сбоя в системе защиты аэропорта. В любом случае результат может быть исследован и разработаны соответствующие мероприятия только после совершения АНВ.

Такое разделение вызвано тем, что методы снижения негативного влияния персонала (вмешательства) существенно отличаются и требуют различных методологических подходов. В первом случае предполагается мониторинг отклонений от алгоритма профессиональной деятельности и инструментальная коррекция этого алгоритма, во втором реализуется функция управления персоналом транспортной безопасности, основанная на мониторинге и оценки качества профессиональной готовности персонала к выполнению своих служебных функций и управлении персоналом на основе принятия соответствующих решений.

Одним из важнейших факторов транспортной безопасности остается человеческий фактор (ЧФ), поскольку авиационная транспортная система рассматривается как эргатическая, причем человеческая составляющая системы проявляется в производственной деятельности всех элементов транспортной системы.

Негативные последствия проявления человеческого фактора приводят к тому, что ситуация становится слабоуправляемой. Безопасность объекта зависит от конкретных исполнителей, которые получают реальный рычаг управления ситуацией. Наиболее эффективной будет система, предоставляющая всю необходимую информацию оперативно и без искажений. Отсюда задача – свести влияние человеческого фактора до минимума.

Следует признать, что ни одна система безопасности (СБ) не застрахована от влияния человеческого фактора полностью. Но современная СБ должна сводить это влияние к минимуму. Отсюда возникает некоторое противоречие между «человеческим фактором» и проблемой формирования и использования в реальной обстановке комплекса технических средств. Авторский взгляд на эту проблему отражен в работе [118].

Одной из важнейших характеристик авиационного персонала, связанной со спецификой его профессиональной деятельности, является ответственность, в том числе ответственность за принимаемые решения. Отсюда вытекает понятие надежности авиационного персонала, которое в значительной степени определяется понятием ошибка. Понятие «ошибка» в деятельности человека-оператора или в работе технического устройства соотносится с понятием «погрешность». В реальном процессе управления невозможно абсолютно точно выдерживать заданные значения регулируемых параметров. Задавая оператору программное значение регулируемого параметра, одновременно указывают и допустимые отклонения от него. Любые отклонения регулируемых оператором параметров, находящиеся в пределах дозволенного «коридора», называются погрешностью управления. Когда человек-оператор допускает отклонение значений этих параметров за пределы установленных ограничений, подобные события квалифицируются как ошибки в работе человека. Ошибка человека-оператора – это такое его действие или бездействие, которое привело к отклонению управляемых параметров системы за допустимые пределы или запрещено правилами. Отказ человека-оператора можно трактовать как переход его в такое состояние, при котором становится невозможным его дальнейшее нормальное функционирование или привели к такому отклонению управляемых параметров за установленные пределы, что управляемая система перестала выполнять возложенные на нее функции [52; 118].

Надежность человека-оператора определяется его способностью в течение заданного интервала времени в предусмотренных условиях сохранять нормальное состояние жизнедеятельности и выдерживать технические параметры управляемой системы в установленных пределах, а также выполнять все возложенные на него функции по поддержанию заданного режима работы управляемой техники. Анализ надежности персонала (АНП) предназначен для качественной и количественной оценки надежности. Объектом анализа является надежность выполнения определенных функций персонала (ФП) во взаимодействии с комплексом

технических средств. Причиной невыполнения или неправильного выполнения ФП являются ошибки или ошибочные действия. Надежность персонала может оцениваться качественно или количественно. Качественный анализ надежности персонала (АНП) проводится с целью определения логико-временной структуры алгоритма выполнения каждой функции персонала в конкретных условиях его профессиональной деятельности и последствий возможных ошибочных действий персонала. Цель – выявление всех важных для оценки надежности персонала факторов деятельности (ФД) [52; 118].

Количественный анализ надежности персонала проводится для вычисления численных значений ее показателей. В качестве основного показателя надежности обычно выбирают вероятность безошибочного выполнения функции оператором (персоналом) или вероятность ошибки персонала (ВОП). Вероятность безошибочного выполнения функции может оцениваться на уровне отдельной операции или в целом, на уровне функции. Если обозначить через p_i вероятность безошибочного выполнения *i*-ой операции, то в предположении, что все операции, входящие в соответствующую функцию, производятся последовательно, легко вычислить вероятность *P* безошибочной реализации функции [118]:

$$P = \prod_{i=1}^{n} p_i, i = \overline{1,n}, \tag{3.18}$$

где n -число операций.

Для расчета вероятности безошибочного выполнения операции или ВОП используются два основных метода: статистический и экспертный.

Статистический метод заключается в исследовании деятельности оператора и фиксации общего числа M_i операций *i*-го вида и допущенных при этом ошибок m_i. Тогда точечная оценка вероятности безошибочного выполнения *i*-ой операции вычисляется по формуле [118]

$$\hat{p}_i = \left(M_i - m_i\right) / M_i .$$

Эта формула справедлива при условии, что при проведении одной операции возможна только одна ошибка оператора. Точечная оценка вероятности ошибки персонала q_i при выполнении *i*-ой операции вычисляется по формуле [118]

$$\hat{q}_i = 1 - p_i = m_i / M_i . \tag{3.19}$$

В случае, когда m_i =0, т.е. за время наблюдений ошибка персонала по *i*-ой операции не зафиксирована, вычисляется нижняя доверительная граница для вероятности безошибочного выполнения *i*-ой операции при доверительной вероятности γ:

$$\underline{p}_i = (1-\gamma)^{1/M_i} . \tag{3.20}$$

Одним из важнейших понятий, связанных с проблемой обеспечения безопасности, а, следовательно, однозначно связанным с деятельностью персонала, является понятие риска. Риск представляет собой оценочную возможность возникновения неблагоприятных последствий в результате действия фактора опасности. Это вероятность того, что потенциальные возможности опасного фактора причинить вред, реализуются. Оценка риска предполагает учет вероятности, так и степени тяжести любых неблагоприятных последствий; иными словами, определяется потенциальный ущерб. При проведении оценки риска важно проводить различие между опасными факторами (возможности причинения вреда) и риском (вероятность причинения этого вреда в течение определенного периода времени) [118].

Наиболее общим и универсальным методом расчета критериального значения риска [*S*] является подход, основанный на экономическом анализе безопасности [118]. Согласно этому методу критерием оптимума уровня безопасности служит минимум величины *Z*, представляющей собой сумму двух составляющих: *X*(*r*) приведенных расходов на обеспечение безопасности, характеризуемой риском *r*, и *Y*(*r*) – прямого ущерба, обусловленного риском *r*:

$$r_{opt} = \arg\min_r Z(r) = \arg\min_r [X(r) + Y(r)]. \tag{3.21}$$

Значение r_{opt} может быть принято в качестве критериального значения $[S]$. Здесь достаточно важна величина Y как функция риска r. При относительно малых рисках для многих опасных объектов считается справедливой линейная зависимость [118]:

$$Y(r) = \alpha r, \tag{3.22}$$

где α – цена риска.

Задача масштабирования угроз персонала имеет значение для формирования процедур управления несанкционированным вмешательством в обеспечение транспортной безопасности и снижения уровня негативного влияния персонала в области безопасности аэропорта, поскольку управление осуществляется по критерию угроз. Имея в виду, что совокупность угроз персонала по своему составу весьма неоднородна и зависит от функционала конкретного специалиста, значимость каждой угрозы необходимо взвесить и отразить в количественном эквиваленте. В таком случае необходимо иметь некоторое распределение угроз по топологии аэропорта, что связано с топологией рабочих мест персонала транспортной безопасности. Здесь возникает вопрос о моделировании этой совокупности угроз.

Каждый из кластеров отображается соответствующей моделью: модель системы обеспечения ТБ, модель персонала ТБ, модель нарушителя (СППД). В процессе противостояния СППД и системы защиты появляется негативное воздействие персонала, которое добавляется к совокупности угроз СППД. В таком случае, появляется необходимость коррекции системы защиты с тем, чтобы ее новое качество гарантировало защиту объекта в новой ситуации. Здесь качество выступает как величина, обратная уязвимости объекта защиты. Отсюда вытекает задача масштабирования негативного влияния персонала для особо важных элементов (точек) объекта защиты.

Выберем на топологии объекта защиты две точки. Предположим, что в некоторой точке проявляется угроза со стороны персонала, которая возникает при

выполнении процедур противостояния угрозе СППД в системе защиты объекта в случае несанкционированного вмешательства персонала (ошибки).

Реализация угрозы снижает качество системы защиты и повышает уязвимость объекта защиты. Тогда коррекция системы защиты в сторону повышения ее качества с целью компенсации негативного воздействия персонала будет зависеть только от уязвимости элемента (точки) объекта.

Реализация угрозы СППД, даже если она точечная, далеко не всегда ограничивается точечным влиянием (последствиями). Если рассматривать вторую точку в связи с угрозой в первой, можно сказать, что в этой точке появляется угроза как некоторая часть угрозы в первой точке. Аналогично для всех других точек по топологии объекта защиты. Поскольку задача вычисления уязвимости решается экспертными методами и не является точной, для перехода к качеству системы защиты достаточно иметь некоторое распределение угроз СППД. Распределение угроз в количественном формате позволяет перейти к количественному распределению уязвимостей по элементам объекта защиты, рассматривая их как требования к системе защиты. Все это дает исходную информация для формирования эвристической модели негативного влияния персонала ТБ, где главная цель получить количественные значения коэффициентов масштабирования.

Персонал обладает определенными характеристиками, позволяющими ему успешно выполнить свои процедуры, однако, уровень его профессиональной готовности далеко не всегда соответствует требованиям, которые заложены в СЭП и отражаются параметрами СЭП. Возникает конфликт интересов, который, по своей сути, и есть несанкционированное вмешательство [118].

3.6 Ситуационная модель управления несанкционированным вмешательством персонала

Проблема синтеза систем управления сложными объектами достаточно сложна и многогранна. С одной стороны, сложные системы не могут иметь адекватного математического описания, и любая попытка создать его обречена на извечный компромисс с ограничениями, приближениями и оценкой степени соответствия реальному объекту. С другой стороны, вполне естественно стремление использовать формальные методы для управления сложными системами. Поэтому при синтезе процесса управления сложной системой неизбежно использование неформальных методов, например, экспертных. Сочетание формальных и неформальных методов и является той спецификой управления сложными объектами, к которым относится авиационный персонал в гражданской авиации (Рисунок 3.13) [118].

Ситуационная оценка основана на системотехническом подходе, который предполагает исследование системы «авиационный персонал» как сложной системы, т.е. на основе оценки ее состояния. Поскольку оценка состояния системы «авиационный персонал» используется как параметр управления, ставится задача оптимизации. Тогда необходимо определиться с критериями оптимизации, в качестве которых предлагаются факторы «риск», «конфликтность» и «компетентность» (Рисунок 3.14, 3.15).

Исследование авиационного персонала как сложной системы предполагает отсутствие возможностей создания абсолютно надежной системы, т.е. существует вероятность возникновения опасных ошибок в служебной деятельности. В таком случае правомерным является использование вероятностного подхода для исследования ситуационной модели [26].

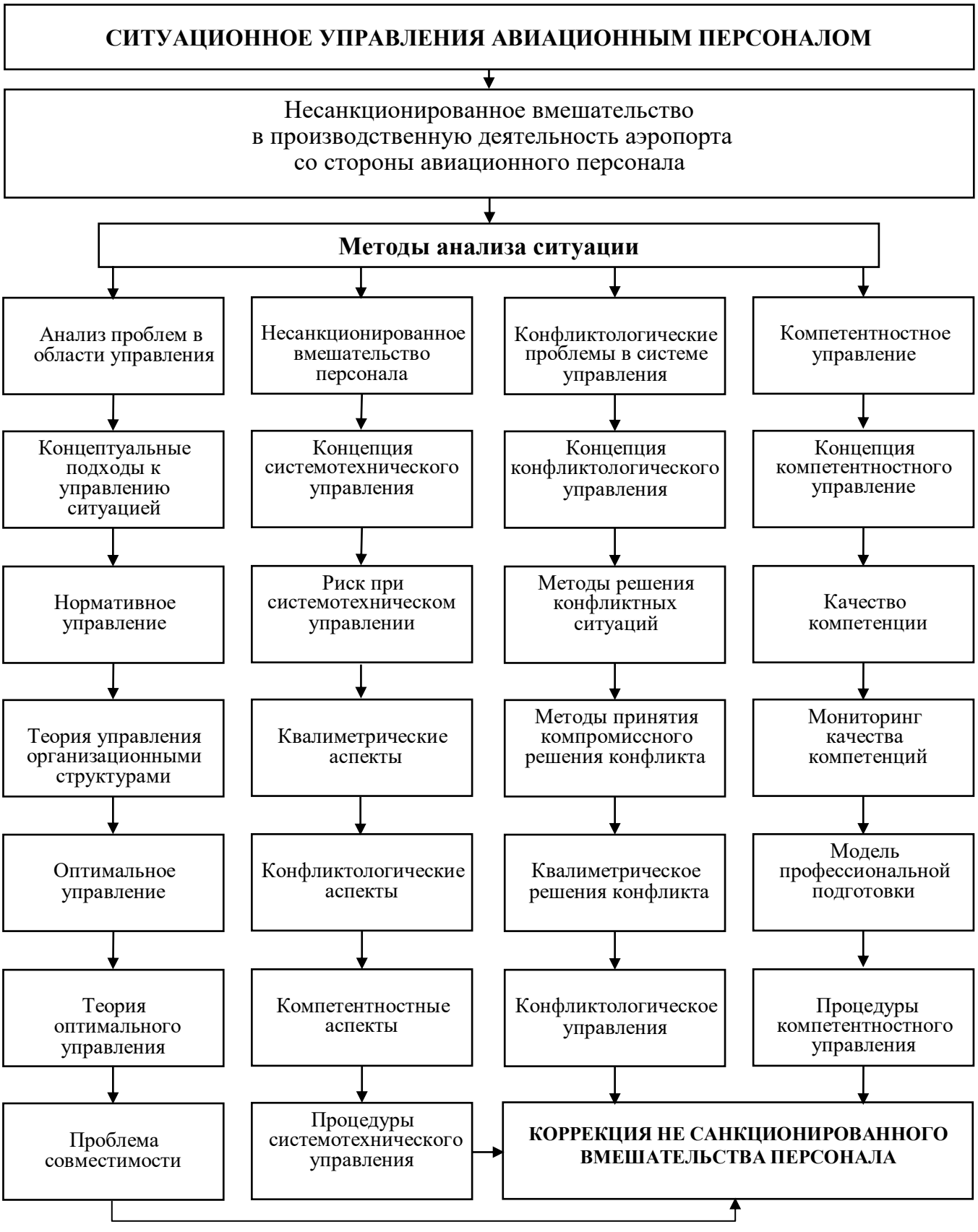


Рисунок 3.13 – Ситуационное управление персоналом (несанкционированное вмешательство)

Вероятностные аспекты связаны с получением количественных значений методами теории вероятностей. Вероятностные аспекты достаточно хорошо разработаны в приложении к безопасности полетов и практически не исследованы в области транспортной безопасности [118].

Безопасность периода продолжительностью *t* часов может характеризоваться вероятностью его благополучного завершения $P_{бп}(t)$ и вероятностью авиационного происшествия $P_{ап}(t)$. Используя теорему полной вероятности, можно записать [118]:

$$P_{бп}(t) + P_{ап}(t) = 1. \qquad (3.23)$$

Выражение является основным уравнением теории безопасности, показатель $P_{ап}$ принято называть еще уровнем риска.

Пусть δ – требуемая точность оценки; β – доверительная вероятность того, что при заданном объеме выборки *n* оценка $\hat{a}$ будет иметь точность δ в пределах доверительного интервала $(\hat{a}-\delta;\hat{a}+\delta)$. Величина β (доверительной вероятности) определяется конкретными условиями задачи и обычно выбирается близкой к единице (0,95; 0,99; 0,999).

При этих условиях математическая статистика позволяет, задаваясь значениями любых двух величин из δ, β, *n*, найти значение третьей величины. Однако для этого нужно знать закон распределения случайной величины (оценки) $\hat{a}$, который в общем случае зависит от тех же неизвестных параметров. При практическом решении задачи иногда удается перейти от $\hat{a}$ к таким функциям выборочных значений, закон распределения которых зависит только от объема выборки *n* и закона распределения случайной величины *X* и не зависит от неизвестных параметров. В частности, это справедливо для выборки объема *n*, произведенной из Гауссовской генеральной совокупности с параметрами m_x и σ_x^2. Возможные методы решения указанных выше задач хорошо представлены в литературе [89; 171; 183].

Несмещенной называют оценку $\hat{a}$, математическое ожидание которой равно оцениваемому параметру *a* при любом числе наблюдений, то есть $M[\hat{a}] = a$.

Эффективной называют оценку, которая (при данном объеме выборки) имеет возможно наименьшую дисперсию, то есть $D[\hat{a}] = \min$.

Состоятельной называется оценка, дисперсия которой стремится к нулю с увеличением числа опытов, то есть $\lim_{n\to\infty} D[\hat{a}] = 0$.

Несмещенная и состоятельная оценка $\hat{a}$ сходится по вероятности к оцениваемому параметру, то есть $\lim_{n\to\infty} P(/\hat{a} - a/ \prec \varepsilon) \le 1$,

где ε – сколь угодно малая величина.

В ряде случаев задача по определению неизвестных параметров распределения решается точечной статистической оценкой.

Точечной называют оценку, которая определяется одним числом. Пусть имеется случайная величина *X* с математическим ожиданием m_x и дисперсией d_x, оба параметры неизвестны. Производится *n* независимых опытов, давших результаты *x1, x2,…xn* . Требуется найти «хорошие» оценки для параметров m_x и d_x .

В этом случае в качестве оценки математического ожидания принимается его среднее арифметическое значение, определяемое:

$$\hat{m}_x = \frac{1}{n}\sum_{i=1}^{n} x_i \,. \tag{3.24}$$

Оценка дисперсии производится по формуле:

$$\hat{d}_x = \frac{n}{n-1}\,\frac{\sum_{i=1}^{n}(x_i - m_x)^2}{n} \,. \tag{3.25}$$

Доверительная вероятность – это вероятность того, что истинное значение параметра *a* будет внутри доверительного интервала. Доверительная вероятность характеризует достоверность оценки, ее надежность [118].

Ситуационная модель отображает количественные оценки качества уровня профессиональной подготовки, включая совокупность факторов, определяемых риском, конфликтом и компетентностью.

3.7 Конфликт интересов в системе управления безопасностью

Конфликт представляет собой некоторое явление, ситуацию, отражающую взаимодействие двух или более сторон, характеризуемую несовпадающими интересами этих сторон. Конфликт лежит в основе всей предметной области, называемой транспортная безопасность гражданской авиации, и отражает противостояние внешних и внутренних угроз безопасности объекта защиты и системы защиты. Поскольку в основе практически всех процессов противостояния угроз безопасности и системы защиты находится персонал, можно утверждать, что конфликт интересов в транспортной безопасности определяется конфликтом между представителями персонала, т.е. несанкционированное вмешательство персонала транспортной безопасности в процедуры обеспечения последней, основано на конфликте. Значимость конфликта для процессов, включающих это явление, определяется уровнем противоборства, степенью противостояния сторон. Решение конфликта представляется как процедура снижения степени противостояния, в идеале до минимальных значений. Отсюда, снижение негативного влияния персонала транспортной безопасности в значительной степени есть решение конфликта (Рисунок 3.14).

Рисунок 3.14 – Функциональная модель минимизации несанкционированного вмешательства персонала

В данной модели субъект противоправной деятельности включает в себя все источники угроз, определенных известным приказом Росавиации, которые как внешние угрозы воздействую на объект защиты. Обеспечение транспортной безопасности осуществляет технологическая платформа ESM через свои функциональные подсистемы. При появлении угрозы формируется инцидент, который обрабатывается по определенному алгоритму, зависящему от типа угрозы. Для реализации алгоритма формируется концептуальная модель деятельности, в результате чего угроза парируется. При выполнении процедур реализации алгоритма обработки инцидента персонал транспортной безопасности должен действовать в каждом конкретном случае в соответствии со стандартной эксплуатационной процедурой. Любые отклонения от стандарта являются угрозой персонала и называются несанкционированным вмешательством, которое проявляется как отклонение реального алгоритма деятельности персонала от

стандартной эксплуатационной процедуры. Такие отклонения можно квалифицировать как ошибку. Функциональные подсистемы ESM осуществляют мониторинг ошибок, идентификацию, локализацию и анализ ошибок, задачей которого является парирование ошибок.

Таким образом, конфликт в системе управления безопасностью, связанный с несанкционированным вмешательством персонала, возникает между стандартной эксплуатационной процедурой и реальным алгоритмом профессиональной деятельности персонала.

Любой конфликт носит ситуативный характер, т.е. определяет только текущую ситуацию. Решение конфликта, которое понимается как снижение уровня противостояния сторон конфликта, представляет собой результат ситуативного анализа процедур, выполняемых персоналом, процедур, заданных в СЭП, и отклонений, которые проявляются как ошибки персонала. Эти результаты отражаются в модели конфликта и определяют процедуры коррекции характеристик персонала и параметров СЭП, что обеспечивает снижение уровня негативного влияния персонала транспортной безопасности.

Ключевым элементом здесь является модель конфликта. Процесс формирования модели конфликта представляет собой достаточно сложную процедуру, если принять во внимание сложность описания самого конфликта. Формализация конфликта в полном объеме практически невозможна из-за высокой степени неопределенности параметров конфликта, значительным уровнем принимаемых допущений и ограничений, поэтому здесь возможен достаточно ограниченный набор типов моделей.

Главная цель моделирования состоит в определении стратегий решения конфликта:

$$W_1 \rightarrow \max_{X_1} \min_{X_2} F_1(X_1X_2)$$

$$W_2 \rightarrow \max_{X_2} \min_{X_1} F_2(X_1X_2)$$

$$X_1X_2\,(\max W_1) \leftrightarrow X_1X_2\,(\min W_2) \qquad (3.26)$$

$$X_1X_2\ (max\ W_2) \leftrightarrow X_1X_2\ (min\ W_1) \qquad (3.27)$$

$$W_1 \rightarrow \max_{x_1 \ldots x_n} F_1\ (X_1, X_2 \ldots X_n)$$

$$W_2 \rightarrow \max_{x_1 \ldots x_n} F_2\ (X_1, X_2 \ldots X_n)$$

$$X_1, X_2 \ldots X_n\ (min\ W_i) \longleftrightarrow X_1, X_2 \ldots X_n\ (max\ W_j)$$

$$X_1, X_2 \ldots X_n\ (max\ W_i) \longleftrightarrow X_1, X_2 \ldots X_n\ (min\ W_j)$$

$$\overline{i = 1,n};\ \overline{j = 1,n};\ i \neq j.$$

Понятно, что и здесь формализация достаточно условна. Таким образом, приемлемого варианта математического моделирования конфликта не существует. Скорее следует искать какие-то эвристические модели или решать отдельные частные, локальные задачи с последующим комплексированием результатов.

Схема ситуационной оценки конфликта в безопасности выглядит следующим образом (Рисунок 3.15) [118]. В основе схемы лежит эвристическая процедура оценки качества компромиссного решения конфликта. В результате выполнения процедуры решается задача параметрического снижения уровня противоречий, зафиксированных при описании конфликта. Процедура реализуется ЛПР соответствующего уровня иерархии и ответственного за анализ конфликтных ситуаций.

Процедура состоит в последовательном и совместном рассмотрении требований сторон конфликта и принудительном удовлетворении этих требований в пределах полномочий ЛПР, т.е. получении компромиссного решения конфликта.

Решение считается удовлетворительным, если качество компромиссного решения, вычисляемое квалиметрическими методами, совпадает с нормативным значением качества, в противном случае принимается решение по управлению персоналом, т.е. разрабатывается и реализуется система административных мер, направленных на ликвидацию конфликта [118].

Математическим аппаратом исследования конфликтов является теория игр [80], которая позволяет структурировать задачу и получить формальное

представление о конфликте в форме стохастических моделей, определить стратегии достижения соглашения, определить соответствующие количественные зависимости.

Рисунок 3.15 – Ситуационная оценка конфликта

Можно получить аналитическое выражение конфликта, например, в следующей форме [118]:

$$\frac{dx}{dt} = x(t) = f(t, x, (t), \quad \int_{-\infty}^{t} x(s-\tau) d_s G_1(s,t,\tau), \ldots$$
$$\ldots, \int_{-\infty}^{t} x(s-\tau) d_s G_r(s,t,\tau)) + u(t, \tau_u), \tag{3.28}$$

где G_i – известные функции; τ – распределенное отклонение аргумента; $u \subset U$ – управление с отклонением аргумента τ_u; U – область возможных управлений. Если память ограничена некоторым интервалом $t-t_1$, то нижний предел интервалов $-t_1$.

Вопрос об использовании аналитического метода решения конфликта в системе управления безопасностью остается открытым, поскольку сложности формализованного решения, вытекающие из высокой степени недостоверности описательных характеристик конфликта, заставляют думать о других методах решения. Решения уравнения конфликта в классическом понимании не существует – решение принимается.

Выводы к главе 3

1. Разработана концепция информационного управления транспортной безопасностью, основанная на методах системотехники, теории оптимального управления, теории краевых задач и квалиметрии, системообразующем понятием которой является понятие «информационно–управляющее пространство», рассматриваемое как некоторый интерфейс между противоборствующими пространствами (угроз и защиты) и решающее задачи по формированию адекватной модели управления транспортной безопасностью.

2. Главная проблема в развитии современных систем управления транспортной безопасностью состоит в том, что в них реализуется концепция

обеспечения транспортной безопасности, а управление присутствует в формате нормативного, т.е. в рамках теории организационных систем. Реализация оптимального управления, в рамках соответствующей теории вызывает проблемы в связи с трудностями формализации.

3. Проблема оптимальности в управлении транспортной безопасностью состоит в том, что современные компьютерные системы предлагают широкие возможности для решения практических задач за счет внедрения эффективных технологий типа BID DATA, DATA MINING, PSIM и т.д., использование которых предполагает развитую систему постановки задач, включающую адаптивный математический аппарат и определенную совокупность адекватных моделей, чего в области транспортной безопасности сегодня нет.

4. Предлагается оптимальное управление транспортной безопасностью формировать на основе доменной структуры информационно-управляющего пространства и выстраивать с учетом уровня развития соответствующих компьютерных технологий.

5. Доменная структура информационно-управляющего пространства основана на следующих понятиях: теория безопасности, гипотетическое поле безопасности, формализация, автоматизация, гармонизация процедур обеспечения и управления, методология, векторное пересечение доменов, функциональный уровень, угрозы, уязвимость, персонал, ошибки, интеллектуальный анализ информации. Информационно-управляющее пространство представляет собой некоторую предметную область, в которой сосредоточены, в том числе, важные теоретические положения, определяющие научную основу информационного управления безопасностью.

6. Структура информационно-управляющего пространства представлена на трех уровнях: доменный, который отражает основные направления и функциональные границы информационных массивов, однородных по смысловому содержанию; кластерный уровень формирует предметные области математического моделирования, однородные с точки зрения методологии и

различающиеся по функциональным признакам; функциональный уровень (матричная структура) включает структурированную совокупность процедурных решений по управлению транспортной безопасностью.

7. Процедуры оптимизации организационного управления информационно-управляющим пространством в качестве критериев оптимизации включают: угрозы безопасности объекта защиты, уязвимость объекта защиты, авиационный персонал, рассматриваемый с точки зрения его негативного вмешательства в процедуры управления.

8. Оптимизация управления транспортной безопасностью с учетом фактора несанкционированного вмешательства персонала в процедуры управления решается путем перехода от уязвимости объекта защиты к качеству системы защиты, численного моделирования пространства защиты и масштабирования результатов моделирования в терминах качества, что формирует требования к системе защиты критических элементов.

9. Алгоритм формирования структуры информационно-управляющего пространства включает несколько принципиально важных комплексных этапов: разработка лингвистической модели ИУП, разработка виртуальной модели ИУП, разработка структурно-логической модели ИУП, разработка функциональных моделей системы мониторинга и системы обработки данных, разработка системной модели формализации и алгоритмизации процессов безопасности, разработка ситуативной модели управления транспортной безопасностью.

ГЛАВА 4 МОДЕЛИРОВАНИЕ И ОПТИМИЗАЦИЯ ПРОСТРАНСТВА БЕЗОПАСНОСТИ АЭРОПОРТА

4.1 Уязвимость объекта транспортной инфраструктуры как критерий оптимизации информационного управления безопасностью

Обеспечение и управление транспортной безопасностью как процесс предполагает результат в достижение приемлемого уровня этой безопасности. Объект транспортной инфраструктуры (ОТИ) находится под воздействием некоторой совокупности угроз его безопасности, защиту от которых осуществляет система обеспечения безопасности (Рисунок 4.1). В какой степени система защиты готова обеспечить приемлемый уровень безопасности можно оценить с помощью некоторого параметра (критерия), в качестве которого предложена уязвимость, отражающая степень удовлетворения требований к объекту защиты по безопасности. Для практических целей уязвимость должна найти свое отображение в количественном эквиваленте, для чего нужна некоторая модель уязвимости.

Модель уязвимости напрямую связана как с процессом моделирования угроз безопасности, так и с процедурами формирования системы обеспечения безопасности. Совокупность угроз безопасности ОТИ в некотором смысле является гипотетической, поскольку для формирования системы защиты необходимо учитывать потенциальные угрозы с целью их предотвращения. Угрозы могут быть учтены в модели уязвимости, для чего формируются названные модели [131].

Как уже было отмечено, переход от угроз безопасности к уязвимости как критерию безопасности достаточно сложен. Алгоритм такого перехода заложен в модели уязвимости.

Выступая в качестве критерия оптимального управления безопасностью аэропорта, уязвимость включает такие понятия как качество и риск.

Рисунок 4.1 – Оптимальность управления по критерию уязвимость

Понятие качество отражает степень соответствия результатов деятельности системы защиты аэропорта установленным требованиям, т.е. соответствие достигнутого и установленного уровня безопасности аэропорта. Понятие риск учитывает уровень возможного ущерба в результате воздействия соответствующей угрозы. Эти критерии включены в модель уязвимости аэропорта (Рисунок 4.2).

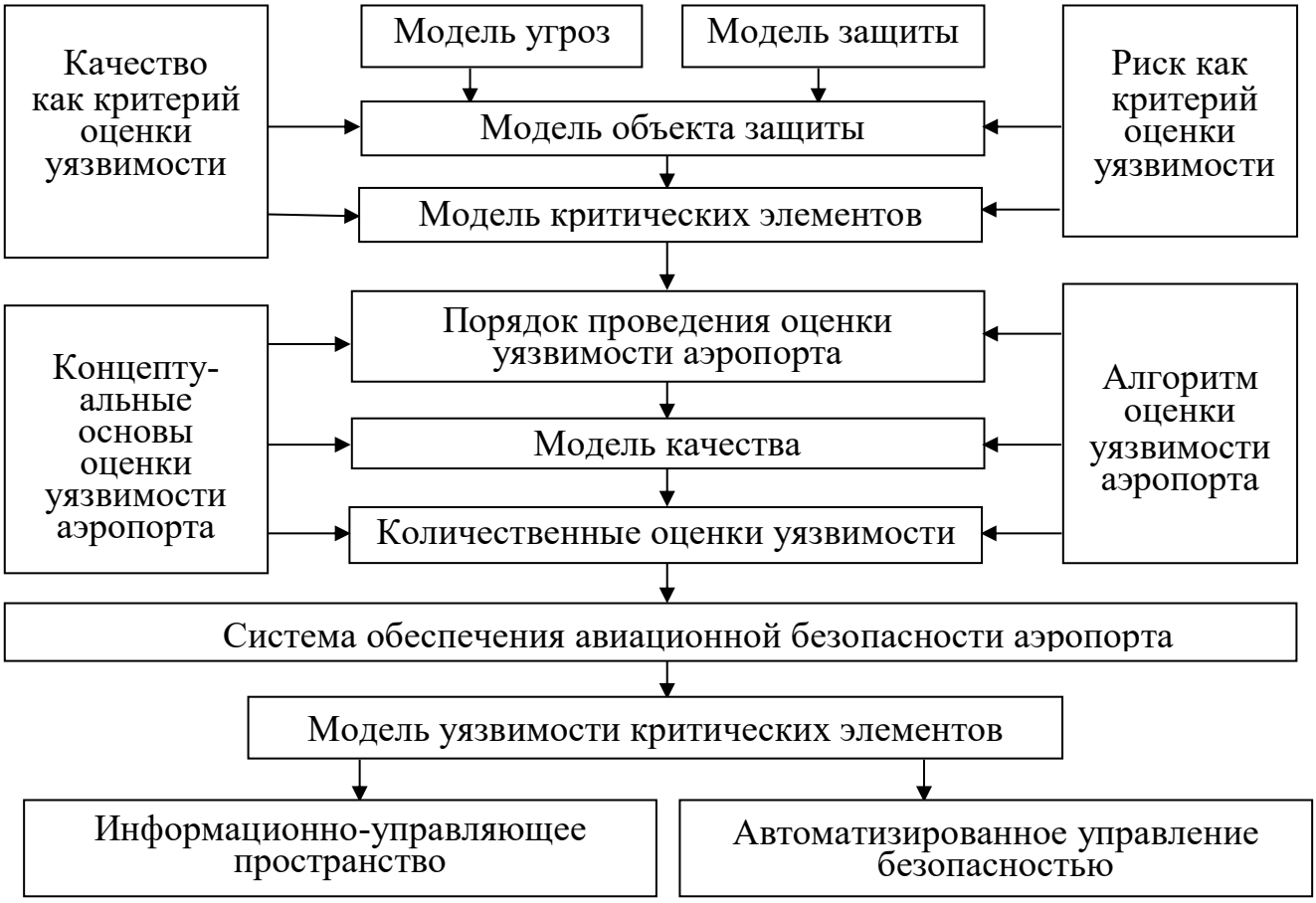


Рисунок 4.2 – Модель уязвимости аэропорта

Автором разработан [118] и успешно эксплуатируется квалиметрический алгоритм оценки уязвимости (Рисунок 4.3). В основе алгоритма лежат квалиметрические процедуры. Алгоритм предусматривает оценку качества (уязвимости) объекта с учётом соответствующих рисков возникновения событий несанкционированного вмешательства в его деятельность.

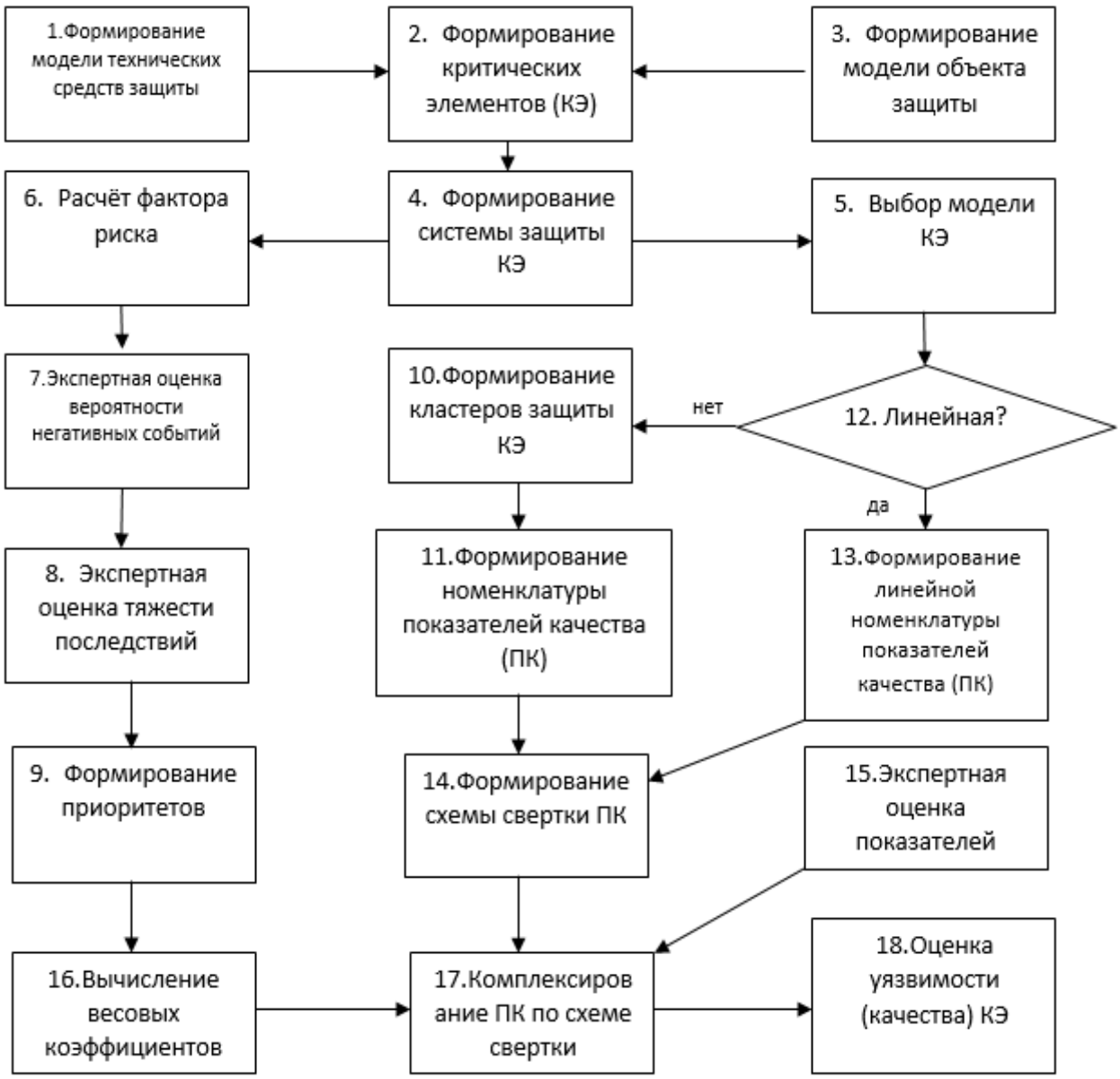


Рисунок 4.3 – Квалиметрический алгоритм оценки уязвимости

Исходными данными для реализации процедуры оценки уязвимости являются модели объекта защиты (3) и технических средств защиты (1), а также система требований к ним. Это является необходимым и достаточным для формирования перечня критических элементов и привязки их к элементам структуры аэропорта. В отношении каждого критического элемента формируется система его защиты (4). Для каждого КЭ выбирается соответствующая модель (5).

Если модель линейная (12), формируется линейная номенклатура показателей качества (13), если нет (12), формируются кластеры технических средств защиты соответствующих критических элементов аэропорта.

Количественное значение ПК вписываются в схему свертки, после чего осуществляется комплексирование показателей (17) результат которого даёт количественное значение оценки уязвимости (качества защиты) аэропорта (18).

Качество можно рассматривать как степень защищенности объекта (аэропорта) от несанкционированного вмешательства в его деятельность, включая АНВ. В таком случае уровень качества всей совокупности средств защиты аэропорта определяет степень его защищенности от угрозы совершения АНВ. Тогда уровень качества (его оценка) и есть оценка уязвимости, что соответствует принятым определениям [131].

Транспортная безопасность связана с динамическими характеристиками и параметрами угроз и предполагает адекватную реакцию системы защиты на эти угрозы путем управления структурой, характеристиками и параметрами системы обеспечения транспортной безопасности. Уязвимость определяет степень защищенности объекта транспортной инфраструктуры и технических средств от угроз несанкционированного вмешательства в их деятельность, что дает возможность управлять уровнем транспортной безопасности.

Практическое моделирование указанных моделей (Рисунок 4.2), включая модель уязвимости, предполагает достаточно обоснованный выбор методов моделирования. Строгий анализ здесь не имеет смысла, поскольку при весьма обширном количестве таких методов необходимо учитывать серьезную неопределенность в постановке задач моделирования, что заставляет применять метод к конкретным параметрам описания задачи. С другой стороны, необходимо отразить соответствующую специфику известных методов, прежде всего численных методов для дифференциальных уравнений в частных производных.

Достаточно часто при исследовании угроз безопасности применяют сеточное моделирование, в том числе с формализацией в виде дифференциальных уравнений

в частных производных. Решение в этом случае может быть получено численными методами, например, методом Зейделя. Здесь каждой узловой точке сеточной области соответствует элемент двумерного массива с индексами, равными координатам узла. В каждой итерации происходит последовательный обход узлов. Для текущего узла происходит расчет уточненного приближения [38]:

$$U(i,j)=\frac{1}{Ax(i,j)+Ax(i-1,j)+Ay(i,j)+Ay(i,j-1)}\Big[Ax(i,j)\cdot U(i+1,j)+ \\ Ax(i-1,j)\cdot U(i-1,j)+Ay(i,j)\cdot U(i,j+1)+Ay(i,j-1)\cdot U(i,j-1)+f(i,j)\Big]. \quad (4.1)$$

При расчете по формуле (4.1) используются уже обновленные в данной итерации приближения в соседних узлах. Полученное приближение записывается на место старого значения. Процесс заканчивается, когда норма относительного изменения решения (норма поправки) будет достаточно малой

$$\frac{\left\|\mathbf{U}^{(k)}-\mathbf{U}^{(k-1)}\right\|}{\left\|\mathbf{U}^{(k)}\right\|}\le\varepsilon,$$

где $\mathbf{U}^{(k)}$ и $\mathbf{U}^{(k-1)}$ – векторы решений на k-ой и $(k-1)$-ой итерациях, ε – заданное малое положительное число (допустимая погрешность).

Процесс распространения угрозы для распределенных объектов рассматривается как процесс диффузии. Тогда математической моделью распространения угрозы будет уравнение диффузии (4.2), частный вид дифференциального уравнения в частных производных [38; 123]:

$$\frac{\partial}{\partial x}\left(\sigma(x,y)\frac{\partial u}{\partial x}\right)+\frac{\partial}{\partial y}\left(\sigma(x,y)\frac{\partial u}{\partial y}\right)=f(x,y),\quad (x,y)\in D, \quad (4.2)$$

где u – уровень угрозы, $\sigma(x,y)$ – проницаемость угрозы, $f(x,y)$ – плотность распределения источников опасности.

Введем понятия "проницаемость среды" и "плотность распределения источников угроз". Проницаемость среды характеризует некое препятствие среды распространению угроз [38]. Причем положительное значение плотности распределения источников угроз характеризует угрозы безопасности, а

отрицательное – источники активного противодействия угрозам. Будем считать, что плотность источников угроз носят относительный характер, определенный по некоторой шкале угроз. Привязка этих значений к конкретным угрозам представляет самостоятельную задачу.

Уравнение диффузии является далеко не единственным, которое может быть выбрано в качестве модели, существует достаточно представительная линейка дифференциальных уравнений в частных производных, из которой может быть осуществлен выбор. Характер уравнения определяется порядком частных производных, числом независимых переменных, линейностью, видами коэффициентов уравнения, стационарностью. Прогнозируемым вариантом является модель, включающая несколько типов уравнений, тогда прямое математическое моделирование невозможно и предлагается использовать физическое моделирование на основе гибридных сеточных моделей, которые представляют собой аналого-цифровой вычислительный комплекс (АЦВК) класса сетка-ЦВМ, сочетающий аналоговые возможности моделирующей сетки и цифровые преимущества компьютерной обработки информации.

Оценка уязвимости, путем реализации соответствующих методов и процедур, представляет собой оценку соответствия между требованиями по безопасности к объекту защиты и параметрами защиты.

В общем случае моделирующий алгоритм может быть записан с помощью операторных уравнений вида:

$$\boldsymbol{Z_i(t) = \varphi_i\{t, t_0, z_i(t), (t, X_{Li}]_{t0}^{t}\}} \quad (4.3)$$

В каждой j-ой реализации на модели i-ой подсистемы вектор-функцию $X_{Li}(t)$ выбирают из некоторого известного множества функций $L_i(t), t \in T_i$.

Основой этого метода служит преобразование Лапласа, которое связывает функцию F(s) комплексной переменной s (изображение) с соответствующей функцией f(t) действительной переменной t (оригинала):

$$\boldsymbol{F(s) = L[f(t)] = \int f(t)e^{-st}\,dt} \quad (4.4)$$

Алгоритм численного решения системы дифференциальных уравнений Колмогорова возможен с использованием методов Рунге-Кутта [172].

4.2 Моделирование пространства угроз безопасности аэропорта (стационарная задача)

Рассмотрим процесс распространения угрозы для распределенных объектов как процесс диффузии [123; 129]. Математической моделью распространения угрозы будет уравнение диффузии (4.2). Уравнение диффузии представляет собой частный вид дифференциального уравнения в частных производных. Бывает нестационарным и стационарным. Решение уравнения диффузии – это нахождение зависимости концентрации вещества (или иных объектов) от пространственных координат и времени, причем задан коэффициент (в общем случае также зависящий от пространственных координат и времени), характеризующий проницаемость среды для диффузии.

Правая часть $f(x,y)$ уравнения означает некоторые источники угрозы. На начальных этапах исследования ограничимся рассмотрением точечных источников угроз. Возможно пространственное распределение источников угроз с некоторой плотностью.

Введем понятия "проницаемость среды" и "плотность распределения источников угроз". Проницаемость среды характеризует некое препятствие среды распространению угроз. Уровень угрозы в конкретной точке пространства будет определяться расположением источника угрозы относительно этой точки, значением угрозы и проницаемостью среды для угрозы.

Уравнение решается в области D, включающей защищаемый объект и окружающую территорию. На границе области Γ должны быть заданы граничные условия:

$$u\big|_{\Gamma} = 0,$$

что означает отсутствие опасности на границе области.

Проницаемость угрозы $\sigma(x,y)$ может быть различной в области D. На защищаемой территории проницаемость должна быть существенно меньше, чем за границами защищаемой территории. Будем считать проницаемость среды и плотность распределения источников опасности экспертно определяемыми оценками.

Так как проницаемость среды различна в различных подобластях области D, то необходимо учитывать условия сопряжения сред [126]. На границе раздела сред примем условия идеального контакта: решение u потоки $\sigma(x,y)\frac{\partial u}{\partial x}$ на границе сопряжения непрерывны. Тогда обычное разностное уравнение аппроксимирует условия сопряжения с погрешностью порядка $O(h^2)$. Скачков решения на границе раздела сред в случае идеального контакта не возникает. Таким образом, моделирование угрозы в случае идеального контакта сред будем рассматривать как краевую задачу.

Если на границе контакта сред не выполнены условия идеального контакта, т.е. на границе имеются источники угроз (отрицательную угрозу можно рассматривать как фактор противодействия), то в каждом отдельном случае необходимо специально формулировать условия сопряжения. Решение задачи на границе раздела сред в этом случае будет терпеть разрыв. На данном этапе исследования будем рассматривать идеальное сопряжение сред.

Рассмотренная модель описывает стационарный (установившийся) процесс. Различные варианты предложенной модели реализованы в системе MATLAB. Разработанные варианты главной программы и функций, реализующих итерационный процесс, представлены в приложении А.

По условиям задачи моделирования одиночной опасности предполагается, что она действует на плоскости, ограниченной линией защиты. Возможен вариант, когда граница совпадает с границей критического элемента (КЭ). Результаты должны быть представлены в виде распределения по топологии объекта защиты локальных значений опасности от заданной одиночной, входной.

Задача решена в прямоугольной области, с координатами левого нижнего угла x1=0, y1=0 и правого верхнего угла x2=1 и y2=1. Программа, ее описание и числовые данные представлены в приложении А. График поверхности решения (Рисунок 4.4) показывает, что в защищаемой области с практически нулевой проницаемостью уровень опасности резко снижается, но не является нулевым.

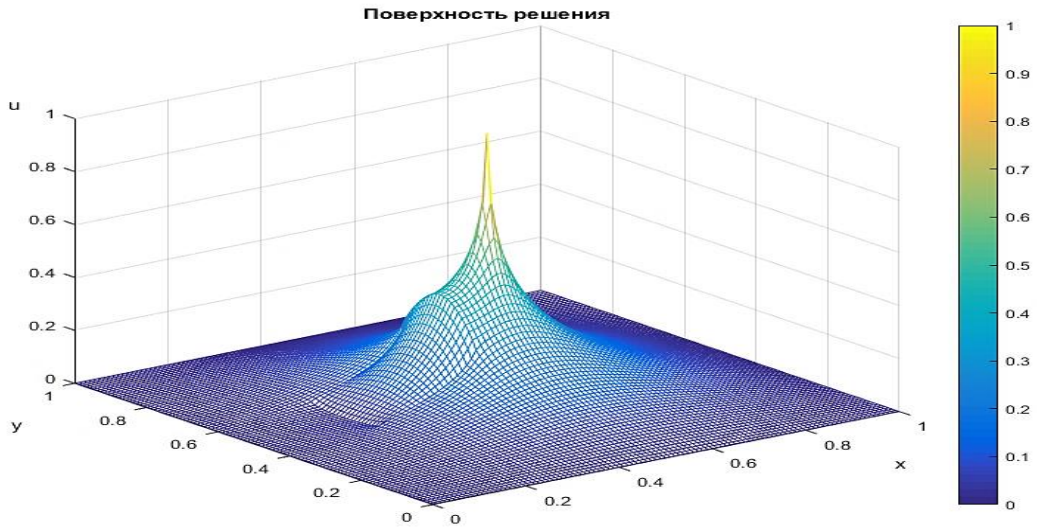


Рисунок 4.4 – К задаче с одним источником опасности.
Поверхность решения

Значения опасности следуют из графика линий уровня (Рисунок 4.5), где защищаемая область выделена прямоугольником.

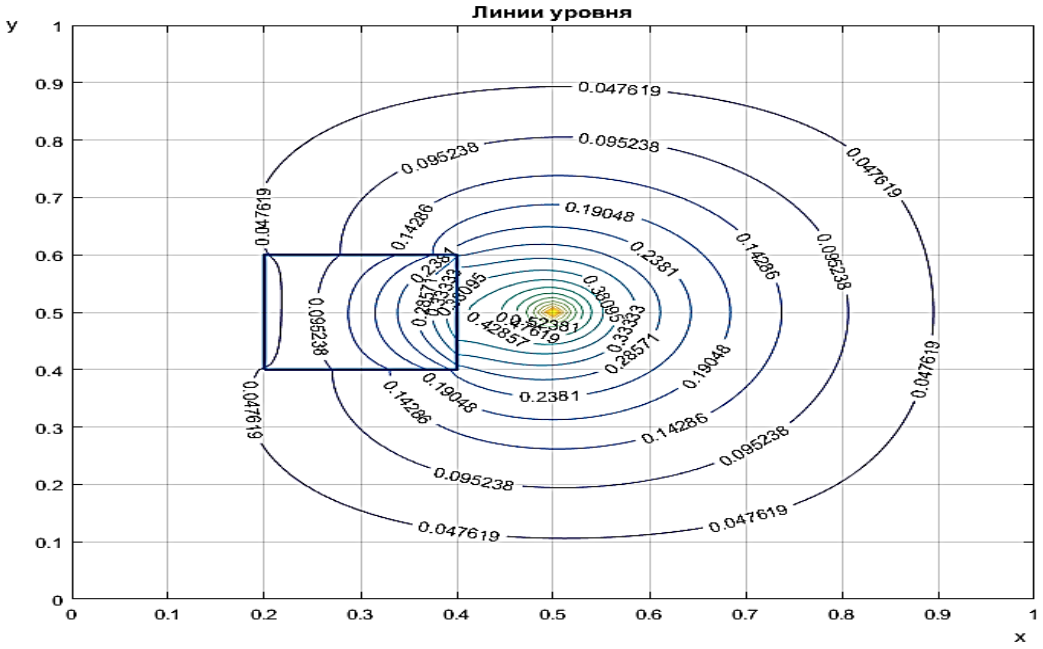


Рисунок 4.5 – К задаче с одним источником опасности. Линии уровня

Решение получено за 1979 итераций. Зависимость относительной нормы поправки от номера итерации представлена на рисунке 4.6.

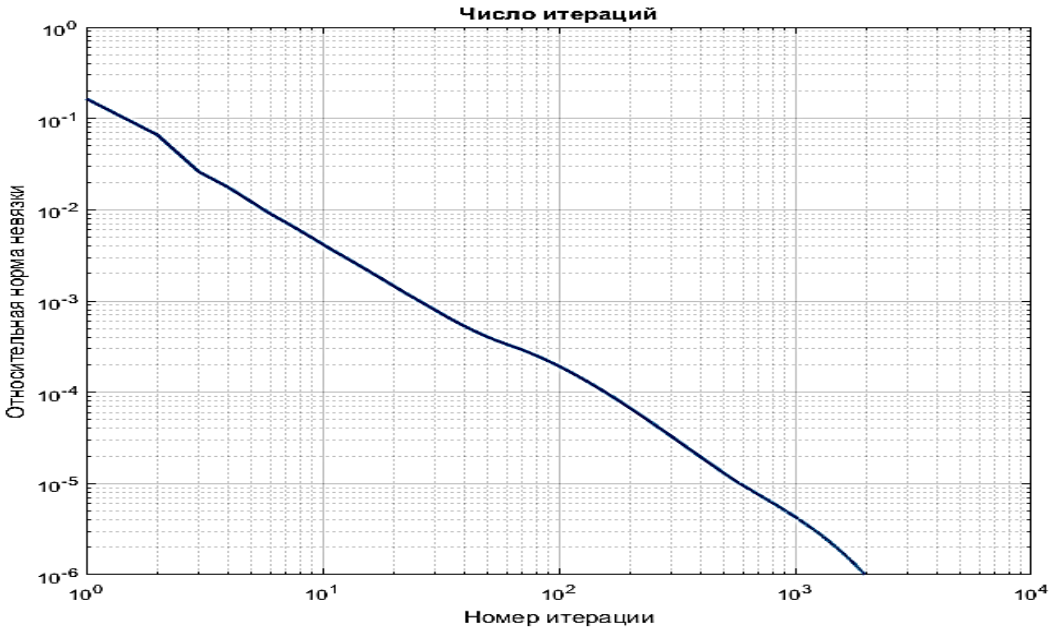


Рисунок 4.6 – К задаче с одним источником опасности. Норма поправки

Задача с одним источником опасности решалась также для случая, когда в защищаемой области появляется отрицательная проницаемость с плотностью,

равной -10, что можно трактовать как активное противодействие опасности.

График поверхности решения для проницаемости защищаемой области, равной 10, представлен на рисунке 4.7. Проницаемость защищаемой области подобрана с учетом максимального снижения уровня опасности.

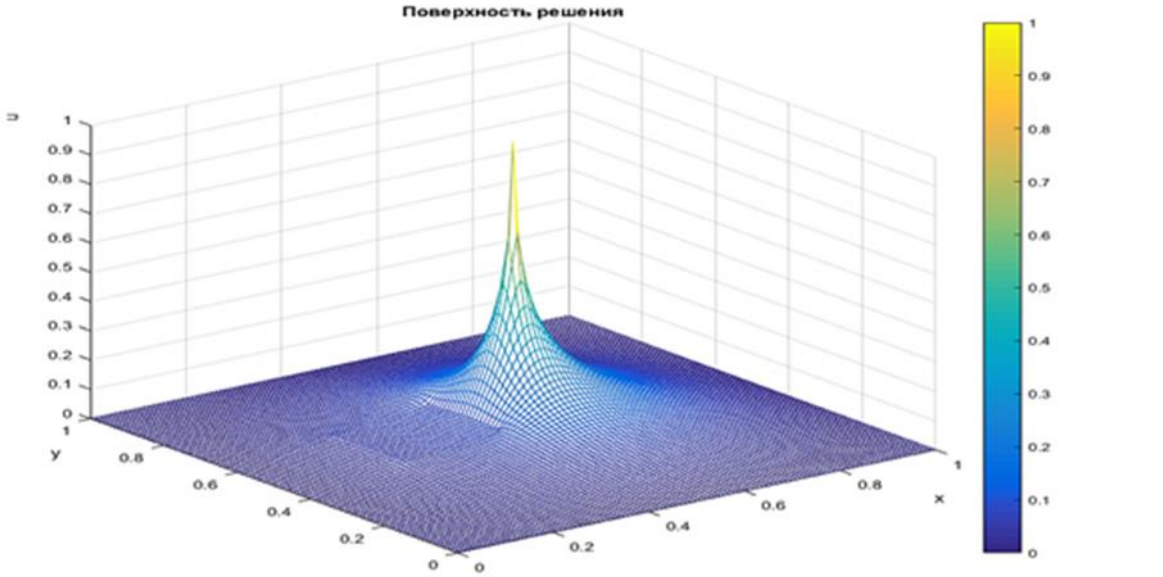


Рисунок 4.7 – К задаче с одним источником опасности и с противодействием. Поверхность решения

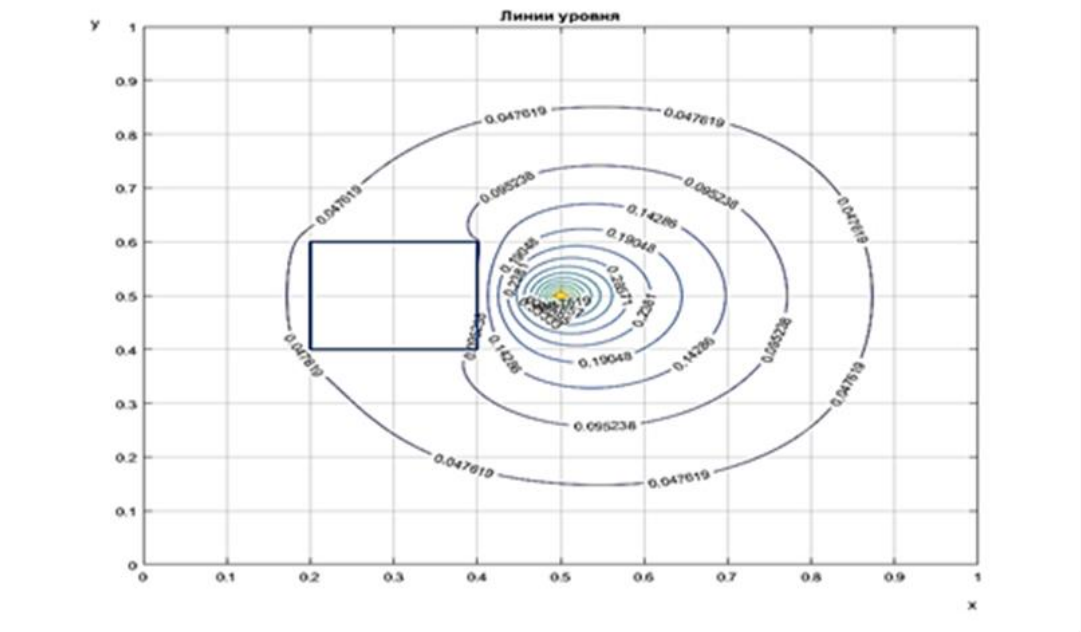


Рисунок 4.8 – К задаче с одним источником опасности и с противодействием. Линии уровня

Поверхность решения (Рисунок 4.7) и линии уровня решения (Рисунок 4.8) показывают, что для существенного снижения опасности необходимо противодействие с плотностью, значительно превышающей плотность опасности. Требуется также большая проницаемость мер противодействия в защищаемой области.

Результат моделирования опасности, распределенной в некоторой области, в виде поверхности решения представлен на рисунке 4.9.

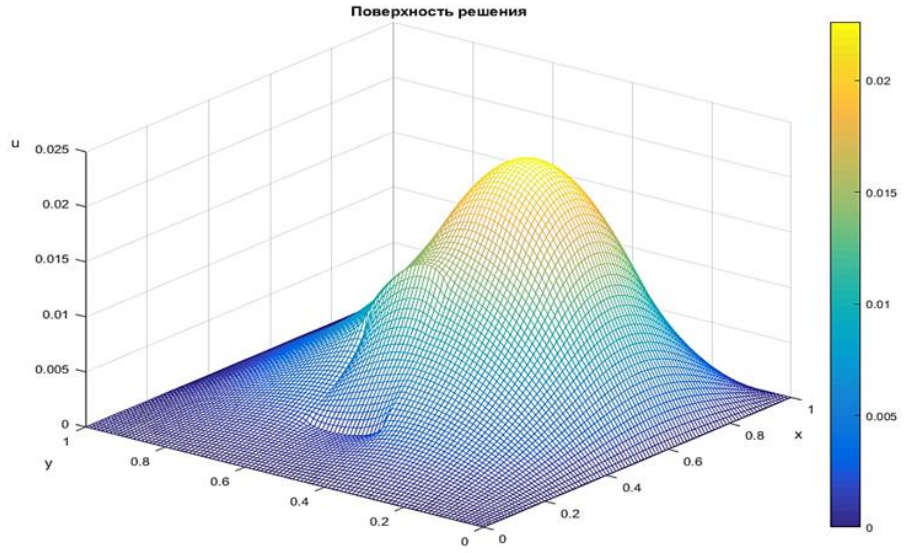


Рисунок 4.9 – К задаче с опасностью, распределенной в некоторой области. Поверхность решения

График линий уровня решения задачи с опасностью, распределенной в некоторой области представлен на рисунке 4.10.

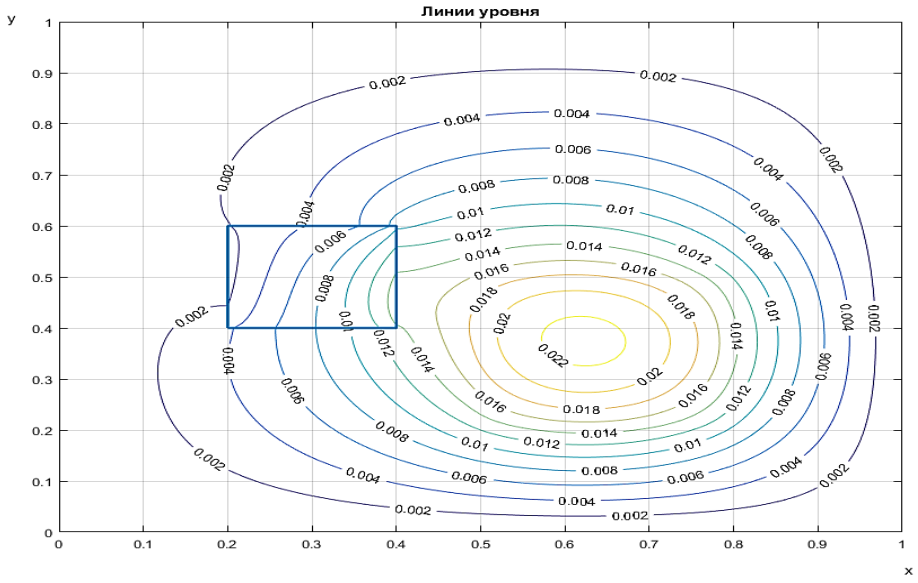


Рисунок 4.10 – К задаче с опасностью, распределенной в некоторой области. Линии уровня

Характер снижения опасности в защищаемой области близок к результату при одиночной опасности.

Решение той же задачи с плотностью противодействия, равной -1 и проницаемостью противодействия sigma1=10 показало практически полное устранение опасности (Рисунок 4.11. и Рисунок 4.12).

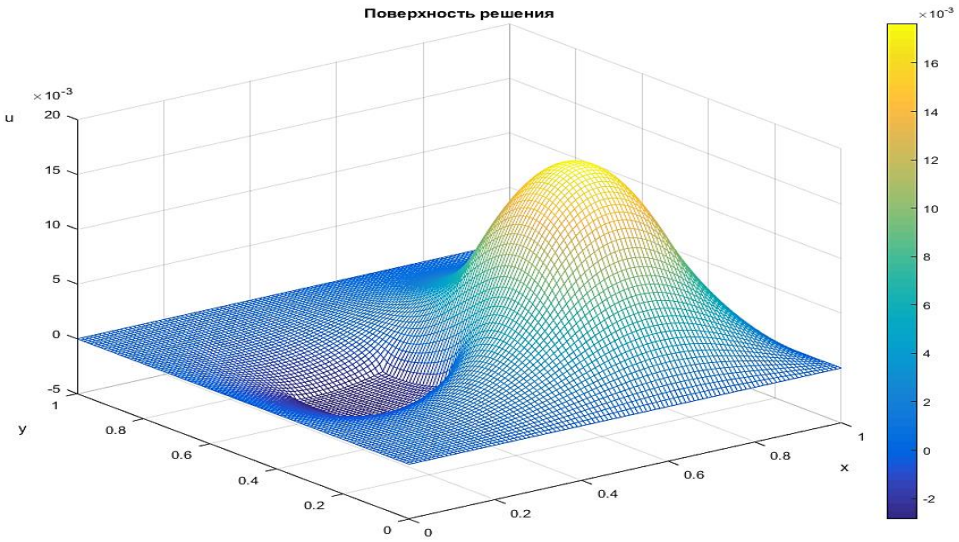


Рисунок 4.11 – К задаче с опасностью, распределенной в некоторой области, и с противодействием. Поверхность решения

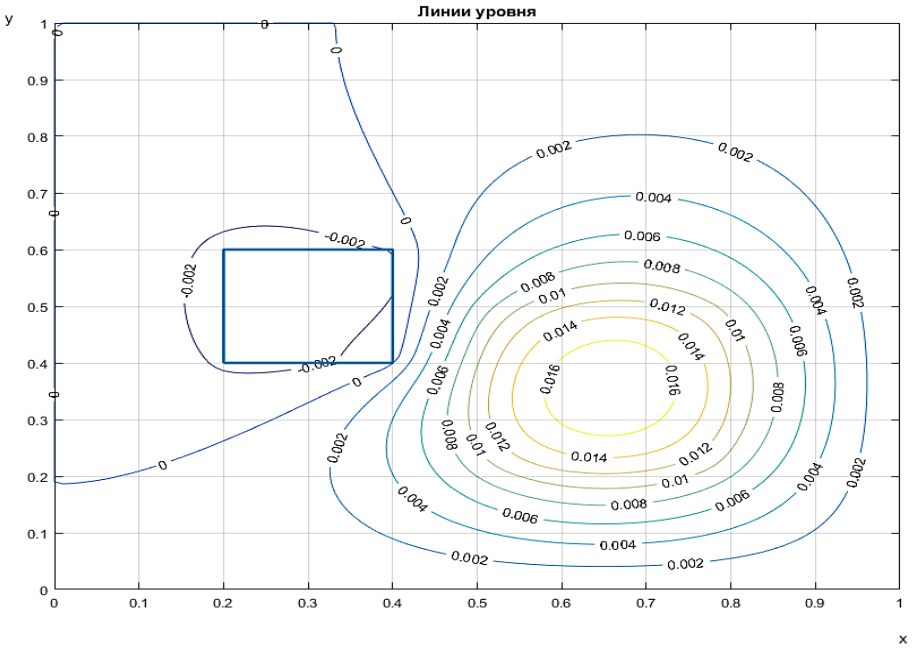


Рисунок 4.12 – К задаче с опасностью, распределенной в некоторой области, и с противодействием. Линии уровня

Моделирование опасности, распределенной во внешней области, показало небольшое снижение опасности в защищаемой области (Рисунок 4.13 и Рисунок 4.14).

