Федеральное государственное бюджетное образовательное учреждение
высшего образования «Оренбургский государственный университет»

На правах рукописи

Костин Владимир Николаевич

МЕТОДИКИ, МОДЕЛИ И МЕТОДЫ ОБОСНОВАНИЯ И РАЗРАБОТКИ СИСТЕМ ФИЗИЧЕСКОЙ ЗАЩИТЫ КРИТИЧЕСКИ ВАЖНЫХ ОЪЕКТОВ

Специальность 05.13.01 – Системный анализ, управление и обработка информации (в науке и технике)

Диссертация на соискание ученой степени
доктора технических наук

Научный консультант:
Боровский Александр Сергеевич
доктор технических наук, доцент

Оренбург 2021

Оглавление

Введение

Актуальность темы исследования. В последнее десятилетие в связи с нарастающими угрозами международного терроризма намечается интенсивное развитие систем физической защиты (СФЗ) критически важных объектов (КВО). Согласно ГОСТ Р 22.2.06-2016 критически важный объект – объект, нарушение или прекращение функционирования которого приведет к потере управления экономикой Российской Федерации, субъекта Российской Федерации или административно-территориальной единицы субъекта Российской Федерации, ее необратимому негативному изменению (разрушению) либо существенному снижению безопасности жизнедеятельности населения [1]. В соответствии с действующими руководящими документами ФСТЭК под критически важным объектом понимают объект, оказывающий существенное влияние на национальную безопасность Российской Федерации, прекращение или нарушение функционирования которого приводит к чрезвычайной ситуации [2].

Согласно федеральному закону РФ 68 – ФЗ от 21.12.1994 к КВО относятся [3]:

1. Ядерно и/или радиационно опасные объекты: атомные электростанции; радиохимические заводы; хранилища ядерного топлива, пункты размещения ядерного оружия и материалов, организации, имеющие ядерные установки.

2. Химически опасные объекты: предприятия химической, нефтехимической и нефтеперерабатывающей промышленности; заводы и склады химического оружия; объекты водоснабжения; хранилища сжиженных токсичных газов.

3. Биологически опасные объекты: предприятия, производящие или использующие возбудителей особо опасных инфекций или инфекционных заболеваний.

4. Техногенно опасные объекты: тепловые и гидроэлектрические электростанции; центры управления работой ЕЭС; аэропорты; информационные вычислительные центры управления транспортом; морские грузовые и рыбные порты;

метрополитены; предприятия ракетно-космического и авиационного комплекса; плотины крупных водохранилищ.

5. Пожаровзрывоопасные объекты: нефтеперерабатывающие и газоперерабатывающие заводы; нефтяные, газовые скважины и нефтеналивные терминалы; хранилища нефти и токсичных газов; титаниево-магниевые заводы; места хранения вооружения и взрывчатых веществ; газгольдерные, кислородные станции; магистральные газо- и нефтепродуктопроводы.

6. Объекты государственного управления, информационной и телекоммуникационной инфраструктуры: предприятия по добыче, переработке и хранению драгоценных металлов, камней и полиграфической продукции; «пункты государственного, военного управления; организации мониторинга окружающей среды; учреждения, обладающие уникальными научными образцами, информацией или оборудованием; организации телерадиовещания» [3]; архивы федерального уровня; комбинаты государственных резервов.

Главной особенностью современных КВО является наличие ключевой системы информационной инфраструктуры (КСИИ) – «информационно-управляющей или информационно-телекоммуникационной системы (ИУС, ИТС), которая осуществляет управление КВО или осуществляет информационное обеспечение управления КВО, а также наличие специализированных автоматизированных систем управления (АСУ) производственными и технологическими процессами. Важность этих процессов и последствия нарушения их функционирования на КВО выдвигают в разряд первоочередных задач обеспечения их защиты от дестабилизирующих факторов, как внутренних, так и внешних» [5].

Решением Совета безопасности Российской Федерации от 08.11.2005 определен перечень КВО, в состав которых могут входить КСИИ: «системы органов государственной власти; системы органов управления правоохранительных структур; системы финансово-кредитной и банковской деятельности; системы предупреждения и ликвидации чрезвычайных ситуаций (ЧС); географические и навигационные системы; сети связи общего пользования на участках без резервных видов связи; системы специального назначения; спутниковые системы для

обеспечения органов управления и в специальных целях; системы управления добычей и транспортировкой нефти, нефтепродуктов и газа; программно-технические комплексы центров управления взаимоувязанной сетью связи; системы управления водоснабжением и энергоснабжением; системы управления транспортом (наземным, воздушным, морским); системы управления потенциально опасными объектами» [4]. В федеральном законе ФЗ 187 от 26.06.17 г. введен термин «значимые объекты критической информационной инфраструктуры (КИИ)» [7].

Указом Президента РФ от 07.07.2011 № 899 «Об утверждении приоритетных направлений развития науки, технологий и техники в Российской Федерации и перечня критических технологий Российской Федерации» подчеркивается важность этой проблемы, в котором одними из приоритетных направлений развития науки определены безопасность и противодействие терроризму, а технологии обеспечения защиты и жизнедеятельности населения и опасных объектов при угрозах террористических проявлений включены в перечень критических технологий [12]. Это выдвигает задачу обеспечения безопасности КВО в разряд первоочередных.

Актуальность данной темы также подтверждается постановлением правительства № 875 от 29.08.2014 «Об антитеррористической защищенности объектов ФСТЭК …», где сказано, что обеспечение антитеррористической защищенности – реализация совокупности проектных решений, организационно-технических и специальных мероприятий, направленных на обеспечение безопасности работников, объектов, зданий (сооружений) организаций ФСТЭК России с целью предотвращения совершения террористического акта и (или) минимизации его последствий, которые обеспечивает СФЗ, а именно совокупность сил охраны организации ФСТЭК России, вооружения и специальных средств, организационных, административных и правовых мер, в том числе инженерно-техническая укрепленность объектов (территории) организации ФСТЭК, направленных на предотвращение и пресечение совершения террористических актов и иных несанкционированных действий в отношении организации ФСТЭК России [2, 6, 7]; а также Ука-

зом Президента РФ от 05.12.2016 № 646 «О принятии новой доктрины информационной безопасности», где сказано, что различные террористические и экстремистские организации используют новые механизмы воздействия на объекты критической информационной инфраструктуры [13].

Защита КВО должна осуществляться за счет реализуемых механизмов контроля и управления доступа к объектам защиты. Ошибки разработчиков систем безопасности для КВО могут привести к возникновению ЧС при несанкционированном проникновении злоумышленников. Поэтому в последнее время намечается интенсивное развитие СФЗ, которые обеспечивают антикриминальную, антитеррористическую, информационную, ядерную и другие виды безопасности КВО [15].

Следовательно, особую важность приобретают аспекты, касающиеся разработки и создания систем физической защиты КВО и организации их эффективной работы. В условиях возрастающих требований к обеспечению безопасности КВО решение задачи повышения эффективности и рентабельности проектных решений разработки (совершенствования средств анализа) СФЗ становится все более актуальным. Дорогостоящий и сложный процесс проектирования СФЗ предъявляет высокие требования к проектным решениям, особенно к принятым на начальных стадиях разработки проекта. Теоретические основы содержания этапов технологии проектирования СФЗ сложны и, несмотря на интенсивные исследования, далеки от совершенства.

Степень разработанности темы исследования. Вопросами исследования проблем обоснования и разработки СФЗ занимались многие зарубежные и отечественные ученые. В работе автора М. Гарсия «Проектирование и оценка систем физической защиты» рассмотрены теоретические подходы к проектированию, анализу и оценке эффективности СФЗ в целом, так и ее отдельных подсистем [16]. В ее работе «Оценка уязвимости систем физической защиты» рассмотрена методика оценки уязвимости объектов, описаны вопросы разработки моделей угроз и оценки эффективности СФЗ [17].

Среди зарубежных работ необходимо отметить автора Джеймса Ф. Бродера «Анализ риска и исследование безопасности», «в которой приводится общая математическая модель оценки безопасности и пример аналитических формул количественной оценки рисков. Выполнен обширный обзор возможных ЧС и планирования действий при их возникновении» [18].

Из отечественных работ, основной является монография А. В. Бояринцева, А. Н. Бражника, А. Г. Зуева «Проблемы антитерроризма: Категорирование и анализ уязвимости объектов», в которой рассматривается методология оценки уязвимости и категорирования объектов, и на этой основе предлагается методика обоснования требований к СФЗ [20]. В монографии изложены вопросы оценки и анализа эффективности СФЗ, проведен сравнительный анализ и классификация как отечественных, так и зарубежных программных средств оценки эффективности СФЗ.

Ю. А. Оленин в работе «Системы и средства управления физической защитой объектов» рассмотрел методику разработки инженерно-технических средств СФЗ, на основе системного подхода предложил пути повышения эффективности управления СФЗ, описал методы графоаналитической формализации процедур повышения эффективности управления СФЗ, в основе которого лежит формируемая средствами обнаружения и системой контроля и управления доступом сигнальная информация [41].

В монографии И. Д. Моторного, Г. Е. Шепитько, в работах В. Г. Синилова, Р. Г. Магауенова исследуются вопросы повышения эффективности охранной сигнализации, разработки систем и средств управления защиты от хищений для нережимных объектов. Кроме того, В. Г. Синилов, Р. Г. Магауенов разработали вопросы организации защиты объектов с помощью инженерно-технических средств охраны (ИТСО), описали «основные положения организации защиты объектов, принципы построения комплексов охраны объектов, классифицировали технические средства и варианты их применения» [21].

Необходимо отметить научные труды Я. Д. Вишнякова «Общая теория рисков», Н. Н. Радаева, В. В. Лесных, А. В. Бочкова «Методические аспекты задания

требований оценки и обеспечения защищенности объектов газовой отрасли от противоправных действий», В. А. Акимова, В. В. Лесных, Н. Н. Радаева «Риски в природе, техносфере, обществе и экономике», В.В. Волхонского «Модели и методы формирования и оценки эффективности функционирования комплексов средств физической защиты». В работах данных авторов «рассматриваются новые теоретические и практические подходы к обоснованию и разработке СФЗ для различных категорий объектов. В исследованиях Э. И. Абалмазова нашли свое отражение вопросы интегральной оценки эффективности СФЗ. В научных изысканиях А. М. Омельянчука предложены методы оптимизации СФЗ на основе метода матрицы угроз» [21]. В трудах Е. Т. Мишина, Е. Е. Соколова, А. В. Измайлова рассматриваются принципы построения СФЗ и характеристики технических средств защиты.

Несмотря на это, средства разработки, анализа и оптимизации СФЗ в настоящее время остаются мало исследованы. Основная проблема состоит в том, что СФЗ – это конфликтная система с антагонистическими отношениями, которая динамично развивается, поэтому в процесс ее исследований вносится неопределенность. Отсутствие устоявшейся терминологии (понятий), аппарата исследований и системы критериев эффективности, а также многовариантность построения СФЗ приводят к возрастанию влияния субъективных факторов при принятии проектных решений. Помимо этого, для решения вопросов анализа и оптимизации СФЗ предварительно необходимо разработать формализованное представление предметной области, способы структурного, а затем параметрического синтеза систем защиты [16].

Таким образом, результатом исследований СФЗ, по нашему мнению, должны быть методологические основы в виде методик, моделей и методов обоснования и разработки СФЗ на всех этапах ее проектирования. Их назначение состоит в оценке уровня безопасности объекта, необходимость которой возникает при анализе защищенности объекта от нарушителей с целью принятия решений по обеспечению его защиты.

Для повышения качества (обоснованности, достоверности), снижения трудоемкости и времени работ при проектировании СФЗ должны использоваться специальные методы обработки информации, основанные на математических методах системного анализа и оптимизации систем защиты.

Сложность решаемых задач при управлении проектированием СФЗ КВО базируется на двух этапах: предпроектные исследования и рабочее проектирование.

Уровень безопасности КВО закладывается при проектировании СФЗ, поэтому повышается роль технологии проектирования СФЗ за счет принятия обоснованных управленческих решений при проведении предпроектных исследований, которые включают в себя: оценку внешней среды и объекта с целью определения задач СФЗ; обоснование и разработку СФЗ; оценку эффективности СФЗ и выработку решений по структурной модернизации СФЗ для обеспечения достаточности защиты объекта.

Несмотря на множество проводимых исследований, методический аппарат предпроектных исследований проектирования СФЗ разработан слабо, нет единой методологии, хотя именно на этом этапе принимаются значимые решения по структурным компонентам формирования системы, от которых зависит перспективность проектно-технических направлений исследований. Ошибки предпроектных исследований приводят к увеличению затрат на проведение рабочего проектирования до 70 %, следовательно полноценное решение задач повышения обоснованности принимаемых решений на всех этапах проектирования СФЗ возможно при системном анализе и едином системно-концептуальном подходе.

Научная проблема заключается в необходимости повышения достоверности и обоснованности принимаемых решений на всех этапах проектирования систем физической защиты путем разработки методик, моделей и методов на базе информационных критериев оптимальности, совокупности математических методов и современных форм обработки информации для обеспечения необходимой безопасности КВО.

Анализ тенденций развития СФЗ показал наличие противоречий в задачах разработки СФЗ: противоречия между усложнением структуры объектов охраны, ростом возможностей ИТСО и неадекватной способностью СФЗ к реализации своих функций. С другой стороны, рост технических возможностей нарушителей и активизации террористических угроз также требует постоянного совершенствования СФЗ и ее соответствия возможностям средств нарушителя, а именно способностью СФЗ к обеспечению своевременного обнаружения и нейтрализации нарушителей.

Поэтому проблема разработки методик, моделей и методов, направленных на повышение обоснованности выработки научно-технических и технологических решений на всех этапах проектирования СФЗ для обеспечения необходимой безопасности КВО, является актуальной.

Объект исследования – технологический процесс разработки СФЗ КВО.

Предмет исследования – методики, модели и методы системного анализа, алгоритмы методов и моделей математического программирования, методы обработки информации в задачах разработки СФЗ КВО.

Цели исследования – разработка новых научно-технических и технологических решений в задачах проектирования СФЗ, направленных на создание методик, моделей и методов повышения уровня обоснованности принимаемых управленческих решений для обеспечения необходимой безопасности КВО.

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

1. Посредством системного анализа, формализации и постановки задачи обеспечения безопасности КВО при управлении проектированием СФЗ разработать методологические основы исследования процесса проектирования СФЗ.

2. Разработать методики, использующие информационный критерий оптимального развития систем для решения задач:

2.1 категорирования КВО по критерию значимого различия потенциальной опасности объектов;

2.2 оценки опасности нарушителей по энтропийному показателю;

2.3 определения базовых нарушителей для категорируемых объектов;

2.4 оценки изменения активности внешней среды (нарушителей) во времени.

3. Разработать модель обоснования критериев эффективности подсистем СФЗ: обнаружения, задержки, реагирования и нейтрализации, на основе градиентного смещения плана эксперимента в минимум функции риска.

4. Разработать методику размещения и выбора ИТСО объекта, обеспечивающую заданные критерии эффективности СФЗ, предложенные в п. 3.

5. Разработать методику объединения технических средств обнаружения в группы для формирования структуры организационного управления по критерию оптимальной информационной нагрузки.

6. Разработать методы оценки эффективности СФЗ и выработки управленческих решений по результатам ее оценки:

6.1 метод оценки и повышения эффективности СФЗ на основе двух зависимых марковских цепей;

6.2 метод оценки времени утечки информации о функционировании СФЗ на основе критерия значимого изменения информации.

Научная новизна результатов заключается в следующем:

1. Разработаны методологические основы исследования процесса проектирования СФЗ, отличающиеся введением формализованного критерия обеспечения безопасности КВО при управлении проектированием СФЗ, новым информационным наполнением этапов проектирования, введением в процесс разработки методики объединения технических средств обнаружения в группы, а также методов оценки эффективности и времени утечки информации о функционировании СФЗ для выработки обоснованных решений по повышению эффективности СФЗ (п. 2 паспорта специальности 05.13.01).

2. Разработаны методики, использующие впервые введенный информационный критерий оптимальности развития системы на основе адаптированного информационно-вероятностного метода (ИВМ) (п. 4 паспорта специальности 05.13.01), а именно:

- категорирования КВО, отличающаяся введением энтропийной шкалы оценки масштаба видов потерь при ЧС для повышения достоверности ее оценки и использованием информационного критерия в интерпретации значимого различия опасности категорий, позволяющая обоснованно производить декомпозицию спектра опасности на категории;

- оценки опасности нарушителей, отличающаяся весовой сверткой характеристик нарушителей и последствий их действий к энтропийному потенциалу, позволяющая производить сравнительный анализ их опасности для определения показателей защищенности систем защиты от их действий;

- определения базовых нарушителей для категорируемых объектов, отличающаяся оценкой однородности потенциалов опасности КВО и подготовленности типовых нарушителей, повышающая уровень достоверности назначения базовых нарушителей для КВО;

- оценки изменения активности внешней среды (нарушителей) во времени, отличающаяся использованием информационного критерия для определения момента появления новой ситуации, позволяющей определить параметры активности нарушителей на момент времени предполагаемой модернизации СФЗ по причине значимого изменения внешней среды.

3. Разработана модель обоснования комплексного критерия эффективности СФЗ на основе градиентного смещения плана эксперимента в минимум функции риска, отличающаяся использованием весовых оценок вклада в эффективность подсистем СФЗ: обнаружения, задержки, реагирования и нейтрализации, позволяющая обоснованно задавать требуемые критерии эффективности подсистем СФЗ (п. 3 паспорта специальности 05.13.01).

4. Разработана методика размещения и выбора ИТСО объекта, отличающаяся использованием совокупности методов: модернизированной задачи о покрытии и синтеза вариантов назначения ИТСО на покрытия с использованием динамического программирования, обеспечивающих критерии эффективности для разных по важности критических элементов, позволяющая формировать структурную схему размещения ИТСО СФЗ (п. 7 паспорта специальности 05.13.01).

5. Разработана методика объединения технических средств обнаружения в группы для формирования структуры организационного управления, отличающаяся использованием критерия оптимальной информационной нагрузки на элементы управления организационной структуры, позволяющая формировать организационные структуры с равномерной и оптимальной информационной нагрузкой на ее элементы (п. 7 паспорта специальности 05.13.01).

6. Разработаны методы оценки эффективности СФЗ и выработки на этой основе управленческих решений:

- метод оценки и повышения эффективности СФЗ на основе двух зависимых марковских цепей, отличающийся информационной связью марковских цепей и моделью оптимального управления приращением эффективности, позволяющий вырабатывать рациональные решения структурных изменений СФЗ для повышения ее эффективности (п. 4 паспорта специальности 05.13.01);

- метод оценки времени утечки информации о функционировании СФЗ, отличающийся впервые введенным информационным показателем СФЗ – временем утечки информации о функционировании СФЗ, и использованием аналоговой электрической схемы переходных процессов для моделирования процесса утечки информации, позволяющей вырабатывать управленческие решения по изменению информационной среды СФЗ для снижения информационного потенциала опасности нарушителя (п. 4 паспорта специальности 05.13.01).

Теоретическая значимость работы заключается в дальнейшем развитии теории системного анализа, как междисциплинарной науки, применительно к задачам разработки СФЗ путем введения:

- информационных показателей и критериев оптимальности развития систем в процесс проектирования СФЗ;

- функционала управления безопасностью КВО в модель обоснования показателей эффективности СФЗ;

- метода оценки времени утечки информации о функционировании СФЗ, а также развитием методов синтеза сложных систем в методике размещения и вы-

бора ИТСО, представленные как комплексный теоретический подход к разработке СФЗ.

Практическая значимость работы:

1. Разработаны методологические основы исследования процесса проектирования СФЗ, практическая ценность которых определяется повышением достоверности исходных данных: внешней среды и категории КВО, наличием критерия оптимальности безопасного состояния КВО для обоснования эффективности подсистем СФЗ, введением в процесс проектирования СФЗ методики объединения технических средств обнаружения в группы и методов оценки эффективности и времени утечки информации о функционировании СФЗ для выработки обоснованных решений, направленных на повышение ее эффективности.

2. Разработаны методики, использующие информационный показатель оптимального развития систем и энтропийную шкалу оценки масштабов потерь, повышающие достоверность и обоснованность решения задач: категорирования КВО, оценки потенциалов их опасности и обоснования требований вероятности безопасного состояния КВО; оценки потенциалов опасности нарушителей; определения базовых нарушителей для категорируемых объектов; оценки изменения активности нарушителей во времени для прогнозирования периода модернизации СФЗ.

3. Разработана модель обоснования критериев эффективности подсистем физической защиты, необходимых проектировщику на этапе рабочего проектирования.

4. Разработана методика размещения и выбора ИТСО объекта, позволяющая формировать план их расположения на объекте защиты и обеспечивающая заданные требования эффективности СФЗ.

5. Разработана методика объединения технических средств обнаружения в группы для формирования структуры организационного управления, обеспечивающая равномерную и оптимальную информационную нагрузку на элементы управления организационной структурой СФЗ.

6. Разработаны методы оценки эффективности СФЗ:

- метод оценки и повышения эффективности СФЗ, позволяющий количественно оценить эффективность СФЗ по каждому маршруту проникновения нарушителя и оптимально изменять структуру СФЗ для обеспечения заданной эффективности;

- метод оценки времени утечки информации о функционировании СФЗ, основанный на впервые введенном показателе – времени утечки информации о СФЗ для выработки решений по обновлению информационной среды СФЗ, что позволяет уменьшить потенциал опасности нарушителя на 13 %.

Методология и методы исследования включают методы системного анализа, имитационного моделирования, марковские цепи, теорию множеств, теорию графов; методы многомерного анализа (главных компонент, кластерный анализ), теорию вероятностей и планирования эксперимента; методы математического программирования, информационно-вероятностный метод, методы анализа переходных процессов теории электрических цепей.

Положения, выносимые на защиту:

1. Системный подход представления предметной области. Формализованная постановка задачи обеспечения безопасности КВО и структурная схема управления разработкой СФЗ. Методологические основы исследования процесса разработки СФЗ в виде структуры информационно связанных методик, моделей и методов для выработки обоснованных решений на всех этапах проектирования.

2. Методики, использующие информационный показатель оптимального развития систем для решения задач:

- категорирования КВО по критерию значимого различия потенциальной опасности объектов;

- оценки опасности нарушителей по энтропийному показателю;

- определения базовых нарушителей для категорируемых объектов;

- оценки изменения активности внешней среды (нарушителей) во времени.

3. Модель обоснования критериев эффективности подсистем СФЗ: обнаружения, задержки, реагирования и нейтрализации на основе градиентного смещения плана эксперимента в минимум функции риска.

4. Методика размещения и выбора ИТСО объекта, обеспечивающая заданные критерии эффективности СФЗ, предложенные в п. 3.

5. Методика объединения технических средств обнаружения в группы для формирования структуры организационного управления по критерию оптимальной информационной нагрузки.

6. Методы оценки эффективности СФЗ и выработки управленческих решений по результатам ее оценки:

- метод оценки и повышения эффективности СФЗ на основе двух зависимых марковских цепей;

- метод оценки времени утечки информации о функционировании СФЗ на основе критерия значимого изменения информации.

Основания для выполнения работы. Исследование проблемы – «обеспечения безопасности и противодействие терроризму» – относится к приоритетному направлению развития науки, а сама технология обеспечения защиты и жизнедеятельности населения и опасных объектов при угрозах террористических проявлений включена в перечень критических технологий. Все это определено Указом Президента Российской Федерации от 07.07.2011 № 899 «Об утверждении приоритетных направлений развития науки, технологий и техники в Российской Федерации и перечня критических технологий Российской Федерации» [12].

Предлагаемые методологические основы в виде методик, моделей и методов в задачах управления проектированием СФЗ были успешно применены в работах, выполняемых на ОАО «Концерн «Созвездие» г. Воронеж, ФГБУ «3 ЦНИИ» министерства обороны РФ ст. Донгузская, Оренбургской обл., ЗАО «Центр безопасности информации «ЦИНТУР» г. Оренбург, ООО «Уральский центр систем безопасности «УЦСБ» г. Екатеринбург, предприятие корпорации «Ростех» АО «Радиозавод» г. Пенза, в учебном процессе ФГБОУ ВО Оренбург-

ский государственный университет и ФГБОУ ВО Пензенский государственный университет.

Разработанные методики, модели и методы позволяют эффективно разрабатывать на этапе предпроектных исследований структурную модель СФЗ путем предлагаемого подхода, а также существенно уменьшить ошибки рабочего проектирования.

Данная научная работа выполнялась в рамках НИР «Шифр Охрана – 2011», договор № 572 от 11.06.2009 (г. Воронеж, ОАО «Концерн «Созвездие»), ряд задач решался в рамках НИР «Ясногорец-3» (ФГКУ «3 ЦНИИ» МО РФ), госбюджетных НИР: И130621142522 от 26.07.2013 г., И130918174735 от 04.10.2014 г., И131210202925 от 12.12.2015 г., И01201000576 от 14.03.2017 г. (г. Оренбург, Оренбургский государственный университет).

Степень достоверности и апробация результатов. Основные результаты диссертации докладывались, обсуждались на научно-технических конференциях различного уровня, в их числе:

- Региональная конференция молодых ученых и специалистов, Оренбург, ОГАУ, 1998, 1999 гг.

- XIV межвузовская научно-практическая конференция, Оренбург, Филиал военного университета ВПВО РФ, 1999 г.

- IV, V, IX, X, XI Всероссийская научно-практическая конференция с международным участием «Современные информационные технологии в науке, образовании и практике», Оренбург, 2003, 2004, 2010, 2012, 2014 гг.

- Научно-техническая конференция с международным участием «Перспективные информационные технологии в научных исследованиях, проектировании и обучении», Самара, 2006 г.

- Международная научно-практическая конференция «Инновации в науке, бизнесе и образовании», Оренбург, 2008 г.

- V Международная научная конференция «Информационные технологии и системы», Банное, 2016 г.

- XIII Международная научно-техническая конференция «Новые информационные технологии и системы», Пенза, 2016 г.

- VII Всероссийская научная конференция (с приглашением зарубежных ученых - ITIDS 2019), Уфа, 2019 г.

- VI Международная конференция и молодежная школа «Информационные технологии и нанотехнологии» (ИТНТ – 2020), Самара, 2020 г.

Результаты диссертационной работы отражены в 41 публикации, в том числе в 1 монографии, 35 статьях (включая 1 – в изданиях, индексируемых в *Scopus*, 13 – в изданиях из перечня ВАК), имеется 5 – свидетельств об официальной регистрации программ для ЭВМ и 5 – отчетов по НИР.

Структура работы. Работа включает введение, 6 глав основного материала, заключение, список использованных источников и 2 приложений. Работа изложена на 249 страницах машинописного текста, содержит 75 рисунков и 61 таблицу. Список использованных источников содержит 138 наименований.

ГЛАВА 1 СИСТЕМНЫЙ АНАЛИЗ ПРОЕКТИРОВАНИЯ СИСТЕМ ФИЗИЧЕСКОЙ ЗАЩИТЫ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ

1.1 Основные положения, термины и сущность процесса проектирования систем физической защиты

1.1.1 Актуальность проблемы физической защиты критически важных объектов

В настоящее время во всем мире большое внимание уделяется развитию вопросов безопасности КВО. В рамках исследований проблемы безопасности в России появился ряд нормативных документов Совета Безопасности РФ и ФСТЭК РФ, что подтверждает актуальность данной проблемы [1 - 14]. Согласно ГОСТ Р 22.2.06-2016 «критически важный объект РФ – объект, нарушение или прекращение функционирования которого приведет к потере управления экономикой Российской Федерации, субъекта Российской Федерации или административно-территориальной единицы субъекта Российской Федерации, ее необратимому негативному изменению (разрушению) либо существенному снижению безопасности жизнедеятельности населения».

В федеральном законе РФ 68 – ФЗ от 21.12.1994 г. определен перечень объектов, которые относятся к КВО [3].

Особое место среди КВО занимают объекты информатизации. Объект информатизации – совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения; помещения или объекты, в которых эти средства и системы установлены, или помещения и объекты, предназначенные для ведения конфиденциальных переговоров [9].

Повышение безопасности КВО (структурно сложных и распределенных объектов: аэропортов; морских портов; береговой охраны; важных стратегических объектов: атомных электростанций, гидроэлектростанций; объектов нефтяной и газовой промышленности: нефте- и газоперерабатывающих заводов) является ак-

туальной и трудно разрешимой проблемой [1 - 4]. В этом плане основное направление борьбы общества – повышение эффективности защиты важных объектов.

В отношении перечисленных выше КВО законодательно закреплены особые условия функционирования их производства, а также получения, хранения и использования опасных материалов в технологических целях.

Основными особенностями вышеперечисленных объектов являются:

- объект защиты состоит из множества технологически связанных локальных зон;

- объект защиты, как правило, имеет сложную конфигурацию периметра;

- на объекте защиты технологические процессы многообразны, структурно удалены друг от друга и, как правило, автоматизированы. Все это накладывает определенные ограничения на организацию системы безопасности таких объектов [16, 20].