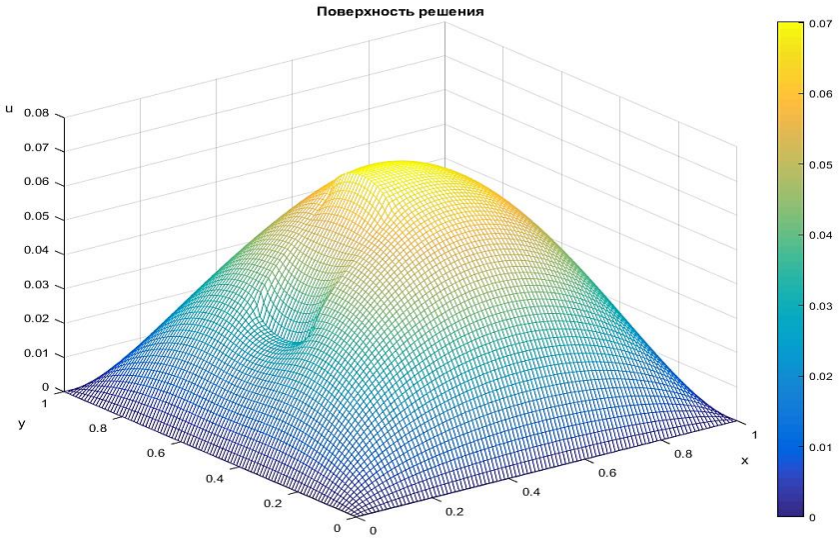


Рисунок 4.13 – График поверхности решения задачи с опасностью, распределенной во всей внешней области

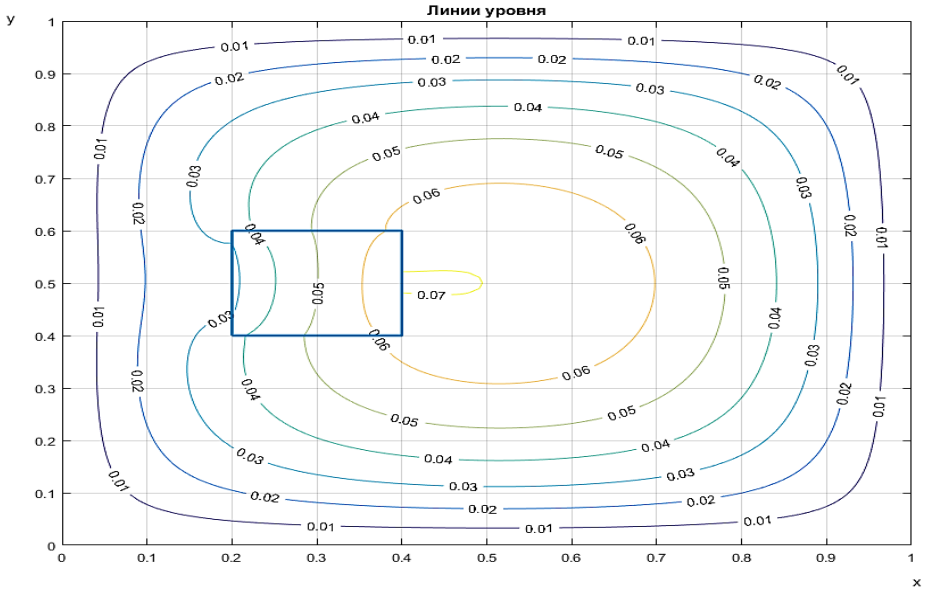


Рисунок 4.14 – К задаче с опасностью, распределенной во внешней области. Линии уровня

Применение противодействия с плотностью -10 при проницаемости защищаемой области, равной 10, позволило устранить опасность (Рисунок 4.15 и Рисунок 4.16).

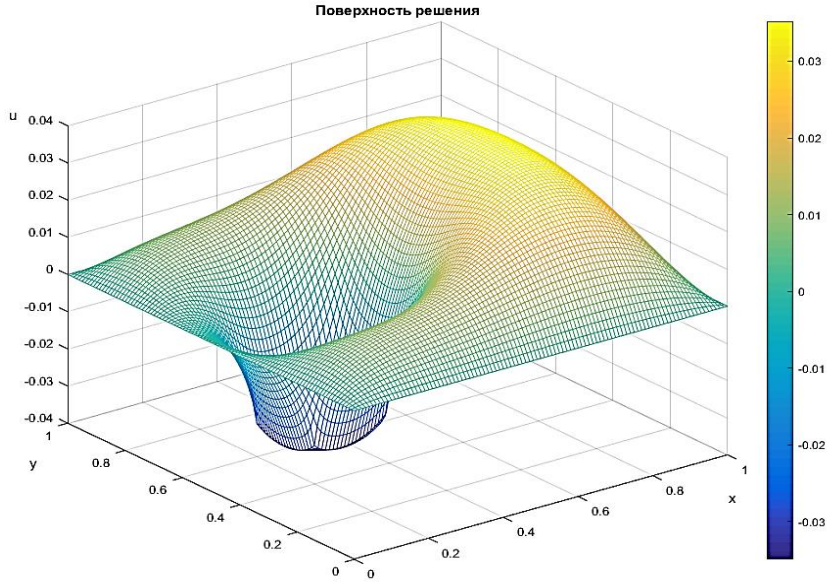


Рисунок 4.15 – К задаче с опасностью, распределенной во внешней области, и с противодействием. Поверхность решения

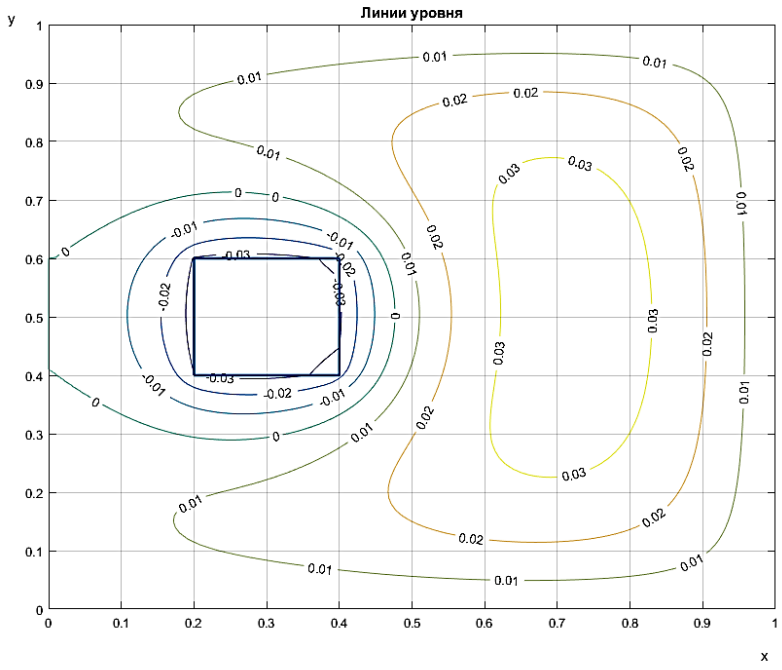


Рисунок 4.16 – К задаче с опасностью, распределенной во внешней области, и с противодействием. Линии уровня

Алгоритмы решения представленных задач, описание программных компонентов, численные значения переменных и других параметров представлены в приложении А.

Построенная математическая модель и решение ряда модельных задач показали принципиальную применимость методов моделирования объектов с распределенными параметрами для решения задач управления безопасностью. Модель позволяет на качественном уровне анализировать безопасность. Дальнейшее развитие модели заключается в привязке параметров модели к параметрам безопасности объекта.

4.3 Моделирования пространства уязвимостей аэропорта (нестационарная задача)

В нестационарном случает модель описывается уравнением параболического типа

$$\frac{\partial}{\partial x}\left(\sigma(x,y)\frac{\partial u}{\partial x}\right)+\frac{\partial}{\partial y}\left(\sigma(x,y)\frac{\partial u}{\partial y}\right)=c\frac{\partial u}{\partial t},\quad (x,y)\in D, \tag{4.5}$$

где c характеризует скорость процесса.

Кроме граничных условий задаются начальные условия

$$U(x,0)=\psi(x),\quad 0\le x\le l,\quad t=0. \tag{4.6}$$

Рассмотрим нестационарную задачу, описываемую уравнением (4.5) с граничными условиями и начальными условиями (4.6).

Введем в пространственно-временной области $0\le x\le l,\quad 0\le t\le T$ конечно-разностную сетку $\omega_{h,\tau}$

$$\omega_{h,\tau}=\left\{x_i=ih, i=\overline{0,N}; t^k=k\tau, k=\overline{0,K}\right\}, \tag{4.7}$$

с пространственным шагом $h=l/N$ и шагом по времени $\tau=T/K$.

Введем понятие временно́го слоя: нижнего временного слоя $t^k=k\tau$, на котором искомая сеточная функция $u\left(x_i,t^k\right)$ известна (при $k=0$ сеточная функция равна начальным условиям); верхнего временного слоя $t^{k+1}=(k+1)\tau$, на котором необходимо найти распределение сеточной функции. Введем также понятие шаблона конечно-разностной схемы, используя который и соответствующий метод аппроксимации по пространственным переменным, получим неявную конечно-разностную схему [23; 38]

$$-\left[\frac{\sigma(x_i+h/2,y_j)}{h^2}+\frac{\sigma(x_i-h/2,y_j)}{h^2}+\frac{\sigma(x_i,y_j+h/2)}{h^2}+\frac{\sigma(x_i,y_j-h/2)}{h^2}\right]u_{ij}^{k+1}+$$

$$+\frac{\sigma(x_i+h/2,y_j)}{h^2}u_{i+1,j}^{k+1}+\frac{\sigma(x_i-h/2,y_j)}{h^2}u_{i-1,j}^{k+1}+\frac{\sigma(x_i,y_j+h/2)}{h^2}u_{i,j+1}^{k+1}+$$

$$+\frac{\sigma(x_i, y_j - h/2)}{h^2} u_{i,j-1}^{k+1} = c\frac{u_{ij}^{k+1} - u_{ij}^{k}}{\tau}, \quad (x_i, y_i) \in S_h, \tag{4.8}$$

или

$$-\left[\frac{\sigma(x_i + h/2, y_j)}{h^2} + \frac{\sigma(x_i - h/2, y_j)}{h^2} + \frac{\sigma(x_i, y_j + h/2)}{h^2} + \frac{\sigma(x_i, y_j - h/2)}{h^2} + \frac{c}{\tau}\right] u_{ij}^{k+1} +$$

$$+\frac{\sigma(x_i + h/2, y_j)}{h^2} u_{i+1,j}^{k+1} + \frac{\sigma(x_i - h/2, y_j)}{h^2} u_{i-1,j}^{k+1} + \frac{\sigma(x_i, y_j + h/2)}{h^2} u_{i,j+1}^{k+1} +$$

$$+\frac{\sigma(x_i, y_j - h/2)}{h^2} u_{i,j-1}^{k+1} = -\frac{c}{\tau} u_{ij}^{k}, \quad (x_i, y_i) \in S_h. \tag{4.9}$$

Будем считать, что граничные условия не зависят от времени. Аппроксимация начальных условий имеет вид

$$u_i^0 = \psi(x_i), \quad i = \overline{0, N}. \tag{4.10}$$

Разностная схема (4.9), (4.10) аппроксимирует дифференциальную задачу со вторым порядком точности по пространственной переменной и первым порядком точности по временной переменной. Неявная схема является абсолютно устойчивой. В неявной схеме сеточную функцию u_i^{k+1} на верхнем временном слое приходится находить, решая систему линейных алгебраических уравнений. Решение находится последовательно по слоям: на основе начальных условий находится решение на первом слое, используя решение на первом слое, находится решение на втором слое и т.д.

Задача решена в системе MATLAB с использованием программ sec_4 с вызовом функций fdm_3. Указанные функции, разработанные программы, алгоритмы, используемые при решении задачи, а также количественные значения исходных данных и параметров представлены в приложении Б.

Моделируемая функция представляет собой уязвимость объекта транспортной инфраструктуры, вычисленная для отдельных критических элементов. Распределение уязвимостей по топологии исследуемого объекта необходимо для разработки требований к системе защиты, позволяющих решать вопросы формирования структуры технических средств защиты.

Результаты моделирования представлены ниже в виде графиков поверхностей или линий уровня решения.

На рисунке 4.17 представлено начальное распределение угроз.

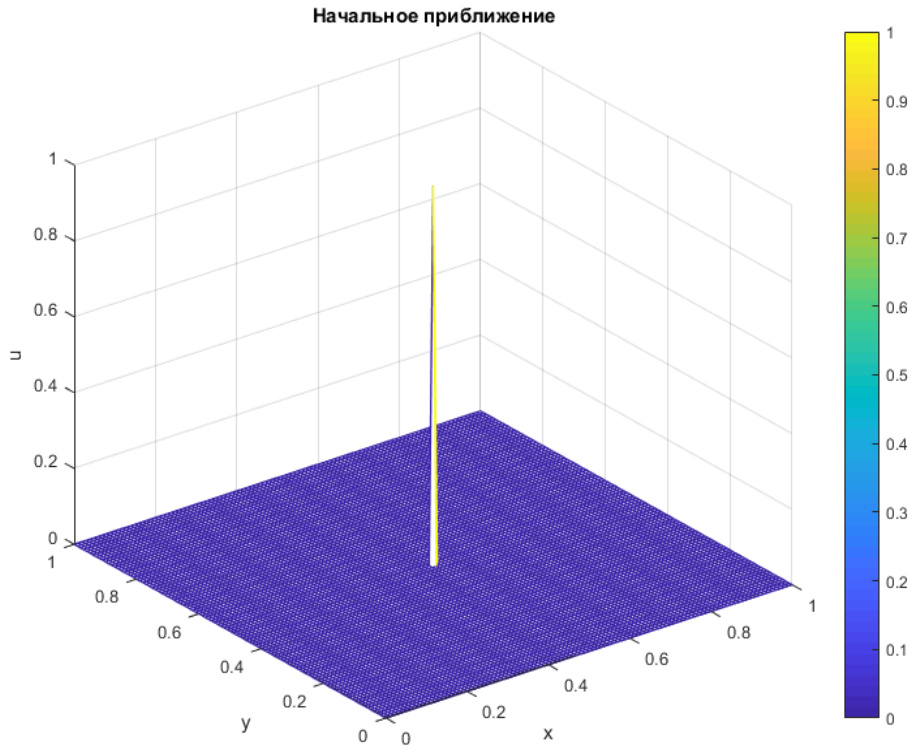


Рисунок 4.17 – Начальное распределение угроз

Графики поверхности решения задачи и графики линий уровня решения задачи для различных временных шагов k показаны на рисунках 4.18 – 4.25.

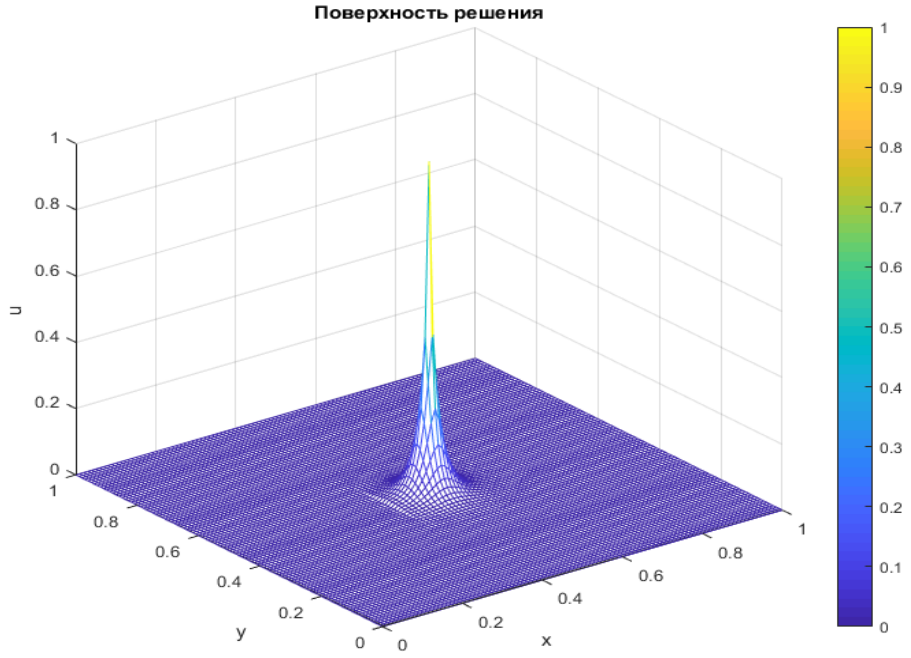


Рисунок 4.18 – График поверхности решения для $k = 1$

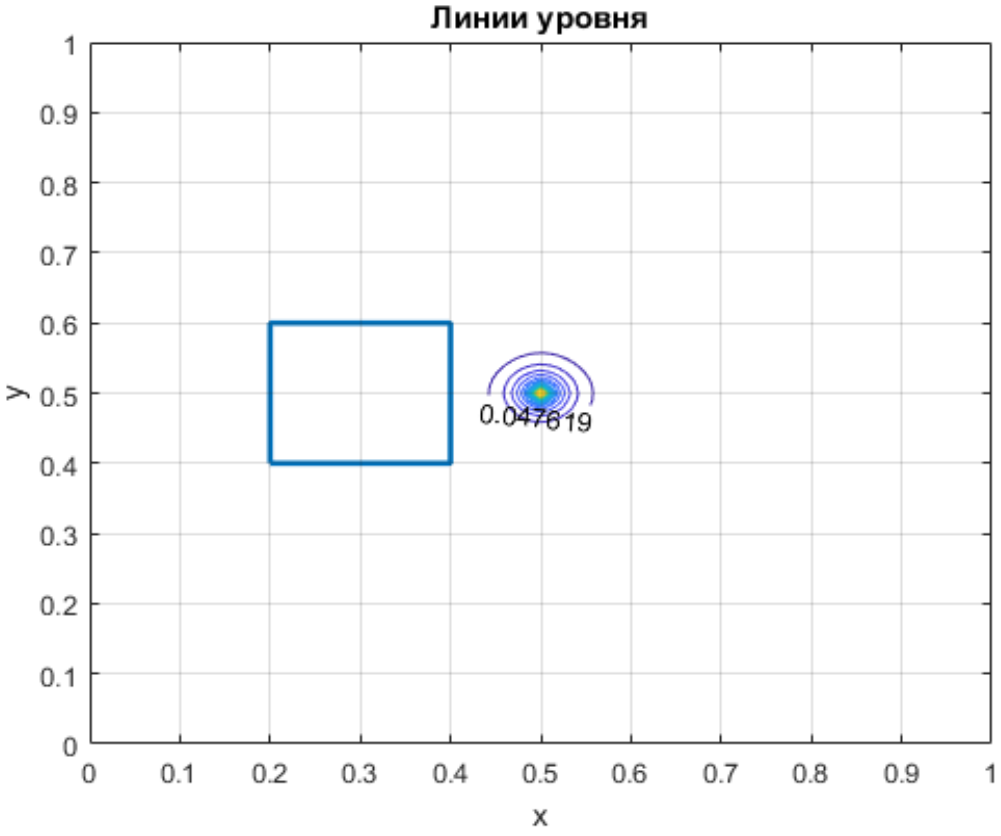


Рисунок 4.19 – График линий уровня решения для $k = 1$

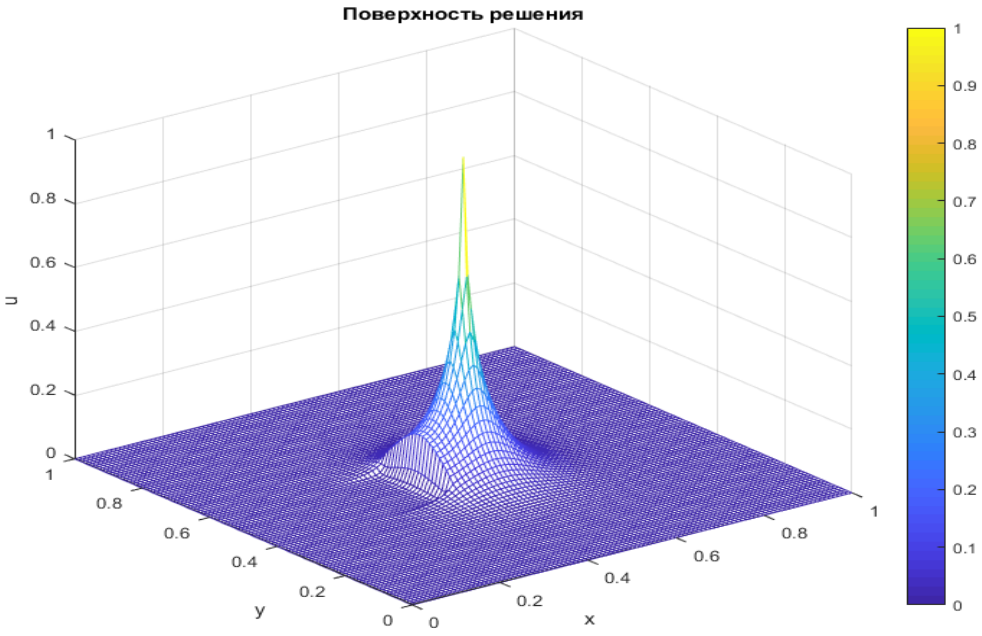


Рисунок 4.20 – График поверхности решения для $k = 10$

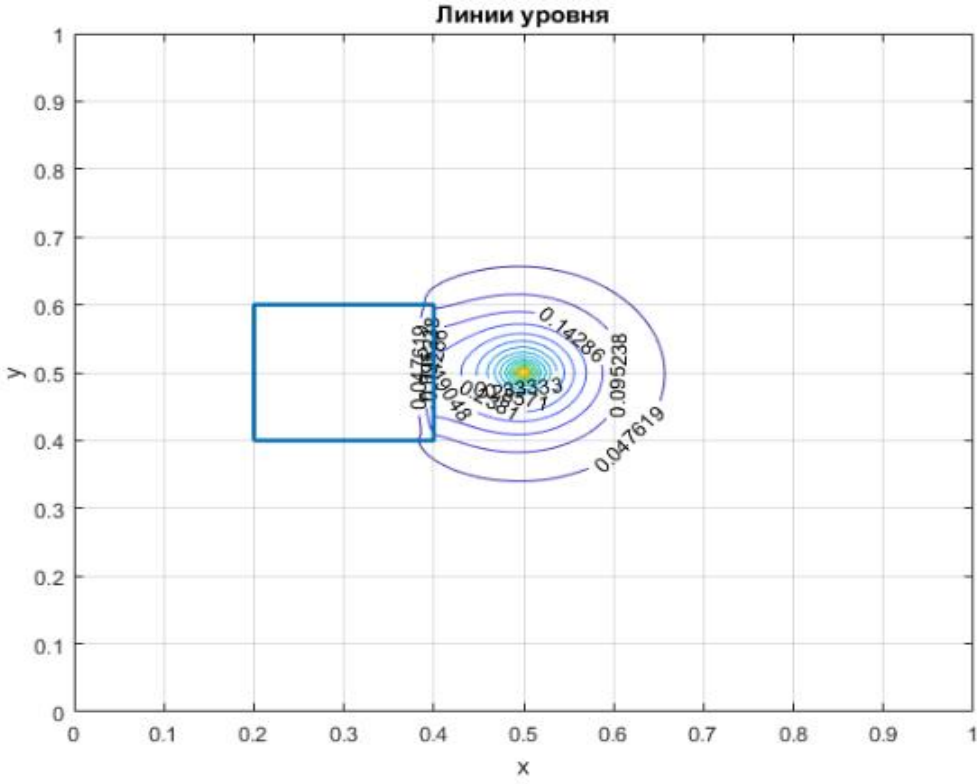


Рисунок 4.21 – График линий уровня решения для $k = 10$

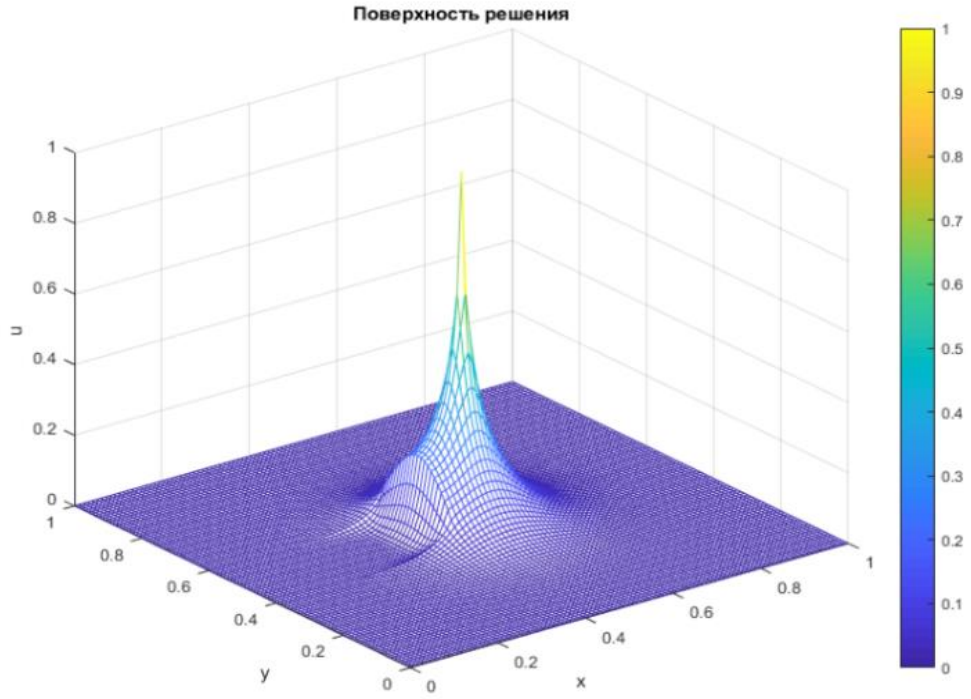


Рисунок 4.22 – График поверхности решения для $k = 40$

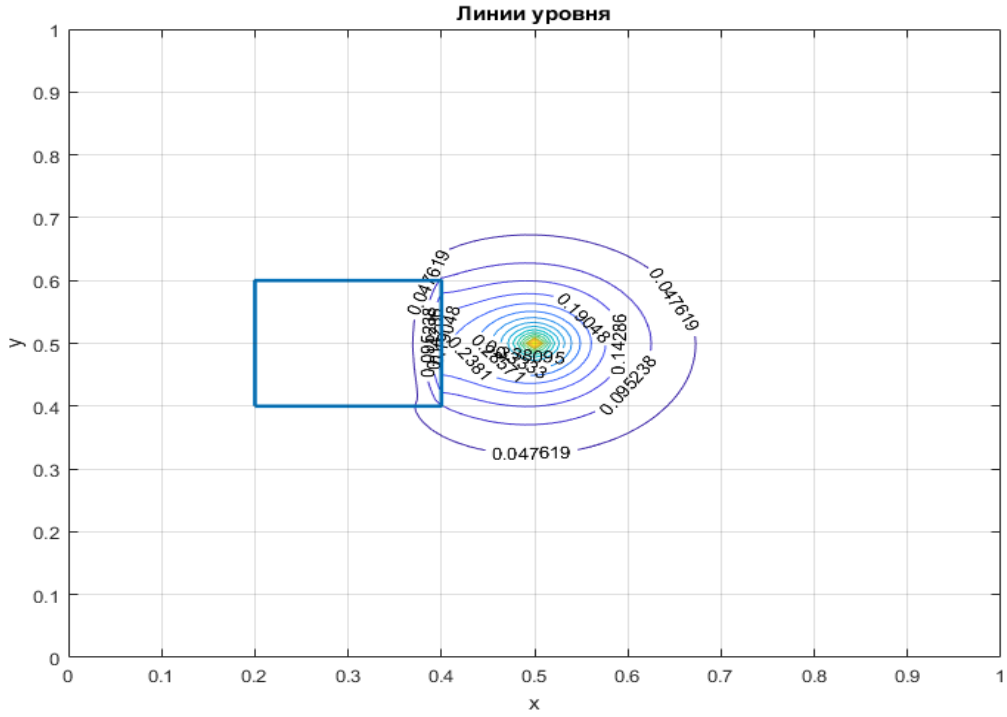


Рисунок 4.23 – График линий уровня решения для $k = 40$

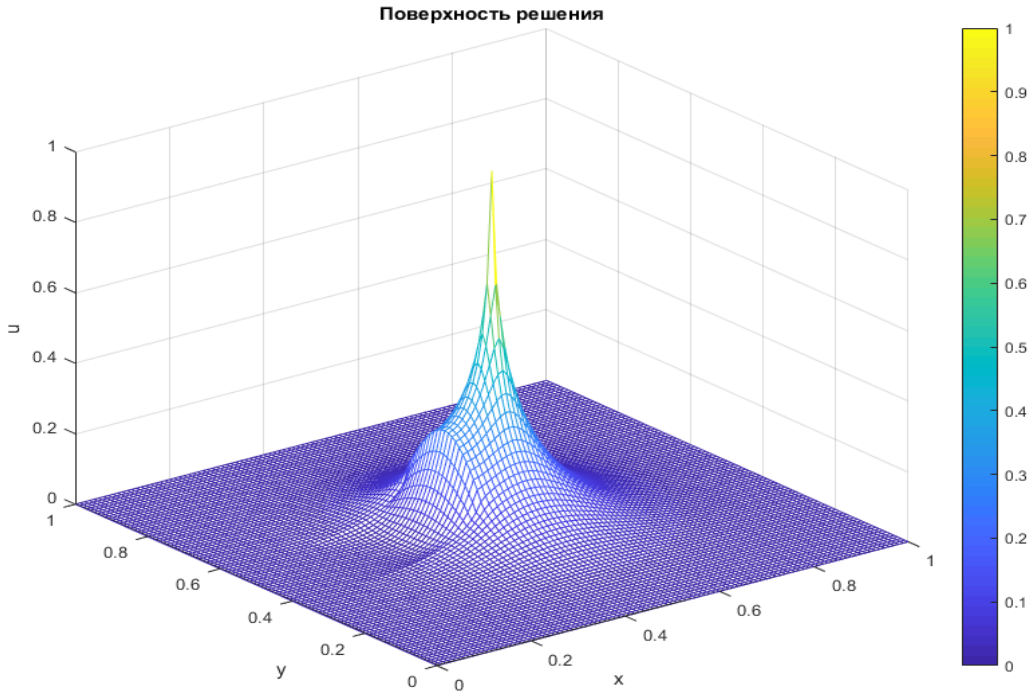


Рисунок 4.24 – График поверхности решения для $k = 160$

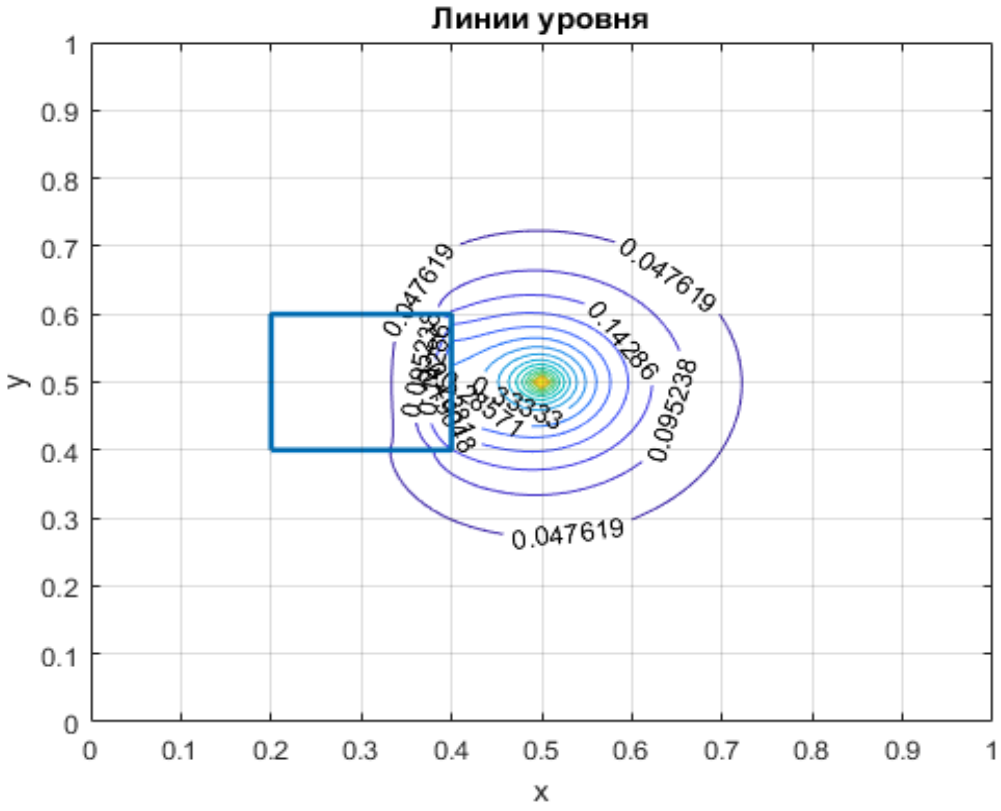


Рисунок 4.25 – График линий уровня решения для $k = 160$

Результаты экспериментального исследования показывают, что процесс достиг стационарного состояния. Показана принципиальная возможность моделирования нестационарных задач распространения угрозы через уязвимость. В дальнейшем необходима привязка параметров уравнения к параметрам реальных угроз.

4.4. Нейросетевое ранжирование аэропортов по критерию уязвимость (экспериментальный шаблон)

Рассматривается набор показателей (признаков в терминах машинного обучения) транспортной безопасности, установленных федеральными нормативными правовыми актами в области обеспечения транспортной безопасности и отраслевыми нормами и приказами. Экспертами отбирается набор показателей, характеризующих безопасность аэропорта. Для каждого показателя каждого аэропорта эксперты назначают оценки по шкале от 0 (полностью не удовлетворяет требованиям) до 10 (полностью удовлетворяет требованиям). В зависимости от мнения эксперта назначается общая оценка безопасности аэропорта. Причем общая оценка не должна являться вычисляемой функцией оценок отдельных показателей, а отражает общее мнение эксперта. Сформированные таким образом данные рассматриваются как набор данных для обучения нейронной сети. Строится и обучается на сформированном наборе данных нейронная сеть. При подаче на вход обученной сети экспертных оценок показателей аэропорта, которые не использовались при обучении, сеть дает оценку безопасности аэропорта.

При решении данной задачи следует иметь в виду следующее важнейшее обстоятельство. В своей работе и при обучении нейронные сети не используют алгоритмические последовательности. Они работают по некоторой аналогии с человеческим мозгом оперируя с создаваемыми образами.

Задача ранжирования аэропортов может быть решена достаточно просто, приблизительно так, как она решается в современных системах безопасности: проводится оценка уязвимости, эксперты сопоставляют требования к аэропортам с точки зрения безопасности с реальными параметрами безопасности аэропорта. В результате анализа делается экспертная оценка такого соответствия в баллах и делается общий вывод о ситуации по безопасности в аэропорту. В рамках некоторой выбранной шкалы можно установить нормативное значение показателя соответствия, на основании чего принимать решения безопасном функционировании аэропорта.

При таком подходе достаточно велик уровень некорректных решений, поскольку все зависит от профессиональной квалификации эксперта. Кроме того, практически невозможно сформулировать требования к аэропортам объективно и точно, поскольку всегда присутствует некоторая неопределенность не только в подходах, но и в понятиях. В конечном итоге, эксперт принимает решения, ориентируясь на свою интуицию и опыт работы. Именно этот нюанс позволяет учесть нейронная сеть. В процессе обучения сети за счет многократного варьирования исходным набором данных можно заложить в сеть многие нюансы, не поддающиеся формальному представлению. Конечно, это требует от постановщика задачи и пользователя сети весьма высокой квалификации, но и дает возможность получить результат, практически не зависимый от субъективного мнения экспертов.

Для проведения экспериментального моделирования был отобран фрагмент из 25 показателей (признаков) (таблица 4.1). В дальнейшем для компактного представления данных будет использованы номера признаков, а не словесные описания.

Сформированный экспертами набор данных представлен в приложении В. В этом приложении показана общая оценка уязвимости аэропорта и оценки, данные экспертами ИКАО. Проверки ИКАО выборочные и могут не совпадать с оценками экспертов.

Таблица 4.1 – Перечень показателей (фрагмент)

Номер показателя	Содержание пункта требованиям по обеспечению транспортной безопасности
1.	Назначить лицо, ответственное за обеспечение транспортной безопасности в субъекте транспортной инфраструктуры.
2.	Назначить лицо, ответственное за обеспечение транспортной безопасности, на каждом ОТИ первой, второй или третьей категории.
3.	Образовать (сформировать) в соответствии с особыми уставными задачами и/или привлечь в соответствии с планами обеспечения транспортной безопасности подразделения транспортной безопасности для защиты ОТИ от актов незаконного вмешательства, включая группы быстрого реагирования специально оснащенные, мобильные, круглосуточно выполняющие свои задачи по реагированию на подготовку совершения или совершения АНВ в зоне транспортной безопасности и/или на критических элементах ОТИ, а также на нарушения внутриобъектового и пропускного режимов группы из числа сотрудников подразделений транспортной безопасности.
4.	Разработать, принять и исполнять внутренние организационно-распорядительные документы, направленные на реализацию мер по обеспечению транспортной безопасности ОТИ и являющиеся приложением к плану обеспечения транспортной безопасности ОТИ.
5.	Разработать и утвердить план обеспечения транспортной безопасности ОТИ в течение трех месяцев и реализовать его в течение шести месяцев с момента утверждения результатов оценки уязвимости ОТИ.

Продолжение таблицы 4.1

Номер показателя	Содержание пункта требованиям по обеспечению транспортной безопасности
6.	Разработать, утвердить и реализовать порядок взаимодействия между силами обеспечения транспортной безопасности ОТИ и силами обеспечения транспортной безопасности других ОТИ, с которыми имеется технологическое взаимодействие.
7.	Проверить сотрудников сил обеспечения транспортной безопасности с целью выявления оснований, предусмотренных частью 1 статьи 10 Федерального закона от 9 февраля 2007 г. № 16-ФЗ «О транспортной безопасности», для прекращения трудовых отношений или отказа в приеме на работу.
8.	Осуществлять специальную профессиональную подготовку, повышение квалификации, переподготовку сотрудников сил обеспечения транспортной безопасности в соответствии с программами и документами, определенными законодательством Российской Федерации.
9.	Допускать к работе на должностях, указанных в номенклатуре (перечне) должностей персонала, непосредственно связанного с обеспечением транспортной безопасности ОТИ, а также привлекать к исполнению обязанностей по защите ОТИ от актов незаконного вмешательства в соответствии с планами обеспечения транспортной безопасности только сотрудников сил обеспечения транспортной безопасности, аттестованных в соответствии с законодательством Российской Федерации.

Продолжение таблицы 4.1

Номер показателя	Содержание пункта требованиям по обеспечению транспортной безопасности
10.	Не допускать совершения АНВ в отношении ОТИ, а также иных действий, приводящих к повреждению устройств и оборудования ОТИ или использованию их не по функциональному предназначению, влекущих за собой человеческие жертвы, материальный ущерб или возможность наступления таких последствий.
11.	Изменять конструктивные или технические элементы, технологические процессы на ОТИ, а также порядок их эксплуатации только после принятия компетентным органом в области обеспечения транспортной безопасности решения о наличии или отсутствии необходимости изменения значения присвоенной категории, проведения дополнительной оценки уязвимости ОТИ и внесения дополнений в планы обеспечения транспортной безопасности ОТИ в части, касающейся произведенных изменений.
12.	Ограничить доступ к сведениям о результатах проведенной оценки уязвимости ОТИ и планам обеспечения транспортной безопасности ОТИ в соответствии с законодательством Российской Федерации.
13.	Реализовать предусмотренные планом обеспечения транспортной безопасности ОТИ дополнительные меры при изменении уровня безопасности в сроки, не превышающие 3 часов для ОТИ первой категорий с момента получения сообщения или принятия решения об изменении уровня безопасности.

Продолжение таблицы 4.1

Номер показателя	Содержание пункта требованиям по обеспечению транспортной безопасности
14.	Создать и оснастить посты (пункты) управления обеспечением транспортной безопасности необходимыми средствами управления и связи, обеспечивающими взаимодействие как между силами обеспечения транспортной безопасности ОТИ, так и с силами обеспечения транспортной безопасности других ОТИ, с которыми имеется технологическое взаимодействие.
15.	Обеспечить круглосуточное непрерывное функционирование постов (пунктов) управления обеспечением транспортной безопасности ОТИ, а также накопление, обработку и хранение в электронном виде данных со всех технических средств обеспечения транспортной безопасности и передачу указанных данных в соответствии с установленным порядком уполномоченным подразделениям федерального органа исполнительной власти в области обеспечения безопасности Российской Федерации, федерального органа исполнительной власти, осуществляющего функции по выработке государственной политики и нормативно-правовому регулированию в сфере внутренних дел, а также территориальные управления федерального органа исполнительной власти, осуществляющего функции по контролю и надзору в сфере транспорта, в соответствии с утвержденными планами обеспечения транспортной безопасности.

Продолжение таблицы 4.1

Номер показателя	Содержание пункта требованиям по обеспечению транспортной безопасности
16.	Обеспечить видеонаблюдение за действиями сил транспортной безопасности на КПП и постах (пунктах) управления обеспечением транспортной безопасности ОТИ.
17.	Установить конфигурацию и границы территории ОТИ, доступ в которую физических лиц, пронос (провоз) материальных объектов не ограничивается (далее – зона свободного доступа ОТИ).
18.	Установить конфигурацию и границы территории или части (наземной, подземной, воздушной, надводной, подводной) ОТИ, проход в которые осуществляется через контрольно-пропускные пункты (посты) (далее – зоны транспортной безопасности), а также критических элементов ОТИ.
19.	Установить конфигурацию и границы участков зоны транспортной безопасности ОТИ, допуск физических лиц и перемещение материальных объектов в которые осуществляется по перевозочным документам и/или пропускам установленных видов в соответствии с номенклатурами (перечнями) должностей и предметы и вещества, которые запрещены или ограничены для перемещения (далее – перевозочный сектор зоны транспортной безопасности).
20.	Установить конфигурацию и границы участков зоны транспортной безопасности ОТИ, доступ в которые ограничен для пассажиров и осуществляется для физических лиц и материальных объектов по пропускам установленных видов в соответствии с номенклатурами (перечнями) должностей и предметы и вещества, которые запрещены или ограничены для перемещения (далее – технологический сектор зоны транспортной безопасности).

Продолжение таблицы 4.1

Номер показателя	Содержание пункта требованиям по обеспечению транспортной безопасности
21.	Установить схему размещения и состав оснащения контрольно-пропускных пунктов (постов) на границах зоны безопасности и/или её секторов, критических элементов ОТИ, а также зоны свободного доступа ОТИ.
22.	Изменять конфигурацию и границы зоны транспортной безопасности, её перевозочного и технологического секторов и критических элементов ОТИ, а также схему размещения и состав оснащения КПП лишь после завершения дополнительной оценки уязвимости и утверждения планов обеспечения транспортной безопасности, учитывающих такие изменения.
23.	Воспрепятствовать преодолению любыми лицами контрольно-пропускных пунктов (постов) без соблюдения условий допуска, наличия и действительности пропусков и иных установленных видов разрешений в зону транспортной безопасности или на критические элементы ОТИ.
24.	Оснастить ОТИ инженерно-техническими системами обеспечения транспортной безопасности в соответствии с утвержденными планами обеспечения транспортной безопасности.
25.	Обеспечить защиту инженерно-технических систем обеспечения транспортной безопасности ОТИ от несанкционированного доступа к элементам управления, обработки и хранения данных.

Набор обучающих данных не имеет пропусков и аномальных значений. Кодировать необходимо только оценку уязвимости. Примем, что при общей оценке

уязвимости 8–10 баллов аэропорт является безопасным и кодируем это состояние 1, оценки ниже 8 соответствуют уязвимости аэропорта и кодируются 0. Так как планируется применить для построения нейронной сети систему MATLAB, автоматически производящую масштабирование данных, то нет необходимости масштабирования данных.

Программа экспериментального варианта нейронной сети (классификатор аэропортов)

Для разработки программы демонстрационного варианта нейронной сети использован инструмент визуального программирования Neural Network Pattern Recognition Tool пакета Deep Learning Toolbox системы MATLAB. Предварительно в рабочее пространство MATLAB необходимо загрузить массив признаков **P**, каждая строка которого соответствует признакам одного аэропорта, и вектор-столбец целевых значений **T**, элементы которого представляют собой оценки безопасности аэропорта (1 или 0). В качестве входных данных (Inputs) выбирается массив **P**, в качестве целевых значений (Targets)– массив **T.**

Инструмент визуального программирования Neural Network Pattern Recognition Tool пакета Deep Learning Toolbox системы MATLAB предоставляет в распоряжение пользователя ряд управляющих кнопок и окон (Рисунки 4.26 – 4.32).

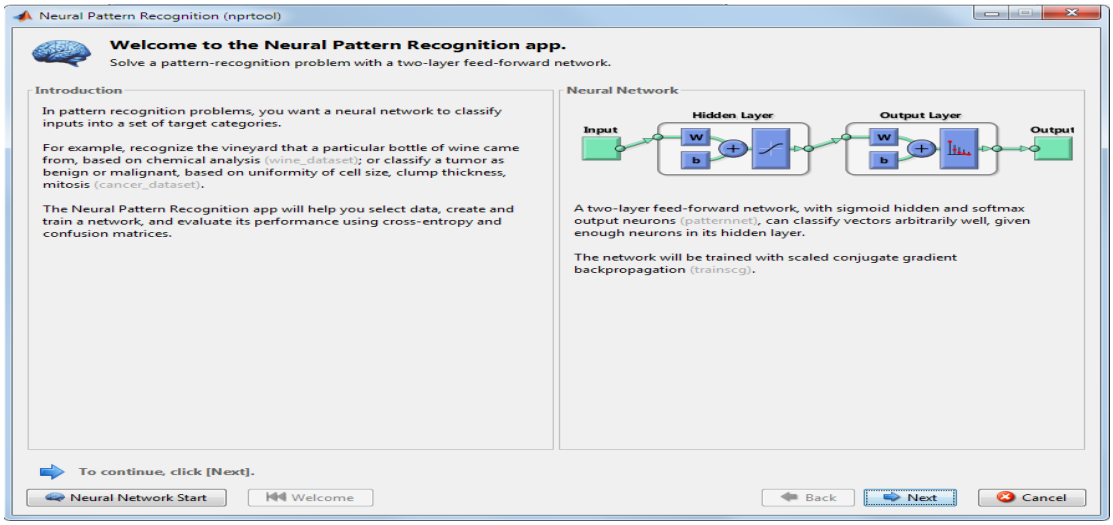


Рисунок 4.26 – Управляющее окно. Стартовое окно

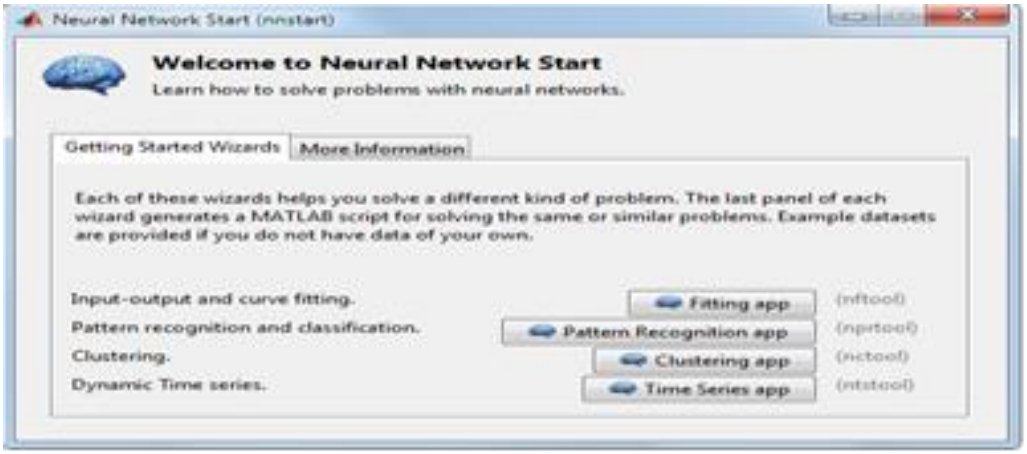


Рисунок 4.27 – Управляющее окно. Приглашение

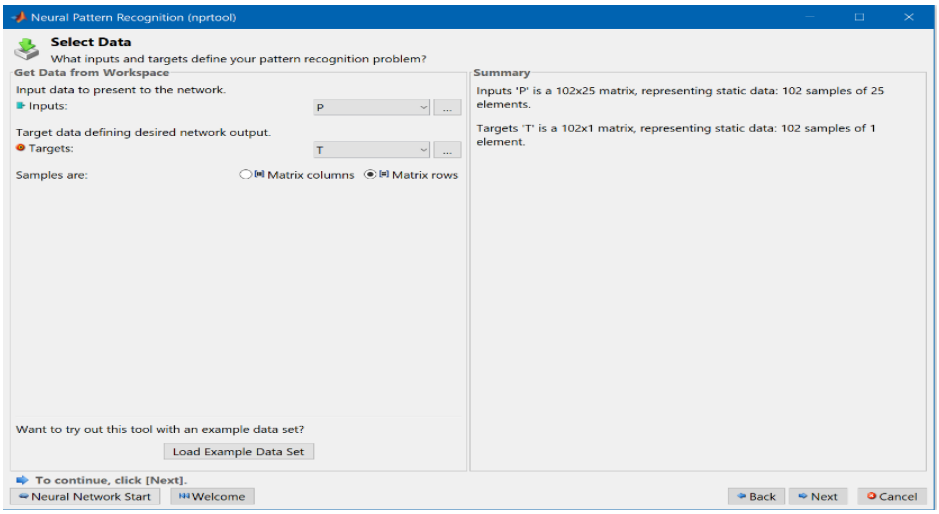


Рисунок 4.28 – Управляющее окно. Выбор данных

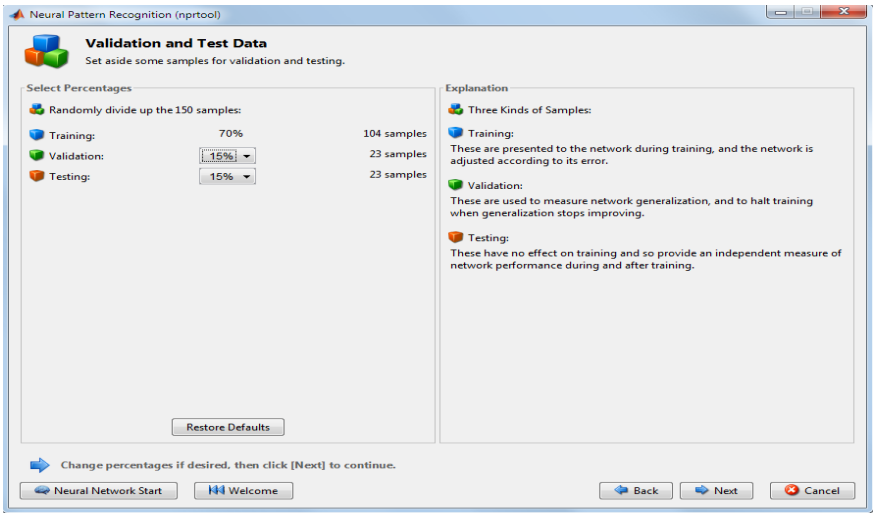


Рисунок 4.29 – Управляющее окно. Validation and Test Data

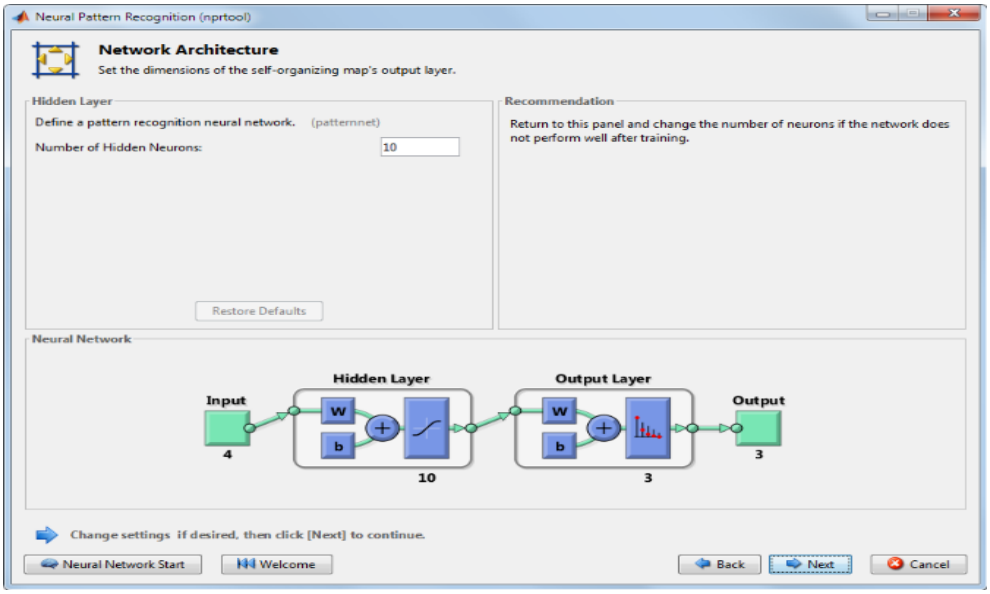


Рисунок 4.30 – Управляющее окно. Архитектура сети

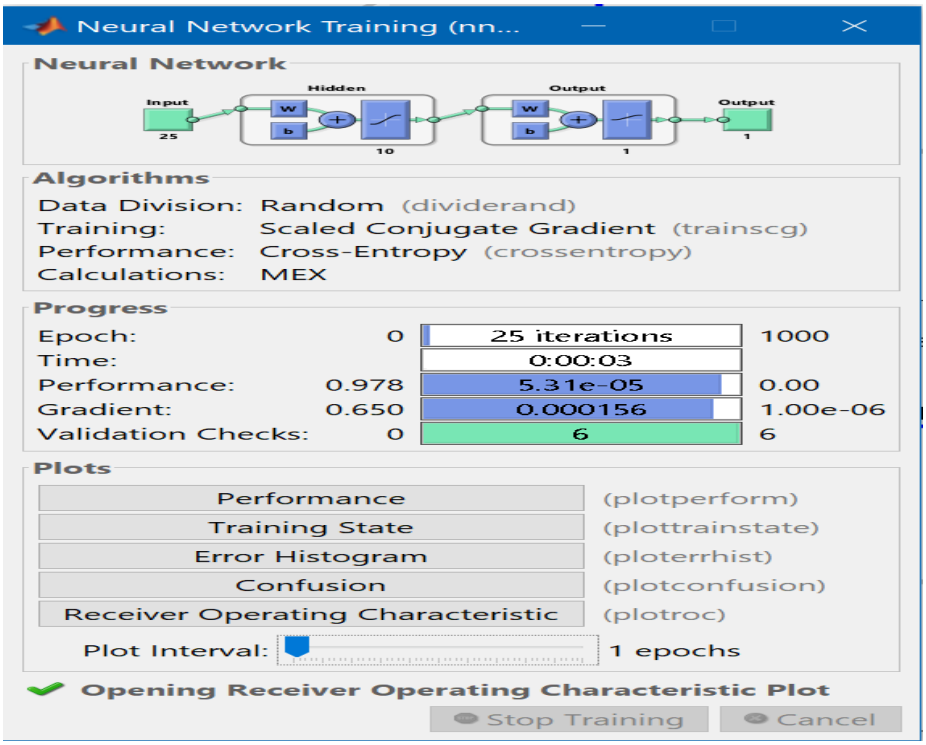


Рисунок 4.31 – Управляющее окно. Обучение сети

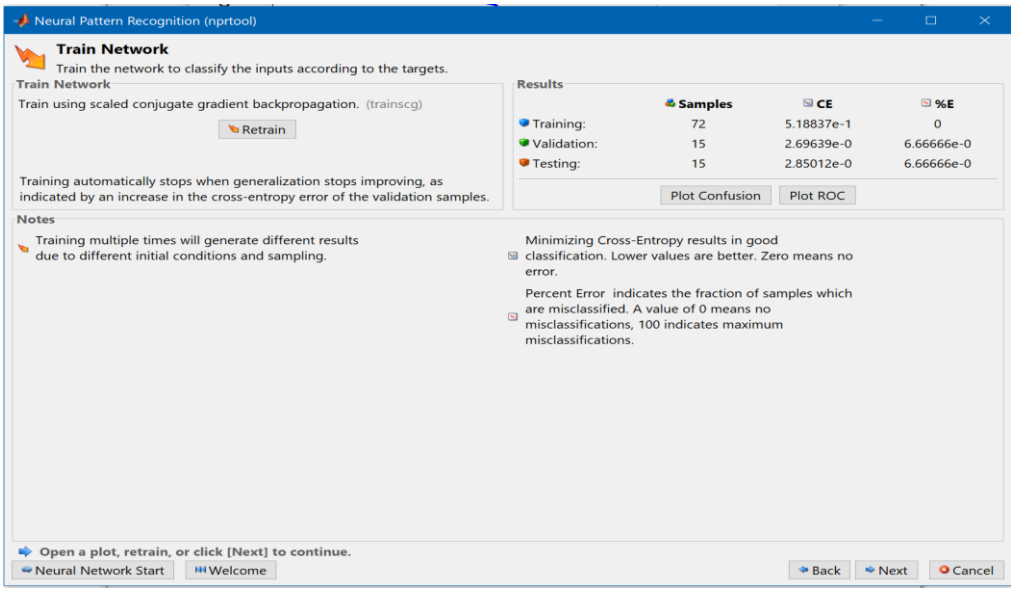


Рисунок 4.32 – Управляющее окно. Завершение обучения

С помощью инструмента Neural Network Pattern Recognition Tool можно сгенерировать программу (приложение В). В программе подразумевается, что входные данные и целевые значения находятся в рабочем пространстве MATLAB. Сгенерированная программа может быть усложнена добавлением возможностей, отсутствующих в Neural Network Pattern Recognition Tool. В частности, можно строить сети с большим числом скрытых слоев, обучающихся различными методами.

Анализ результатов моделирования

На рисунках 4.33 – 4.35 представлены визуальные результаты решения задачи.

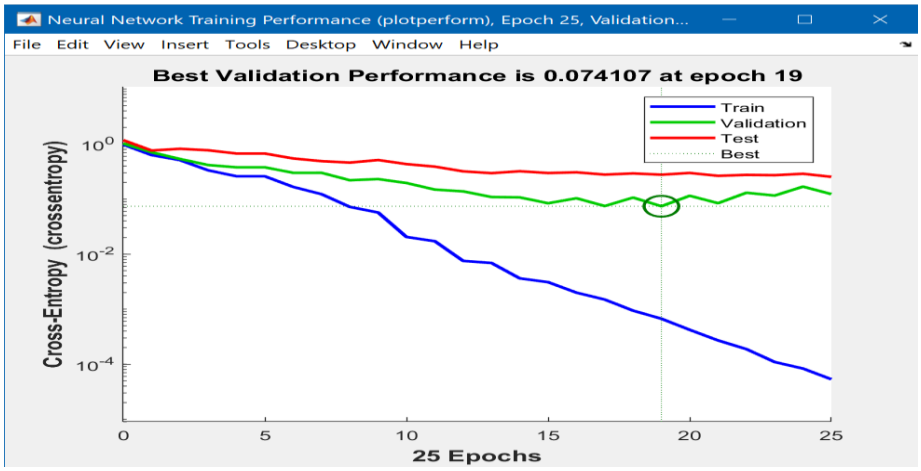


Рисунок 4.33 – Результаты моделирования. Обучение

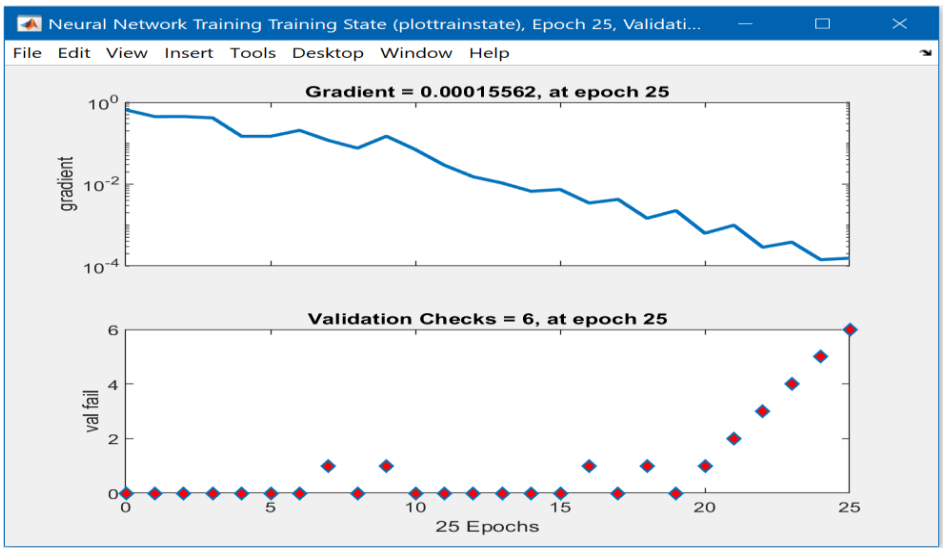


Рисунок 4.34 – Результаты моделирования. Состояние обучения

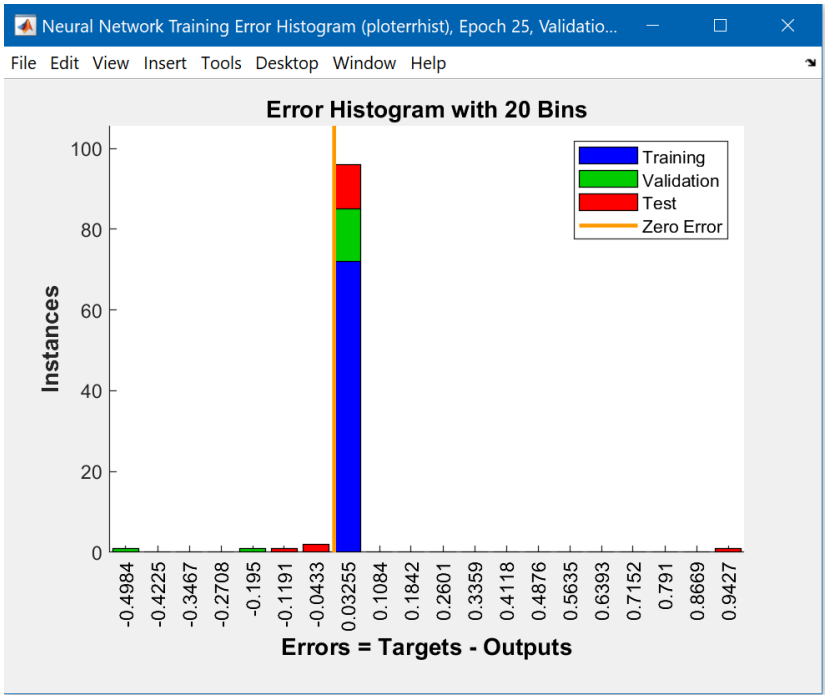


Рисунок 4.35 – Результаты моделирования. Ошибки

На рисунке 4.33 представлен график обучения, из которого можно увидеть поведение ошибки обучения на всех трех множествах. Рисунок 4.34 наглядно демонстрирует изменение градиента функционала ошибки и ее величины на проверочном множестве. Гистограмма (Рисунок 4.35) построена для 20 столбцов.

На обучающем множестве (Confusion) (Рисунок 4.36) все примеры были распознаны безошибочно. На проверочном (валидационном) множестве безопасные аэропорты (выходной класс обозначен как 1) распознаны с точностью 90%.

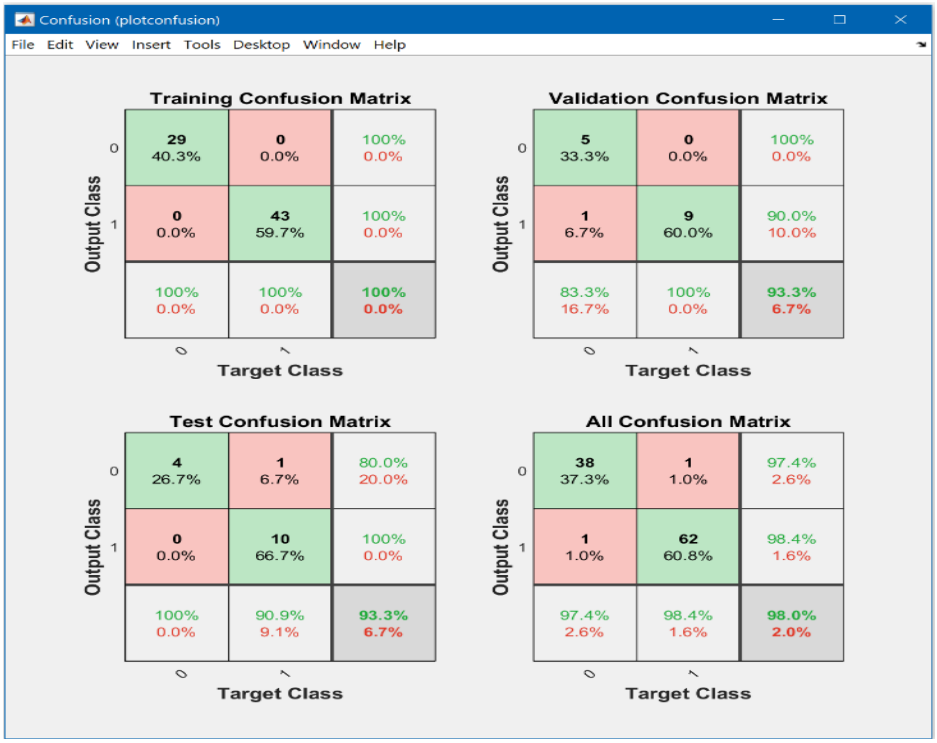


Рисунок 4.36 – Матрица ошибок сети

Снижение точности на проверочном и тестовом множествах объясняется небольшим объемом выборки: из 15% случайно выбранных примеров определенного класса имеется немного.

ROC-кривые (Рисунок 4.37) получились практически идеальными.

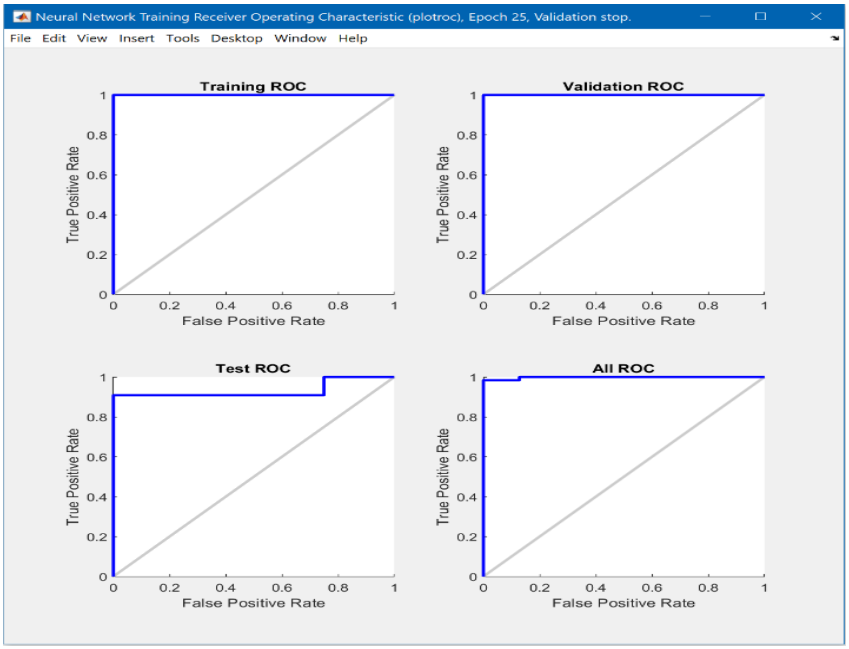


Рисунок 4.37 – ROC-кривые

Ниже представлен расчет основных показателей качества нейросетевого классификатора, который проведен по проверочному (валидационному) множеству (см. также 2.4).

Прецизионность (Precision): $R_{PR} = \frac{N_{TP}}{N_{TP} + N_{FP}} = \frac{9}{9+0} = 1,00$.

Полнота (Recall): $S_R = \frac{N_{TP}}{N_{TP} + N_{FN}} = \frac{9}{9+1} = 0,90$.

Специфичность (Specificity): $S_P = \frac{N_{TN}}{N_{TN} + N_{FN}} = \frac{5}{5+1} = 0,83$.

F_1-мера (F-score):

$$F_1 = 2\frac{R_{PR} * S_R}{R_{PR} + S_R} = 2\frac{1*0,90}{1+0,90} = 0,95.$$

Предложенный авторский подход является первым этапом в решении глобальной задачи создания автоматизированной системы управления уровнем транспортной безопасности объектов с распределенной структурой (аэропортов). Разработан эвристический метод в комбинации с эвристическими процедурами, который все ранее непреодолимые трудности формализации исключает из процесса математического моделирования. Вопрос адекватности математической модели, достоверности и точности полученных результатов решается в рамках системы принятия решений по формированию требований к техническим средствам защиты на основе принципа приемлемости уровня транспортной безопасности. На этом этапе осуществляется переход от интенсивностей распределения угроз безопасности по топологии объекта к показателям качества функционирования системы защиты и ее элементов. Указанный переход базируется, в том числе, и на некоторых более ранних работах автора [111; 116; 129; 130; 250] и является прерогативой дальнейших научных размышлений.

Математический аппарат теории краевых задач блестяще себя проявил при решении задач, связанных с исследованием полей различной физической природы, электромагнитных, температурных, интенсивности нефтяного пласта и многих

других. Введение и использование понятия уязвимость объекта транспортной инфраструктуры в гражданской авиации и создание методов его качественной оценки [118] предполагает возможность в постановочном плане провести некоторую аналогию с понятиями теории поля. В таком случае, использование математического аппарата теории краевых задач для моделирования задач, связанных с безопасностью, представляется вполне допустимым. Более того, на данном этапе исследования результаты численного моделирования были получены в относительных единицах опасности (безопасности), не привязанных к реальным параметрам угроз и не связанных с моделью нарушителя. Это означает, что получены качественные оценки, при этом, следует заметить, что другая задача на данном этапе и не ставилась.

Выводы к главе 4

1. Оптимизация процедур управления транспортной безопасностью предполагает, как результат, достижение приемлемого уровня этой безопасности, используя в качестве критерия оптимальности уязвимость, отражающую степень удовлетворения требований к объекту защиты.

2. Модель уязвимости разработана применительно к критическим элементам объекта защиты и включает количественные оценки угроз, полученные в результате численного моделирования процесса их распространения в формате дифференциальных уравнений в частных производных (стационарная задача) и уязвимостей (нестационарная задача).

3. Процедуры перехода от угроз к уязвимостям и обратная задача реализуются на основе квалиметрического подхода, где количественные значения определяют и отражают степень соответствия параметров угроз (уязвимостей) заданным требованиям к критическим элементам системы защиты объекта с учетом масштабирования.

4. Численное моделирование предполагает различные варианты распределения угроз (с одним источником опасности, с распределенной опасностью, с противодействием опасности) или типов уравнений (уравнение диффузии), что определяет статистический подход к формированию окончательного решения, включая эвристические процедуры.

5. Для ранжирования аэропортов по степени соответствия требованиям по безопасности разработана нейросетевая модель на основе инструмента визуального программирования Neural Network Pattern Recognition Tool пакета Deep Learning Toolbox системы MATLAB, обеспечившая следующее качество работы классификатора: Precision – 1.0, Recall – 0.9, Specificity – 0.83, F-score – 0.95.

6. Разработанный авторский подход является важным этапом в решении глобальной задачи создания автоматизированной системы управления уровнем транспортной безопасности объектов с распределенной структурой (аэропортов), который в комбинации с эвристическими процедурами ранее непреодолимые трудности формализации исключает из процесса математического моделирования. Вопрос адекватности математической модели, достоверности и точности полученных результатов решается в рамках системы принятия решений по формированию требований к техническим средствам защиты на основе принципа приемлемости уровня транспортной безопасности, когда осуществляется переход от интенсивностей распределения угроз безопасности по топологии объекта к показателям качества функционирования системы защиты и ее элементов.

ГЛАВА 5 НЕЙРОСЕТЕВЫЕ МОДЕЛИ ДЛЯ ПАРИРОВАНИЯ УГРОЗ НЕСАНКЦИОНИРОВАННОГО ВМЕШАТЕЛЬСТВА ПЕРСОНАЛА ТРАНСПОРТНОЙ БЕЗОПАСНОСТИ

Авиационный персонал и, в частности, персонал, имеющий отношение к обеспечению транспортной безопасности, реализует свою производственную деятельность в условиях повышенных требований к качеству результатов работы. С другой стороны, достижение абсолютных результатов в этой сфере деятельности практически невозможно, т.е. всегда присутствует некоторое расхождение между требованиями и конечными результатами, что приводит к снижению уровня транспортной безопасности объектов защиты, а в особо критичных ситуациях к возникновению авиационных происшествий. Отсюда возникает понятие негативного влияния персонала на безопасность, т.е. персонал можно рассматривать как некоторую угрозу безопасности объекта (подраздел 1.6).

Естественно, возникает задача минимизации негативного влияния персонала, которая в условиях информационного управления безопасностью требует создания соответствующей методологии, включающей модели, методы, алгоритмы и процедуры, хорошо адаптируемые с современными технологиями ESM, PSIM, DATA MINING. Процесс создания методологии включает некоторую совокупность новых подходов и методов, обеспечивающих решение задачи и проблем, представленных в данном разделе.

5.1 Несанкционированное вмешательство персонала как фактор угрозы безопасности объекта защиты

Проблемы, связанные с человеческим фактором (ЧФ), многогранны и достаточно сложны. Классические подходы к решению этих проблем в гражданской авиации практически себя исчерпали. Идея нового подхода состоит в принципиальном пересмотре физического смысла человеческого фактора,

понимая, что ЧФ при строгом определении все-таки не фактор, а гораздо более сложная и многогранная категория, относящаяся к сложным системам и имеющая целевой функционал, не поддающийся строгому математическому описанию [9].

Изменение степени негативной зависимости авиационных событий от человека связывают с качеством профессиональной подготовки специалиста и совершенствованием технической составляющей, т.е. внутри ЧФ совершенствуют личный и технический элементы. Очевидно, что здесь присутствуют красные линии, которые существенно ограничивают возможности такого подхода.

Еще более сложное положение с ЧФ сложилось в области транспортной безопасности, где совсем мало научных исследований проблемы, а те, что есть, занимаются, в лучшем случае, решением локальных задач [80].

Обычно, предлагаемое решение состоит в минимизации человеческого фактора, что далеко не всегда возможно. Предлагается уйти от представления ЧФ как некоторого фактора и рассматривать его как угрозу безопасности объекта от незаконного вмешательства персонала в деятельность этого объекта. Иными словами, предлагается исследовать негативное влияние персонала авиационной организации на процедуры обеспечения и управления транспортной безопасностью. Минимизировать необходимо часть ЧФ, которая представляет собой угрозу (опасность) производственной деятельности и является несанкционированным вмешательством. В таком случае появляются соответствующие модели и методы, которые идентифицируют негативное влияние персонала авиационной организации. Результат исследования, представленный в некотором количественном эквиваленте, может рассматриваться как параметр управления уровнем негативного влияния, т.е. угроза ЧФ становится управляемой [255] (Рисунок 5.1).

Рисунок 5.1 – К вопросу о новом содержании понятия человеческий фактор

Автор вводит новое понятие: угроза персонала, под которым будем понимать состояние неадекватности профессиональной готовности оператора и параметров ситуации в системе безопасности, определяемое предельным уровнем психофизиологических параметров личности, допускающим появление негативного события (угрозы).

Если составляющие ЧФ вынести за скобки, то остается фактор негативного влияния персонала, т.е. рассматриваются такие проявления в ходе реализации производственной деятельности, которые, часто независимо от желания специалиста-оператора, приводят к определенным нарушениям алгоритма производственной деятельности, результатом чего становятся события-инциденты, квалифицируемые как акт незаконного вмешательства, а это уже угроза безопасности [257].

Таким образом, возникает абсолютно новая ситуация, когда необходимо минимизировать не человеческий фактор как таковой, а ставится задача регулировать негативное влияние персонала авиационной организации на процедуры выполнения производственной деятельности, рассматривая это влияние как угрозу безопасности объекта. В этом случае меняются подходы к решению задачи и методы исследования.

Информационное управление уровнем транспортной безопасности объекта защиты (аэропорта) предполагает решение проблем управления безопасностью с помощью современных компьютерных технологий. Персонал транспортной безопасности является составной частью комплексной системы обеспечения транспортной безопасности. В таком случае, проблема информационного управления авиационным персоналом решается в рамках совокупности моделей и методов, применяемых при управлении безопасностью объекта защиты (Рисунок 5.2).

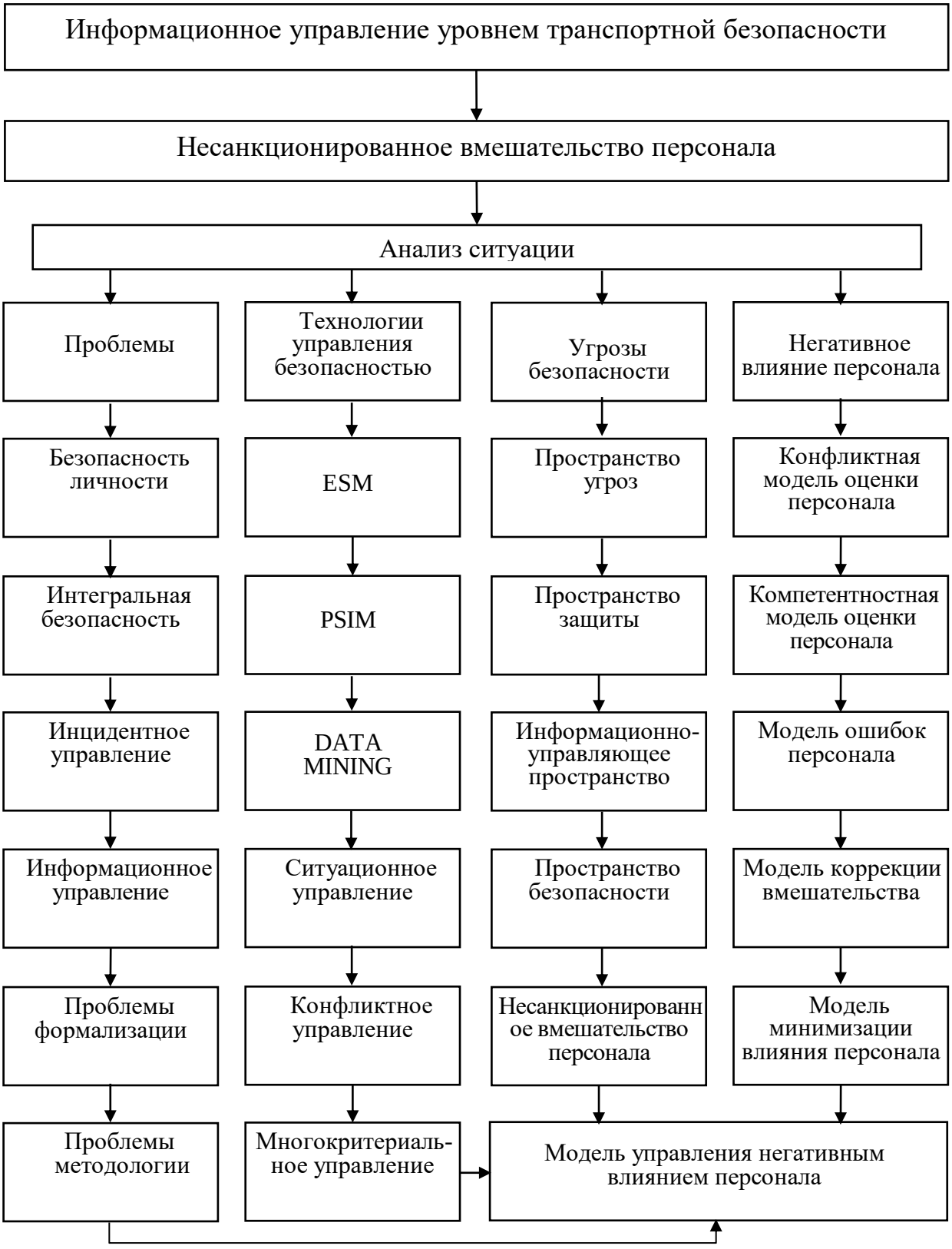


Рисунок 5.2 – Модель информационного управления авиационным персоналом

Представленная модель показывает последовательность решения всей совокупности проблем управления безопасностью в рамках исследования проблем управления персоналом в целях формирования модели управления негативным влиянием персонала.

Следует отметить несколько важных исходных положений:

– по отношению к персоналу в равной степени важны те проблемы, которые возникают при управлении безопасностью объекта защиты в комплексе (подразделы 1.1, 1.6);

– информационное управление безопасностью построено на современных компьютерных технологиях, типа ESM, PSIM и других, обладающих определенными и заметными достоинствами, но, с другой стороны, внедрение которых предполагает решение комплекса достаточно сложных проблем и вопросов, которые далеко не всегда приводятся к известным моделям и методам (подраздел 2.4);

– в рамках решаемой задачи, персонал транспортной безопасности обладает свойством дуальности: персонал вносит весомый вклад в решение конкретных проблем управления безопасностью, вместе с тем, он же оказывает негативное влияние на уровень безопасности объекта защиты, что выделяет эту проблему в самостоятельный объект научного исследования;

– проблема минимизации негативного влияния персонала не решается как типовая задача исследования человеческого фактора (подраздел 1.6).

Несанкционированное вмешательство персонала в процедуры управления безопасностью в условиях информационного управления уровнем транспортной безопасности аэропорта рассматривается как негативная часть этого управления, которая в предельном варианте может привести к авиационному происшествию.

Если ставится задача управления уровнем этого негативного влияния персонала, то она решается на основе исследования ситуации в сложной системе, которой является авиационный персонал. Это исследование предполагает четыре направления анализа ситуации: исследование проблем управления безопасностью,

исследование технологий управления безопасностью, исследование угроз безопасности и исследование собственно негативного влияния персонала.

Среди проблем можно выделить три основных: проблемы, связанные с безопасностью личности и переход к понятию интегральная безопасность (подраздел 1.1); проблемы перехода от инцидентного управления к информационному, что связано с формированием больших информационных массивов (подразделы 2.1., 2.4); проблемы формализации, обусловленные существенной неопределенностью при описании объекта управления (защиты) и фактическим отсутствием моделей и алгоритмов, которые должны быть в основе процедур информационного управления (подразделы 3.2., 3.4).

Информационное управление связано с современными технологиями (ESM, PSIM, DATA MINING) (подразделы 2.4., 3.3); с проблемами системотехники, когда управление выстраивается на основе оценки ситуации в объекте защиты; с уровнем разработанности проблем многокритериальности и конфликтности.

Проблемы, связанные с угрозами безопасности вытекают из некоторой виртуальности этих угроз, поскольку они рассматриваются как потенциальные, (не реализованные). Метод исследования угроз заключается в их представлении в формате некоторой совокупности виртуальных полей безопасности, что позволяет идентифицировать как объект исследования несанкционированное вмешательство персонала (подраздел 3.2).

Программа исследования негативного влияния персонала включает анализ нескольких моделей: конфликтная и компетентностная модели оценки персонала, модель ошибок, модель коррекции и модель минимизации негативного влияния. Исследование этих моделей приводит к модели управления негативным влиянием персонала, на основе которой формируется методология решения проблем авиационного персонала в условиях информационного управления (подразделы 5.4., 5.5).

Модель управления негативным влиянием персонала основана на многокритериальном управлении и количественных оценках параметров этих

критериев, в качестве которых предлагаются конфликт, компетентность и риск. С учетом существенной неопределенности в описании этих критериев процедура количественной оценки параметров становится эвристической.

Фактор негативного влияния персонала рассматривается как такие проявления в ходе реализации производственной деятельности, которые, независимо от желания специалиста-оператора, приводят к определенным нарушениям алгоритма производственной деятельности, результатом чего становятся события-инциденты, квалифицируемые как акт незаконного вмешательства, а это уже угроза безопасности (Рисунок 5.3).

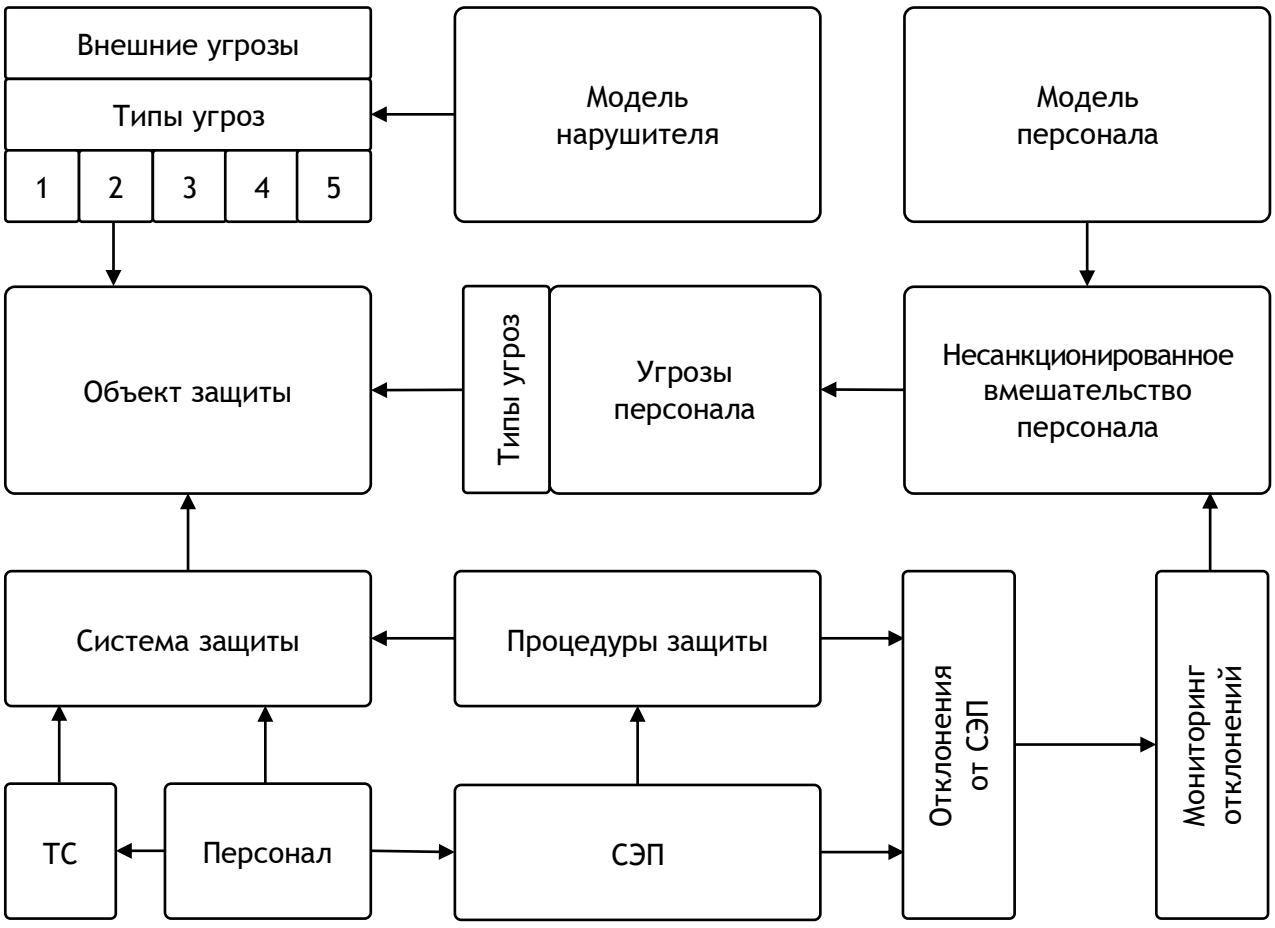


Рисунок 5.3 – Несанкционированное вмешательство персонала

Причины появления отклонений в значительной степени связаны с моделями нарушителя и персонала (Рисунок 5.4).

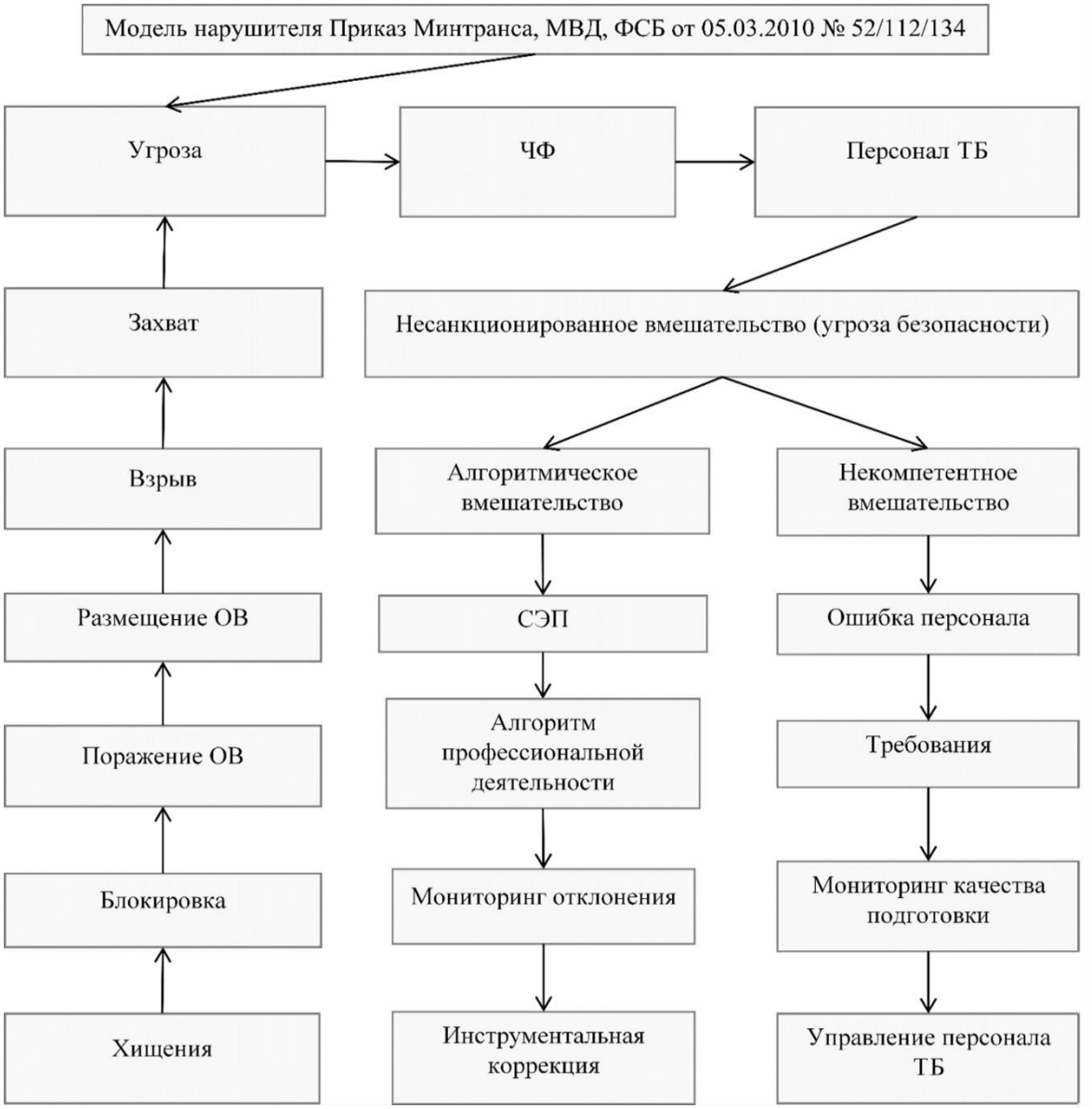


Рисунок 5.4 – К вопросу идентификации угроз персонала

Идентификация угроз персонала обусловлена необходимостью сопоставления этих угроз и угроз, вытекающих из модели нарушителя [158], которая определена приказом Минтранса РФ, МВД РФ и ФСБ РФ от 05.03.2010 г. № 52/112/134. Угрозы персонала всегда вторичны, поскольку они возникают в результате противодействия угрозам нарушителя. В результате анализа модели нарушителя можно выделить определенные группы угроз безопасности аэропорта.

Обеспечение транспортной безопасности аэропорта связано с выстраиванием системы противодействия этим угрозам.

Персонал авиационной организации при реализации своей профессиональной функции находится в определенной ситуации, параметры которой определяются параметрами СЭП и параметрами реального алгоритма профессиональной деятельности конкретного специалиста. Угроза безопасности исследуемому объекту появляется в случае появления несоответствий между этими параметрами (Рисунок 5.5).

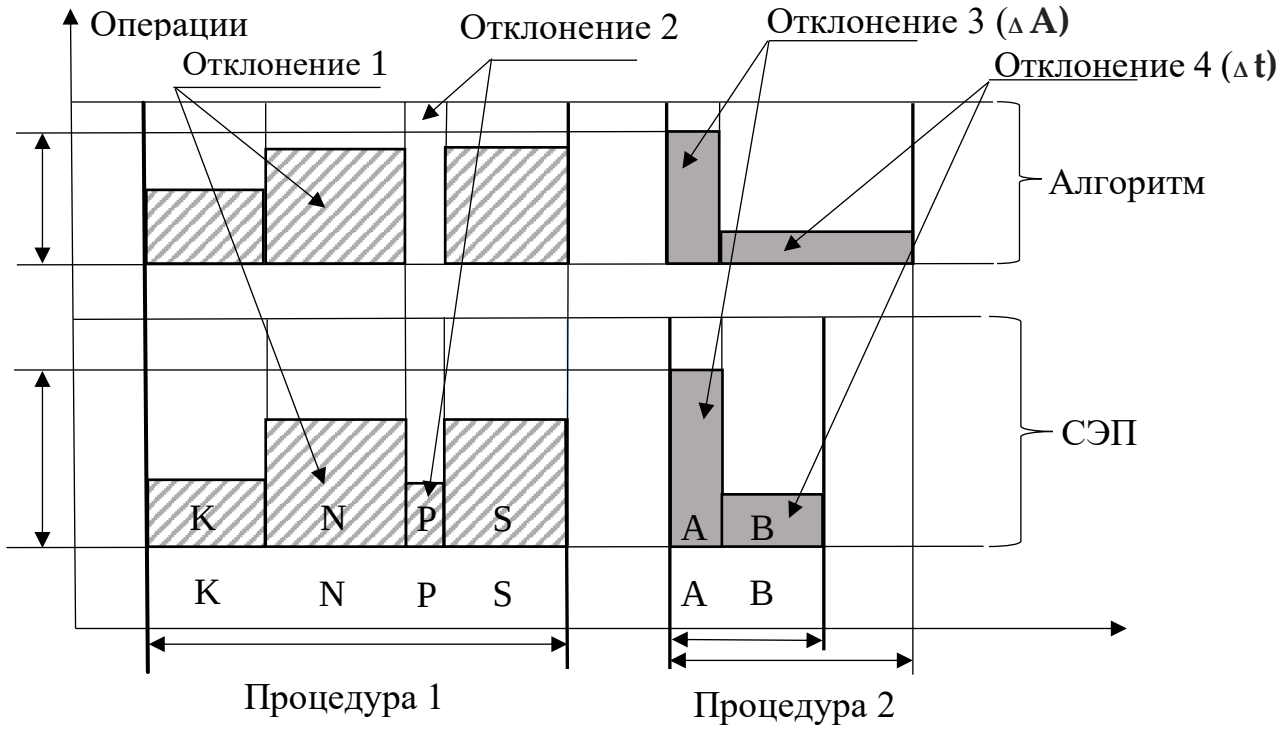


Рисунок 5.5 – Варианты отклонений алгоритма профессиональной деятельности персонала от СЭП

Заданный алгоритм профессиональной деятельности соответствует СЭП полностью, однако, реальное исполнение алгоритма сопровождается отклонениями. Типы отклонений алгоритма от СЭП достаточно многочисленны. Если операции K, N, P, S, A, B – в составе процедур 1 и 2, то отклонение 1 относится

к операции N и состоит в неполном составе выполняемых действий в алгоритме; отклонение 2 – пропуск операции Р в алгоритме; отклонение 3 – недостаточная величина воздействия А в алгоритме; отклонение 4 – операция В выполнена полностью, но за более длительное время. Подобных вариантов может быть много, поэтому вопрос мониторинга отклонений весьма важен.

5.2 Моделирование процедур минимизации несанкционированного вмешательства персонала

Система обеспечения транспортной безопасности ориентирована на исполнение своих функций по формуле: обнаружение-отражение-ликвидация. В штатном режиме, при отсутствии угроз безопасности объекта, система работает на предупреждение опасностей, выполняя заранее заданные алгоритмы. На этом этапе во всех случаях появления отклонений от заданных алгоритмов появляется нештатный (тревожный) сигнал, свидетельствующий о появлении особой ситуации в системе защиты объекта, которая может перейти в ситуацию отработки реальной угрозы безопасности. Наличие нештатного (тревожного) сигнала обуславливает последующую деятельность персонала ТБ (сил обеспечения транспортной безопасности) в условиях особой ситуации (Рисунок 5.6.).

Профессиональная деятельность персонала транспортной безопасности включает некоторую часть, которая названа несанкционированным вмешательством. Эта часть профессиональной деятельности не планируется, хотя и предполагается, и часто для самого специалиста является случайной. В любом случае это негативное воздействие на какие-то параметры объекта защиты, которое приводит к появлению нештатной ситуации и к формированию нештатного сигнала.

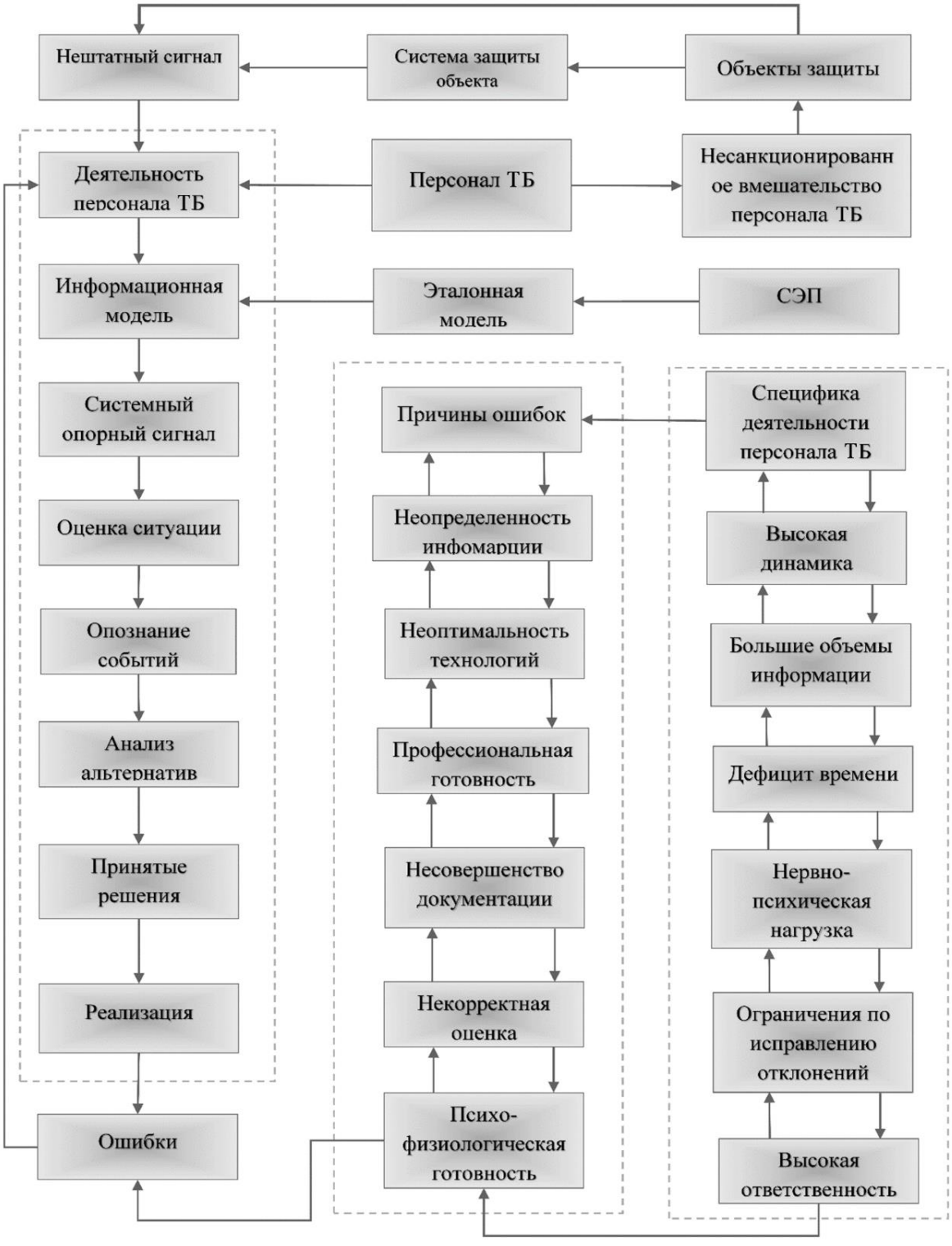


Рисунок 5.6 – Структура профессиональной деятельности

Задачей системы защиты объекта является, в том числе, отработка этого сигнала, в противном случае ситуация усложняется, что может привести к авиационному происшествию или акту незаконного вмешательства. Именно

поэтому несанкционированное вмешательство рассматривается как угроза безопасности.

Общую задачу можно сформулировать следующим образом: разработать рекомендации для персонала в структуре системы обеспечения транспортной безопасности, которые позволят парировать (перевести в штатную ситуацию) ошибки, допущенные при выполнении профессиональной деятельности, или, по крайней мере, их локализовать (не допустить развития).

Появление ошибки связано со спецификой деятельности персонала ТБ, которая определяется высокой динамикой в принятии решений; большими объемами перерабатываемой информации; существенным дефицитом времени в принятии решений и реализации производственных алгоритмов; наличием дополнительных нервно-психологических нагрузок, определяемых тяжестью последствий принятия неправомочного решения; ограниченными возможностями исправления ошибочных ситуаций; высокой ответственностью. Причины появления ошибок достаточно разнообразны. Это могут быть: неопределенность информации, не оптимальность используемых технологий, не полная профессиональная готовность, несовершенство документации, некорректная оценка ситуации, недостаточная психофизиологическая готовность. Вся эта специфика и причины, влияя на производственную деятельность, формируют ошибку.

Специфика определяет причины появления ошибок персонала ТБ, которые можно сгруппировать следующим образом: неопределенность информации, откуда вытекает не оптимальность используемых технологий и несовершенство документации, в этих условиях трудно получить корректную оценку ситуации. Кроме того, ошибки появляются как результат не достаточной профессиональной и психофизиологической готовностью персонала. В таком случае, профессиональная деятельность персонала априори включает некоторую, далеко не маленькую, совокупность ошибок, которые рассматриваются как несанкционированное вмешательство в процедуры защиты объекта и оказывают

негативное воздействие, приводящее к снижению уровня транспортной безопасности.

Представленный подход, основанный на гармонизации структур профессиональной деятельности специалистов ТБ и пилотов воздушных судов, дает возможность исследовать структуру ошибок и методы их минимизации.

Персонал, работающий в области транспортной безопасности, можно квалифицировать понятием специалист-оператор, который управляет по заданной программе сложной системой, осуществляет связь входной информации с выходом путем реализации отдельных операций, обладая правом принятия решений. Профессиональная деятельность специалиста-оператора характеризуется понятиями ошибка и погрешность. Отклонения регулируемых параметров от заданного значения в пределах допустимых ограничений являются погрешностью, за пределами ограничений – ошибкой.

Одним из эффективных инструментов исследования любой совокупности объектов и явлений является классификация. В отношении ошибок предложено достаточно большое количество различных классификаций. Ошибки делятся на систематические, обусловленные постоянными и одинаково действующими факторами, и случайные, возникающие под влиянием нестабильных факторов.

Первая классификация предложена П. Фиттсом и Р. Джонсом [233]. Она основана на следующих категориях: ошибки подмены, ошибки управления, ошибки памяти, ошибки перепутывания, ошибки внимания, ошибки ограничения. Указанные категории охватывают 86% идентифицированных ошибок. На этой основе В. Сиглтон [265] выделил причины таких ошибок: неадекватность предоставления, считывания и интерпретации информации, реверс направления движения, иллюзии, забывание. Дж. Рабидо [262] выделил ошибки моторики в простых и сложных действиях. Дж. Альтман [74] выделял ошибки профессиональной деятельности, ошибки коррекции, ошибки окружения (среды), личностные ошибки оператора. Он также предложил многопараметрическую оценку ошибок: обнаруживаемость, устраняемость, последствия и представлял

такую оценку в формате трехмерной матрицы. Известны и другие классификации, которые все вместе дают возможность, в сочетании с другими методами, количественного (параметрического) исследования ошибок. В результате исследования ошибок может быть сделан вывод о надежности человека – оператора. В гражданской авиации надежность оператора понимается как вероятность парирования некоторого воздействия, которая складывается из вероятностей безошибочного восприятия информации, ситуационной оценки, опознания воздействия, принятия решения, реализации решения.

Таким образом, в основе исследования человеческого фактора в гражданской авиации лежит ошибка авиационного персонала (персонала ТБ). Возникает вопрос о методах исследования [152].

Негативное влияние (воздействие) персонала на результаты выполнения процедур обеспечения транспортной безопасности проявляется как следствие совершения персоналом профессиональных ошибок. Минимизация негативного влияния связана, прежде всего, с «работой над ошибками», которая заключается в системном анализе функциональных характеристик ошибок, исследовании причин их появления, факторов, влияющих на эти причины, классификации и систематизации ошибок, разработке методов минимизации. Основная трудность состоит в том, что в транспортной безопасности количество типов ошибок достаточно велико, кластеризация связана с определенными трудностями выбора оснований для этого, также как с трудностями формализации и моделирования. В рамках поставленной цели даже элементарная классификация представляет собой не такую уж простую задачу. Поэтому разработка некоторого универсального метода минимизации негативного влияния представляется бесперспективной. Скорее всего, следует идти путем решения совокупности частных задач. Для начала, следует функционально определить характеристики ошибок и поставить им в соответствие факторы негативного влияния.

Ошибки (Ош1-ОшК) появляются в системе обеспечения транспортной безопасности (система защиты) в результате выполнения процедур по

нейтрализации внешних угроз (Y_1-Y_n) (Рисунок 5.7). Необходимо подчеркнуть, что это ошибки персонала, т.е. все другие ошибки, возникающие по иным причинам, здесь не рассматриваются. Каждой ошибке ставится в соответствие причина ее появления. Таких причин может быть достаточно много. На этом этапе выявляются параметры ошибок и экспертным путем оценивается степень их негативного влияния (НВ) на процессы обеспечения транспортной безопасности.

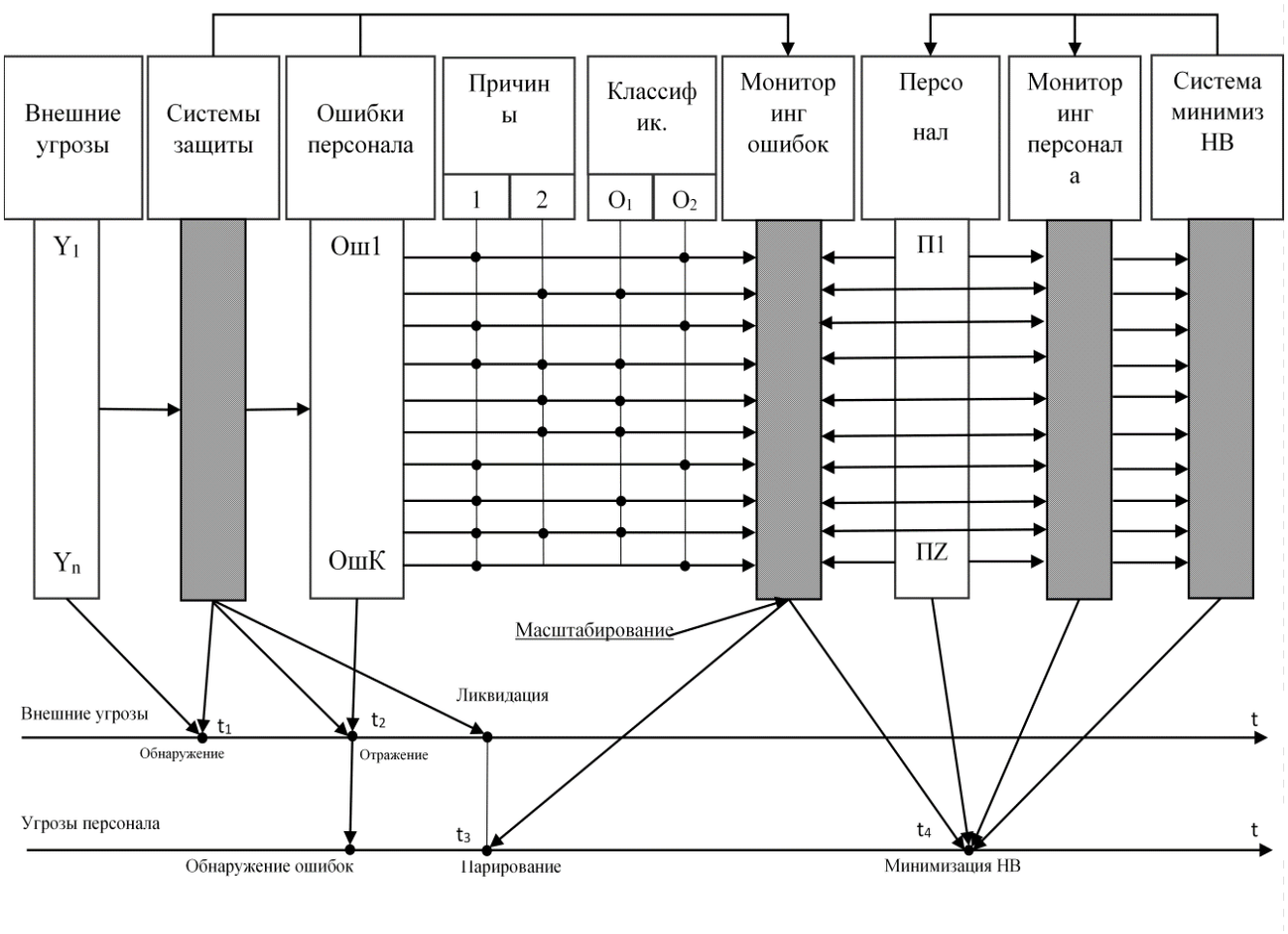


Рисунок 5.7 К вопросу о профессиональных ошибках персонала

Классификация необходима прежде всего для того, чтобы сгруппировать ошибки в несколько кластеров по некоторым основаниям. Предполагается, что для каждого кластера ошибок нужны свои методы минимизации их негативного воздействия. Анализ угроз и ошибок персонала при их нейтрализации показывает,

что иногда более эффективно решать обратную задачу, т.е. исходить из методов минимизации. Предлагается рассмотреть оба метода.

Ошибка специалиста появляется как результат отклонений от СЭП, т.е. не выполняется точно алгоритм, заложенный в СЭП. Такие ошибки можно назвать алгоритмическими, также, как и методы минимизации негативного влияния от таких ошибок персонала [202]. Отсюда, первым основанием для классификации ошибок O1 является алгоритмическое воздействие. При этом предполагается, что ликвидация ошибок (снижение степени их влияния) осуществляется путем вмешательства в соответствующие процедуры, т.е. тоже алгоритмически.

Причиной появления большинства ошибок, в том числе и алгоритмических, является недостаточный (неприемлемый) уровень профессиональной готовности авиационного персонала. По основанию O1 формируется кластер таких ошибок, ликвидация которых принципиально возможна алгоритмически. Если это невозможно или неэффективно, такие ошибки формируют второй кластер, основанием для чего является O2 – некомпетентное воздействие. Мониторинг ошибок осуществляется по двум кластерам, при этом каждой ошибке ставится в соответствие специалист (П1-ПZ), допустивший эту ошибку. Каждая ошибка масштабируется в соответствии с результатами моделирования несанкционированного вмешательства. Управление негативным влиянием авиационного персонала (персонала ТБ) осуществляется на основе компетентностной модели (Рисунок 5.8).

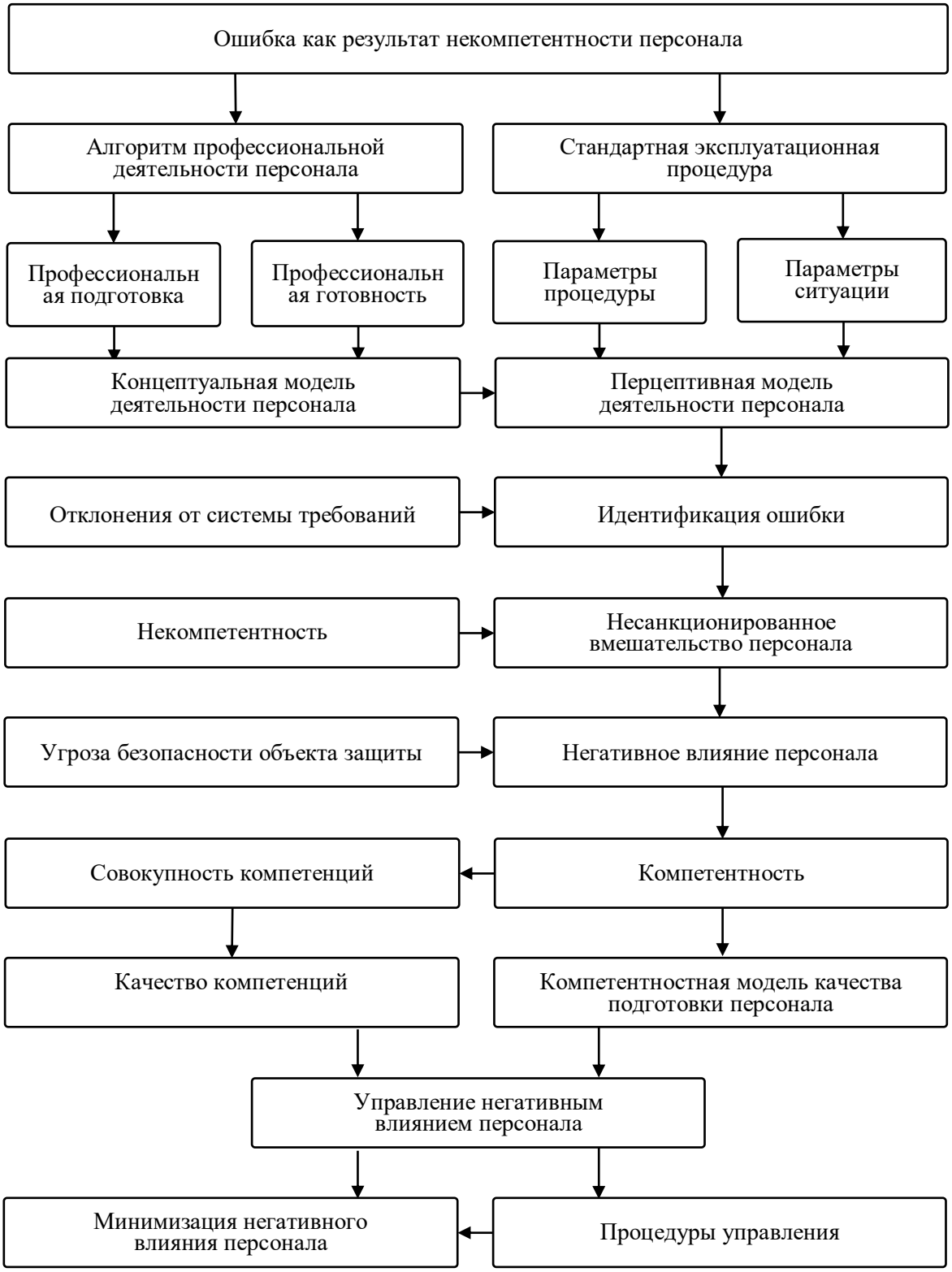


Рисунок 5.8 – Компетентностная модель управления негативным влиянием персонала на безопасность

Мониторинг персонала предполагает периодическую оценку уровня его профессиональной готовности к выполнению своих служебных обязанностей. Каждая ошибка выявляет снижение уровня и включает механизм компенсации этого снижения в системе минимизации негативного воздействия персонала.

Таким образом, предполагается два метода минимизации негативного влияния персонала на результаты обеспечения транспортной безопасности аэропорта: метод, основанный на алгоритмической коррекции допущенных ошибок, и метод коррекции уровня профессиональной готовности персонала к решению служебных задач.

Негативное влияние персонала транспортной безопасности проявляется в результате его некомпетентности как некоторая ошибка. Профессиональная деятельность персонала выстраивается в соответствии с требованиями стандартных эксплуатационных процедур (СЭП). Параметры СЭП задают параметры ситуации по управлению безопасностью, в результате чего формируется перцептивная модель деятельности персонала, т.е. модель требуемой деятельности. Персонал транспортной безопасности выстраивает алгоритм своей профессиональной деятельности в соответствии с уровнем профессиональной подготовки и в рамках того уровня профессиональной готовности, которым он обладает в данный момент времени.

На этой основе персонал формирует концептуальную модель своей деятельности. В процессе работы обе модели сравниваются и, при появлении расхождений, идентифицируется ошибка, которая квалифицируется как несанкционированное вмешательство в процедуры обеспечения транспортной безопасности и проявляется как негативное влияние персонала, что, в свою очередь, квалифицируется как угроза безопасности объекта защиты.

Оценка уровня негативного влияния персонала осуществляется путем исследования компетентности персонала через анализ совокупности компетенций в рамках модели качества подготовки персонала, а само качество компетенций становится параметром управления негативным влиянием.

Компетентностная модель оценки уровня профессиональной подготовки некоторого обобщенного специалиста в области транспортной безопасности может выглядеть следующим образом (Рисунок 5.9).

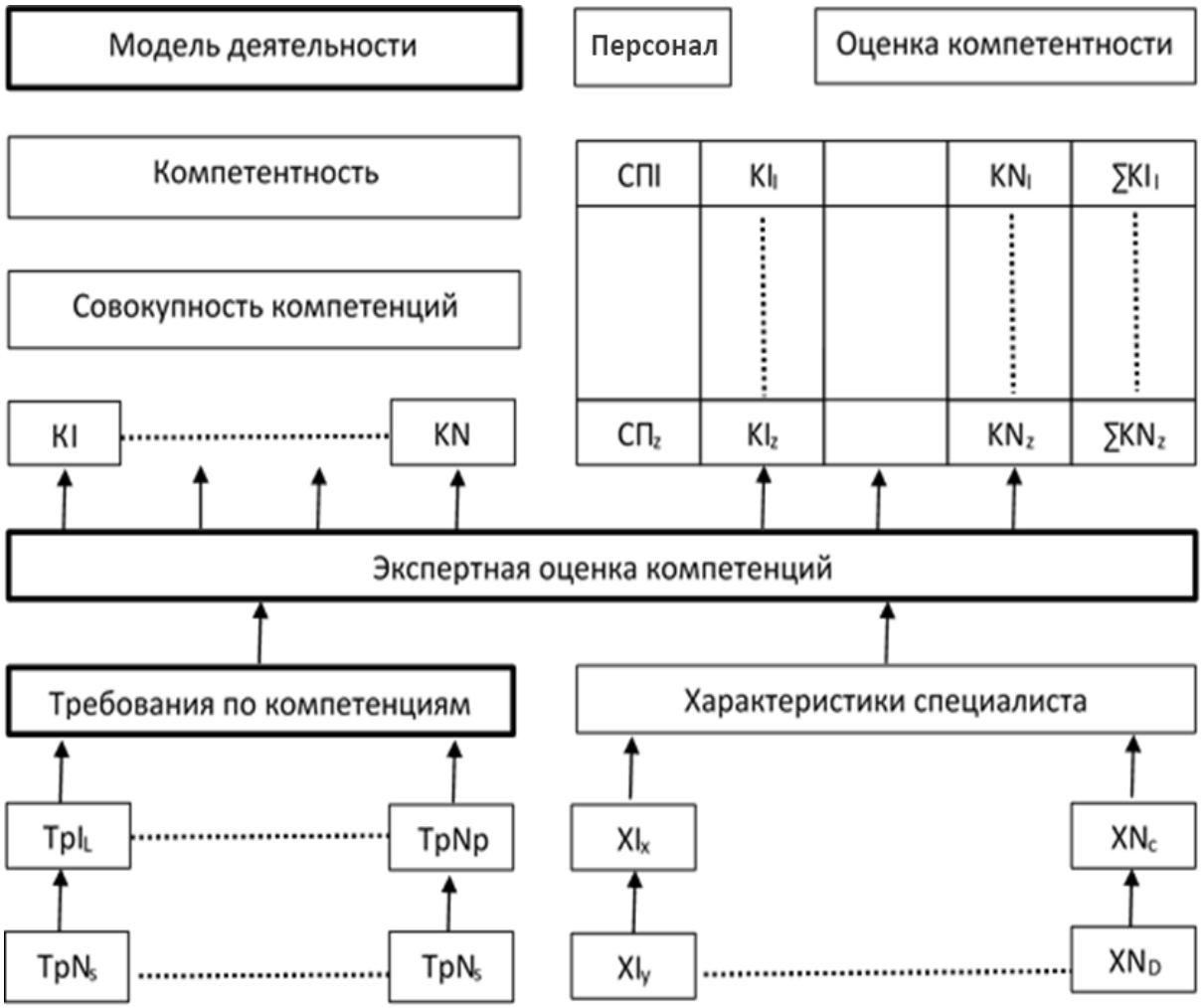


Рисунок 5.9 – Компетентностная модель оценки уровня профессиональной подготовки персонала

Каждая компетенция одновременно выступает как требование и как результат. Для представленного примера указанные требования можно найти в Национальной программе подготовки персонала в области транспортной безопасности [200].

На рисунке 5.9 K1-KN (К1-К10) – совокупность компетенций:

1. К1 – Правовые и нормативные акты по обеспечению ТБ.

2. К2 – Системы обеспечения ТБ.
3. К3 – Системы контроля доступа.
4. К4 – Технические средства и оборудование.
5. К5 – Регламент технического обслуживание ТС.
6. К6 – Методы досмотра и технологии.
7. К7 – Оценка террористической угрозы.
8. К8 – Контроль сопровождаемого багажа.
9. К9 – Умения и навыки выполнения процедур по обеспечению ТБ.
10. К10 – Охрана труда и пожарная безопасность.

Модель деятельности специалиста ТБ определяет область знания, в которой работает специалист, а компетентность отражает степень готовности специалиста к выполнению своих профессиональных обязанностей. Компетентность состоит из совокупности компетенций, каждая из которых относится к некоторой предметной области из области знания, определяемой компетентностью. Ответ на вопрос о готовности специалиста состоит в оценке компетенций, которая осуществляется экспертным путем.

Здесь компетенция выступает как результат. Чтобы его получить компетенция рассматривается как требование. Процедура состоит из следующих этапов: для каждой компетенции вырабатываются соответствующие требования, для К1 – Тр1l……..Тр1m, и т.д., для KN – TpNp…….TpNs. Каждому требованию ставится в соответствие характеристика специалиста, отвечающая этому требованию, и отражающая уровень его подготовленности по данному требованию. Экспертным путем оценивается степень соответствия требования и характеристики и в выбранной шкале ставится количественная оценка. Экспертные методы могут быть реализованы путем тестирования, вопросов – ответов, совокупности заданий и т.д. Полученная оценка есть количественное отображение степени подготовленности данного специалиста (СП) по данной компетенции как результат ее освоения. Эта процедура повторяется для каждого специалиста, т.е. по каждому специалисту из совокупности СП1 – СПz получаем набор оценок К1 – KN.

Экспертная оценка компетентности представляет собой или сумму оценок компетенций специалиста, или среднюю величину этих оценок. Такая оценка компетентности характерна для первичной подготовки специалистов и далеко не всегда отражает его действительный уровень готовности к выполнению своей профессиональной функции. Поскольку ставится задача определения гарантированного уровня подготовки и допуска специалиста к работе, необходимы более тонкие методы оценки этого уровня.

Показанные примеры достаточно примитивны и не удовлетворяют требованиям, предъявляемым к системам аттестации и сертификации персонала транспортной безопасности. Альтернативой является совокупность более сложных правил анализа экспертных оценок, один из вариантов которой представлен ниже.

Специалист в области транспортной безопасности при оценке его уровня готовности в рамках аттестации или сертификации не должен допускаться к выполнению своих служебных обязанностей, если имеет место быть хотя бы один из результатов, обусловленных следующими правилами:

– квалиметрическая оценка компетентности не должна быть ниже установленного нормативного значения;

– оценка по любой компетенции не должна быть ниже 5 баллов;

– оценка по компетенции К2 не должна быть ниже 1 балла;

– сумма оценок по К5 и К8 не должна быть меньше 13 баллов;

– разница между оценками К3 и К6 не должна превышать 1 балл;

– совместно выполняется условие: сумма К3 и К7 должна быть не меньше 11, а К4 – не ниже 7.

Все эти правила однозначно связаны с содержанием компетенций и отражают требования к ним по уровню усвоения. Возможны другие правила, отслеживающие динамику изменений в требованиях.

Квалиметрическая оценка компетентности вычисляется следующим образом:

$$Ккв = а*К1 + б*К2 + в*К3 + г*К4 + д*К5 + е*К6 + ж*К7 + з*К8 + и*К9 + к*К10,$$

где а,б,в,г,д,е,ж,з,и,к – весовые коэффициенты, отражающие значимость каждой компетенции в составе компетентности и связанные между собой правилом нормировки: а+б+в+г+д+е+ж+з+и+к = 1.

В большинстве случаев оценка компетентности на уровне компетенций далеко не всегда эффективна, поскольку компетенция по своему содержанию может охватывать весьма обширную область знаний и количество требований к такой компетенции может быть очень велико, что существенно усложняет экспертную оценку, в результате чего точность оценки заметно снижается и может быть ниже допустимой. В таком случае необходимо использовать квалиметрические процедуры [116], когда каждая компетенция структурируется и представляется иерархическим набором более простых элементов, которые собираются (комплексируются) по квалиметрической формуле, представленной выше, и правилу нормировки. В этом случае количество требований, приходящихся на каждый элемент компетенций может быть снижено до минимального, что упрощает работу эксперта и повышает точность экспертного оценивания.

Любые подобные правила достаточно просто описываются в терминах алгебры логики и алгоритмизируются, что позволяет использовать их в автоматизированном режиме. Алгоритм отражает две возможности оценки готовности специалиста к выполнению своих профессиональных функций: по компетенциям и по компетентности.

Квалиметрическая оценка компетентности (КК) сравнивается с нормативным значением, которое должно быть заранее определено и утверждено в установленном порядке. Если оценка приемлема, специалист продолжает работу, если нет – принимается соответствующее решение.

Наиболее эффективным методом оценки качества подготовки персонала является метод классификации с использованием нейросетей. Результаты такого исследования представлены в подразделе 5.4.

5.3 Информационное управление негативным влиянием персонала

Уровень транспортной безопасности аэропорта представляет собой количественное отображение риска проявления некоторого негативного события. Риск можно оценить через вероятность события и тяжесть последствий его проявления, т.е. в цифре. Уровень ТБ оценивается, также, через уязвимость объекта защиты, т.е. вопрос о количественной оценке уровня безопасности, в принципе, решен.

Уровень транспортной безопасности объекта защиты устанавливается в результате противостояния пространства угроз безопасности и пространства защиты объекта. Приемлемый (устанавливаемый) уровень определяется как результат деятельности подразделения транспортной безопасности аэропорта, включая персонал этой службы. Если персонал в своей профессиональной деятельности совершает ошибку, т.е. допускает несанкционированное действие, уровень транспортной безопасности снижается, поскольку увеличивается риск проявления негативного события. Здесь следует уточнить, что сама по себе ошибка персонала – это еще не факт реализации некоторой угрозы, это факт изменения ситуации в системе защиты объекта, допускающий возможность совершения противоправных действий. Таким образом, каждая ошибка персонала ТБ непосредственно влияет на уровень транспортной безопасности аэропорта.

Принципы информационного управления уровнем несанкционированным вмешательством персонала основаны на принципах управления ЧФ:

1. Безопасность воздушного транспорта рассматривается как интегральная категория, занимающаяся исследованиями различных аспектов такой наукоемкой отрасли как гражданская авиация. Конечной целью этих исследований является приемлемый уровень безопасности личности. Задача управления уровнем несанкционированного вмешательства персонала должна решаться с учетом личностного фактора.

2. Уровень несанкционированного вмешательства персонала отражает часть его профессиональной деятельности, не обусловленную соответствующими нормативными документами. Однако, это не означает, что все несанкционированные действия персонала имеют негативные последствия. Положительный результат профессиональной деятельности рассматривается как соответствие этой деятельности заданным требованиям. Уровень негативного влияния персонала определяется степенью отклонений в процессе его профессиональной деятельности от заданных требований. В таком случае, количественной характеристикой уровня негативного влияния персонала становится качество его профессиональной деятельности, что превращает качество в критерий оптимизации уровня негативного влияния персонала.

3. Система управления уровнем несанкционированного вмешательства персонала не может быть создана как самостоятельная, автономная структура, поскольку несанкционированное вмешательство есть определенная часть общей профессиональной деятельности персонала по обеспечению транспортной безопасности. Целевая функция системы управления состоит в выявлении и идентификации той части деятельности, которая рассматривается как вмешательство. В таком случае, система управления несанкционированным вмешательством должна быть встроена в систему более высокого уровня, занимающуюся обеспечением транспортной безопасности аэропорта.