Традиционная схема организации охраны крупных объектов, занимающих большие территории, до недавнего времени предусматривала использование в качестве основного элемента размещение на охраняемом объекте поста – часового, охранника. В функции поста входят задачи: обнаружение нарушителя, оповещение групп задержания и принятие соответствующих мер по защите охраняемого объекта. Для выполнения этих задач каждый пост должен быть оснащен средствами наблюдения, связи и освещения охраняемого объекта, а также оружием [21].

В настоящее время построение системы охраны по традиционной схеме, особенно на крупных объектах с большой протяженностью охраняемого периметра, с большим числом охраняемых зданий приводит к значительным затратам людских ресурсов [21].

Таким образом, способность СФЗ к обеспечению необходимого уровня защищенности опасных объектов, должна закладываться разработчиками на этапе концептуального проектирования СФЗ и уточняться на этапе рабочего проектирования и остальных этапах ее жизненного цикла (ввод в действие, эксплуатация, модернизация и снятие с эксплуатации), а также при изменении внешней среды или изменении категории объекта защиты.

В науке «имеется большой опыт разработки СФЗ для малых и средних объектов, не нуждающихся в дополнительных мерах безопасности. Однако остаются мало исследованы вопросы принятия эффективных управленческих решений при проектировании СФЗ для обеспечения безопасности КВО как наиболее уязвимых по отношению к внешней среде и поэтому требующих повышенных мер безопасности» [21].

В результате «системного анализа организации охраны объектов различной сложности выявлено наличие противоречий при функционировании СФЗ, которые подробно рассмотрены в монографии» [21] и представлены на рисунке 1.1.

Рисунок 1.1 – Основные противоречия при проектировании СФЗ

1.1.2 Определения, руководящие документы и анализ понятий элементов предметной области – безопасность объектов

Понятие безопасность определяется законами Российской Федерации, ГОСТ и приказами Федеральной службы технического и экспертного контроля (ФСТЭК). Это широкое философское понятие, которое рассматривается как состояние защищенности объекта и его свойство (рисунок 1.2).

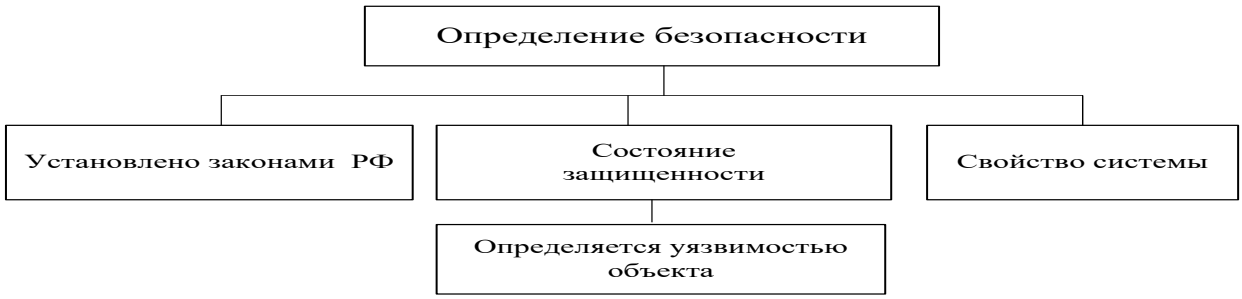


Рисунок 1.2 – Понятие безопасности

В Законе РФ «О безопасности» дается следующая формулировка «безопасности» (применительно к государственной безопасности) [22]: «безопасность – состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз». «Безопасность» и «защищенность» по своей сути синонимы.

С позиций системного анализа в [23] рассмотрена проблема безопасности существования и развития человечества, показана необходимость комплексного подхода к рассмотрению проблем безопасности. Понятие «безопасность» трактуется следующим образом: «Это состояние защищенности личности, общества, государства от внешних и внутренних опасностей и угроз, базирующееся на деятельности людей, государства, мирового сообщества народов по выявлению, предупреждению, устранению и отражению опасностей и угроз, способных погубить их, лишить фундаментальных материальных и духовных ценностей, закрыть путь выживания» [23].

Безопасность объекта (с точки зрения его защиты от несанкционированных действий посторонних лиц – физическая безопасность) как состояние – это такое

состояние защищенности охраняемого объекта, при котором может исключаться возможность (профилактические меры соответствующих служб) реализации угроз, а в случае их возникновения, предотвращаются воздействия на объект и обеспечивается защита материальных и иных ценностей.

Безопасность объекта (физическая безопасность) как свойство – свойство технических, организационных и иных систем (входящих в состав систем физической безопасности объекта) сохранять способность противостоять угрозам и несанкционированным действиям посторонних лиц и предотвращать их с целью защиты жизненно важных интересов объекта.

В источниках [24 - 26] встречается понятие «комплексная безопасность объекта» (КБО), которая определяется как «совокупность организационных мероприятий и действий подразделений охраны, служб безопасности с применением технических средств обеспечения комплексной безопасности, направленных на обеспечение установленных режима, порядка и правил поведения; предотвращение, обнаружение и ликвидацию угроз жизни, среде обитания, имуществу и информации, а также поддержание работоспособности технических средств и систем на охраняемом объекте с целью ограничения или предотвращения вторжения нарушителя для осуществления опасных несанкционированных действий, приводящих к частичному или полному нарушению функционирования объекта» [24].

Развитие систем безопасности неразрывно связаны с процессами широкой автоматизации и интеграции. Интеграция – это качественно новый скачок в построении систем безопасности, она позволит:

- уменьшить затраты путем минимизации аппаратной и программной части; уменьшить количество информации, которую обрабатывает оператор, и сделать ее легко воспринимаемой;

- автоматизировать процесс принятия решений; повысить защищенность системы от внешнего воздействия.

Таким образом, решение проблемы кроется в создании единого комплекса, координирующего и управляющего работой всех систем безопасности, – интегрированной системы безопасности (ИСБ).

Рассматриваемое понятие «безопасность» тесно связано с предметной областью трех взаимодействующих элементов: объекта охраны, потенциального нарушителя и СФЗ, которая уравновешивает противоборство нарушителя и объекта охраны. Схема компоновки элементов предметной области представлена на рисунке 1.3.

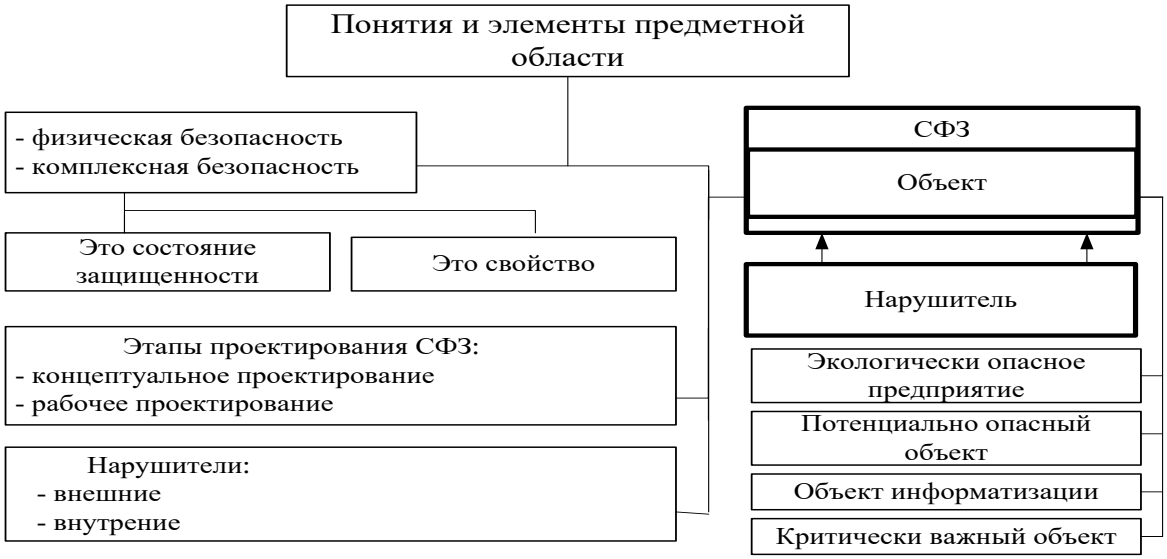


Рисунок 1.3 – Понятия и элементы предметной области

Рассматривая систему защиты КВО как комплекс разнородных элементов, объединенных единой задачей по предотвращению реализации всевозможных угроз нанесения ущерба охраняемому объекту, нельзя не сказать о понятиях и характеристиках элементов предметной области: объект охраны, нарушитель и СФЗ.

Существует множество определений опасного объекта: потенциально опасный объект, критически важный объект, объект информатизации, значимый объект критической информационной инфраструктуры, объект повышенной опасности, экологически опасное предприятие, опасный производственный объект и т. д.

Понятие «потенциально опасный объект», раскрывается в Распоряжении Правительства РФ № 1047-р от 21.06.2010: «Потенциально опасные объекты РФ – объекты, на которых используют, производят, перерабатывают, хранят, эксплуатируют, транспортируют или уничтожают радиоактивные, пожаровзрывоопасные

и опасные химические и биологические вещества, а также гидротехнические сооружения, создающие реальную угрозу возникновения источника кризисной ситуации».

В ГОСТ Р 22.2.06 - 2016 дано определение потенциально опасного объекта (ПОО): «Объект, на котором расположены здания и сооружения повышенного уровня ответственности, либо объект, на котором возможно одновременное пребывание более пяти тысяч человек» [1].

В федеральном законе № 38-ФЗ от 8.03.2015г. «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера» дано определение КВО. «Критически важные объекты – объекты, нарушение или прекращение функционирования которых приводит к потере управления экономикой РФ, субъекта РФ или муниципального образования, необратимому негативному изменению или разрушению экономики РФ, субъекту РФ или муниципального образования либо существенному снижению безопасности жизнедеятельности населения, проживающего на этих территориях, на длительный период» [14].

Усиливающиеся в последнее время темпы внедрения информационных технологий практически во всех областях научно-технического и социально-экономического развития общества свидетельствуют о том, что объективным началом этого развития становится информация [27].

Именно информационная сфера в настоящее время определяет темпы эволюции всех отраслей цивилизации. Вместе с тем, информатизация общества наряду с неоспоримыми преимуществами неизбежно влечет и информатизацию криминала в гигантских масштабах, а это, в свою очередь, обостряет проблему борьбы за обладание информационными ресурсами.

Первоочередными объектами криминальной среды являются информационные ресурсы, деструктивные действия против которых приносят значительный ущерб. Такими объектами являются: органы государственного управления, системы управления инфраструктурой связи, финансов, энергетики, транспорта, водоснабжения и чрезвычайных служб. Информационные элементы этих структур являются критически важными элементами информационной сферы.

В ГОСТ Р 51275-2006 «Защита информации. Объект информатизации…» под «объектом информатизации понимается совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров» [9].

В ГОСТ Р 53114-2008 «Защита информации. Обеспечение информационной безопасности в организации» введено понятие КСИИ – информационно-управляющая или информационно-телекоммуникационная система, которая осуществляет управление критически важным объектом, или информационное обеспечение управления объектом, или официальное информирование граждан, и в результате деструктивных информационных воздействий на которую может сложиться чрезвычайная ситуация, или будут нарушены выполняемые системой функции управления со значительными негативными последствиями [5].

«Современные КВО, как правило, имеют в своем составе КСИИ, которая обеспечивает управлением технологическими процессами объекта с использованием специализированных АСУ. Проблема информационной безопасности КСИИ КВО определяется важностью решаемых ими задач, когда деструктивные действия нарушителей в отношении КСИИ могут привести к возникновению ЧС» [21]. Это накладывает дополнительные требования при разработке СФЗ по обеспечению не только антитеррористической, но и информационной безопасности КВО.

В «Федеральном законе от 26 июля 2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» введено понятие значимые объекты критической информационной инфраструктуры» [7], к которым относится:

- информационные системы федерального, регионального и объектового масштаба;
- автоматизированные системы управления технологическим процессом производства или функционированием значимым объектом;

- информационно-телекоммуникационные сети объектов, которые отнесены к значимым объектам.

В соответствии с этим же законом к значимым объектам критической информационной инфраструктуры РФ, на которые распространяются требования ФСТЭК России относятся:

- объекты информатизации с АСУ производственными и технологическими процессами на КВО;

- объекты, на которых выполняются работы, связанные со сведениями, составляющими государственную тайну;

- военные объекты, образцы вооружения и военной техники при испытаниях на полигонах Минобороны России (образцы вооружения и военной техники при их разработке, производстве и полигонных испытаниях);

- значимые объекты критической информационной инфраструктуры, средств и систем связи и управления в отношении технических средств и систем Минобороны России, СВР России, ФСБ России, ФСО России и ГУСПа, а также объекты и технические средства федеральных органов государственной власти, защита которых входит в компетенцию ФСТЭК;

- объекты, на которых выполняются работы, связанные со сведениями, составляющими служебную тайну (персональные данные и т. п.);

- значимые объекты, являющиеся государственными информационными системами, не составляющими государственную тайну.

Деструктивные действия нарушителей в отношении значимых объектов критической информационной инфраструктуры могут привести к негативным последствиям на КВО и даже к возникновению ЧС.

Чрезвычайная ситуация – обстановка на определенной территории или акватории, сложившаяся в результате аварии, опасного природного явления, катастрофы, стихийного или иного бедствия, которая может повлечь или повлекла за собой человеческие жертвы, ущерб здоровью людей или окружающей природной среде, значительные материальные потери и нарушение условий жизнедеятельности людей (государственный стандарт РФ ГОСТ Р 22.0.02-2016 «Безопасность в

чрезвычайных ситуациях. Термины и определения основных понятий»). ЧС различаются по характеру источника (природные, техногенные, биолого-социальные и военные) и по масштабам (трансграничные, федеральные, региональные, территориальные, местные, локальные) [1].

Классификация ЧС природного и техногенного характера, принятая в постановлении Правительства Российской Федерации от 21 мая 2007 №304 «О классификации чрезвычайных ситуаций природного и техногенного характера» приведена в таблице 1.1 [19].

Таблица 1.1 – Классификация ЧС природного и техногенного характера

Масштаб ЧС	Пострадало и нарушены условия жизнедеятельности людей	Размер материального ущерба (млн. руб.)	Размер зоны ЧС
Локального характера	не более 10	не более 0,1	Не выходит за пределы территории объекта производственного или социального назначения
Муниципального характера	не более 50	не более 5	Не выходит за пределы одного поселения или внутригородской территории федерального значения
Межмуниципального характера	не более 50	не более 5	Не выходит за пределы двух или более поселений, внутригородских территорий федерального значения или межселенную территорию
Регионального характера	свыше 50, но не более 500	свыше 5, но не более 500	Не выходит за пределы одного субъекта РФ
Межрегионального характера	свыше 50, но не более 500	свыше 5, но не более 500	Затрагивает территорию двух и более субъектов РФ
Федерального характера	свыше 500	свыше 500	Выходит за пределы территории РФ

В соответствии с приведенной классификацией ЧС предполагается, что:

- ЧС, возникающие в результате террористического акта (ТА) (диверсии) на объектах высокой категории и развиваются по пессимистическому сценарию, могут приобрести федеральный, региональный и межрегиональный характер;

- ЧС, возникающие в результате ТА (диверсии) на объектах средней категории и развиваются по пессимистическому сценарию, могут приобрести муниципальный и межмуниципальный характер;

- ЧС, возникающие в результате ТА (диверсии) на объектах низкой категории и развивающиеся по пессимистическому сценарию, могут приобрести локальный характер.

Для конкретного объекта вероятные угрозы могут различаться, поэтому представляется необходимым классифицировать угрозы по определенным признакам, которыми могут быть: характер угроз; тип источника угроз; тип нарушителей; величина и значимость потенциальных потерь в случае реализации угрозы. Последний классификационный признак основан на существующих методических рекомендациях по оценке ущерба от ЧС техногенного и природного характера. Перечислим их:

1. «Методические рекомендации по оценке ущерба от аварий на опасных производственных объектах» (РД 03-496-02). Утверждены постановлением Госгортехнадзора России № 63 от 29.10.2002. Документом определяется структура ущерба применительно к авариям на опасных производственных объектах, приводятся методики количественной оценки экономического ущерба от аварий.

2. В 2004 году ФГУ ВНИИ ГОЧС разработана «Единая межведомственная методика оценки ущерба от ЧС природного, техногенного и террористического характера, а также классификации и учета чрезвычайных ситуаций». Методика утверждена приказом МЧС России от 01.12.2004.

Оценка возможного ущерба при возникновении ЧС необходима для определения категории объекта.

«Потенциальная опасность объекта (категория) определяется масштабом и характером ЧС, возникающей в случае удачной реализации угрозы» [21]. Трудность оценки ущерба от ЧС на объекте заключается в том, что сам ущерб носит комплексный характер, а все его составляющие (финансовые, людские, экологические и т. д.) разнородны и их оценка затруднена.

Под «категорией объекта понимается комплексная оценка состояния опасности объекта, учитывающая его экономическую, научно-техническую, технологическую или иную (например, культурную или общественную) значимость в зависимости от характера и концентрации сосредоточенных ценностей, последст-

вий от возможных преступных посягательств на них, сложности требуемой надежности охраны. В основе этого определения лежит понятие категории объекта из ГОСТ Р 50776-95» [21].

«Цель категорирования – определение количественных и качественных требований к СФЗ, то есть необходимо провести классификацию объектов по категориям важности (значимости), чтобы определить качественные и количественные требования к их СФЗ» [21].

Анализ литературных источников и различных ведомственных методик [16, 20, 21, 29 - 31] показал, что на сегодняшний день не существует единого подхода к проведению категорирования объектов повышенной опасности, и это несмотря на то, что на совместном заседании Совета Безопасности РФ и Государственного совета РФ 13 ноября 2003 года категорирование объектов объявлено общегосударственной задачей.

В настоящее время основным документом по общегосударственному категорированию являются «Методические рекомендации по категорированию объектов науки, промышленности , энергетики и жизнеобеспечения по степени их потенциальной опасности и диверсионно-террористической уязвимости».

Категорирование осуществляется с учетом действия наиболее опасного типа нарушителя (диверсионно-террористическая группа) с использованием свертки нескольких частных видов потерь.

Для оценки потенциальной опасности объектов вводятся шесть частных видов и масштабов потерь.

Частные виды потерь – это:

- политические (оцениваются снижением всех уровней авторитета властей и общей нестабильностью);

- людские (потери, заключающиеся в утрате жизни людей, их здоровья);

- финансовые (определяются утратами материальных ценностей);

- экономические (учитывают затраты на переселение людей из зоны аварий и компенсационные выплаты);

- экологические (потери природных ресурсов, приводящие к ухудшению

экологической обстановки в регионе);

- культурно-информационные (потери, определяются утратами художественных ценностей, передовых технологий, конфиденциальной информации).

Частные виды потерь определяются для шести масштабов потенциальных потерь:

- локальный (ущерб в пределах территории объекта) – 1;

- местный (ущерб в пределах территории населенного пункта) – 2;

- территориальный (ущерб в пределах территории субъекта РФ) – 3;

- региональный (ущерб затрагивает масштаб двух субъектов РФ) – 4;

- государственный (ущерб затрагивает масштаб более двух субъектов РФ) – 5;

- межгосударственный (ущерб выходит за пределы территории РФ) – 6.

По результатам экспертного анализа заполняется матрица категорирования и определяется комплексный показатель масштаба потерь в виде суммы баллов и по ее величине определяется категория объекта [20].

Обоснование количественных требований к СФЗ заключается в выборе показателя эффективности СФЗ и в обосновании значений критериев эффективности СФЗ.

Таким образом, основные понятия и определения объекта защиты можно свести в структуру, представленную на рисунке 1.4.

Нарушитель [32, 33], используя уязвимости объекта и выбирая из всего множества целей объекта (в ряде случаев цели нарушителя трактуются как жизненно важные зоны объекта, их называют критическими элементами) цель посягательства, представляет потенциальную угрозу. Когда цель выбрана, то нарушитель создает реальную угрозу для конкретной цели объекта.

Рисунок 1.4 – Основные понятия и определения объекта защиты

Для реализации реальной угрозы нарушитель осуществляет попытку проникновения на охраняемый объект. А в случае удачного выполнения намеченных целей нарушителем, реальная угроза превращается в осуществленную угрозу.

Собственники объекта, его администрация при построении системы безопасности объекта должны опираться на правовые акты четырех уровней: международного, федерального, отраслевого (ведомственного) и объектового [20].

Для разработки модели нарушителя необходимо определение угроз и целей защиты.

«Модель нарушителя - это логическое описание, включающее совокупность количественных (вес, скорость перемещения, рост и т. п.) и качественных (цели и способы действия, степень подготовленности, осведомленность об объекте и т. п.) характеристик нарушителя, с учетом которых определяются требования к комплексу ИТСО» [25].

В методиках формирования модели нарушителя описаны признаки классификации нарушителей, определен допустимый уровень потерь для нарушителей, приведены зависимости превышения сил реагирования над нарушителями от допустимого уровня потерь нарушителей и от допустимого уровня потерь сил реагирования. Определены типы нарушителей, их возможности, тактика действия

нарушителей. Достаточно подробно описывается применение диаграммы последовательности действий нарушителя, под которой понимается графическое изображение элементов системы защиты, используемое для оценки эффективности СФЗ[16].

Типовые нарушители определены приказом министра промышленности и энергетики РФ от 04.05.2007 №150 «Об утверждении рекомендаций по антитеррористической защищенности объектов промышленности и энергетики» [34], а также постановлении правительства № 875 от 29.08.2014 «Об антитеррористической защищенности объектов ФСТЭК ..» [2]. Модель нарушителя включает шесть различных типов нарушителей (ТН), их характеристики представлены в таблице 1.2.

Таблица 1.2 – Характеристики типовых нарушителей

Характеристики нарушителей	Тип нарушителя					
	X_1	X_2	X_3	X_4	X_5	X_6
Численность	5 – 12	2 – 4	1	1	1	1
Цель действий	террор. акт	терр. акт	терр. акт	хищение	хищение	хищение, терр. Акт
Последствия действий нарушителя	федеральный, региональный, территориальный	за пределами объекта	в пределах объекта	в пределах объекта	в пределах объекта	в пределах объекта
Уровень осведомленности	общий уровень. (0,7)	средний уровень осведомленности (0,6)	низкий уровень осведомленности (0,3)	низкий уровень осведомленности (0,3)	высокий уровень осведомленности (0,9)	высокий уровень осведомленности (0,9)
Холодное и огнестрельное оружие оснащение	высокая вероятность	высокая вероятность	высокая вероятность	низкая вероятность	низкая вероятность	Вооружен
Уровень подготовки преодоления барьеров, готовность вступить в бой	Высокий p>0,8	Высокий уровень подготовки	Высокий уровень подготовки	Низкий уровень подготовки	Низкий уровень подготовки	Средний уровень подготовки
Может вступать в сговор с работниками объекта	Да	Да	–	–	Да	Да
Возможность делиться на группы	Да	Да	Нет	Нет	Нет	Нет
Возможность пожертвовать собой	Да	Да	Да	–	–	–
Тактика действий: насильственная, обманная, скрытная, комбинированная	Насильственная	Скрытная	–	Скрытная, подкуп	Легальный проход	Легальный проход

Таким образом, нарушитель как элемент сложной системы имеет множество характеристик, представленных в виде схемы на рисунке 1.5, которые формируют его потенциал технической, физической и информационной подготовленности нарушителя.

Рисунок 1.5 – Основные характеристики типовых нарушителей

В приказе ФСТЭК № 31 изложены требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах [6].

Для формирования требований к защите информации в АСУ выделяют следующее:

- классификацию автоматизированной системы управления по требованиям защиты информации (далее – классификация автоматизированной системы управления);

- определение угроз безопасности информации, реализация которых может привести к нарушению штатного режима функционирования автоматизированной

системы управления, и разработку на их основе модели угроз безопасности информации;

- определение требований к системе защиты АСУ.

Классификация АСУ проводится заказчиком в зависимости от уровня значимости (критичности) информации, обработка которой осуществляется в автоматизированной системе управления.

Устанавливаются три класса защищенности автоматизированной системы управления, определяющие уровни защищенности автоматизированной системы управления. Класс защищенности автоматизированной системы управления определяется в соответствии с приложением N 1 к настоящим Требованиям.

В приказе ФСТЭК России от 09.08.2018 N 138 определены требования к мерам защиты информации в автоматизированной системе управления [35]. Организационные и технические меры защиты информации, реализуемые в автоматизированной системе управления в рамках ее системы защиты, в зависимости от класса защищенности, угроз безопасности информации, используемых технологий и структурно-функциональных характеристик автоматизированной системы управления и особенностей ее функционирования должны обеспечивать следующее:

- в автоматизированных системах управления 1 класса защищенности - нейтрализацию (блокирование) угроз безопасности информации, связанных с действиями нарушителя с высоким потенциалом;

- в автоматизированных системах управления 2 класса защищенности - нейтрализацию (блокирование) угроз безопасности информации, связанных с действиями нарушителя с потенциалом не ниже среднего;

- в автоматизированных системах управления 3 класса защищенности - нейтрализацию (блокирование) угроз безопасности информации, связанных с действиями нарушителя с низким потенциалом.

Потенциал нарушителя определяется в ходе оценки его возможностей и мотивации, проводимой при анализе угроз безопасности информации в соответствии с пунктом 13.3 настоящих Требований.

Система физической защиты – совокупность персонала физической защиты, осуществляемых им организационно-технических мероприятий, действий и инженерно-технических средств, предназначенная для реализации физической защиты на потенциально опасном объекте [2, 25].

Целью СФЗ является предотвращение ТА, диверсий и хищений в отношении предметов физической защиты. Данная цель достигается путем создания и обеспечения функционирования единой системы мер, направленных на решение совокупности задач СФЗ.

В зависимости от физического представления существует множество различных структурных схем СФЗ, наиболее распространенными среди которых являются следующие:

1) СФЗ с точки зрения организационно-технической структуры, представлена на рисунке 1.6.

Рисунок 1.6 – Схема СФЗ по типу организационно технической структуры

2) СФЗ в виде функционально завершенных компонентов представлена на рисунке 1.7. Такое представление СФЗ позволяет задавать требования к компонентам в нормативных документах;

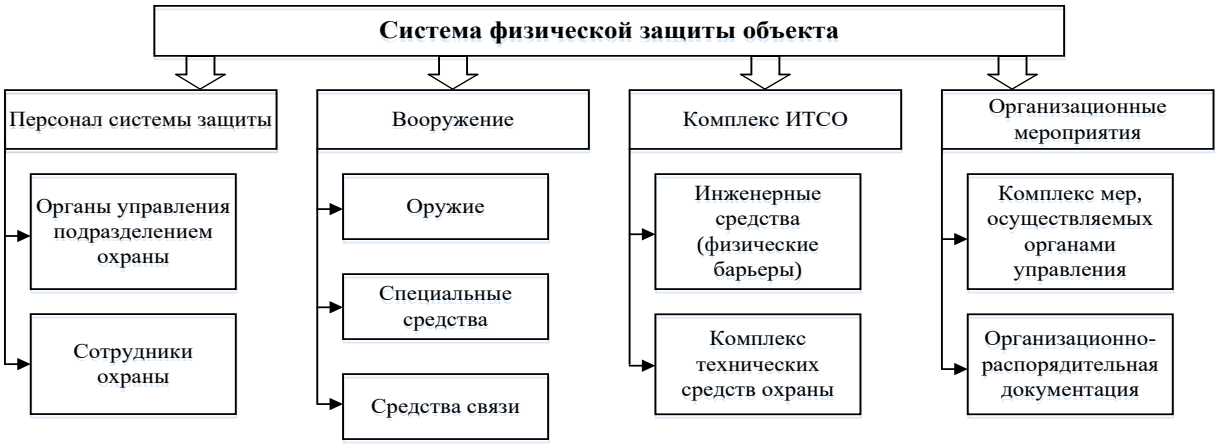


Рисунок 1.7 – Структура СФЗ в виде функциональных компонентов

3) структура СФЗ в виде функциональных подсистем: система охранной сигнализации, система контроля и управления доступом, система теленаблюдения, система оперативной связи и оповещения, система защиты информации, электропитания, освещения и др. представлена на рисунке 1.8.

Рисунок 1.8 – Схема СФЗ по типу функциональных подсистем

«Физическая защита обеспечивает предупреждение несанкционированного физического проникновения на охраняемую территорию» [21].

«Инженерная защита предусматривает использование конструкционных элементов зданий, барьеров по периметру охраняемого объекта» [21].

«Техническая защита включает систему охранной сигнализации, систему телевизионного наблюдения, систему контроля доступа, охранное освещение, систему связи и т. д.» [21].

Специальная защита осуществляет проверку надежности персонала службы охраны и других категорий служащих для исключения утечки информации. Как правило, она включает комплекс организационно-технических и специальных ме-

роприятий, таких как:

- обеспечение требований безопасности на этапах проектирования, строительства и эксплуатации зданий; периодическое проведение обследований помещений на предмет возможно установленных в них подслушивающих устройств; проверку и защиту технических средств передачи, обработки, накопления информации; проведение специальных мероприятий по выявлению неблагонадежных сотрудников;

4) схема СФЗ по характеру решаемых задач представлена на рисунке 1.9.