4. Несанкционированное вмешательство проявляется как ошибка персонала в процессе профессиональной деятельности. Все процедуры в системе несанкционированного вмешательства связаны с операциями по отработке идентифицированной ошибки: парированием (приведением ситуации в системе в штатный режим) или локализацией (исключением негативного развития событий). Идентификация ошибки связана со сравнением параметров в заданном и реализованном режимах, фиксацией отклонений, анализом и категорированием ошибки, включением процедур парирования и локализации.

5. Все процедуры, связанные с профессиональной деятельностью специалиста – оператора, основаны на понятии компетентность. В системе управления несанкционированным вмешательством персонала важнейшим свойством компетентности является ее дуальность: компетенция одновременно может быть представлена как требования к уровню профессиональной готовности персонала и как результат достижения этого уровня в формате знаний, умений и навыков. Качество компетенции понимается как степень соответствия уровня готовности персонала по данному предметному вопросу требованиям, которые предъявляются к персоналу по этому вопросу для выполнения профессиональной деятельности. Компетентность специалиста складывается из совокупности компетенций.

6. Несанкционированное вмешательство персонала рассматривается как угроза безопасности аэропорта, т.е. угроза персонала ассоциируется с негативным влиянием персонала и сопоставляется с внешними угрозами безопасности объекта защиты. Однако, если внешние угрозы при своей реализации становятся субъектами прямого действия, то угрозы персонала прямого действия не имеют. Ошибка персонала, как основной элемент угрозы, изменяет процедуру защиты объекта, тем самым изменяя ситуацию в системе защиты объекта, снижает качество защиты и снижает уровень безопасности. Исследование внешних угроз возможно путем их представления в формате гипотетических полей и с использованием методов математического моделирования. Такой подход к исследованию угроз персонала невозможен, поэтому необходимы эвристические методы и теория принятия решений.

7. В современных системах безопасности факт негативного влияния человеческого фактора признается и на этой основе ставится задача минимизации доли человеческого участия в управлении процессами безопасности. Такую задачу можно решать только с учетом следующих обстоятельств:

– полное исключение человека из контура управления в системе безопасности даже теоретически невозможно, поскольку всегда остается некоторая

совокупность операций, которые человек выполняет лучше или которые вообще не поддаются автоматизации;

– существует некоторый приемлемый уровень автоматизации процедур управления в системе безопасности, определяющий баланс между человеческой и технической компонентами, однако, эффективных методов вычисления этого баланса не существует. Задача решается путем исключения человека там, где это удается сделать, часто в ущерб эффективности и оптимальности процедур;

– негативное влияние человека в подавляющем большинстве случаев проявляется как ошибка, которая представляет собой случайную величину в условиях существенной неопределенности. Решение каких-то прогнозных задач, связанных с человеком, в этих условиях весьма затруднительно, поскольку эти задачи являются плохо формализуемыми и слабо структурированными.

Отсюда следует, что задача минимизации человеческого фактора должна быть преобразована в задачу управления и поддержания приемлемого уровня негативного влияния персонала.

Задача оптимизации процедур профессиональной деятельности персонала в области транспортной безопасности состоит в разработке некоторой структуры, представляющей собой совокупность организационных и программно-технических средств, обеспечивающих минимизацию негативного влияния персонала на уровень транспортной безопасности. Негативное влияние персонала проявляется в результате появления ошибок при реализации целевого функционала его деятельности, т.е. ошибки следует рассматривать как составную часть основной деятельности персонала по обеспечению транспортной безопасности. В таком случае, система минимизации негативного влияния персонала должна осуществлять функции по мониторингу, обнаружению, идентификации, анализу ошибок персонала и принимать соответствующие решения по парированию и локализации ошибок. Парировать здесь понимается как перевести процесс выполнения соответствующей процедуры в штатную ситуацию, а локализовать означает не допустить негативного развития событий. Функциональная модель

минимизации несанкционированного вмешательства персонала транспортной безопасности представлена на рисунке 5.10.

Система обеспечения транспортной безопасности противостоит внешним угрозам со стороны субъекта противоправной деятельности, направленным на объект защиты (в частности аэропорт). Угрозы персонала ТБ суммируются с внешними угрозами, поскольку они появляются в результате выполнения процедур обеспечения транспортной безопасности.

Рисунок 5.10 – Функциональная модель минимизации несанкционированного вмешательства персонала

В данной работе разрабатываемая система минимизации негативного влияния персонала (СМНВП) ориентирована на использование одной из лучших

отечественных систем безопасности технологической платформы ESM (Electronica Security Manager), [103; 118].

В ESM реализован диалоговый режим, когда персонал ТБ принимает непосредственное участие в процедурах отработки инцидентов в рамках своей должностной инструкции или, в формате специалиста-оператора, выполняя заданный алгоритм в диалоге с системой. При этом алгоритм профессиональной деятельности персонала ТБ сформирован и жестко прописан в стандартных эксплуатационных процедурах. Предполагается, что СЭП гармонизированы с алгоритмами отработки инцидентов в ESM. Любое отклонение как от СЭП, так и от алгоритма ESM, есть ошибка персонала.

Ошибка персонала ТБ рассматривается как несанкционированное (незаконное) вмешательство в процедуры обеспечения транспортной безопасности аэропорта, результат которого является угрозой безопасности и в особых случаях приравнивается к АНВ. В таком случае важнейшей задачей становится мониторинг ошибок, реализуемый в СМНВП. Мониторинг основан на постоянном отслеживании любых отклонений (несоответствий) от СЭП и алгоритмов СМНВП, обнаружении ошибок, их идентификации и анализе. Система включает режим парирования ошибок и, если результат не обеспечивает приемлемый уровень безопасности, включается режим локализации ошибок, который окончательно решает задачу минимизации негативного влияния персонала.

Важно понимать, что в СМВНП решается задача, принципиально отличающаяся от задачи минимизации человеческого фактора. Минимизация ЧФ состоит в постепенном свертывании отдельных функций по обеспечению ТБ человеческой компоненты в эргатической системе безопасности и возложении этих функций на техническую компоненту. Минимизация несанкционированного вмешательства персонала не связана с объемом участия человека в процессе, а представляет собой автоматизированную процедуру управления уровнем этого вмешательства.

Структура и основные функции ESM и СМВНП представлены в модели на рисунке 5.11. Подсистемы СМВНП решают следующие задачи:

– A – конфигурирование оборудования;
– B – управление базами данных;
– C – сбор, обработка и анализ информации;
– D – обеспечение пользовательских интерфейсов;
– E – защита информации и разделение доступа к ней;
– F – управление подсистемами безопасности;
– G – интеграция с информационными системами управления.

В решении этих задач в диалоговом режиме принимает участие авиационный персонал, выполняющий роль специалиста-оператора K_1-Kn.

Особо важную роль играет персонал при реализации в системе инцидентного управления, при этом решаются следующие задачи:

1. регистрация события и видеозапись,
2. открытие инцидента,
3. формирование сигнала тревоги,
4. анализ событий и ситуации,
5. идентификация инцидента и проверка,
6. активизация средств защиты,
7. фиксация события,
8. включение процедур отражения,
9. оповещение,
10. включение процедур управления инцидентом,
11. включение процедур ликвидации и завершения инцидента.

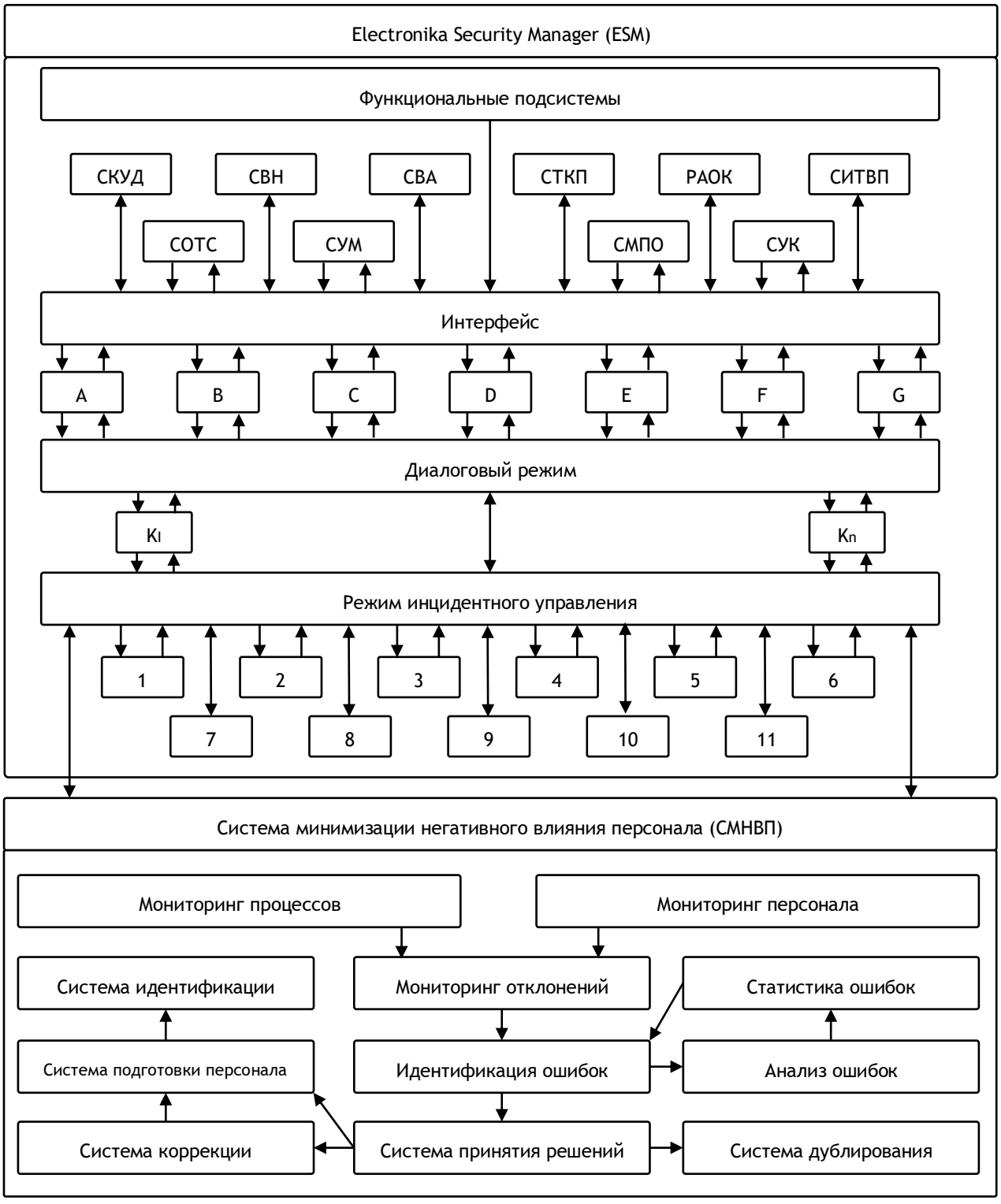


Рисунок 5.11 – Структурно-логическая модель системы минимизации негативного влияния персонала

На любом этапе взаимодействия авиационного персонала с ESM в диалоге возникают ошибки, которые фиксируются и передаются в систему минимизации негативного влияния персонала (СМНВП) [121].

Функциональная деятельность системы ESM основана на логической совокупности алгоритмических последовательностей, отображающих сложные процессы и процедуры обнаружения и ликвидации негативных событий. Функциональная деятельность системы СМНВП ориентирована на этот же принцип, поскольку все процедуры, включенные в ее функционал, однозначно связаны с процедурами ESM и реализуются в рамках инцидентного управления.

Управление транспортной безопасностью в ESM осуществляется через инцидент, т.е. через некоторое проявление угрозы. Поскольку персонал транспортной безопасности является одним из важнейших элементов обеспечения безопасности, его негативное влияние проявляется при отработке системой последовательности инцидентов. В таком случае, в системе СМНВП решается задача по управлению персоналом таким образом, чтобы исключить это негативное воздействие для чего осуществляется перестройка или алгоритмов работы персонала и технических средств, или коррекция уровня профессиональной готовности персонала к выполнению своих функций.

СМВНП работает в двух режимах – в штатном режиме и в режиме инцидента. В штатном режиме персонал отрабатывает свои алгоритмы по заранее разработанному сценарию, не предполагающему внешнее вмешательство. Тогда любая ошибка персонала связана с недостаточным уровнем профессиональной готовности специалиста.

Мониторинг ошибок персонала в СМНВП осуществляется постоянно и в реальном масштабе времени. Прежде всего реализуется мониторинг процессов обеспечения транспортной безопасности в ESM. Как в штатном режиме, так и в режиме инцидента, система следит за соответствием параметров алгоритмов работы ESM проектным значениям, тем самым подтверждая легитимность действий системы. Параллельно в этих же режимах осуществляется мониторинг

профессиональных действий персонала, подтверждающий адекватность реализуемых процедур параметрам проектного алгоритма деятельности специалиста (СЭП). Важнейшим в системе мониторинга является мониторинг отклонений, сравнивающий между собой параметры двух, указанных выше, алгоритмов и фиксирующий любые обнаруженные разночтения, что свидетельствует о появлении ошибки персонала или, что значительно реже, сбоя в системе технических средств. Завершением мониторинга является идентификация ошибки, которая состоит в определении ее параметров по определенному стандарту [75; 103; 122].

Система анализа работает в контакте с системой статистики, в которой хранятся данные о ранее совершенных ошибках и вновь поступающих.

Система приятия решений выбирает процедуры, которые должны обеспечить минимальный ущерб для безопасности по каждой ошибке персонала. Процедуры могут быть полностью автоматизированные или эргатические, т.е. выполняемые с участием человека. В системе приняты три уровня значимости ошибки по степени ее негативного влияния на безопасность:

1. минимальный, когда ошибка не меняет ситуацию в системе защиты объекта, негативное влияние не проявляется. Ошибка фиксируется в системе статистики, но не требует действий по ее нейтрализации, т.е. уровень негативного влияния приемлем;

2. значительный, когда ошибка изменяет ситуацию в системе защиты, в результате чего снижается уровень транспортной безопасности, вероятность негативных событий и негативных последствий увеличивается, т.е. ошибка классифицируется как незаконное вмешательство в деятельность по обеспечению транспортной безопасности. В этом случае включается режим парирования ошибки, в котором есть две альтернативы: дублирование и коррекция. Если ошибка возникла по вине программно-технических средств, т.е. произошел технический сбой под воздействием несанкционированных действий персонала, подключаются процедуры дублирования данного участка алгоритма отработки инцидента или

подпрограмма коррекции ошибки, которые выполняются в автоматизированном режиме. Если ошибка в действиях персонала, включается процедура коррекции его действий;

3. опасный, когда ошибка приводит к ситуации, в которой инцидент развивается крайне негативно и отражение угрозы аэропорту становится проблематичным. Это означает, что специалист-оператор не способен справится с ситуацией и самостоятельно парировать совершенную ошибку. В этом случае система включает процедуру дублирования, т.е. специалист отстраняется от работы и заменяется другим специалистом. По отношению к нарушителю система переходит в режим локализации ошибки, а специалист направляется в систему переподготовки персонала. В данном случае система выходит из режима реального времени, а специалист допускается к работе только после подтверждения его профессионального уровня в системе сертификации.

5.4 Разработка нейросетевого классификатора персонала по критерию профессиональной готовности

Ранее было показано, что одной из важнейших задач работы с персоналом транспортной безопасности является получение полной уверенности в приемлемом уровне его готовности к выполнению профессиональных функций, которая должна обеспечить безошибочность его работы и, следовательно, минимальный уровень негативного влияния на процедуры обеспечения транспортной безопасности. Одним из важнейших факторов такой готовности является уровень профессиональной подготовки персонала. Были исследованы различные подходы к оценке этого уровня (подраздел 5.2) и установлено, что одним из самых эффективных методов оценки следует считать нейросетевую классификацию.

Оценка уровня готовности должна дать ответ на вопрос кто из специалистов способен выполнить свою целевую функцию с минимальными ошибками. Любые формальные методы, включая тестирование, не способны дать ответ на этот

вопрос, поскольку задача многокритериальна и, практически, не формализуема. Дело в том, что здесь формальные правила оценки недостаточны. Можно сравнить процедуры тестирования с помощью программных средств и непосредственно опытным преподавателем. Преподаватель при оценке включает весь свой опыт и интуицию. В процессе тестирования при собеседовании преподаватель отлавливает такие нюансы, которые невозможно выявить из ответов на тестовые задания. Поэтому вполне обычна ситуация, когда преподавать положительно оценивает результат при явно неудовлетворительных оценках теста и, наоборот, при положительных оценках теста преподаватель делает вывод о неготовности специалиста. Нейросетевая классификация персонала способна именно так решать эту задачу.

Решение скрыто в процедуре обучения сети. При наличии достаточного количества цифровых исходных данных с оценками уровня профессиональной подготовки персонала сеть обучается так и до тех пор, пока ответ классификатора будет соответствовать требованиям.

Прежде чем строить нейронную сеть, необходимо сформировать *обучающую выборку* (learning set, training set). Это множество обучающих примеров (learning sample, training sample), содержащих признаки (feature), описывающие отдельные объекты, и целевые переменные, метки (target). Для решаемой задачи признаки должны характеризовать степень готовности специалистов к выполнению своих функций, а целевое значение – итоговая оценка годности специалиста.

При подготовке данных для обучения нейронных сетей выделяют три основные задачи: конструирование признаков; отбор признаков; преобразование признаков.

Конструирование признаков – это выбор признаков предметной области. Для оценки уровня готовности персонала транспортной безопасности к выполнению профессиональной деятельности выбрана система компетенций и проверяемых требований (подраздел 5.2). Перечень компетенций (К) и требований имеет следующий вид (фрагмент):

1. **К1 – Правовые и нормативные акты по обеспечению ТБ**
2. **К2 – Системы обеспечения ТБ**

Т2-1 Основные понятия, цель и основы обеспечения ТБ.

Т2-2 Состояние ТБ в ГА. Административно-организационные аспекты.

Т2-3 Полномочия, роль и обязанности работников САБ. Организация работы САБ. Организационно-распорядительные документы.

Т2-4 Система управления обеспечением ТБ. Концепции обеспечения ТБ.

Т2-5 Обеспечение ТБ при наземном обслуживании ВС.

3. **К3 – Системы контроля доступа**

Т3-1 Организация пропускного и внутриобъектового режимов.

Т3-2 Конфигурация аэропорта и охраняемые зоны ограниченного доступа.

Т3-3 Меры ТБ в пределах контролируемой и неконтролируемой зоны. Контроль доступа к ВС.

4. **К4 – Технические средства и оборудование**
5. **К5 – Методы досмотра и технологии**

Т5-1 Предметы и вещества, запрещенные и (или) ограниченные к перемещению в контролируемую зону.

Т5-2 Организация досмотра персонала, посетителей и ТС.

Т5-3 Правила проведения предполетного и послеполетного досмотров.

Т5-4 Досмотр пассажиров с использованием ТС. Контактный метод досмотра.

Т5-5 Досмотр багажа и ручной клади с помощью рентгено-телевизионной системы безопасности (интроскопа).

Т5-6 Метод наблюдения и опроса (профайлинг).

6. **К6 – Оценка террористической угрозы**

Т6-1 Общие сведения о терроризме и АНВ. Общие сведения о ВУ, ВВ, оружие и боеприпасах. Обнаружение, опознавание, сокрытие.

Т6-2 Угрозы в деятельности ГА. Характеристики нарушителей. Психология поведения нарушителей.

Т6-3 Особенности кризисных ситуаций. Определение степени серьезности происшествия

7. К7 – Умения и навыки выполнения процедур по обеспечению ТБ

Т7-1 Порядок действия САБ в нестандартных ситуациях.

Т7-2 Программа противодействия АНВ.

Т7-3 Меры охраны и защиты ВС на земле. Порядок проведения досмотра ВС на земле.

Т7-4 Контроль за выполнением технологических процессов обеспечения ТБ.

Т7-5 Управление кризисными ситуациями. Навыки решения конфликтных ситуаций.

Т7-6 Методы проведения аудиторских и инспекционных проверок.

Т7-7 Нормы, правила и процедуры обеспечения ТБ.

Эксперт, проверяющий сотрудников, по каждому требованию каждой компетенции выставляет баллы по десятибалльной шкале. Также выставляется итоговая оценка готовности специалиста выполнять свои обязанности. Итоговая оценка не определяется суммой баллов, минимальным баллом и т.п. Оценка учитывает важность компетенции, общее впечатление эксперта от ответов и другие факторы.

Столбцы таблицы – это значения признаков. Каждая строка таблицы описывает результат проверки одного специалиста. "Отсев" в результатах проверки означает, что данный специалист не готов исполнять обязанности на конкретном рабочем месте.

Отбор признаков – это выбор признаков, оказывающих наибольшее влияние на результат. Так как в нашем случае необходимо проверить все компетенции специалиста, то отбор признаков не производится.

Преобразование признаков включает:

– обработку аномальных значений, противоречий и дубликатов;
– восстановление пропущенных значений;
– преобразование данных.

Исходными данными являются экспертные оценки по результатам тестирования специалистов. Набор тестов фиксированный. По результатам каждого теста должен быть зафиксирован результат. Экспертная оценка может лежать в диапазоне от 0 до 10, что несложно проверить в программе фиксации результатов тестирования. Поэтому, в обучающей выборке отсутствуют аномальные значения, противоречия, дубликаты и пропущенные значения.

Преобразование (трансформация) данных заключается в кодировании данных и масштабировании – приведению к определенному диапазону. Нейронные сети работают только с числами, так как их работа основана на арифметических операциях взвешенной суммы. Поэтому все входные и выходные данные нейронной сети должны быть закодированы в виде чисел. Наш набор данных содержит признаки в виде чисел, которые не надо кодировать, и бинарные целевые значения: "годен" и "отсев". Закодируем значение "годен" единицей, а "отсев" – нулем. Масштабирование данных означает приведение всех признаков к одному диапазону, так, чтобы максимальные значения признаков не превышали 1. Признаки масштабируются независимо друг от друга. Используем линейное масштабирование (нормализацию)

$$p_{ij} = \frac{\left(x_{ij} - x_{j\min}\right)(b-a)}{x_{j\max} - x_{j\min}} + a$$

где p_{ij} – нормализованное значение j-го признака в i-ом примере, x_{ij} – исходное значение j-го признака в i-ом примере, $[a,b]$ – допустимый диапазон изменения нормализованных признаков, определяемый диапазоном изменения выходных сигналов нейронов входного слоя сети, $\left[x_{j\min}, x_{j\max}\right]$ – диапазон изменения исходных значений j-го признака.

В системе MATLAB нейроны входного слоя используют функцию активации гиперболический тангенс, для которого $a=-1$, $b=1$. Для системы оценок $x_{j\min}=0$, $x_{j\max}=10$. Например, признак $x_{ij}=4$ (приложение Г). Тогда масштабированное значение признака равно

$$p_{ij} = \frac{(4-0)(1+1)}{10-0} - 1 = 0{,}8 - 1 = -0{,}2\,.$$

В системе MATLAB при использовании тулбокса (пакета) Deep Learning Toolbox [39] преобразование производится автоматически, поэтому нет необходимости в явном преобразовании.

Демонстрационный вариант нейронной сети разрабатывался в системе MATLAB R2019b с использованием инструмента визуального программирования Neural Network Pattern Recognition App пакета Deep Learning Toolbox системы MATLAB. Средства управления представляют собой кнопки и соответствующие окна (Рисунки 5.12 – 5.14).

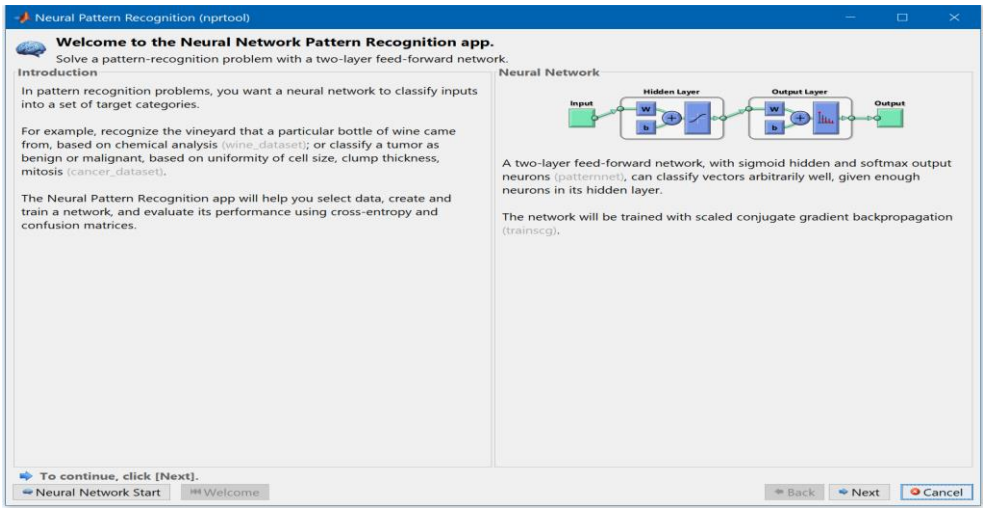


Рисунок 5.12 – Управляющие окна. Начало

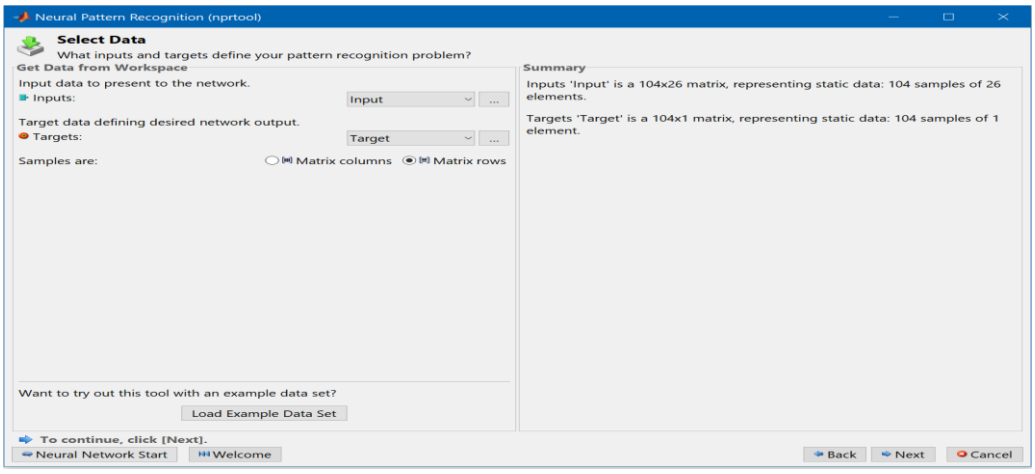


Рисунок 5.13 – Управляющие окна. Выбор данных

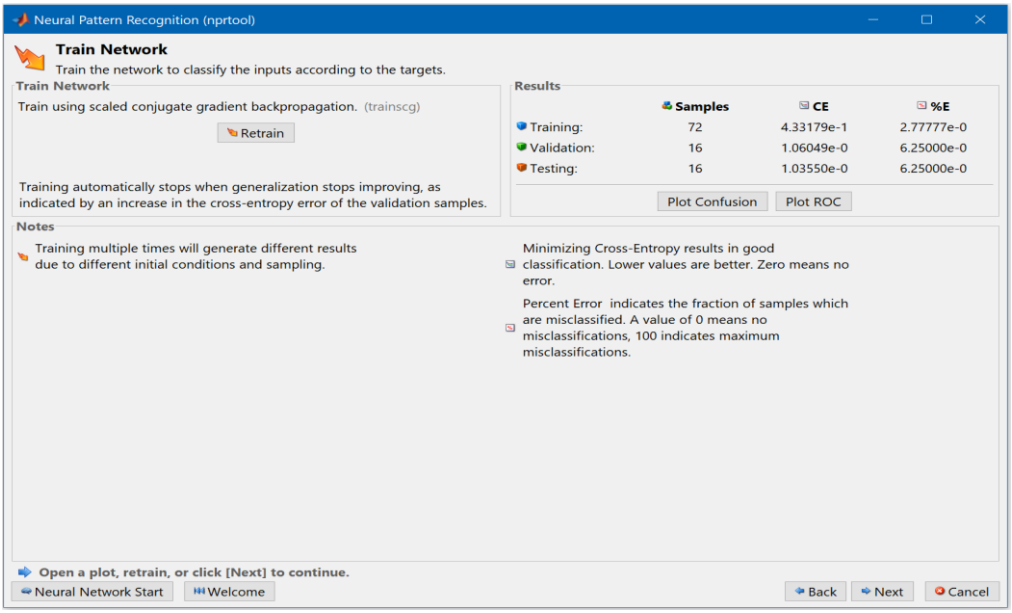


Рисунок 5.14 – Управляющие окна. Завершение обучения

Было подготовлено два текстовых массива: массив признаков **Input** и массив целевых значений **Target**. Массив **Input** получен из части таблицы исходных данных (приложение Г), содержащей признаки без "шапки" путем преобразования в текстовый файл. Массив **Target** содержит столбец целевых значений в текстовой форме. Стартовое окно инструмента после открытия в программе меню Apps / Neural Net Pattern Recognition представлено на рисунке 5.12. Используем **Next** и открываем окно выбора данных **Select Data** (Рисунок 5.13).

В качестве входных данных (Inputs) выбираем массив **Input**, в качестве целевых значений (Targets) – массив **Target.** Массивы загружаются стандартными для MATLAB средствами. Так как обучающие примеры представляют строки массивов, то из радиокнопок **Samples are**: необходимо выбрать **Matrix rows.**

Используя соответствующие кнопки и окна, распределяем набор данных, выбираем архитектуру сети, методы и алгоритм обучения сети.

В окне процесса обучения представлена основная информация о процессе обучения: способ разделения исходного обучающего множества – случайный (Random), обучающий алгоритм – масштабированный метод сопряженных

градиентов (Scaled Conjugate Gradient), функция ошибок – кросс-энтропия (Cross-Entropy) и реализация вычислений MEX или MATLAB executable – для ускорения вычислений вызываются скомпилированные функции языка C++. В окне выводятся также характеристики процесса обучения: количество эпох, время обучения, значения функционала ошибки и градиента функционала ошибки на последней эпохе и число проверок достоверности – количество последовательных итераций, при которых производительность проверки не уменьшается. Имеется ряд кнопок, позволяющих выводить различные графики.

Окно обучения сети после завершения обучения (Рисунок 5.14) изменилось. Стала доступна кнопка повторного обучения **Retrain**. Так как начальные значения весов сети вычисляются случайным образом и примеры по наборам распределяются случайно, то повторное обучение даст разные результаты. Поэтому, при неудовлетворительной точности классификации можно многократно повторять обучение, нажимая кнопку **Retrain**.

Можно вернуться к более ранним шагам обучения и изменить, например, число нейронов в скрытом слое. В окне обучения также видны значения кросс-энтропии и ошибок обучения для каждого набора данных. Основным показателем является ошибка для контрольного множества (Validation).

Графики на рисунке 5.15 показывают, что на обучающем наборе **Train** значение кросс-энтропии монотонно убывает. На контрольном наборе **Validation** после третьей эпохи начинается рост кросс-энтропии.

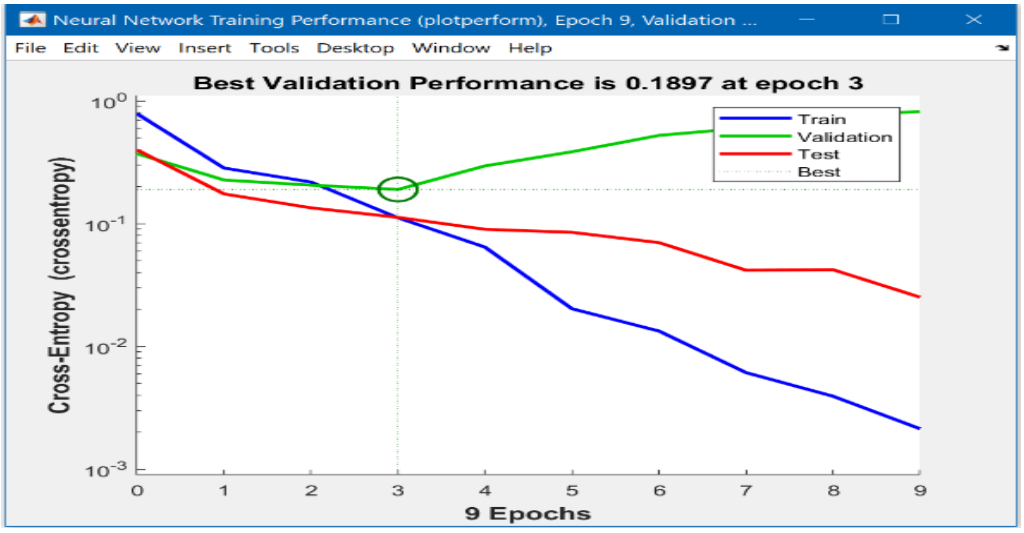


Рисунок 5.15 – Результаты моделирования. Процесс обучения сети

Это свидетельствует о том, что после третьей эпохи начинается переобучение. Поэтому лучшим принят результат, достигнутый на третьей эпохе.

Из графиков видно, что градиент (норма вектора градиента) уменьшается, что приводит к снижению скорости обучения сети. График на рисунке 5.16 показывает относительный рост ошибки на контрольном множестве, что свидетельствует о переобучении.

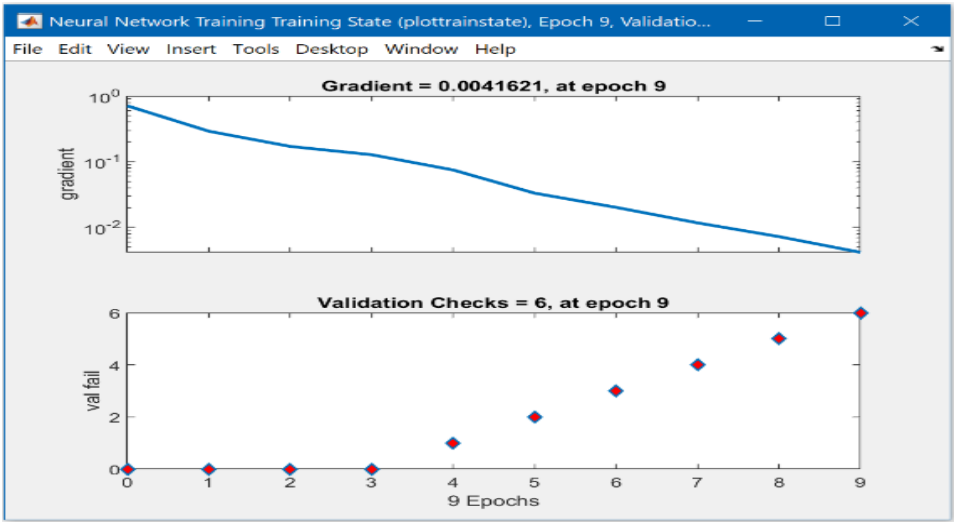


Рисунок 5.16 – Результаты моделирования. Состояние обучения

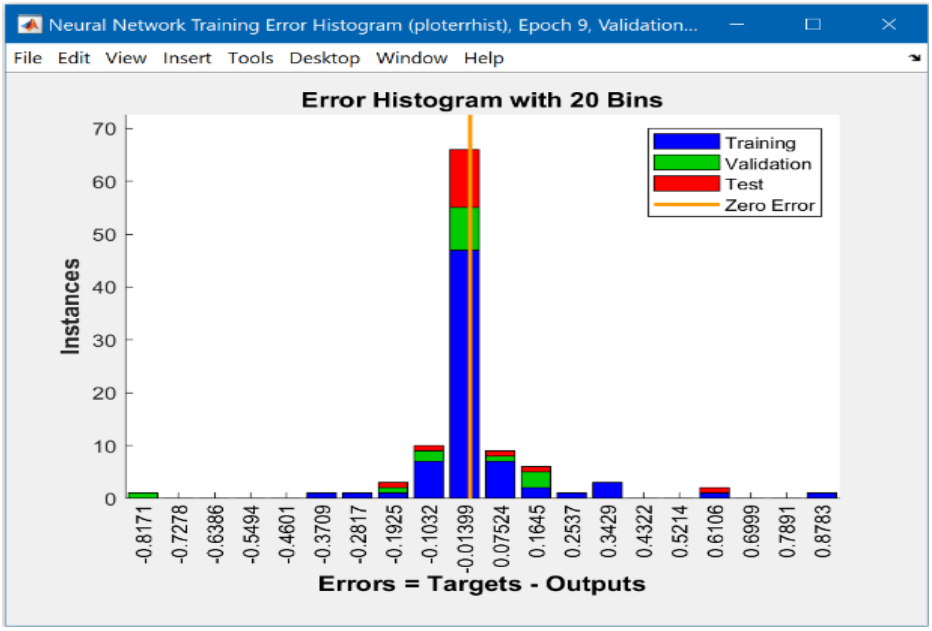


Рисунок 5.17. – Анализ ошибок. Гистограмма ошибок

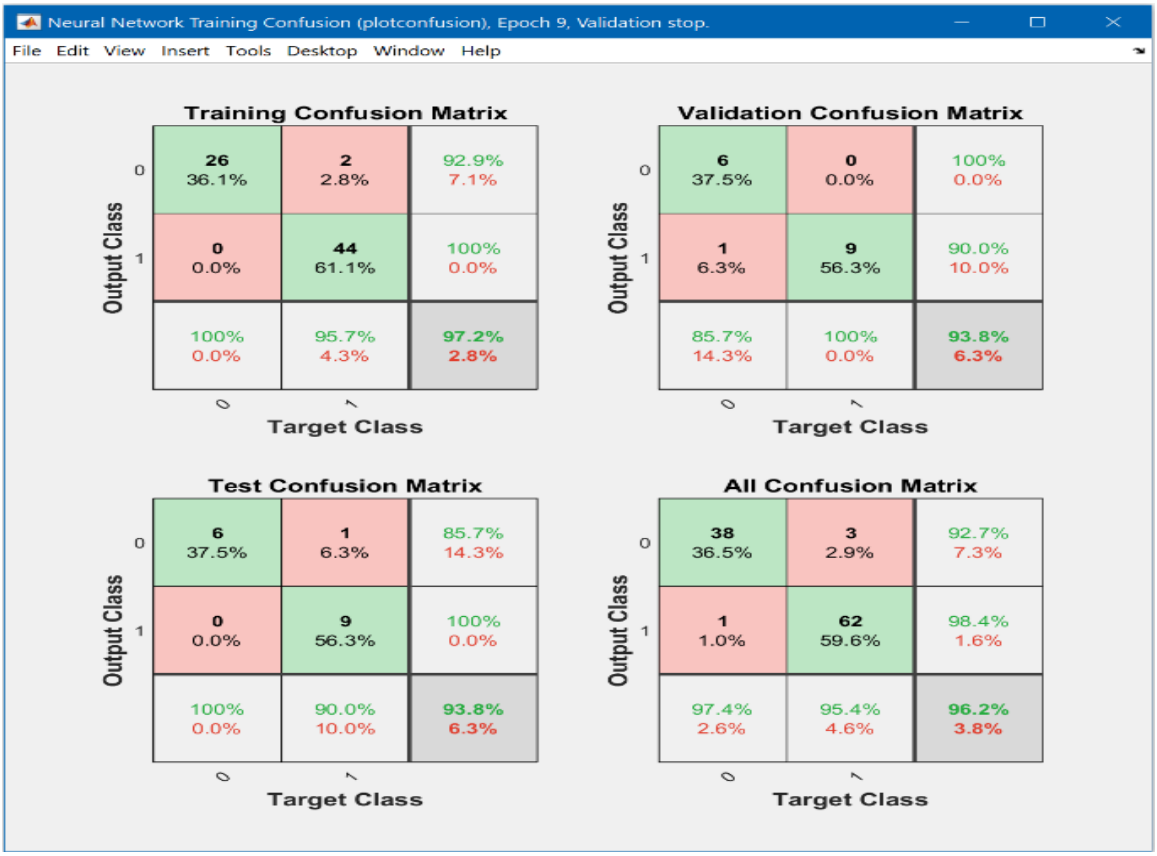


Рисунок 5.18 – Анализ ошибок. Матрица ошибок

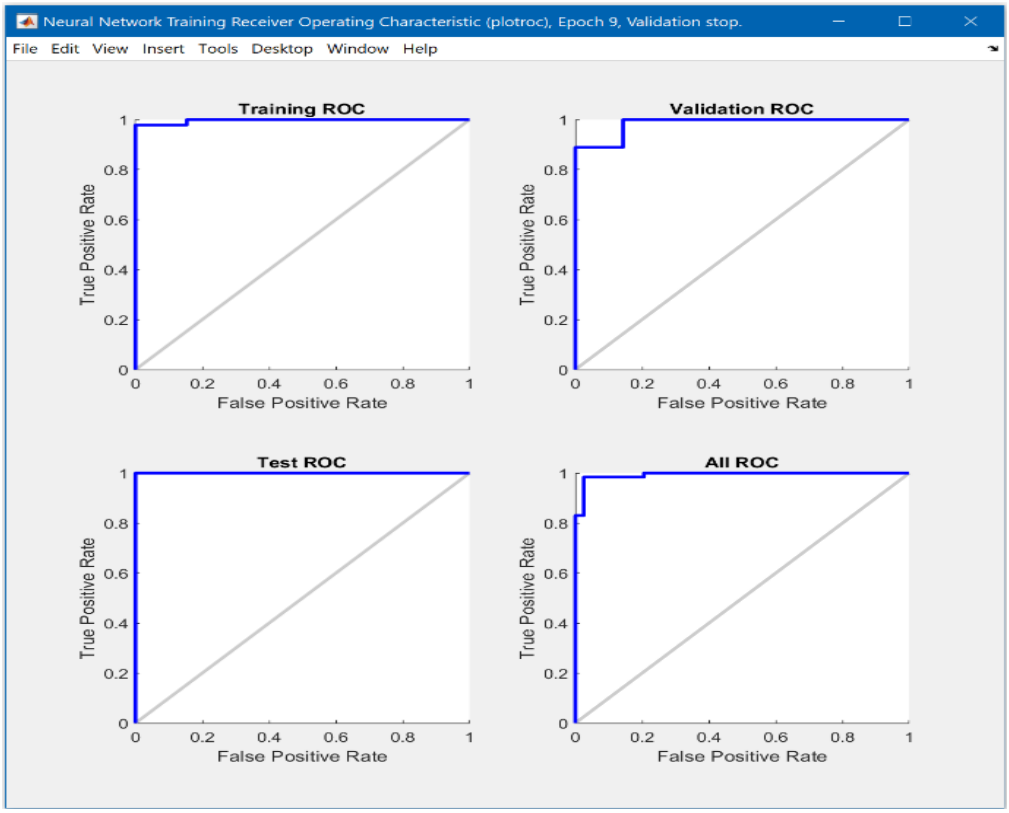


Рисунок 5.19 – Анализ ошибок. ROC-кривые

Гистограмма ошибок (Рисунок 5.17) и матрица ошибок сети (**Confusion**) (Рисунок 5.18) показывают высокое качество классификации. В решаемой задаче "истина" (выходной класс равен 1) – сотрудники, удовлетворяющие требованиям. "Ложь" (выходной класс равен 0) – сотрудники, не удовлетворяющие требованиям. На контрольном множестве сотрудники, не удовлетворяющие требованиям (класс 0), определены с точностью 100%. Сотрудники, удовлетворяющие требованиям (класс 1), определены с точностью 90%. Если обучающая выборка не содержит резко отличающихся примеров и достаточно большая, то изменение соотношения между обучающим, контрольным и тестовым множествами не оказывают существенного влияния на результат обучения. ROC-кривые (Рисунок 5.19) получились практически идеальными.

Рассчитаем основные показатели качества нейросетевого классификатора, используя матрицу ошибок (Рисунок 5.18). Расчет проведем по контрольному (валидационному) множеству.

Из матрицы ошибок получаем: $N_{TP}=9$; $N_{FP}=0$; $N_{TN}=6$; $N_{FN}=1$. Прецизионность (Precision) равна

$$R_{PR}=\frac{N_{TP}}{N_{TP}+N_{FP}}=\frac{9}{9+0}=1,00.$$

То есть точность предсказания положительного исхода (сотрудника, удовлетворяющего требованиям) равна 100%.

Полнота (Recall), или чувствительность (Sensitivity):

$$S_R=\frac{N_{TP}}{N_{TP}+N_{FN}}=\frac{9}{9+1}=0,90.$$

Доля истинно положительных примеров равна 90%, т.е. из всех сотрудников, определенных как удовлетворяющие требованиям, 90% действительно удовлетворяют требованиям.

Специфичность (Specificity):

$$S_P=\frac{N_{TN}}{N_{TN}+N_{FN}}=\frac{5}{6+1}=0,86.$$

То есть доля правильно классифицированных неудовлетворительных сотрудников составляет 86%.

F_1-мера (F-score):

$$F_1=2\frac{R_{PR}*S_R}{R_{PR}+S_R}=2\frac{1*0,90}{1+0,90}=0,95.$$

F_1-мера близка к 1, что говорит о высоком качестве классификации.

Тулбокс Neural Network Pattern Recognition App позволяет сгенерировать программу системы MATLAB. Программа рассчитана на то, что исходные данные загружены в рабочее пространство MATLAB. Сгенерированная программа может быть усложнена, добавлением возможностей, отсутствующих в Neural Network Pattern Recognition App. В частности, можно строить сети с большим числом скрытых слоев, обучающихся различными методами.

Для оценки уровня готовности персонала транспортной безопасности необходимо сохранить обученную нейронную сеть. Для оценки уровня готовности конкретного сотрудника необходимо моделировать работу сети на наборе

признаков этого сотрудника. При условии, что объект обученная нейронная сеть загружен в рабочее пространство MATLAB, моделирование выполняется командой:

$$y = net(x),$$

где **x** – массив признаков (оценок) сотрудников, **y** – оценка сотрудника (число, близкое к единице, соответствуют сотруднику, готовому к выполнению обязанностей, число, близкое к нулю – не готовому).

Многократно обучая нейронную сеть с помощью **Retrain**, можно добиться неплохих показателей качества классификации. Но, в этом случае сеть определенной структуры успешно работает на конкретном случайно выбранном контрольном множестве. Нет гарантии, что при определении готовности конкретного сотрудника, сеть продемонстрирует правильный результат. На новом примере сеть может показать низкую точность (при многократном повторном обучении были результаты с высокой и низкой точностью). Результаты экспериментов по исследованию стабильности работы нейронных сетей различной структуры представлены в таблице 5.1.

Лучшей будет сеть, показывающая при многократном повторном обучении стабильно высокие показатели с малым разбросом. Для исследования с этой точки зрения нейронные сети с различным числом нейронов в скрытом слое многократно обучались по **Retrain** и оценивалось среднее значение точности и среднее квадратическое отклонение точности. Лучшей будет сеть с максимальным средним значением точности и минимальным средним квадратическим отклонением.

Таблица 5.1. Результаты исследования стабильности работы нейронных сетей

Скр. слой	Вых. классы	Точность классификации, %										Сред. знач. точн.	Квадратичное откл. точн.
2	0	87,5	66,7	81,8	100	100	100	100	100	77,8	100	91,4	12,2
	1	87,5	100	100	90,9	84,6	100	100	100	85,7	100	94,9	6,8

10	0	100	100	100	100	80	80	80	100	100	87,5	92,8	9,61
	1	90	100	100	100	100	100	100	90,9	100	100	97,9	4,2
20	0	100	100	100	100	100	100	75,0	100	100	100	97,5	7,91
	1	100	100	100	81,8	77,8	88,9	100	90,0	91,7	100	93,0	8,36

Наиболее критичным является разброс оценок сотрудников, не удовлетворяющих требованиям. Сеть с двумя нейронами в скрытом слое показала наибольший разброс оценок сотрудников, не удовлетворяющих требованиям. Меньший разброс показали сети с 10 и 20 нейронами в скрытом слое. Причем, однозначного преимущества эти сети не показали, поэтому при реализации программы нейросетевой оценки персонала транспортной безопасности следует рассмотреть сети с 10 и 20 нейронами в скрытом слое.

5.5 Разработка автономных программных средств нейросетевой классификации персонала

Пакет Deep Learning Toolbox системы MATLAB удобен для построения и исследования нейронной сети на множестве обучающих примеров. В MATLAB можно сохранить параметры обученной сети. Другая программа MATLAB, загрузив параметры сети и получив данные сотрудника может оценить его готовность. Однако, такой подход нецелесообразен по ряду причин:

– Потребуются покупки дорогостоящих лицензий для каждого рабочего места.

– Программа на MATLAB потребует специальных навыков пользователей по работе с системой MATLAB, так как программа работает в режиме интерпретации, исполняемый файл отсутствует.

– Программа будет неудобной для конечного пользователя из-за сложности организации в MATLAB удобного русского пользовательского интерфейса.

– Программа будет предъявлять достаточно высокие требования к аппаратно-программной платформе, так как современные версии MATLAB рассчитаны на последние версии 64 разрядной операционной системы Windows 10.

Альтернативным подходом является разработка автономного приложения на языке C++, что позволит:

– Обеспечить низкую стоимость программы.

– Получение исполняемого файла, который можно запускать на Windows-компьютерах различной конфигурации.

– Использование привычного для пользователя русского графического интерфейса, что минимизирует требования к пользователям.

При разработке автономной программы целесообразно использовать подобранную в MATLAB структуру сети. Так как значение порога отсечения скрыто от пользователя, то потребуется исследование и подбор порога отсечения нейронной сети. Но включать в функционал программы обучение нейронной сети нецелесообразно, так как это не только необоснованно усложнит программу, но и опасно из-за несанкционированных попыток конечного пользователя обучить сеть на собственных примерах. Поэтому было принято решение разработать служебную программу Neuronet, позволяющую обучать нейронную сеть с архитектурой, подобранной в MATLAB. Программа Neuronet должна позволять обучать нейронную сеть при пороге отсечения, заданном в программе, и выдавать файл весовых коэффициентов обученной сети. В диалоговой программе Neurotest, доступной конечному пользователю, "зашиваются" полученные весовые коэффициенты. Поэтому пользователь не может обучить сеть на собственных примерах.

Программный комплекс «Neuronet»

Программа «Neuronet» предназначена для обучения нейронной сети на множестве примеров, каждый из которых содержит признаки, характеризующих степень готовности специалиста к выполнению трудовых функций, и целевое значение, определяющее оценку готовности специалиста к выполнению своих

функций. Целевое значение "1" означает сотрудника, удовлетворяющего требованиям, "0" – не удовлетворяющего. В результате работы программы формируются и сохраняются на диске весовые коэффициенты, которые "зашиваются" в программу оценки персонала Neurotest.

Программа выполняет следующие функции:

– загрузка обучающей выборки, расположенной в текстовом файле;
– обучение нейронной сети на наборе примеров;
– сохранение в файле весовых коэффициентов обученной сети.

Режим работы: оконный режим в операционной системе. Контроль правильности выполнения программы осуществляется средствами программы, которые реализовано в виде сообщений при обнаружении ошибок выполнения. Программа «Neuronet» является служебной программой для обучения нейронной сети. Настроенные в процессе обучения весовые коэффициенты использованы в программе для оценки уровня готовности персонала транспортной безопасности к выполнению профессиональной деятельности.

При запуске программы выполнение передаётся функции main, в которой формируется главное окно приложения. Главное окно приложения организовано с помощью класса Main Window. Данный класс организует меню пользователя, реагирует на действия пользователя посредством вызова соответствующих слотов. В конструкторе Main Window создаётся меню пользователя с помощью метода create Menus, и, посредством вызова метода create Actions, создаются действия, которые организуют реакцию программы на нажатие пользователем соответствующих пунктов меню.

Обучающие примеры (вектор входных признаков и целевое значение), которые необходимы для обучения нейросети, загружаются из текстового файла. При нажатии на «File» и выборе пункта «Open» происходит генерирование сигнала triggered, на который класс Main Window реагирует вызовом слота open. Работа слота open начинается с создания диалогового окна, предназначенного для открытия с диска файла с обучающей выборкой и чтения его содержимого.

Прочитанные данные сохраняются в векторе data. Из общего объема загруженных данных в программе формируется три массива в пропорции 70%, 15% и 15%, которые соответственно, определяют обучающее, контрольное и тестовое множества. После этого выполняется преобразование элементов массивов, в результате которого их значения приводятся к отрезку действительных чисел [0, 1].

После чтения данных и их преобразования слот open генерирует сигнал calc, на который класс Main Window реагирует вызовом слота calcNet.

Слот calcNet создаёт трёхслойную нейронную сеть (вызов конструктора класса neuronet) со следующей архитектурой: 26 входных нейронов, 20 нейронов срытого слоя и 1 выходной нейрон.

Обучение нейросети происходит с помощью алгоритма градиентного спуска с моментом. Подобранные параметры обучения: момент равен 0.7, скорость обучения равна 0.1. В качестве функции активации в скрытом слое используется логистическая функция, в выходном слое – функция softmax. В цикле обучения случайным образов выбираются обучающие примеры для обучения и подаются на вход сети вызовом метода SetNetInputs класса neuronet. Нейросеть с помощью метода calcOutput вычисляет значения нейронов выходного слоя, после чего с помощью метода обратного распространения ошибки, который в программе обеспечивается посредством вызовов методов calcError, learn и update, корректируются веса. С помощью метода getOutput возвращается значение нейрона выходного слоя. Полученный выход сети сравнивается с пороговым значением. Если выход сети ниже порога отсечения, то пример относится к категории «отсев», иначе – к категории «годен». Кроме этого, в цикле обучения определяются числа правильно и неправильно распознанных положительных и отрицательных примеров. Процедура обучения продолжается пока ошибка сети на тренировочном наборе не станет меньше заданной точности, равной 0.0001.

Для предотвращения переобучения реализован ранний останов. Для этого после каждых шести циклов обучения, определяется ошибка на контрольном множестве. Полученная ошибка запоминается в программе, запоминаются весовые

коэффициенты нейросети на соответствующей эпохи обучения, и определяется характер изменения ошибки. После того, как ошибка контрольного множества перестаёт уменьшаться, в программе выполняется фиксация значений весовых коэффициентов для дальнейшего их сохранения на диске. Также, как и для обучающего множества, для контрольного множества определяются числа правильно и неправильно распознанных положительных и отрицательных примеров.

После обучения нейросети выполняется проверка качества обучения на тестовом множестве. Здесь также определяются числа правильно и неправильно распознанных положительных и отрицательных примеров.

Работа слота calcNet завершается сохранением в файле «weights.bin» настроенных весов сети и отправлением сигнала для вывода матрицы несоответствий на экран в виде таблицы, на который класс MainWindow реагирует вызовом слота viewResult.

Для завершения программы, кроме стандартного средства рабочего окна операционной системы, в классе MainWindow используется слот close, который вызывается при получении сигнала от пункта меню «Просмотр». Слот close описан в модуле QWidget и является стандартным средством завершения GUI-приложения.

Программа Neuronet разработана на языке C++ с использованием библиотеки Qt версии 5.13.1. Для реализации предусмотренной функциональности приложения были разработаны следующие модули: MainWindow, MainWidget, TableWidget, MyLabel, neuronet и layer. Иерархия родословных связей модулей программы представлена на рисунке 5.20.

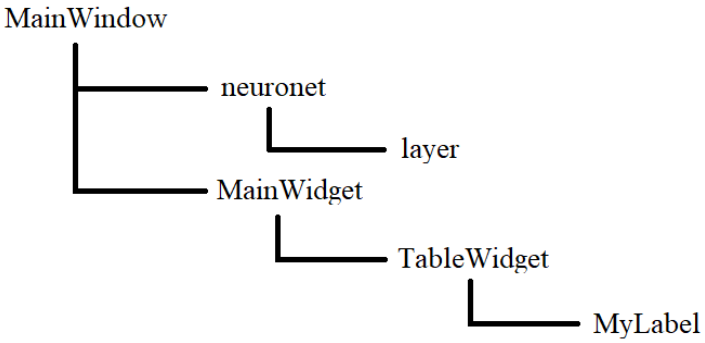


Рисунок 5.20 – Иерархия классов программы

Модуль MainWindow (файлы mainwindow.*) располагается на вершине иерархии и является родительским для остальных модулей. Он реализует главное окно приложения. Данный класс организует меню пользователя, реагирует на действия пользователя посредством вызова соответствующих слотов.

Модуль MainWidget (файлы mainwidget.*) организует вывод матриц несоответствия для тренировочного, контрольного, тестового и суммарного множеств. Непосредственный вывод матрицы несоответствия на экран выполняет модуль TableWidget (файлы tablewidget.*).

Класс MyLabel (файлы mylabel.*) предназначен для отображения числа и процента распознанных (нераспознанных) примеров на выделенных цветовых полях в матрице ошибок.

Модуль neuronet (файлы neuronet.*) реализует нейронную сеть, которая формирует оценку готовности сотрудника к выполнению своих обязанностей. Составляющую нейросеть слои реализованы в модуле layer.

Входными данными являются обучающие примеры, характеризующие степень готовности специалиста к выполнению трудовых функций, и целевые классы, определяющие итоговую оценку готовности. Примеры размещаются в текстовом файле. В каждой строке файла размещён один обучающий пример. В строке первая цифра – это целевое значение, далее через пробел записаны признаки.

Выходными данными являются настроенные весовые коэффициенты скрытого и выходного слоёв нейронной сети, которые сохраняются в файле «weights.bin». Формат файла – бинарный.

В ходе выполнения программы выдаются сообщения:

– Сообщение "Ошибка. Файл данных повреждён" может появиться при чтении из файла обучающих примеров, когда в примере отсутствуют некоторые признаки или целевой класс. В этом случае следует проверить в файле правильность набора данных.

– Сообщение "Ошибка. Невозможно открыть файл для чтения" может появиться запрет доступа к файлу со стороны операционной системы.

В результате работы программы весовые коэффициенты обученной нейронной сети будут сохранены на диске и использованы при разработке программы оценки персонала транспортной безопасности. Это служебная программа, предназначенная для обучения нейронной сети. Обучается нейронная сеть с архитектурой, полученной при исследовании сети в MATLAB. Эта программа не предназначена для конечного пользователя.

После запуска программы «Neuronet» на экране появится главное окно программы, в котором расположен один пункт «File». При нажатии левой кнопки мыши на «File» появится выпадающее меню, где содержится два пункта – «Open» и «Exit». С помощью «Open» происходит загрузка из текстового файла обучающих примеров. При нажатии левой кнопки мыши на «Open» появляется диалоговое окно, которое поможет пользователю выбрать на диске файл с обучающими примерами.

После открытия файла и считывания обучающих примеров, они разбиваются на три массива в пропорции 70%, 15 % и 15%, чтобы сформировать три множества примеров соответственно тренировочное, контрольное и тестовое.

После окончания обучения нейросети в главном окне приложения будут выведены четыре матрицы несоответствия обучающего, контрольного, тестового и суммарного множества, которое состоит из этих трёх множеств (Рисунок 5.18), а

также в текущем каталоге будет создан файл с именем «weights.bin», в который программа сохранит весовые коэффициенты обученной нейронной сети.

Анализ результатов экспериментального исследования «neuronet»

Целесообразно оценить работоспособность нейронной сети, реализованной в программе Neuronet, и выбор оптимального порога (точки) отсечения. Исследовалась нейронная сеть следующей конфигурации: входной слой, содержащий 26 нейронов, скрытый слой, содержащий 10 нейронов и выходной слой, включающий один нейрон. Сеть обучалась методом градиентного спуска с использованием алгоритма обратного распространения ошибки до достижения средней квадратической ошибки – 0.0001.

Результатом обучения сети является матрица ошибок (Рисунок 5.21). Сеть обучалась при различных порогах отсечения, задаваемых в программе. Чтобы уменьшить влияние случайной инициализации сети для каждого порога отсечения проводилось по пять экспериментов. Примеры матриц ошибок для различных порогов отсечения приведены в приложении Г.

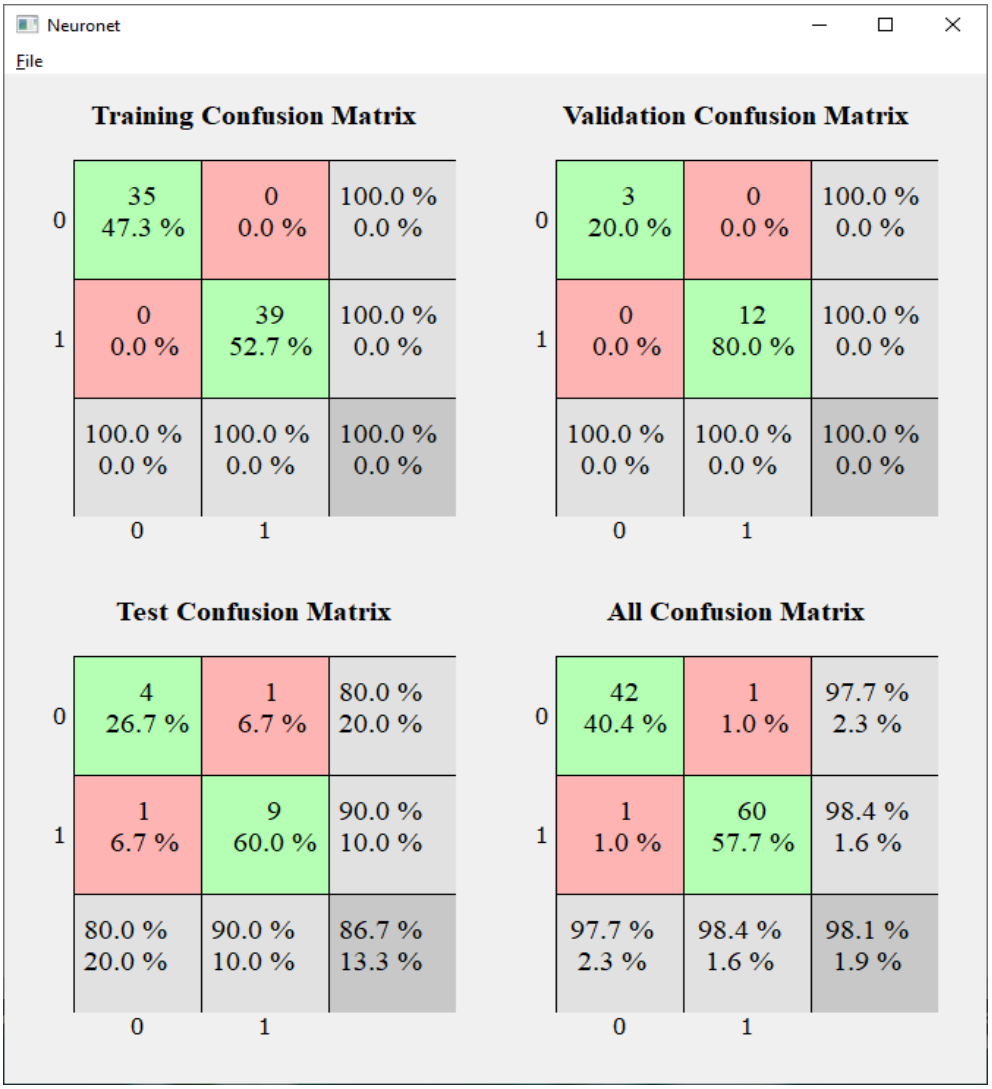


Рисунок 5.21 – Матрица ошибок

Усредненные характеристики сети определялись по контрольному множеству (Validation Set) и представлены в таблице 5.2. В таблице приняты следующие обозначения (обозначения соответствуют матрице ошибок, показанной на рисунке 5.21):

– N_{TN} – количество истинно отрицательных исходов;

– N_{FP} – количество ложно положительных исходов;

– N_{FN} – количество ложно отрицательных исходов;

– N_{TP} – количество истинно положительных исходов.

Таблица 5.2 Результаты экспериментов с разными порогами отсечения

Порог отсечения	Исходы	Результаты экспериментов					Средние значения метрик					
		1	2	3	4	5	R_{AC}	R_{PR}	S_R	S_P	F_1	FPR
0,50	N_{TN}	2	2	3	4	5	0,9600	0,9538	1,0000	0,8000	0,9760	0,2000
	N_{FP}	1	1	0	0	1						
	N_{FN}	0	0	0	0	0						
	N_{TP}	12	12	12	12	12						
0,60	N_{TN}	3	2	2	2	2	0,9467	0,9385	1,0000	0,7333	0,9680	0,2626
	N_{FP}	0	1	1	1	1						
	N_{FN}	0	0	0	0	0						
	N_{TP}	12	12	12	12	12						
0,65	N_{TN}	3	3	3	3	3	0,8933	1,0000	0,8667	1,0000	0,9264	0,0000
	N_{FP}	0	0	0	0	0						
	N_{FN}	2	0	3	2	1						
	N_{TP}	10	12	9	10	11						
0,70	N_{TN}	3	3	3	3	3	0,7333	1,0000	0,6667	1,0000	0,8000	0,0000
	N_{FP}	0	0	0	0	0						
	N_{FN}	4	4	4	4	4						
	N_{TP}	8	8	8	8	8						
0,80	N_{TN}	3	3	3	3	3	0,5867	1,000	0,4833	1,000	0,6510	0,0000
	N_{FP}	0	0	0	0	0						
	N_{FN}	6	6	6	6	7						
	N_{TP}	6	6	6	6	5						
0,90	N_{TN}	3	3	3	3	3	0,5733	1,0000	0,4667	1,0000	0,6048	0,0000
	N_{FP}	0	0	0	0	0						
	N_{FN}	5	4	6	6	11						
	N_{TP}	7	8	6	6	1						

В таблице приведены средние значения метрик качества нейронной сети: точность, прецизионность и др.

Программный комплекс «Neurotest»

Программа «Neurotest» предназначена для оценки компетенций и требований персонала транспортной безопасности к выполнению задач профессиональной деятельности с помощью предварительно обученной нейронной сети.

Программа выполняет следующие функции:

– определение оценки готовности персонала транспортной безопасности к выполнению задач профессиональной деятельности;

– сохранение информации о выставленных баллах по требованиям компетенций специалиста и его оценки готовности;

– просмотр ранее сохранённых данных об оценивании персонала.

Программа оценки готовности специалиста транспортной безопасности к выполнению профессиональных задач обеспечивает:

– ввод личных данных специалиста и выставленных баллов по каждому требованию компетенции;

– формирование итоговой оценки готовности специалиста;

– автоматическое сохранение информации о результатах оценивания специалиста в базе данных;

– просмотр сохранённых результатов оценивания персонала.

Режим работы программы «Neurotest» – оконный режим в операционной системе. Программа не требует дополнительной настройки.

При запуске программы выполнение передаётся функции main, в которой сначала осуществляется поиск в каталоге приложения файла базы данных с именем «answers». Если файл отсутствует, что может быть при первом запуске программы, будет предпринята попытка создания базы данных и назначения имени файла данных «answers». В программе данные сохраняются в одной таблице. В качестве СУБД выбрана SQLite, поскольку программа не предполагает распределённого выполнения и работает с локальными данными.

При отсутствии файла данных и последующего успешного его создания, с помощью SQL запроса средствами Qt создаётся таблица данных, схема которой приведена в таблице 5.3.

После проверки наличия файла базы данных или успешного его создания в случае отсутствия, функция main формирует главное окно приложения. Главное окно приложения организовано с помощью класса MainWindow.

Таблица 5.3 Таблица данных

Содержание поля	Имя поля	Тип	Примечание
Порядковый номер записи	id	INTEGER	Первичный ключ
Фамилия	surname	VARCHAR(20)	Обязательное поле
Имя	name	VARCHAR(20)	Обязательное поле
Отчество	patronymic	VARCHAR(20)	Обязательное поле
Дата выставления оценки	testdate	VARCHAR(20)	Обязательное поле
Время выставления оценки	testtime	VARCHAR(15)	Обязательное поле
Компетенция k1	k1	INTEGER	Обязательное поле
Компетенция k2, требование t1	k2t1	INTEGER	Обязательное поле
Компетенция k2, требование t2	k2t2	INTEGER	Обязательное поле
Компетенция k2, требование t3	k2t3	INTEGER	Обязательное поле
Компетенция k2, требование t4	k2t4	INTEGER	Обязательное поле
Компетенция k2, требование t5	k2t5	INTEGER	Обязательное поле
Компетенция k3, требование t1	k3t1	INTEGER	Обязательное поле
Компетенция k3, требование t2	k3t2	INTEGER	Обязательное поле
Компетенция k3, требование t3	k3t3	INTEGER	Обязательное поле
Компетенция k4	k4	INTEGER	Обязательное поле
Компетенция k5, требование t1	k5t1	INTEGER	Обязательное поле

Продолжение таблицы 5.3

Содержание поля	Имя поля	Тип	Примечание
Компетенция k5, требование t2	k5t2	INTEGER	Обязательное поле
Компетенция k5, требование t3	k5t3	INTEGER	Обязательное поле
Компетенция k5, требование t4	k5t4	INTEGER	Обязательное поле
Компетенция k5, требование t5	k5t5	INTEGER	Обязательное поле
Компетенция k5, требование t6	k5t6	INTEGER	Обязательное поле
Компетенция k6, требование t1	k6t1	INTEGER	Обязательное поле
Компетенция k6, требование t2	k6t2	INTEGER	Обязательное поле
Компетенция k6, требование t3	k6t3	INTEGER	Обязательное поле
Компетенция k7, требование t1	k7t1	INTEGER	Обязательное поле
Компетенция k7, требование t2	k7t2	INTEGER	Обязательное поле
Компетенция k7, требование t3	k7t3	INTEGER	Обязательное поле
Компетенция k7, требование t4	k7t4	INTEGER	Обязательное поле
Компетенция k7, требование t5	k7t5	INTEGER	Обязательное поле
Компетенция k7, требование t6	k7t6	INTEGER	Обязательное поле
Компетенция k7, требование t7	k7t7	INTEGER	Обязательное поле
Итоговый результат	result	VARCHAR(6)	Обязательное поле

Данный класс организует меню пользователя, реагирует на действия пользователя посредством вызова соответствующих слотов. В конструкторе класса создаётся трёхслойная сеть. При создании сети конструктор класса neuronet принимает на вход в качестве параметров число слоёв и количество нейронов

каждого слоя: 26 входных нейронов, что соответствует числу входных признаков, 20 нейронов срытого слоя и 2 выходных нейрона, значения выходов которых классифицирует специалиста транспортной безопасности удовлетворяющих или неудовлетворяющих требованиях. После создания нейросети устанавливаются значения весовых коэффициентов скрытого и выходного слоёв. Эти значения были получены при обучении нейросети на совокупности примеров и сохранены в файле weights.bin.

При разработке программы Neurotest данные из файла weights.bin размещены в тексте программы в массивах w1 и w2, которые представляют собой веса, соответственно скрытого и выходного слоёв.

Кроме этого, в конструкторе MainWindow создаётся меню пользователя с помощью метода createMenus(), где присутствуют пункты «Тест», «Результаты», «Помощь», «Выход», и, посредством вызова метода createActions(), создаются действия, которые организуют реакцию программы на нажатие пользователем соответствующих пунктов меню.

Определение оценки

При выборе пункта «Тест» происходит определение оценки готовности специалиста, при этом реакцией этого будет вызов слота testing() класса MainWindow.

Работа слота testing() начинается с создания диалогового окна для ввода личных данных пользователя, который реализован в классе InputFIODialog. После получения личных данных при закрытии окна (было нажатие кнопки Ok) происходит создание диалогового окна для ввода баллов по требованию компетенций. Это окно и процедура ввода баллов организованы в классе InputDialog. После закрытия диалогового окна (пользователь нажал кнопку Ok) класс InputDialog возвращает массив m введённых баллов, который преобразуется во входной вектор признаков. Здесь преобразование подразумевает нормализацию введённого массива баллов, которая для каждого элемента выполняет следующую операцию

$$mas[j] = m[j] / 10.0 * 0.99 + 0.01 ,$$

где m – исходный массив, mas – нормализованный вектор, $0 \leq j < 26$. В результате преобразования значения исходного массива будут приведены к диапазону вещественных чисел (0, 1).

Определение оценки готовности специалиста реализовано в классе neuronet посредством вызовов методов SetNetInputs, calcOutput и getOutput. Метод SetNetInputs в качестве входа нейронной сети устанавливает полученный вектор признаков mas. Далее с помощью метода calcOutput вычисляются значения нейронов выходного слоя, а метод getOutput возвращает эти значения.

Далее определяется индекс нейрона, имеющего максимальное значение выходы. Если найденный индекс равен 0, то итоговая оценка готовности специалиста – «отсев», если – 1, то итоговая оценка – «годен». Итоговая оценка в информационном окне выводится на экран.

С помощью метода saveRecord класса MainWindow информация о специалисте (фамилия, имя, отчество, выставленные баллы, итоговая оценка, а также дата и время оценивания) сохраняется в базе данных.

Просмотр результатов

При выборе пункта «Просмотр» отображаются результаты ранее проведённых проверок компетенций, при этом программа реагирует вызовом слота viewRecords класса MainWindow.

В слоте viewRecords создаётся объект класса TableView, который реализует доступ к файлу базы данных и вывод её содержимого на экран в виде таблицы. В конструкторе класса TableView создаётся модель таблицы, в которую будут выведены записи, при этом поля, сохраняющие выставленные баллы, устанавливаются с помощью метода setColumnHidden как неотображаемые. Таким образом, остальные поля surname, name, patronymic, testdate, testtime и result выводятся в таблицу, при этом записи с помощью метода setSort упорядочиваются по полю surname в алфавитном порядке.

Взаимодействие с пользователем в классе TableView осуществляется посредством вызовов слотов handleTableClick, viewRecord и deleteRecord. Первые два слота предназначены для вывода полной информации о специалисте со всеми выставленными ему баллами при двойном клике на строке таблице и нажатии клавиши просмотра соответственно. Третий слот вызывается при удалении записи из таблицы.

Вывод полной информации реализован в классе ViewInfo, конструктор которого получает номер строки таблицы базы данных, которую следует отобразить.

Для завершения программы, кроме стандартного средства рабочего окна операционной системы, в классе MainWindow используется слот close, который вызывается при получении сигнала от пункта меню «Просмотр». Слот close описан в модуле QWidget и является стандартным средством завершения GUI-приложения.

Программа Neurotest разработана на языке C++ с использованием библиотеки Qt версии 5.13.1. Для реализации предусмотренной функциональности приложения были разработаны следующие модули: MainWindow, TableView, InputDialog, InputFioDialog, MenuBar, CustomLineEdit, CustmSLineEdit, ViewInfo, MenuButton,

Counter, neuronet и layer. Исходные тексты этих модулей приведены в приложении Г.

Иерархия родословных связей модулей программы представлена на рисунке 5.22.

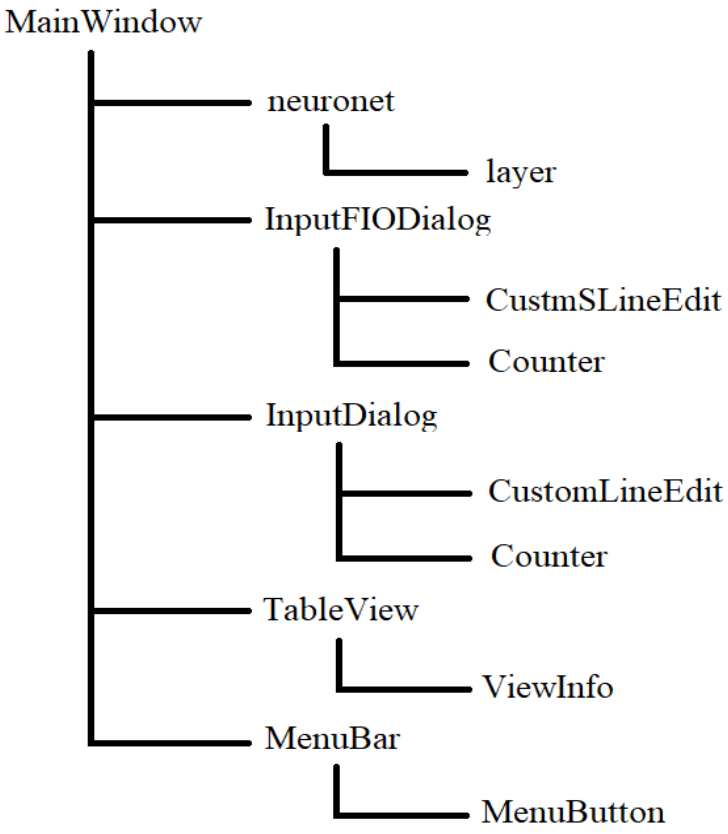


Рисунок 5.22 – Иерархия классов программы

Модуль MainWindow (файлы mainwindow.*) располагается на вершине иерархии и является родительским для остальных модулей. Он реализует основное окно приложения. Для взаимодействия с пользователем MainWindow включает модуль MenuBar (файлы menubar.*), реализующий интерфейс (пункты «Тест», «Результаты», «Помощь», «Выход») посредством четырех объектов класса MenuButton (файлы menubutton.*), которые при активации генерирует сигналы, на которые MainWindow реагирует вызовом соответствующего слота.

Модуль InputFioDialog (файлы inputfiodialog.*) формирует диалоговое окно для ввода личных данных специалиста. Ввод личных данных реализован с учётом валидации, которая осуществляется с помощью модуля. CustmSLineEdit (файлы custmslineedit.*).

Модуль InputDialog (файлы inputfiodialog.*) разработан для создания диалогового окна, с помощью которого выполняется ввод баллов по требованиям компетенций. Контроль правильности ввода баллов осуществляется с помощью модуля CustomLineEdit (файлы customlineedit.*).

Модули InputFioDialog и InputDialog контролируют заполняемость всех полей, в которые должны быть введены данные, чтобы продолжить дальнейшую работу. Контроль числа введённых данных реализован с помощью Counter (файлы counter.*), который с помощью сигналов sigActive() и sigDeactive() оповещает данные модули о возможности или невозможности продолжить работу.

Просмотр ранее проведённых оценок компетенций организует модуль TableView (файлы tableview.*), где выполняется доступ к базе данных, и отображение полей сохранённых записей в виде таблицы. В строке отображаются данные о специалисте, кроме выставленных ему баллов. Модуль ViewInfo выводит всю сохранённую информацию о специалисте.

Модуль neuronet (файлы neuronet.*) реализует нейронную сеть. Составляющую нейросеть слои реализованы в модуле layer. Входными данными являются личные данные специалиста и массив выставленных ему баллов по требованию компетенций. Выходными данными являются информация о специалисте (личные данные, выставленные баллы и итоговая оценка готовности), которая выводится в файл базы данных, и итоговая оценка готовности, выводимая на экран.

В ходе выполнения программы, программисту выдаются сообщения:

– Сообщение "Невозможно открыть базу данных". Может появиться при создании файла данных, когда он отсутствует. Возможная причина – накопитель защищён от записи или недостаточно места для сохранения файла.

– Сообщение "Невозможно создать таблицу". Может появиться при недостатке места для добавления таблицы в файл данных.

– Сообщение "Ошибка помещения данных в базу". Может появиться при порче файла базы данных.

После запуска программы «Neurotest» на экране появится главное окно приложения, которое содержит четыре пункта: «Тест», «Результаты», «Помощь», «Выход» соответствующими функциями.

При вводе личных данных применяется валидация, согласно которой данные можно ввести только на кириллице, первая буква фамилии, имени или отчества должны быть прописной, остальные – срочными. В противном случае поле ввода будет игнорировать нажатие клавиш на клавиатуре. Размер поля ввода равен 20 символам. Перемещение между полями ввода осуществляется с помощью клавиш курсора «↑» и «↓» и клавишей «Tab». Также выбрать поле для ввода или редактирования можно с помощью «мыши».

После заполнения всех полей ввода кнопка «Ok», которая с момента появления окна оставалась неактивной, становится активной, и после нажатия на неё текущее окно закроется и появится диалоговое окно для выставления баллов по требованию компетенций (Рисунок 5.23).

В окне для ввода баллов перечислены требования компетенций, напротив которых размещены поля для ввода баллов. Внизу окна справа размещены две кнопки: «Ok» и «Cancel», причём кнопка «Ok» является неактивная, и остаётся такой до тек пор, пока в поля ввода не будут занесены все баллы. Также при вводе баллов применяется проверка правильности ввода (цифры от 0 до 9). Выбор поля для ввода баллов организовано также, как и в случае ввода личных данных специалиста.

После нажатия на кнопку «Ok» (если она стала активной) диалоговое окно закроется и введённый массив баллов будет использован для вычисления итоговой оценки готовности специалиста транспортной безопасности к выполнению профессиональных задач.

Результат проверки специалиста в виде выставленной ему оценки «годен» или «отсев» выводится на экран с помощью информационного окна.

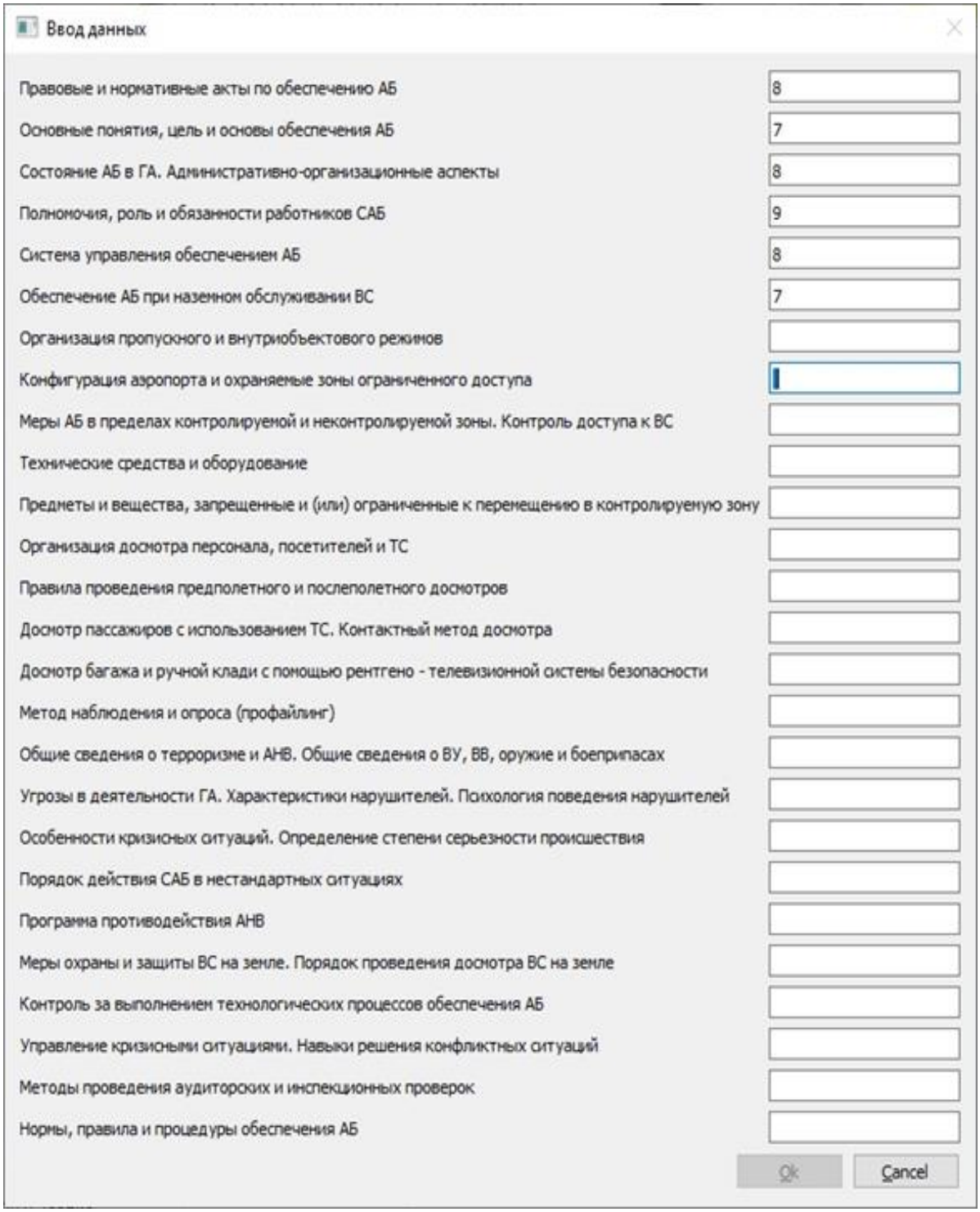


Рисунок 5.23 – Диалоговое окно для выставления баллов

После вывода на экран оценки, информация о специалисте (фамилия, имя, отчество, выставленные баллы, итоговая оценка, а также дата и время оценивания) автоматически сохраняется в базе данных.

При выборе пункта меню «Результаты» появится диалоговое окно, в котором отображаются результаты ранее проведённых проверок компетенций. Диалоговое окно представлено на рисунке 5.24.

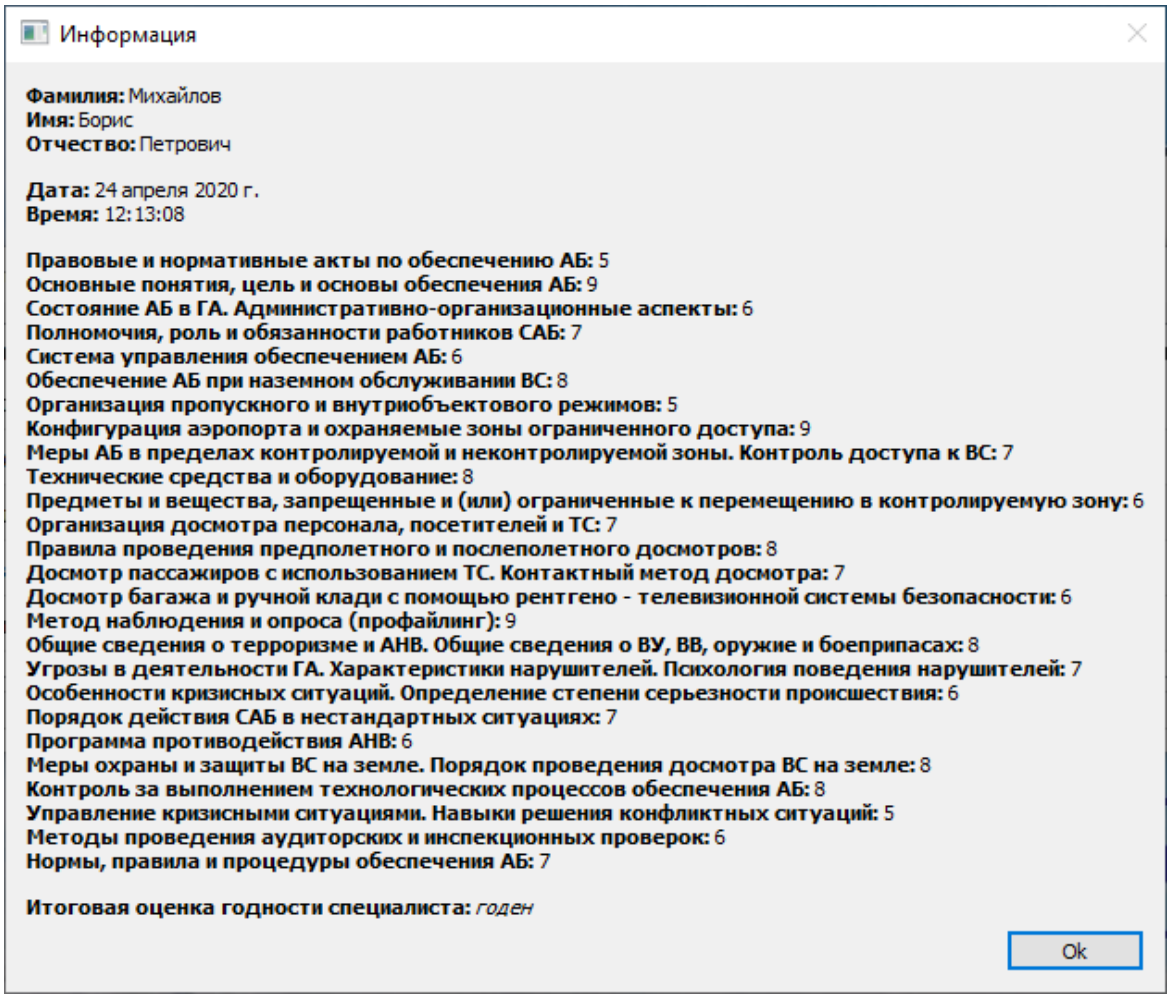


Рисунок 5.24 – Окно просмотра результатов

Результаты проверок компетенций представлены в виде таблице на рисунке 5.25.

Рисунок 5.25 – Информационное окно результата проверки компетенций

В каждой строке таблицы содержится фамилия, имя и отчество специалиста, дата и время оценивания, и оценка, которую «выставила» программа. Строки в таблице упорядочены по полю «Фамилия» в алфавитном порядке. Клавишами управления курсором «↑» и «↓» можно выполнять перемещения между строками таблицы.

В окне просмотра результатов добавлены три кнопки – «Просмотр», «Удалить» и «Ok». Кнопка «Просмотр» предназначена для просмотра баллов, которые были выставлены по каждому требованию компетенций. Клавишами управления курсором «↑» и «↓» выбирается интересующая запись о специалисте и при нажатии кнопку «Просмотр» откроется окно, в котором будет отображена информация о специалисте со всеми выставленными ему баллами.

Анализ результатов экспериментального исследования «Neurotest»

Исследование системы проводились с использованием выборочных примеров из таблицы исходных данных (приложение Г). Произвольным образом были взяты 42 примера (40% от общего числа) из таблицы исходных данных. Маловероятно, чтобы эти примеры полностью совпали с примерами контрольной выборки, представляющими собой случайно выбранные программной Neurotest 15% примеров обучающей выборки.

Результаты испытаний представлены в таблице 5.4. В столбце "Известный результат" показаны известные результаты обучающих примеров (см. приложение Г), в столбце "Предсказанный результат" – результаты работы программы. Сотрудники, удовлетворяющие требованиям, отмечены, как "Годен", а не удовлетворяющие требованиям – как "Отсев".

Всего рассмотрено $N = 42$ примеров. Получены следующие результаты:

- число истинно положительных результатов $N_{TP} = 21$;
- число истинно отрицательных результатов $N_{TN} = 21$;
- число ложно положительных результатов $N_{FP} = 0$;
- число ложно отрицательных результатов $N_{FN} = 0$.

Полученные результаты обеспечивают следующие показатели качества работы программы.

Точность (Accuracy) – число правильно классифицированных претендентов, отнесенное к общему числу исходов

$$R_{AC} = \frac{N_{TP} + N_{TN}}{N} = \frac{21+21}{42} = 1,00,$$

Прецизионность – точность предсказания положительного исхода (в нашем случае – претендента, удовлетворяющего требованиям), т. е. какая доля объектов, выделенных классификатором как положительные, действительно является положительными

$$R_{PR} = \frac{N_{TP}}{N_{TP} + N_{FP}} = \frac{21}{21+0} = 1,00.$$

Полнота (Recall) – это доля истинно положительных примеров, правильно определенных классификатором. В нашей задаче – это доля верно классифицированных удовлетворительных претендентов от общего числа удовлетворительных претендентов в контрольной выборке

$$S_R = \frac{N_{TP}}{N_{TP} + N_{FN}} = \frac{21}{21+0} = 1,00.$$

Специфичность (Specificity) – в нашей задаче это доля правильно классифицированных неудовлетворительных претендентов.

$$S_P = \frac{N_{TN}}{N_{TN} + N_{FP}} = \frac{21}{21+0} = 1,00.$$

F_1-мера (F_1-score) – гармоническое среднее между прецизионностью и полнотой

$$F_1 = 2\frac{R_{PR} * S_R}{R_{PR} + S_R} = 2\frac{1,00*1,00}{1,00+1,00} = 2\frac{1,00}{2,00} = 1,00.$$

Таблица 5.4 Результаты испытаний программы Neurotest

Компетенция	К1	К2	К2	К2	К2	К2	К3	К3	К3	К4	К5	К5	К5	К5	К5	К5	К6	К6	К6	К7	К7	К7	К7	К7	К7	Известный результат	Предсказанный результат
Требование		Т2-1	Т2-2	Т2-3	Т2-4	Т2-5	Т3-1	Т3-2	Т3-3		Т5-1	Т5-2	Т5-3	Т5-4	Т5-5	Т5-6	Т6-1	Т6-2	Т6-3	Т7-1	Т7-2	Т7-3	Т7-4	Т7-5	Т7-6	Т7-7		
1	6	7	5	9	6	8	7	8	7	7	7	4	8	6	8	8	6	6	9	9	4	8	6	6	6	6	годен	
2	7	7	3	7	5	7	7	5	4	5	5	5	8	6	8	5	5	7	6	5	8	6	6	5	8	7	отсев	отсев
3	4	6	6	8	8	8	4	4	8	6	6	6	7	5	7	8	8	6	9	9	6	6	7	7	7	7	годен	
4	9	7	7	9	9	9	6	9	7	7	5	6	6	8	9	9	6	8	8	8	6	7	8	8	6	6	годен	годен
5	6	8	8	8	4	8	7	7	6	4	4	7	7	6	6	7	9	7	6	6	7	8	6	6	7	5	отсев	отсев
6	6	7	7	5	5	7	7	6	8	9	9	6	8	8	7	9	7	7	6	5	9	7	9	8	8	8	годен	
7	7	7	5	5	7	7	7	8	6	5	8	5	6	8	8	9	6	6	8	8	8	7	9	7	8	8	годен	
8	9	9	9	6	6	8	5	5	6	7	7	6	6	7	7	8	8	8	9	6	6	6	9	9	7	7	годен	годен
9	9	6	6	6	8	5	5	8	7	8	6	6	5	8	9	7	8	9	6	6	8	8	8	8	9	6	годен	
10	6	8	8	7	7	9	8	8	8	8	8	9	6	8	7	7	9	9	5	8	6	6	7	7	5	7	годен	
11	6	8	8	8	6	5	6	7	7	8	6	8	7	6	5	5	6	7	7	8	8	7	9	9	8	9	годен	
12	6	9	6	6	7	6	7	7	7	8	7	6	6	6	9	7	7	8	6	9	9	7	7	7	7	7	годен	
13	5	6	8	8	6	7	7	5	8	6	7	8	8	8	6	8	7	8	5	7	7	8	8	9	8	7	годен	годен
14	4	7	7	8	6	5	8	8	8	9	6	6	8	8	8	8	9	8	8	9	8	8	8	8	8	8	годен	
15	9	9	9	8	7	6	9	6	9	6	6	6	9	8	7	7	7	8	6	9	8	7	7	9	9	6	годен	
16	6	6	7	7	4	7	7	3	6	5	6	6	8	7	9	7	6	6	6	7	6	8	5	6	6	5	отсев	отсев
17	8	8	8	5	5	6	8	5	6	6	8	6	6	6	5	7	8	5	7	4	4	4	8	7	7	7	отсев	отсев
18	9	9	9	8	8	8	8	6	6	6	9	8	9	8	7	8	8	6	6	9	9	7	7	9	9	9	годен	
19	5	5	8	8	6	7	7	7	5	6	5	5	6	6	8	6	5	6	6	6	6	8	5	7	7	7	отсев	
20	9	7	7	7	5	8	8	6	6	5	8	8	6	6	6	8	7	7	6	6	8	8	6	6	6	7	годен	годен
21	8	8	8	8	6	6	5	7	8	5	7	7	6	8	8	7	5	7	8	7	6	6	6	8	8	8	годен	
22	5	5	8	6	6	6	7	7	7	5	7	6	6	5	8	7	7	6	6	6	5	9	6	7	8	6	отсев	
23	8	8	8	9	9	7	8	8	8	9	9	9	8	8	6	8	7	9	9	8	8	8	9	8	7	7	годен	годен
24	8	9	9	7	9	9	9	9	6	8	8	8	7	7	7	9	7	7	7	7	9	7	5	6	7	7	годен	
25	7	3	3	6	6	4	7	4	4	7	7	5	8	5	5	4	5	8	5	5	6	6	6	7	7	5	отсев	отсев

Продолжение таблицы 5.4

Компетенция	К1	К2	К2	К2	К2	К2	К3	К3	К3	К4	К5	К5	К5	К5	К5	К5	К6	К6	К6	К7	К7	К7	К7	К7	К7	Известный результат	Предсказанный результат
26	5	6	4	4	4	6	6	7	5	7	7	7	5	8	8	6	6	5	8	6	8	6	8	8	8	6	годен	
27	6	6	8	8	5	8	5	5	6	6	7	6	8	6	6	6	7	8	5	6	7	8	7	6	8	6	отсев	отсев
28	4	7	7	6	6	5	7	6	6	6	7	4	6	6	6	7	7	7	6	4	7	7	7	4	4	6	отсев	
29	6	6	6	8	7	8	8	6	5	8	8	9	9	8	7	9	8	8	8	8	9	6	6	6	6	9	годен	годен
30	9	8	6	8	6	6	8	8	7	7	7	5	8	8	8	8	7	7	7	8	8	5	5	5	8	8	годен	
31	7	7	7	6	5	7	5	7	5	5	5	6	5	6	7	5	7	8	6	5	7	8	6	7	5	7	отсев	
32	8	9	9	8	8	8	6	9	9	9	9	8	6	8	8	9	6	6	7	7	9	6	8	8	6	8	годен	годен
33	3	3	5	3	6	6	3	6	5	4	5	6	3	5	3	6	6	6	5	5	4	3	3	6	6	6	отсев	
34	7	7	7	6	6	6	6	6	6	6	7	6	7	5	7	6	6	7	7	7	5	7	7	6	6	7	годен	
35	7	4	6	6	4	4	7	7	8	4	6	6	4	5	5	7	7	7	8	8	8	9	7	7	7	7	годен	
36	8	7	7	5	5	7	7	7	6	6	7	7	5	6	6	6	7	6	6	5	8	7	4	3	7	7	отсев	отсев
37	3	8	8	8	9	6	8	7	8	9	7	7	7	9	9	6	6	7	7	7	9	9	6	6	4	9	годен	
38	9	6	6	6	5	6	6	6	6	5	8	6	6	5	8	3	9	5	5	6	5	7	7	5	7	7	отсев	
39	9	7	3	7	4	8	8	7	3	7	7	6	9	6	7	5	7	6	7	4	6	6	6	5	7	5	отсев	отсев
40	7	7	7	9	5	4	7	7	7	5	8	6	6	6	6	5	5	6	6	6	7	7	3	5	7	5	отсев	
41	7	9	9	5	8	6	6	6	7	7	7	9	6	8	8	8	4	8	8	5	8	6	6	6	6	6	годен	годен
42	8	7	7	9	7	7	6	3	7	6	8	3	8	5	8	6	6	6	6	5	8	7	5	7	5	7	отсев	
43	9	9	8	7	4	5	9	5	7	5	8	5	6	6	6	6	8	3	7	6	5	6	8	6	5	5	отсев	
44	9	6	6	6	5	7	7	7	9	9	9	9	7	9	4	8	8	6	6	6	9	7	7	7	7	7	годен	годен
45	4	5	3	7	5	7	6	5	3	7	7	7	5	5	8	5	8	8	6	6	7	6	5	4	5	5	отсев	
46	7	7	6	6	5	4	7	7	8	6	6	8	8	5	7	7	7	6	6	8	8	6	8	8	8	8	годен	
47	9	6	6	8	4	8	8	5	6	6	5	5	6	6	6	6	6	3	6	7	8	7	7	5	5	5	отсев	отсев
48	6	6	8	8	7	7	7	8	8	6	6	6	9	7	8	8	8	6	8	8	8	3	6	9	9	9	годен	
49	6	9	9	7	7	7	8	9	3	8	7	8	8	8	9	7	8	7	7	6	8	6	9	7	9	8	годен	
50	8	8	9	7	8	9	8	8	8	6	7	8	6	7	6	8	8	5	8	7	7	5	9	9	6	8	годен	
51	5	7	7	8	4	8	9	7	6	7	9	9	9	9	4	6	6	7	9	7	9	8	9	7	9	7	годен	годен
52	7	8	8	8	7	5	6	5	5	7	8	5	8	9	9	7	4	8	8	8	6	7	7	5	8	7	годен	
53	6	7	7	5	5	7	8	9	9	9	7	7	7	8	3	8	7	8	8	6	6	5	8	6	5	5	годен	
54	3	5	6	7	4	7	6	8	5	6	8	5	7	7	8	6	6	8	6	7	6	5	5	4	8	6	отсев	отсев
55	2	4	6	5	5	5	6	8	5	6	7	7	6	6	6	5	8	8	5	5	6	8	7	6	7	5	отсев	

Продолжение таблицы 5.4

Компетенция	К1	К2	К2	К2	К2	К2	К3	К3	К3	К4	К5	К5	К5	К5	К5	К5	К6	К6	К6	К7	К7	К7	К7	К7	К7	Известный результат	Предсказанный результат
56	5	6	6	6	6	7	5	7	5	5	6	5	5	6	8	6	6	6	8	3	7	6	8	6	7	6	отсев	отсев
57	4	5	6	6	7	4	5	6	4	5	7	7	7	6	5	7	8	5	8	6	7	5	8	5	7	7	годен	годен
58	3	4	4	4	5	8	6	8	6	5	6	6	7	7	5	5	7	7	5	6	7	7	8	6	8	5	отсев	
59	4	5	5	5	4	4	5	6	4	6	9	9	9	8	4	7	7	7	3	9	8	8	8	6	8	8	годен	
60	6	5	5	6	7	8	9	8	7	6	6	7	9	9	7	9	8	8	6	6	8	8	9	9	7	7	годен	годен
61	4	5	5	4	3	5	7	8	6	6	7	3	8	7	8	6	6	6	5	7	7	7	8	5	8	6	отсев	
62	6	7	7	8	5	8	7	7	5	6	7	6	8	7	8	5	3	7	7	7	6	6	6	6	8	7	отсев	отсев
63	9	9	7	7	6	7	5	7	4	6	6	7	7	5	7	6	7	6	5	8	8	7	5	7	7	6	годен	
64	6	7	7	5	4	5	7	6	5	6	6	5	6	5	5	5	5	8	6	7	6	8	5	6	3	6	отсев	
65	3	3	5	5	4	7	6	8	6	6	6	7	7	5	7	6	6	6	6	5	7	7	8	5	8	6	отсев	отсев
66	8	7	8	6	6	5	5	6	4	4	7	5	8	5	8	5	8	7	7	6	4	6	4	6	6	6	отсев	
67	4	4	3	5	5	7	7	7	6	5	7	6	7	7	4	6	8	8	6	5	7	5	8	6	8	5	отсев	
68	5	6	6	6	6	5	5	7	7	7	5	5	6	7	8	7	8	6	3	6	7	6	6	5	5	7	отсев	отсев
69	7	7	5	5	4	7	6	8	9	9	9	8	8	5	5	9	5	5	8	8	5	6	6	7	8	9	годен	годен
70	9	9	8	8	8	9	9	8	8	9	9	7	7	7	8	8	8	6	9	9	8	6	8	7	8	7	годен	
71	3	3	5	5	4	7	6	7	6	6	6	6	6	6	5	6	6	7	5	5	7	7	5	6	5	7	отсев	отсев
72	4	4	6	6	6	4	4	3	6	8	8	9	7	8	8	6	8	8	8	8	5	7	7	9	7	8	годен	
73	9	9	9	6	6	8	8	8	4	5	8	6	6	6	5	9	7	7	8	6	9	6	6	3	9	9	годен	
74	5	5	4	6	6	6	7	8	9	9	7	7	8	8	7	8	5	6	8	8	7	7	8	9	7	7	годен	годен
75	9	5	7	5	6	7	7	9	6	5	7	6	7	6	7	5	7	6	3	6	6	5	6	7	5	7	отсев	отсев
76	7	7	6	6	8	8	7	7	7	8	8	9	6	6	6	6	5	9	7	7	8	7	6	8	8	8	годен	
77	4	4	4	5	6	6	6	4	5	5	7	7	9	7	7	7	5	5	6	6	8	5	7	6	8	7	отсев	
78	5	5	4	3	5	7	5	8	5	5	9	7	7	6	8	6	8	7	7	6	6	6	6	6	8	5	отсев	отсев
79	6	6	5	5	4	7	7	8	8	8	8	9	9	9	7	6	9	7	7	9	7	7	7	4	9	9	годен	
80	5	6	6	8	6	7	8	8	6	7	5	8	8	5	6	8	4	8	5	6	6	5	8	7	7	7	годен	годен
81	5	6	6	8	5	5	6	9	6	6	8	6	5	5	3	5	8	8	6	7	6	8	6	6	6	6	отсев	отсев
82	7	7	8	8	9	9	9	7	6	6	8	8	8	9	7	7	8	6	6	9	7	7	9	7	6	6	годен	
83	4	7	7	9	9	6	6	4	3	4	9	9	4	6	7	8	8	8	6	6	6	5	4	6	5	6	годен	
84	6	6	7	8	9	8	7	8	7	9	9	7	8	7	7	7	8	8	9	6	6	8	7	7	7	7	годен	
85	9	9	8	7	8	7	8	9	9	9	8	8	8	9	7	7	3	6	6	8	8	8	9	9	7	7	годен	годен

Продолжение таблицы 5.4

Компетенция	К1	К2	К2	К2	К2	К2	К3	К3	К3	К4	К5	К5	К5	К5	К5	К6	К6	К6	К7	К7	К7	К7	К7	К7	К7	Известный результат	Предсказанный результат
86	5	6	5	7	6	8	6	8	8	8	6	6	9	9	7	5	8	8	7	7	7	8	8	6	6	6	годен	
87	3	3	5	6	4	5	3	3	7	5	7	5	5	6	7	6	9	5	6	3	6	6	8	7	5	7	отсев	отсев
88	8	8	6	6	8	7	9	9	7	9	9	7	7	7	7	9	7	4	8	7	7	9	7	7	7	7	годен	
89	5	7	7	7	8	6	9	9	7	7	8	8	8	7	7	8	5	6	6	7	9	7	8	8	9	6	годен	годен
90	7	7	7	7	9	9	9	8	8	8	8	6	6	6	6	6	9	5	8	7	3	8	5	7	7	7	годен	
91	5	5	5	8	6	5	5	6	5	6	8	4	9	3	7	6	6	8	5	6	6	7	7	6	8	6	отсев	отсев
92	5	8	8	9	9	8	9	7	7	7	8	7	7	7	9	4	7	8	8	9	7	6	8	8	9	9	годен	
93	4	6	6	7	5	5	4	4	3	3	8	7	6	6	6	7	8	8	6	5	7	7	7	3	8	6	отсев	отсев
94	4	6	5	5	6	4	5	5	7	6	8	7	7	7	9	7	7	7	8	8	7	6	6	8	7	7	годен	
95	8	7	8	7	8	8	9	8	7	9	6	6	6	5	7	8	7	6	5	8	6	7	8	9	7	6	годен	годен
96	5	7	7	7	5	7	5	6	7	9	9	8	9	9	8	3	9	9	8	7	7	9	8	8	9	8	годен	
97	9	9	8	7	9	9	6	7	9	9	8	6	8	8	6	6	8	9	7	7	8	7	5	6	7	8	годен	
98	8	8	7	7	9	9	5	9	7	7	8	8	8	5	7	7	9	7	7	6	8	9	8	5	8	7	годен	годен
99	4	7	7	6	4	4	6	5	5	7	7	8	8	8	7	7	8	6	8	8	7	7	6	6	7	7	годен	
100	8	9	8	9	7	5	8	8	8	8	8	7	7	5	8	8	6	6	6	6	3	9	9	7	7	7	годен	годен
101	8	5	5	5	8	9	9	9	7	7	8	8	9	6	6	9	7	7	6	8	9	7	6	8	6	6	годен	
102	3	3	6	6	3	4	7	8	5	5	8	9	6	6	7	7	7	5	5	7	7	7	5	6	5	6	отсев	отсев
103	6	6	8	8	6	8	9	9	9	9	8	8	8	7	8	7	8	9	8	8	6	8	7	7	7	8	годен	годен
104	7	7	8	6	6	8	9	6	8	8	7	7	7	5	6	6	6	5	9	9	5	7	7	9	8	8	годен	

Выводы к главе 5

1. Разработан новый подход к понятию человеческий фактор в транспортной безопасности, когда это не человек и не фактор, а полноправный функциональный элемент системы обеспечения безопасности, негативное влияние которого в структуре системы транспортной безопасности неизбежно, и рассматривается как угроза безопасности аэропорта в совокупности с другими внешними и внутренними угрозами, что дает возможность применить единую методологию исследования опасностей. Анализ степени участия специалиста в процессах обеспечения транспортной безопасности заменяется исследованием и разработкой методики управления уровнем негативного влияния персонала на процедуры обеспечения транспортной безопасности.

2. Негативное влияние персонала проявляется как результат ошибок при реализации целевого функционала его деятельности, т.е. ошибки следует рассматривать как составную часть основной деятельности персонала по обеспечению транспортной безопасности. Уровень несанкционированного вмешательства персонала отражает часть его профессиональной деятельности, не обусловленную соответствующими нормативными документами, количественной характеристикой которого становится качество его профессиональной деятельности, что превращает качество в критерий оптимизации уровня негативного влияния персонала.

3. Несанкционированное вмешательство персонала рассматривается как угроза безопасности аэропорта, т.е. угроза персонала ассоциируется с негативным влиянием персонала и сопоставляется с внешними угрозами безопасности объекта защиты. Однако, если внешние угрозы при своей реализации становятся субъектами прямого действия, то угрозы персонала прямого действия не имеют. Ошибка персонала, как основной элемент угрозы, изменяет процедуру защиты объекта, тем самым изменяя ситуацию в системе защиты объекта, снижает качество защиты и снижает уровень безопасности. Исследование внешних угроз возможно

путем их представления в формате гипотетических полей и с использованием методов математического моделирования. Такой подход к исследованию угроз персонала невозможен, поэтому необходимы эвристические методы и теория принятия решений.

4. Разработаны функциональные и структурно-логические модели системы минимизации негативного влияния персонала на транспортную безопасность аэропорта, отражающие предложенный подход в оценке человеческого фактора, рассматривающий незаконное вмешательство персонала как угрозу безопасности объектов гражданской авиации, а ошибку персонала как фактор реализации угрозы. Предложенные модели разработаны до уровня функциональных элементов и отдельных процедур.

5. Разработана компетентностная модель оценки уровня профессиональной подготовки персонала и иерархическая структура компетенций, определяющие порядок оценки качества профессиональной подготовки авиационного специалиста, на основе чего принимается решение о готовности специалиста исполнять свои функциональные обязанности.

6. Разработаны алгоритмы работы системы минимизации негативного влияния персонала и системы коррекции, определяющие функциональные процедуры и этапы решения задачи управления уровнем негативного влияния персонала. Разработан алгоритм квалиметрической оценки компетенций и компетентности специалиста, реализующий функционал коррекции уровня готовности персонала к выполнению профессиональных обязанностей. Все алгоритмы разработаны в рамках инцидентного подхода к функционированию СМНВП и ESM, а в структуре алгоритмов предусмотрена возможность перехода к информационному управлению, основанному на принципах PSIM с применением технологии DATA MINING.

7. Установлена причина появления угрозы персонала, которой является неадекватность содержания процедур и параметров деятельности персонала параметрам ситуации в объекте защиты, обусловленная несовершенством

человека, что проявляется в отклонениях параметров алгоритма деятельности персонала от параметров стандартных эксплуатационных процедур.

8. Показано, что система управления уровнем несанкционированного вмешательства персонала не может быть создана как самостоятельная, автономная структура, поскольку несанкционированное вмешательство есть определенная часть общей профессиональной деятельности персонала по обеспечению транспортной безопасности. Тогда, система управления несанкционированным вмешательством должна быть встроена в систему более высокого уровня, занимающуюся обеспечением транспортной безопасности аэропорта при условии согласования информационных, технических, организационных, временных и других параметров обеих систем.

9. Задача классификации персонала транспортной безопасности с точки зрения его готовности исполнять свои профессиональные функции в соответствии с требованиями решена в нейросетевом базисе путем создания нейроклассификатора с использованием инструментов MATLAB и автономного классификатора, включающего два программных комплекса Neuronet и Neurotest, которые обеспечили высокое качество работы.

ЗАКЛЮЧЕНИЕ

1. В работе впервые решена научная проблема повышения эффективности управления транспортной (авиационной) безопасностью аэропорта. Проблема состоит в методологических ограничениях на возможности управления, обусловленные принципами теории управления организационными структурами (менеджмент), на основе которых построены действующие системы обеспечения транспортной безопасности. Решение предполагает научное обоснование, разработку и реализацию корректного перехода от концепции обеспечения безопасности к концепции эффективного управления в терминах теории оптимального управления.

2. Разработаны: гипотеза исследования, предполагающая решение проблем на основе методологии информационного управления безопасностью с применением современных технологий; принципы интеллектуального управления транспортной безопасностью, основанные на оптимальном, ситуационном и адаптивном подходах к управлению; концепция информационного управления транспортной безопасностью, основанная на методах системотехники, теории оптимального управления, теории краевых задач и квалиметрии, системообразующем понятием которой является понятие «информационно – управляющее пространство», рассматриваемое как некоторый интерфейс между противоборствующими пространствами (угроз и защиты), что обеспечивает адекватное соответствие модели информационно-управляющего пространства и приемлемого уровня транспортной безопасности аэропорта.

3. Разработан алгоритм формирования структуры информационно-управляющего пространства (ИУП), включающий несколько принципиально важных комплексных этапов: разработка виртуальной модели ИУП, разработка структурно-логической модели ИУП, разработка функциональных моделей системы мониторинга и системы обработки, разработка системной модели формализации и алгоритмизации процессов безопасности, разработка ситуативной

модели управления, реализация которых создает основу теории и практики информационного управления транспортной безопасностью.

4. Разработанная структура информационно-управляющего пространства представлена на трех уровнях: доменный уровень отражает основные направления и функциональные границы информационных массивов, однородных по смысловому содержанию; кластерный уровень формирующий предметные области математического моделирования, однородные с точки зрения методологии и различающиеся по функциональным признакам; функциональный уровень (матричная структура), включающий структурированную совокупность процедурных решений по управлению транспортной безопасностью, что упрощает процедуры моделирования и оптимизирует процессы алгоритмизации информационного управления.

5. Оптимизация процедур управления транспортной безопасностью предполагается как процесс достижения приемлемого уровня этой безопасности с использованием уязвимости в качестве критерия оптимальности. Модель уязвимости включает количественные оценки угроз, полученные в результате численного моделирования процесса их распространения в формате дифференциальных уравнений в частных производных (стационарная задача) и пространства уязвимостей (нестационарная задача).

6. Процедуры перехода от угроз к уязвимостям и от уязвимостей к угрозам реализуются на основе квалиметрического подхода, где количественные значения определяют и отражают степень соответствия параметров угроз (уязвимостей) заданным требованиям к критическим элементам системы защиты объекта с учетом масштабирования. Численное моделирование предполагает различные варианты распределения угроз или типов уравнений, что определяет статистический подход к формированию окончательного решения, включая эвристические процедуры. Результаты численного моделирования получены в относительных единицах опасности (безопасности), не привязанных к реальным параметрам угроз и не связанных с моделью нарушителя, что позволило решить

методологические и процедурные вопросы, сохранив при этом достоверность и адекватность используемых моделей.

7. В работе впервые исследованы возможности применения принципов искусственного интеллекта в задачах управления транспортной безопасностью аэропорта. Для ранжирования аэропортов по степени соответствия требованиям безопасности разработана нейросетевая модель на основе инструмента визуального программирования Neural Network Pattern Recognition Tool пакета Deep Learning Toolbox системы MATLAB, обеспечившая следующее качество работы классификатора: Precision – 1.0, Recall – 0.9, Specificity – 0.83, F-score – 0.95.

8. Исследованы факторы несанкционированного вмешательства персонала авиационной безопасности аэропорта в процедуры обеспечения безопасности в процессе своей профессиональной деятельности. Негативное влияние персонала рассматривается как угроза безопасности, идентифицируется в совокупности внешних и внутренних угроз, встраивается в структуру универсальных моделей безопасности с использованием эвристических алгоритмов.

9. Установлена причина появления угрозы безопасности аэропорта со стороны авиационного персонала, квалифицируемая как несанкционированное вмешательство, в основе чего лежит ошибка, т.е. неадекватность содержания процедур и параметров деятельности персонала параметрам ситуации в объекте защиты, что проявляется в отклонениях параметров алгоритма деятельности персонала от параметров стандартных эксплуатационных процедур безопасности. Разработана методология минимизации негативного влияния персонала на производственную деятельность, основанная на понятиях индекс ошибки и инцидент. В результате функционального и структурно-логического анализа на этой основе разработаны модели оптимизации процедур минимизации негативного влияния персонала.

10. Решена задача классификации персонала транспортной безопасности с точки зрения его готовности исполнять свои профессиональные функции в соответствии с требованиями транспортной безопасности. Задача решена в

нейросетевом базисе путем создания нейроклассификатора, с использованием инструментов MATLAB, и автономного классификатора, включающего два программных комплекса Neuronet и Neurotest.

СПИСОК СОКРАЩЕНИЙ И УСЛОВНЫХ ОБОЗНАЧЕНИЙ

АБ – авиационная безопасность

АВК – аэровокзальный комплекс

АВС – аэровокзальная служба

АИОС – автоматизированная информационно-обучающая система

АИСУ – автоматизированная информационная система управления

АНВ – акт незаконного вмешательства

АНП – анализ надежности персонала

АП – авиационное происшествие

АС – аварийная ситуация

АТ – авиационная техника

АТС – авиационная транспортная система

БП – безопасность полетов

ВАБ – вероятностный анализ безопасности

ВС – воздушное судно

ВУ – взрывное устройство

ГА – гражданская авиация

ГИС – геоинформационные системы

ЕКГА – Европейская конференция гражданской авиации

ЗПР – задача принятия решений

ИАС – инженерно-авиационная служба

ИАТА – международная ассоциация воздушного транспорта

ИКАО – международная организация гражданской авиации

ИС – исходное событие / интегрированная система

ИТС – инженерно-технический состав

КИС – корпоративная информационная система

КПП – контрольно-пропускной пункт

КС – катастрофическая ситуация

КЭ – критический элемент

ЛПР – лицо, принимающее решение

ЛС – лётный состав

МВД – министерство внутренних дел

НПП – наставление по производству полетов

ОрВД – организация воздушного движения

ОС – особая ситуация

ОТИ – объект транспортной инфраструктуры

РУБП – руководство по управлению безопасностью полетов

САБ – служба авиационной безопасности

СБ – система безопасности

СП – системный подход

СППД – субъект противоправной деятельности

СС – служба связи

ССОИ – система сбора и обработки информации

СУ – система управления

СУБД – система управления базами данных

СУБП – система управления безопасностью полетов

СЭП – стандартная эксплуатационная процедура

ТБ – транспортная безопасность

ТКС – телекоммуникационная среда

ТПР – теория принятия решений

ТС – технические средства

ТЭ – техническая эксплуатация

УАБ – уровень авиационной безопасности

УВД – управление воздушным движением

ФАП – федеральные авиационные правила

ФД – функциональная деятельность

ФС – функциональная система

ФУ – функциональное управление

ЧФ – человеческий фактор

ESM – Electronika Security Manager

Data Mining – интеллектуальный анализ данных

PSIM – Physical Security Information Management

СПИСОК ЛИТЕРАТУРЫ

1. Айзерман М.А. Выбор вариантов: основы теории / М.А. Айзерман, Ф.Т. Алескеров. – Москва: Наука, 1990. -240 с.

2. Акимов В.А. и др. Природные и техногенные чрезвычайные ситуации: опасности, угрозы, риски. – Москва: ЗАО ФИД «Деловой экспресс», 2001– 344 с.

3. Акоф Ф.Р. О целеустремленных системах : пер. с англ. / Ф.Р. Акоф, Ф.О. Эмери. – Москва: Сов. Радио, 1974. – 271с.

4. Алексеев О.Г. Комплексное применение методов дискретной оптимизации. Москва: Наука, 1987. – 154 с.

5. Алыгин А.П. Риск и его роль в общественной жизни. – Москва: Мысль,1989. –187 с.

6. Анфилатов В.С. Системный анализ в управлении / В.С. Анфилатов, А.А. Емельянов, А.А. Кукушкин – Москва: Финансы и статистика, 2003. – 368 с.

7. Анцупов А.Я., Шипилов А.И. Конфликтология: учебник для вузов / А.Я. Анцупов, А.И. Шипилов – Москва: ЮНИТИ, 1999. -551с.

8. Аоки М. Оптимизация стохастических систем – Москва: Наука, 1971. – 360 с.

9. Ариничева О.В. Совершенствование методов управления ресурсами системы «экипаж – воздушное судно» путем снижения влияние человеческого фактора на безопасность полетов: автореф. дисс. … канд. техн. наук: 05.22.14. – Санкт-Петербург, 2008. – 20 с.

10. Бекмухамбетов А.А. Совершенствование деятельности оператора на базе теории и практики управления рисками при обеспечении безопасности полетов: автореф. дисс. ... канд. техн. наук: 05.22.14. – Санкт-Петербург, 2005. - 20 с.

11. Берсенев В.Л. Экстремальные задачи стандартизации / В.Л. Берсенев, Э.Х. Гимади, В.Т. Дементьев – Новосибирск: Наука, 1978. – 335 с.

12. Бешелев С.Д. Экспертные оценки в принятии плановых решений. – МОСКВА: Экономика, 1976. – 240 с.

13. Бешелев С.Д. Математико-статистические методы экспертных оценок / С.Д. Бешелев, Ф.Г. Гуревич – Москва: Статистика, 1980. – 264 с.

14. Благоразумов А.К. Разработка системы информационного мониторинга безопасности авиационной деятельности / А.К. Благоразумов, Г.Е. Глухов, И.Г. Кирпичев // Научный вестник МГТУ ГА. – 2015. – № 218. – С. 67-70.

15. Бокс Дж., Дженкинс Г. Анализ временных рядов, прогноз и управление: пер. с англ. / Под ред. В.Ф. Писаренко. – Вып. 1 и 2. – Москва: Мир, 1974. – 406 с.

16. Большие системы: моделирование организационных механизмов / В.Н. Бурков, Б. Данеев, А.К. Еналеев и др. // Академия наук СССР (АН СССР), Институт проблем управления им. В. А. Трапезникова (ИПУ); под ред. В. И. Опойцева. – Москва : Наука, 1989. – 245 с. – ISBN 5-02-006561-7.

17. Борисов В.И. Проблемы векторной оптимизации. Исследование операций // Методологические аспекты. – Москва: Наука, 1972. – С.102-113

18. Брусникин В.Ю. Оптимизация процесса обмена информацией между авиапредприятиями в рамках единого информационного пространства / В.Ю. Брусникин, Г.Е. Глухов, С.А. Гаранин // Научный вестник ГосНИИ ГА. – 2017. – № 17. – С. 27-33.

19. Брукинг Э. Интеллектуальный капитал : пер. с англ. / Под ред. Л.Н. Ковалик. – Санкт-Петербург: Питер, 2001. – 288 с.

20. Бурков В.Н. Модели и механизмы теории активных систем в управлении качеством подготовки специалистов / В.Н. Бурков, Д.А. Новиков. – Москва: Исследовательский центр проблем качества подготовки специалистов, 1998. – 157 с.

21. Бурков В.Н. Введение в теорию управления организационными системами / В.Н. Бурков, Н.А. Коргин, Д.А. Новиков // ред. Д.А. Новикова. Изд. 2-ое – Москва: Книжный дом «Либроком», 2014. – 264 с.

22. Бусленко Н.П. Моделирование сложных систем – Москва: Наука, 1978. – 400 с.

23. Вазов В. Разностные методы решения дифференциальных уравнений в частных производных / В. Вазов, Дж. Форсайт. – Москва: ИЛ. 1963. – 488 с.

24. Вальковский В.А. Алгоритмы, математическое обеспечение и архитектура многопроцессорных вычислительных систем / В.А. Вальковский , В.Е. Котов, Й. Миклошко. – Москва: Наука, 1982. – 336 с.

25. Ван Гиг Дж. Общая прикладная теория систем: В 2-х т.: пер. с англ. – Москва: Мир, 1981. – Т.1 – 336 с. ; Т.2 – 736 с.

26. Вентцель Е.С. Теория случайных процессов и ее инженерные приложения / Е.С. Вентцель, Л.А. Овчаров. – Москва: Наука, 1991. – 360 с.

27. Вилкас Э.И. Решения: теория, информация, моделирование / Э.И. Вилкас, Е.З. Майминас. – Москва: Радио и связь, 1981. – 328 с.

28. Владимиров В.А. Оценка риска и управление техногенной безопасностью. Монография / В.А. Владимиров, В.И. Измалков, А.В. Измалков. – Москва: ФИД «Деловой экспресс», 2002. – 184 с.

29. Власова Е. А. Приближенные методы математической физики / Е. А. Власова, В. С. Зарубин, Г. Н. Кувыркин; Под ред. В. С. Зарубина, А. П. Крищенко. – Москва: Издательство МГТУ им. Н. Э. Баумана, 2001. – 700 с.

30. Воеводин В.В. Математические модели и методы в параллельных процессах – Москва: Наука, 1985. – 296с.

31. Волков А.К. Разработка и исследование моделей и алгоритмов поддержки принятия решений в задачах обеспечения авиационной безопасности: автореф. дисс. … канд. техн. наук : 05.22.14 – Москва: ГосНИИГА, 2019. – 20 с.

32. Волков А.К. Методы мониторинга деятельности операторов досмотровой техники службы авиационной безопасности аэропортов: автореф. дисс. … канд. техн. наук : 05.22.14 – Москва: ГосНИИГА, 2018. – 20 с.

33. Волынский В.Ю. Методологические основы оценки уязвимости объектов гражданской авиации к актам незаконного вмешательства в их деятельность / Ю.М. Волынский-Басманов, Ю.Б. Михайлов, А.Ю. Федоров // Транспортная безопасность и технологии. – 2011. – № 1(24). – С. 66-75.

34. Волынский-Басманов Ю.М. Методика определения и количественной оценки рисков получения объектами гражданской авиации ущербов в результате реализации актов незаконного вмешательства / Ю.М. Волынский-Басманов, Ю.Б. Михайлов // Транспортная безопасность и технологии. – 2011. – № 3 (26). – С. 66-70.

35. Волынский Б.А. Модели для решения краевых задач / Б.А. Волынский, В.Е. Бухман. – Москва: Физматгиз, 1960. – 451 с.

36. Воробьев А.С. К вопросу об обеспечении безопасности полетов гражданской авиации на основе управления рисками / А.С. Воробьев, С.А. Воронин, В.М. Сохабеев // Научный вестник ГосНИИ ГА. – 2014. – № 6. – С. 83-88.

37. Головкин Б.А. Параллельные вычислительные системы. – Москва: Наука, 1980. – 520 с.

38. Горбаченко В.И. Нейрокомпьютеры в решении краевых задач теории поля. Уч. пособие для вузов. – Москва: Радиотехника, 2003. – 336 с.

39. Горбаченко В. И. Вычислительная линейная алгебра с примерами на MATLAB. – Санкт-Петербург: БХВ-Петербург, 2011. – 320 с.

40. ГОСТ Р 56461-2015. Национальный стандарт РФ. Безопасность транспортная. Общие требования : дата введения 2015-06-15 / Росстандарт. – Москва: Стандартинформ, 2015. – 14 с.

41. Данскин Дж. М. Теория максимина: пер. с англ. – Москва: Сов. Радио, 1970. – 200 с.

42. Деревнина А.Ю. Модели и методы стратегического управления университетом на основе эволюционного подхода: автореф. дисс… д-ра техн. наук : 05.13.10 / Деревнина Анна Юрьевна. – Москва: ИЦПКПС, 2007. – 40 с.

43. Демин Д.С. Исследование социальных аспектов в структуре транспортной безопасности гражданской авиации / Д.С. Демин, В.В. Джамай, Н.И. Овченков // Вестник Московского государственного областного университета. Серия: Экономика. – 2023. – №1. – С. 44-53.

44. Дружинин Г.В. Методы оценки и прогнозирования качества. – Москва: Радио и связь, 1982. – 160 с.

45. Дружинин В.В. Вопросы военной системотехники / В.В. Дружинин, Д.С. Конторов. – Москва: Воениздат, 1976. – 224 с.

46. Дружинин В.В. Системотехника / В.В. Дружинин, Д.С. Конторов – Москва: Радио и связь, 1985. – 200 с.

47. Дружинин В.В. Введение в теорию конфликта / В.В. Дружинин, Д.С. Конторов. – Москва: Радио и связь, 1989. – 288 с.

48. Дружинин В.В. Проблемы системологии: проблемы теории сложных систем / В.В. Дружинин, Д.С. Конторов – Москва: Сов. радио, 1976. – 296 с.

49. Друкер П. Эффективное управление: пер. с англ. – Москва: Фаир-пресс, 2003. – 284 с.

50. Евланов Л.Г. Теория и практика принятия решений. – Москва: Экономика, 1984. – 176 с.

51. Евланов Л.Г. Экспертные оценки в управлении / Л.Г. Евланов, В.А. Кутузов – Москва: Экономика, 1978. – 132 с.

52. Елисеев Б.П. К вопросу надежности человека – оператора в системе управления авиационным персоналом / Б.П. Елисеев, Е.В. Марьенкин // Научный вестник МГТУГА. – Москва: МГТУГА, 2011. – №174. – С. 35-39.

53. Елисеев Б.П. Некоторые замечания по поводу понятия риск в связи с управлением авиационным персоналом / Б.П. Елисеев, Е.В. Марьенкин // Научный вестник МГТУГА. – Москва: МГТУГА, 2011. №174. – С. 39-43.

54. Елисеев Б.П. Методология системотехнического управления профессиональным образованием в гражданской авиации: дис. д-ра техн. наук : 05.13.10. / Елисеев Борис Петрович. – Уфа, 2011. – 410 с.

55. Елисов Л.Н. Методология и средства квалиметрии инженерно-технического состава гражданской авиации: автореф. дисс. … докт. техн. наук : 05.22.14., 05.13.10. / Елисов Лев Николаевич. – Москва: МГТУГА, 1995. – 40 с.

56. Елисов Л.Н. К вопросу о точности эвристических алгоритмов при решении оптимизационных задач в эксплуатации / Научный вестник МГТУГА. – 2012. – № 179. – С. 123-126.

57. Елисов Л.Н. Качество профессиональной подготовки авиационного персонала и безопасность полетов. – Москва: ИЦПКПС, 2006. – 244 с.

58. Елисов Л.Н. Концепция управления авиационной безопасностью на основе квалиметрических оценок ее состояния // Научный вестник МГТУГА. – Москва: МГТУГА, 2004. – №75(9). – С. 107-113.

59. Елисов Л.Н. Управление и сертификация в АТС: монография / Л.Н. Елисов, В.В. Баранов. – Москва: Воздушный транспорт, 1999. – 352 с.

60. Емельянов А.М. Использование фреймов для анализа структуры поступков // Сб.: Проблемы бионики. – Харьков, 1980. – вып. 25. – С. 43-58.

61. Емельянов С.В. Многокритериальные методы принятия решений. / С.В. Емельянов, О.И. Ларичев. – Москва: Знание, 1986. – 29 с.