Рисунок 1.9 – Схема СФЗ по характеру решаемых задач

Подсистема обнаружения вторжения – это выявление нарушителя при попытке несанкционированного проникновения на объект. Здесь необходимо четко представлять, что обнаружение без оценки ситуации – это не обнаружение. После обнаружения нарушителя подсистема задержки должна препятствовать продвижению для осуществления враждебного акта до прибытия сил реагирования и нейтрализации.

Подсистема реагирования и нейтрализации должна упредить нарушителя и производить его удержание[16]. В зависимости от количественного состава на силы реагирования может возлагаться задача по проведению нейтрализации нарушителя.

Проектирование и анализ СФЗ требуют комплексного научного подхода, который предполагает проектирование в две стадии: предпроектные исследования и рабочее проектирование. Предпроектные исследования включают следующие этапы [33]:

- анализ системы физической защиты и уязвимости объекта;

- разработку принципов обеспечения защиты объекта;

- разработку состава и структуры комплексов ИТСО СФЗ и технико-экономического обоснования разработки системы защиты.

Таким образом, СФЗ имеет разнородную структуру подсистем с различным назначением и физической природой функционирования. Состав подсистем и решаемые задачи СФЗ представлены на рисунке 1.10.

Рисунок 1.10 – Основные понятия и определения СФЗ

1.2 Системный анализ предметной области

1.2.1 Представление системы физической защиты как системы взаимосвязанных антагонистических подсистем

Модель обеспечения безопасности объекта представлена следующим образом (рисунок 1.11).

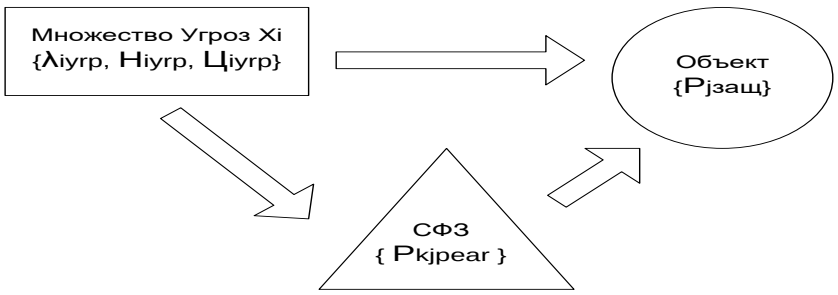


Рисунок 1.11 – Модель обеспечения безопасности объекта

В модели определено три множества [21, 66]:

- множество угроз $X=\{x_i \mid i=1,N\}$. Каждая i-ая угроза характеризуется: $\lambda_{iугр}$ – интенсивностью проявления i-ой угрозы за определенный интервал времени; $H_{iугр}$ – значимостью (опасностью) i-ой угрозы в нанесении ущерба (потерь) $Ц_{iугр}$ при реализации угрозы;

- множество ИТСО $Z=\{z_k \mid k=1,M\}$ которые выполняют функцию блокировки угроз (степень сопротивления попыткам проникновения), и характеризуются соответственно $P_{i\,угр}^{k\,j\,реаг}$ – вероятностью своевременной реакции системы на i-ую угрозу;

- множество $Y=\{y_j \mid j=1,L\}$ зон объекта защиты, характеризующихся инженерно-технической укрепленностью с показателями: $P_{j\,защ}^{зоны}$ – уровень защищенности j-ой зоны, определяется вероятностью преодоления рубежей охраны зоны, $Ц_j$ – ценность j-ой зоны, определяется важностью объекта и формирует мотивацию выбора нарушителем j-ой зоны.

С другой стороны, используя методологию системного подхода, понятие «обеспечение безопасности» можно рассматривать как единство трех систем, а именно технической, социально-правовой и человеко-машинных связей, причем техническая система включает две подсистемы: объект охраны – то, что необходимо защищать, это могут быть здания, помещения, открытые и режимные территории с ограждением, отдельные предметы (автомобили, сейфы, музейные экспонаты и т. д.) и техническая система – СФЗ, которая осуществляет защиту объектов от угроз со стороны нарушителей. Безусловно, функционирование этих трех систем происходит на фоне воздействующих факторов:

1) окружающая (внешняя) и внутренняя среда:

- физические условия функционирования объекта (границы объекта, местоположение и планы зданий, составляющие инфраструктуры объекта: отопление, вентиляция, система энергоснабжения и т.д., рельеф, растительность, животный мир, шумовой фон (железные дороги, аэропорты, автомагистрали), климат, почва);

- рабочие процессы на объекте (технологические процессы выпуска продукции, условия работы, тип и количество персонала).

2) угрозы:

- терроризм, преступность, экстремизм;

- техногенные катастрофы (аварийное отключение энергоснабжения, пожар, утечка газов, радиационная опасность и т. д.);

- природные факторы (землетрясение, наводнение, дожди т. д.).

3) социально-правовые факторы:

- правовая база антитеррористической и антипреступной борьбы на всех уровнях: международном, федеральном, отраслевом и объектовом [1 - 14];

- взаимоотношения федеральных органов исполнительной власти с органами государственной власти субъектов РФ и органами местного самоуправления в вопросах обеспечения защищенности объектов инфраструктуры от террористических и террористических угроз;

- отношения собственника объекта к роли системы безопасности.

Влияние внешней среды на систему может проявляться в виде таких угроз, как стихийные бедствия, техногенные катастрофы, физические действия со стороны нарушителей. Кроме того, влияние внешней среды проявляется в учете внешних физических условий эксплуатации защищаемого объекта, что накладывает ограничения на применение определенных технических средств охраны. Особенность технологических процессов производства также накладывает ограничения на правила допуска в определенные зоны объекта и т.д.

В рамках концепции безопасности нас будет интересовать угроза, заключающаяся в физическом проникновении на объект. Данное событие наступает при

невыполнении своих функций хотя бы одной из подсистем СФЗ, представленных на рисунке 1.12.

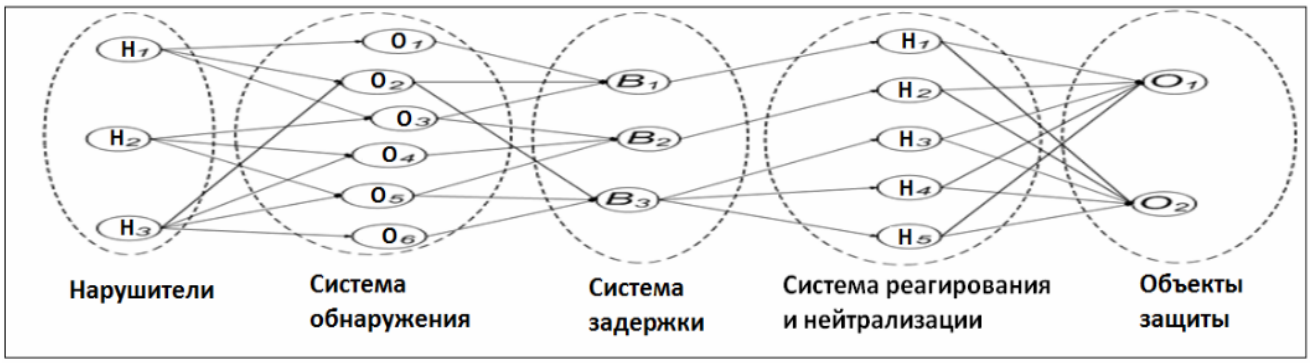


Рисунок 1.12 – Предметная область: нарушитель, СФЗ и объект защиты

С точки зрения системного анализа основным исследуемым объектом является СФЗ, а субъектом – объект охраны, который защищает СФЗ. Причем СФЗ взаимодействует с объектом охраны и находится с ним в рамках неантагонистических отношений, тогда как по отношению к нарушителю она находится в антагонистических отношениях.

Системный подход представления модели СФЗ с учетом основных элементов и их функционального взаимодействия для обеспечения безопасности приведен на рисунке 1.13.

СКУД – система контроля управления доступом; СОС – средства охранной сигнализации; СТН – средства телевизионного наблюдения; ИСО – инженерные средства охраны.

Рисунок 1.13 – Системный подход представления СФЗ

СФЗ относится к более сложным системотехническим комплексам. Они представляют собой сложную техническую систему с не полностью детерминированными связями и коллектив людей, участвующих в ее использовании. Функционально СФЗ подразделяется на подсистемы обнаружения, задержки, реагирования и нейтрализации. В свою очередь каждая из этих подсистем разбивается на более мелкие, так подсистема обнаружения включает систему внешних датчиков, систему внутренних датчиков, систему оценки сигнала тревоги, систему сбора данных о тревоге и их отображения, систему контроля на пропускном пункте.

Достаточность СФЗ определяется для всех критических элементов, находящихся на территории объекта, а также по отношению к другим элементам объекта, функционально связанными с критическими элементами.

Таким образом, объектом исследования является СФЗ, состоящая из взаимосвязанных элементов разной физической природы и характеризующаяся изменением во времени состава структуры СФЗ и их взаимосвязей для реализации своего назначения.

Например, СФЗ эволюционирует во времени: изменяется структура и состав элементов в зависимости от изменения целей защиты, изменяются характеристики датчиков обнаружения, системы сбора информации о сигналах тревоги и их оценки (увеличиваются скорости передачи данных по каналам связи) и т.д.

Диалектика развития взаимодействия угроз и объектов защиты такова, что совершенствуется технологический процесс производства, поэтому растет ценность выпускаемой продукции, а вместе с этим увеличивается потенциал потери ценности при возникновении ЧС на КВО. Как следствие этого увеличивается значимость воздействия потенциала угроз (происходит наращивание потерь от воздействия нарушителей). То есть современные КВО характеризуются увеличением опасности, так как увеличивается ущерб от возникновения ЧС.

Кроме того, у потенциальных нарушителей с развитием прогресса увеличивается степень осведомленности (совершенствуются способы и технологии получения информации) и оснащенность современными средствами и технологиями совершения несанкционированного доступа на территорию КВО.

Если на рисунке 1.12 слева представить нарушителя как потенциал угроз, а справа – потенциал защиты объекта, то для обеспечения безопасности системы их потенциалы воздействия друг на друга должны быть уравновешены. Для существования такого баланса противостояния и вводится СФЗ, которая также в диалектическом единстве развивается и совершенствуется адекватно возрастанию потенциала угроз.

Таким образом, развивается технология сложного и опасного производства, увеличивается масштаб возможных последствий ЧС, а, следовательно, и значимость воздействия угроз на КВО. В этих условиях адекватно развивается и совершенствуется СФЗ объектов. Совершенствуется СФЗ структурно, технически, организационно, функционально и строится на новых принципах и технологиях, включая в состав разнородные по физическому принципу функционирования системы и элементы. То есть СФЗ модернизируется, совершенствуется и должна соответствовать угрозам, чтобы обеспечить достаточное равновесие или необходимый запас противодействия угрозам, чтобы с заданной вероятностью исключить возможность несанкционированного проникновения нарушителей на объект.

Таким образом, вектор (градиент) потенциала угроз, воздействующих на объекты, должен быть уравновешен системой противодействия – СФЗ. В этом случае система будет устойчива и оптимальна с точки зрения минимизации затрат на обеспечение безопасного функционирования.

1.2.2 Принцип управления обеспечением достаточности защиты объектов

Достаточность защиты объекта определяется исходя из требований нормативных руководящих документов по организации и оценке защиты, наличия необходимых ресурсов и тому подобных факторов. Состояние защищенности будет достаточным, если предпринимаемые меры защиты будут соответствовать действиям возможных угроз» [36].

Безопасность определяется следующими факторами:

- состоянием хозяйственной и финансовой деятельностью предприятия;

- уровнем обеспеченности системы защиты материальными, техническими и прочими ресурсами и степенью подготовленности кадров;

- уровнем развития преступности в регионе и государстве [36].

Зависимости перечисленных факторов приведены на рисунке 1.14.

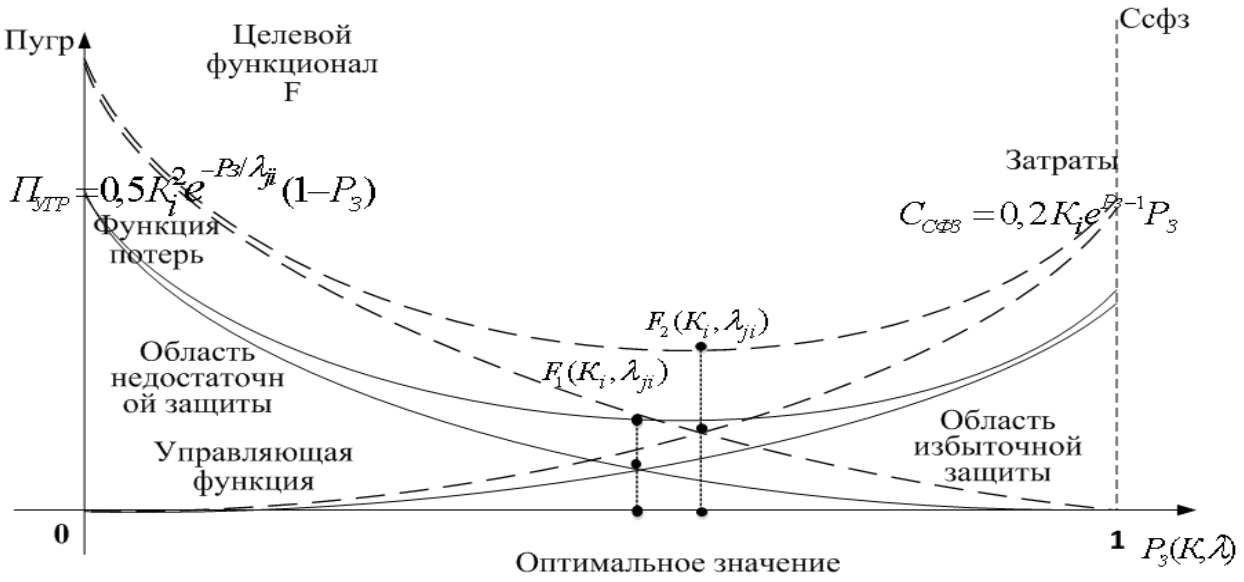


Рисунок 1.14 – Зависимость ущерба от эффективности СФЗ

На рисунке 1.14 обозначено: ось $P_3(K, \lambda)$ – вероятность защиты объекта , точка на оси зависит от категории и активности угроз λ_{ji}; ось Пугр – потери при реализации угроз; ось Ссфз – уровень затрат на СФЗ для обеспечения защищенности; P_3=1 – состояние, при котором СФЗ отражает все угрозы λ_{ji}; функции потерь – возможности угроз по нанесению ущерба; кривая F – результирующая кривая [36].

С увеличением защищенности объекта кривая затрат F на СФЗ направлена вверх. С увеличением категории (важности) объекта необходимый уровень вероятности защиты увеличивается.

Кривая функция потерь характеризует зависимость возможностей угроз по нанесению ущерба объекту K_i –ой категории от уровня его защищенности.

Кривая F – результирующая: она отражает общие потери и затраты на СФЗ в зависимости от защищенности объекта K_i -ой категории и указывает на степень достаточности защиты объекта. С увеличением категории (важности) объекта

кривая F располагается выше и правее, то есть безопасность и затраты на обеспечение безопасности возрастают.

Из рисунка 1.4 следует, что в точке минимума функции F данное состояние для объекта экономически эффективно, так как при этом обеспечивается адекватная нарушителям защита.

На участке левее от точки минимума – область указывает на преобладание возможностей сил угроз над способностями СФЗ им противостоять. Данный участок соответствует области недостаточной эффективности СФЗ и характеризуется избыточными потерями объекта.

На участке правее от точки минимума – область указывает на преобладание СФЗ над возможностями сил угроз. Данная область используется в случае, когда доминирующим требованием является обеспечение гарантированной безопасности на заданном уровне.

Анализ показывает, что существует оптимальное значение затрат на СФЗ, позволяющее минимизировать общий ущерб при нарушениях безопасности. Именно в этом смысле рассматривается задача создания экономически оптимальной СФЗ.

Таким образом, показателем качества разработки СФЗ является критерий – функционал обеспечения безопасности КВО:

$$F = П_{УГР}(P_З(K_i, \lambda_{ji})) + C_{СФЗ}(P_З(K_i, \lambda_{ji})) \to \min, \qquad (1.1)$$

где $П_{УГР}(P_З(K_i, \lambda_{ji}))$ – потери КВО K_i -ой категории от реализации угроз;

$P_З(K_i, \lambda_{ji})$ – вероятность защиты КВО K_i -ой категории;

$C_{СФЗ}(P_З(K_i, \lambda_{ji}))$ – затраты на СФЗ для реализации вероятности защиты $P_З(K_i, \lambda_{ji})$.

Для реализации данного функционала использовалась формализованная схема управления, представленная на рисунке 1.15.

Наилучшей стратегией обеспечения безопасности КВО является использование СФЗ, обеспечивающей необходимый уровень безопасности с минимальны-

ми общими затратами. Оптимальная СФЗ снижает суммарные ожидаемые потери примерно на порядок по сравнению с базовыми решениями.

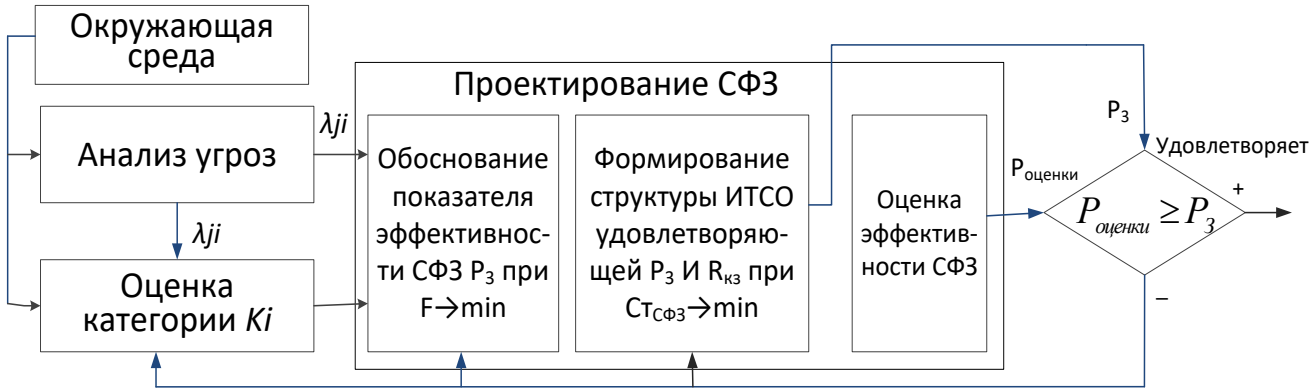


Рисунок 1.15 – Схема управления обеспечения безопасности КВО

В случае, когда доминирующим требованием является обеспечение гарантированной безопасности на заданном уровне, реализация концепции экономически оптимальной СФЗ может корректироваться в сторону избыточности защиты. Это относится, например, к защите ядерных объектов и сведений, составляющих государственную тайну и т.д.

Таким образом, изложенные принципы организации безопасности объектов позволяют осуществить анализ действующих либо вновь создаваемых СФЗ.

1.3 Системный анализ технологического процесса проектирования систем физической защиты

1.3.1 Анализ информационных процессов проектирования систем физической защиты критически важных объектов

В настоящее время существует ряд «руководящих и методических документов, определяющих перечни угроз или методику определения списка защищаемых объектов, а также характеристики моделей типовых нарушителей. При этом правила использования перечней угроз и их характеристик для формирования базовой угрозы и последующего обоснования требований к СФЗ и

формирования в его структуре интегрированного комплекса (ИК) СФЗ в этих документах отсутствуют» [16, 17, 20].

Функциональная модель этапов проектирования СФЗ представлена в виде последовательных этапов, а именно:

- категорирования объекта;

- определения базовых угроз и формирования модели нарушителя;

- выбора показателя эффективности создаваемого ИК СФЗ;

- проведения оценки эффективности разрабатываемой СФЗ и анализа уязвимости объекта;

- формирования требований к составу и характеристикам СФЗ;

- выбора и оптимизации структуры и параметров СФЗ;

- ввода в эксплуатацию СФЗ;

- модернизация ИК СФЗ при изменениях внешней среды или категории объекта.

С первым этапом тесно связан, как правило, и анализ существующей СФЗ, в частности, данные о границах охраняемых зон, рубежах защиты, о технических средствах обнаружения, наблюдения, контроля доступа, о силах реагирования, о системе связи и оповещения. Данный этап проводится с привлечением группы экспертов и является одним из трудоемких, масштабных особенно для крупных распределенных объектов.

Категорирование проводится с целью определения степени опасности объекта при условной реализации определенных «видов угроз и решается аналитическими и экспертными методами путем определения видов и масштабов ущерба (потерь). В результате классификации объект относится к определенной категории, что, в свою очередь, формирует количественные требования к эффективности СФЗ, необходимые в дальнейшем для разработки и оценки системы» [16, 17, 20].

При проектировании СФЗ КВО необходимо определить модель нарушителя, представляющего угрозу определенному объекту защиты, как совокупность

характеристик, которые формируют потенциал возможности нарушителя как интегральную характеристику опасности.

На основе полученных потенциалов нарушителей и опасности КВО при возникновении ЧС для каждого критического элемента и объекта в целом определяется базовый нарушитель, определяющий необходимый уровень эффективности СФЗ для обеспечения безопасности объекта.

Важной характеристикой нарушителя является интенсивность действий, которая характеризует время подготовки к реализации цели и является входным параметром в модель определения требований безопасности КВО.

Для формирования требований к безопасности должны быть учтены все факторы, определяющие условия функционирования СФЗ, возможные угрозы, а также обоснованный перечень требований [20].

Обоснование количественных требований сводится к решению частных задач:

- обоснование комплексного показателя потенциальных потерь объекта и его критериев;

- выбор и обоснование значений критериев эффективности СФЗ.

Достижение количественных требований СФЗ определяется выполнением качественных требований, под которыми понимаются рекомендации и правила по структуре и организации функционирования СФЗ, определенных руководящими документами.

Следующим шагом является проверка соответствия существующего ИК СФЗ заданным требованиям безопасности для данной категории объекта. С этой целью проводится анализ уязвимости объекта. Не проведение анализа уязвимости и научно обоснованных рекомендаций может привести к тому, что не будут учтены какие-либо угрозы, а в систему обеспечения безопасности вложены затраты, которые будут превышать необходимые. Анализ уязвимости объекта выполняется экспертными методами и/или методами имитационного моделирования и включает в себя:

- расчет интегрального показателя и комплексную оценку эффективности ИК СФЗ (при установленных видах угроз и приоритетах целей защиты) путем сравнения полученных расчетных данных с заданными критериями;

- разработку мероприятий по достижению заданных критериев;

- оценку (подтверждение) эффективности этих мер.

Мероприятия по достижению заданных критериев эффективности являются требованиями к структуре и функциональным параметрам разрабатываемой СФЗ и тем самым завершают этап разработки концепции создания системы.

Результатами этапа являются:

а) предложения по структуре СФЗ и содержание организационно-распорядительных документов об обеспечении безопасности объекта;

б) рекомендации по организационно-штатной структуре и предложения по организации сил реагирования объекта;

в) требования к инженерно-техническим средствам и системам, входящим в СФЗ.

Перечень руководящих документов определяют субъект анализа уязвимости. Анализ производится с привлечением специализированных организаций, имеющих в своем составе квалифицированных специалистов в различных областях знаний и располагающих специальным программно-методическим обеспечением.

Формирование концепции СФЗ – требований к составу, структуре и топологии – является самой сложной задачей при создании таких систем. Проблема формирования концепции СФЗ наименее разработана в методическом плане. Требования к оборудованию системы защиты устанавливаются ведомственными нормативными актами в отношении каждого конкретного объекта с учетом перечня угроз, результатов анализа уязвимости объекта и оценки эффективности СФЗ.

Для анализа угроз и оценки эффективности ИК СФЗ используется модель нарушителя в виде абстрактного (формализованного или неформализованного) описания нарушителя [16, 17, 20].

Одним из основных этапов проектирования СФЗ является осуществление оптимального выбора средств для формирования структуры СФЗ, при определенных ограничениях (эксплуатационных, технических, компромисса «эффективность-стоимость»).

При проектировании СФЗ объекта применяется принцип последовательных рубежей. Рациональное расположение рубежей безопасности на объекте и размещение на них технических средств защиты (обнаружения и противодействия) составляют основу физической защиты каждого объекта. Результатом этого этапа проектирования является план размещения технических средств защиты на объекте.

Прежде чем оценивать эффективность СФЗ, необходимо отметить отличительные особенности, которыми обладает СФЗ и которые влияют на оценку ее эффективности. Кратко перечислим их [37, 38]:

- действие нарушителей происходит в условиях неопределенности, то есть проектировщики имеют лишь общее представление о целях потенциального нарушителя, его тактике, стратегии, оснащенности и т.д. и эту «неопределенность» пытаются оценить с помощью различных вероятностных моделей [39], выражающихся в различных моделях нарушителей, перечнях угроз, сценариях развития конфликтных ситуаций;

- функционирование СФЗ происходит в случайные моменты времени: случайны моменты времени срабатывания датчиков; случайное время движения нарушителей, время преодоления физических барьеров и т.д.;

- трудность в организации и проведении эксперимента на объекте защиты для получения достоверных оценок. Безусловно, наилучший способ – это натурный эксперимент, однако это связано с привлечением, специально подготовленных людских ресурсов и значительных материальных средств. Вот почему чаще всего для оценки эффективности СФЗ используют компьютерные модели.

Эффективность СФЗ оценивается на последнем этапе проектирования с целью определения количественных значений показателей эффективности.

Если произвести синтез этапов проектирования, представленных в разных регламентирующих документах, то можно сформировать агрегированный технологический процесс проектирования СФЗ в виде диаграммы IDF0 (рисунок 1.16).

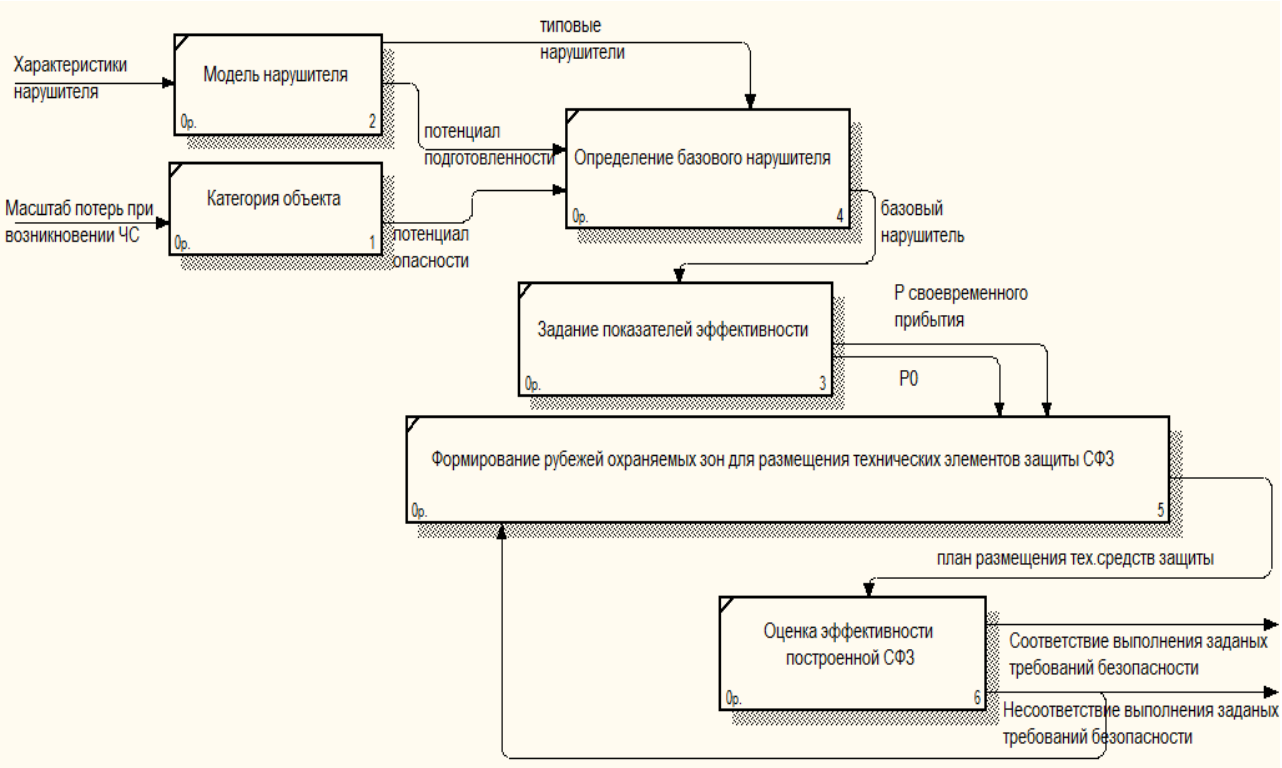


Рисунок 1.16 – Технологический процесс проектирования СФЗ

Каждый этап, в свою очередь, также представлен в виде процесса, который необходимо математически описать, то есть построить математическую модель и автоматизировать процесс моделирования с целью получения необходимых результатов для принятия управленческих решений, направленных на повышение эффективности (качества) технологического процесса проектирования СФЗ.