62. Жмеренецкий В.Ф. Активное обеспечение безопасности полета летательного аппарата: методология, модели, алгоритмы / В.Ф. Жмеренецкий, К.Д. Полулях, О.Ф. Акбашев. – Москва: Леланд, 2014. – 320 с.

63. Интеллектуальные интерактивные учебно-тренировочные комплексы / Авторский коллектив под общей редакцией д.т.н., проф. Васильца В.М. – Москва: Воениздат. 2006. – 260 с.

64. К вопросу о теории авиационной безопасности / Л.Н. Елисов, В.Л. Филиппов, Н.И. Овченков, С.М. Мусин // Научный вестник ГосНИИГА, 2019. – №27. – С. 109-120.

65. Каллан Р. Основные концепции нейронных сетей: пер. с англ. – Москва: ИД Вильямс, 2003. – 288 с.

66. Кафидов В.В. Управление персоналом. – Москва: Академический проект, 2003. – 144 с.

67. Квейд Э. Анализ систем: пер. с англ. – Москва: Сов. радио, 1975. – 447 с.

68. Кини Р.Л. Принятие решения при многих критериях предпочтения и запрещения / Р.Л. Кини, Г. Райфа. – Москва: Радио и связь, 1977. – 302 с.

69. Клейнер Г.Б. Производственные функции: Теория, методы, применение. – Москва: Финансы и статистика, 1986. – 239 с.

70. Климов С.М. Интеллектуальные ресурсы общества. – Санкт-Петербург: ИВЭСЭП, Знание, 2002. – 199 с.

71. Козлов В.В. Безопасность полетов: от обеспечения к управлению. – Москва: Оперативная полиграфия, 2010. – 144 с.

72. Козлов В.В. Человеческий фактор: история, теория и практика в авиации. – Москва: Полиграф, 2002. – 280 с.

73. Конвенция о борьбе с незаконными актами в отношении международной гражданской авиации. – Пекин: ИКАО, 2010. – Doc 9960. – 14 с.

74. Котик М.А. Природа ошибок человека-оператора (на примерах управления транспортными средствами) / М.А. Котик, А.М. Емельянов. – Москва: Транспорт, 1993. – 252 с.

75. Котик М.А. Ошибки управления / М.А. Котик, А.М. Емельянов. – Таллинн: Валгус, 1985. – 390 с.

76. Косьянчук В.В. Применение линейных регрессионных моделей для прогнозирования динамики рисков при обеспечении безопасности полетов / В.В. Косьянчук, И.А. Селиванов. // Научный вестник ГосНИИ ГА. – 2018. – №23. – С. 110-122.

77. Кошкин Р.П. Математические модели процессов создания и функционирования поисково-аналитических информационных систем гражданской авиации // Научный вестник ГосНИИ ГА. – 2014. – № 5. – С. 39-49.

78. Крапивин Е.Ф. Теоретико-игровые методы синтеза сложных систем в конфликтных ситуациях. – Москва: Сов.радио, 1972. – 117 с.

79. Круглов В. В. Искусственные нейронные сети. Теория и практика / В. В. Круглов, В. В. Борисов. – Москва: Горячая линия - Телеком, 2001. – 382 с.

80. Круглякова О.В. Человеческий фактор и безопасность полетов. // Сб. Логико-методологические проблемы технической эксплуатации ЛА и обеспечения безопасности полетов. – Москва: МИИГА, 1991. – С. 112-121.

81. Куклев Е. А. Автоматизированная система мониторинга и контроля полетов воздушных судов по критерию приемлемого риска на основе управления базами данных // Научный Вестник МГТУ ГА: серия Эксплуатация воздушного транспорта и ремонт авиационной техники. Безопасность полетов. – 2007. – № 122 (12). – С. 37-44.

82. Куклев, Е. А. Оценивание уровня безопасности полетов в гражданской авиации в рисковых ситуациях на основе цепей случайных событий // Наука и техника транспорта. – 2003. – №2. – С. 4-14.

83. Ларичев О.И. Теория и методы принятия решений. – Москва: Логос, 2000. –296 с.

84. Литвак Б.Г. Экспериментальная информация: методы получения и анализа. – Москва: Радио и связь, 1982. – 184 с.

85. Лукашин Ю.П. Адаптивные методы краткосрочного прогнозирования. – Москва: Статистика, 1979. – 253 с.

86. Лукашин Ю.П. Регрессионные и адаптивные методы прогнозирования. – Москва: МЭСИ, 1997. – 54 с.

87. Льюс Р.Д. Игры и решения : пер. с англ. / Р.Д. Льюс, Х. Райфа. – Москва: Иностр. литература, 1961. – 642 с.

88. Месарович М. Теория иерархических многоуровневых систем / М. Месарович, Д. Мако, Я. Такахара. – Москва: Мир, 1973. – 344 с.

89. Месарович М. Общая теория систем: математические основы / М. Месарович, Я. Такахара. – Москва: Мир, 1978. – 312 с.

90. Михайлов Ю.Б. Безопасность на транспорте и ее количественная оценка / Ю.Б. Михайлов, Ю.М. Волынский-Басманов. – Москва: НУЦ Абинтех, 2012. – 268 с.

91. Михеева Е.Н. Управление качеством. – Москва: Дашков и К., 2010. – 708 с.

92. Многокритериальные задачи принятия решений / Под ред. Д.М. Гвишиани, С.В. Емельянова. – Москва: Машиностроение, 1978. – 192 с.

93. Моисеев Н.Н. Математические задачи системного анализа. – Москва: Наука, 1981. – 488 с.

94. Моисеев Н.Н. Элементы теории оптимальных систем. – Москва: Наука, 1975. – 526 с.

95. Мушик Э., Мюллер П. Методы принятия технических решений: пер с нем. – Москва: Мир, 1990. – 208 с.

96. Налобин Н.В. Организация системы авиационной безопасности аэропорта на основе методов количественной оценки ее состояния: дисс. … канд. техн. наук : 05.02.22. / Налобин Николай Валентинович. – Москва, 2005. – 197 с.

97. Нейросетевая классификация авиационного персонала как элемент информационно-управляющего пространства безопасности объекта транспортной инфраструктуры / Л.Н. Елисов, Н.И. Овченков, В.И. Горбаченко, И.А. Абрамов // Нейроинформатика, ее приложения и анализ данных, XXVIII Всероссийский семинар: материалы. – Красноярск: Институт вычислительного моделирования СО РАН, 2020. – С. 66-73.

98. Нил Д. Кластеры вместо суперкомпьютеров // Computerworld Россия. – 23.01.2001. – № 2 (259). – 26 с.

99. Новиков П.П. Принятие решений человеком в авиационных системах управления. – Москва: Воздушный транспорт, 1980. – 348 с.

100. Ноздрин В.И. Ошибки членов экипажа воздушного судна – признак несовместимости действий экипажа, условий полета и реакции воздушного судна //ВИНИТИ. Проблемы безопасности полетов. – Москва: 1998. – №6. – С. 25-27.

101. Носов Н.А. Инженерно-психологический анализ спорадических ошибок оператора и способы их предупреждения: автореф. дисс. … канд. психол. наук: 19.00.03. – Москва: 1981. - 16 с.

102.Обеспечение безопасности и правопорядка в транспортной политике России. Тезисы выступлений МНПК. – Москва: ВНИИ МВД России, Гос ЦНИАТ, 2003. – 265 с.

103. Овченков Н.И. Методы динамической интеграции средств обеспечения авиационной безопасности аэропорта: автореф. дисс. … канд. техн. наук : 05.22.14. – Москва: МГТУГА, 2015. – 20 с.

104.Овченков Н.И. Об особенностях применения отечественных программных продуктов для обеспечения транспортной безопасности // Транспортная безопасность и технологии, 2016. – №1(44). – С. 38-39.

105.Овченков Н.И. PSIM: фундаментальный принцип безопасности промышленных объектов // Алгоритм безопасности, 2016. – № 4. – С.70-73.

106. Овченков Н.И. Угрозы безопасности аэропортов: лучше предотвратить, чем ликвидировать // Аэропорт-партнер, 2004. – № 6. – С. 4-6.

107. Овченков Н.И. Кто предупрежден, тот вооружен, или как обеспечить безопасность аэропорта // Транспортная безопасность и технологии, 2005. – №1. – С. 72-74.

108. Овченков Н.И. Система безопасности: как не ошибиться в решении // Транспортная безопасность и технологии, 2005. – №2. – С. 82-84.

109. Овченков Н.И. Разработка концепции авиационной безопасности аэропорта: с чего начать // Транспортная безопасность и технологии, 2006. – №2 (7). – С. 2-5.

110. Овченков Н.И. Как сохранить полный контроль над объектом в условиях ужесточения требований законодательства к обеспечению авиационной безопасности // Транспортная безопасность и технологии, 2006. – №3 (8). – С. 8-11.

111. Овченков Н.И. Как обеспечить контролируемый доступ на территорию аэропорта и снизить негативное влияние человеческого фактора // Транспортная безопасность и технологии, 2007. – №1 (10). С.8-10.

112. Овченков Н.И. Управление человеческим фактором при построении системы безопасности // Транспортная безопасность и технологии, 2007. – №3 (12). – С. 10-13.

113. Овченков Н.И. Система безопасности должна строиться, исходя из задач руководителя, и оцениваться по экономической эффективности // Аэропорт-партнер, 2009. – №5. – С. 22-24.

114. Овченков Н.И. Комплексный подход к защите аэропорта: от модели к практической реализации // Транспортная безопасность и технологии, 2011. – №3 (26). – С. 72-74.

115. Овченков Н.И. Проблема адаптивности интегрированных систем авиационной безопасности аэропорта // Материалы IV международной молодежной научной конференции «Гражданская авиация-XXI век». – Ульяновск: УВАУ ГА, 2012. – С. 14-16.

116. Овченков Н.И. Квалиметрические принципы управления интеграцией технических средств авиационной безопасности аэропорта // Материалы IV международной молодежной научной конференции «Гражданская авиация – XXI век». – Ульяновск: УВАУ ГА, 2012. – С. 16-17.

117.Овченков Н.И. Некоторые проблемы обеспечения авиационной безопасности аэропорта и их решение / Л.Н. Елисов, Н.И. Овченков // «XXIV international scientific and technical conference Trans 16 MOTAUTO. Proceedings. – Bulgaria, Sofia, 2016. – vol 2. – pp. 73-74.

118. Овченков Н.И. Введение в теорию авиационной безопасности / Л.Н. Елисов, Н.И. Овченков, Р.С. Фадеев // под. общ. ред. Л.Н. Елисова. – Ярославль: Филигрань. 2016. – 320 с.

119.Овченков Н.И. Проблема человеческого фактора в области авиационной безопасности и некоторые подходы к её решению / Н.И. Овченков, Д.В. Аверин // Научный вестник Гос НИИ ГА, 2020. – № 30. – С. 107-117.

120.Овченков Н.И. Концепция, модели и методы управления авиационной безопасностью по критерию человеческий фактор / Н.И. Овченков, Д.В. Аверин // Научный вестник Гос НИИ ГА, 2020. – № 31. – С. 108-118.

121. Овченков Н.И. Оценка достоверности обнаружения негативных событий как динамическая процедура в многофункциональной технологической платформе «программный комплекс ESM» / Л.Н. Елисов, Н.И. Овченков // Научный вестник МГТУГА. – Москва: МГТУГА, 2015. – №218. – С.29-34.

122. Овченков Н.И. Статистическое прогнозирование уровня профессиональной подготовки авиационного персонала при решении задачи обеспечения авиационной безопасности аэропорта / Л.Н. Елисов, Н.И. Овченков // VI international scientific and technical conference «Engineering, technologies, education, security», PROCEEDINGS, VOLUME 1, ISSN PRINT 2535-0315, ISSN ONLINE 2535-0323, YEAR II, ISSUE 1 (4), SOFIA, BULGARIA, 2018. – pp.72-76.

123. Овченков Н.И. Методы решения краевых задач как математическая основа теории авиационной безопасности / Л.Н. Елисов, Н.И. Овченков // Международная научно-техническая конференция «Гражданская авиация на современном этапе развития науки, техники и общества», материалы конференции. – Москва: МГТУГА, 2016. – С. 94.

124. Овченков Н.И. К вопросу о физическом моделировании пространства угроз безопасности аэропорта / Л.Н. Елисов, Н.И. Овченков // Международная научно-техническая конференция «Гражданская авиация на современном этапе развития науки, техники и общества», материалы конференции. – Москва: МГТУГА, 2018. – С. 140-141.

125. Овченков Н.И. Авиационная безопасность как объект математического моделирования / Л.Н. Елисов, Н.И. Овченков // Научный вестник Московского государственного технического университета гражданской авиации. – Москва: МГТУГА, 2017. – Том 20, № 3. – С. 13-20.

126. Овченков Н.И. Некоторые вопросы сеточного и нейросетевого моделирования задач управления авиационной безопасностью аэропорта / Л.Н.

Елисов, Н.И. Овченков // Научный вестник Московского государственного технического университета гражданской авиации. – Москва: МГТУГА, 2017. – Том 20, №3. – С. 21–29.

127. Овченков Н.И. К вопросу структурного моделирования субъектов транспортной безопасности / Л.Н. Елисов, Н.И. Овченков // Научный вестник Московского государственного технического университета гражданской авиации. – Москва: МГТУГА, 2013. №197. – С. 58-61.

128. Овченков Н.И. Интегральная безопасность воздушного транспорта / Л.Н. Елисов, Н.И. Овченков // Научный вестник Московского государственного технического университета гражданской авиации. – Москва: МГТУГА, 2017. – Том 20, № 6. – С. 36-44.

129. Овченков Н.И. Численная реализация эвристической модели угроз безопасности объекта гражданской авиации / Л.Н. Елисов, Н.И. Овченков // Вестник СПбГУ ГА. – Санкт-Петербург: СПбГУ ГА, 2018. – №1(18). – С. 42-57.

130. Овченков Н.И. Модель динамической структуры средств обеспечения транспортной безопасности / Л.Н. Елисов, Н.И. Овченков // Научный вестник Московского государственного технического университета гражданской авиации. – Москва: МГТУГА, 2013. – №192. – С. 58-62.

131. Овченков Н.И., Оценка уязвимости объектов транспортной инфраструктуры и транспортных средств в гражданской авиации / Л.Н. Елисов, Н.И. Овченков // Научный вестник Московского государственного технического университета гражданской авиации. – Москва: МГТУГА, 2014. – № 204. – С. 65-68.

132. Овченков Н.И. О некоторых классах оптимизационных задач, решаемых с применением неформальных методов / Л.Н. Елисов, С.В. Громов, Н.И. Овченков // Научный вестник Московского государственного технического университета гражданской авиации. – Москва: МГТУГА, 2012. – №186. – С. 130-135.

133. Овченков Н.И. Квалиметрические процедуры интеграции радиотехнических средств защиты аэропорта / Л.Н. Елисов, Н.И. Овченков //

Научный вестник Московского государственного технического университета гражданской авиации. – Москва: МГТУГА, 2012. – № 186. – С. 138-142.

134. Овченков Н.И. Некоторые проблемы автоматизации процедур управления авиационной безопасностью аэропорта / В.Л. Филиппов, Н.И. Овченков // Научный вестник ГосНИИГА. – 2018. – № 24. – С. 66-74.

135. Овченков Н.И. О решении плохо формализуемых и слабо структурированных задач в области авиационной безопасности / В.Л. Филиппов, Н.И. Овченков // Вестник СПбГУ ГА. – Санкт-Петербург: СПбГУГА, 2019. – № 1. – С. 34-46.

136. Овченков Н.И. Гибридные методы моделирования объектов с распределенными параметрами / О.Л. Вензель, Н.И. Овченков // Международная научно-техническая конференция «Гражданская авиация на современном этапе развития науки, техники и общества», материалы конференции. – Москва: МГТУГА, 2018. – С. 85.

137. Овченков Н.И. Комбинированные модели для решения задач идентификации безопасности аэропорта / Л.Н. Елисов, Н.И. Овченков // Международная научно-техническая конференция «Гражданская авиация на современном этапе развития науки, техники и общества», материалы конференции. – Москва: МГТУГА, 2018. – С. 86.

138. Определение компетентности эксперта с помощью модели / В.М. Кормышев, В.Б. Щербатский, В.Г. Лисиенко, В.А. Култышева. – Ульяновск: УГТУ, 2002. – 45 с.

139. Основные принципы учета человеческого фактора в руководстве по техническому обслуживанию воздушных судов. ИКАО, 2003. – Doc 9824 AN/450. – 230 с.

140. Песаран М. Динамическая регрессия: теория и алгоритмы : пер. с англ. / М. Песаран, Л. Слейтер. – Москва: Финансы и статистика, 1984. – 312 с.

141. Подиновский В.В. Методы многокритериальной оптимизации. Вып.1. – Москва: Военная академия им. Ф.Э. Дзержинского, 1971. – 122 с.

142.Попов Э.В. Экспертные системы. – Москва: Наука, 1987. – 415 с.

143.Поспелов Д.А. Ситуационное управление: теория и практика. – Москва: Наука, 1986. – 284 с.

144.Поспелов Д.А. Построение экспертных систем. – Москва: Мир, 1987. – 440 с.

145.Прангишвили И.В. Энтропийные и другие системные закономерности: Вопросы управления сложными системами // Институт проблем управления. – Москва: Наука, 2003. – 428 с.

146.Предупреждение неблагоприятных событий в полете, обусловленных деятельностью экипажа / Г.С. Карапетян, Н.Ф. Михайлик, С.П. Пичко, А.И. Прокофьев. – Москва: Транспорт, 1989. – 173 с.

147.Приложение 17 к Конвенции о международной гражданской авиации (ИКАО) «Безопасность. Защита международной гражданской авиации от актов незаконного вмешательства». – ИКАО, 2022. – издание 12. – 74 с.

148. Пфанцгаль И.П. Теория измерений. – Москва: Мир,1976. – 248 с.

149. Райншке К. Модели надежности и чувствительности систем. – Москва: Мир, 1979. – 320 с.

150. Растригин Л.А. Современные принципы управления сложными объектами. – Москва: Сов. радио, 1980. – 240 с.

151.Риски и безопасность авиационных систем: монография / Г.Н. Гипич В.Г. Евдокимов, В.А. Куклев, В.С. Шапкин. – Москва: ФГУП ГосНИИ ГА, 2013. – 232 с.

152.Роль человеческого фактора в авиационных происшествиях / Обзорная информация ЦНТИ ГосНИИ ГА № 11(81). // Воздушный транспорт, 1986. – 40 с.

153.Розов С.А. Определение уровня безопасности полетов с учетом проявления человеческого фактора, внешней среды и безотказности авиационной техники: дис. … канд. техн. наук: 05.22.14. / Розов Сергей Анатольевич. – Москва, 2001. – 168 с.

154.Российская Федерация. Законы. Воздушный кодекс Российской Федерации : Федеральный закон от 19 марта 1997 г. № 60-ФЗ : [принят Государственной Думой 19 февраля 1997 г., одобрен Советом Федерации 5 марта 1997 г.]. – Москва: Собрание законодательства РФ, 24.03.1997. – №12, ст. 1383. – 107 с.

155.Российская Федерация. Законы. О противодействии терроризму : Федеральный Закон РФ от 06.03.2006 № 35-ФЗ : [принят Государственной Думой 26 февраля 2006 г., одобрен Советом Федерации 1 марта 2006 г.]. – Москва: Парламентская газета, №32, 10.03.2006. – 24 с.

156. Российская Федерация. Законы. О транспортной безопасности : Федеральный закон РФ от 09.02.2007 № 16-ФЗ : [принят Государственной Думой 19 января 2007 г., одобрен Советом Федерации 2 февраля 2007 г.]. – Москва: Собрание законодательства РФ, 12.02.2007. – №7, ст. 837. – 42 с.

157.Российская Федерация. Правительство. Об уровнях безопасности объектов транспортной инфраструктуры и транспортных средств и о порядке их объявления (установления) : Постановление Правительства РФ от 29.12.2020 № 2344 : [опубликован на «Официальном интернет-портале правовой информации» (www.pravo.gov.ru) 31 декабря 2020 г. N 0001202012310110, в Собрании законодательства Российской Федерации от 11 января 2021 г. N 2 (часть I) ст. 396].

158. Российская Федерация. Правительство. Об утверждении Перечня потенциальных угроз совершения актов незаконного вмешательства в деятельность объектов транспортной инфраструктуры и транспортных средств : Приказ Минтранса РФ, ФСБ России, МВД России от 05.03.2010 № 52/112/134 : [зарегистрировано в Минюсте РФ 02.04.2010 N 16782]. – Москва: "Российская газета", N 78, 14.04.2010.

159. Российская Федерация. Правительство. Об утверждении правил охраны аэропортов и объектов их инфраструктуры : Постановление Правительства РФ от 01.02.2011 № 42 : [опубликовано в изданиях "Собрание законодательства РФ", 07.02.2011, N 6, ст. 890, "Российская газета", N 25, 08.02.2011].

160. Российская Федерация. Правительство. Об утверждении требований по обеспечению транспортной безопасности, в том числе требований к антитеррористической защищенности объектов (территорий), учитывающих уровни безопасности для различных категорий объектов транспортной инфраструктуры воздушного транспорта : Постановление Правительства РФ 05.10.2020 №1605 : [опубликован на «Официальном интернет-портале правовой информации (www.pravo.gov.ru) 12.10.2020].

161.Российская Федерация. Правительство. Об утверждении Положения о приаэродромной территории и Правил разрешения разногласий, возникающих между высшими исполнительными органами государственной власти субъектов российской федерации, уполномоченными Правительством Российской Федерации федеральными органами исполнительной власти и Федеральной службой по надзору в сфере защиты прав потребителей и благополучия человека при согласовании проекта акта об установлении приаэродромной территории и при определении границ седьмой подзоны приаэродромной территории : Постановление Правительства РФ от 2 декабря 2017 г. № 1460 : [опубликован «Собрание законодательства РФ», 11.12.2017, N 50 (Часть III), ст. 7619]. – 18 с.

162. Российская Федерация. Правительство. Об утверждении Федеральных авиационных правил «Требования авиационной безопасности к аэропортам» : Приказ Минтранса РФ от 28.11.2005 № 142 : [Зарегистрирован в Минюсте России 28.12.2005 N 7321. Опубликован в издании «Бюллетень нормативных актов федеральных органов исполнительной власти», №4, 23.01.2006.]

163.Российская Федерация. Правительство. О Порядке проведения оценки уязвимости объектов транспортной инфраструктуры, судов ледокольного флота, используемых для проводки по морским путям, судов, в отношении которых применяются правила торгового мореплавания и требования в области охраны судов и портовых средств, установленные международными договорами Российской Федерации : Приказ Минтранса РФ от 01.11.2021 № 370 : [опубликован

на «Официальном интернет-портале правовой информации (pravo.gov.ru), 30.11.2021].

164.Российская Федерация. Правительство. Федеральные авиационные правила. Требования авиационной безопасности к аэропортам : Приказ Минтранса от 28 ноября 2005г. №142. [Зарегистрировано в Минюсте России 28.12.2005 N 7321. Опубликован в издании "Бюллетень нормативных актов федеральных органов исполнительной власти", N 4, 23.01.2006.]. – 14 с.

165.Руководство по обучению в области человеческого фактора. – ИКАО, 1998. – Doc 9683 AN/450. – 190 с.

166.Руководство по организации контроля за обеспечением авиационной безопасности. – ИКАО, 2015. – Doc 10047. – 72 с.

167.Руководство по управлению безопасностью полетов (РУБП). – ИКАО, 2018. – Doc 9859 AN/474, издание 4. – 218 с.

168.Румшинский Л.З. Математическая обработка результатов эксперимента. – Москва: Наука, 1971. - 192 с.

169.Рутковская Д. Нейронные сети, генетические алгоритмы и нечеткие системы / Д. Рутковская, М. Пилиньский, Л. Рутковский // перевод с польск. И. Д. Рудинского. – Москва: Горячая линия – Телеком, 2006. – 452 с.

170.Рыков А.С. Методы системного анализа: многокритериальная и нечеткая оптимизация, моделирование и экспертные оценки. – Москва: НПО «Издательство Экономика», 1999. – 191 с.

171.Рыков А.С. Методы системного анализа: оптимизация. – Москва: НПО «Издательство Экономика», 1999. – 255 с.

172.Рыков А.С. Модели и методы системного анализа: принятие решений. – Москва: ИЦПКПС, 2004. – 420 с.

173. Рябинин, И. А. Надежность и безопасность структурно сложных систем. – Санкт-Петербург: Политехника, 2000. – 248 с.

174.Саати Т. Принятие решений. Метод анализа иерархий. – Москва: Радио и связь, 1993. – 243 с.

175. Саката Сиро. Практическое руководство по управлению качеством. – Москва: Машиностроение, 1980. – 214 с.

176. Сборник трудов общества независимых расследователей авиационных происшествий. – Москва: ОРАП, 2011. – №23. – 267 с.

177. Селюков В.К. Риск-менеджмент организации : учеб. пособие. – Москва: МГТУ им. Н.Э. Баумана, 2008. – 188 с.

178. Сертификационные требования к персоналу инженерно-авиационной службы предприятий воздушного транспорта. – Москва: ГОСНИИГА, 1992. – 26 с.

179. Симак А.А. Методика количественного оценивания эффективности синтезированных мероприятий по предотвращению авиационных происшествий / А.А. Симак, В.Д. Шаров // Всероссийская научно-техническая конференция. 8 Научные чтения по авиации, посвященные памяти Н.Е. Жуковского. Материалы. Часть 2. – Москва: ВВИА. – 2007. – С. 64.

180. Системный подход и человеческий фактор в орнитологической безопасности аэропорта / Л.Н. Елисов, Н.И. Овченков, В.Л. Филиппов, А.А. Лаптев, Е.А. Коняев // Научный вестник ГосНИИ ГА. – 2019. – №29. – С. 99-107.

181. Ступаков, В. С. Риск-менеджмент: учеб. пособие / В.С. Ступаков, Г.С. Токаренко. – Москва: Финансы и статистика, 2005. – 288 с.

182. Сигеру О. Нейроуправление и его применения / О. Сигеру, Х. Марзуки, Ю. Рубия. // Под ред. А. И. Галушкина. – Москва: ИПРЖР, 2000. – Кн. 2. – 272 с.

183. Статистические методы анализа безопасности сложных технических систем // Под ред. В.П. Соколова. – Москва: Логос, 2001. – 232 с.

184. Статистическое моделирование и прогнозирование // Под ред. А.Г. Гранберга. – Москва: Финансы и статистика, 1990. – 383 с.

185. Статистические методы прогнозирования на основе временных рядов / Ю.В. Сажин, А.В. Катынь и др. – Саранск: изд. Морд. Университета, 2000. – 116 с.

186. Субетто А.И. Квалиметрия. – Ленинград: ВНИСИ, 1988. – 312 с.

187. Теория прогнозирования и принятия решений: учеб. пособие // Под ред. С.А. Саркисяна. – Москва: Высшая школа, 1977. – 351 с.

188. Терроризм и безопасность на транспорте в России (1991-2002гг.): Белая книга (аналитический доклад) // Под ред. В.М. Лопатина – Санкт-Петербург: Юридический центр Пресс, 2004. – 687 с.

189. Терроризм и безопасность на транспорте: материалы 11 МНТК. – Москва: НИИГПРФ, 2003. – 147 с.

190. Тим Постон. Теория катастроф / Тим Постон, Стюарт Иэн. – Москва: Мир, 1980. – 607 с.

191. Трахтенгерц Э.А. Компьютерная поддержка принятия решений. – Москва: СИНТЕГ, 1998. – 376 с.

192. Уотермен Д, Руководство по экспертным системам : пер. с англ. – Москва: Мир, 1989. – 388 с.

193. Фадеев Р.С. Организация производственной деятельности службы авиационной безопасности аэропорта на основе прогнозирования уровня мобилизационной готовности персонала: дисс. … канд. техн. наук : 05.02.22 / Фадеев Руслан Сергеевич. - Москва: МГТУГА, 2009. – 175 с.

194. Фадеев Р.С. Система прогнозирования уровня авиационной безопасности аэропорта в части, касающейся человеческого фактора // Научный вестник МГТУГА. – Москва: МГТУГА, 2007. – №112. – С. 68-76.

195. Фадеев Р.С. Аддитивные модели прогнозирования уровня авиационной безопасности аэропорта // Научный вестник МГТУГА. – Москва: МГТУГА, 2007. – №112. – С.76-80.

196. Фадеев Р.С. Концепция решения задачи временной оптимизации процесса поддержания уровня авиационной безопасности аэропорта / Р.С. Фадеев, Л.Н. Елисов // Научный вестник МГТУГА. – Москва: МГТУГА, 2006. – №108. – С.64-73.

197. Фарлоу С. Уравнения с частными производными для научных работников и инженеров. – Москва: Мир, 1985. – 384 с.

198. Федеральная система контроля качества (Национальная программа контроля качества авиационной безопасности). – Москва: Минтранс РФ, 2019.

199. Федеральная система обеспечения авиационной безопасности (Национальная программа авиационной безопасности). – Москва: Минтранс РФ, 2019. – 42 с.

200. Федеральная система подготовки персонала в области авиационной безопасности (Национальная программа подготовки персонала в области авиационной безопасности). Москва: Минтранс РФ, 2019. – 61 с.

201. Филиппов В.Л. Обучение сетей радиальных базисных функций для решения задач аппроксимации / В.Л. Филиппов, Л.Н. Елисов, В.И. Горбаченко. // International Journal of Civil Engineering and Technology (IJCIET), Volume 10, Issue 3, March 2019. – pp. 872-881. – Article ID: IJCIET_10_03_085, ISSN PRINT: 0976-6308, ONLINE: 0976-6316.

202. Филиппов В.Л. A new approach to assessing the human factor in the automated system of control of aviation security of the airport / В.Л. Филиппов, Л.Н. Елисов, Н.И. Овченков // International scientific journal «Security and Future», ISSN PRINT 2535-0668, ISSN ONLINE 2535-082X, YEAR III, ISSUE 2/2019, SOFIA, BULGARIA. – pp. 41-42.

203. Фролов Ю.В. Интеллектуальные системы и управленческие решения. – Москва: МГПУ, 2000. – 294 с.

204. Хартман Г. Современный факторный анализ. – Москва: Статистика, 1972. – 486 с.

205. Хенли Э. Дж. Надежность технических систем и оценка риска. / Э. Дж. Хенли, Х. Кумамото. – Москва: Машиностроение, 1984. – 538 с.

206. Хруцкий В.Е. Оценка персонала. – Москва: Финансы и статистика, 2007. – 224 с.

207. Цветков В.Я. Информационное управление // LAP LAMBERT Academic Publishing Gmbh and Co.KG. – Saarbrucken, Germany, 2012. – 201 с.

208.Цурков В.И. Декомпозиция в задачах большой размерности. – Москва: Наука, 1981. – 352 с.

209. Человеческий фактор в системе мер безопасности гражданской авиации. – ИКАО, 2002. – Doc 9808 AN/765. – 120 с.

210. Шапкин В.С. К вопросу о применении рискоориентированного подхода в задаче обеспечения безопасности полетов / В.С. Шапкин, С.С. Демин, А.В. Никитин, Д.С. Демин, Д.В. Ковтушенко // Научный вестник ГосНИИ ГА. – 2017. – № 6. – С. 61-72.

211. Шаров В.Д. Возможности теории нечетких множеств при оценивании факторов риска авиационного происшествия / В.Д. Шаров, А.Г. Гузий, С.М. Гладкин // Проблемы безопасности полетов. – 2007. – №12. – С. 10-18.

212. Шаров В.Д. Об одном методе оценки эффективности мероприятий по предотвращению авиационных происшествий // Проблемы безопасности полетов. Информационный сборник. – Москва: ВИНИТИ, 2006. – №11. – С. 3-8.

213. Шаров В.Д. Применение байесовского подхода для уточнения вероятностей событий в автоматизированной системе прогнозирования и предотвращения авиационных происшествий // Управление большими системами. – №43 (2013). – С. 240-253.

214. Шаров В.Д. Разработка алгоритма управления риском для безопасности полетов на уровне авиакомпании // Научный вестник МГТУ ГА. – 2009. – №149. – С. 31-38.

215.Шаров В.Д. Разработка системы управления рисками в организации по техническому обслуживанию и ремонту / В.Д. Шаров, Р.В. Еникеев // Научный вестник МГТУ ГА. – 2010. – №162. – С. 30-39.

216. Шаров В.Д. Синтез функции априорного оценивания уровня безопасности предстоящих полетов по группе факторов «Среда» // Проблемы безопасности полетов. – Москва: ВИНИТИ. – 2007. – №11.

217.Шенк Р. Обработка концептуальной информации. – Москва: Энергия, 1980. – 361 с.

218. Шибанов Г.П. Количественная оценка деятельности человека в системах человек – техника. – Москва: Машиностроение, 1983. – 264 с.

219. Штойер Р. Многокритериальная оптимизация. Теория, вычисления и приложения. – Москва: Радио и связь, 1992. – 504 с.

220. Щипин К.С. Система прогнозирования на основе многокритериального анализа временных рядов: дисс. … канд. техн. наук : 05.13.10. – Москва: МГИСС, 2004. – 134 с.

221. Юдин Д.Б. Математические методы управления в условиях неполной информации. – Москва: Сов. радио, 1974. – 400 с.

222.Aggarwal C.C. Neural Networks and Deep Learning: A Textbook. – Springer, 2018. – 497 p.

223.Atansov A. Contents and characteristics of the innovation process in military education in Bulgaria, International Scientific Conference, 2018. – pp. 286-291.

224.Beale M. H., Hagan M. T., Demuth H. B. Neural Network Toolbox. User's Guide. – Natick: Math Works, Inc., 2017. – 446 p.

225.Belling Ch., Reynard W.D. Human factors in aircraft incident: results of 7-years study. – Avia Spase Envirom Med, 1984. – 55, 10. – pp. 960-965.

226.Blagorazumov, P. Chernikov, G. Glukhov, A. Karapetyan, V. Shapkin, L. Elisov. The Background to the Development of the Information System for Aviation Security Oversight in Russia // International Journal of Civil Engineering and Technology, 2018. – 9(10). – pp. 341-350.

227.BSI (2008), Risk Management Code of Practice, British Standard BS 31100:2008, The British Standards Institution, London.

228.Carbonell J.G. Towards a process model of human personality traits // Artificial Intelligence, 1980. – v.15. – pp. 49-74.

229.De Rosa M. Data Mining and Data Analysis for Counterterrorism / Washington, D.C. Center for Strategic and International Studies, 2004. – 24 p.

230.Edwards E. Human factor in aviation. Aerospace, 1985. – 12, 6. – pp. 13-17.

231. Elias B., Krouse W., Rappaport E. Homeland Security: Air Passenger prescreening and counterterrorism. Report for Congress: The Library of Congress, 2005. – 34 p.

232. Elisov L.N., Gorbachenko V.I., Zhukov M.V. Learning Radial Basis Function Networks with the Trust Region Method for Boundary Problems // Automation and Remote Control. – 2018. – Vol.79, No.9. – pp. 1621-1629.

233. Fitts P.M., Jones R.E. Analysis of factors contributing to 460 pilot-error experiences in operating aircraft control // Selected papers of human factors in the design and use of control systems. N.Y., 1961. – pp. 332-358.

234. A Geron Hands-On Machine Learning with Scikit-Learn and Tensor Flow: Concepts, Tools, and Techniques to Build Intelligent Systems (Sebastopol: O'Reilly), 2017. – 574 p.

235. Gertman, D.I., Blackman, H.S. Human reliability and safety analysis data handbook New York, 1995. – 448 p.

236.Glukhov G.E. Analysis of safety indices of flights and aviation security in relation to the task on construction of two-level system of continuous information monitoring of aviation activity safety // International Journal of Civil Engineering and Technology (IJCIET). – 2019. – volume 10, issue 04. – pp. 2654-2662.

237. Goodwin P.D. Human factors and pilot performans: Safety, First Aid and Survival / P.D. Goodwin. – Air Pilot Publishing, 2006. – 344 p.

238. Green K.B. Systems analysis techniques // Systems psychology. N.Y., 1970. – pp.79-130.

239. Gubanov O., Brusnikin V., Bykova V., Garanin S., Koval S. and Maslennikova G. The central civil aviation safety regulatory and guidance library of the

Russian Federation. International Journal of Givil Engineering and Technology (IJMET). – 2019 January. – volume 10, issue 1. – pp. 988-997.

240. Hyndman Rob J., Athanasopoulos G. Forecasting: principles and practice. 2ed, Australia, Monash University, 2018. – 382 p.

241. Methods for Differential Equations. Springer, 2015. – 128 p.

242. Harris T. I am OK – You are OK. A practical guide to transactional analysis. N.Y., 1969.

243. Kitler. W., (scientific dir.) Local self-government in the national defense of the Republic of Poland, AON, Warszawa, 2015.

244. N Khan, D Milner, B Marr Introduction to People Analytics: A Practical Guide to Datadriven HR (London: Kogan Page), 2020. – p 353.

245. Kuliczkowski. M., Wojcieszko. M., (ed) Public administration in the process of state defense preparations – selected problems, War Studies Academy, Warszawa, 2018.

246. Landry S.J. Advances in Human Aspects of Aviation/S.J. Landry // U.S.A., CRC Press, 2012. – 858 p.

247. Minsky M. Minsky frame system theory // In Theoretical Issues in Natural Language Processing. Cambridge, 1975.

248. Ovchenkov N.I. Qualimetric forecasting of aviation personnel professional development level while solving airport aviation security provision issues /«XXVI international scientific and technical conference Trans and MOTAUTO - 18». Proceedings, vol. 2, ISSN PRINT 1313-5031, ISSN WEB 2535-0307, YEAR I, ISSUE 2 (4), SOFIA, BULGARIA, 2018. – pp. 105-108.

249. Ovchenkov N.I. Information support for decision-making while forecasting aviation personnel professional development level // «XXVI international scientific and technical conference Trans and MOTAUTO – 18». Proceedings, vol. 2, ISSN PRINT 1313-5031, ISSN WEB 2535-0307, YEAR I, ISSUE 2 (4), SOFIA, BULGARIA, 2018. – pp. 163-168.

250. Ovchenkov N.I., Fadeev R.S. Model of airport vulnerability in civil aviation // International scientific journal «Security and Future», ISSN PRINT 2535-0668, ISSN ONLINE 2535-082X, YEAR IV, ISSUE 1/2020, SOFIA, BULGARIA. – pp. 3-5.

251. Ovchenkov N.I. Certain issues to minimize the human factor impact in transportation security / Averin D.V., Ovchenkov N.I. // «XXVIII international scientific conference Trans and Motauto 2020», Proceedings, ISSN PRINT 1313-5031, ISSN WEB 2535-0307, YEAR IV, ISSUE 1(7), VARNA, BULGARIA, 2020. – pp. 5-8.

252. Ovchenkov N.I., Yelisov L.N. Technical aspects of automation of transport security // International scientific journal «Trans and motauto world», ISSN PRINT 2367-8399, ISSN WEB 2534-8493, YEAR II, ISSUE 2, SOFIA, BULGARIA,2017. – pp. 64-68.

253. Ovchenkov N.I., Yelisov L.N. The relevance of concepts of quality and risk and their use in modern systems of transport security // V international scientific and technical conference «Engineering, technologies, education, security», PROCEEDINGS, VOLUME 3, ISSN PRINT 2535-0315, ISSN WEB 2535-0323, YEAR I, ISSUE 1 (3), SOFIA, BULGARIA, 2017. – pp. 243-248.

254. Ovchenkov N.I., Yelisov L.N. Elements of theory to solve the problem of management of transport safety //International scientific journal «SECURITY AND FUTURE», ISSN PRINT 2535-0668, ISSN (ONLINE) 2535-082X, YEAR I, ISSUE 3, SOFIA, BULGARIA, 2017. – pp. 98-101.

255. Ovchenkov N.I., Yelisov L.N. Problems of aviation personel's professional development while solving issues of airport security threats parryings // VI international scientific and technical conference «Engineering, technologies, education, security», PROCEEDINGS, VOLUME 1, ISSN PRINT 2535-0315, ISSN ONLINE 2535-0323, YEAR II, ISSUE 1 (4), SOFIA, BULGARIA, 2018. – pp. 5-11.

256. Ovchenkov N.I. Harmonization of the human factor in integrated aviation security system / Filippov V.L., Ovchenkov N.I. // VII international scientific conference «Engineering, technologies, education, security 2019», PROCEEDINGS, VOLUME III,

ISSN PRINT 2535-0315, ISSN ONLINE 2535-0323, YEAR III, ISSUE 3(9), SOFIA, BULGARIA,2019. – pp. 228-231.

257. Ovchenkov N.I. A new approach to assessing the human factor in the automated system of control of aviation security of the airport / Filippov V.L., Elisov L.N. Ovchenkov N.I. // International scientific journal «Security and Future», ISSN (PRINT) 2535-0668, ISSN (ONLINE) 2535-082X, YEAR III, ISSUE 2/2019, Bulgaria, Sofia, 2019. – pp. 41-43.

258. Ovchenkov N.I. Security threat propagation model civil aviation facility / Filippov V.L., Elisov L.N. Ovchenkov N.I. // III International scientific conference «CONFSEC», PROCEEDINGS, ISSN PRINT 2603-2945, ISSN ONLINE 2603-2953, YEAR 3, ISSUE 1(5),019, SOFIA, BULGARIA. – pp. 13-15.

259. Ovchenkov N.I. On one approach to solving the problem of formalization and modeling of the airport security threats space / Yelisov L.N., Ovchenkov N.I. //International scientific journal «SECURITY AND FUTURE», ISSNPRINT 2535 - 0668, ISSN (ONLINE) 2535-082X, YEAR I, Vol.2 (2018), ISSUE 4. – pp. 152-157.

260. J Price, J Forrest Practical Aviation Security: Predicting and Preventing Future Threats (Oxford: Butterworth-Heinemann), 2016. – p 598.

261. Radulov, N., Artificial intelligence and security. Security 4.0, Security & Future, 3 (1), 2019. – pp. 3-5.

262. Rabideau G.F. Field measurement of human performance in man-machine systems // Human factors, 1964. – V6. №6. – p. 663-672.

263. Research carried out with the CAWI method – Digital competences and the proliferation of threats, November 2018.

264. S. Petkov, P. Petkov, G. Nikolov, A. Tumbarska, “Mathematical model of the management of high-energy detonation processes through an energy generator (screen)” // European Journal of Engineering Research and Science, 2018. – Vol. 3, Issue 5. – pp. 65- 70.

265. Singleton W.T. Theoretical approaches to human error // Ergonomies (England), 1973. – V16. № 6. – pp. 727-737.

266. Smillie R.J., Ayoub M.A. Accident causation theories: A simulation approach // J. of Occupational Accidents, 1976. – V.1 №1. – pp. 47-68.

267. Szyłkowska M., Human factor in the proliferation of threats // The Intentional Scientific Journal: "Security & Future" Issue 2/2018, s. 55-58., ISSN (Print) 2535-0668, ISSN (Online) 2535-082X. 2018., SOFIA, BULGARIA.

268. Szyłkowska M. Security system creating in conditions of uncertainty and risk-outline of problem // The Intentional Scientific Journal: "Security & Future" Issue 2/2019, Vol. 3, pp. 38-40, ISSN (Print) 2535-0668, ISSN (Online) 2535-082X, 2019, SOFIA, BULGARIA.

269. Trejnis. Z., Kościelecki.L., (ed), Challenges and threats to security and defense of the Republic of Poland in the 21st century in the social and technological-environmental dimension, ASPRA-JR Publishing House, Warszawa, 2018.

270. Snyman J. A., Wilke D. N. Practical Mathematical Optimization: Basic Optimization Theory and Gradient-Based Algorithms. – Springer, 2018. – 372 p.

271. Sweet Aviation and Airport Security: Terrorism and Safety Concerns (Boca Raton: CRC Press), 2008. – p. 384.

272. Yadav N., Yadav A., Kumar M. An Introduction to Neural Network Methods for Differential Equations. Springer, 2015. – 128 p.

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ ЯРОСЛАВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ П.Г. ДЕМИДОВА

На правах рукописи

Овченков Николай Иванович

МОДЕЛИ И МЕТОДЫ ИНФОРМАЦИОННОГО УПРАВЛЕНИЯ ТРАНСПОРТНОЙ БЕЗОПАСНОСТЬЮ АЭРОПОРТА

Том 2. ПРИЛОЖЕНИЯ

2.9.6 – «Аэронавигация и эксплуатация авиационной техники»
(технические науки)

Диссертация
на соискание ученой степени
доктора технических наук

Научный консультант:

доктор технических наук, доцент

Борзова Анжела Сергеевна

Москва – 2024

ОГЛАВЛЕНИЕ

ПРИЛОЖЕНИЕ А Моделирование угроз безопасности аэропорта в формате дифференциальных уравнений в частных производных для стационарной задачи (обязательное) 3

ПРИЛОЖЕНИЕ Б Моделирование угроз безопасности аэропорта в формате дифференциальных уравнений в частных производных для нестационарной задачи (обязательное) 13

ПРИЛОЖЕНИЕ В Нейросетевое ранжирование аэропортов (справочное) 19

ПРИЛОЖЕНИЕ Г Нейросетевая оценка уровня готовности персонала (справочное)..... 27

ПРИЛОЖЕНИЕ А
МОДЕЛИРОВАНИЕ УГРОЗ БЕЗОПАСНОСТИ АЭРОПОРТА В ФОРМАТЕ ДИФФЕРЕНЦИАЛЬНЫХ УРАВНЕНИЙ В ЧАСТНЫХ ПРОИЗВОДНЫХ ДЛЯ СТАЦИОНАРНОЙ ЗАДАЧИ
(ОБЯЗАТЕЛЬНОЕ)

Различные варианты модели реализованы в системе MATLAB. Разработанные варианты главной программы и функций, реализующих итерационный процесс, представлены ниже.

Программа sec_1 моделирует источник опасности, заданный в одной точке. Задача решается в прямоугольной области, с координатами левого нижнего угла x1=0, y1=0 и правого верхнего угла x2=1 и y2=1. Задаются шаг сетки h, проницаемость внешней среды sigma, строится сетка, вычисляются массивы разностных коэффициентов. Координаты источника опасности задаются переменными xDan=0.5 и yDan=0.5. Величина опасности задается переменной uDan=1.0. Задаются координаты xProt1=0.2, yProt1=0.4, xProt2=0.4, yProt2=0.6 защищаемой области и проницаемость защищаемой области, практически равная нулю, sigma1=1.0e-12. Задавать проницаемость защищаемой области равной нулю нецелесообразно, так как это означает полную защиту от проникновения угроз на защищаемой области.

Решение задачи производится вызовом функции fdm_2. После получения решения строятся трехмерный график решения, график линий уровня решения и график относительной нормы поправки от номера итерации.

Функция fdm_2 запрашивает допустимую погрешность решения по относительной норме поправки к решению и реализует метод Зейделя. Особенностью реализации метода Зейделя является то, что решение в точке задания опасности не изменяется.

Входные данные функции: nx, ny – количество узлов по оси X и количество узлов по оси Y, Ax и Ay – массивы коэффициентов разностной схемы, uDan – величина угрозы, xDan, yDan – координаты угрозы, h – шаг сетки.

Выходные данные функции: U – двумерный массив решений в узлах сетки, nmax – число итераций, за которое получено решение, it – массив номеров итераций, nn – массив относительных поправок к решению.

Программа sec_2 моделирует опасность, распределенную в заданной области, и вызывает функцию fdm_1. Отличие этой программы и функции заключается в расчете опасности во всех точках.

Программа sec_3 моделирует опасность, распределенную по всей внешней области, и вызывает функцию fdm_1.

sec_1 Программа моделирования одиночной угрозы

```
% Модель одиночной опасности
% В точке задан источник опасности

% Модель описывается эллиптическим ДУЧП вида
% d/dx(sigma*dU/dx)+d/dy(sigma*dU/dy)=funf(x,y)
% с граничными условиями первого рода U|r=fi(x,y) по всей границе.
% Уравнение решается в прямоугольной области x1<=x<=x2, y1<=y<=y2
% с постоянным шагом h по осям X и Y.
clear; % Очистка рабочей области
clc; % Очистка командного окна
close all; % закрытие всех графических окон
x1=0;
x2=1;
y1=0;
y2=1;
h=0.01;  % шаг, кратный размеру области
sigma=1.00; % Проницаемость среды
% Задача решается при нулевых граничных условиях

[x,y]=meshgrid(x1:h:x2,y2:-h:y1); % формирование разностной сетки

% Расчет функции правой части в узлах сетки
nx=round((x2-x1)/h)+1; % Количество узлов по оси X
ny=round((y2-y1)/h)+1; % Количество узлов по оси Y
funf=zeros(ny+2,nx+2);

% Массивы коэффициентов
Ax=sigma*ones(nx,ny)/(h^2);
Ay=sigma*ones(ny,nx)/(h^2);

% Координаты источника опасности
xDan=0.5;
yDan=0.5;
```

```
% Величина опасности
uDan=1.0;

%sigma1=0.0001; % Проницаемость защищаемой области
sigma1=1.0e-12; % Проницаемость защищаемой области
xProt1=0.2; % Координаты защищаемой области
yProt1=0.4;
xProt2=0.4;
yProt2=0.6;

% Разностные коэффициенты для защищаемой области
Ax(round(yProt1/h)+1:round(yProt2/h),round(xProt1/h)+1:round(xProt2/h))=sigm
a1/(h^2);
Ay(round(yProt1/h)+1:round(yProt2/h),round(xProt1/h)+1:round(xProt2/h))=sigm
a1/(h^2);

% Плотность угроз внутри защищаемой области
funf(round(yProt1/h)+1:round(yProt2/h),round(xProt1/h)+1:round(xProt2/h))=0;

%=========Вызов функции решения==========================
[U,nmax,it,nn]=fdm_2(uDan,xDan,yDan,h,nx,ny,Ax,Ay,funf);
%[U,x,y,nmax,it,nn]=fdm_ell_eq(x1,x2,y1,y2,h,funf,fi,sigma);
fprintf('Решение получено за %u итераций ',nmax);

%============Построение трехмерного графика решения=======

%axis square ij % Начало координат в верхнем левом углу
figure;
mesh(x,y,U)
%surf(x,y,U);
colorbar;
title('Поверхность решения');
xlabel('x');
ylabel('y');
zlabel('u');
%===========Построение линий уровня решения===========
figure;

axis square ij % Начало координат в верхнем левом углу
contour(x,y,U,20,'ShowText','on')
% [CMatr,h1]=contour(x,y,U);
% clabel(CMatr,h1);
grid on;
xlabel('x');
ylabel('y');
title('Линии уровня');
hold on
plot([xProt1,xProt1,xProt2,xProt2,xProt1],[yProt1,yProt2,yProt2,yProt1,yProt
1],'LineWidth',2)

%===========Построение графика зависимости относительной нормы поправки от
номера итерации====
figure;
loglog(it, nn, '-')
xlabel('Номер итерации');
ylabel('Относительная норма поправки');
grid on
xlabel('Номер итерации');
ylabel('Относительная норма невязки');
title('Число итераций')
```

Функция решения методом конечных разностей для единичной угрозы

```
function [U,nmax,it,nn]=fdm_2(uDan,xDan,yDan,h,nx,ny,Ax,Ay,f)
% Функция решения методом конечных разностей эллиптического ДУЧП вида
% d/dx(sigma*dU/dx)+d/dy(sigma*dU/dy)=funf(x,y)                (1)
% с граничными условиями первого рода U|r=fi(x,y)по всей границе.
% Уравнение решается в прямоугольной области x1<=x<=x2, y1<=y<=y2
% с постоянным шагом h по осям X и Y.
% ВХОДНЫЕ ДАННЫЕ:% nx, ny - Количество узлов по оси X, количество узлов по оси
Y
% Ax и Ay - массивы коэффициентов разностной схемы
% uDan - величина угрозы, xDan, yDan - координаты угрозы
% h - шаг сетки
% ВЫХОДНЫЕ ДАННЫЕ:
% U - двумерный массив решений в узлах сетки;
% nmax - число итераций, за которое получено решение;
% it - массив номеров итераций;
% nn - массив относительных поправок к решению.

% МЕТОД РЕШЕНИЯ:
% Разностная аппроксимация строится на основе интегро-интерполяционного
% метода. Поскольку используется постоянный шаблон, то система разностных
% уравнений в явном виде не формируется, а строятся два массива Ax и Ay,
% содержащие коэффициенты разностной схемы, связывающие текущий узел сетки
% с соседними узлами справа по оси X и вниз по оси Y
%              O(i,j)--Ax(i)--O(i+1,j)
%              |
%              |
%              Ay(i)
%              |
%              |
%              O(i,j+1)
% Для решения системы разностных уравнений  используется метод Зейделя, в
% котором разностные уравнения формируются по одному шаблону для всех
% внутренних узлов с использование массивов Ax и Ay.

epsilon=input ('Введите  epsilon=');% запрос допустимой погрешности
disp('Ждите, идут вычисления')
U=zeros(ny,nx);% формирование нулевого начального приближения
% Нулевые граничные условия сформированы
% Угроза на сетке
% Координаты опасности
xDan=round(xDan/h)+1;
yDan=round(yDan/h)+1;
U(xDan,yDan)=uDan;

nn=0; % массив номеров итераций
it=0; % массив числа итераций
iter=0;  % Счетчик итераций

%======ИТЕРАЦИОННЫЙ ПРОЦЕСС==========
while 1
    iter=iter+1;
    if iter>100000
        disp('Число итераций больше заданного числа, равного 100000')
        break % аварийный конец итераций
    end;
    delta=0; % формирование нулевого максимального приращения решения
    for i=2 :ny-1
```

```
            for j=2 :nx-1
                if and(i==yDan,j==xDan)
                    U(i,j)=uDan;
                else
                    Uk=U(i,j); % запоминание старого значения решения в узле
                    U(i,j)=1/(Ax(i,j)+Ax(i-1,j)+Ay(i,j)+Ay(i,j-1))*...
                        (Ax(i,j)*U(i+1,j)+Ax(i-1,j)*U(i-
1,j)+Ay(i,j)*U(i,j+1)+Ay(i,j-1)*U(i,j-1)+f(i,j));
                    delta1=abs(U(i,j)-Uk);
                    if delta1>delta
                        delta=delta1; % формирование нормы поправки решения
                    end
                end
             end;
        end
        rel_delta=delta/norm(U,inf); % относительная поправка решения
        if  rel_delta<=epsilon;% проверка выполнения критерия останова по относ.
норме приращения
            nmax=iter;
            break
        end;

        %=====Формирование массивов для графика изменения относительной поправки
от номера итерации
        nn(iter)=rel_delta;
        it(iter)=iter;
    end;
```

sec_2 Программа моделирования распределенной угрозы

```
    % Модель при угрозе по некоторой внешней области

    % Модель описывается эллиптическим ДУЧП вида
    % d/dx(sigma*dU/dx)+d/dy(sigma*dU/dy)=funf(x,y)
    % с граничными условиями первого рода U|r=fi(x,y) по всей границе.
    % Уравнение решается в прямоугольной области x1<=x<=x2, y1<=y<=y2
    % с постоянным шагом h по осям X и Y.
    clear; % Очистка рабочей области
    clc; % Очистка командного окна
    close all; % закрытие всех графических окон
    x1=0;
    x2=1;
    y1=0;
    y2=1;
    h=0.01;  % шаг, кратный размеру области

    [x,y]=meshgrid(x1:h:x2,y2:-h:y1); % формирование разностной сетки

    sigma=1.00; % Проницаемость среды

    % Задача решается при нулевых граничных условиях

    % Расчет функции правой части в узлах сетки
    nx=round((x2-x1)/h)+1; % Количество узлов по оси X
    ny=round((y2-y1)/h)+1; % Количество узлов по оси Y
    funf=zeros(ny+2,nx+2);

    % Матрицы коэффициентоы
    Ax=sigma*ones(nx,ny)/(h^2);
```

```
Ay=sigma*ones(ny,nx)/(h^2);

% Координаты области угроз (danger)- источника опасности
xDan1=0.5;
yDan1=0.5;
xDan2=0.8;
yDan2=0.8;
% Величина угрозы
funDan=1.0;
% Угроза на сетке
funf(round(yDan1/h)+1:round(yDan2/h),round(xDan1/h)+1:round(xDan2/h))=funDan
;

sigma1=1.0e-12; % Проницаемость защищаемой области
xProt1=0.2; % Координаты защищаемой области
yProt1=0.4;
xProt2=0.4;
yProt2=0.6;

Ax(round(yProt1/h)+1:round(yProt2/h),round(xProt1/h)+1:round(xProt2/h))=sigm
a1/(h^2);

Ay(round(yProt1/h)+1:round(yProt2/h),round(xProt1/h)+1:round(xProt2/h))=sigm
a1/(h^2);

% Плотность угроз внутри защищаемой области
funf(round(yProt1/h)+1:round(yProt2/h),round(xProt1/h)+1:round(xProt2/h))=0;


%=========Вызов функции решения============================
[U,nmax,it,nn]=fdm_1(nx,ny,Ax,Ay,funf);
%[U,x,y,nmax,it,nn]=fdm_ell_eq(x1,x2,y1,y2,h,funf,fi,sigma);

fprintf('Решение получено за %u итераций ',nmax);



%============Построение трехмерного графика решения=======

%axis square ij % Начало координат в верхнем левом углу
figure;
mesh(x,y,U)
%surf(x,y,U);
colorbar;
xlabel('x');
ylabel('y');
zlabel('u');
title('Поверхность решения');

%===========Построение линий уровня решения===========
figure;

axis square ij % Начало координат в верхнем левом углу
contour(x,y,U,'ShowText','on')
% [CMatr,h1]=contour(x,y,U);
% clabel(CMatr,h1);
grid on;
xlabel('x');
ylabel('y');
```

```
      title('Линии уровня');
      hold on
      plot([xProt1,xProt1,xProt2,xProt2,xProt1],[yProt1,yProt2,yProt2,yProt1,yProt
1],'LineWidth',2)
      %===========Построение графика зависимости относительной нормы поправки от
номера итерации====
      figure;
      loglog(it, nn, '-')
      xlabel('Номер итерации');
      ylabel('Относительная норма поправки');
      grid on
      title('Число итераций')
```

Функция решения методом конечных разностей эллиптического дифференциального уравнения в частных производных для распределенной угрозы

```
      function [U,nmax,it,nn]=fdm_1(nx,ny,Ax,Ay,f)
      % Функция решения методом конечных разностей эллиптического ДУЧП вида
      % d/dx(sigma*dU/dx)+d/dy(sigma*dU/dy)=funf(x,y)                (1)
      % с граничными условиями первого рода U|r=fi(x,y)по всей границе.
      % Уравнение решается в прямоугольной области x1<=x<=x2, y1<=y<=y2
      % с постоянным шагом h по осям X и Y.
      % ВХОДНЫЕ ДАННЫЕ:% nx, ny - Количество узлов по оси X, количество узлов по оси
Y
      % Ax и Ay - массивы коэффициентов разностной схемы
      % ВЫХОДНЫЕ ДАННЫЕ:
      % U - двумерный массив решений в узлах сетки;
      % x,y - массивы координат сетки;
      % nmax - число итераций, за которое получено решение;
      % it - массив номеров итераций;
      % nn - массив относительных поправок к решению.

      % МЕТОД РЕШЕНИЯ:
      % Разностная аппроксимация строится на основе интегро-интерполяционного
      % метода. Поскольку используется постоянный шаблон, то система разностных
      % уравнений в явном виде не формируется, а строятся два массива Ax и Ay,
      % содержащие коэффициенты разностной схемы, связывающие текущий узел сетки
      % с соседними узлами справа по оси X и вниз по оси Y
      %              O(i,j)--Ax(i)--O(i+1,j)
      %              |
      %              |
      %              Ay(i)
      %              |
      %              |
      %              O(i,j+1)
      % Для решения системы разностных уравнений  используется метод Зейделя, в
      % котором разностные уравнения формируются по одному шаблону для всех
      % внутренних узлов с использование массивов Ax и Ay.


      epsilon=input ('Введите  epsilon=');% запрос допустимой погрешности
      disp('Ждите, идут вычисления')
      U=zeros(ny,nx);% формирование нулевого начального приближения
      % Нулевые граничные условия сформированы
```

```
nn=0; % массив номеров итераций
it=0; % массив числа итераций
iter=0;  % Счетчик итераций

%======ИТЕРАЦИОННЫЙ ПРОЦЕСС==========
while 1
    iter=iter+1;
    if iter>100000
        disp('Число итераций больше заданного числа, равного 100000')
        disp('ВНИМАНИЕ! Выводимые графики показывают результаты, полученные
за заданное число итераций');
        break % аварийный конец итераций
    end;
    delta=0; % формирование нулевого максимального приращения решения
    for i=2 :ny-1
        for j=2 :nx-1
            Uk=U(i,j); % запоминание старого значения решения в узле
            U(i,j)=1/(Ax(i,j)+Ax(i-1,j)+Ay(i,j)+Ay(i,j-1))*...
                (Ax(i,j)*U(i+1,j)+Ax(i-1,j)*U(i-
1,j)+Ay(i,j)*U(i,j+1)+Ay(i,j-1)*U(i,j-1)+f(i,j));
            delta1=abs(U(i,j)-Uk);
            if delta1>delta
                delta=delta1; % формирование нормы поправки решения
            end
        end
    end;
    rel_delta=delta/norm(U,inf); % относительная поправка решения
    if  rel_delta<=epsilon;% проверка выполнения критерия останова по относ.
норме приращения
        nmax=iter;
        break
    end;

   %=====Формирование массивов для графика изменения относительной поправки от
номера итерации
     nn(iter)=rel_delta;
     it(iter)=iter;
  end;
```

sec_3 Программа моделирования угрозы, распределенной во всей внешней области

```
% Модель области постоянной плотности угрозы во всей внешней области

% Модель описывается эллиптическим ДУЧП вида
% d/dx(sigma*dU/dx)+d/dy(sigma*dU/dy)=funf(x,y)
% с граничными условиями первого рода U|r=fi(x,y) по всей границе.
% Уравнение решается в прямоугольной области x1<=x<=x2, y1<=y<=y2
% с постоянным шагом h по осям X и Y.
clear; % Очистка рабочей области
clc; % Очистка командного окна
close all; % закрытие всех графических окон
x1=0;
x2=1;
y1=0;
y2=1;
h=0.01;  % шаг, кратный размеру области
```

```
[x,y]=meshgrid(x1:h:x2,y2:-h:y1); % формирование разностной сетки

sigma=1.00; % Проницаемость среды

% Задача решается при нулевых граничных условиях

% Расчет функции правой части в узлах сетки
nx=round((x2-x1)/h)+1; % Количество узлов по оси X
ny=round((y2-y1)/h)+1; % Количество узлов по оси Y

% Матрицы коэффициенты
Ax=sigma*ones(nx,ny)/(h^2);
Ay=sigma*ones(ny,nx)/(h^2);

% Угроза по всей внешней области
funDan=1.0;
funf=ones(ny+2,nx+2)*funDan;

sigma1=1.0e-12; % Проницаемость защищаемой области
xProt1=0.2; % Координаты защищаемой области
yProt1=0.4;
xProt2=0.4;
yProt2=0.6;
Ax(round(yProt1/h)+1:round(yProt2/h),round(xProt1/h)+1:round(xProt2/h))=sigm
a1/(h^2);
Ay(round(yProt1/h)+1:round(yProt2/h),round(xProt1/h)+1:round(xProt2/h))=sigm
a1/(h^2);

% Плотность угроз внутри защищаемой области
funf(round(yProt1/h)+1:round(yProt2/h),round(xProt1/h)+1:round(xProt2/h))=0;


%=========Вызов функции решения============================
[U,nmax,it,nn]=fdm_1(nx,ny,Ax,Ay,funf);
%[U,x,y,nmax,it,nn]=fdm_ell_eq(x1,x2,y1,y2,h,funf,fi,sigma);

fprintf('Решение получено за %u итераций ',nmax);

%============Построение трехмерного графика решения=======

figure;
mesh(x,y,U)
%surf(x,y,U);
colorbar;
xlabel('x');
ylabel('y');
zlabel('u');
title('Поверхность решения');

%===========Построение линий уровня решения===========
figure;

axis square ij % Начало координат в верхнем левом углу
contour(x,y,U,'ShowText','on')
% [CMatr,h1]=contour(x,y,U);
% clabel(CMatr,h1);
grid on;
xlabel('x');
```

```
      ylabel('y');
      title('Линии уровня');
      hold on
      plot([xProt1,xProt1,xProt2,xProt2,xProt1],[yProt1,yProt2,yProt2,yProt1,yProt
1],'LineWidth',2)

      %===========Построение графика зависимости относительной нормы поправки от
номера итерации====
      figure;
      loglog(it, nn, '-')
      xlabel('Номер итерации');
      ylabel('Относительная норма поправки');
      grid on
      xlabel('Номер итерации');
      ylabel('Относительная норма поправки');
      title('Число итераций')
```

ПРИЛОЖЕНИЕ Б
МОДЕЛИРОВАНИЕ УГРОЗ БЕЗОПАСНОСТИ АЭРОПОРТА В ФОРМАТЕ ДИФФЕРЕНЦИАЛЬНЫХ УРАВНЕНИЙ В ЧАСТНЫХ ПРОИЗВОДНЫХ ДЛЯ НЕСТАЦИОНАРНОЙ ЗАДАЧИ
(ОБЯЗАТЕЛЬНОЕ)

Различные варианты нестационарной модели реализованы в системе MATLAB. Разработанные варианты главной программы и функции, реализующих итерационный процесс, представлены ниже.

Программа sec_4 моделирует нестационарную задачу с источником угрозы, заданным в одной точке. Задача решается в прямоугольной области, с координатами левого нижнего угла `x1=0, y1=0` и правого верхнего угла `x2=1 и y2=1`. Задаются шаг сетки `h`, проницаемость внешней среды `sigma=1`, строится сетка, вычисляются массивы разностных коэффициентов. Координаты источника угрозы задаются переменными `xDan=0.5` и `yDan=0.5`. Величина угрозы задается переменной `uDan=1.0`. Задаются координаты `xProt1=0.2, yProt1=0.4, xProt2=0.4, yProt2=0.6` защищаемой области и малая проницаемость защищаемой области `sigma1=0.01`. Задавать проницаемость защищаемой области равной нулю нецелесообразно, так как это означает полную защиту от проникновения угроз на защищаемой области.

Решение задачи производится вызовом функции `fdm_3`. После получения решения строятся трехмерный график решения, график линий уровня решения и график относительной нормы поправки от номера итерации.

Функция `fdm_3` реализует решение системы разностных уравнений на каждом временном шаге методом Зейделя.

Входные данные функции:

– `Uk_1` – решение на предыдущем временном шаге;

– `c` – "скорость" по времени;

– `tau` – шаг по времени;

– `epsilon` – допустимое относительное изменение решения (критерий окончания итерационного процесса);
– `uDan` – величина угрозы, `xDan, yDan` – координаты угрозы;
– `nx, ny` – количество узлов по оси `X,` количество узлов по оси `Y;`
– `Ax и Ay` – массивы коэффициентов разностной схемы;
– `h` – шаг сетки.
– Выходные данные функции:
– `U` – двумерный массив решений в узлах сетки;
– `nmax` – число итераций, за которое получено решение;
– `it` – массив номеров итераций;
– `nn` – массив относительных поправок к решению.

sec_4 Программа моделирования нестационарной задачи с одиночной угрозой

```
% Нестационарная задача
% Модель одиночной угрозы
% В точке задан источник угрозы

% Модель описывается параболическим ДУЧП вида
% d/dx(sigma*dU/dx)+d/dy(sigma*dU/dy)=c/tau*dU/d(tau)
% с граничными условиями первого рода U|r=fi(x,y) по всей границе.
% Уравнение решается в прямоугольной области x1<=x<=x2, y1<=y<=y2
% с постоянным шагом h по осям X и Y.
% K - число шагов по времени
clear; % Очистка рабочей области
clc; % Очистка командного окна
close all; % закрытие всех графических окон
x1=0;
x2=1;
y1=0;
y2=1;
h=0.01;  % шаг, кратный размеру области
sigma=1.00; % Проницаемость среды
% Задача решается при нулевых граничных условиях

[x,y]=meshgrid(x1:h:x2,y2:-h:y1); % формирование разностной сетки

% Расчет функции правой части в узлах сетки
nx=round((x2-x1)/h)+1; % Количество узлов по оси X
ny=round((y2-y1)/h)+1; % Количество узлов по оси Y
funf=zeros(ny+2,nx+2);

% Массивы коэффициентов
```

```
Ax=sigma*ones(nx,ny)/(h^2);
Ay=sigma*ones(ny,nx)/(h^2);

% Координаты источника опасности
xDan=0.5;
yDan=0.5;
% Величина опасности
uDan=1.0;

sigma1=0.010; % Проницаемость защищаемой области
%sigma1=10000.0; % Проницаемость защищаемой области
xProt1=0.2; % Координаты защищаемой области
yProt1=0.4;
xProt2=0.4;
yProt2=0.6;

% Разностные коэффициенты для защищаемой области
Ax(round(yProt1/h)+1:round(yProt2/h),round(xProt1/h)+1:round(xProt2/h))=sigm
a1/(h^2);
Ay(round(yProt1/h)+1:round(yProt2/h),round(xProt1/h)+1:round(xProt2/h))=sigm
a1/(h^2);



% Плотность угроз внутри защищаемой области
funf(round(yProt1/h)+1:round(yProt2/h),round(xProt1/h)+1:round(xProt2/h))=-
10;

% формирование  начального приближения
U0=zeros(ny,nx);
xD=round(xDan/h)+1;
yD=round(yDan/h)+1;
U0(yD,xD)=uDan;

%============Построение трехмерного графика начального приближения=======

%axis square ij % Начало координат в верхнем левом углу
figure;
mesh(x,y,U0)
%surf(x,y,U);
colorbar;
title('Начальное приближение');
xlabel('x');
ylabel('y');
zlabel('u');

U=U0;% Предыдущее приближение равно начальному приближению

c=1.0e+2; % "скорость"
tau=1.0e-1; % Шаг по времени
K=160; % Число временных шагов
epsilon=0.0001;

% Цикл по временным шагам

for k=1:K
    k
    Uk=U;
    %=========Вызов функции решения==========================
    [U,nmax,it,nn]=fdm_3(Uk,c, tau, epsilon,uDan,xDan,yDan,h,nx,ny,Ax,Ay);
    %fprintf('Решение получено за %u итераций ',nmax);
```

```
        R=Uk==U;
    %
    end
     %============Построение трехмерного графика решения=======

        %axis square ij % Начало координат в верхнем левом углу
        figure;
        mesh(x,y,U)
        %surf(x,y,U);
        colorbar;
        title('Поверхность решения');
        xlabel('x');
        ylabel('y');
        zlabel('u');
        %===========Построение линий уровня решения===========
        figure;
        axis square ij % Начало координат в верхнем левом углу
        contour(x,y,U,20,'ShowText','on')
        % [CMatr,h1]=contour(x,y,U);
        % clabel(CMatr,h1);
        grid on;
        xlabel('x');
        ylabel('y');
        title('Линии уровня');
        hold on

plot([xProt1,xProt1,xProt2,xProt2,xProt1],[yProt1,yProt2,yProt2,yProt1,yProt1],'Li
neWidth',2)

    % %===========Построение графика зависимости относительной нормы поправки от
номера итерации====
    % figure;
    % loglog(it, nn, '-')
    % xlabel('Номер итерации');
    % ylabel('Относительная норма поправки');
    % grid on
    % xlabel('Номер итерации');
    % ylabel('Относительная норма невязки');
    % title('Число итераций')
```

Функция решения методом конечных разностей параболического дифференциального уравнения в частных производных для единичной угрозы

```
    function [U,nmax,it,nn]=fdm_3(Uk_1,c, tau, epsilon,uDan,xDan,yDan,h,nx,ny,Ax,Ay)
    % Функция решения методом конечных разностей параболического ДУЧП вида
    % d/dx(sigma*dU/dx)+d/dy(sigma*dU/dy)=c/tau*dU/d(tau)              (1)
    % с граничными условиями первого рода U|r=fi(x,y)по всей границе.
    % Уравнение решается на каждом временном слое
    % в прямоугольной области x1<=x<=x2, y1<=y<=y2
    % с постоянным шагом h по осям X и Y и шагом tau по временной переменной

    % ВХОДНЫЕ ДАННЫЕ
    % Uk_1 - решение на предыдущем временном шаге
    % c - "скорость" по времени
    % tau - шаг по времени
    % epsilon - допустимое относительное изменение решения
```

```
% uDan - величина угрозы, xDan, yDan - координаты угрозы
% nx, ny - Количество узлов по оси X, количество узлов по оси Y
% Ax и Ay - массивы коэффициентов разностной схемы
% h - шаг сетки

% ВЫХОДНЫЕ ДАННЫЕ:
% U - двумерный массив решений в узлах сетки;
% nmax - число итераций, за которое получено решение;
% it - массив номеров итераций;
% nn - массив относительных поправок к решению.

% МЕТОД РЕШЕНИЯ:
% Разностная аппроксимация строится на основе интегро-интерполяционного
% метода. Поскольку используется постоянный шаблон, то система разностных
% уравнений в явном виде не формируется, а строятся два массива Ax и Ay,
% содержащие коэффициенты разностной схемы, связывающие текущий узел сетки
% с соседними узлами справа по оси X и вниз по оси Y
%              O(i,j)--Ax(i)--O(i+1,j)
%              |
%              |
%              Ay(i)
%              |
%              |
%              O(i,j+1)
% Для решения системы разностных уравнений  используется метод Зейделя, в
% котором разностные уравнения формируются по одному шаблону для всех
% внутренних узлов с использование массивов Ax и Ay.


%U=zeros(ny,nx);% формирование нулевого начального приближения
U=Uk_1;
% Нулевые граничные условия сформированы
% Угроза на сетке
% Координаты опасности
xDan=round(xDan/h)+1;
yDan=round(yDan/h)+1;
U(xDan,yDan)=uDan;

nn=0; % массив номеров итераций
it=0; % массив числа итераций
iter=0;  % Счетчик итераций

%======ИТЕРАЦИОННЫЙ ПРОЦЕСС==========
while 1
    iter=iter+1;
    if iter>100000
        disp('Число итераций больше заданного числа, равного 100000')
        break % аварийный конец итераций
    end
    delta=0; % формирование нулевого максимального приращения решения
    for i=2 :ny-1
        for j=2 :nx-1
            if and(i==yDan,j==xDan)
                U(i,j)=uDan;
            else
                Uk=U(i,j); % запоминание старого значения решения в узле
                U(i,j)=1/(Ax(i,j)+Ax(i-1,j)+Ay(i,j)+Ay(i,j-1)+c/tau)*...
                   (Ax(i,j)*U(i+1,j)+Ax(i-1,j)*U(i-1,j)+Ay(i,j)*U(i,j+1)+
                   Ay(i,j-1)*U(i,j-1)+(c*Uk_1(i,j))/tau);
                delta1=abs(U(i,j)-Uk);
                if delta1>delta
```

```
                        delta=delta1; % формирование нормы поправки решения
                    end
                end
            end
        end
        rel_delta=delta/norm(U,inf); % относительная поправка решения
        if  rel_delta<=epsilon % проверка выполнения критерия останова по относ.
норме приращения
            nmax=iter;
            break
        end

        %=====Формирование массивов для графика изменения относительной поправки
от номера итерации
        nn(iter)=rel_delta;
        it(iter)=iter;
    end
```

ПРИЛОЖЕНИЕ В
НЕЙРОСЕТЕВОЕ РАНЖИРОВАНИЕ АЭРОПОРТОВ
(СПРАВОЧНОЕ)

Ниже в таблице представлен сформированный экспертами набор данных, показана общая оценка уязвимости аэропорта и оценки, данные экспертами ИКАО. Проверки ИКАО выборочные и могут не совпадать с оценками экспертов.

Набор обучающих данных не имеет пропусков и аномальных значений.

Кодировать необходимо только оценку уязвимости. Примем, что при общей оценке уязвимости 8–10 баллов аэропорт является безопасным и кодируем это состояние 1, оценки ниже 8 соответствуют уязвимости аэропорта и кодируются 0. Так как планируется применить для построения нейронной сети систему MATLAB, автоматически производящую масштабирование данных, то нет необходимости масштабирования данных.

В качестве проблемы обучающего набора следует отметить несбалансированность набора – в наборе, естественно, преобладают безопасные аэропорты.

Для программы использован инструмент визуального программирования Neural Network Pattern Recognition Tool пакета Deep Learning Toolbox системы MATLAB.

Предварительно в рабочее пространство MATLAB необходимо загрузить массив признаков **`P`**, каждая строка которого соответствует признакам одного аэропорта, и вектор-столбец целевых значений **`T`**, элементы которого представляют собой оценки безопасности аэропорта (1 или 0).

В программе подразумевается, что что входные данные и целевые значения находятся в рабочем пространстве MATLAB.

Таблица В.1 – Набор данных

Номер примера	Показатели безопасности																									Общая оценка уязвимости (эксперт ИКАО)
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	
1	10	10	8	7	6	6	5	7	9	7	5	7	8	9	6	7	7	8	7	6	8	8	5	6	9	8
2	10	10	7	6	7	8	7	7	9	6	6	8	6	8	9	9	7	6	9	9	8	8	7	9	7	8
3	10	10	9	7	8	8	7	8	8	9	7	8	7	6	9	8	8	8	7	9	8	6	8	8	7	9 (ИКАО)
4	10	10	6	6	6	9	9	8	9	7	6	6	5	7	8	8	9	6	8	7	7	8	6	9	9	9
5	0	10	5	7	7	8	7	7	8	7	5	5	5	7	8	8	7	8	6	7	7	7	5	6	8	7
6	10	10	7	8	7	8	8	9	8	8	9	7	6	6	5	9	8	8	7	6	6	9	6	8	7	8
7	10	10	9	9	8	7	8	8	8	8	8	7	6	6	6	5	9	7	7	8	8	6	6	8	9	8
8	10	10	7	6	9	9	7	6	9	8	8	8	6	6	5	5	5	8	8	7	7	6	9	8	8	7
9	10	10	9	5	8	9	9	8	8	7	6	6	6	8	9	9	8	6	7	7	9	6	9	6	6	8
10	10	10	8	8	7	7	8	7	6	8	8	8	8	6	6	7	5	7	7	7	5	5	8	9	9	7
11	10	10	5	7	6	7	6	6	8	8	7	8	8	8	7	6	8	5	9	7	7	8	6	6	9	8
12	0	6	6	7	6	5	8	7	7	6	6	8	8	8	5	9	9	8	6	8	5	7	6	5	6	7 (ИКАО)
13	10	10	7	7	6	7	7	8	6	6	8	8	8	6	7	6	8	6	7	7	7	8	6	7	6	7
14	10	7	6	6	6	7	8	7	7	7	5	7	6	7	6	8	8	8	6	6	8	6	8	6	6	8
15	10	10	8	8	6	8	8	6	7	7	7	8	9	9	7	5	6	7	8	7	6	8	6	7	8	8
16	10	10	6	8	9	9	8	9	7	9	8	7	7	9	9	9	7	8	8	9	8	5	8	7	9	9 (ИКАО)
17	0	7	7	6	8	7	8	5	7	6	6	6	7	5	6	7	8	8	5	8	9	8	7	7	5	6
18	10	10	6	7	6	7	7	7	9	8	7	8	6	6	8	9	9	7	8	9	9	9	6	6	6	8
19	0	7	9	9	8	8	6	6	7	5	7	6	6	8	9	8	9	9	9	8	7	9	7	6	8	8
20	10	5	6	8	6	8	8	6	6	6	8	9	8	8	5	7	7	9	8	9	7	6	8	9	8	8
21	0	10	7	8	8	8	7	8	7	8	8	9	6	9	9	6	7	9	8	9	7	6	8	8	9	9
22	10	6	8	8	9	9	6	9	9	7	6	7	7	8	8	7	9	6	9	9	8	8	7	7	8	8
23	10	7	8	7	7	6	7	7	7	6	8	7	8	6	6	6	8	8	7	6	8	7	7	7	7	7 (ИКАО)

Продолжение таблицы В.1

24	0	10	7	8	7	6	6	9	7	7	7	7	7	9	9	7	7	7	6	9	8	8	7	8	7	8
25	10	7	6	6	6	7	9	6	6	8	8	7	9	7	8	8	6	6	8	9	9	8	7	7	7	8
26	10	10	8	8	9	8	9	9	6	7	8	6	8	8	8	6	7	7	7	7	6	9	9	9	8	
27	10	10	7	7	8	8	8	8	8	9	7	6	8	6	8	9	8	7	7	9	8	8	7	7	7	
28	10	10	8	8	5	8	8	8	9	8	6	7	7	7	7	9	7	8	8	8	7	6	8	8	8	
29	0	10	7	7	8	7	7	7	9	5	8	7	8	7	9	7	7	7	8	9	9	8	7	6	8	
30	0	8	8	8	8	7	8	8	8	8	6	7	6	8	8	8	7	6	7	9	7	7	6	6	7	
31	10	9	6	7	8	8	8	6	6	8	8	7	7	7	6	7	6	6	7	7	6	8	7	7	7	7 (ИКАО)
32	10	10	6	7	6	7	7	6	6	5	9	8	6	5	7	6	6	5	7	8	8	7	7	7	7	7 (ИКАО)
33	10	9	7	8	9	8	9	7	9	8	8	7	7	9	8	8	7	7	7	8	7	9	8	8	8	9
34	0	9	7	6	5	7	7	6	6	5	6	6	5	8	8	7	7	6	5	8	7	6	8	9	6	6 (ИКАО)
35	10	10	9	9	8	6	8	8	9	7	8	9	8	8	9	8	8	9	9	8	8	7	9	8	9	9
36	10	7	7	6	8	7	6	5	6	7	8	8	8	7	6	5	7	6	7	6	5	6	8	6	6	7
37	10	9	8	8	8	7	7	9	8	8	8	6	6	6	8	9	8	8	9	9	8	8	7	7	8	8
38	10	7	6	7	6	6	6	7	7	7	7	6	8	8	6	9	9	8	7	6	8	7	8	7	7	7
39	0	10	6	8	8	8	7	7	5	7	7	6	8	6	8	8	7	7	7	7	8	6	8	7	7	7 (ИКАО)
40	10	10	9	7	8	9	9	8	9	8	9	9	8	7	9	8	7	6	8	9	6	7	8	8	6	8
41	10	10	9	9	8	9	7	7	8	8	5	9	5	8	8	6	9	7	9	9	7	8	8	7	9	7
42	10	7	8	7	9	8	8	9	8	8	7	7	9	8	9	8	7	8	8	8	8	7	9	9	8	8
43	0	8	7	9	9	8	8	6	9	9	8	8	7	7	7	9	7	7	9	8	9	8	8	9	9	9
44	10	10	8	8	8	9	9	9	9	7	9	9	7	7	9	8	8	9	8	9	8	8	9	8	8	9
45	0	7	8	9	9	8	9	9	9	8	8	7	8	9	9	7	8	7	8	7	8	9	8	9	9	9
46	0	9	7	7	8	8	8	7	7	5	6	8	5	7	7	7	7	8	7	8	7	8	7	8	8	7
47	10	9	8	8	8	7	8	8	8	7	8	7	9	9	8	8	8	8	9	7	8	8	9	9	9	8
48	10	10	8	7	9	9	9	7	8	8	8	9	9	7	8	9	9	7	8	9	9	8	8	8	8	9
49	10	10	7	8	7	8	8	7	8	8	8	9	8	8	5	7	6	7	5	7	7	5	8	8	8	7
50	0	7	9	9	9	8	7	8	9	7	8	8	7	9	9	9	8	9	8	9	8	8	7	9	7	9

Продолжение таблицы В.1

51	10	8	8	8	7	8	7	7	8	8	9	8	5	6	7	7	8	8	7	7	9	7	9	7	8	8
52	0	7	8	7	9	8	7	9	8	7	8	9	7	9	9	9	7	8	7	9	7	9	9	9	7	9 (ИКАО)
53	10	9	7	8	8	9	9	6	9	9	9	6	7	7	8	8	9	7	9	7	6	8	9	9	9	9
54	0	10	8	9	8	9	6	8	9	8	8	5	9	7	7	9	8	9	8	7	9	8	5	6	5	7 (ИКАО)
55	0	10	9	9	9	9	6	8	8	7	7	8	8	8	9	8	7	7	8	8	9	9	8	8	8	8
56	10	9	7	8	6	5	6	8	7	8	6	9	9	7	5	8	8	5	9	6	5	6	6	7	7	6
57	0	9	7	5	7	8	8	7	6	6	8	9	6	8	7	8	9	7	8	8	5	8	6	9	7	7
58	0	9	7	8	8	8	7	7	7	7	5	8	8	9	9	8	9	8	7	9	8	9	8	9	9	8
59	10	10	7	7	7	9	8	7	7	8	8	8	8	8	8	9	9	8	9	8	9	8	6	9	9	9 (ИКАО)
60	0	10	7	7	5	7	6	6	6	7	7	7	7	8	5	7	7	5	6	6	7	6	7	7	8	7
61	0	8	9	9	8	9	9	8	7	7	9	8	9	8	9	8	7	9	8	9	8	9	6	8	7	9 (ИКАО)
62	10	8	6	7	5	6	7	7	7	7	6	8	7	8	6	6	6	7	7	7	8	8	8	5	8	7
63	0	7	6	7	7	5	7	5	7	7	7	5	7	6	8	7	8	8	6	7	6	5	6	7	7	6
64	0	7	8	8	8	9	9	8	9	8	7	8	9	7	9	9	8	7	7	7	8	8	9	9	9	9 (ИКАО)
65	0	8	7	7	7	7	7	7	6	8	7	6	6	6	7	7	6	6	5	6	6	5	6	6	6	6
66	10	10	7	9	9	9	7	9	9	8	9	8	8	8	9	9	8	7	7	9	8	8	9	9	9	9
67	10	10	8	9	9	8	8	8	8	7	8	9	9	6	8	9	8	8	8	6	8	7	8	7	7	8
68	10	10	6	7	7	7	7	9	8	9	8	8	5	8	7	7	6	8	9	8	8	9	8	8	8	8
69	10	9	8	9	8	8	7	8	8	8	6	7	7	7	8	8	8	8	7	7	9	9	7	8	8	8
70	10	9	7	8	7	7	5	8	9	9	9	6	9	9	8	8	7	7	8	8	8	9	7	7	9	8
71	0	10	8	9	9	9	8	9	9	8	9	9	8	8	8	9	9	9	8	8	9	8	9	9	9	9
72	0	10	7	8	7	7	8	7	7	6	5	7	7	6	7	8	7	7	7	6	8	6	7	6	7	7
73	10	9	7	8	8	8	8	8	9	9	9	9	9	8	9	8	8	7	7	7	9	9	8	8	7	9
74	10	8	8	8	8	8	6	8	8	9	8	7	7	7	8	8	8	7	7	8	8	7	9	9	9	9
75	0	10	7	7	7	9	9	8	8	8	8	7	7	5	8	9	9	9	8	7	7	9	9	9	9	8
76	0	10	8	8	8	8	6	9	8	7	7	7	8	8	9	9	7	7	8	8	8	8	9	9	8	8

Продолжение таблицы В.1

77	10	10	7	7	8	9	8	8	8	8	9	9	9	9	6	8	9	8	8	8	9	9	7	7	7	8
78	10	8	8	8	7	7	9	9	9	8	9	8	8	5	9	8	9	8	8	9	7	8	8	8	8	8
79	10	8	7	6	8	9	9	9	8	8	8	8	8	7	9	8	8	9	9	9	8	7	8	8	9	9
80	10	10	9	8	9	9	8	9	9	10	10	9	8	9	9	9	8	10	9	9	8	8	10	9	9	10 ИКАО
81	10	8	7	8	9	8	8	8	9	7	9	9	8	7	8	9	8	7	9	9	7	9	7	9	7	9
82	0	10	6	7	7	8	9	9	9	6	7	8	8	6	9	8	8	8	7	8	9	8	7	8	7	8
83	0	8	8	8	8	7	7	9	8	8	8	8	7	7	8	8	9	6	9	9	7	7	8	8	8	8
84	10	9	7	8	8	9	8	9	9	9	8	8	9	9	9	8	8	7	8	9	9	8	9	9	9	9
85	0	10	8	9	8	8	9	8	8	7	8	9	9	7	7	6	9	6	9	9	8	8	8	8	8	8
86	10	8	8	9	9	9	8	9	8	9	8	7	7	8	8	8	7	9	9	9	8	9	8	8	9	9
87	0	10	7	9	9	9	8	8	8	8	7	7	8	9	9	9	9	9	8	7	9	9	9	8	9	9
88	10	8	8	8	8	8	7	9	9	5	9	9	8	6	7	7	9	8	8	8	7	9	9	8	8	8
89	0	10	8	9	9	9	9	8	9	8	8	8	9	9	9	8	9	9	8	9	8	9	8	8	9	9
90	0	7	7	7	8	8	9	9	9	6	6	9	9	5	7	7	7	8	7	8	7	9	7	7	7	7 (ИКАО)
91	10	10	9	9	9	9	8	9	9	6	8	9	9	8	9	8	9	9	8	8	8	9	9	9	9	9
92	0	8	7	8	8	7	7	8	6	9	8	9	6	7	8	7	7	7	7	7	8	7	7	7	7	7
93	10	10	7	8	7	7	7	7	8	8	7	7	6	7	7	7	7	5	8	8	7	8	8	7	8	7
94	10	10	8	9	9	9	9	9	9	10	9	9	8	10	9	8	9	10	9	8	10	9	9	10	9	10
95	10	10	7	8	7	8	7	8	8	8	7	9	9	7	8	7	9	9	9	8	7	9	8	7	7	8
96	10	10	6	7	6	6	6	8	6	6	6	8	8	9	9	7	8	7	8	7	7	7	7	7	8	7
97	10	8	7	7	6	6	8	8	5	8	7	6	6	8	8	6	7	6	6	7	5	7	6	7	7	7 (ИКАО)
98	0	9	6	7	9	9	8	8	7	7	6	8	8	8	9	9	9	9	9	9	8	7	7	7	8	8
99	10	10	9	9	9	9	8	8	9	9	6	9	10	8	10	9	9	10	8	9	9	10	8	9	9	10
100	10	10	8	8	8	7	7	7	7	7	6	8	8	9	9	9	9	7	9	8	8	8	7	9	9	8
101	10	10	6	8	8	8	7	6	8	6	6	7	7	7	7	7	8	8	7	9	7	8	8	8	8	7
102	10	9	7	7	8	8	8	6	7	8	8	9	9	8	7	9	9	9	8	7	7	9	9	9	9	8

Программа нейросетевого классификатора

```
% Программа "Нейроклассификатор" классификации аэропортов по безопасности %
% This script assumes these variables are defined:
%
% P - input data.
% T - target data.
x = P';
t = T';

% Choose a Training Function
% For a list of all training functions type: help nntrain
% 'trainlm' is usually fastest.
% 'trainbr' takes longer but may be better for challenging problems.
% 'trainscg' uses less memory. Suitable in low memory situations.
trainFcn = 'trainscg'; % Scaled conjugate gradient backpropagation.

% Create a Pattern Recognition Network
hiddenLayerSize = 10;
net = patternnet(hiddenLayerSize, trainFcn);

% Choose Input and Output Pre/Post-Processing Functions
% For a list of all processing functions type: help nnprocess
net.input.processFcns = {'removeconstantrows','mapminmax'};

% Setup Division of Data for Training, Validation, Testing
% For a list of all data division functions type: help nndivision
net.divideFcn = 'dividerand'; % Divide data randomly
net.divideMode = 'sample'; % Divide up every sample
net.divideParam.trainRatio = 70/100;
net.divideParam.valRatio = 15/100;
net.divideParam.testRatio = 15/100;

% Choose a Performance Function
% For a list of all performance functions type: help nnperformance
```

```
net.performFcn = 'crossentropy'; % Cross-Entropy

% Choose Plot Functions
% For a list of all plot functions type: help nnplot
net.plotFcns = {'plotperform','plottrainstate','ploterrhist', ...
'plotconfusion', 'plotroc'};

% Train the Network
[net,tr] = train(net,x,t);

% Test the Network
y = net(x);
e = gsubtract(t,y);
performance = perform(net,t,y)
tind = vec2ind(t);
yind = vec2ind(y);
percentErrors = sum(tind ~= yind)/numel(tind);

% Recalculate Training, Validation and Test Performance
trainTargets = t .* tr.trainMask{1};
valTargets = t .* tr.valMask{1};
testTargets = t .* tr.testMask{1};
trainPerformance = perform(net,trainTargets,y)
valPerformance = perform(net,valTargets,y)
testPerformance = perform(net,testTargets,y)

% View the Network
view(net)

% Plots
% Uncomment these lines to enable various plots.
%figure, plotperform(tr)
%figure, plottrainstate(tr)
%figure, ploterrhist(e)
%figure, plotconfusion(t,y)
```

```
%figure, plotroc(t,y)

% Deployment
% Change the (false) values to (true) to enable the following code blocks.
% See the help for each generation function for more information.
if (false)
% Generate MATLAB function for neural network for application
% deployment in MATLAB scripts or with MATLAB Compiler and Builder
% tools, or simply to examine the calculations your trained neural
% network performs.
genFunction(net,'myNeuralNetworkFunction');
y = myNeuralNetworkFunction(x);
end
if (false)
% Generate a matrix-only MATLAB function for neural network code
% generation with MATLAB Coder tools.
genFunction(net,'myNeuralNetworkFunction','MatrixOnly','yes');
y = myNeuralNetworkFunction(x);
end
if (false)
% Generate a Simulink diagram for simulation or deployment with.
% Simulink Coder tools.
gensim(net);
end
```

ПРИЛОЖЕНИЕ Г
НЕЙРОСЕТЕВАЯ ОЦЕНКА УРОВНЯ ГОТОВНОСТИ ПЕРСОНАЛА (СПРАВОЧНОЕ)

Выбран набор показателей для оценки уровня готовности персонала транспортной безопасности к выполнению профессиональной деятельности. Выполнена подготовка набора обучающих данных (см.5.1 в т.1) для нейросетевой оценки уровня готовности персонала транспортной безопасности к выполнению профессиональной деятельности.

В системе MATLAB (см.5.4 в томе 1) разработана нейронная сеть для классификации сотрудников. Эксперименты показали высокое качество полученного нейросетевого классификатора для оценки уровня готовности персонала транспортной безопасности к выполнению профессиональной деятельности.

Разработана программа «Neuronet» (см.5.5 в томе 1), предназначенная для обучения нейронной сети. С помощью этой программы получены весовые коэффициенты обученной нейронной сети, использованные при разработке программы оценки персонала транспортной безопасности.

Проведено исследование разработанной нейронной сети, выбран лучший порог отсечения нейрона выходного слоя. Исследования показали, что разработанная сеть по характеристикам качества работы не уступает сети, реализованной средствами MATLAB.

Разработана программа «Neurotest» (см.5.5 в томе 1), предназначенная для оценки компетенций персонала транспортной безопасности к выполнению задач профессиональной деятельности с помощью предварительно обученной нейронной сети.

Г.1 Исходные данные для нейросети

Таблица А.1 – Исходные данные для обучения нейронной сети

Компетенция	К 1	К 2	К 2	К 2	К 2	К 2	К 3	К 3	К 3	К 4	К 5	К 5	К 5	К 5	К 5	К 5	К 6	К 6	К 6	К 7	К7	К7	К7	К7	К7	К7	Результат проверки
Требование		Т 2-1	Т 2-2	Т 2-3	Т 2-4	Т 2-5	Т 3-1	Т 3-2	Т 3-3		Т 5-1	Т 5-2	Т 5-3	Т 5-4	Т 5-5	Т 5-6	Т 6-1	Т 6-2	Т 6-3	Т 7-1	Т 7-2	Т 7-3	Т 7-4	Т 7-5	Т 7-6	Т 7-7	
1	6	7	5	9	6	8	7	8	7	7	7	4	8	6	8	8	6	6	9	9	4	8	6	6	6	6	годен
2	7	7	3	7	5	7	7	5	4	5	5	5	8	6	8	5	5	7	6	5	8	6	6	5	8	7	отсев
3	4	6	6	8	8	8	4	4	8	6	6	6	7	5	7	8	8	6	9	9	6	6	7	7	7	7	годен
4	9	7	7	9	9	9	6	9	7	7	5	6	6	8	9	9	6	8	8	8	6	7	8	8	6	6	годен
5	6	8	8	8	4	8	7	7	6	4	4	7	7	6	6	7	9	7	6	6	7	8	6	6	7	5	отсев
6	6	7	7	5	5	7	7	6	8	9	9	6	8	8	7	9	7	7	6	5	9	7	9	8	8	8	годен
7	7	7	5	5	7	7	7	8	6	5	8	5	6	8	8	9	6	6	8	8	8	7	9	7	8	8	годен
8	9	9	9	6	6	8	5	5	6	7	7	6	6	7	7	8	8	8	9	6	6	6	9	9	7	7	годен
9	9	6	6	6	8	5	5	8	7	8	6	6	5	8	9	7	8	9	6	6	8	8	8	8	9	6	годен
10	6	8	8	7	7	9	8	8	8	8	8	9	6	8	7	7	9	9	5	8	6	6	7	7	5	7	годен
11	6	8	8	8	6	5	6	7	7	8	6	8	7	6	5	5	6	7	7	8	8	7	9	9	8	9	годен
12	6	9	6	6	7	6	7	7	7	8	7	6	6	6	9	7	7	8	6	9	9	7	7	7	7	7	годен
13	5	6	8	8	6	7	7	5	8	6	7	8	8	8	6	8	7	8	5	7	7	8	8	9	8	7	годен
14	4	7	7	8	6	5	8	8	8	9	6	6	8	8	8	8	9	8	8	9	8	8	8	8	8	8	годен
15	9	9	9	8	7	6	9	6	9	6	6	6	9	8	7	7	7	8	6	9	8	7	7	9	9	6	годен
16	6	6	7	7	4	7	7	3	6	5	6	6	8	7	9	7	6	6	6	7	6	8	5	6	6	5	отсев
17	8	8	8	5	5	6	8	5	6	6	8	6	6	6	5	7	8	5	7	4	4	4	8	7	7	7	отсев
18	9	9	9	8	8	8	8	6	6	6	9	8	9	8	7	8	8	6	6	9	9	7	7	9	9	9	годен
19	5	5	8	8	6	7	7	7	5	6	5	5	6	6	8	6	5	6	6	6	6	8	5	7	7	7	отсев
20	9	7	7	7	5	8	8	6	6	5	8	8	6	6	6	8	7	7	6	6	8	8	6	6	6	7	годен

Компетенция	К1	К2	К2	К2	К2	К2	К3	К3	К3	К4	К5	К5	К5	К5	К5	К5	К6	К6	К6	К7	К7	К7	К7	К7	К7	Результат проверки
21	8	8	8	8	6	6	5	7	8	5	7	7	6	8	8	7	5	7	8	7	6	6	6	8	8	8	годен
22	5	5	8	6	6	6	7	7	7	5	7	6	6	5	8	7	7	6	6	6	5	9	6	7	8	6	отсев
23	8	8	8	9	9	7	8	8	8	9	9	9	8	8	6	8	7	9	9	8	8	8	9	8	7	7	годен
24	8	9	9	7	9	9	9	9	6	8	8	8	7	7	7	9	7	7	7	7	9	7	5	6	7	7	годен
25	7	3	3	6	6	4	7	4	4	7	7	5	8	5	5	4	5	8	5	5	6	6	6	7	7	5	отсев
26	5	6	4	4	4	6	6	7	5	7	7	7	5	8	8	6	6	5	8	6	8	6	8	8	8	6	годен
27	6	6	8	8	5	8	5	5	6	6	7	6	8	6	6	6	7	8	5	6	7	8	7	6	8	6	отсев
28	4	7	7	6	6	5	7	6	6	6	7	4	6	6	6	7	7	7	6	4	7	7	7	4	4	6	отсев
29	6	6	6	8	7	8	8	6	5	8	8	9	9	8	7	9	8	8	8	8	9	6	6	6	6	9	годен
30	9	8	6	8	6	6	8	8	7	7	7	5	8	8	8	8	7	7	7	8	8	5	5	5	8	8	годен
31	7	7	7	6	5	7	5	7	5	5	5	6	5	6	7	5	7	8	6	5	7	8	6	7	5	7	отсев
32	8	9	9	8	8	8	6	9	9	9	9	8	6	8	8	9	6	6	7	7	9	6	8	8	6	8	годен
33	3	3	5	3	6	6	3	6	5	4	5	6	3	5	3	6	6	6	5	5	4	3	3	6	6	6	отсев
34	7	7	7	6	6	6	6	6	6	6	7	6	7	5	7	6	6	7	7	7	5	7	7	6	6	7	годен
35	7	4	6	6	4	4	7	7	8	4	6	6	4	5	5	7	7	7	8	8	8	9	7	7	7	7	годен
36	8	7	7	5	5	7	7	7	6	6	7	7	5	6	6	6	7	6	6	5	8	7	4	3	7	7	отсев
37	3	8	8	8	9	6	8	7	8	9	7	7	7	9	9	6	6	7	7	7	9	9	6	6	4	9	годен
38	9	6	6	6	5	6	6	6	6	5	8	6	6	5	8	3	9	5	5	6	5	7	7	5	7	7	отсев
39	9	7	3	7	4	8	8	7	3	7	7	6	9	6	7	5	7	6	7	4	6	6	6	5	7	5	отсев
40	7	7	7	9	5	4	7	7	7	5	8	6	6	6	6	5	5	6	6	6	7	7	3	5	7	5	отсев
41	7	9	9	5	8	6	6	6	7	7	7	9	6	8	8	8	4	8	8	5	8	6	6	6	6	6	годен
42	8	7	7	9	7	7	6	3	7	6	8	3	8	5	8	6	6	6	6	5	8	7	5	7	5	7	отсев
43	9	9	8	7	4	5	9	5	7	5	8	5	6	6	6	6	8	3	7	6	5	6	8	6	5	5	отсев
44	9	6	6	6	5	7	7	7	9	9	9	9	7	9	4	8	8	6	6	6	9	7	7	7	7	7	годен
45	4	5	3	7	5	7	6	5	3	7	7	7	5	5	8	5	8	8	6	6	7	6	5	4	5	5	отсев
46	7	7	6	6	5	4	7	7	8	6	6	8	8	5	7	7	7	6	6	8	8	6	8	8	8	8	годен
47	9	6	6	8	4	8	8	5	6	6	5	5	6	6	6	6	6	3	6	7	8	7	7	5	5	5	отсев
48	6	6	8	8	7	7	7	8	8	6	6	6	9	7	8	8	8	6	8	8	8	3	6	9	9	9	годен
49	6	9	9	7	7	7	8	9	3	8	7	8	8	8	9	7	8	7	7	6	8	6	9	7	9	8	годен
50	8	8	9	7	8	9	8	8	8	6	7	8	6	7	6	8	8	5	8	7	7	5	9	9	6	8	годен

Компетенция	К1	К2	К2	К2	К2	К2	К3	К3	К3	К4	К5	К5	К5	К5	К5	К5	К6	К6	К6	К7	К7	К7	К7	К7	К7	Результат проверки
51	5	7	7	8	4	8	9	7	6	7	9	9	9	9	4	6	6	7	9	7	9	8	9	7	9	7	годен
52	7	8	8	8	7	5	6	5	5	7	8	5	8	9	9	7	4	8	8	8	6	7	7	5	8	7	годен
53	6	7	7	5	5	7	8	9	9	9	7	7	7	8	3	8	7	8	8	6	6	5	8	6	5	5	годен
54	3	5	6	7	4	7	6	8	5	6	8	5	7	7	8	6	6	8	6	7	6	5	5	4	8	6	отсев
55	2	4	6	5	5	5	6	8	5	6	7	7	6	6	6	5	8	8	5	5	6	8	7	6	7	5	отсев
56	5	6	6	6	6	7	5	7	5	5	6	5	5	6	8	6	6	6	8	3	7	6	8	6	7	6	отсев
57	4	5	6	6	7	4	5	6	4	5	7	7	7	6	5	7	8	5	8	6	7	5	8	5	7	7	годен
58	3	4	4	4	5	8	6	8	6	5	6	6	7	7	5	5	7	7	5	6	7	7	8	6	8	5	отсев
59	4	5	5	5	4	4	5	6	4	6	9	9	9	8	4	7	7	7	3	9	8	8	8	6	8	8	годен
60	6	5	5	6	7	8	9	8	7	6	6	7	9	9	7	9	8	8	6	6	8	8	9	9	7	7	годен
61	4	5	5	4	3	5	7	8	6	6	7	3	8	7	8	6	6	6	5	7	7	7	8	5	8	6	отсев
62	6	7	7	8	5	8	7	7	5	6	7	6	8	7	8	5	3	7	7	7	6	6	6	6	8	7	отсев
63	9	9	7	7	6	7	5	7	4	6	6	7	7	5	7	6	7	6	5	8	8	7	5	7	7	6	годен
64	6	7	7	5	4	5	7	6	5	6	6	5	6	5	5	5	5	8	6	7	6	8	5	6	3	6	отсев
65	3	3	5	5	4	7	6	8	6	6	6	7	7	5	7	6	6	6	6	5	7	7	8	5	8	6	отсев
66	8	7	8	6	6	5	5	6	4	4	7	5	8	5	8	5	8	7	7	6	4	6	4	6	6	6	отсев
67	4	4	3	5	5	7	7	7	6	5	7	6	7	7	4	6	8	8	6	5	7	5	8	6	8	5	отсев
68	5	6	6	6	6	5	5	7	7	7	5	5	6	7	8	7	8	6	3	6	7	6	6	5	5	7	отсев
69	7	7	5	5	4	7	6	8	9	9	9	8	8	5	5	9	5	5	8	8	5	6	6	7	8	9	годен
70	9	9	8	8	8	9	9	8	8	9	9	7	7	7	8	8	8	6	9	9	8	6	8	7	8	7	годен
71	3	3	5	5	4	7	6	7	6	6	6	6	6	6	5	6	6	7	5	5	7	7	5	6	5	7	отсев
72	4	4	6	6	6	4	4	3	6	8	8	9	7	8	8	6	8	8	8	8	5	7	7	9	7	8	годен
73	9	9	9	6	6	8	8	8	4	5	8	6	6	6	5	9	7	7	8	6	9	6	6	3	9	9	годен
74	5	5	4	6	6	6	7	8	9	9	7	7	8	8	7	8	5	6	8	8	7	7	8	9	7	7	годен
75	9	5	7	5	6	7	7	9	6	5	7	6	7	6	7	5	7	6	3	6	6	5	6	7	5	7	отсев
76	7	7	6	6	8	8	7	7	7	8	8	9	6	6	6	6	5	9	7	7	8	7	6	8	8	8	годен
77	4	4	4	5	6	6	6	4	5	5	7	7	9	7	7	7	5	5	6	6	8	5	7	6	8	7	отсев
78	5	5	4	3	5	7	5	8	5	5	9	7	7	6	8	6	8	7	7	6	6	6	6	6	8	5	отсев
79	6	6	5	5	4	7	7	8	8	8	8	9	9	9	7	6	9	7	7	9	7	7	7	4	9	9	годен
80	5	6	6	8	6	7	8	8	6	7	5	8	8	5	6	8	4	8	5	6	6	5	8	7	7	7	годен

Компетенция	К1	К2	К2	К2	К2	К2	К3	К3	К3	К4	К5	К5	К5	К5	К5	К5	К6	К6	К6	К7	К7	К7	К7	К7	К7	Результат проверки
81	5	6	6	8	5	5	6	9	6	6	8	6	5	5	3	5	8	8	6	7	6	8	6	6	6	отсев
82	7	7	8	8	9	9	9	7	6	6	8	8	8	9	7	7	8	6	6	9	7	7	9	7	6	годен
83	4	7	7	9	9	6	6	4	3	4	9	9	4	6	7	8	8	8	6	6	6	5	4	6	5	годен
84	6	6	7	8	9	8	7	8	7	9	9	7	8	7	7	7	8	8	9	6	6	8	7	7	7	годен
85	9	9	8	7	8	7	8	9	9	9	8	8	8	9	7	7	3	6	6	8	8	8	9	9	7	годен
86	5	6	5	7	6	8	6	8	8	8	6	6	9	9	7	5	8	8	7	7	7	8	8	6	6	годен
87	3	3	5	6	4	5	3	3	7	5	7	5	5	6	7	6	9	5	6	3	6	6	8	7	5	отсев
88	8	8	6	6	8	7	9	9	7	9	9	7	7	7	7	9	7	4	8	7	7	9	7	7	7	годен
89	5	7	7	7	8	6	9	9	7	7	8	8	8	7	7	8	5	6	6	7	9	7	8	8	9	годен
90	7	7	7	7	9	9	9	8	8	8	8	6	6	6	6	6	9	5	8	7	3	8	5	7	7	годен
91	5	5	5	8	6	5	5	6	5	6	8	4	9	3	7	6	6	8	5	6	6	7	7	6	8	отсев
92	5	8	8	9	9	8	9	7	7	7	8	7	7	7	9	4	7	8	8	9	7	6	8	8	9	годен
93	4	6	6	7	5	5	4	4	3	3	8	7	6	6	6	7	8	8	6	5	7	7	7	3	8	отсев
94	4	6	5	5	6	4	5	5	7	6	8	7	7	7	9	7	7	7	8	8	7	6	6	8	7	годен
95	8	7	8	7	8	8	9	8	7	9	6	6	6	5	7	8	7	6	5	8	6	7	8	9	7	годен
96	5	7	7	7	5	7	5	6	7	9	9	8	9	9	8	3	9	9	8	7	7	9	8	8	9	годен
97	9	9	8	7	9	9	6	7	9	9	8	6	8	8	6	6	8	9	7	7	8	7	5	6	7	годен
98	8	8	7	7	9	9	5	9	7	7	8	8	8	5	7	7	9	7	7	6	8	9	8	5	8	годен
99	4	7	7	6	4	4	6	5	5	7	7	8	8	8	7	7	8	6	8	8	7	7	6	6	7	годен
100	8	9	8	9	7	5	8	8	8	8	8	7	7	5	8	8	6	6	6	6	3	9	9	7	7	годен
101	8	5	5	5	8	9	9	9	7	7	8	8	9	6	6	9	7	7	6	8	9	7	6	8	6	годен
102	3	3	6	6	3	4	7	8	5	5	8	9	6	6	7	7	7	5	5	7	7	7	5	6	5	отсев
103	6	6	8	8	6	8	9	9	9	9	8	8	8	7	8	7	8	9	8	8	6	8	7	7	7	годен
104	7	7	8	6	6	8	9	6	8	8	7	7	7	5	6	6	6	5	9	9	5	7	7	9	8	годен

Г.2 Программа MATLAB

```
% Solve a Pattern Recognition Problem with a Neural Network
% Script generated by Neural Pattern Recognition app
% Created 13-Dec-2019 11:04:01
%
% This script assumes these variables are defined:
%
%   Input – input data.
%   Target – target data.

X = Input';
t = Target';

% Choose a Training Function
% For a list of all training functions type: help nntrain
% 'trainlm' is usually fastest.
% 'trainbr' takes longer but may be better for challenging problems.
% 'trainscg' uses less memory. Suitable in low memory situations.
trainFcn = 'trainscg';  % Scaled conjugate gradient backpropagation.

% Create a Pattern Recognition Network
hiddenLayerSize = 10;
net = patternnet(hiddenLayerSize, trainFcn);

% Choose Input and Output Pre/Post-Processing Functions
% For a list of all processing functions type: help nnprocess
net.input.processFcns = {'removeconstantrows','mapminmax'};

% Setup Division of Data for Training, Validation, Testing
% For a list of all data division functions type: help nndivision
net.divideFcn = 'dividerand';  % Divide data randomly
net.divideMode = 'sample';  % Divide up every sample
net.divideParam.trainRatio = 70/100;
net.divideParam.valRatio = 15/100;
```

```
net.divideParam.testRatio = 15/100;

% Choose a Performance Function
% For a list of all performance functions type: help 33enism33ormance
net.performFcn = ‘crossentropy’;  % Cross-Entropy

% Choose Plot Functions
% For a list of all plot functions type: help nnplot
net.plotFcns = {‘plotperform’,’plottrainstate’,’ploterrhist’, …
‘  'plotconfus’on‘, 'plot’oc'};

% Train the Network
[net,tr] = train(net,x,t);

% Test the Network
y = net(x);
e = gsubtract(t,y);
performance = perform(net,t,y)
tind = vec2ind(t);
yind = vec2ind(y);
percentErrors = sum(tind ~= yind)/numel(tind);

% Recalculate Training, Validation and Test Performance
trainTargets = t .* tr.trainMask{1};
valTargets = t .* tr.valMask{1};
testTargets = t .* tr.testMask{1};
trainPerformance = perform(net,trainTargets,y)
valPerformance = perform(net,valTargets,y)
testPerformance = perform(net,testTargets,y)

% View the Network
view(net)

% Plots
% Uncomment these lines to enable various plots.
```

```
%figure, plotperform(tr)
%figure, plottrainstate(tr)
%figure, ploterrhist(e)
%figure, plotconfusion(t,y)
%figure, plotroc(t,y)

% Deployment
% Change the (false) values to (true) to enable the following code blocks.
% See the help for each generation function for more information.
if (false)
   % Generate MATLAB function for neural network for application
   % deployment in MATLAB scripts or with MATLAB Compiler and Builder
   % tools, or simply to examine the calculations your trained neural
   % network performs.
   genFunction(n’t,'myNeuralNetworkFunct’on');
   y = myNeuralNetworkFunction(x);
end
if (false)
   % Generate a matrix-only MATLAB function for neural network code
   % generation with MATLAB Coder tools.
   genFunction(n’t,'myNeuralNetworkFunct’o’','MatrixO’l’','’es');
   y = myNeuralNetworkFunction(x);
end
if (false)
   % Generate a Simulink diagram for simulation or deployment with.
   % Simulink Coder tools.
 34enismsim(net);
end
```

Г.3 Программа Neuronet

ОСНОВНАЯ ПРОГРАММА

```
#include <QApplication>
#include “mainwindow.h”
int main(int argc, char *argv[])
{
   Qapplication app(argc, argv);
   MainWindow mainWin;
   mainWin.resize(600,600);
   mainWin.show();
   return app.exec();
}
```

Модуль MainWindow

Описание класса

```
#include <QmainWindow>

#define prisnak 26
#define hiddenLayer 20
#define nSign 2

#define N_ew 6

struct ew {
   int epoch;
   float err;
   float* w1, * w2;
};

class MainWidget;
class Qmenu;

class MainWindow : public QmainWindow
{
   Q_OBJECT
```

```
public:
   explicit MainWindow();
protected:
   void closeEvent(QcloseEvent *event);
signals:
   void showed();
   void calc();
   void goodbye();
private slots:
   void open();
   void calcNet();
   void viewResult();
private:
   void createActions();
   void createMenus();

   Qmenu *fileMenu;
   Qaction *openAction;
   Qaction *exitAction;
   bool isShowed;

   Qstring 36nti 36me;
   unsigned int nTrain, nValid, nTest;
   float* train;
   float* test;
   float* valid;
   int test_Ntp, test_Nfp, test_Ntn, test_Nfn;
   int train_Ntp, train_Nfp, train_Ntn, train_Nfn;
   int valid_Ntp, valid_Nfp, valid_Ntn, valid_Nfn;
   ew masew[N_ew];
   MainWidget *cWidget;
};
```

Реализация класса

```
#include «mainwindow.h»
#include “neuronet.h”
```

```
#include “mainwidget.h”
#include <QtGui>
#include <QmenuBar>
#include <QfileDialog>
#include <QmessageBox>
#include <QgridLayout>

MainWindow::MainWindow()
{
   isShowed = false;
   train = nullptr;
   test = nullptr;
   valid = nullptr;
   for (37nti  = 0; i < N_ew; i++)
   {
      masew[i].w1 = new float[prisnak * hiddenLayer];
      masew[i].w2 = new float[hiddenLayer * nSign];
      masew[i].err = 100.0;
   }
   createActions();
   createMenus();
   connect(this, SIGNAL(calc()),this,SLOT(calcNet()),Qt::UniqueConnection );
   connect(this, SIGNAL(showed()),this,SLOT(viewResult()),Qt::UniqueConnection );
}

void MainWindow::open()
{
      Qstring 37nti 37me = QfileDialog::getOpenFileName(this,
                           tr(“Open Data file”), “.”,
                           tr(“Data files (*.txt)”));
      if (!fileName.isEmpty()){
         Qvector<int> data;
         int n=0;
         Qfile lFile(37nti 37me);
         if(lFile.open(QIODevice::ReadOnly|QIODevice::Text)){
```

```
QtextStream stream(&lFile);
int j, k;
while(!stream.atEnd())
{
   for (j = 0; j < prisnak + 1; j++) {
      if(!stream.atEnd()){
      stream>>k;
      data.push_back(k);
      } else {if (j==1){n--;break;} else
         QmessageBox::warning(this, “Error”, Qstring(“Data file %1 is bad!”).arg(lFile.fileName()),
                              QmessageBox::Ok);
         return;
      }
   }
   n++;
}
unsigned int nTV = n * 0.3;
if(nTV % 2 !=0) nTV--;
nTest = nTV / 2;
nValid = nTest;
nTrain = n – nTV;
if(train!=nullptr)delete [] train;
if(test!=nullptr)delete [] test;
if(valid!=nullptr)delete [] valid;
train = new float[nTrain * (prisnak + 1)];
test = new float[nTest * (prisnak + 1)];
valid = new float[nValid * (prisnak + 1)];
n = 0;
for(unsigned 38nti =0; i<nTrain; i++){
   train[i*(prisnak + 1)]=data[n++];
   for(unsigned int j=1; j<prisnak+1; j++)
      train[i*(prisnak + 1)+j]= static_cast<float>(data[n++])/ 10.0 * 0.99 + 0.01;
}
```

```
            for(unsigned 39nti =0; i<nValid; i++){
               valid[i*(prisnak + 1)]=data[n++];
               for(unsigned int j=1; j<prisnak+1; j++)
                  valid[i*(prisnak + 1)+j]= static_cast<float>(data[n++])/ 10.0 * 0.99 +
0.01;
            }
            for(unsigned 39nti =0; i<nTest; i++){
               test[i*(prisnak + 1)]=data[n++];
               for(unsigned int j=1; j<prisnak+1; j++)
                  test[i*(prisnak + 1)+j]=static_cast<float>(data[n++])/ 10.0 * 0.99 + 0.01;
            }
            data.resize(0);
            lFile.close();
            emit calc();
         }
         else
            QmessageBox::warning(this, “Error”, Qstring(“Could not open file %1 for
reading”).arg(lFile.fileName()),                    QmessageBox::Ok);
      }
}

void MainWindow::closeEvent(QcloseEvent *event)
{
    event->accept();
}

void MainWindow::createActions()
{
   openAction = new Qaction(tr(“&Open...”), this);
   openAction->setShortcut(QkeySequence::Open);
   openAction->setStatusTip(tr(“Open an existing spreadsheet file”));
   connect(openAction, SIGNAL(triggered()), this, SLOT(open()));

   exitAction = new Qaction(tr(“E&xit”), this);
   exitAction->setShortcut(tr(“Ctrl+Q”));
```

```
    exitAction->setStatusTip(tr("Exit the application"));
    connect(exitAction, SIGNAL(triggered()), this, SLOT(close()));
}

void MainWindow::createMenus()
{
    fileMenu = menuBar()->addMenu(tr("&File"));
    fileMenu->addAction(openAction);

    fileMenu->addSeparator();
    fileMenu->addAction(exitAction);
}

void MainWindow::calcNet()
{
    float out[nSign] = { 0.01, 0.01 };
    neuronet *N = new neuronet(3, prisnak, hiddenLayer, nSign);
    int told = 0;
    int ep = 0;
    float outp[nSign], test_err = 0.0;
    int ind[N_ew], K = 0;
    bool f = false;
    ew best_ep; best_ep.err=100.0;
    do {
        told = 0;
        train_Ntp = 0; train_Nfp = 0; train_Ntn = 0; train_Nfn = 0;
        for (unsigned 40nti  = 0; i < nTrain; i++) {
            int I = rand() % nTrain;
            out[told] = 0.01;
            told = (int)train[I * (prisnak + 1)];
            out[told] = 0.99;
            N->SetNetInputs(&train[I * (prisnak + 1) + 1]);
            N->calcOutput();
            N->calcError(out);
            N->learn();
```

```
    N->update();
    N->getOutput(outp);
    int num = 0;
    if(outp[1]>=0.65) num = 1;
    if (told == num)
       if (told == 0)train_Nfp++;
       else train_Ntp++;
    else
       if (told == 0)train_Nfn++;
       else train_Ntn++;
}
if (ep % N_ew == 0&&ep>0) {
    int Ntp = 0, Ntn = 0, Nfp = 0, Nfn = 0;
    float ERR = 0;
    for (unsigned int j = 0; j < nTest; j++) {
       int num, corrnum = (int)test[j * (prisnak + 1)];
       N->SetNetInputs(&test[j * (prisnak + 1) + 1]);
       N->calcOutput();
       N->getOutput(outp);
       float err1 = outp[corrnum] – 0.9, err2, err;
       if (corrnum == 0) err2 = outp[1] – 0.1;
       else err2 = outp[0] – 0.1;
       err = (err1 * err1 + err2 * err2) / 2;
       ERR += err;
       num = 0;
       if(outp[1]>=0.65) num = 1;
       if (corrnum == num)
          if (corrnum == 0)Nfp++;
          else Ntp++;
       else
          if (corrnum == 0)Nfn++;
          else Ntn++;
    }
    K++; if (K >= N_ew) {
       K = K% N_ew; f = true;
```

```
        }
        for (int j = 0; j < N_ew; j++) ind[j] = (K + j) % N_ew;
        masew[ind[N_ew – 1]].err = ERR / nTest;
        masew[ind[N_ew – 1]].epoch = ep;
        float*w1 = N->getWeights(1),*w2 = N->getWeights(2);
        for(42nti =0; i<prisnak*hiddenLayer; i++)
           masew[ind[N_ew – 1]].w1[i]=w1[i];
        for(42nti =0; i<hiddenLayer*nSign; i++)
           masew[ind[N_ew – 1]].w2[i]=w2[i];
        int l = 0;
        float valid_err = masew[ind[l]].err;
        for (int j = 1; j < N_ew; j++) {
           if (masew[ind[j]].err < masew[ind[l]].err) l = j;
           valid_err += masew[ind[j]].err;
        }
        if (best_ep.err > masew[ind[l]].err) {
           best_ep = masew[ind[l]];
           test_Ntp = Ntp; test_Nfp = Nfp; test_Ntn = Ntn; test_Nfn = Nfn;
        }
     }
     ++ep;
}while (N->getError() > 0.0001);
valid_Ntp=0, valid_Ntn=0, valid_Nfp=0, valid_Nfn=0;
for (unsigned int j = 0; j < nValid; j++) {
     int num, corrnum = (int)valid[j * (prisnak + 1)];
     N->SetNetInputs(&valid[j * (prisnak + 1) + 1]);
     N->calcOutput();
     N->getOutput(outp);
     int num = 0;
     if(outp[1]>=0.65) num = 1;
     if (corrnum == num)
        if (corrnum == 0)valid_Nfp++;
        else valid_Ntp++;
     else
        if (corrnum == 0)valid_Nfn++;
```

```
            else valid_Ntn++;
    }
    Qfile FD(“weights.bin”);
    if(FD.open(QIODevice::WriteOnly|QIODevice::Truncate))
    {
        QdataStream dstream(&FD);
        dstream.setVersion(QdataStream::Qt_5_12);
        for(43nti =0; i<prisnak*hiddenLayer;i++)
            dstream<<best_ep.w1[i];
        for(43nti =0; i<hiddenLayer*nSign;i++)
            dstream<<best_ep.w2[i];
        FD.close();
    }
    emit showed();
}

void MainWindow::viewResult()
{
    cWidget = new MainWidget;
    cWidget->setDataTrain({train_Nfp,train_Nfn,train_Ntn,train_Ntp});
    cWidget->setDataValid({valid_Nfp,valid_Nfn,valid_Ntn,valid_Ntp});
    cWidget->setDataTest({test_Nfp,test_Nfn,test_Ntn,test_Ntp});
    int all_Nfp = test_Nfp + valid_Nfp + train_Nfp;
    int all_Nfn = test_Nfn + valid_Nfn + train_Nfn;
    int all_Ntp = test_Ntp + valid_Ntp + train_Ntp;
    int all_Ntn = test_Ntn + valid_Ntn + train_Ntn;
    cWidget->setDataAll({all_Nfp,all_Nfn,all_Ntn,all_Ntp});
    setCentralWidget(cWidget);
}
```

Модуль neuronet

Описание класса

```
#include <cstdarg>
#include <cmath>
```

```
#include <cstdlib>
class neuronet {
   int rang;          // Число слоёв в сети
   layer** layers;   // Массив слоев сеии
   int cycle;         // Число циклов обучения сети
   double error;
public:
   neuronet() {
      rang = 0; layers = nullptr; cycle = 0; error = 1.0;
   };
   neuronet(unsigned n, unsigned n1, ...);
   ~neuronet();
   void calcOutput();
   void calcError(float* model);
   void learn();
   void update();
   void SetNetInputs(float* inps);
   void getOutput(float outp[]);
   float getError();
   float* getWeights(int _rank);
};
```

Реализация класса

```
neuronet::neuronet(unsigned n, unsigned n1, ...)
{
   unsigned num, prenum;
   va_list valist;
   rang = 0;
   layers = nullptr;
   cycle = 1;
   if (n > 0) {
      rang = n;
      layers = new layer * [rang];
      for (unsigned i = 0; i < rang; i++)
         layers[i] = nullptr;
      num = n1;
```

```
        layers[0] = new layer(num, 0);
        va_start(valist, n1);
        for (unsigned i = 1; i < rang; i++)
        {
            prenum = num;
            num = va_arg(valist, unsigned);
            layers[i] = new layer(num, prenum);
            float* inp = layers[i – 1]->getOutputs();
            layers[i]->setInputs(inp);
        }
        va_end(valist);
    }
}

neuronet::~neuronet()
{
    if (rang)
    {
        for (unsigned i = 0; i < rang; i++)
            layers[i]->~layer();
        delete[] layers;
        layers = nullptr;
    }
}

void neuronet::calcOutput()
{
    for (unsigned i = 1; i < rang-1; i++)
        layers[i]->calcOutput();
    layers[rang – 1]->SoftMax();

}

float* neuronet::getWeights(int _rank)
{
```

```
    return layers[_rank]->getWeights();
}

void neuronet::calcError(float* model)
{
    float sum = 0.0;
    unsigned neuronRang, layersRang = layers[rang – 1]->getRang();
    float* outputLayers = layers[rang – 1]->getOutputs(), * errorLayers = layers[rang – 1]-
>getErrors();
    for (unsigned i = 0; i < layersRang; i++)
    {
        errorLayers[i] = layers[rang – 1]->funcAct(outputLayers[i]) * (model[i] –
outputLayers[i]);
        sum += (model[i] – outputLayers[i]) * (model[i] – outputLayers[i]);
    }
    error = sqrt(sum / layersRang);
    float* postErrors, * weights;
    for (unsigned j = rang – 2; j > 0; j--) // по скрытым слоям
    {
        layersRang = layers[j]->getRang();
        postErrors = errorLayers;
        errorLayers = layers[j]->getErrors();
        weights = layers[j + 1]->getWeights();
        outputLayers = layers[j]->getOutputs();
        for (unsigned i = 0; i < layersRang; i++) // по нейронам
        {
            sum = 0.0;
            for (unsigned k = 0; k < layers[j + 1]->getRang(); k++)
                sum += postErrors[k] * weights[layersRang * k + i];
            errorLayers[i] = layers[j]->funcAct(outputLayers[i]) * sum;
        }
    }
}

void neuronet::learn()
```

```
{
   // По всем слоям, кроме входного
   for (int j = rang – 1; j > 0; j--)
   {
      // по нейронам
      unsigned n_rang = layers[j]->getRang();
      unsigned n_inps = layers[j]->getNumInputs();
      float* inputs = layers[j]->getInputs();
      float* outputs = layers[j]->getOutputs();
      float* errors = layers[j]->getErrors();
      float* deltas = layers[j]->getDeltas();
      for (unsigned i = 0; i < n_rang; i++)
         for (unsigned k = 0; k < n_inps; k++)
            deltas[i * n_inps + k] = E * errors[i] * inputs[k] + A * deltas[i * n_inps + k];
   }
}

void neuronet::update()
{
   for (unsigned i = 1; i < rang; i++)
      layers[i]->update();
}

// Инициализация входов сети
void neuronet::SetNetInputs(float* inp)
{
   layers[1]->setInputs(inp);
}

void neuronet::getOutput(float outp[])
{
   unsigned layerRang = layers[rang – 1]->getRang();
   float* outputs = layers[rang – 1]->getOutputs();
   for (unsigned i = 0; i < layerRang; i++)
      outp[i] = outputs[i];
```

```
}

float neuronet::getError()
{
   return error;
}
```

Модуль layer

Описание класса

```
#include <cmath>
#include <cstdlib>

class layer {
   unsigned rang;            // Число нейронов в слое
   unsigned inps;   // число входов каждого нейрона слоя
   float* weights; // массив весов нейронов слоя размером rang x inps
   float* outputs; // массив выходов нейронов слоя размером rang
   float* inputs; // указатель на выходы нейронов предыдыдущего слоя
   float* deltas; // массив изменения весов нейронов слоя размером rang x inps
   float* errors; // массив ошибок выходов нейронов слоя размером rang

public:
   layer() {
      rang = 0; inps = 0; weights = nullptr; outputs = nullptr; inputs = nullptr; deltas =
nullptr; errors = nullptr; funcAct = nullptr;
   };
   layer(unsigned nrang, unsigned ninputs);
   ~layer();
   float(*funcAct) (float); // функция активации
   void calcOutput();
   void update();
   void SoftMax();
   void setRang(unsigned nR) { rang = nR; };
   void setOutput(float* Inp);
   void setInputs(float* Inp) { inputs = Inp; };
```

```
    float* getOutputs() { return outputs; };
    float* getInputs() { return inputs; };
    float* getWeights() { return weights; };
    float* getErrors() { return errors; };
    float* getDeltas() { return deltas; };
    unsigned getRang() { return rang; };
    unsigned getNumInputs() { return inps; };
};
```