Таким образом, процесс разработки СФЗ – это последовательность технологически связанных этапов. Конечным этапом проектирования СФЗ является оценка параметров ее подсистем, которые сведены к характеристикам: вероятность обнаружения нарушителя и вероятность своевременного развертывания в точке упреждения сил реагирования для нейтрализации угрозы. Это позволяет исполь-

зовать известные подходы, основу которых составляют аналитические и вероятностные модели [16, 17].

Особенностью решения задачи проектирования СФЗ является:

- отсутствие достоверной информации о внешней среде, исходные данные о предметной области являются противоречивыми [21].

- аналитическое выражение и алгоритм решения задачи неизвестен или трудно формализуем, либо его решение вызывает непреодолимую трудность.

Все это приводит к необходимости разработки новых методов и информационных технологий, их объединения с традиционными методами теории поддержки принятия решений, современными методами на основе теории информации и методами синтеза сложных систем. Разрешить данные ограничения возможно путем использования новых подходов на основе последних достижений теории информации, графов, гиперграфов, методов синтеза сложных систем, имитационного моделирования и планирования эксперимента, многомерных методов статистического анализа, марковских моделей [40].

Вопросы информационной поддержки принятия управленческих решений в задаче проектирования СФЗ остаются мало исследованными. Необходимо разработать концептуальную и теоретически обоснованную методологию проектирования, оценки и анализа эффективности СФЗ.

1.3.2 Задачи, проблемы и недостатки этапов концептуального проектирования систем физической защиты критически важных объектов

Последовательно рассмотрим проблемы проектирования СФЗ.

Категория объекта определяется степенью его важности и/или опасности при возникновении ЧС. Степень важности и опасности характеризуется показателями потерь: политическими, экономическими, экологическими, людскими, культурными и информационными. Количество категорий определяет диапазон (спектр) изменения величины опасности. Возникает проблема определения количества категорий, то есть декомпозиции спектра опасности на необходимое коли-

чество категорий. При этом в совокупности категорий любые смежные категории должны значимо отличаться друг от друга по величине опасности, но внутри категории все объекты однородны. Если категорий много, то теряется значимое отличие опасности между смежными категориями. Если мало, то снижается точность определения требований к безопасности объекта. Таким образом, количество категорий должно быть обоснованно [28 - 30].

Категорирование КВО по степени их опасности на сегодняшний день является неполным, касается лишь отдельных категорий объектов. Так, по положениям п. 7 Ст. 4 ТрБ, в результате идентификации здания или сооружения оно должно быть отнесено к одному из трех уровней ответственности: повышенный; нормальный; пониженный.

В источнике [28] проведен «анализ используемых методик категорирования: методика категорирования опасных производственных объектов ФГУП НТЦ «Промышленная безопасность»; методика, изложенная в статье [28] и предложенная для включения в состав специальных технических регламентов по системам антитеррористической и противокриминальной защиты; методика общегосударственного категорирования объектов» [28] НПП «ИСТА-Системс».

В результате анализа методики статьи [28], автор делает вывод в пользу методики НПП «ИСТА-Системс», которая описана в источнике [20].

В данной методике для оценки потенциальной опасности объекта вводятся шесть частных видов и масштабов потерь. Частные виды потерь K_i: политические, людские, финансовые, экономические, экологические, культурные.

Частные виды потерь K_i определяются для шести масштабов потенциальных потерь $П_j$: локальный – 1; местный – 2; территориальный – 3; региональный – 4; государственный – 5; межгосударственный – 6.

По результатам экспертного анализа заполняется матрица категорирования (таблица 1.3).

Таблица 1.3 – Матрица категорирования объектов

Масштаб	Потери (ущерб)						
	Показатель $П_j$	Политические	Людские	Финансовые	Экономические	Культурные	Экологические
Коэффициент значимости K_i		K_1	K_2	K_3	K_4	K_5	K_6
Межгосударственный	$П_1$						
Федеральный	$П_2$						
Региональный	$П_3$						
Территориальный	$П_4$						
Местный	$П_5$						
Локальный	$П_6$						

Комплексный показатель категорирования определяется по таблице категорирования как *S*:

$$S = \sum_{i=1}^{6}\sum_{j=1}^{6} a_{ij} K_i П_j, \qquad (1.2)$$

где a_{ij} принимает значение 1 для элемента матрицы, соответствующего экспертно определенному уровню частного вида потерь (0 – в остальных случаях).

При K_i=1, $П_j$=1…6, значение *S*, определяемое по формуле (1.2), изменится от 6 (частные виды потерь локальные) до 36 (частные виды потерь межгосударственные) баллов. Показатели интегральных потерь для десяти категорий объектов представлены в таблице 1.4.

Таблица 1.4 – Критерии категорирования по уровню интегральных потерь

Категория объекта	1	2	3	4	5	6	7	8	9	10
Сумма балов S	≥33	30-32	27-29	24-26	21-23	19-20	15-17	12-14	9-11	6-8

Недостатком этой методики является то, что количество категорий и величина интервалов интегральных потерь в каждой категории одинакова и математически не обоснована. Кроме того, при определении интегрального показателя потерь учитывается вес масштаба потерь через коэффициент $П_j$=1…6, то есть линейная шкала потерь от единицы до шести вызывает сомнения из-за узкого диапазона и не согласуется с характеристиками потерь при ЧС таблицы 1.1.

Существующие математические методы классификации объектов, такие как

кластерный анализ (многомерные статистические методы), не учитывают весовой вклад характеристик в оценку критерия классификации и не позволяют оценить значимо ли различие между классами в полученной их структуре классов. Методы оценки значимого различия между группами с использованием теории статистических гипотез на основе критерия Хотеллинга, Вилкоксона лишены последнего недостатка, однако также не учитывают весовой вклад характеристик в оценку потенциала опасности категории объекта. Кроме того, данные методы используют, когда структура классов уже сформирована. Иерархический метод Саати определяет весовые значения классов на основе парных сравнений, но в нем так же, как в кластерном анализе, нет критерия значимого различия классов.

Методы распознавания образов, например, на основе нейронных сетей используются, когда уже сформированы классы (образы) как обучающая выборка.

В настоящее время задача категорирования объектов решается, как правило, экспертными методами с использованием искусственного интеллекта. Группа экспертов определяет требуемую величину безопасного состояния объекта. При этом нет строгого критерия значимости различия по величине опасности смежных категорий КВО.

Таким образом, в существующих методах категорирования не обосновано количество категорий, нет сравнительной оценки комплексной опасности различных категорий объектов и не проводится анализ значимости различия категорий объектов.

Определив категорию объекта, формируется модель нарушителя. Каждый нарушитель имеет множество характеристик, которые определяют потенциал его подготовленности и опасности как возможность (способность) преодоления СФЗ. Приказом министра промышленности и энергетики и постановлением правительства № 875 от 29.08.2014 «Об антитеррористической защищенности объектов ФСТЭК...» установлены характеристики типовых нарушителей (таблица 1.2). Комплексной характеристикой нарушителя является интегральный показатель – потенциал опасности нарушителя, при определении которого возникает проблема сведения множества разнородных характеристик к единому оценочному потен-

циалу. В настоящее время сравнительная оценка типовых нарушителей проводится только по отдельным характеристикам: по скорости перемещения, по преодолению физических барьеров и по затруднению обнаружения и т.д. [42, 43].

В настоящее время вопросы формирования моделей типовых нарушителей (ТН) решаются в основном на вербальном уровне экспертными методами [20], где присутствует элемент субъективизма, или на основе теории нечеткой логики и нечетких гиперграфов [21]. Кроме того, не производится анализ связи характеристик и оценка их весового вклада в формирование потенциала опасности ТН и не производится оценка интервала времени прогнозирования интенсивности действий террористических угроз.

Необходимо на основе МГК проанализировать связь характеристик ТН и с использованием информационно-вероятностного метода оценить их потенциал опасности. По результатам оценки предложить соответствующий уровень эффективности СФЗ для защиты от ТН. Данная задача решается для дифференцирования необходимых требований при определении величины эффективности СФЗ от воздействия типовых нарушителей.

При проектировании СФЗ на перспективу необходимо прогнозировать изменение параметров террористических угроз на определенный промежуток времени. Существует множество математических методов, которые позволяют прогнозировать поведение параметров системы во времени [44]. Однако методов оценки глубины прогнозирования развития систем крайне мало. Среди них марковские модели, которые позволяют определять время наступления предельных вероятностей переходов состояний в системе для однородной марковской цепи, но для решения этой задачи метод не подходит.

Определив категорию объекта и потенциалы опасности типовых нарушителей, необходимо решить задачу определения базового нарушителя для критических элементов КВО.

В настоящее время эта задача решается, как правило, экспертными методами с использованием искусственного интеллекта. Группа экспертов определяет базового нарушителя для каждой категории объектов.

Для оценки функционирования СФЗ необходимо выбрать показатель эффективности, который наиболее полно характеризовал степень безопасного состояния объекта, и обосновать критерий эффективности функционирования подсистем СФЗ. Задача СФЗ – обеспечить заданный уровень безопасного состояния объекта.

Вопросы задания критерия эффективности СФЗ в настоящее время в основном решаются экспертным путем. В некоторых источниках применяют линейную шкалу распределения значений показателя эффективности.

Анализируя данные методики, автор статьи [28] изложил основные положения методики НПП «ИСТА-Системс», которые описаны в [20]. В этом источнике определена методика задания требований к СФЗ. В качестве критерия эффективности СФЗ взят показатель – вероятность своевременного пресечения несанкционированных действий нарушителя и обосновывается шкала критерия эффективности СФЗ в зависимости от номера категории объекта. За нижнюю оценку принята вероятность обнаружения ультразвуковых извещателей с учетом характеристик надежности (0,6…0,7). За верхнюю оценку принято значение 0,95 - величина, близкая к предельному значению. Для оценки вероятности пресечения действий нарушителя остальных категорий объектов используют следующую аппроксимирующую формулу:

$$\Delta P_{np(i+1)} = (1 - \Delta P_{npi})\, k\,, \qquad (1.3)$$

где $P_{np(i+1)}$ – приращение вероятности пресечения для СФЗ $(i+1)$- й категории объекта;

ΔP_{npi} – вероятность пресечения для СФЗ i-ой категории объекта;

k – эвристически подобранный коэффициент (шаг приращения), равный 0,15.

С учетом изложенного выше вероятности пресечения для десяти категорий объектов представлены в таблице 1.5.

Таблица 1.5 – Критерии эффективности СФЗ для категорий объектов

Категория объекта	10	9	8	7	6	5	4	3	2	1
Значение вероятности пресечения нарушителя	0,7	0,75	0,79	0,82	0,85	0,87	0,89	0,91	0,93	0,95

В данной методике ничем не обоснована последовательная линейная шкала в определении величин показателя эффективности для последующих категорий. Кроме того, недостатком данной методики является то, что величина вероятности пресечения угрозы 0,95 для первой категории объектов далеко не близкая к предельной. По мнению автора, близкой к предельной является величина 0,999 (для объектов наивысшей важности).

Широкий анализ показателей эффективности проведен в монографии А. С. Боровского [21]. Из множества показателей выбран показатель эффективности, характеризующий степень выполнения СФЗ функционального назначения, вероятность нахождения объекта охраны в безопасном состоянии, введенный В. В. Никитиным [43]. Таким образом, вероятность нахождения объекта защиты в безопасном состоянии (вероятность защиты объекта) определим как произведение вероятностей выполнения своей задачи каждой из составляющих СФЗ: системы обнаружения, задержки, реагирования и нейтрализации нарушителя:

$$P_З = P_О \cdot P_{СВП} \cdot P_Н, \tag{1.4}$$

где $P_О = P_Д \cdot P_{ОЦЕН} \cdot P_{БР}$ вероятность обнаружения нарушителя, зависит от: $P_Д$ – вероятности обнаружения средствами наблюдения; $P_{ОЦЕН}$ – вероятности оценки истинности сигнала оператором; $P_{БР}$ – вероятности безотказной работы системы связи;

$P_{СВП}$ – вероятность своевременного прибытия сил реагирования в точку перехвата при условии обнаружения нарушителя;

$P_Н$ – вероятность нейтрализации нарушителя при условии своевременного прибытия сил реагирования – показатель не исследуется. При этом стоимость размещения и обслуживания ИТСО должна стремиться к минимуму.

Показатели $P_О$ и $P_{СВП}$ в совокупности определяют величину эффективности СФЗ, то есть один и тот же уровень защищенности объекта можно получить при множестве разных комбинаций значений величин $P_О$ и $P_{СВП}$ – это особенность формирования требований к эффективности СФЗ.

Как определить и обосновать величины частных показателей? Для обоснования требований частных показателей эффективности СФЗ необходимо разработать имитационную модель функционирования процесса обнаружения нарушителя и действий сил реагирования и на ее основе разработать метод задания частных показателей эффективности.

В настоящее время на первое место выдвигаются информационные показатели оценки эффективности СФЗ. Данные показатели эффективности должны характеризовать степень информационного превосходства СФЗ над информационным потенциалом нарушителя.

В этой связи предлагается один из подходов к обоснованию величины показателей эффективности СФЗ для различных категорий объектов на основе информационно-вероятностного метода и концептуальной модели функционирования СФЗ.

Следующим этапом проектирования является проблема формирования оптимального варианта размещения ИТСО на объекте, удовлетворяющем требованиям величины безопасного состояния объекта. Особенность решения задачи – размещение технических средств наблюдения должно обеспечить своевременное обнаружение нарушителя на всех путях проникновения при минимальной стоимости затрат.

Вопросы синтеза элементов СФЗ с использованием логико-вероятностных методов (ЛВМ) рассматривались в статьях [37, 45], делался акцент на большую трудоемкость ЛВМ [45, 46].

Данные вопросы исследованы в недостаточной степени. В настоящее время для решения задачи используется математический аппарат искусственного интеллекта.

Решение задачи осложняется, если объект защиты состоит из разных по важности или опасности критических элементов при возникновении ЧС. В этой части проектирования решается задача декомпозиции системы, синтеза и оптимизации размещения ИТСО с целью обеспечения заданных требований безопасности критических элементов.

Важным этапом проектирования СФЗ является оценка эффективности функционирования СФЗ, то есть оценка возможностей по пресечению проникновения нарушителя. Вопросам оценки эффективности посвящено большое количество работ. Первая проблема – необходимо оценить эффективность СФЗ по всем возможным путям проникновения нарушителя. Причем, оценка каждого пути – это результат моделирования противодействия систем (обнаружения, задержки, реагирования и нейтрализации) физической защиты проникновению нарушителя. Вторая проблема: как оценить общий показатель эффективности противодействия в целом по всем маршрутам проникновения.

В настоящее время существует несколько методов оценки эффективности СФЗ [37]:

- детерминистический подход;

- логико-вероятностный метод;

- вероятностно-временной метод.

Детерминистический метод имеет строгую последовательность процедур, содержащихся в регламентированных документах.

Для каждого фактора состояния разработана аналитическая модель, так для оценки организационных мероприятий модель имеет вид:

$$N_{орг} = \frac{\sum_{i=1}^{k} a_i d_i}{d_m k a_m}, \qquad (1.5)$$

где k – число показателей состояния в организационных мероприятиях;

a_m – максимально возможное значение веса показателя состояния;

d_m – максимально возможное значение показателя реального состояния;

a_i – значение веса показателя состояния для оценки i-го организационного мероприятия, назначенного экспертом;

d_i – показатель реального состояния i-го организационного мероприятия, назначенного экспертом.

Интерпретация результатов решения модели следующее – СФЗ в основном соответствует требованиям норм и правил, если $N \leq 0{,}05$.

Аналогичные модели разработаны для оценки эффективности инженерно-технических средств и действий подразделений охраны.

Логико-вероятностный метод широко используется для оценки живучести, устойчивости, надежности, эффективности, технического риска структурно-сложных систем [45 - 47].

Метод включает следующие четыре этапа [46]:

- постановка задачи моделирования путем построения специальной структурной схемы функциональной целостности – представляется в виде графа с использованием специальных изобразительных средств – схем функциональной целостности;

- определение логической функции работоспособности системы;

- построение многочлена расчетной вероятностной функции;

- вычисление вероятностных показателей системы.

В качестве аналогов данному методу можно отметить:

1) метод деревьев отказов (FTA), который заключается в построении и анализе модели безопасности, представляющей собой логико-вероятностную модель причинно-следственных связей отказов исследуемой системы с отказами ее элементов и прочими воздействиями; суть его заключается в отыскании оптимального решения, по возможности снижающего вероятность несчастного случая; дает информацию о том, как наиболее эффективно следует распределить средства, чтобы получить наибольший экономический эффект от их вложения;

2) метод деревьев событий (ETA) – индуктивно-логический метод для идентификации различных последствий аварийной ситуации; метод основан на дискретизации развития аварийной ситуации в нескольких событиях; последствия аварийной ситуации определяются на основе вероятности реализации определенного сценария развития аварии.

Для моделирования и автоматизации расчетов надежности и безопасности систем разработаны программные комплексы (ПК): ПК, разработанный ОАО «СПИК СЗМА» АСМ СЗМА; ПК Risk, разработанный в ОЦРК Минатома РФ под руководством профессора Р. Т. Исламова и CRISS, разработанный в ОКБМ

им. Африкантова под руководством А. М. Бахметьева; ПК Risk Spectrum – компания Relcon Teknik AB, Швеция и SAPFIRE – комиссия ядерного регулирования США.

Применительно к данной предметной области целью исследования является определение степени риска – вероятностной величины, характеризующей возможность невыполнения СФЗ своего функционального назначения [37].

Алгоритм метода:

- формируется сценарий развития опасной ситуации в виде графа (в виде деревьев) [16,46,47, 50];

- определяется функция опасности системы $y(z_1,\dots z_n)$, которая заменяется вероятностной функцией $P\{y(z_1,\dots z_n)\}$;

- определяется значение вероятностной функции в предположении реализации опасного события $Y(y)=P\{y(z_1,\dots z_n)=1\}$.

В научной литературе [49] приведен пример использования логико-вероятностного подхода для оценки эффективности СФЗ.

Вероятностно-временной метод подробно изложен в литературе [16]. Остановимся кратко на его сущности. СФЗ успешно выполняет свои функции только в случае, если время защиты меньше времени, необходимого нарушителям для выполнения своей цели. Для этого анализируются маршруты движения нарушителей и сил реагирования для каждой цели. Оценивается время, необходимое нарушителям для преодоления физических барьеров, для движения по территории объекта, для совершения акции и т.д. Для сил реагирования оценивается время сбора, время движения и осмотра участка периметра, на котором сработала сигнализация и т.д. Безусловно, все эти показатели являются случайными величинами. Поэтому в моделях оценки эффективности СФЗ данные показатели представляются случайными величинами, имеющими среднее значение со стандартным отклонением. Использование стандартного отклонения позволяет учесть то, что нарушителям и силам реагирования требуется не всегда одинаковое время для выполнения задачи. В настоящее время данная методика используется в разработанных компьютерных программах оценки эффективности СФЗ: EASI (Estimate of Adver-

sary Sequence Interruption), ASSESS (Analytic System and Software for Evaluating Safeguards and Security) [50], разработанных в США; СПРУТ (НПП «ИСТА-Системс», Россия), Вега-2 (ФГУП «СНПР - Элерон», Россия) [51 - 53].

Так, например, в программном комплексе «Вега-2» при оценке рассматривается последовательность преодоления нарушителем физических барьеров. Последовательность проникновения нарушителя оценивается временем преодоления барьеров, вероятностью обнаружения до преодоления барьеров, вероятностью обнаружения после их преодоления [51]. Такие же сценарии последовательности действия разрабатываются и для сил реагирования. В программном комплексе СПРУТ в качестве входных данных для моделирования должны быть заданы вероятностные и временные параметры для каждого участка маршрута нарушителя и также задаются временные параметры прибытия сил реагирования и нейтрализации к рубежам, к которым предусмотрено их своевременное прибытие с момента получения сигнала тревоги [41].

Таким образом, существующие специализированные программные комплексы (EASI, ASSESS, SAFE, СПРУТ, Вега-2) в основном используются только на этапе анализа эффективности уже спроектированных СФЗ.

Оценке эффективности СФЗ посвящено много научных статей, в которых рассматривается несколько подходов к оценке эффективности [54 - 63]. Например, А. В. Леус предлагает показатели оценки эффективности и математическую модель на основе трехмерного куба [54]. Достоинство метода: при оценке вероятности безопасного состояния используется логарифмическая функция, позволяющая перейти к сложению показателей защищенности объекта. Это удобно при анализе эффективности СФЗ. С. И. Корчагин предлагает методику оценки СФЗ с помощью вероятностного подхода. Достоинство: в модели осуществляется переход к одномерной структуре комплекса, за счет этого упрощаются расчеты оценки эффективности СФЗ[55]. С. С. Звежинский рассматривает эффективность охранной сигнализации для малых объектов[56]. При оценке эффективности учитывается важность критических элементов путем введения коэффициента важности в

целевую функцию оценки рационального расположения ИТСО на рубежах охраны.

Оценка эффективности СФЗ с использованием логико-вероятностных методов (ЛВМ) рассматривается в статьях О. А. Панина [37, 45], где делается акцент на большой трудоемкости ЛВМ. Полученные результаты комплексной оценки СФЗ по данной методике [45] занижают показатель защищенности общей системы.

Подводя итог, можно сделать вывод: при детерминистическом подходе за эффективность принимается степень выполнения требований по физической защите в соответствии с нормативными документами. В логико-вероятностном методе под эффективностью понимают вероятность нахождения системы в безопасном состоянии согласно построенному сценарию развития опасной ситуации. При вероятностно-временном методе под эффективностью понимается вероятность того, что у сил реагирования резерв времени окажется больше нуля.

В случае подтверждения эффективности СФЗ, производится формирование организационных структур. Проблемы формирования структур: оценки информационной нагрузки на каждый элемент управления организационной структуры; получение структуры, в которой оптимальна информационная нагрузка на элементы по горизонтали и вертикали организационной структуры. Сейчас эти вопросы решаются без применения и обоснования критериев эффективности, а также использования какого-либо математического аппарата. Как правило, построение структур – это волевое принятие решений экспертов в данной области.

«Криминальная эффективность» в отношении критически важных элементов информационной сферы настолько высока, что угрожающая тенденция их безопасности очевидна.

Отсюда все более актуальной становится проблема обеспечения безопасности критически важных элементов информационной сферы. Очевидно, что решение этой проблемы должно осуществляться системно на основе исследования технологий обеспечения безопасности информационной сферы [56 - 57].

В системном плане совокупность средств, реализующих данные технологии, представляет собой систему противодействия угрозам безопасности. То об-

стоятельство, что она характеризуется множеством свойств, относит вопросы ее исследования к числу сложных как в научном, так и в практическом плане.

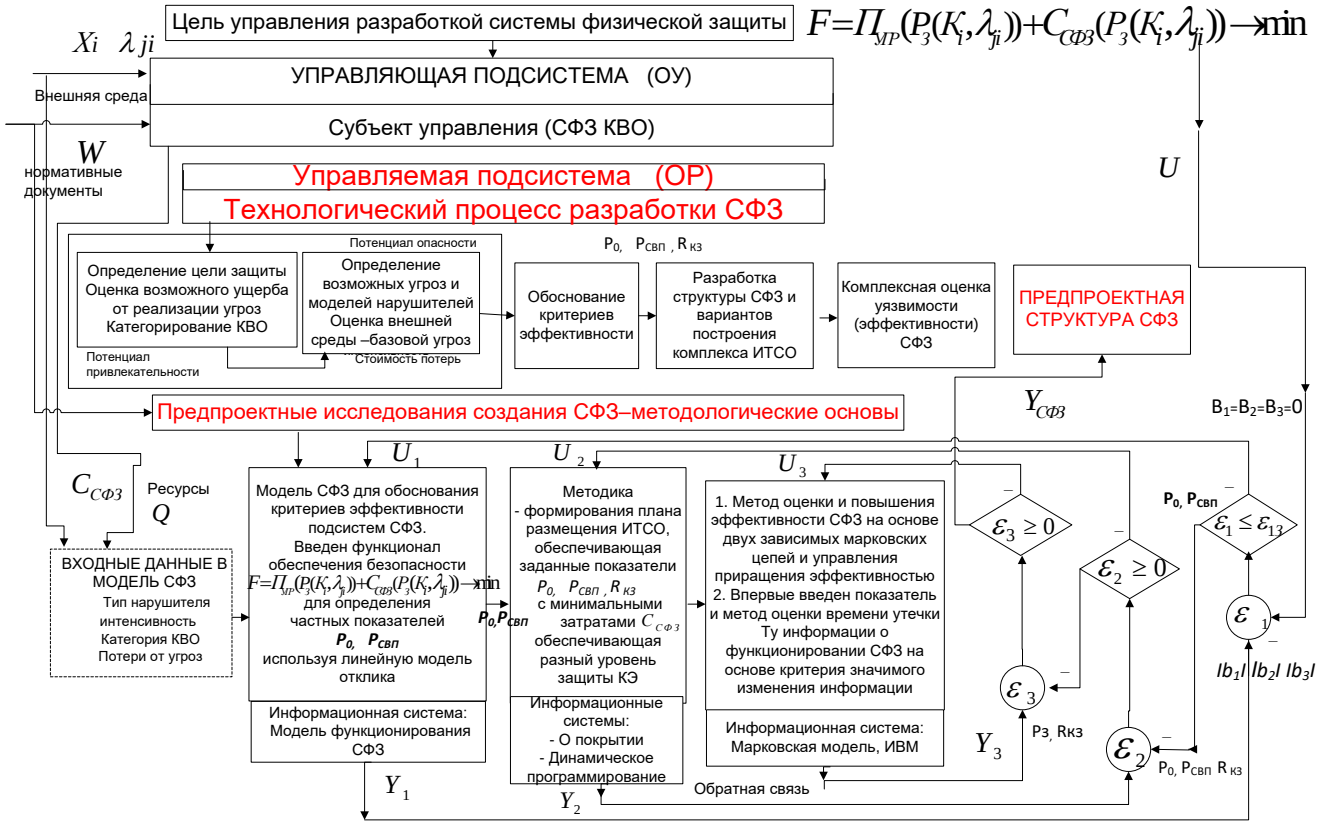
Важность данных процессов и последствия нарушения их функционирования на КВО выдвигают задачу их защиты от деструктивных действий нарушителей, и в первую очередь – защиту от утечки конфиденциальной информации [54 - 57].

Поэтому важной характеристикой СФЗ является временной интервал утечки информации об организации защиты КВО. Возникает задача оценки временного интервала утечки информации, которая определяет интенсивность действий (время подготовки) угрозы, то есть нарушитель, прежде чем совершить проникновение, должен подготовиться – получить информацию о структуре и организации СФЗ КВО. Скорость утечки информации и определяет время подготовки нарушителя к действию. По результатам оценки определяются управленческие решения по обновлению системы доступа к критическим элементам объекта [64].

Данная задача регламентируется руководящими документами в части определения, что такое утечка информации, и актуальности решения задачи минимизации утечки информации. Однако нормативных показателей и методического аппарата решения задачи оценки времени утечки информации не существует.

Перспективным направлением исследований будет создание средств выработки управленческих решений на всех этапах проектирования СФЗ, ориентированных на использование методов системного анализа: а именно систем, основанных на информационных оценках ситуаций, многомерных методах обработки информации, методах декомпозиции и синтеза систем, имитационных моделей и теории эксперимента.

Исходя из анализа предметной области, безопасность КВО обеспечивается СФЗ, эффективность которой определяется качеством управления технологического процесса ее создания. Поэтому была разработана схема обеспечения управления проектированием СФЗ на этапе предпроектных исследований, представленная на рисунке 1.17.



W – нормативные документы (решения совета безопасности, ГОСТы, приказы ФСТЭК, ведомственные требования и др.); Q – ресурсы; U_i – управляющее воздействие (управляющие решения – прямая связь); Y_i – выходная информация, характеризующая состояние объекта управления (обратная связь); Yсфз – выходные параметры модели; *b1, b2, b2* – параметры функции потерь; *Po, $P_{СВП}$, Rкз* – показатели эффективности подсистем СФЗ; *Рз* – показатель эффективности СФЗ; ε_i – ошибка; ε_{i3} –заданное значение.

Рисунок 1.17. – Управление проектированием СФЗ на этапе предпроектных исследований

1.4 Цели и задачи исследования

Цель исследований – разработка новых научно-технических и технологических решений в задачах проектирования СФЗ, направленных на создание методик, моделей и методов повышения уровня обоснованности принимаемых управленческих решений для обеспечения необходимой безопасности КВО.

Для достижения поставленной цели необходимо решить следующие задачи:

1. Посредством системного анализа, формализации и постановки задачи обеспечения безопасности КВО при управлении проектированием СФЗ разработать методологические основы исследования процесса создания СФЗ.

2. Разработать методики, использующие информационный критерий оптимального развития систем для решения задач:

2.1 категорирования КВО по критерию значимого различия потенциальной опасности объектов;

2.2 оценки опасности нарушителей по энтропийному показателю;

2.3 определения базовых нарушителей для категорируемых объектов;

2.4 оценки изменения активности внешней среды (нарушителей) во времени.

3. Разработать модель обоснования критериев эффективности подсистем СФЗ: обнаружения, задержки, реагирования и нейтрализации, на основе градиентного смещения плана эксперимента в минимум функции риска.