Реализация класса

```
std::random_device radm;
std::mt19937_64 mt(radm());
std::uniform_real_distribution<float> rd;


float Sigmoid(float f)
{
    return (1.0 – f) * f;
    //return (f>0)?1:0;       //ReLU
}

layer::layer(unsigned nrang, unsigned ninputs)
{
    rang = 0;
    weights = 0;
    if (nrang == 0)return;
    rang = nrang;
    inps = ninputs;
    inputs = nullptr;
    outputs = nullptr;
    if (inps) {
        outputs = new float[rang];
        funcAct = Sigmoid;
        weights = new float[rang * inps];
        deltas = new float[rang * inps];
        errors = new float[rang];
```

```
        // cicle init neurons
        float k = 1.0 / sqrt(inps);
        for (unsigned i = 0; i < rang; i++)
            for (unsigned j = 0; j < inps; j++) {
                weights[i * inps + j] = 2.0*k * rd(mt) – k;
                deltas[i * inps + j] = 0;
            }
    }
}

layer::~layer()
{
    delete[] outputs;
    outputs = nullptr;
    if (rang)
    {
        delete[] weights;
        weights = nullptr;
        delete[] deltas;
        deltas = nullptr;
        delete[] errors;
        errors = nullptr;
    }
}

void layer::calcOutput()
{
    for (unsigned i = 0; i < rang; i++) {
        float sum = 0.0;
        for (unsigned j = 0; j < inps; j++)
            sum += inputs[j] * weights[i * inps + j];
        outputs[i] = 1.0 / (1.0 + exp(-sum)); //Sigmoid
    }
}
```

```
void layer::update()
{
   for (unsigned i = 0; i < rang; i++)
      for (unsigned j = 0; j < inps; j++)
         weights[i * inps + j] += deltas[i * inps + j];
}

void layer::SoftMax()
{
   for (unsigned i = 0; i < rang; i++) {
      outputs[i] = 0.0;
      for (unsigned j = 0; j < inps; j++)
         outputs[i] += inputs[j] * weights[i * inps + j];
   }
   float sum = 0.0;
   for (unsigned int j = 0; j < rang; j++)
      sum += exp(outputs[j]);
   for (unsigned 51nti  = 0; i < rang; i++) {
      outputs[i] = exp(outputs[i]) / sum;
   }
}

void layer::setOutput(float* Inp)
{
   outputs = Inp;
}
```

Модуль MainWidget

Описание класса

```
#include <Qwidget>

class TableWidget;
```

```
class MainWidget : public Qwidget
{
public:
   explicit MainWidget(Qwidget *parent = nullptr);
   void viewResult();
   void setDataTrain(const Qvector<int> &_dataList);
   void setDataTest(const Qvector<int> &_dataList);
   void setDataValid(const Qvector<int> &_dataList);
   void setDataAll(const Qvector<int> &_dataList);
private:
   TableWidget *tw_train, *tw_valid, *tw_test, *tw_all;
};
```

Реализация класса

```
#include «mainwidget.h»
#include “tablewidget.h”
#include <QgridLayout>

MainWidget::MainWidget(Qwidget *parent) : Qwidget(parent)
{
   tw_train = new TableWidget;
   tw_valid = new TableWidget;
   tw_test = new TableWidget;
   tw_all = new TableWidget;
   tw_train->setTableName(“Training Confusion Matrix”);
   tw_valid->setTableName(“Test Confusion Matrix”);
   tw_test->setTableName(“Validation Confusion Matrix”);
   tw_all->setTableName(“All Confusion Matrix”);
   QgridLayout *gLayout = new QgridLayout;
   gLayout->addWidget(tw_train,0,0);
   gLayout->addWidget(tw_valid,1,0);
   gLayout->addWidget(tw_test,0,1);
   gLayout->addWidget(tw_all,1,1);
   setLayout(gLayout);
}
```

```
void MainWidget::viewResult()
{
}

void MainWidget::setDataTrain(const Qvector<int> &_dataList)
{
   tw_train->setDataList(_dataList);
}

void MainWidget::setDataTest(const Qvector<int> &_dataList)
{
   tw_test->setDataList(_dataList);
}

void MainWidget::setDataValid(const Qvector<int> &_dataList)
{
   tw_valid->setDataList(_dataList);
}

void MainWidget::setDataAll(const Qvector<int> &_dataList)
{
   tw_all->setDataList(_dataList);
}
```

Модуль TableWidget

Описание класса

```
#include <Qwidget>

class TableWidget :public Qwidget
{
   Q_OBJECT
public:
   explicit TableWidget(Qwidget *parent = nullptr);
   void setDataList(const Qvector<int> &_dataList);
```

```
    void setTableName(const Qstring &_name);

private:
    void createWid();
    int getSumDataList();
    Qvector<int> dataList;
    Qstring tableName;
};
```

Реализация класса

```
#include “tablewidget.h”
#include “mylabel.h”
#include <Qlabel>
#include <Qrect>
#include <QgridLayout>
#include <QVBoxLayout>


TableWidget::TableWidget(Qwidget *parent) : Qwidget(parent)
{
    dataList.resize(4);
}

void TableWidget::setDataList(const Qvector<int> &_dataList)
{
    int j = 0;
    for(auto i = _dataList.begin(); i != _dataList.end(); i++)
        dataList[j++] = *i;
    createWid();
}

void TableWidget::setTableName(const Qstring &_name)
{
    tableName = _name;
}
```

```
void TableWidget::createWid()
{
   int sump = getSumDataList();
   double pntp = (double)dataList[3]/(double)sump*100;
   double pntn = (double)dataList[2]/(double)sump*100;
   double pnfn = (double)dataList[1]/(double)sump*100;
   double pnfp = (double)dataList[0]/(double)sump*100;

   double ratio_tp = (double)dataList[3]/(double)(dataList[3]+dataList[2])*100;
   double ratio_tn = (double)dataList[2]/(double)(dataList[3]+dataList[2])*100;
   double ratio_fp = (double)dataList[0]/(double)(dataList[0]+dataList[1])*100;
   double ratio_fn = (double)dataList[1]/(double)(dataList[0]+dataList[1])*100;

   double total_pt = (double)(dataList[0]+dataList[3])/(double)sump*100;
   double total_pf = (double)(dataList[2]+dataList[1])/(double)sump*100;
   Qfont font("Times New Roman",15, Qfont::Normal);
   QfontMetrics fm(font);
   Qvector<int> tsize;
   int w = fm.width("12.88 %") + 20;
   Qstring sntp = Qstring::number(dataList[3])+"\n"+Qstring::number(pntp,'f',1)+" %";
   Qstring sntn = Qstring::number(dataList[2])+"\n"+Qstring::number(pntn,'f',1)+" %";
   Qstring snfn = Qstring::number(dataList[1])+"\n"+Qstring::number(pnfn,'f',1)+" %";
   Qstring snfp = Qstring::number(dataList[0])+"\n"+Qstring::number(pnfp,'f',1)+" %";
   Qstring sratio_t = Qstring::number(ratio_tp,'f',1)+"
%\n"+Qstring::number(ratio_tn,'f',1)+" %";
   Qstring sratio_f = Qstring::number(ratio_fp,'f',1)+" %\n"; sratio_f
+=Qstring::number(ratio_fn,'f',1)+" %";
   Qstring stotal = Qstring::number(total_pt,'f',1)+"
%\n"+Qstring::number(total_pf,'f',1)+" %";
   Qsize sML = Qsize(w,w);
   Qcolor color(180,255,180), color1(255,180,180), color2(200,200,200),
color3(225,225,225);
   Qlabel *tit = new Qlabel(tableName);
   tit->setAlignment(Qt::AlignHCenter);
   Qlabel *num20 = new Qlabel("0");
```

```
Qlabel *num21 = new Qlabel(“1”);
num20->setAlignment(Qt::AlignHCenter);
num21->setAlignment(Qt::AlignHCenter);
num20->setFont(Qfont(“Helvetica [Cronyx]”, 12));
num21->setFont(Qfont(“Helvetica [Cronyx]”, 12));
Qlabel *num00 = new Qlabel(“0 “);
Qlabel *num10 = new Qlabel(“1 “);
num00->setAlignment(Qt::AlignVCenter|Qt::AlignRight);
num10->setAlignment(Qt::AlignVCenter|Qt::AlignRight);
num00->setFont(Qfont(“Helvetica [Cronyx]”, 12));
num10->setFont(Qfont(“Helvetica [Cronyx]”, 12));
tit->setFont(Qfont(“Times New Roman”,15, Qfont::Bold));
MyLabel *lbfp = new MyLabel;
MyLabel *lbfn = new MyLabel;
MyLabel *lbtn = new MyLabel;
MyLabel *lbtp = new MyLabel;
MyLabel *lbfl21 = new MyLabel;
MyLabel *lbtr22 = new MyLabel;
MyLabel *lbfl03 = new MyLabel;
MyLabel *lbtr13 = new MyLabel;
MyLabel *lbtot = new MyLabel;
lbfp->setText(snfp);
lbfn->setText(snfn);
lbtn->setText(sntn);
lbtp->setText(sntp);
lbfl21->setText(sratio_f);
lbtr22->setText(sratio_t);
lbfl03->setText(sratio_f);
lbtr13->setText(sratio_t);
lbtot->setText(stotal);
lbfp->setSize(sML);
lbfn->setSize(sML);
lbtn->setSize(sML);
lbtp->setSize(sML);
lbfl21->setSize(sML);
```

```
lbtr22->setSize(sML);
lbfl03->setSize(sML);
lbtr13->setSize(sML);
lbtot->setSize(sML);
lbfp->setColor(color);
lbfn->setColor(color1);
lbtn->setColor(color1);
lbtp->setColor(color);
lbfl21->setColor(color3);
lbtr22->setColor(color3);
lbfl03->setColor(color3);
lbtr13->setColor(color3);
lbtot->setColor(color2);
QgridLayout *tLayout = new QgridLayout;
tLayout->setSpacing(0);
tLayout->setContentsMargins(15,15,15,15);
tLayout->addWidget(num00, 0, 0);
tLayout->addWidget(num10, 1, 0);
tLayout->addWidget(lbfp, 0, 1);
tLayout->addWidget(lbfn, 0, 2);
tLayout->addWidget(lbtn, 1, 1);
tLayout->addWidget(lbtp, 1, 2);
tLayout->addWidget(lbfl21, 2, 1);
tLayout->addWidget(lbtr22, 2, 2);

tLayout->addWidget(lbfl03, 0, 3);
tLayout->addWidget(lbtr13, 1, 3);
tLayout->addWidget(lbtot, 2, 3);

tLayout->addWidget(num20, 3, 1);
tLayout->addWidget(num21, 3, 2);

QVBoxLayout *hLayout =  new QVBoxLayout;
hLayout->addWidget(tit);
hLayout->addLayout(tLayout);
```

```
    setLayout(hLayout);
}

int TableWidget::getSumDataList()
{
    int sum = 0;
    for(auto i : dataList)
        sum+=i;
    return sum;
}
```

Модуль MyLabel

Описание класса

```
#include <QtWidgets>

class MyLabel : public Qwidget
{
    Q_OBJECT
    Qlabel *mLabel;
public:
    explicit MyLabel(Qwidget *parent = nullptr);
    void setText(const Qstring &_text);
    Qstring getText() const {return wText;};
    void setSize(Qsize &_size);
    Qsize minimumSizeHint() const;
    void setColor(Qcolor &_color);
private:
    Qstring wText;
    Qsize wSize;
    Qcolor wColor;
};
```

Реализация класса

```
#include «mylabel.h»
```

```
MyLabel::MyLabel(Qwidget *parent) : Qwidget(parent)
{
   mLabel = new Qlabel(this);
   mLabel->setFont(Qfont("Times New Roman",15, Qfont::Normal));
   mLabel->setAlignment(Qt::AlignHCenter);
   Qpalette pal;
   pal.setColor(this->backgroundRole(),Qt::yellow);
   setPalette(pal);
   setAutoFillBackground(true);

   int X = fontMetrics().width(wText)/2;
   int Y = height()/2;
   mLabel->move(X,Y);
   Qframe *frm = new Qframe;
   frm->setFrameStyle(Qframe::StyledPanel | Qframe::Plain);
   frm->setParent(this);
   frm->setFrameShape(Qframe::Box);
}

void MyLabel::setText(const Qstring &_text)
{
   wText = _text;
   mLabel->setText(wText);
}

void MyLabel::setColor(Qcolor &_color)
{
   wColor = _color;
   Qpalette pal;
   pal.setColor(this->backgroundRole(),wColor);
   setPalette(pal);
}

void MyLabel::setSize(Qsize &_size)
{
```

```
    wSize = _size;
    resize(wSize);
    int X = width()/2-fontMetrics().width(wText)/2;
    int Y = height()/3-fontMetrics().height();
    mLabel->move(X,Y);
}

Qsize MyLabel::minimumSizeHint() const
{
    return Qsize(wSize);
}
```

Г.4 Примеры матриц ошибок для различных порогов отсечения

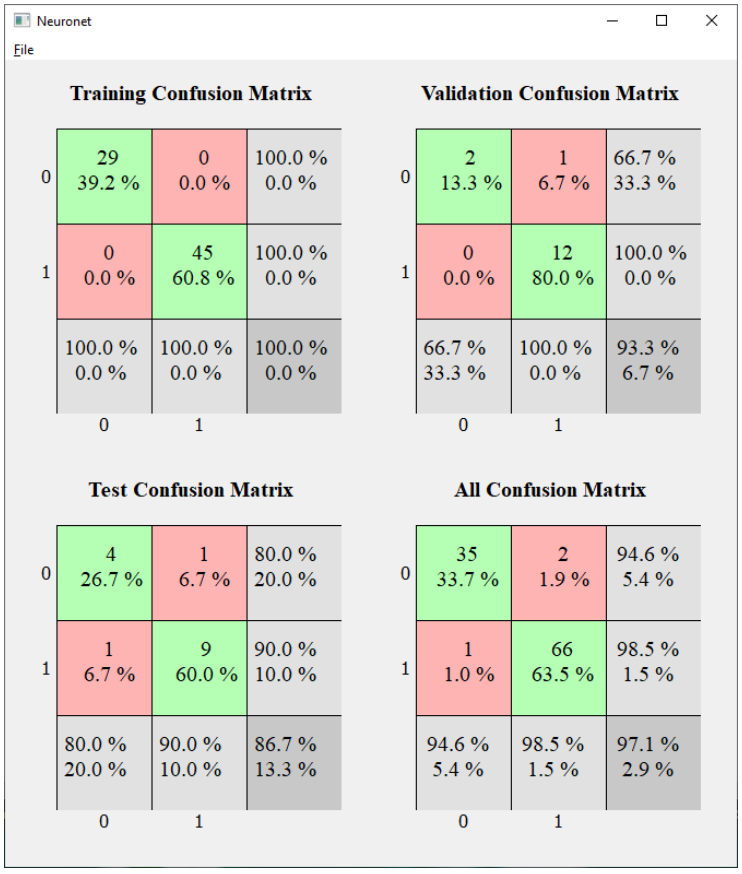


Рисунок Г.1 – Порог отсечения 0,50

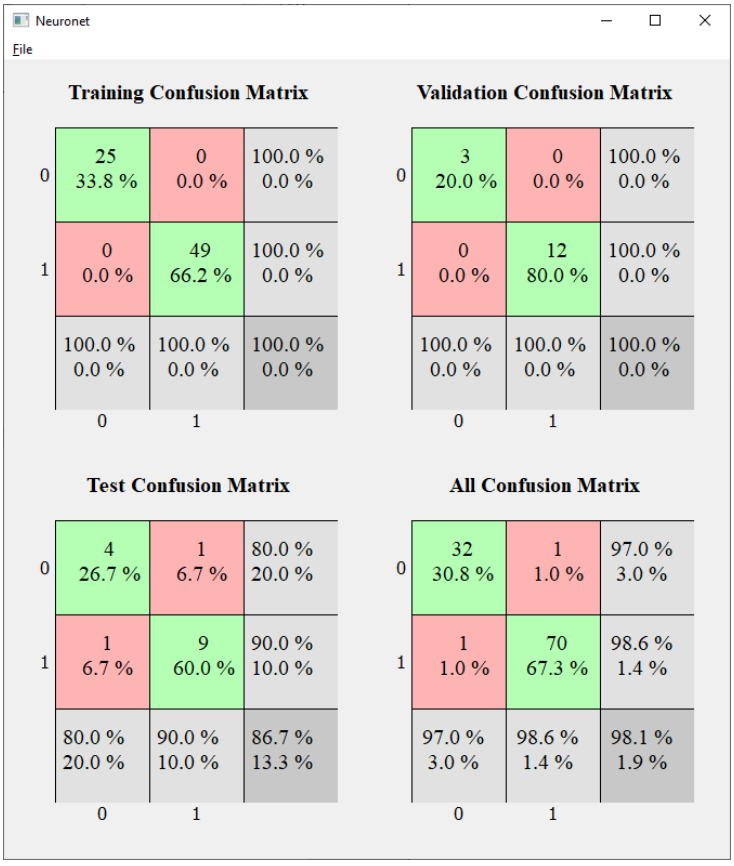


Рисунок Г.2 – Порог отсечения 0,60

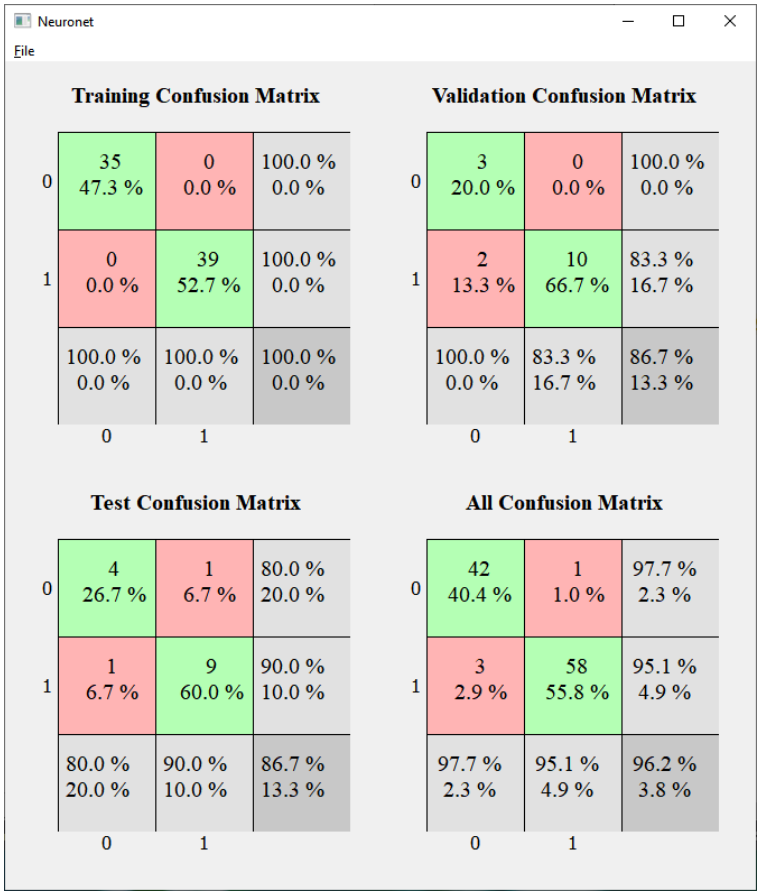


Рисунок Г.3 – Порог отсечения 0,65

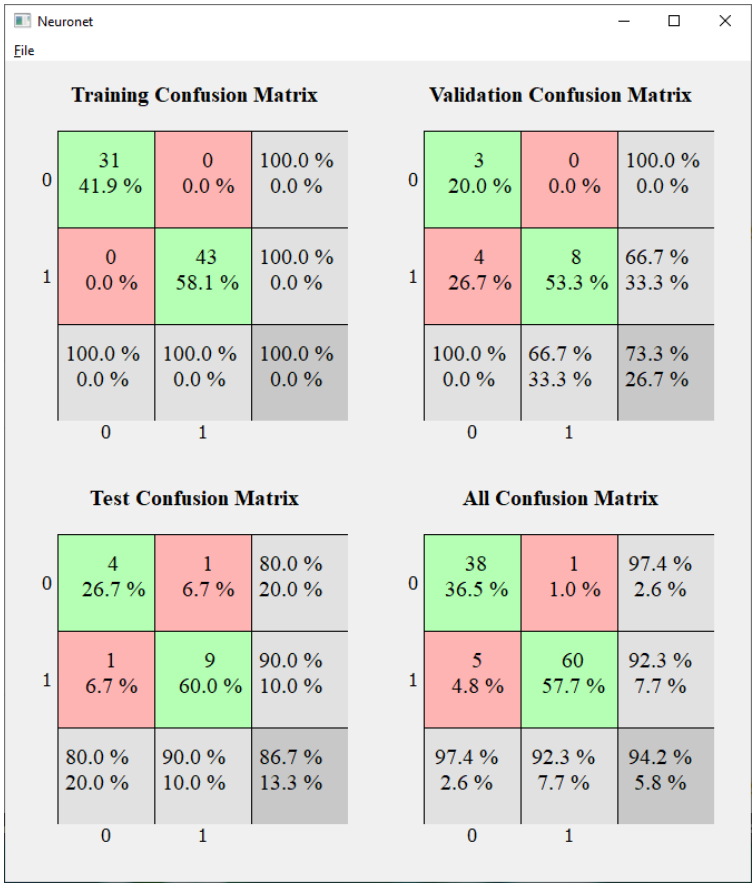


Рисунок Г.4 – Порог отсечения 0,70

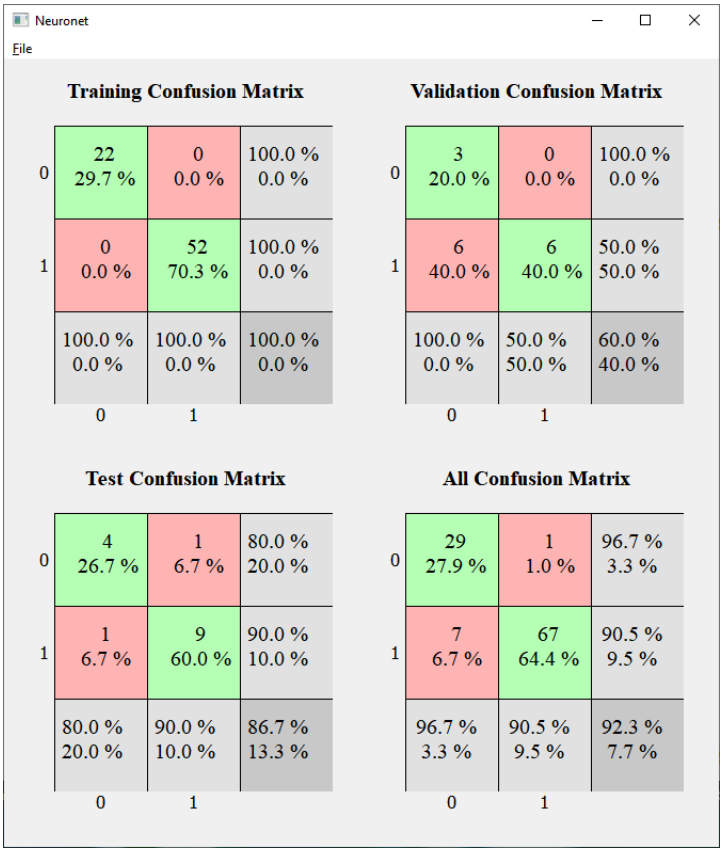


Рисунок Г.5 – Порог отсечения 0,80

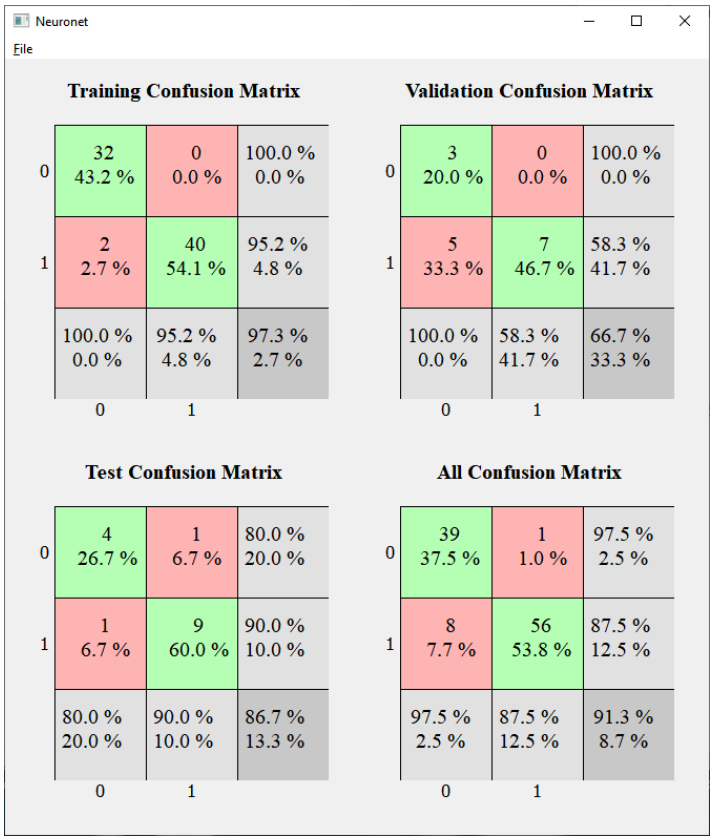


Рисунок Г.6 – Порог отсечения 0,90

Г.5 Программа Neurotest

ОСНОВНАЯ ПРОГРАММА

```
#include <QApplication>
#include <QDesktopWidget>
#include <QtSql>

#include "mainwindow.h"

static bool createConnection()
{
   QSqlDatabase db = QSqlDatabase::addDatabase("QSQLITE");
   db.setDatabaseName("answers");
   if (!db.open()) {
      qDebug() << "Не может открыть базу данных:" << db.lastError();
      return false;
   }
   return true;
}

int createFakeData()
{
   QSqlQuery query;
   query.exec("DROP TABLE answers");
   QString   str  = "CREATE TABLE answers ("
                    "id INTEGER PRIMARY KEY NOT NULL, "
                    "surname VARCHAR(20) NOT NULL, "
                    "name VARCHAR(20) NOT NULL, "
                    "patronymic VARCHAR(20) NOT NULL, "
                    "testdate VARCHAR(20) NOT NULL, "
                    "testtime VARCHAR(15) NOT NULL, "
                    "k1 INTEGER, "
                    "k2t1 INTEGER, "
                    "k2t2 INTEGER, "
                    "k2t3 INTEGER, "
                    "k2t4 INTEGER, "
```

```
                "k2t5 INTEGER, "
                "k3t1 INTEGER, "
                "k3t2 INTEGER, "
                "k3t3 INTEGER, "
                "k4 INTEGER, "
                "k5t1 INTEGER, "
                "k5t2 INTEGER, "
                "k5t3 INTEGER, "
                "k5t4 INTEGER, "
                "k5t5 INTEGER, "
                "k5t6 INTEGER, "
                "k6t1 INTEGER, "
                "k6t2 INTEGER, "
                "k6t3 INTEGER, "
                "k7t1 INTEGER, "
                "k7t2 INTEGER, "
                "k7t3 INTEGER, "
                "k7t4 INTEGER, "
                "k7t5 INTEGER, "
                "k7t6 INTEGER, "
                "k7t7 INTEGER, "
                "result VARCHAR(6) "
                 ");";

    if (!query.exec(str)) {
        qDebug() << "Невозможно создать таблицу";
        return -1;
    }
    return 0;
}

int main(int argc, char *argv[])
{
    QApplication app(argc, argv);
    bool create = !QFile::exists("answers");
```

```
    if (!createConnection())
        return 1;
    if (create)
        createFakeData();
    MainWindow mainWin;

mainWin.setWindowFlags(Qt::Window|Qt::WindowMinimizeButtonHint|Qt::Window
CloseButtonHint);
    QDesktopWidget *d = QApplication::desktop();
    qreal scl = static_cast<qreal>(d->width())/1920.0;
    mainWin.setFixedSize(1200*scl, 675*scl);
    mainWin.show();
    return app.exec();
}
```

Модуль MainWindow

Описание класса

```
#include <QMainWindow>

#define prisnak 26
#define hiddenLayer 20
#define nSign 2

class MenuButton;
class neuronet;

struct testData
{
    QString surname, name, patronymic;
    int competences[prisnak];
    QString result;
};

class MainWindow : public QMainWindow
```

```
{
    Q_OBJECT
public:
    explicit MainWindow();
protected:
    void closeEvent(QCloseEvent *event);
    void paintEvent(QPaintEvent *pEvent);
private slots:
    void about();
    void testing();
    void viewRecords();
private:
    void createMenus();
    void createActions();
    void saveRecord();

    MenuButton *pButTest;
    MenuButton *pButResult;
    MenuButton *pButExit;
    MenuButton *pButHelp;
    qreal scl;

    float *mas;
    int i, num;
    neuronet *N;
    testData* testRes;
};
```

Реализация класса

```
#include <QtGui>
#include <QtWidgets>
#include <QtSql>
#include "mainwindow.h"
#include "menubar.h"
#include "menubutton.h"
#include "mainwindow.h"
```

```
#include "neuronet.h"
#include "inputdialog.h"
#include "inputfiodialog.h"
#include "tableview.h"

float w1[26*20];
float w2[20*2];
MainWindow::MainWindow()
{
   mas = new float[prisnak]; i = 0;
   N = new neuronet(3, prisnak, hiddenLayer, nSign);
   testRes = new testData;
   QDesktopWidget *d = QApplication::desktop();
   scl = static_cast<qreal>(d->width())/1920.0;
   N->setWeightsLayer(1,w1);
   N->setWeightsLayer(2,w2);
   createMenus();
   createActions();
}

void MainWindow::paintEvent(QPaintEvent *pEvent)
{
   QPixmap p;
   if(p.load("plane.jpg")){
      QPainter lPainter;
      lPainter.begin(this);
      lPainter.scale(scl, scl);
      lPainter.drawPixmap(0,0,p);
      lPainter.end();
   }
}

void MainWindow::testing()
{
   int *m;
```

```
    InputFIODialog* pInputFIODialog = new InputFIODialog(this);
    if(pInputFIODialog->exec()==QDialog::Accepted){
        InputDialog* pInputDialog = new InputDialog(this);
        if (pInputDialog->exec() == QDialog::Accepted){
            m = pInputDialog->numMas();
            for(int j=0;j<prisnak;j++){
                mas[j]=static_cast<float>(m[j])/ 10.0 * 0.99 + 0.01;
                testRes->competences[j] = m[j];
            }
            i++;
            float outp[nSign];
            N->SetNetInputs(mas);
            N->calcOutput();
            N->getOutput(outp);
            float oMax = outp[0];
            num = 0;
            if (oMax < outp[1]) { oMax = outp[1]; num = 1; }
            QString s;
            if(num) s = "годен";
            else s = "отсев";
            testRes->result = s;

            QMessageBox::about(this,
                               tr("Итоговая оценка"),
                               QString("<h2>Итоговая оценка годности специалиста: %1
</h2>").arg(s)
                               );
            testRes->surname = pInputFIODialog->sUrname();
            testRes->name = pInputFIODialog->nAme();
            testRes->patronymic = pInputFIODialog->pAtronymic();
            saveRecord();
        }
        delete pInputDialog;
    }
    delete pInputFIODialog;
```

```
}

void MainWindow::saveRecord()
{
   QSqlTableModel *model = new QSqlTableModel(this);
   model->setTable("answers");
   model->select();
   int row = model->rowCount(), ind;
   if(row>0){
      QSqlRecord  rec = model->record(row-1);
      ind = rec.value("id").toInt()+1;
   }
   else ind = row+1;
   QDate d = QDate::currentDate();
   QTime t = QTime::currentTime();
   QString sDate = d.toString(Qt::SystemLocaleLongDate);
   QString sTime = t.toString(Qt::SystemLocaleLongDate);
   model->insertRows(row,1);
   model->setData(model->index(row,0),ind);
   model->setData(model->index(row,1),testRes->surname);
   model->setData(model->index(row,2),testRes->name);
   model->setData(model->index(row,3),testRes->patronymic);
   model->setData(model->index(row,4),sDate);
   model->setData(model->index(row,5),sTime);
   for(int j=0;j<prisnak;j++)
      model->setData(model->index(row,j+6),testRes->competences[j]);
   model->setData(model->index(row,32),testRes->result);
   if(!model->submitAll())
   {
      qDebug()<<"Ошибка помещения данных в базу";
   }
   delete model;
}

void MainWindow::viewRecords()
```

```
{
    TableView* tv = new TableView;
    tv->exec();
    delete tv;
}

void MainWindow::createMenus()
{
    pButTest = new MenuButton(tr("&Тест"));
    pButTest->setShortcut(tr("Ctrl+T"));
    pButTest->setStatusTip(tr("Начало тестирования компетенций"));
    pButResult = new MenuButton(tr("&Результаты"));
    pButResult->setShortcut(tr("Ctrl+P"));
    pButResult->setStatusTip(tr("Отображает результаты проверок компетенций"));
    pButHelp = new MenuButton(tr("&Помощь"));
    pButHelp->setShortcut(tr("Ctrl+П"));
    pButHelp->setStatusTip(tr("Отображает информационное окно О приложении"));
    pButExit = new MenuButton(tr("&Выход"));
    pButExit->setShortcut(tr("Ctrl+B"));
    pButExit->setStatusTip(tr("Выход из приложения"));

    MenuBar *pMBar = new MenuBar(this);

    pMBar->addItem(pButTest);
    pMBar->addItem(pButResult);
    pMBar->addItem(pButHelp);
    pMBar->addItem(pButExit);
    pMBar->addItem(nullptr);
    setMenuWidget(pMBar);
}

void MainWindow::createActions()
{
    connect(pButTest, SIGNAL(clicked()), this, SLOT(testing()));
    connect(pButResult, SIGNAL(clicked()), this, SLOT(viewRecords()));
```

```
    connect(pButExit, SIGNAL(clicked()), this, SLOT(close()));
    connect(pButHelp, SIGNAL(clicked()), this, SLOT(about()));
}

void MainWindow::closeEvent(QCloseEvent *event)
{
     event->accept();
}

void MainWindow::about()
{
    QMessageBox::about(this, tr("О программе Neurotest"),
        tr("<h2>Программа Neurotest</h2>"
          "<p>Copyright &copy; 2020 Компьютерные технологии, "
          "Пензенский государственный университет"
          "<p>Программа Neurotest предназначена для нейросетевой оценки "
          "уровня готовности персонала транспортной безопасности "
          "к выполнению задач профессиональной деятельности. "
          ""));
}
```

Модуль neuronet

Описание класса

```
#include <cmath>
#include <cstdlib>
#include <cstdarg>
class neuronet {
    int rang;           // Число слоёв в сети
    layer** layers;   // Массив слоев сеии
    int cycle;          // Число циклов обучения сети
    double error;
public:
    neuronet() {
        rang = 0; layers = nullptr; cycle = 0; error = 1.0;
```

```
    };
    neuronet(unsigned n, unsigned n1, ...);
    ~neuronet();
    void calcOutput();
    void SetNetInputs(float* inps);
    void setWeightsLayer(int lay, float* w);
    void getOutput(float outp[]);
};
```

Реализация класса

```
neuronet::neuronet(unsigned n, unsigned n1, ...)
{
    unsigned num, prenum;
    va_list valist;
    rang = 0;
    layers = nullptr;
    cycle = 1;
    if (n > 0) {
        rang = n;
        layers = new layer * [rang];
        for (int i = 0; i < rang; i++)
            layers[i] = nullptr;
        num = n1;
        layers[0] = new layer(num, 0);
        va_start(valist, n1);
        for (int i = 1; i < rang; i++)
        {
            prenum = num;
            num = va_arg(valist, unsigned);
            layers[i] = new layer(num, prenum);
            float* inp = layers[i - 1]->getOutputs();
            layers[i]->setInputs(inp);
        }
        va_end(valist);
    }
}
```

```
neuronet::~neuronet()
{
   if (rang)
   {
      for (int i = 0; i < rang; i++)
         layers[i]->~layer();
      delete[] layers;
      layers = nullptr;
   }
}

void neuronet::calcOutput()
{
   for (int i = 1; i < rang; i++)
      layers[i]->calcOutput();
   layers[rang - 1]->SoftMax();

}

// Инициализация входов сети
void neuronet::SetNetInputs(float* inp)
{
   layers[1]->setInputs(inp);
}

void neuronet::setWeightsLayer(int lay, float* w)
{
   layers[lay]->setWeights(w);
}

void neuronet::getOutput(float outp[])
{
   unsigned layerRang = layers[rang - 1]->getRang();
   float* outputs = layers[rang - 1]->getOutputs();
```

```
    for (unsigned i = 0; i < layerRang; i++)
        outp[i] = outputs[i];
}
```

Модуль layer

Описание класса

```
#include <cmath>
#include <cstdlib>

class layer {
    unsigned rang;              // Число нейронов в слое
    unsigned inps;   // число входов каждого нейрона слоя
    float* weights; // массив весов нейронов слоя размером rang x inps
    float* outputs; // массив выходов нейронов слоя размером rang
    float* inputs; // указатель на выходы нейронов предыдыдущего слоя
    float* errors; // массив ошибок выходов нейронов слоя размером rang

public:
    layer() {
        rang = 0; inps = 0; weights = nullptr; outputs = nullptr; inputs = nullptr; errors =
nullptr; funcAct = nullptr;
    };
    layer(unsigned nrang, unsigned ninputs);
    ~layer();
    float(*funcAct) (float); // функция активации
    void SoftMax();
    void calcOutput();
    void setRang(unsigned nR) { rang = nR; };
    void setOutput(float* Inp);
    void setInputs(float* Inp) { inputs = Inp; };
    void setWeights(float* w);
    float* getOutputs() { return outputs; };
    float* getInputs() { return inputs; };
    float* getWeights() { return weights; };
```

```
    float* getErrors() { return errors; };
    unsigned getRang() { return rang; };
    unsigned getNumInputs() { return inps; };
};
```

Реализация класса

```
layer::layer(unsigned nrang, unsigned ninputs)
{
    rang = 0;
    weights = 0;
    if (nrang == 0)return;
    rang = nrang;
    inps = ninputs;
    inputs = nullptr;
    outputs = nullptr;
    if (inps) {
        outputs = new float[rang];
        funcAct = Sigmoid;
        weights = new float[rang * inps];
        errors = new float[rang];
    }
}

layer::~layer()
{
    delete[] outputs;
    outputs = nullptr;
    if (rang)
    {
        delete[] weights;
        weights = nullptr;
        delete[] errors;
        errors = nullptr;
    }
}
```

```
void layer::calcOutput()
{
   for (unsigned i = 0; i < rang; i++) {
      float sum = 0.0;
      for (unsigned j = 0; j < inps; j++)
         sum += inputs[j] * weights[i * inps + j];
      outputs[i] = 1.0 / (1.0 + exp(-sum)); //Sigmoid
   }
}


void layer::SoftMax()
{
   for (unsigned i = 0; i < rang; i++) {
      outputs[i] = 0.0;
      for (unsigned j = 0; j < inps; j++)
         outputs[i] += inputs[j] * weights[i * inps + j];
   }
   float sum = 0.0;
   for (unsigned int j = 0; j < rang; j++)
      sum += exp(outputs[j]);
   for (unsigned int i = 0; i < rang; i++) {
      outputs[i] = exp(outputs[i]) / sum;
   }
}

void layer::setOutput(float* Inp)
{
   outputs = Inp;
}

void layer::setWeights(float* w)
{
   for(unsigned int i=0; i<rang*inps; i++)
      weights[i]=w[i];
```

```
}
```

Модуль *InputFioDialog*

Описание класса

```
#include <QDialog>

class CustmSLineEdit;

class InputFIODialog : public QDialog
{
   Q_OBJECT
public:
   InputFIODialog(QWidget* pwgt = 0);
   QString sUrname() const;
   QString nAme () const;
   QString pAtronymic () const;
public slots:
   void slotButtonActive();
   void slotButtonDeactive();
private:
   CustmSLineEdit* pSurname;
   CustmSLineEdit* pName;
   CustmSLineEdit* pPatronymic;
   QList<CustmSLineEdit*> lines;
   QPushButton* pcmdOk;
};
```

Реализация класса

```
#include <QtWidgets>
#include "inputfiodialog.h"
#include "custmslineedit.h"
#include "counter.h"

InputFIODialog::InputFIODialog(QWidget* pwgt/*= 0*/)
   : QDialog(pwgt, Qt::WindowTitleHint | Qt::WindowSystemMenuHint)
```

```
{
   setWindowTitle("Ввод личных данных");
   pSurname = new CustmSLineEdit;
   pName  = new CustmSLineEdit;
   pPatronymic  = new CustmSLineEdit;

   QLabel* plblSurname    = new QLabel("&Фамилия");
   QLabel* plblName     = new QLabel("&Имя");
   QLabel* plblPatronymic     = new QLabel("&Отчество");
   lines.push_back(pSurname);
   lines.push_back(pName);
   lines.push_back(pPatronymic);
   plblSurname->setBuddy(pSurname);
   plblName->setBuddy(pName);
   plblPatronymic->setBuddy(pPatronymic);
   Counter *c = new Counter(3);
   pcmdOk     = new QPushButton("&Ok");
   QPushButton* pcmdCancel = new QPushButton("&Cancel");
   pcmdOk->setEnabled(false);
   for(auto l=lines.begin();l!=lines.end();l++)
   {
      if(*l!=lines.last())
         connect(*l,&CustmSLineEdit::jumpForward,                    *(l+1),
&CustmSLineEdit::jumpIn);
      if(*l!=lines.first())
      connect(*l,&CustmSLineEdit::jumpBackward, *(l-1), &CustmSLineEdit::jumpIn);
      connect(*l, SIGNAL(textChanded()), c, SLOT(slotInc()));
      connect(*l, SIGNAL(textDeleted()), c, SLOT(slotDec()));
   }
   connect(lines.last(),&CustmSLineEdit::jumpForward,                lines.first(),
&CustmSLineEdit::jumpIn);
   connect(lines.first(),&CustmSLineEdit::jumpBackward,                lines.last(),
&CustmSLineEdit::jumpIn);
   connect(pcmdOk, SIGNAL(clicked()), SLOT(accept()));
   connect(pcmdCancel, SIGNAL(clicked()), SLOT(reject()));
```

```
    connect(c, SIGNAL(sigActive()), this, SLOT(slotButtonActive()));
    connect(c, SIGNAL(sigDeactive()), this, SLOT(slotButtonDeactive()));
    QGridLayout* ptopLayout = new QGridLayout;
    ptopLayout->addWidget(plblSurname, 0, 0);
    ptopLayout->addWidget(plblName, 1, 0);
    ptopLayout->addWidget(plblPatronymic, 2, 0);
    ptopLayout->addWidget(pSurname, 0, 1);
    ptopLayout->addWidget(pName, 1, 1);
    ptopLayout->addWidget(pPatronymic, 2, 1);
    ptopLayout->addWidget(pcmdOk, 3,0);
    ptopLayout->addWidget(pcmdCancel, 3, 1);
    setLayout(ptopLayout);
}

QString InputFIODialog::sUrname() const
{
    return pSurname->text();
}

QString InputFIODialog::nAme() const
{
    return pName->text();
}

QString InputFIODialog::pAtronymic() const
{
    return pPatronymic->text();
}

void InputFIODialog::slotButtonActive()
{
    pcmdOk->setEnabled(true);
}

void InputFIODialog::slotButtonDeactive()
```

```
{
   pcmdOk->setEnabled(false);
}
```

Модуль *CustmSLineEdit*

Описание класса

```
#include <QtWidgets>

class CustmSLineEdit : public QLineEdit
{
   Q_OBJECT
public:
   explicit CustmSLineEdit(const QString & contents = "", QWidget *parent = nullptr);
   ~CustmSLineEdit() {};
signals:
   void jumpForward();
   void jumpBackward();
   void textChanded();
   void textDeleted();
public slots:
   void jumpIn();
protected:
   virtual void focusInEvent(QFocusEvent *event);
   virtual void keyPressEvent(QKeyEvent * event);
   virtual void mouseReleaseEvent(QMouseEvent *event);

private:
   bool selectOnMouseRelease;
};
```

Реализация класса

```
#include "custmslineedit.h"

CustmSLineEdit::CustmSLineEdit(const QString & contents, QWidget *parent):
```

```
    QLineEdit(contents, parent), selectOnMouseRelease(false)
{
    setValidator(new QRegExpValidator(QRegExp("[А-Я][а-я]{1,15}"), this));
}
void CustmSLineEdit::jumpIn()
{
    setFocus();

    selectOnMouseRelease = false;
    selectAll();
}

void CustmSLineEdit::focusInEvent(QFocusEvent *event)
{
    QLineEdit::focusInEvent(event);
    selectOnMouseRelease = true;
}

void CustmSLineEdit::keyPressEvent(QKeyEvent * event)
{
    int key = event->key();
    int cursorPos = cursorPosition();

if (cursorPos == 0)
    if((key==Qt::Key_Left) || (key==Qt::Key_Right))
    {
        event->accept();
        return;
    }

    // удаление текста с помощью Backspace
    if (cursorPos < 3)
        if (key == Qt::Key_Backspace) {
            if(text().length()<3)
                emit textDeleted();
```

```
        // return;
    }

    // удаление текста с помощью Delete
    if (key == Qt::Key_Delete){
        if(hasSelectedText()&&((text().length()-selectedText().length())<3))
            emit textDeleted();
        else
            if(text().length()<3)
                emit textDeleted();
        }

    // переход на строку ниже с помощью right arrow
    if (cursorPos > 0)
        if (key == Qt::Key_Down) {
            emit jumpForward();
            event->accept();
            return;
    }

    if (cursorPos > 0)
    if (key == Qt::Key_Up) {
        emit jumpBackward();
        event->accept();
        return;
    }

    // после отпусканя клавиши переход курсора в новую позицию
    QLineEdit::keyPressEvent(event);
    int freshCurPos = cursorPosition();
    if (freshCurPos == 2) emit textChanded();
}

void CustmSLineEdit::mouseReleaseEvent(QMouseEvent *event)
{
```

```
    if(!selectOnMouseRelease)
        return;

    selectOnMouseRelease = false;
    selectAll();

    QLineEdit::mouseReleaseEvent(event);
}
```

Модуль *InputDialog*

Описание класса

```
#define prisnak 26

#include <QDialog>
#include <QtSql>

class CustomLineEdit;
class QLineEdit;

class InputDialog : public QDialog
{
    Q_OBJECT
public:
    explicit InputDialog(QWidget* pwgt = nullptr);
    int *numMas() const;
public slots:
    void slotButtonActive();
private:
    QList<CustomLineEdit*> lines;
    int *numbers;
    QPushButton* pcmdOk;
};
```

Реализация класса

```
#include "inputdialog.h"
#include "customlineedit.h"
#include "counter.h"

QVector<QString> s = {"Правовые и нормативные акты по обеспечению ТБ",
                      "Основные понятия, цель и основы обеспечения ТБ",
                      "Состояние ТБ в ГА. Административно-организационные аспекты",
                      "Полномочия, роль и обязанности работников подразделения ТБ",
                      "Система управления обеспечением ТБ",
                      "Обеспечение ТБ при наземном обслуживании ВС",
                      "Организация пропускного и внутриобъектового режимов",
                      "Конфигурация аэропорта и охраняемые зоны ограниченного доступа",
                      "Меры ТБ в пределах контролируемой и неконтролируемой зоны. Контроль доступа к ВС",
                      "Технические средства и оборудование",
                      "Предметы и вещества, запрещенные и (или) ограниченные к перемещению в контролируемую зону",
                      "Организация досмотра персонала, посетителей и ТС",
                      "Правила проведения предполетного и послеполетного досмотров",
                      "Досмотр пассажиров с использованием ТС. Контактный метод досмотра",
                      "Досмотр багажа и ручной клади с помощью рентгено - телевизионной системы безопасности",
                      "Метод наблюдения и опроса (профайлинг)",
                      "Общие сведения о терроризме и АНВ. Общие сведения о ВУ, ВВ, оружие и боеприпасах",
                      "Угрозы в деятельности ГА. Характеристики нарушителей. Психология поведения нарушителей",
                      "Особенности кризисных ситуаций. Определение степени серьезности происшествия",
                      "Порядок действия САБ в нестандартных ситуациях",
                      "Программа противодействия АНВ",
                      "Меры охраны и защиты ВС на земле. Порядок проведения досмотра ВС на земле",
```

```
                "Контроль за выполнением технологических процессов обеспечения ТБ",
                "Управление кризисными ситуациями. Навыки решения конфликтных ситуаций",
                "Методы проведения аудиторских и инспекционных проверок",
                "Нормы, правила и процедуры обеспечения ТБ"};

//  методы класса InputDialog

InputDialog::InputDialog(QWidget* pwgt): QDialog(pwgt, Qt::WindowTitleHint | Qt::WindowSystemMenuHint)
{
   setWindowTitle("Ввод данных");
   QList<QLabel*> nums;
   for (int i=0;i<prisnak;i++){
      lines.push_back(new CustomLineEdit);
      nums.push_back(new QLabel(s[i]));
   }
   pcmdOk     = new QPushButton("&Ok");
   QPushButton* pcmdCancel = new QPushButton("&Cancel");
   Counter *c = new Counter(prisnak);
   pcmdOk->setEnabled(false);
   connect(pcmdOk, SIGNAL(clicked()), SLOT(accept()));
   connect(pcmdCancel, SIGNAL(clicked()), SLOT(reject()));

   //Layout setup

   QGridLayout* ptopLayout = new QGridLayout;
   auto k = 0;
   auto nm=nums.begin();
   for(auto l=lines.begin();l!=lines.end();l++)
   {
      ptopLayout->addWidget(*(nm++), k, 0);
      ptopLayout->addWidget(*l, k++, 1);
      if(*l!=lines.last())
```

```
            connect(*l,&CustomLineEdit::jumpForward,                    *(l+1),
&CustomLineEdit::jumpIn);
        if(*l!=lines.first())
            connect(*l,&CustomLineEdit::jumpBackward,                    *(l-1),
&CustomLineEdit::jumpIn);
        connect(*l, SIGNAL(editingFinished()), c, SLOT(slotInc()));
    }
    connect(lines.last(),&CustomLineEdit::jumpForward,                  lines.first(),
&CustomLineEdit::jumpIn);
    connect(lines.first(),&CustomLineEdit::jumpBackward,                 lines.last(),
&CustomLineEdit::jumpIn);
    connect(c, SIGNAL(sigActive()), this, SLOT(slotButtonActive()));
    QHBoxLayout *hLayout = new QHBoxLayout;
    hLayout->addStretch(1);
    hLayout->addWidget(pcmdOk);
    hLayout->addWidget(pcmdCancel);
    QVBoxLayout *vLayout = new QVBoxLayout;
    vLayout->addLayout(ptopLayout);
    vLayout->addLayout(hLayout);
    setLayout(vLayout);
    numbers = new int[prisnak];
}

int *InputDialog::numMas() const
{

    int i=0;
    for(auto l=lines.begin();l!=lines.end();l++ )
    {
        CustomLineEdit* L= *l;
        numbers[i++]=L->text().toInt();
    }
    return numbers;
}
```

```
void InputDialog::slotButtonActive()
{
   pcmdOk->setEnabled(true);
}
```

Модуль *CustomLineEdit*

Описание класса

```
#include <QtWidgets>

class CustomLineEdit : public QLineEdit
{
   Q_OBJECT
public:
   explicit CustomLineEdit(const QString & contents = "", QWidget *parent = nullptr);
   virtual ~CustomLineEdit() {};
signals:
   void jumpForward();
   void jumpBackward();
public slots:
   void jumpIn();
protected:
   virtual void focusInEvent(QFocusEvent *event);
   virtual void keyPressEvent(QKeyEvent * event);
   virtual void mouseReleaseEvent(QMouseEvent *event);

private:
   bool selectOnMouseRelease;
};
```

Реализация класса

```
#include "customlineedit.h"

CustomLineEdit::CustomLineEdit(const QString & contents, QWidget *parent) :
   QLineEdit(contents, parent), selectOnMouseRelease(false)
{
```

```
    setValidator(new QIntValidator(0, 9, this));
    setInputMask("9");
}

void CustomLineEdit::jumpIn()
{
    setFocus();

    selectOnMouseRelease = false;
    selectAll();
}

void CustomLineEdit::focusInEvent(QFocusEvent *event)
{
    QLineEdit::focusInEvent(event);
    selectOnMouseRelease = true;
}

void CustomLineEdit::keyPressEvent(QKeyEvent * event)
{
    int key = event->key();

    if((key==Qt::Key_Left) || (key==Qt::Key_Right))
    {
        event->accept();
        return;
    }

    // переход на следующую строку после нажатия клавиши Space
    if (key == Qt::Key_Space) {
        emit jumpForward();
        event->accept();
        return;
    }
```

```
    // переход на следующую строку после нажатия клавиши right arrow
    if (key == Qt::Key_Down) {
        emit jumpForward();
        event->accept();
        return;
    }

    if (key == Qt::Key_Up) {
        emit jumpBackward();
        event->accept();
        return;
    }

    // после отпусканя клавиши переход курсора в новую позицию
    QLineEdit::keyPressEvent(event);

    if ( (key != Qt::Key_Down) && (key != Qt::Key_Up))
        emit jumpForward();
}

void CustomLineEdit::mouseReleaseEvent(QMouseEvent *event)
{
    if(!selectOnMouseRelease)
        return;

    selectOnMouseRelease = false;
    selectAll();

    QLineEdit::mouseReleaseEvent(event);
}
```

Модуль *Counter*

Описание класса

```
#include <QObject>
```

```
#include <QLinkedList>

class Counter : public QObject
{
   Q_OBJECT
private:
   int m_nValue, m_Limit;
   QLinkedList<QObject*> pObj;
public:
   Counter(int Limit);
public slots:
   void slotInc();
   void slotDec();

signals:
   void sigActive();
   void sigDeactive();

};
```

Реализация класса

```
Counter::Counter(int Limit) : QObject()
                , m_nValue(0)
{
   m_Limit = Limit;
}

void Counter::slotInc()
{
   int i=0;
   for(auto P=pObj.begin();P!=pObj.end();P++)
      if(*P==sender()) break;
      else i++;
   if(i==pObj.size()){
      pObj.append(sender());
      ++m_nValue;
```

```
    }

    if (m_nValue == m_Limit)
        emit sigActive();
}

void Counter::slotDec()
{
    if(pObj.removeOne(sender()))
    {
        if (m_nValue == m_Limit)
            emit sigDeactive();
        --m_nValue;
    }
}
```

Модуль *TableView*

Описание класса

```
#include <QtWidgets>
class QSqlTableModel;
class QTableView;

enum {
    Answers_Id = 0,
    Answers_Surname = 1,
    Answers_Name = 2,
    Answers_Patronymic = 3,
    Answers_Date = 4,
    Answers_Time = 5,
    Answers_Result = 32
};

class TableView : public QDialog
{
```

```
    Q_OBJECT
public:
    explicit TableView(QWidget* pwgt = nullptr);
    public slots:
    void viewRecord();
   void handleTableClick(const QModelIndex&);
    void deleteRecord();
private:
    QSqlTableModel *model;
    QTableView *view;
};
```

Реализация класса

```
include <QtGui>
#include <QtSql>
#include "tableview.h"
#include "inputdialog.h"

TableView::TableView(QWidget* pwgt) : QDialog(pwgt, Qt::WindowTitleHint |
Qt::WindowSystemMenuHint)
{
    model = new QSqlTableModel(this);
    model->setTable("answers");
    model->select();
    model->setEditStrategy(QSqlTableModel::OnFieldChange);

    model->setSort(Answers_Surname, Qt::AscendingOrder);
    model->select();
    model->setHeaderData(Answers_Surname, Qt::Horizontal, tr("Фамилия"));
    model->setHeaderData(Answers_Name, Qt::Horizontal, tr("Имя"));
    model->setHeaderData(Answers_Patronymic, Qt::Horizontal, tr("Отчество"));
    model->setHeaderData(Answers_Date, Qt::Horizontal, tr("Дата"));
    model->setHeaderData(Answers_Time, Qt::Horizontal, tr("Время"));
    model->setHeaderData(Answers_Result, Qt::Horizontal, tr("Оценка"));
    view = new QTableView;
    view->setModel(model);
```

```
    view->setSelectionMode(QAbstractItemView::SingleSelection);
    view->setSelectionBehavior(QAbstractItemView::SelectRows);
    view->setColumnHidden(0, true);

    for(int i=6; i<32;i++)
        view->setColumnHidden(i, true);

    QHeaderView *header = view->horizontalHeader();
    header->setStretchLastSection(true);
    header->setFont(QFont("Times New Roman",12, QFont::Bold));
    QPushButton *buttonView = new QPushButton(tr("Просмотр"));
    QPushButton *buttonDelete = new QPushButton(tr("Удалить"));
    QPushButton *buttonOk = new QPushButton(tr("Ok"));
    QHBoxLayout *hLayout = new QHBoxLayout;
    hLayout->addWidget(buttonView);
    hLayout->addWidget(buttonDelete);
    hLayout->addStretch(1);
    hLayout->addWidget(buttonOk);
    QVBoxLayout *mainLayout = new QVBoxLayout;
    mainLayout->addWidget(view);
    mainLayout->addLayout(hLayout);
    setLayout(mainLayout);
    connect(view, SIGNAL(doubleClicked(QModelIndex)), this,
SLOT(handleTableClick(QModelIndex)));
    connect(buttonOk, SIGNAL(clicked()), SLOT(accept()));
    connect(buttonView, SIGNAL(clicked()), this, SLOT(viewRecord()));
    connect(buttonDelete, SIGNAL(clicked()), this, SLOT(deleteRecord()));
    setWindowTitle(tr("Результаты проверки компетенций"));
    QDesktopWidget *d = QApplication::desktop();
    qreal scl = static_cast<qreal>(d->width())/1920.0;
    QFont font("Times New Roman",12, QFont::Normal);
    QFontMetrics fm(font);
    view->setFont(font);
    view->setColumnWidth(1,fm.width("Qwertyuiopasdfghjklz"));
    view->setColumnWidth(2,fm.width("Qwertyuiopasdfghjklz"));
```

```
    view->setColumnWidth(3,fm.width("Qwertyuiopasdfghjklz"));
    view->setColumnWidth(4,fm.width("qwertyuiopasdfghjklzxc"));
    view->setColumnWidth(5,fm.width("qwertyuiopa"));
    view->setEditTriggers(QAbstractItemView::NoEditTriggers);
    int w =(fm.width("Qwertyuiopasdfghjklz") + 20*scl)*4 +
fm.width("qwertyuiopasd")+fm.width("успех")+50*scl;
    setFixedWidth(w);
}

void TableView::viewRecord()
{
    QModelIndex qml = view->currentIndex();
    int row = qml.row();
    QSqlRecord rec = model->record(row);
    ViewInfo *vi = new ViewInfo(rec);
    vi->exec();
    delete vi;

}

void TableView::handleTableClick(const QModelIndex& idx)
{
    int row = idx.row();
    QSqlRecord rec = model->record(row);
    ViewInfo *vi = new ViewInfo(rec);
    vi->exec();
    delete vi;
}

void TableView::deleteRecord()
{
    QMessageBox* pmbx = new QMessageBox(QMessageBox::Information,
            "MessageBox",
            "<b>Удалить запись?</b>",
            QMessageBox::Yes | QMessageBox::No | QMessageBox::Cancel
```

```
            );
    int n = pmbx->exec();
    delete pmbx;
    if(n==QMessageBox::Yes){
        QModelIndex qml = view->currentIndex();
        int row = qml.row();
        model->removeRow(row);
        model->submitAll();
        view->hideRow(row);
    }
}
```

Модуль *ViewInfo*

Описание класса

```
class ViewInfo : public QDialog
{
    Q_OBJECT
public:
    explicit ViewInfo(const QSqlRecord rec, QWidget* pwgt = 0);
private:
    QSqlRecord rec;
    QPushButton* butOk;
};
```

Реализация класса

```
ViewInfo::ViewInfo(const QSqlRecord _rec, QWidget* pwgt) :
    QDialog(pwgt, Qt::WindowTitleHint | Qt::WindowSystemMenuHint)
{
    setWindowTitle("Информация");
    rec = _rec;
    butOk = new QPushButton("Ok");
    connect(butOk, SIGNAL(clicked()), SLOT(accept()));
    QLabel *lText = new QLabel("<p><b>Фамилия:</b> "
                        + rec.value("surname").toString()
                        + "<br><b>Имя:</b> "
```

```
+ rec.value("name").toString()
+ "<br><b>Отчество:</b> "
+ rec.value("patronymic").toString()
+ "</p><p><b>Дата:</b> "
+ rec.value("testdate").toString()
+ "<br><b>Время:</b> "
+ rec.value("testtime").toString()
+ "</p><p><b>Правовые и нормативные акты по обеспечению ТБ:</b> "
+ rec.value("k1").toString()
+ "<br><b>Основные понятия, цель и основы обеспечения ТБ:</b> "
+ rec.value("k2t1").toString()
+ "<br><b>Состояние ТБ в ГА. Административно-организационные аспекты:</b> "
+ rec.value("k2t2").toString()
+ "<br><b>Полномочия, роль и обязанности работников САБ:</b> "
+ rec.value("k2t3").toString()
+ "<br><b>Система управления обеспечением ТБ:</b> "
+ rec.value("k2t4").toString()
+ "<br><b>Обеспечение ТБ при наземном обслуживании ВС:</b> "
+ rec.value("k2t5").toString()
+ "<br><b>Организация пропускного и внутриобъектового режимов:</b> "
+ rec.value("k3t1").toString()
+ "<br><b>Конфигурация аэропорта и охраняемые зоны ограниченного доступа:</b> "
+ rec.value("k3t2").toString()
+ "<br><b>Меры ТБ в пределах контролируемой и неконтролируемой зоны. Контроль доступа к ВС:</b> "
+ rec.value("k3t3").toString()
+ "<br><b>Технические средства и оборудование:</b> "
+ rec.value("k4").toString()
```

```
+ "<br><b>Предметы и вещества, запрещенные и (или) ограниченные к перемещению в контролируемую зону:</b> "
+ rec.value("k5t1").toString()
+ "<br><b>Организация досмотра персонала, посетителей и ТС:</b> "
+ rec.value("k5t2").toString()
+ "<br><b>Правила проведения предполетного и послеполетного досмотров:</b> "
+ rec.value("k5t3").toString()
+ "<br><b>Досмотр пассажиров с использованием ТС. Контактный метод досмотра:</b> "
+ rec.value("k5t4").toString()
+ "<br><b>Досмотр багажа и ручной клади с помощью рентгено - телевизионной системы безопасности:</b> "
+ rec.value("k5t5").toString()
+ "<br><b>Метод наблюдения и опроса (профайлинг):</b> "
+ rec.value("k5t6").toString()
+ "<br><b>Общие сведения о терроризме и АНВ. Общие сведения о ВУ, ВВ, оружие и боеприпасах:</b> "
+ rec.value("k6t1").toString()
+ "<br><b>Угрозы в деятельности ГА. Характеристики нарушителей. Психология поведения нарушителей:</b> "
+ rec.value("k6t2").toString()
+ "<br><b>Особенности кризисных ситуаций. Определение степени серьезности происшествия:</b> "
+ rec.value("k6t3").toString()
+ "<br><b>Порядок действия САБ в нестандартных ситуациях:</b> "
+ rec.value("k7t1").toString()
+ "<br><b>Программа противодействия АНВ:</b> "
+ rec.value("k7t2").toString()
+ "<br><b>Меры охраны и защиты ВС на земле. Порядок проведения досмотра ВС на земле:</b> "
+ rec.value("k7t3").toString()
```

```
                + "<br><b>Контроль за выполнением технологических процессов обеспечения ТБ:</b> "
                + rec.value("k7t4").toString()
                + "<br><b>Управление кризисными ситуациями. Навыки решения конфликтных ситуаций:</b> "
                + rec.value("k7t5").toString()
                + "<br><b>Методы проведения аудиторских и инспекционных проверок:</b> "
                + rec.value("k7t6").toString()
                + "<br><b>Нормы, правила и процедуры обеспечения ТБ:</b> "
                + rec.value("k7t7").toString()
                + "</p><b>Итоговая оценка годности специалиста:</b><i> "
                + rec.value("result").toString());
    QHBoxLayout* phLayout = new QHBoxLayout;
    phLayout->addStretch(1);
    phLayout->addWidget(butOk);
    QVBoxLayout* pvLayout = new QVBoxLayout;
    pvLayout->addWidget(lText);
    pvLayout->addLayout(phLayout);
    setLayout(pvLayout);
}
```

Модуль *MenuBar*

Описание класса

```
#include <QWidget>

class MenuButton;
class QHBoxLayout;

class MenuBar : public QWidget
{
    Q_OBJECT
public:
    explicit MenuBar(QWidget* pwgt = nullptr);
```

```
    ~MenuBar() {};
    void addItem(MenuButton* pwgt);
private:
    QHBoxLayout *pHLayout;
};
```

Реализация класса

```
#include <QtWidgets>
#include "menubar.h"
#include "menubutton.h"

MenuBar::MenuBar(QWidget *parent) : QWidget(parent)
{
    setBackgroundRole(QPalette::Base);
    setAutoFillBackground(true);
    pHLayout = new QHBoxLayout;
}

void MenuBar::addItem(MenuButton* pwgt)
{
    if(pwgt == nullptr) {
        pHLayout->addStretch(5);
        pHLayout->setMargin(0);
        pHLayout->setSpacing(-1);
        setLayout(pHLayout);
    }
    else
    {
        pwgt->setBackgroundRole(QPalette::Base);
        pwgt->setAutoFillBackground(true);
        pHLayout->addWidget(pwgt);
    }
}
```

Модуль *MenuBar*

Описание класса

```
#include <QtWidgets>
class MenuButton : public QPushButton
{
   Q_OBJECT
public:
   explicit MenuButton(const QString &text, QWidget *parent = nullptr);
   ~MenuButton(){};
protected:
   virtual void enterEvent(QEvent *event);
   virtual void leaveEvent(QEvent *event);
};
```

Реализация класса

```
MenuButton::MenuButton(const QString &text, QWidget *parent)
   : QPushButton(text, parent)
{
   setFlat(true);
}
void MenuButton::enterEvent(QEvent *event)
{
   QColor color(230,245,255);
   QPalette pal;
   pal.setColor(this->backgroundRole(),color);
   setPalette(pal);
   QPushButton::enterEvent(event);
}
void MenuButton::leaveEvent(QEvent *event)
{
   QPalette pal;
   pal.setColor(this->backgroundRole(),Qt::white);
   setPalette(pal);
   QPushButton::leaveEvent(event);
}
```