4. Разработать методику размещения и выбора ИТСО объекта, обеспечивающую заданные критерии эффективности СФЗ, предложенные в п. 3.

5. Разработать методику объединения технических средств обнаружения в группы для формирования структуры организационного управления по критерию оптимальной информационной нагрузки.

6. Разработать методы оценки эффективности СФЗ и выработки управленческих решений по результатам ее оценки:

6.1 метод оценки и повышения эффективности СФЗ на основе двух зависимых марковских цепей;

6.2 метод оценки времени утечки информации о функционировании СФЗ на основе критерия значимого изменения информации.

ГЛАВА 2 ИНФОРМАЦИОННО-ВЕРОЯТНОСТНЫЙ МЕТОД ОЦЕНКИ ОПАСНОСТИ ОБЪЕКТОВ ЗАЩИТЫ ПРИ ВОЗНИКНОВЕНИИ ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЙ

2.1 Методика категорирования объектов на основе универсального информационно-вероятностного метода

При анализе методик категорирования выявлены проблемы и недостатки применяемых математических методов (п. 1.3.3) и на этой основе разработан информационный подход к решению данной задачи.

Автором предлагается использовать ИВМ декомпозиции множества объектов на значимо различные классы по обобщенному энтропийному критерию (при этом каждый объект описывается множеством разнородных характеристик), то есть метод формирует значимо различимые классы объектов. Метод учитывает значимость вклада характеристик при формировании энтропийного потенциала классов объектов за счет введения оценок П. Фишборна [67]. Достоинством метода - значимо различные категории объектов формируются на основе критерия оптимального соотношения порции преемственности энтропии между смежными категориями, который выступает как информационная мера значимого развития опасности категории объектов.

Категорирование объектов осуществляется на концептуальном уровне по интегральному масштабу опасности объекта при ЧС без анализа функциональной структуры объекта.

Математический аппарат модели опирается на положения, изложенные в трудах профессора А. Ю. Мушкова, В. А.Тихомирова [68].

Постановка задачи. На основе ИВМ произвести декомпозицию генеральной совокупности объектов на значимо различающиеся по степени опасности множества объектов, характеризующиеся разнородными параметрами частных видов потерь, то есть классифицировать по категориям опасности. При этом внутри каждой категории объекты по опасности должны быть однородны.

Меру организованности любой системы можно описать с помощью энтропии [67, 68]. Аналогично - степень потенциальной опасности объекта при возникновении ЧС опишем в виде потенциала опасности – энтропии.

Решение задачи. Ситуация оценки потенциалов опасности объектов характеризуется таблицей, у которой столбцы образованы множеством объектов, нарастающих по степени опасности, а строки – множеством признаков, характеризующих опасность объекта при возникновении ЧС.

Используется схема формализованного расчета существующей системы вероятностных оценок. В соответствии с принципом максимума неопределенности эта оценка получена в результате решения задачи на условный экстремум:

$$H(P) = -\sum_{j=1}^{m} p_j \lg p_j \rightarrow \max, \qquad (2.1)$$

$$\sum_{j=1}^{m} p_j = 1, \qquad (2.2)$$

$$\prod_{j=1}^{m} r^{p_j} = const. \qquad (2.3)$$

Выражение 2.1 – энтропия Больцмана-Шеннона, выступающая в качестве меры неопределенности, выражение 2.2 - условие нормировки, а 2.3 определяет постоянство среднегеометрического показателя:

$$r_{ji} = \sum_{i=1}^{n} r_{ji}. \qquad (2.4)$$

Решение задачи нахождения максимума функции (2.1) при ограничениях (2.2 -2.3) с использованием метода неопределенного множителя Лагранжа позволяет получить зависимость вектора потенциального распределения вероятностей для определения из множества рассматриваемых ситуаций (объектов) в виде векторов $R^n : K = (x_1, x_2, ..., x_n) \in R^n$ наилучшего решения. То есть для данного класса векторов существует наилучшее решение: вектор $\vec{X}_m$ - нулевая гипотеза H_0, которая принимается при заданном уровне значимости. Следовательно, ре-

шение данной задачи связано с вычислением вектора $\overline{X}_m$, количественно определяющего потенциал опасности объекта и оценкой уровня значимости $\alpha_o^{Э\Phi}$ и мощности критерия $\beta_o^{Э\Phi}$ принятия решения.

Входная информация представлена в виде двумерного пространства:

- имеется множество *n* опасных объектов;

- каждый объект имеет множество *m* характеристик, определяющих потенциал опасности объекта.

Таким образом, декомпозиция множества объектов на категории (формирование категорий на множестве объектов) характеризуется таблицей 2.1 (входных данных), у которой столбцы образованы множеством различной опасности объектов $\{A_i\}$, i=1, …,n, а строки образованны множеством характеристик, формирующих потенциал опасности объектов x_j, j=1, …, m.

Таблица 2.1 – Входные данные

Характеристики объектов	Множество опасных объектов				
	$\{A_1\}$	…	$\{A_i\}$	…	$\{A_n\}$
X_1	X_{11}	…	X_{1i}	…	X_{1n}
…	…	…	…	…	…
X_j	X_{j1}	…	X_{ji}	…	X_{jn}
…	…	…	…	…	…
X_m	X_{m1}	…	X_{mi}	…	X_{mn}

Вклад характеристик в формирование потенциалов опасности объектов характеризует меру уверенности в ситуации неопределенности и определяется в виде распределения вероятностей P_{ji}. Характеристики исследуемых объектов $\{X_{ji}\}$ могут задаваться как в единых шкалах, так и в различных физических шкалах. Для приведения характеристик $\{X_{ji}\}$ к единой общей шкале использовали нормализацию относительно экстремальных значений $\{X_{ji}\}$ без смены ингредиента для максимальных значений:

$$r_{ji} = x_{ji} / x_{\max j}, \qquad (2.5)$$

со сменой ингредиента на противоположный для минимальных значений:

$$r_{ji} = x_{\min\, j} / x_{ji}\,. \qquad (2.6)$$

В результате чего перешли к шкалам в интервале $x_{ji} \to r[0,1]$. Таким образом, выражения (2.5) и (2.6) позволили перейти в другое измерение пространства (таблица 2.2), имеющее нормализацию в единых шкалах в интервале [0,1].

Таблица 2.2 – Нормированная матрица

Характеристики объектов	Множество опасных объектов				
	$\{A_1\}$	…	$\{A_i\}$	…	$\{A_n\}$
X_1	r_{11}	…	r_{1i}	…	r_{1n}
…	…	…	…	…	…
X_j	r_{j1}	…	r_{ji}	…	r_{jn}
…	…	…	…	…	…
X_m	r_{m1}	…	r_{mi}	…	r_{mn}

Элементы r_{ji} поля матрицы будем определять с элементарными событиями. Нормированная мера r_{ji} будет соотноситься с вероятностью $p(r)$, которая отождествляется с понятием элементарного потенциала. Определение меры введено для того, чтобы интерпретировать понятие вероятность. Следует отметить, что понятие вероятность совмещает в себе меру возможности наступления события и степень уверенности в появлении событий.

При формализации задачи множество объектов охраны определим как события {A}, а множество их характеристик как события {x}.

Связь между характеристиками, формирующими потенциал опасности объекта, осуществляется через нормированную меру, которая отождествляется с вероятностью $p(a)$. Распределение структуры вероятностей $p(a)$ позволяет произвести оценку нулевой гипотезы H_0 при заданном уровне значимости $\alpha_o^{\Э\Ф}$ и мощности критерия $\beta_o^{\Э\Ф}$ принятия решения.

Процесс накопления информации приводит к уменьшению неопределенности, а количество информации при наступлении события связано с вероятностью его появления.

В схему оценки опасности объектов введем понятия: априорные, апостериорные и условные вероятности, а так же определим условную вероятность $p(r)$, как величину влияния *j*-ой характеристики объекта на формирование потенциала опасности объекта при условии, что события состоялись.

Для оценки величины $p(r)$, используем то, что оценки потенциалов событий $\{r\}$ отождествляются с функцией принадлежности, которая определяет каждому r действительное число в интервале [0,1]. Функция имеет вид:

$$p_{ji}(r) = r_{ji} / \sum_{i=1}^{n} r_{ji}. \qquad (2.7)$$

Фоменюком В.В. определен принцип “потенциального распределения вероятностей”, который позволяет оценить вероятность влияния *j*-ой характеристики объекта на формирование его потенциала опасности. Понятие потенциального распределения вероятностей имеет вид:

$$\hat{p}_j(r) = \sum_{i=1}^{n} r_{ji} / \sum_{j=1}^{m}\sum_{i=1}^{n} r_{ji}. \qquad (2.8)$$

В основе принципа потенциального распределения вероятностей заложено то, что с большей вероятностью предпочитаются те характеристики объекта (системы), которые имеют больший вклад в значение оценочного потенциала опасности объекта.

При формировании оценочных потенциалов опасности объектов весовой вклад характеристик различен. Априорное распределения весовых значений вероятности p_j связано с отношением порядка, которое исследовано в трудах П. Фишборна и образует арифметическую прогрессию: $\check{p}_j = 2*(m-j+1)/m*(m+1)$.

Вводя априорную вероятность в модель потенциального распределения вероятностей (2.8) и теорему Байса, учитывается различный вес характеристик в

формировании оценочного потенциала путем объединения априорной и апостериорной вероятности, получаем распределение условных вероятностей:

$$P_j = \sum_{i=1}^{n} r_{ji} \overset{\vee}{p}_j \Big/ \sum_{j=1}^{m}\sum_{i=1}^{n} r_{ji} \overset{\vee}{p}_j . \qquad (2.9)$$

Вероятность влияния *j*-ой характеристики в формировании оценки потенциала *i*-го объекта определим на основе теоремы Байеса, в которой обращается порядок утверждений условных вероятностей, то есть связываются $p_{ji}(r)$ и p_j. Вероятность $p(a)$ вычисляется:

$$p_{ji}(a) = p_{ji}(r) \cdot p_j \Big/ \sum_{i=1}^{n} \sum_{j=1}^{m} p_{ji} \cdot (r) p_j . \qquad (2.10)$$

Определим ошибки первого и второго рода в интерпретации нашей задачи.

Допустить *ошибку первого рода* - отвергнуть гипотезу H_o, когда она верна. Такая ошибка ($\alpha_o^{\Im\Phi}$) называется уровнем значимости, которая характеризует риск получить большое количество категорий, с незначительным изменением опасности объектов внутри категории.

Если $\alpha_o^{\Im\Phi}$ увеличивать, то увеличивается вероятность получить смежные категории объектов с рангами опасности значимо не различимыми. При этом очевидно, что риск проектировщика тем выше, чем меньше степень упорядоченности и организации рассматриваемой системы (ситуации), характерной для варианта категории объектов.

Допустить о*шибку второго рода* – принять гипотезу H_o, когда она неверна. Ошибка второго рода ($\beta_o^{\Im\Phi}$) характеризует риск заказчика.

Заказчик рискует, если система обладает низкой степенью упорядоченности и организации, однако он также рискует, когда система обладает низкой степенью приспособляемости к изменению внешних условий. Ошибка второго рода характеризует еще и степень порции энтропии преемственности от смежной категории объектов (в какой мере смежные категории разнородны).

Если $\beta_o^{ЭФ}$ увеличивать, то увеличивается вероятность получить категорию с неоднородными по опасности объектами внутри самой категории, то есть потенциалы опасности крайних (граничных) объектов в одной и той же категории будут значимо отличаться.

Измерение степени упорядоченности и организации системы осуществляется посредством оценки количества энтропии. Величину неопределенности опишем энтропией К. Шеннона: $H_i(p) = -\sum_{j=1}^{m} p_{ji}(a) \lg p_{ji}(a)$. Принимается та гипотеза, которой соответствует меньшее значение величины:

$$\alpha_i^{ЭФ} = H_{best}(p) - H_i(p), \tag{2.11}$$

где $H_{best}(p)$ – значение энтропии гипотетического объекта, обладающего оптимальными характеристиками для данной информационной ситуации;

$H_i(p)$ – значение энтропии для *i*-го варианта опасности объекта.

Количество в системе информации I_i равно ровно уменьшению энтропии $\Delta H_i(p)$. При этом разность между максимальной энтропией $H_{\max}$ и энтропией $H_i(p)$, и есть количество информации I_i, накопленной в данной системе:

$$I_i = H_{\max} - H_i(p). \tag{2.12}$$

Максимальная энтропия определяется из условия, когда вес характеристик одинаков (события равновероятны) в формировании потенциала опасности объекта при возникновении ЧС.

Чтобы система в процессе своего развития не достигла предела «приспособленности» она должна сохранять в себе непредсказуемость, характеризуемую определенной порцией преемственности энтропии. Удельный вес порции преемственности определяется:

$$G_H^i = H_i(p) / I_i. \tag{2.13}$$

В результате анализа большого количества работ из различных научных областей доказано существование оптимального значения величины G_H. Оптималь-

ное значение порции энтропии для технических систем составляет $G_H^{ОПТ} = 0{,}272$, а интервал изменения величины составляет $0{,}25 \le G_H^{ОПТ} \le 0{,}30$ – это интервал наилучшего соотношения непредсказуемости и детерминированности.

Значение энтропии $H_{best}(p)$ определялось при условии $G_H^{ОПТ} = 0{,}25$.

Чем больше расчетная величина G_H^i отличается от оптимального значения, тем выше вероятность принятия гипотезы H_o, когда она не верна. Поэтому ошибка второго рода, определяемая мощностью критерия (удельный вес порции энтропии), имеет вид:

$$\beta_i^{ЭФ} = G_H^i - G_H^{ОПТ} . \qquad (2.14)$$

Значения $\alpha_o^{ЭФ}$ и $\beta_o^{ЭФ}$ характеризуют систему договоренностей. То есть для принятия гипотезы H_o необходимо заказчику и разработчику договориться о численном значении $\alpha_o^{ЭФ}$ и $\beta_o^{ЭФ}$. Если выполняется неравенство вида:

$$\alpha_i^{ЭФ} \le \alpha_o^{ЭФ} \quad \text{и} \quad \beta_i^{ЭФ} \le \beta_O^{ЭФ},$$

то нулевая гипотеза H_o (вариант опасности объекта) принимается, в противном случае гипотеза отвергается.

На основе транспонирования характеристик таблицы 1.3 и шестибалльной шкалы потерь методики НПП «ИСТА-Системс» сформирована таблица на рисунке 2.1 в виде последовательного нарастания опасности генеральной совокупности КВО.

Элементами таблицы являются значения частных потерь от 1 до 6 в зависимости от масштаба потенциальных потерь при ЧС, взятых из рассмотренной методики. Используя (2.5 – 2.14) для данных таблицы рисунка 2.1 получили потенциал опасности КВО при ЧС в виде функции энтропии – H. На рисунке 2.1 представлен интерфейс результатов расчета программы по шестибалльной шкале потерь.

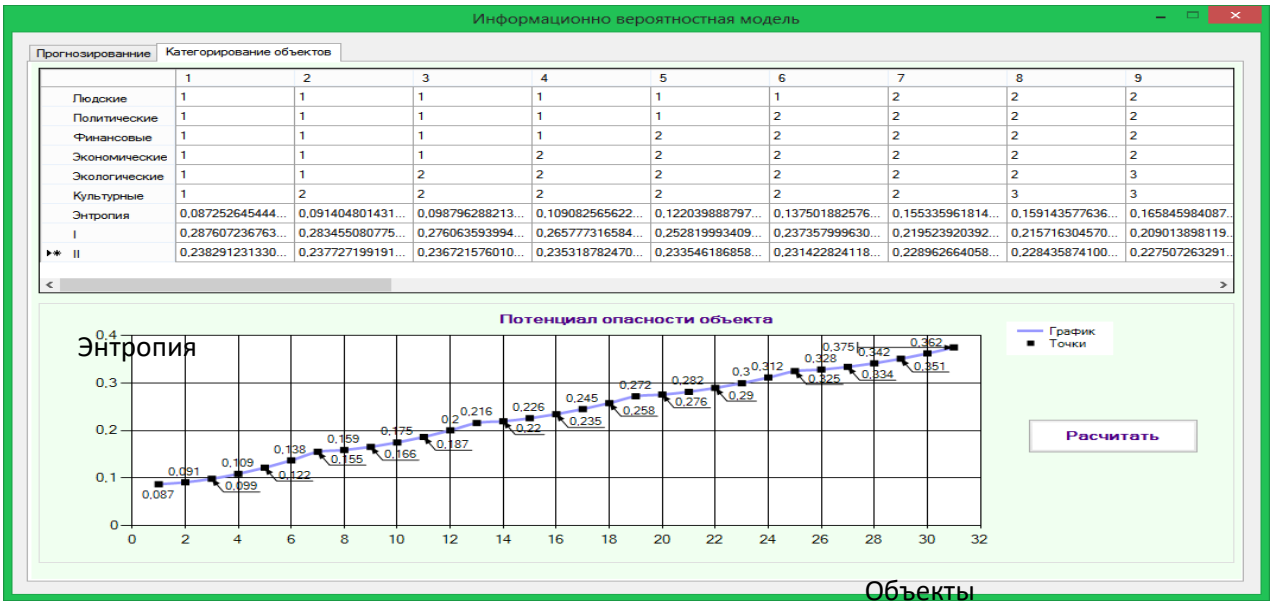


Рисунок 2.1 – Интерфейс результатов расчета по шестибалльной шкале потерь

Необходимо произвести декомпозицию всего спектра опасных объектов на значимо различные категории по величине опасности.

Алгоритм формирования категорий. Выбирая последовательно объекты из таблицы рисунка 2.1 по возрастанию опасности и применяя расчетные формулы (2.11 – 2.14) для выбранных объектов, определяли значения ошибок второго и первого рода. Основой для задания величины ошибок категорирования является оптимальное значение веса порции преемственности энтропии $G_H^{ОПТ}$ =0,272. В процессе расчетов по условиям решения задачи определялось значение величины $\beta_i^{ЭФ}$, а затем $\alpha_i^{ЭФ}$.

Если расчетные значения $\beta_i^{ЭФ}$ и $\alpha_i^{ЭФ}$ превышали требуемые, то во множество выбранных объектов включали очередной объект и расчеты (2.5 – 2.14) повторялись. Итерация повторялась, пока ошибки не удовлетворяли заданным требованиям. Аналогично формировались все последующие категории объектов. Модель адекватно описывает линейное, возрастающее распределение опасности объектов по шестибалльной шкале.

Процесс расчета автоматизирован при помощи разработанной программы на языке программирования C# [70 - 73], свидетельство о государственной регистрации № 2016616793 [74].

На основе изложенного математического аппарата получили шесть значимо различающихся по опасности категорий объектов. Результаты значений интервалов категорий сведены в таблицу 2.3.

Таблица 2.3 – Критерии категорирования по уровню интегральных потерь

Характеристика	Номер категории объектов					
	1 кат.	2 кат.	3 кат.	4 кат.	5 кат.	6 кат.
Порядковые номера совокупности объектов из таблицы рис. 2.1	26 – 31	21 – 25	16 – 20	11 – 15	6 – 10	1 – 5
Сумма балов S масштаба потерь	≥32	27 – 31	22 – 26	16 – 21	11 – 15	6 – 10
Потенциал опасности H	0,342	0,300	0,258	0,216	0,159	0,099

Таким образом, по степени потенциальной опасности при уровне значимости различий $\alpha_O^{ЭФ} = 0{,}02$ объекты необходимо классифицировать по шести категориям. При этом ошибка второго рода составляет $\beta_O^{ЭФ} = 0{,}04$.

2.2 Методика категорирования объектов по энтропийной шкале потенциала опасности чрезвычайных ситуаций

Шестибалльная шкала масштабов потерь, предлагаемая методикой НПП «ИСТА-Системс», не отражает действительный уровень ущерба, так как не согласуется с данными таблицы 1.1. Определим значимость потерь различных ЧС на основе информационно-вероятностного метода.

Постановка задачи. Необходимо на основе данных таблицы 1.1 оценить количественно одним информационным показателем каждый масштаб ЧС для использования их в задачах категорирования объектов. Построить функцию зависимости информационного показателя уровня масштаба потерь при ЧС и оценить характер зависимости.

Для описания масштабов ЧС с помощью информационного показателя использовался математический аппарат – информационно-вероятностный метод, то

есть каждый уровень масштаба потерь оценивался порцией энтропии. В результате решения задачи получили нелинейное распределение потенциалов опасности ЧС [75]. Результаты представлены в таблице 2.4.

Таблица 2.4 – Соотношение потенциалов опасности ЧС по шестибалльной и энтропийной шкале

Оценочные шкалы	Уровень масштаба потерь при ЧС					
	Локального *	Муниципального*	Межмуниципального*	Регионального *	Межрегионального *	Федерального *
Шестибалльная	1	2	3	4	5	6
Энтропийная	0,0066	0,116	0,173	0,555	0,621	0,878

*- характера

На основе метода наименьших квадратов изменение энтропии описано с помощью степенной функциональной зависимости. График нелинейной функции представлен на рисунке 2.2 – изменение потенциала опасности (энтропии) ЧС в зависимости от уровня масштаба последствий.

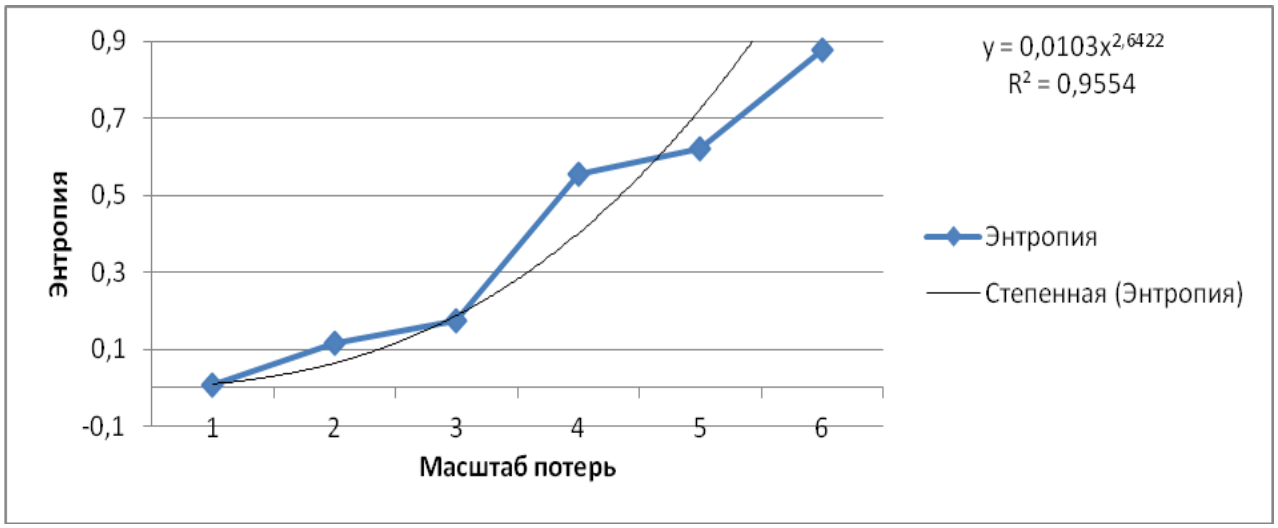


Рисунок 2.2 – График энтропии опасности от масштаба потерь при ЧС

Анализ результатов показывает, что распределение потенциалов опасности ЧС в зависимости от степени последствий носит нелинейный характер (в отличие от методики НПП «ИСТА-Системс» [20]). Следовательно, и величина требований к показателям защищенности различных категорий объектов должна иметь нели-

нейных характер и соответствовать функции последствий при возникновении ЧС на соответствующей категории объектов. Полученные результаты имеют существенное различие с шестибалльной линейной шкалой оценки степени опасности ЧС. Различие между минимальным и максимальным потенциалом опасности ЧС составляет сто раз – это логичный (соизмеримый) результат, который согласуется с действительным масштабом потерь.

Входные данные таблицы рисунка 2.1 заменим соответствующими энтропийными потенциалами из таблицы 2.4, то есть шестибалльную шкалу заменим энтропийной шкалой и повторим расчеты по формулам (2.5 – 2.14), то получим, что объекты по величине опасности распределены нелинейно.

График изменения опасности объектов, выраженный энтропийным потенциалом, представлен на рисунке 2.3.

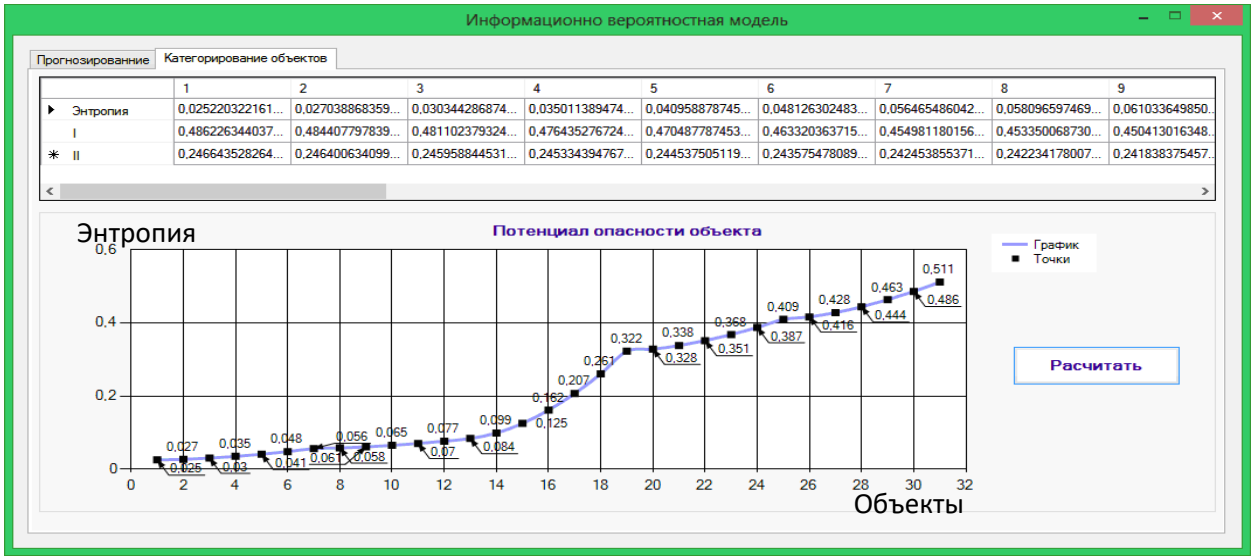


Рисунок 2.3 – Интерфейс результатов расчета по энтропийной шкале потерь

В результате применения информационного критерия оптимальности развития систем (2.13) получили семь значимо различных по опасности категорий, которые сведены в таблицу 2.5. Для проверки правильности и корректности работы метода использовались критерии Вилкоксона, знаков Фишера.

Таблица 2.5 – Критерии категорирования по уровню интегральных потерь

Характеристика	Номер категории объектов						
	1 кат.	2 кат.	3 кат.	4 кат.	5 кат.	6 кат.	7 кат.
Порядковые номера совокупности объектов из таблицы рис. 2.3	27-31	23-26	19-22	16-18	12-15	7-11	1-6
Сумма баллов S масштаба потерь	≥30	27-29	25-26	23-24	21-22	14-20	6-13
Изменение потенциала опасности категории (Н)	0,416-0,511	0,351-0,416	0,261-0,351	0,125-0,261	0,070-0,125	0,048-0,070	0,025-0,048

При проверке статистических гипотез для данных рисунка 2.3 при уровне значимости критерия Фишера $\alpha = 0,05$ получили распределение групп категорий, которое согласуется с результатами информационно-вероятностного метода [75, 76].

Увеличилось количество формируемых категорий, и вместе с этим изменился состав формируемых групп в категориях. Наибольшей по количеству элементов в категории является седьмая группа. Это объясняется тем, что в эту группу входит множество обычных социальных и культурных объектов, близких по значимой опасности возникновения ЧС.

Выводы:

1. Полученные результаты имеют существенное различие с шестибалльной линейной шкалой оценки степени опасности ЧС. Различие между минимальным и максимальным потенциалом опасности ЧС составляет сто раз – это логичный (соизмеримый) результат, который согласуется с действительным масштабом потерь.

2. Потенциал опасности категорируемых объектов носит нелинейный характер (рисунок 2.3).

3. Математически обоснована необходимость классификации объектов по семи значимо различным категориям.

4. Опасность первой категории превышает седьмую категорию в 14 раз (таблица 2.5), что расходится с методикой НПП «ИСТА-Системс» (в методике 6 раз).

5. Значения интервалов категорий (таблица 2.5) свидетельствуют, что категории объектов по количественному составу распределены неравномерно.

2.3 Оценка связи характеристик критически важных объектов и их влияния на потенциал опасности с использованием метода главных компонент и информационно-вероятностного метода

В настоящее время данная задача решается в основном экспертными методами [20] и (или) на основе теории нечеткой логики и нечетких гиперграфов [21]. Последние методы исследований [21] не позволяют оценить величину связи частных видов потерь и их весовой вклад в формирование потенциала опасности объекта.

Предлагается на основе МГК проанализировать связь между характеристиками в виде частных видов потерь, формирующих потенциал опасности объекта при возникновении ЧС, и на основе информационно-вероятностного метода оценить энтропийный потенциал опасности каждой категории объектов. По результатам оценки опасности категорий предложить соответствующий уровень вероятности нахождения объекта в безопасном состоянии. Достоинство решения задачи: обработка одной и той же информации разными математическими методами с последующим анализом результатов.

Постановка задачи. На основе ИВМ и МГК оценить структурную связь характеристик опасности в виде частных потерь на КВО при возникновении ЧС и формализовать или интерпретировать физический смысл содержания основных компонент матрицы нагрузок, определяющих потенциал опасности объекта. На основе полученной информации оценить потенциал опасности каждой категории объектов и предложить требуемый уровень их защищенности.

Решение задачи. Результаты исследований, полученные в пункте 2.1 диссертации, являются исходными данными для решения задачи методом главных компонент. В таблице 2.6 представлены результаты оценок опасности последствий ЧС каждой категории объектов в виде шести частных видов и масштабов потерь по шестибалльной шкале.

Таблица 2.6 – Параметры последствий ЧС объектов по шестибалльной шкале

Частные виды потерь	Масштаб потерь объектов						
	1 кат.	2 кат.	3 кат.	4 кат.	5 кат.	6 кат.	7 кат.
Политические	5	4	3	3	2	2	1
Людские	5	4	4	3	2	2	1
Финансовые	5	5	4	3	2	2	1
Экономические	6	5	4	3	3	2	1
Экологические	6	5	4	3	3	2	2
Информационные	6	5	4	3	3	2	2

Проведенные исследования в пункте 2.2 определили каждому масштабу потерь соответствующую энтропийную величину ущерба, которая имеет нелинейный характер, кроме того, минимальный и максимальный масштаб потерь отличается не в шесть раз, а порядка ста раз. Это более соответствует действительному масштабу потерь. Результаты энтропийной оценки масштаба потерь приведены в таблице 2.2. В таблице 2.6 перейдем от шестибалльной к энтропийной шкале опасности, получим таблицу 2.7.

Таблица 2.7 – Характеристики категорий объектов по энтропийной шкале

Частные виды потерь	Масштаб потерь объектов						
	1 кат.	2 кат.	3 кат.	4 кат.	5 кат.	6 кат.	7 кат.
Политические	0,621	0,555	0,173	0,173	0,116	0,116	0,0066
Людские	0,621	0,555	0,555	0,173	0,116	0,116	0,0066
Финансовые	0,621	0,621	0,555	0,173	0,116	0,116	0,0066
Экономические	0,878	0,621	0,555	0,173	0,173	0,116	0,0066
Экологические	0,878	0,621	0,555	0,173	0,173	0,116	0,116
Информационные	0,878	0,621	0,555	0,173	0,173	0,116	0,116

С целью определения системных связей между частными видами потерь матрицы наблюдений использовался один из главных методов факторного анализа – метод главных компонент [77 - 79]. Этот метод позволяет на основе данных корреляционной матрицы разделить совокупность ортогональных векторов (компонент) или направлений по числу рассматриваемых переменных. По этому методу собственные значения выделяются в порядке убывания, что существенно для описания данных в случае использования лишь незначительного числа компонент.

После определения матрицы для лучшей интерпретации факторов используют вращение матрицы факторных нагрузок в пространстве общих факторов.

Для осуществления вращения матрицы факторных нагрузок (факторного отображения) А наиболее распространенным является метод варимакс, предложенный П. Кайзером.

Результаты компонентного анализа потенциально опасных объектов по исходным данным таблицы 2.7 приведены в таблице 2.8.

Таблица 2.8 – Оценка характеристик объектов по факторным нагрузкам

Частные виды потерь	Факторные нагрузки					
	$F_{1\ потенциал\ опасности}$	F_2	F_3	F_4	F_5	F_6
Политические	0,987	-0,115	-0,061	0	0,031	0
Людские	*0,990*	-0,152	0,15	-0,103	-0,039	0
Финансовые	0,987	-0,135	-0,031	0,067	-0,018	0
Экономические	0,987	-0,135	-0,08	-0,062	0,062	0
Экологические	0,952	0,291	-0,134	0	-0,076	0
Информационные	0,960	0,262	0,133	0,088	0,014	0

Из таблицы 2.8 видно, что все виды частных потерь объединились в первой компоненте – интерпретируем ее как «потенциал опасности» объекта при возникновении ЧС. Первая компонента составляет 78 % информационной нагрузки, вторая – 10 %, третья – 7 %. Остальные компоненты малозначимы.

Перейдем от матрицы факторных нагрузок к матрице главных компонент категорируемых объектов (таблица 2.9).

Таблица 2.9 – Оценка категорируемых объектов по факторным нагрузкам

Категории объектов	Энтропийный потенциал опасности	Факторные нагрузки					
		F_1	F_2	F_3	F_4	F_5	F_6
1 кат.	0,584	1,625	0,034	-0,443	0,269	1,47	0
2 кат.	0,471	1,021	-0,538	-0,149	0,558	-1,9	0
3 кат.	0,443	0,629	-0,203	1,825	0,612	0,086	0
4 кат.	0,355	-0,406	2,385	-1,515	-0,653	-0,155	0
5 кат.	0,122	-0,877	-0,56	0,384	-1,701	0,06	0
6 кат.	0,082	-0,953	-0,706	-0,102	1,515	0,44	0
7 кат.	0,053	-1,039	-0,412	-0,201	0,073	-0,179	0

Из таблицы 2.9 видно, что все категории объектов по первой компоненте расположились по убыванию привлекательности относительно начала координат. По первой компоненте F_1 наиболее привлекательными являются объекты первой и второй категории. Седьмая категория самая непривлекательная.

В таблице 2.9 с помощью информационно-вероятностного метода по факторным нагрузкам F_1, F_2 и F_3 оценили энтропийный потенциал опасности категорируемых объектов. Уровень опасности при возникновении ЧС на категорируемых объектах носит нелинейный логарифмический характер (рисунок 2.6).

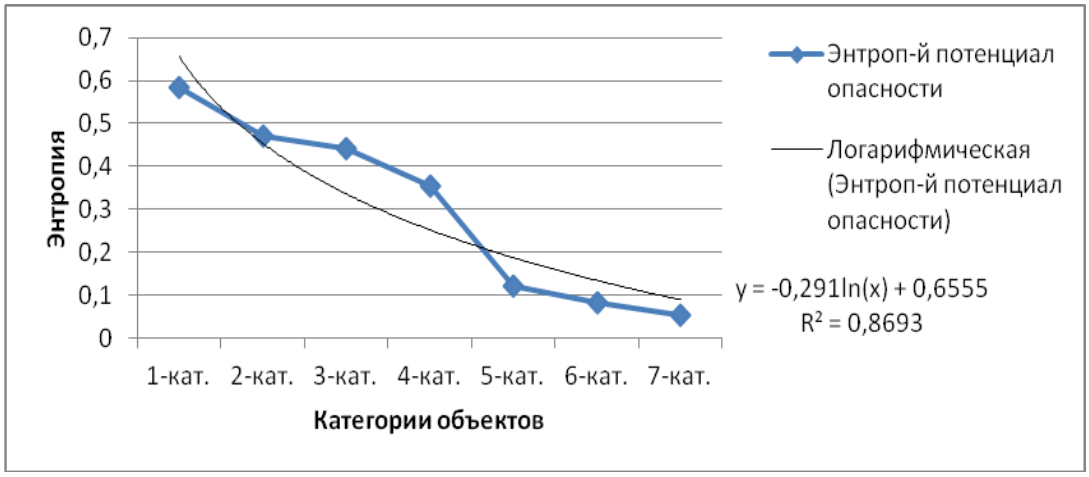


Рисунок 2.6 – Величина энтропии опасности категорируемых объектов

Анализ результатов показывает, что математический аппарат адекватно отражает физическую сущность категорий объектов.

Соотношения величины опасности между максимальной и минимальной категорией объекта составляет порядка одиннадцати раз. Это более логичный результат, чем в методике оценки опасности категорируемых объектов НПП «ИСТА-Системс», которая оценивает соотношение потенциалов шесть раз.

Величину опасности категорируемых объектов в виде энтропийного потенциала опасности оценим по входным данным из таблицы 2.7, а результаты оценки энтропийного потенциала каждой категории представлены в таблице 2.10. Из таблицы видно, что потенциал опасности объектов первой категории превышает потенциал седьмой категории объектов порядка четырнадцати раз. Результаты согласуются с методом главных компонент, однако ИВМ в отличие от МГК использует 100 % информации и является определяющим в оценке потенциалов опасности.

Таблица 2.10 – Потенциалы категорируемых объектов по энтропийной шкале

Частные виды потерь	Масштаб потерь объектов						
	1 кат.	2 кат.	3 кат.	4 кат.	5 кат.	6 кат.	7 кат.
Политические	0,621	0,555	0.173	0,173	0,116	0,116	0,0066
Людские	0,621	0,555	0,555	0,173	0,116	0,116	0,0066
Финансовые	0,621	0,621	0,555	0,173	0,116	0,116	0,0066
Экономические	0,878	0,621	0,555	0,173	0,173	0,116	0,0066
Экологические	0,878	0,621	0,555	0,173	0,173	0,116	0,116
Информационные	0,878	0,621	0,555	0,173	0,173	0,116	0,116
Энтропийный потенциал опасности	1.371	1.182	1.011	0.522	0.289	0.206	0.102
P безопасного состояния объекта	**0,999**	0,95	0,90	0,77	0,69	0,65	**0,60**

Показателем защищенности объекта выберем вероятность его безопасного состояния. Имея потенциалы опасности категорируемых объектов, можно определить величину показателя их защищенности (вероятность безопасного состояния) как функцию потенциала опасности. То есть требуется обосновать шкалу критерия эффективности СФЗ в зависимости от категории объекта. Очевидно, должно быть соответствие между потенциалом опасности категории и степенью его защищенности, то есть характер изменения зависимостей должен быть подобный. Следовательно, и величины требований к показателям эффективности защищенности различных категорий объектов также должны определяться подобной (аналогичной) зависимостью, то есть иметь нелинейных характер и соответствовать функции последствий ЧС. Функцию изменения энтропийных потенциалов от номера категории свяжем с требуемой величиной вероятности безопасного состояния по первой категории (за верхнюю оценку принято значение вероятности защиты 0,999 – величина близкая к предельной) и последней категории (чувствительность датчика обнаружения – 0,65 и вероятность своевременной нейтрализации – 0,95). Таким образом, сопоставим каждой категории требуемую величину защищенности. Характер изменения энтропии опасности объектов и их вероятности безопасного состояния как подобные величины приведены в таблице 2.10 и на рисунке 2.6.

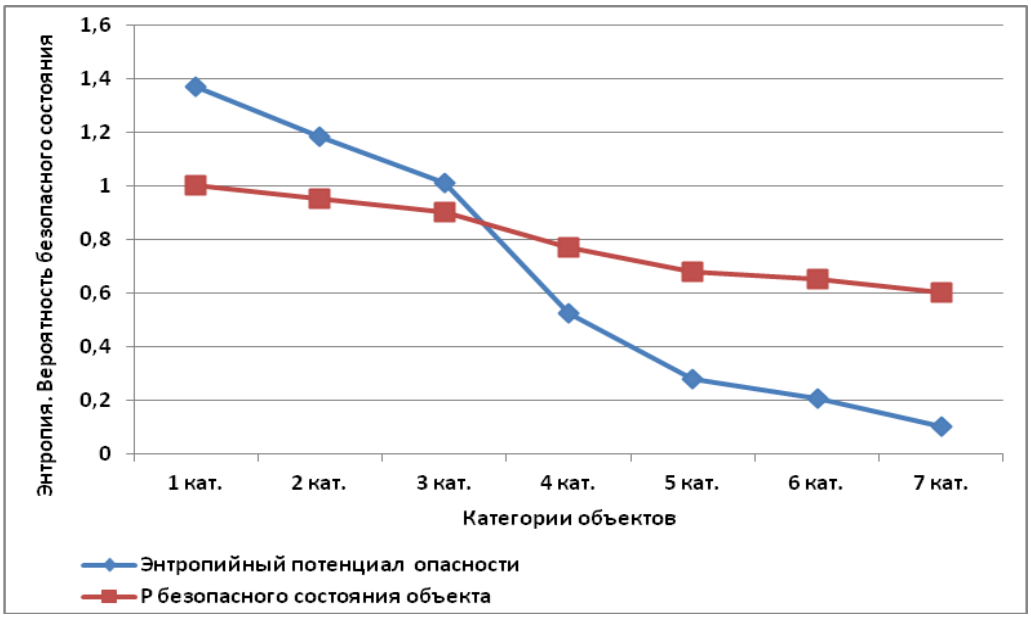


Рисунок 2.6 – Энтропия опасности и показатели защищенности категорий КВО

Анализ графиков показывает нелинейный характер зависимости потенциала опасности категорируемых объектов и соответствующий им показатель вероятности безопасного состояния объектов [80].

Таким образом, интегральной характеристикой категорируемых объектов, определяющей их привлекательность, является потенциал опасности объекта при возникновении ЧС. Характеристики частных потерь определяют потенциал опасности категории объектов, который формирует потенциал привлекательности объекта. Потенциал опасности первой категории КВО превосходит седьмую категорию в 14 раз. Распределение потенциалов опасности категорий КВО носит нелинейный характер, следовательно, и распределение показателей их защищенности носит нелинейный характер. Полученные результаты могут использоваться при обосновании требований к безопасности КВО.

2.4 Выводы

1. Анализ результатов показывает, что распределение потенциалов опасности ЧС в зависимости от степени последствий носит нелинейный характер (в отличие от источника [20]). При проведении категорирования объектов логично ис-

пользовать нелинейную энтропийную шкалу оценки последствий ЧС, которая более соответствует действительным потерям.

2. Полученные значения потенциалов могут использоваться для оценки уровня опасности объектов при их категорировании (определении степени опасности), а также при задании величины требований к показателям эффективности защищенности объектов.

3. Различие между минимальным и максимальным потенциалом опасности ЧС составляет сто раз – это логичный (соизмеримый) результат, который согласуется с действительным масштабом потерь.

4. Потенциал опасности категорируемых объектов носит нелинейный характер (рисунок 2.6). Следовательно, и величина требований к показателям защищенности различных категорий объектов должна определяться аналогичной зависимостью, то есть иметь нелинейных характер.

5. Представлено математическое обоснование необходимости классификации объектов по семи значимо различным категориям по степени потенциальной опасности.

6. Опасность первой категории превышает седьмую категорию в 14 раз (таблица 2.10), что расходится с методикой НПП «ИСТА-Системс».

7. Значения интервалов категорий (таблица 2.5) свидетельствуют о том, что категории объектов по количественному составу распределены неравномерно.

8. Основной интегральной характеристикой категорируемых объектов является их привлекательность для проведения терактов.

ГЛАВА 3 СИСТЕМНЫЙ АНАЛИЗ ТЕРРОРИСТИЧЕСКИХ УГРОЗ

3.1 Методика исследования связи характеристик нарушителей и оценки их потенциала опасности на основе информационно-вероятностного метода и метода главных компонент

При проектировании СФЗ КВО необходимо определить модель нарушителя как совокупность определенных характеристик [81].

Предлагается на основе МГК проанализировать связь характеристик типовых нарушителей и с использованием ИВМ оценить их потенциал опасности. По результатам оценки предложить соответствующий уровень эффективности СФЗ. Данная задача решается для дифференцирования необходимых требований при определении требуемой величины защищенности от типовых нарушителей.

В настоящее время эти вопросы решаются в основном экспертными методами [59, 66, 82], где присутствует элемент субъективизма, или как вариант на основе теории нечеткой логики и нечетких гиперграфов [20, 21]. Последние методы не позволяют оценить связь характеристик и их весовой вклад в формирование потенциала опасности типовых нарушителей.

Особенностью раздела диссертации является обработка одних и тех же данных разными математическими методами с последующим анализом результатов.

Постановка задачи. Необходимо на основе МГК оценить структурную связь характеристик типовых нарушителей, интерпретировать (формализовать) определения основных компонент матрицы нагрузок. На основе перехода к матрице главных компонент типовых нарушителей необходимо оценить их потенциал опасности. Сравнить результаты, полученные ИВМ и МГК.

Решение задачи. Типовых нарушителей выберем согласно таблице 1.2. На основе этих данных и шкалы перехода от качественных характеристик к количественным методикам [9] сформирована таблица 3.1, то есть осуществлен переход к количественным характеристикам типовых нарушителей. Характеристика «по-

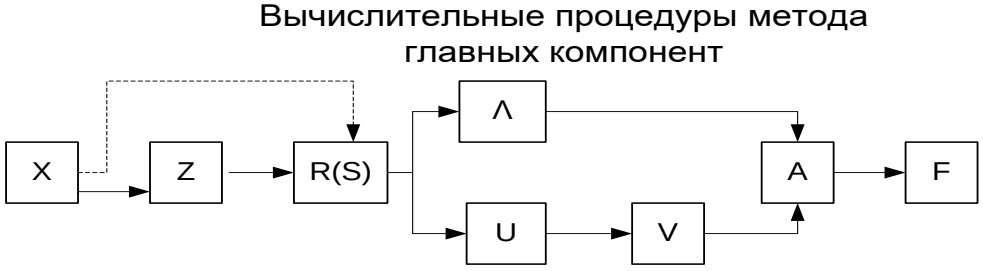
следствия действий нарушителя» заменена соответствующим энтропийным потенциалом уровня последствий по результатам исследований главы 2.2.

Таблица 3.1 – Количественные характеристики типовых нарушителей

Тип нарушителя	Характеристики нарушителей					
	Численность	Цель действий	Последствия действий	Уровень информационной осведомленности	Холодное и огнестрельное оружие (техническая оснащенность)	Уровень физической подготовки преодоления
X_1	12-20	10	0,878	0,7	0,9	1
X_2	4-6	9	0,5546	0,6	0,8	0,9
X_3	1	8	0,1731	0,4	0,7	0,8
X_4	1	2	0,0067	0,3	0,3	0,3
X_5	1	2	0,1158	0,9	0,3	0,3
X_6	1	5	0,1731	1	1	0,6

С целью исследования связей между характеристиками нарушителей (параметрами матрицы) использовался один из главных методов факторного анализа – МГК [77, 78]. Метод позволяет на основе данных корреляционной матрицы разделить совокупность ортогональных компонент по числу рассматриваемых переменных.

Алгоритм решения задачи МГК представлен на рисунке 3.1.



X – входная матрица n × m ;
n – количество исследуемых объектов;
m – количество характеристик объектов;
Z – матрица приведенных значений характеристик;
R – матрица парных корреляций;
Λ – диагональная матрица характеристических чисел;
V – матрица нормированных характеристических векторов;
A – матрица факторных признаков;
F – матрица главных компонент r × n .

Рисунок 3.1 – Алгоритм метода главных компонент

Применяя МГК к характеристикам нарушителей (таблица 3.1), получили результаты, которые сведены в таблицу 3.2. Характеристики нарушителя можно описать с помощью двух главных компонент, которые содержат в себе соответственно 69 % и 25 % информационной нагрузки. Полученные компоненты – новые ортогональные оси.

Таблица 3.2 – Матрица факторных нагрузок характеристик нарушителей

Характеристики нарушителей	Факторные нагрузки					
	F_1 физическая. техническая подготовка, мотивация к ТА	F_2 информированность	F_3	F_4	F_5	F_6
Численность	**0,843**	0,101	-0,507	0,089	0	0
Цель действий	**0,95**	0,179	0,215	-0,092	0	0
Последствия действий	**0.94**	0.031	-0.325	-0.144	0	0
Уровень информационной осведомленности	0.116	**-0.975**	-0.154	-0.061	0	0
Холодное огнестрельное оружие (техническая оснащенность)	**0.8**	-0.368	0.422	0.092	0	0
Уровень физической подготовки	**0.952**	0.128	0.217	0.078	0	0

По характеристикам, входящим в первую компоненту, ее можно интерпретировать как «степень подготовки и мотивации к совершению ТА». В эту компоненту объединились характеристики: численность, цель, последствия, техническая оснащенность и уровень физической подготовки. Базовыми параметрами в первой компоненте являются – цель действий и уровень физической подготовки.

Вторую компоненту интерпретируем как «информированность об объекте», так как в эту компоненту вошла одна характеристика – уровень информационной осведомленности.

Следовательно, основной комплексной характеристикой нарушителя является компонента – подготовка и мотивация нарушителя к совершению ТА.

Перейдем от матрицы факторных нагрузок к матрице главных компонент типовых нарушителей, которая представлена в таблице 3.3.

Используя информационно-вероятностный метод [68] по первым трем компонентам, определили энтропийный потенциал опасности типовых нарушителей (таблица 3.3).

Талица 3.3 – Матрица главных компонент для типовых нарушителей

Тип нарушителя	Энтропийный потенциал нарушителя	Факторные нагрузки					
		F_1 Степень мотивации к ТА	F_2 информи-рованность	F_3	F_4	F_5	F_6
X_1	**0,607**	1,631	0,131	-1,237	-0,879	0	0
X_2	0,525	0,75	0,303	0,4	0,700	0	0
X_3	0,377	0,037	0,905	1,384	0,285	0	0
X_4	**0,040**	-1,25	1,203	-0,393	-1,528	0	0
X_5	0,298	-1,099	-0,829	-1,132	1,513	0	0
X_6	0,550	-0,069	-1,714	0,978	-0,091	0	0

Первый тип нарушителя превосходит четвертый тип нарушителя по потенциалу опасности (мотивации и информированности) в 15 раз (рисунок 3.2).

Анализ энтропийных потенциалов таблицы 3.3 показывает, что наиболее мотивированными к проведению ТА является первый, второй и шестой тип нарушителя. Наименее мотивирован к проведению ТА четвертый тип нарушителя, так как он обычный похититель материальных средств. По информированности (вторая компонента) шестой и пятый тип нарушителя имеет наибольшую информированность, так как это внутренние нарушители. Менее информированы третий и четвертый типы нарушителей, так как они одиночные нарушители и не вступают в сговор.

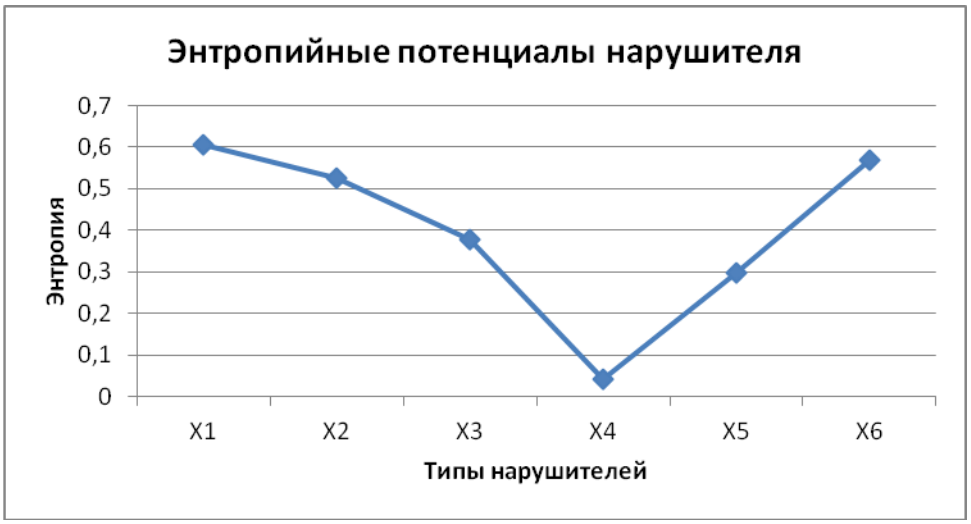


Рисунок 3.2 – Энтропийные потенциалы опасности нарушителей

Второй подход применения МГК для исследования связи характеристик нарушителей основан на результатах формирования категорий объектов в п. 2.1 и использования энтропийной шкалы для оценки характеристики «последствия

действия нарушителя» (таблица 3.1), связывающей информационно между собой каждую категорию опасности объектов с соответствующим типовым нарушителем. Пример результатов формирования частных видов потерь от действий типовых нарушителей по шестибалльной шкале приведен в таблице 3.4.

Таблица 3.4 – Последствия целевой реализации типовых нарушителей по шестибалльной шкале

Частные виды потерь от действий нарушителя	Типовые нарушители					
	X_1	X_2	X_3	X_4	X_5	X_6
Политические	6	5	4	1	2	3
Людские	6	5	4	1	2	3
Финансовые	4	2	2	2	5	4
Экономические	6	5	4	2	2	3
Экологические	6	5	4	1	3	2
Информационные	4	2	2	2	5	5

Для оценки потенциальной опасности нарушителей («последствия действия нарушителя») использовались шесть частных видов потерь, что и в пункте 2.1. диссертации:

- политические (определяются снижением всех уровней авторитета властей и общей нестабильностью);

- людские (потери в утрате жизни людей и их здоровья);

- финансовые (заключаются в утрате материальных ценностей);

- экономические (учитывают затраты на переселение людей из зоны аварий и связанные с этим компенсационные выплаты);

- экологические (потери природных ресурсов, приводящие к ухудшению экологической обстановки в регионе);

- информационные (потери, заключающиеся в утрате художественных ценностей, передовых технологий, конфиденциальной информации).

Частные виды потерь выражены для шести масштабов потенциальных потерь, которые затем меняются на соответствующие энтропийные потенциалы (таблица 3.5). Целесообразность замены на энтропийную шкалу обоснована при проведении исследований в пункте 2.2 диссертации:

1 - локальный – равен энтропийному ущербу H=0,0066;

2 - местный – H=0,116;

3 - территориальный - H=0,173;

4 - региональный -H=0,555;

5 - государственный - H=0,621;

6 - межгосударственный - H=0,878.

Таблица 3.5 – Энтропийная шкала последствий целевой реализации типовых нарушителей

Частные виды потерь от действий нарушителя	Типовые нарушители					
	X_1	X_2	X_3	X_4	X_5	X_6
Политические	0,878	0,621	0,555	0,0066	0,116	0,173
Людские	0,878	0,621	0,555	0,0066	0,116	0,173
Финансовые	0,555	0,116	0,116	0,116	0,555	0,555
Экономические	0,878	0,621	0,555	0,116	0,116	0,173
Экологические	0,878	0,621	0,555	0,0066	0,173	0,116
Информационные	0,555	0,116	0,116	0,116	0,555	0,555

Применяя МГК к характеристикам последствий от действия типовых нарушителей (таблица 3.5), определили, что их можно описать с помощью двух главных компонент, которые содержат в себе 95% информационной нагрузки (таблица 3.6).

Таблица 3.6 – Оценка характеристик нарушителей по факторным нагрузкам

Частные виды потерь от действий нарушителя	Факторные нагрузки					
	F_1 подрыв автор. власти	F_2 информационные потери	F_3	F_4	F_5	F_6
Политические	**- 0,989**	0,013	-0,403	0,049	0	0
Людские	**- 0,985**	0,013	0,101	0,095	0	0
Финансовые	**+ 0,672**	-0,557	-0,114	0,301	0	0
Экономические	**- 0,971**	-0,061	0,094	0,098	0	0
Экологические	**- 0,988**	0,061	0,158	0,111	0	0
Информационные	+ 0,473	**+0,805**	0,172	0,10	0	0

Анализ результатов показывает, что все характеристики, кроме «информационных ценностей», объединяются в первую компоненту. Базовой характеристикой в первой компоненте являются «политические» потери, то есть целью является политическая мотивация – подрыв авторитета и дестабилизация власти. Финансовая характеристика находится на противоположной стороне оси компоненты, то есть она для террориста не имеет значения.

Первую компоненту интерпретируем как «подрыв (снижение) авторитета

власти». В эту компоненту объединились следующие характеристики: политические, экономические и экологические последствия, людские потери. Финансовая составляющая имеет противоположный знак в первой компоненте, то есть она имеет противоположный характер связи с политическими, экономическими и экологическими последствиями. Базовым параметром первой компоненты является политическая характеристика.

Вторую компоненту можно интерпретировать как «информационная» составляющая последствий проведения ТА. Базовый параметр второй компоненты – информационные потери.

Перейдем от матрицы факторных нагрузок к матрице главных компонент типовых нарушителей (таблица 3.7).

Таблица 3.7 – Оценка характеристик нарушителей по факторным нагрузкам

Типы нарушителей	Энтропийный потенциал ущерба	Факторные нагрузки					
		F_1-подрыв авторитета власти.	F_2 - информационные потери	F_3	F_4	F_5	F_6
X_1	**0,573**	**-1,31**	**-0,245**	-0,128	1,497	0	0
X_2	0,549	**-0,816**	0,002	0,088	-0,524	0	0
X_3	0,531	**-0,772**	-0,151	0,696	-1,689	0	0
X_4	**0,040**	**1,331**	-1,549	-0,465	0,111	0	0
X_5	0,340	0,733	**0,069**	1,528	0,77	0	0
X_6	0,402	0,84	1,874	-1,716	-0,165	0	0

В первой компоненте «подрыв авторитета власти» первые три типа нарушителя имеют наибольший вес, так как их цель – влияние на власть. Четвертый тип нарушителя имеет наименьший вес, так как он – обычный похититель. Во второй компоненте больший вес имеют пятый, шестой тип нарушителя и в меньшей степени четвертый тип нарушителя. Пятый и шестой тип нарушителей являются внутренними, они обладают информацией и будут стремиться завладеть ценной информацией.

Применяя ИВМ [74] к двум информационным компонентам, получили энтропийные потенциалы ущербов от действий нарушителей. Первый тип нарушителя превосходит по энтропийному потенциалу ущерба четвертый тип нарушителя в 14 раз. Результаты приведены в таблице 3.7 и на рисунке 3.4.

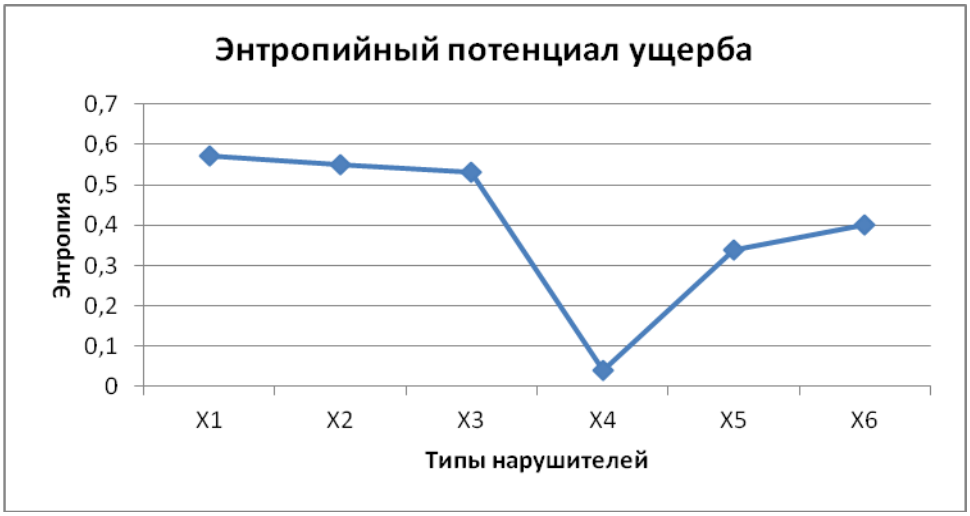


Рисунок 3.3 – Оценка потенциала ущерба, наносимого нарушителем

Анализ данных рисунков 3.2 и 3.3 на однородность по критериям Вилкоксона и знаков Фишера показывает, что величины потенциалов опасности типовых нарушителей и наносимого ими ущерба, полученные по разным исходным данным, согласуются, то есть, нет значимого различия.

Второй подход к анализу потенциалов нарушителей. К данным таблиц 3.1, 3.5 применим математический аппарат ИВМ [68, 69]. В результате получим потенциалы опасности нарушителей по разным данным, которые представлены в таблицах 3.8, 3.9.

По данным таблицы 3.8 потенциал опасности типового нарушителя X_1 превосходит потенциал обычного нарушителя X_4 в 14 раз, а если определять методом главных компонент – в 15 раз.

Таблица 3.8 – Количественные характеристики нарушителей

Характеристики нарушителей	Типы нарушителей					
	X_1	X_2	X_3	X_4	X_5	X_6
Численность	10	4	1	1	1	1
Цель действия	10	9	8	2	2	5
Последствия действия	0,878	0,555	0,173	0,007	0,116	0,173
Уровень информационной осведомленности	0,7	0,6	0,4	0,3	0,9	1
Холодное, огнестрельное оружие (техническая оснащенность)	1	0,9	0,8	0,3	0,3	0,9
Уровень физической подготовки	1	0,9	0,8	0,3	0,4	0,8
Энтропийный потенциал нарушителя	1,140	0,861	0,540	0,084	0,287	0,607
Вероятность защиты от нарушителя	**0,99**	0,879	0,763	**0,6**	0,672	0,785

Таблица 3.9 – Последствия потерь от нарушителей по энтропийной шкале

Частные виды потерь от действий нарушителей	Типы нарушителей					
	X_1	X_2	X_3	X_4	X_5	X_6
Политические	0,878	0,621	0,555	0,0066	0,116	0,173
Людские	0,878	0,621	0,555	0,0066	0,116	0,173
Финансовые	0,555	0,116	0,116	0,116	0,555	0,555
Экономические	0,878	0,621	0,555	0,116	0,116	0,173
Экологические	0,878	0,621	0,555	0,0066	0,173	0,116
Информационные	0,555	0,116	0,116	0,116	0,555	0,555
Энтропийный потенциал последствий	1,095	0,739	0,672	0,119	0,520	0,569
Вероятность защиты от нарушителя	**0,99**	0,868	0,834	**0,6**	0,757	0,776

По данным таблицы 3.9 потенциал последствий наносимого ущерба самого подготовленного типового нарушителя X_1 превосходит потенциал обычного нарушителя X_4 по энтропийной шкале порядка 10 раз.

Анализ результатов таблиц 3.8 и 3.9 по критерию Хотеллинга показал, что между потенциалами опасности нарушителей и потенциалами возможных ущербов последействий действия нарушителей нет значимого различия, то есть они однородны. Кроме того, потенциалы опасности и ущерба последействия нарушителей должны согласоваться и с их возможностями по преодолению СФЗ объектов, то есть каждому потенциалу нарушителя необходимо поставить соответствующий потенциал защиты объекта – эффективность СФЗ (величину защищенности – вероятность безопасного состояния объекта). Иначе говоря, требуется определить необходимую величину показателя защищенности соответствующей категории опасности объекта (вероятность безопасного состояния объекта) в зависимости от потенциала опасности его базового нарушителя. Очевидно, должно быть соответствие между потенциалом опасности типового нарушителя и степенью защищенности от его действий, то есть характер изменения зависимостей потенциалов нарушителей и им противодействия СФЗ должны быть подобными функциями.

Построим зависимость изменения энтропийных потенциалов от типа нарушителя и свяжем ее с требуемой величиной вероятности безопасного состояния по первому типу нарушителя (за верхнюю оценку принято значение вероятности защиты – 0,99 – величина близкая предельной) и четвертого типа нарушителя

(чувствительность датчика обнаружения – 0,6). Таким образом, сопоставим каждому типу нарушителя требуемую величину защищенности – эффективность СФЗ (вероятность безопасного состояния объекта). Результаты вероятностей безопасного состояния объектов от действия типовых нарушителей, как подобные величины опасностям (типовым нарушителям), приведены в таблицах 3.8, 3.9 (последние строки) и на рисунке 3.4.

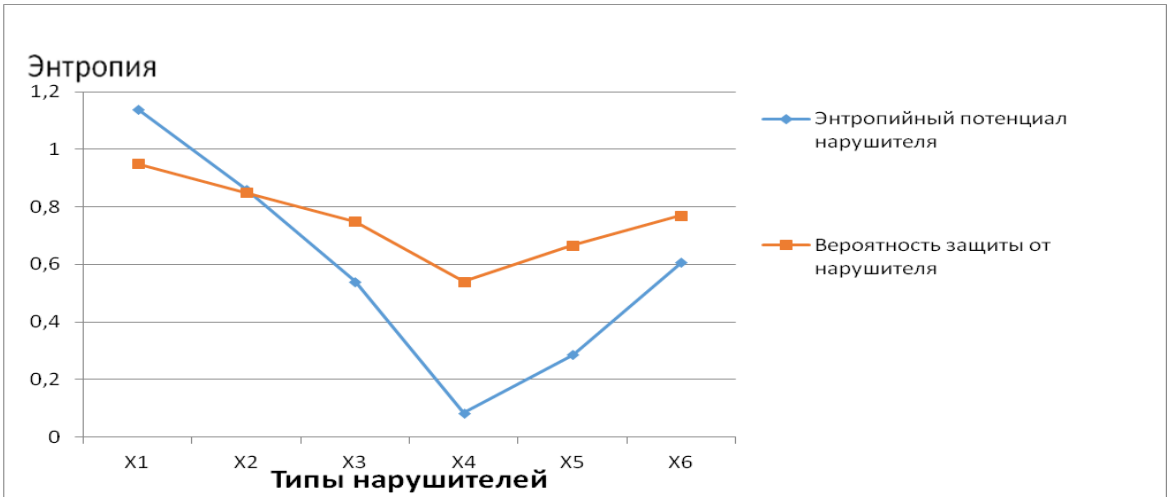


Рисунок 3.4 – График изменения опасности типовых нарушителей и вероятности защиты от них

Выводы:

1. Потенциалы опасности нарушителей и потенциалы последствий целевой реализации согласуются [84].

2. Основной комплексной характеристикой типовых нарушителей является мотивация к действию, которая влечет за собой уровень технической оснащенности, физической и информационной подготовленности, и соответственно определяет степень последствий реализации целевых действий.

3. Полученные весовые потенциалы типовых нарушителей (таблица 3.8 и 3.9) и степени вероятностей защищенности от них по разным методикам согласуются и не противоречат физическому смыслу. Результаты могут использоваться при формировании модели нарушителя.

4. Полученную информацию по категорируемым объектам и типовым нарушителям можно объединить в одно информационное поле для формирования базовых нарушителей для различных категорий объектов.

3.2 Методика оценки связи признаков категорируемых объектов и типовых нарушителей для определения базовых угроз методом главных компонент и информационно-вероятностным методом

Анализ результатов, проведенных в пунктах 2.2 и 3.1 диссертации, показал, что каждый охраняемый объект имеет потенциал привлекательности, в соответствии с которым формируется необходимый потенциал защищенности в виде значения величины эффективности СФЗ. В свою очередь каждый типовой нарушитель обладает потенциалом подготовленности (опасности), который определяется степенью его мотивации. Таким образом, множество типовых нарушителей оказывает определенное воздействие на множество категорируемых объектов в соответствии с их потенциалом возможностей. Типовые нарушители и категорируемые объекты имеют множество характеристик, определяющих соответственно их потенциал мотивации (опасности) и привлекательности, которые информационно пересекаются между собой. Очевидно, что между категориями КВО и типовыми нарушителями должно существовать определенное соответствие, которое представлено на рисунке 3.5. Соответствие базируется на общей соизмеримости или соотношений характеристик этих множеств: каждому КВО должен соответствовать определенный базовый нарушитель из множества типовых нарушителей.

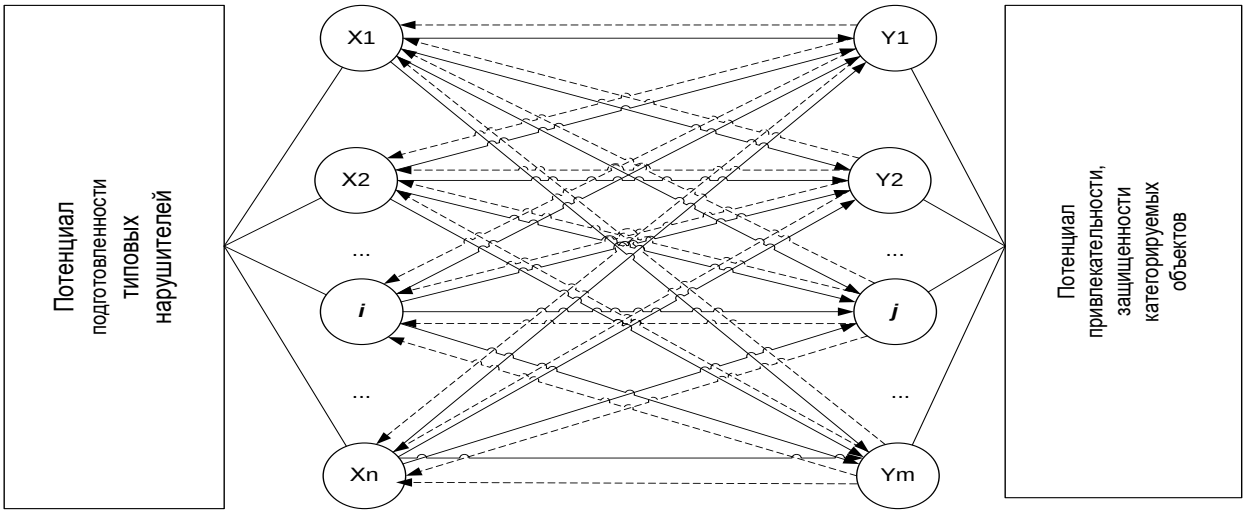


Рисунок 3.5 – Модель соответствия категорий объектов и базовых нарушителей

Для решения задачи определения базовых нарушителей опишем исходные характеристики категорируемых объектов и типовых нарушителей на основе исследований, проведенных в п. 2.2 и п. 3.1.

Для оценки потенциальной опасности объекта от действий нарушителей использовали шестибалльную шкалу масштабов частных видов потерь, рассмотренных в п. 3.1 диссертации, представленную в таблице 3.10.

Таблица 3.10 – Оценка последствий реализации цели ТН по шестибалльной шкале

Частные виды потерь от действий нарушителей	Масштаб потерь от типа нарушителя					
	X_1	X_2	X_3	X_4	X_5	X_6
Политические	6	5	4	1	2	3
Людские	6	5	4	1	2	3
Финансовые	4	2	2	2	5	4
Экономические	6	5	4	2	2	3
Экологические	6	5	4	1	3	2
Информационные	4	2	2	2	5	5

В таблице 3.11 представлены результаты оценок опасности последствий ЧС категорируемых объектов по такой же шестибалльной шкале (шкалы в таблицах одинаковы – это важно), полученные в п. 2.2 диссертации.

Таблица 3.11 – Характеристики последствий ЧС КВО по шестибалльной шкале

Частные виды потерь объектов	Масштаб потерь категорий объектов						
	1 кат.	2 кат.	3 кат.	4 кат.	5 кат.	6 кат.	7 кат
Политические	5	4	3	3	2	2	1
Людские	5	4	4	3	2	2	1
Финансовые	5	5	4	3	2	2	1
Экономические	6	5	4	3	3	2	1
Экологические	6	5	4	3	3	2	2
Информационные	6	5	4	3	3	2	2

Так как шкалы оценок масштабов совпадают, предлагается объединить в одно информационное поле таблицы 3.10 и 3.11 и на основе МГК и с использованием ИВМ определить базовых нарушителей для каждой категории КВО, то есть определить существующее соответствие. По результатам опасности базовых нарушителей предложить соответствующий уровень защищенности (безопасности) объектов.

Постановка задачи. Необходимо на основе обработки объединенного общего информационного поля характеристик нарушителей и категорируемых объек-

тов (таблицы 3.10 и 3.11) ИВМ и МГК определить типовых нарушителей для различных категорий объектов (задать базовых нарушителей категориям объектов). Иными словами, необходимо определить степень потенциала воздействия *i*-го типового нарушителя на *j*-ую категорию объекта защиты. Результатом решения будет соответствие типового нарушителя для каждой категории КВО и на этой основе можно предложить необходимую величину защищенности каждой категории объектов.

Решение задачи. Объединив информационное поле таблиц 3.10 и 3.11, получим таблицу 3.12 и транспонированную ей таблицу 3.13 с общим однородным информационным полем (единая шкала таблиц). В таблице 3.12 заменили шестибалльную шкалу на энтропийную шкалу опасности последствий ситуаций, что позволит привести исходные данные к более действительной шкале измерения. Применяя ИВМ к данным таблицы 3.12 получили энтропийные потенциалы характеристик. Их анализ показывает, что весовой вклад характеристик однороден [85].

Таблица 3.12 – Характеристики объектов и ТН по энтропийной шкале

Типовые нарушители и объекты	Масштаб потерь по энтропийной шкале для объектов и нарушителей					
	Политические	Людские	Финансовые	Экономические	Экологические	Информационные
X_1	0,878	0,878	0,555	0,878	0,878	0,555
X_2	0,621	0,621	0,116	0,621	0,621	0,116
X_3	0,555	0,555	0,116	0,555	0,555	0,116
X_4	0,007	0,007	0,116	0,116	0,007	0,116
X_5	0,116	0,116	0,621	0,116	0,173	0,621
X_6	0,173	0,173	0,555	0,173	0,116	0,621
1 кат.	0,621	0,621	0,621	0,878	0,878	0,878
2 кат.	0,555	0,555	0,621	0,621	0,621	0,621
3 кат.	0,173	0,555	0,555	0,555	0,555	0,555
4 кат.	0,173	0,173	0,173	0,173	0,173	0,173
5 кат.	0,116	0,116	0,116	0,173	0,173	0,173
6 кат.	0,116	0,116	0,116	0,116	0,116	0,116
7 кат.	0,007	0,007	0,007	0,007	0,116	0,116
Вес характеристики Н	0,701	0,709	0,672	0,794	0,781	0,737

Применяя ИВМ к данным таблицы 3.13, получили энтропийные потенциалы типовых нарушителей и категорируемых объектов (приведены в нижней строчке таблицы 3.13 и на рисунке 3.6).

Таблица 3.13 – Характеристики объектов и нарушителей по энтропийной шкале

Частные виды потерь	Типовые нарушители и категории объектов												
	X_1	X_2	X_3	X_4	X_5	X_6	1 кат.	2 кат.	3 кат.	4 кат.	5 кат.	6 кат.	7 кат.
Политические	,878	,621	,555	,007	,116	,173	,621	,555	,173	,173	,116	,116	,007
Людские	,878	,621	,555	,007	,116	,173	,621	,555	,555	,173	,116	,116	,007
Финансовые	,555	,116	,116	,116	,621	,555	,621	,621	,555	,173	,116	,116	,007
Экономические	,878	,621	,555	,116	,116	,173	,878	,621	,555	,173	,173	,116	,007
Экологические	,878	,621	,555	,007	,173	,116	,878	,621	,555	,173	,173	,116	,116
Информационные	,555	,116	,116	,116	,621	,621	,878	,621	,555	,173	,173	,116	,116
Инфор., потенциал	,633	,497	,446	,160	,368	,375	,733	,629	,547	,269	,229	,210	,122

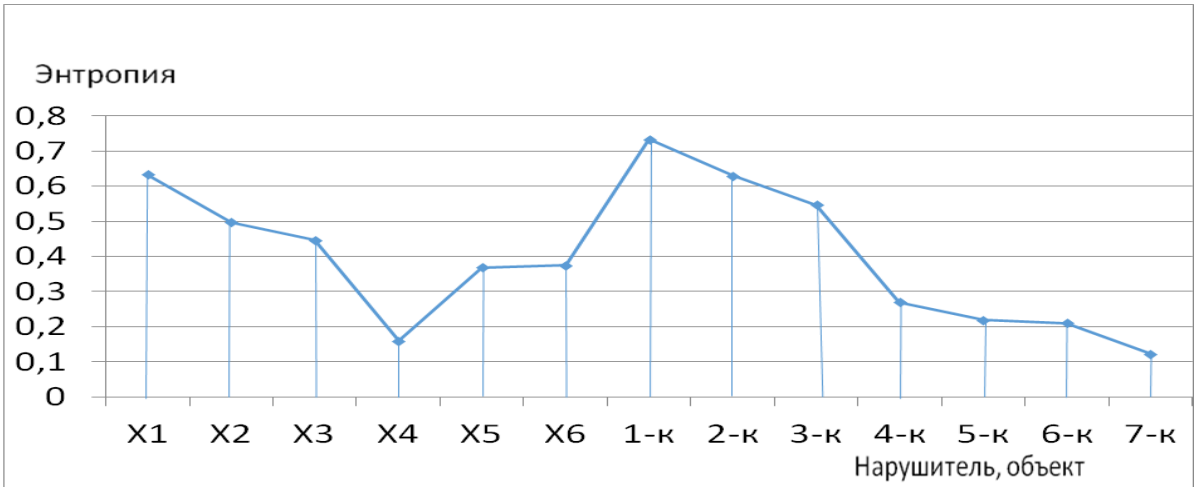


Рисунок 3.6 – График энтропийного потенциала

Решив задачу объединения однородных потенциалов в кластеры по методике п. 2.1 диссертации с уровнем мощности критерия $\beta_{O}^{ЭФ}$ =0,04, получили результаты объединения типовых нарушителей и категорируемых объектов в кластеры (таблица 3.14).

Таблица 3.14 – Таблица соответствий базовых ТН и категорий объектов

Типовые нарушители	Категория объекта	Энтропийная опасность Н	Вероятность безопасного состояния
X_1+(X_5+ X_6)	1 категория.	0,733	**0,99**
X_1	2 категория.	0,633	0,95
X_2, X_3+ (X_5+X_6)	3 категория,	0,497	0,93
X_3, X_5, X_6	4 категория	0,280	0,76
X_3, X_6, X_5	5 категория	0,239	0,69
X_3, X_5, X_6	6 категория	0,200	0,64
X_4	7 категория	0,122	**0,60**

С целью определения связей между характеристиками матрицы наблюдений

использовался один из главных методов факторного анализа – МГК [77, 78].

По данным таблицы 3.12, используя МГК, определим факторные нагрузки общих характеристик, которые приведены в таблице 3.15.

Таблица 3.15 – Факторные нагрузки характеристик

Частные виды потерь объектов от нарушителей	Факторы нагрузок (компоненты)					
	$F_{1\text{-полит.}}$	$F_{2\text{-финан., информ.}}$	F_3	F_4	F_5	F_6
Политические	**0,900**	-0,353	0,034	-0,08	0	0
Людские	**0,950**	-0,259	-0,023	0,18	0	0
Финансовые	0,451	**0,878**	-0,37	0	0	0
Экономические	**0,971**	-0,071	-0,041	0,04	0	0
Экологические	**0,976**	-0,167	-0,034	-0,14	0	0
Информационные	0,454	**0,879**	0,389	0	0	0

Первый фактор интерпретируем «политическая составляющая». Второй фактор определим как «финансовая» и «информационная» составляющая рассматриваемых элементов анализа. Вес первой компоненты составляет 75 %, второй – 20 %, третьей – 4,1 %, четвертой – 1,5 %, пятой – 0,49 %, шестой – 0,01 %.

Перейдем от матрицы факторных нагрузок к матрице главных компонент типовых нарушителей и категорируемых объектов (таблица 3.16).

Проведем кластерный анализ по первым трем компонентам при заданном уровне мощности критерия $\beta_O^{ЭФ} = 0{,}04$. Для этой цели использовали информационно-вероятностную модель формирования классов объектов. Результаты программного решения задачи приведены на рисунке 3.7 и таблице 3.17.

Таблица 3.16 – Факторные нагрузки категорий объектов и ТН

Нарушители, объекты	Энтропийный потенциал	Факторы объектов (компоненты)			
		$F_{1\text{-полит.}}$	$F_{2\text{-финан., информац.}}$	F_3	F_4
X_1	0,390	**1,412**	-1,446	-0,35	0,465
X_2	0,333	0,727	-1,27	-0,32	0,338
X_3	0,308	0,461	-1,356	-0,23	-1,75
X_4	0,048	-1,204	-0,116	-2,78	0,02
X_5	0,195	-0,464	1,57	1,155	-1,81
$\boldsymbol{X}_6$	0,204	-0,397	1,368	1,002	1,746
1 кат.	0,409	**1,72**	1,077	-0,12	-0,40
2 кат.	0,363	1,07	0,808	-0,08	-0,53
3 кат.	0,321	0,587	0,845	-0,10	1,308
4 кат.	0,152	-0,721	-0,28	0,018	0,276
5 кат.	0,111	-0,939	-0,304	0,882	0,23
6 кат.	0,106	-0,962	-0,408	0,918	0,103
7 кат.	0,021	-1,291	-0,488	0,918	0,103

Рисунок 3.7 – Результаты решения оценки энтропийных потенциалов

Таблица 3.17 – Соответствие типовых нарушителей категориям объектов

Типовой нарушитель	Категории объектов	Потенциал опасности H
X_1	1-я категория	0,390
$X_2, X_3+(X_5, \boldsymbol{X}_6)$	2-я категория	0,333
X_3	3-я категория	0,308
$X_3, \boldsymbol{X}_6, X_5$	4-я категория	0,204
$X_4, \boldsymbol{X}_6, X_5$	5-я категория	0,135
$\boldsymbol{X}_6, X_5$	6-я категория	0,106
X_4	7-я категория	0,048

Необходимо отметить, что потенциал подготовленности согласуется с потенциалом опасности последействий нарушителей. Кроме того, потенциал подготовленности нарушителя согласуется с их возможностями по преодолению СФЗ объектов, то есть каждому потенциалу нарушителя можно поставить соответствующий потенциал защиты объекта – величину эффективности СФЗ – (величину защищенности – например, вероятность безопасного состояния объекта). То есть требуется определить необходимую величину – вероятность безопасного состояния объекта – в зависимости от потенциала опасности базового нарушителя для соответствующей категории опасности объекта.

Очевидно, должно быть соответствие между потенциалом опасности типового нарушителя и степенью защищенности от его действий, то есть характер из-

менения зависимостей потенциалов нарушителей и противодействия им должны быть подобными функциями.

Если построить зависимость изменения энтропийных потенциалов от типа нарушителя и связать ее с требуемой величиной вероятности безопасного состояния по первому типу нарушителя (за верхнюю оценку принято значение вероятности защиты – 0,99 – величина близкая к предельной) и самого слабого типа нарушителя (чувствительность датчика обнаружения – 0,65 и вероятность своевременного прибытия – 0,95 дают величину безопасного состояния – 0,6), то есть сопоставим каждому типу нарушителя требуемую величину защищенности объекта (вероятность безопасного состояния) от его действий. Результаты вероятностей безопасного состояния СФЗ как подобные величины опасностям (типовым нарушителям) приведены в таблице 3.14.

Таким образом, определены базовые нарушители для каждой категории объектов, которые приведены в таблицах 3.14 и 3.17. Полученные результаты разными методами согласуются и не противоречат физическому смыслу. Результаты вероятностей безопасного состояния категорируемых объектов (таблицы 3.14) могут использоваться при обосновании требований к эффективности СФЗ категорируемых объектов [87].

3.3 Определение базовых угроз для категорируемых объектов с использованием кластерного анализа

Для подтверждения полученных результатов исследований решим ту же самую задачу методом кластерного анализа, который производит разбиение множества объектов на кластеры, основываясь на обобщенном сходстве признаков, то есть это совокупность методов многомерной классификации, целью которой является образование групп (кластеров) схожих между собой объектов [86].

На основании приведенных данных в таблице 3.15 необходимо провести классификацию 13 объектов по 6 признакам при помощи иерархического агломеративного метода и метода к- средних кластерного анализа на 7 категорий.

На 1 шаге рассчитаем среднее ($\bar{x}_j$) и среднеквадратичное отклонение (σ), используя таблицу исходных данных (таблица 3.18).

Таблица 3.18 – Данные для решения задачи кластерного анализа

Типовые нарушители и объекты	Масштаб потерь по энтропийной шкале для объектов и нарушителей					
	Политические	Людские	Финансовые	Экономические	Экологические	Информационные
X_1	0,878	0,878	0,555	0,878	0,878	0,555
X_2	0,621	0,621	0,116	0,621	0,621	0,116
X_3	0,555	0,555	0,116	0,555	0,555	0,007
X_4	0,007	0,007	0,116	0,116	0,007	0,116
X_5	0,116	0,116	0,621	0,116	0,173	0,621
X_6	0,173	0,173	0,555	0,173	0,116	0,621
1 кат.	0,621	0,621	0,621	0,878	0,878	0,878
2 кат.	0,555	0,555	0,621	0,621	0,621	0,621
3 кат.	0,173	0,555	0,555	0,555	0,555	0,555
4 кат.	0,173	0,173	0,173	0,173	0,173	0,173
5 кат.	0,116	0,116	0,116	0,173	0,173	0,173
6 кат.	0,116	0,116	0,116	0,116	0,116	0,116
7 кат.	0,007	0,007	0,007	0,007	0,116	0,116

На 2 шаге нормируем исходные данные по формуле, сформировав матрицу Z :

$$z_{ij} = \frac{x_{ij} - \bar{x}_j}{\sigma_j}. \tag{3.1}$$

На следующем шаге вычислим матрицу расстояний. Расстояния между *i*-ым и *j*-ым объектами считаем по формуле:

$$d_{ij} = \sqrt{\sum_{k=1}^{m} (x_{ik} - x_{jk})^2}. \tag{3.2}$$

Вычислив расстояния между объектами, объединим кластеры по методу ближнего соседа. Суть метода состоит в поиске в матрице D минимального расстояния (также объединение строк и столбцов, соответствующих данному расстоянию матрицы D с выбором минимального). К примеру:

$$d_{S_1,S_4} = \min\{d_{12},\ d_{15}\} = \min\{2,990;\ 3,277\} = 2,99. \tag{3.3}$$

Проведя 11 операций объединения кластеров, получим объединения (рисунок 3.8).

Элементы кластера номер 1 (Таблица.ПОСЛЕ.sta)
и расстояния до центра кластера.
Кластер содержит 5 набл.

	Набл.No. C_4	Набл.No. C_10	Набл.No. C_11	Набл.No. C_12	Набл.No. C_13
Расст.	0,064913	0,069886	0,024016	0,021644	0,075550

Элементы кластера номер 2 (Таблица.ПОС
и расстояния до центра кластера.
Кластер содержит 2 набл.

	Набл.No. C_5	Набл.No. C_6
Расст.	0,026889	0,026889

Элементы кластера номер 3 (Таблица.ПОСЛЕ.sta)
и расстояния до центра кластера.
Кластер содержит 6 набл.

	Набл.No. C_1	Набл.No. C_2	Набл.No. C_3	Набл.No. C_7	Набл.No. C_8	Набл.No. C_9
Расст.	0,230187	0,158164	0,204326	0,251259	0,147826	0,206868

Рисунок 3.8 – Метод к - средних для трех классов

Здесь на 1 шаге объединяются кластер 4 и 10, 11, 12 и 13. На 2 шаге объединяются кластер 5 и 6. На 3 шаге объединяются кластер 1 и 7, и 8, 3 и 9.

На рисунке 3.9 на 1 шаге объединяются кластер 5 и 6, 4 и 10, 11, 12 ,13. На 2 шаге объединяются кластер 1 и 7, 2 и 8, 3 и 9.

Элементы кластера номер 1 (Таблица.ПОСЛЕ.sta)
и расстояния до центра кластера.
Кластер содержит 7 набл.

	Набл.No. C_4	Набл.No. C_5	Набл.No. C_6	Набл.No. C_10	Набл.No. C_11	Набл.No. C_12	Набл.No. C_13
Расст.	0,101423	0,207653	0,193303	0,074793	0,070177	0,086222	0,138661

Элементы кластера номер 2 (Таблица.ПОСЛЕ.sta)
и расстояния до центра кластера.
Кластер содержит 6 набл.

	Набл.No. C_1	Набл.No. C_2	Набл.No. C_3	Набл.No. C_7	Набл.No. C_8	Набл.No. C_9
Расст.	0,230187	0,158164	0,204326	0,251259	0,147826	0,206868

Рисунок 3.9 – Метод к - средних для двух классов

Вывод: анализ данной классификации показывает, что почти все классы объединяются согласно логическому смыслу и не противоречат информационно-вероятностному методу. Недостатком данного метода является то, что метод кластерного анализа не учитывает весовую значимость вклада характеристик в формирование оценочного потенциала, то есть в оценку расстояний между классифицируемыми объектами.

Таким образом, более логичный результат определения базовых угроз получен при использовании информационно-вероятностного метода. Данный метод учитывает весовой вклад каждой компоненты в оценку привлекательности объекта и мотивированности нарушителя и формирует объединения в группы категории объектов и им соответствующие типы нарушителей. Полученные соотношения в группах и будут являться базовыми нарушителями для соответствующих категорий объектов.

3.4 Методика оценки интервала времени прогнозирования интенсивности действий террористических угроз на основе энтропийного подхода

Так как характеристики СФЗ проектируются на определенный период времени – жизненный цикл, то входные данные по террористическим угрозам должны прогнозироваться на определенный период времени (время модернизации СФЗ). Поэтому в разделе произведена оценка временного интервала прогнозирования развития террористических угроз как развитие системы и возникновение новой ситуации. Полученные результаты используются как входные данные при обосновании и оценке показателей эффективности проектируемой СФЗ.

Множество типовых нарушителей (угроз) определяется множеством их характеристик. Одной из характеристик нарушителя является вероятность действий, то есть, с какой интенсивностью нарушитель будет оказывать воздействие на охраняемый объект определенной категории. С учетом реалией сегодняшнего времени такую характеристику можно определить как временной ресурс на подго-

товку противоправных действий [20]. Чтобы определить эту характеристику, необходимо спрогнозировать развитие террористических угроз, то есть оценить интенсивность действий типовых нарушителей к определенному моменту времени. В качестве меры эволюции системы выступает информационная энтропия. Очевидно, что чем дальше по времени осуществляется прогноз развития, тем больше неопределенность и тем меньше достоверность и надежность получаемых характеристик, то есть имеется оптимально приемлемое время прогнозирования.

Особенность информационного метода заключается в определении величины изменения прогнозируемых параметров развития ситуации (системы) в виде порции приращения соотношений энтропии. При достижении заданной величины соотношений энтропии (ошибок прогнозирования) производится оценка характеристик системы и глубины прогнозирования по времени. Полученные характеристики являются оптимальными, так как система обладает наилучшим соотношением энтропии как меры степени упорядоченности и организованности структуры системы.

Если порция энтропии от предыдущей системы будет велика, то система будет недоразвитой, то есть это модернизация старой системы (не новая система).

Если порция энтропии от предыдущей системы мала, то возникает опасность, что новая система будет не приспособлена (не адаптирована) к существующей среде, то есть новая система обладает малой преемственностью от предыдущей системы.

Вопросы прогнозирования рассматривались в зарубежных источниках [89], а также в работах отечественных исследователей [68, 90] только с позиции теории принятия решений, как выбор наилучшей системы из совокупности существующих систем. Результатом же применения данного метода являются прогнозируемые характеристики развития террористических угроз на определенный момент времени, которые являются входными данными для задания требований к СФЗ.

Разработка методов и средств прогнозирования включает следующие задачи:

1) разработку методов и средств построения функций, описывающих поведение прогнозируемого параметра;

2) разработку методов и средств оценки временного интервала прогноза при заданных ошибках.

В разделе исследуется вторая задача – прогнозирование временного интервала. Конечным результатом исследований должны быть интенсивности действий типовых нарушителей на определенный период времени при заданных ошибках первого и второго рода.

Типовых нарушителей выберем согласно руководящим документам [2, 34]. Приказом министра промышленности и энергетики РФ от 04.05.2007 №150 «Об утверждении рекомендаций по антитеррористической защищенности объектов промышленности и энергетики» и Постановлением правительства № 875 от 29.08.2014 «Об антитеррористической защищенности объектов ФСТЭК...» определены следующие типы нарушителей. Модель нарушителя включает шесть различных типов потенциальных нарушителей. Характеристики нарушителей были приведены в таблице 1.2:

x_1 – внешний нарушитель 1-го типа;

x_2 – внешний нарушитель 2-го типа: малочисленная группа лиц (2 – 5 человека). Целью такого нарушителя является совершение террористического акта;

x_3 – внешний нарушитель 3-го типа: одиночный подготовленный нарушитель, не имеющий санкционированного доступа на территорию объекта. Его цель - террористический акт;

x_4 – внешний нарушитель 4-го типа;

x_5 – внутренний нарушитель 1-го типа: работник объекта (специалист), имеющий санкционированный доступ на территорию объекта;

x_6 – внутренний нарушитель 2-го типа: работник охраны объекта.

Имеется, например, определенная статистика по каждому типу нарушителя в регионе (федерации) за предыдущие несколько лет, которая представлена в таблице 3.19. Информационное поле таблицы – количество проявлений в регионе за год.

Таблица 3.19 – Статистика террористических угроз

Множество типов нарушителей	Временной интервал рассматриваемых ситуаций (время)				
	2010 г.	2011 г.	2012 г.	2013 г.	2014 г.
X_1	2	3	2	1	2
X_2	4	5	4	5	6
X_3	7	6	8	7	8
X_4	2	3	1	4	3
X_5	3	2	3	4	4
X_6	2	1	3	1	2

Постановка задачи. Необходимо путем прогноза определить интенсивности действий типовых нарушителей и оценить глубину временного интервала прогнозирования с использованием информационного критерия оптимальности развития систем (определить продолжительность прогноза).

Используя информационно-вероятностный метод террористическую ситуацию каждого интервала времени (года) опишем в виде энтропии. Математический аппарат модели опирается на источники [68, 90]. Прикладной характер использования математического аппарата приведен в параграфе 2.1 настоящей диссертации. Однако отдельные моменты в новой интерпретации необходимо повторить.

Решение задачи.

Информационное отображение ситуации укладывается в следующую схему: имеется n сравниваемых между собой периодов времени; каждому периоду времени поставлена в соответствие совокупность m типовых нарушителей, определяющих энтропийный потенциал периода времени. Входные данные прогнозирования характеризуются таблицей 3.20, у которой столбцы – временная шкала развития ситуаций $\{A_i\}$, строки – множеством типов нарушителей.

Таблица 3.20 – Модифицированная морфологическая матрица

Множество типов нарушителей	Временная шкала развития ситуации				
	$\{A_i\}$	...	$\{A_i\}$	…	$\{A_n\}$
X_1	X_{11}	…	X_{1i}	…	X_{1n}
…	…	…	…	…	…
X_j	X_{j1}	…	X_{ji}	…	X_{jn}
…	…	…	…	…	…
X_m	X_{m1}	…	X_{mi}	…	X_{mn}

При решении данной задачи ошибка первого рода $\alpha_o^{ЭФ}$ заключается в непринятии гипотезы H_o, когда она верна. В нашем случае чем больше $\alpha_o^{ЭФ}$, тем больше вероятность оказаться в прежней ситуации, то есть принять старую систему (параметры новой ситуации незначимо отличаются от начальной ситуации).

Совершить ошибку второго рода $\beta_o^{ЭФ}$ – принять гипотезу H_o, когда она неверна. Она характеризует степень порции энтропии преемственности от предыдущей ситуации. Таким образом, чем больше $\beta_o^{ЭФ}$, тем больше вероятность того, что прогнозируемые параметры не будут обладать преемственностью от исходных данных начальной системы.

В нашем случае ошибка второго рода означает, что дальнейшее прогнозирование нецелесообразно, так как возникает большая неопределенность ситуации, то есть параметры прогнозируемой новой ситуации обладают низкой надежностью и значимо отличаются от исходных, то есть большое различие.

Величины $\alpha_O^{ЭФ}$ и $\beta_o^{ЭФ}$ количественно характеризуют систему договоренностей. Для принятия гипотезы H_O необходимо заказчику и разработчику договориться о численном значении $\alpha_O^{ЭФ}$ и $\beta_o^{ЭФ}$. Если выполняется условие:

$$\alpha_i^{ЭФ} \le \alpha_O^{ЭФ} \text{ и } \beta_i^{ЭФ} \le \beta_O^{ЭФ}, \tag{3.4}$$

то гипотеза H_o (временной интервал прогнозирования) принимается, в противном случае гипотеза отвергается.

Прогнозирование поведения параметров ситуации на будущие года по данным таблицы 3.1 осуществлялось на основе метода наименьших квадратов (многочлен Чебышева) по критерию:

$$\min \sum_{i=0}^{n} [f(x_i) - P_3(x_i)]^2, \tag{3.5}$$

с использованием полинома третьей степени $P_3(x_i)$, так как данный полином описывает статистические результаты с наименьшей ошибкой согласования со статистическими данными $f(x_i)$ таблицы 3.19 [20].

Последовательно с помощью аппроксимирующей функции получали прогнозируемые результаты ситуаций. К полученным данным таблицы 3.19 применяется математический аппарат информационно-вероятностного метода главы 2.1 (формулы 2.5 – 2.14). Задача решается итерационно, пока ошибки не достигнут заданных значений. Процесс расчета автоматизирован при помощи разработанной программы на языке программирования C# [74], результаты приведены на рисунке 3.10. Выборочный вид полинома имеет вид:

$$P_3(x) = 0{,}15227 - 0{,}09448 \cdot x + 0{,}03091 \cdot x^2 - 0{,}00287 \cdot x^3. \qquad (3.6)$$

	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
x1	2	3	2	2	3	2,8	2,9	3	3,1	3,2	3,3
x2	4	5	4	5	6	6,4	6,8	7,2	7,6	8	8,4
x3	7	6	8	7	8	8,4	8,7	9	9,3	9,6	9,9
x4	2	3	1	4	3	3,8	4,1	4,4	4,7	5	5,3
x5	3	2	3	4	4	4,8	5,2	5,6	6	6,4	6,8
x6	2	1	3	1	2	1,8	1,8	1,8	1,8	1,8	1,8
Энтроп	0,70077	0,755548	0,702515	0,774806	0,869529	0,942349	0,967328	0,9896	1,01238	1,034135	1,054956
I	0,16876	0,113982	0,167015	0,094723	0	0,038446	0,070991	0,101176	0,130487	0,158532	0,185426
II	0,0932	0,07884	0,09275	0,07371	0,0478	0,02709	0,01983	0,01327	0,0065	5E-05	0,00637

Рисунок 3.10 – Прогнозирование развития ситуации

Таким образом, полученные результаты показывают, что прогнозирование развития террористических угроз по времени целесообразно осуществлять на шесть лет. При этом ошибка второго рода составляет $\beta_i^{ЭФ} = 0{,}0064$, то есть G_H^i стремится к наилучшему соотношению удельного веса порции преемственности энтропии (непредсказуемости и детерминированности). Характеристики террористических угроз на 2020 г. приведены на рисунке 3.10 в последнем столбце и используются как входные данные для следующего этапа проектирования СФЗ (задание требований к показателям эффективности СФЗ) [91].

Дальнейшее по времени прогнозирование нецелесообразно, так как увеличивается ошибка первого рода и второго рода, то есть параметры террористической ситуации обладают низкой достоверностью (надежностью) и не согласуются с исходными данными.

3.5 Выводы

1. Прогнозирование интенсивности террористических угроз по времени целесообразно осуществлять на шесть лет. При этом G_H^i стремится к наилучшему соотношению удельного веса порции преемственности энтропии.

2. Интенсивности террористических угроз на 2020 г. могут быть использованы как входные данные в методике при задании требований к СФЗ.

3. Потенциалы опасности нарушителей и потенциалы последствий целевой реализации согласуются.

4. Основной комплексной характеристикой типовых нарушителей является мотивация к действию, которая влечет за собой уровень оснащенности, физической и информационной подготовленности и соответственно степень последствий реализации цели.

5. Полученные весовые потенциалы типовых нарушителей и степени вероятностей защищенности от них по разным методикам однородны и не противоречат физическому смыслу природы явлений. Результаты могут использоваться при формировании модели нарушителя и определении базового нарушителя к каждой категории опасности объектов.

6. Определены базовые нарушители для каждой категории объектов. Полученные результаты разными методами согласуются и не противоречат физическому смыслу явлений. Результаты вероятностей безопасного состояния категорируемых объектов могут быть использоваться при обосновании требований к эффективности СФЗ [133].

ГЛАВА 4 МОДЕЛЬ ОПРЕДЕЛЕНИЯ ТРЕБОВАНИЙ К СИСТЕМЕ ФИЗИЧЕСКОЙ ЗАЩИТЫ

4.1 Построение концептуальной имитационной модели функционирования системы физической защиты при обеспечении безопасности объекта

Концептуальная модель функционирования СФЗ предназначена для определения необходимых требований к уровню безопасности объекта в зависимости от его важности (стоимости потерь), стоимости СФЗ и типа нарушителя (интенсивности и степени воздействия). В качестве требований к СФЗ определены следующие частные показатели эффективности, полученные из формулы (1.4): вероятность обнаружения угрозы – P_o, вероятность своевременного прибытия сил реагирования – $P_{\text{СВП}}$, при условии обнаружения нарушителя и получения команды. Заданная эффективность системы может быть обеспечена при множестве разных значений частных показателей, внося разный вклад в эффективность СФЗ, и поэтому частные показатели должны быть обоснованы.

Характер изменения зависимости уровня ущерба от стоимости СФЗ, полученной при условии увеличения защищенности $P_З$ с ростом стоимости СФЗ, приведен на рисунке 1.14. Из рисунка следует, что кривая ущерба в некоторой точке имеет наименьшее значение, которое можно считать оптимальным. Эта кривая называется функцией риска.

Рост затрат на СФЗ выше оптимального значения ведет к увеличению суммарных затрат. В этом случае повышение надежности СФЗ и соответствующее снижение вероятности ущерба нивелируется чрезмерно высокой стоимостью самой СФЗ.

Поэтому наилучшей стратегией, видимо, является использование СФЗ, обеспечивающей минимум суммарных затрат. Таким образом, необходимо с использованием модели реализовать функционал:

$$F = П_{УГР}(P_З(K_i, \lambda_{ji})) + C_{СФЗ}(P_З(K_i, \lambda_{ji})) \to \min.$$

Вид и характер поведения целевой функции ущерба известен, однако параметры функционала управления неизвестны, то есть нельзя определить минимум функции. Получение аналитического выражения, описывающего модель функционирования СФЗ с учетом характеристик обнаружения угрозы, вероятности своевременного и точного прибытия сил нейтрализации, составляет непреодолимую сложность. Поэтому использовалась имитационная модель функционирования СФЗ. Использование марковской модели невозможно – не выполняется условие марковости для переходов между событиями. Полумарковские модели чрезвычайно сложны в описании и требуют постоянного уточнения в процессе моделирования.

Для определения оптимальных значений параметров целевой функции, а, следовательно, и параметров проектируемой СФЗ необходимо следующее:

- построить имитационную пространственно-временную модель функционирования СФЗ и оценить ее адекватность;

- сформировать план проведения активного эксперимента, на основе которого с помощью неоднократного моделирования необходимо получить данные для проведения регрессионного анализа;

- получить аналитическое уравнение потерь стоимости объекта от воздействия угроз и затрат на СФЗ, провести его анализ;

- смещая центр плана в сторону антиградиента, последовательно получать новую аналитическую модель с меньшим значением потерь. Как только градиент изменит направление в этой области, необходимо найти точку с минимальным значением потерь;

- по центральной точке плана эксперимента определить требуемые значения параметров проектируемой СФЗ.

Решение задачи. Имитационная модель функционирования системы включает объект, систему угроз и СФЗ, которая, в свою очередь, включает системы обнаружения и систему реагирования и нейтрализации угрозы.

Считаем, что на предыдущих этапах проектирования СФЗ проведено категорирование объекта охраны и выявлена типовая базовая угроза для объекта и ин-

тенсивность ее действий – λ_{ji} как частное интенсивности базового нарушителя на количество объектов данной категории в регионе. В данной задаче интенсивность принята один раз в двенадцать месяцев.

Входом в модель является стоимость СФЗ как функция от вероятности обнаружения P_o, коэффициента задержки *Kz* и коэффициента своевременного прибытия сил реагирования *Кс*, а также стоимость объекта *С*, стоимость ущерба от воздействия нарушителя угрозы и интенсивность воздействия типового нарушителя.

Концептуальная модель функционирования СФЗ представлена на рисунке 4.1.

Рисунок 4.1 – Концептуальная модель функционирования СФЗ

λ_{ji} – интенсивность проявления *j*-го нарушителя;
Po – вероятность обнаружения нарушителя;
$P_{СВП}$ – вероятность своевременного прибытия сил реагирования;
1 – *Po* – вероятность потерь ресурсов объекта (реализации угрозы) – вероятность необнаружения нарушителя;
1 – $P_{СВП}$ – вероятность несвоевременного прибытия сил реагирования (вероятность реализации цели нарушителем).

Из перечисленных потоков моделируется только один входной поток λ_0, а остальные вероятности переходов являются производными в зависимости от условий возникновения ситуации.

Дальнейшая детализация модели нецелесообразна, так как модель переходит из концептуальной в принципиальную, которая используется для оценки уже существующей или спроектированной СФЗ.

Рассмотрим математические посылки имитационного моделирования.

Учитывая принцип зональности при построении СФЗ, сценарий взаимодействия угрозы и сил реагирования представим на рисунке 4.2.

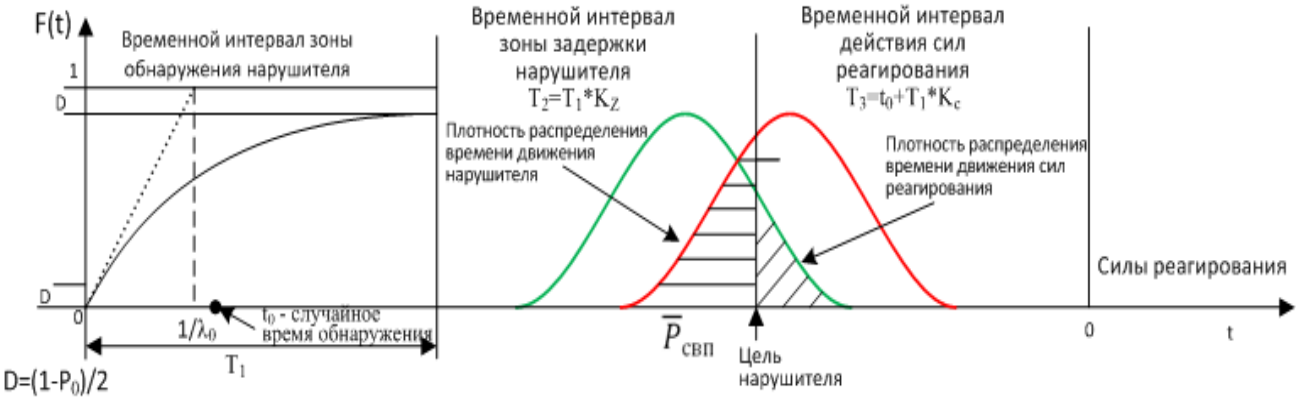


Рисунок 4.2 – Модель противодействия нарушителя и СФЗ

Моделируется две величины: время атаки угрозы и время реакции СФЗ на угрозу. По их соотношениям формируется результат работы СФЗ. Время атаки состоит из случайного времени преодоления зоны обнаружения T_1 и случайного времени преодоления зоны задержки T_2.

Ввиду того, что эти участки преодолеваются угрозой первый раз (нет опыта преодоления этого участка), поэтому время преодоления зоны обнаружения и зоны задержания составляет большую неопределенность. Нет статистики по закону распределения времени преодоления нарушителем неизвестного пересеченного участка местности. Проведенный эксперимент для определения закона распределения времени перемещения (преодоления) участка показал, что экспериментальные данные не противоречат нормальному закону распределения. Интервалы времени преодоления зоны обнаружения и зоны задержании формируются по нормальному закону в соответствии с рисунком 4.2.

Математическое ожидание интервала времени обнаружения T_1 определялось из экспоненциального закона обнаружения в соответствии с заданным уровнем вероятности обнаружения (рисунок 4.2). Это положение взято из теории обнаружения радиолокационных целей [92]. Если в течение этого времени угроза не обнаружена, то считается, что произошел несанкционированный доступ. Величи-

на моделируемого времени T_1 носит относительную величину и не имеет единиц измерения.

Интервал времени T_2 связан с интервалом T_1 через коэффициент Kz, учитывающий степень подготовки угрозы и степень оснащенности объекта заградительными средствами.

Общее время движения угрозы будет складываться из случайных величин T_1 и T_2, которые моделируются по нормальному закону.

Рассмотрим процесс реакции СФЗ на угрозу.

Вероятность обнаружения угрозы зависит от длительности времени пребывания на объекте и подчиняется экспоненциальному закону распределения:

$$Po = 1 - e^{-\lambda_o t}. \tag{4.1}$$

В формуле 4.1 интенсивность выступает как параметр закона распределения и характеризует эффективность системы обнаружения.

Необходимо от вероятности обнаружения перейти во временную шкалу времени обнаружения. Нас интересует интенсивность в единицу времени. Выразим из формулы 4.1 величину λ_0, осуществляя нормализацию для единицы времени, то есть примем t = 1. Тогда интенсивность будет зависеть от вероятности обнаружения и определяться по формуле:

$$\lambda o = -\ln(1 - Po), \tag{4.2}$$

где P_0 – заданная вероятность обнаружения нарушителя при проникновении.

Тогда в соответствии с заданной интенсивностью обнаружения λ_0 случайное время обнаружения будет определяться по формуле:

$$t_O = -\frac{1}{\lambda o}\ln(1 - R), \tag{4.3}$$

где R – случайная величина, распределенная по равномерному закону в интервале от 0 до 1. После подстановки формулы 4.2 в формулу 4.3 получаем случайное время обнаружения угрозы в виде зависимости:

$$t_o = \frac{\ln(1-R)}{\ln(1-Po)} \cdot t, \ при\, t = 1, \qquad (4.4)$$

то есть от вероятности обнаружения перешли к нормированному среднему времени обнаружения.

После формирования случайной величины t_0 формируется случайный интервал времени $T_З$ – это математическое ожидание времени движения сил реагирования до охраняемого элемента объекта после обнаружения, которое будем определять в соответствии с рисунком 4.2.

Итак, с момента времени t_0 (после обнаружения вторжения) начинает функционировать система реагирования и нейтрализации нарушителя. Вероятность своевременного прибытия для нейтрализации вторжения зависит от момента обнаружения проникновения нарушителя. Чем позднее время обнаружения, тем меньше вероятность своевременного прибытия, то есть вероятность обнаружения и вероятность своевременного прибытия функционально зависимы.

Время движения сил реагирования и нейтрализации угрозы моделируется по нормальному закону, так как многократное (тренированное) перемещение по известному изученному участку территории – это определенная работа, а время выполнения работы подчинено нормальному закону распределения.

Будем полагать, что силы реагирования и нейтрализации находятся на нормированном удалении от элемента охраны ближе, чем временное расстояние между границей объекта и элементом охраны, то есть математическое ожидание времени движения сил реагирования составит $T_З$. В противном случае эффективность нейтрализации угрозы группой реагирования будет равна нулю. Математическое выражение для определения среднего времени реакции сил реагирования имеет вид:

$$T_З = to + T_1 \cdot Kc, \qquad (4.5)$$

где Kc – коэффициент, учитывающий среднее время удаления сил реагирования от критического элемента объекта охраны. Этот коэффициент вместе с коэффициентом Kz определяет вероятность своевременного прибытия сил реагирования $P_{СВП}$.

Так как среднее квадратичное отклонение нам неизвестно, то будем считать, что распределение относительно математического ожидания будет укладываться в шесть σ (правило трех σ).

Вероятность своевременного прибытия сил реагирования $P_{СВП}$ определяем как среднее статистическое значение случаев успешного реагирования на обнаруженные угрозы.

4.2 Проведение эксперимента и формирование уравнения отклика целевой функции затрат на создание систем физической защиты

Для обеспечения необходимой точности результатов оценки эффективности СФЗ (3 %) процесс моделирования проводился 10 000 раз.

Адекватность модели подтверждается корректным описанием процесса функционирования и применением хорошо апробированного математического аппарата. Адекватность модели проверялась в точке равновесия системы при P_0=0,5 и $P_{СВП}$ =0,5 при этом в среднем получили 750 реализаций угроз успешных и 250 неуспешных, то есть результат не противоречит физической сущности функционирования СФЗ.

Расходы на СФЗ могут составлять от 10 до 20 % от стоимости охраняемого объекта [20, 36]. При отсутствии всяких данных о величине затрат на СФЗ в зависимости от вероятности обнаружения и вероятности своевременного прибытия сил реагирования и величине ущерба от реализации угрозы примем допущения:

- стоимость СФЗ связана линейно с вероятностью обнаружения угрозы. Стоимость СФЗ увеличивается на 1 % от стоимости объекта при увеличении вероятности обнаружения на одну десятую;

- стоимость СФЗ связана с коэффициентами *Кс* и *Kz* так же линейно (определяют вероятность своевременного прибытия сил реагирования). Стоимость СФЗ увеличивается на 0,4 % и 0,7 % от стоимости объекта при увеличении соответственно *Кс* и *Kz* на одну десятую;

- ущерб от проникновения угрозы составляет 30 % от стоимости объекта *С*.

Текущая годовая цена потерь от реализации угроз и обслуживания СФЗ определялась по формуле:

$$Ц = C \cdot (M \cdot 0,3 + 0,1 \cdot Po + 0,04 \cdot (1 - Kc) + 0,07 \cdot Kz) + Co, \qquad (4.6)$$

где M – среднее количество реализованных угроз в год;

C – стоимость объекта составляет 100 000 000 руб.;

C_0 – стоимость СФЗ, связанная с постоянными расходами, независящая от ее оперативных свойств (например, расход на электроэнергию, заработная плата персонала, техническую диагностику). C_0 = 3 % от С;

Kc – коэффициент стоимости СФЗ, связанный удаленностью охраняемого элемента и караула СФЗ (при Kc = 0, караул находится в непосредственной близости от охраняемого элемента);

Kz – коэффициент стоимости СФЗ, связанный со степенью оснащенности объекта заградительными средствами.

Для получения уравнения регрессии затрат на СФЗ и потерь системы от проникновения угроз формировалась полная матрица планирования эксперимента (таблица 4.1), в которой x_1, x_2, x_3 – это соответственно факторы P_o, Kz, Kc, а . x_1x_2, x_1x_3, x_2x_3, $x_1x_2x_3$ – взаимодействие соответствующих факторов.

Уравнение регрессии имеет вид:

$$\bar{y} = b_0x_0 + b_1x_1 + b_2x_2 + b_3x_3 + b_{12}x_1x_2 + b_{13}x_1x_3 + b_{23}x_2x_3 + b_{123}x_1x_2x_3 \qquad (4.7)$$

Если полученная линейная модель неадекватна, то это значит, что не удается аппроксимировать поверхность отклика плоскостью. В этом случае или уменьшают интервалы варьирования, или выбирают другую точку в качестве базового уровня [93 - 94].

Таблица 4.1 – Матрица планирования эксперимента

Номер опыта	Кодированные входные факторы (управляемые переменные)							
	X_0	X_1	X_2	X_3	X_1X_2	X_1X_3	X_2X_3	$X_1X_2X_3$
1	+	-	-	-	+	+	+	-
2	+	+	-	-	-	-	+	+
3	+	-	+	-	-	+	-	+
4	+	+	+	-	+	-	-	-
5	+	-	-	+	+	-	-	+
6	+	+	-	+	-	+	-	-
7	+	-	+	+	-	-	+	-
8	+	+	+	+	+	+	+	+

Так как в полученном уравнении число оцениваемых коэффициентов регрессии равно числу опытов N, следовательно, степеней свободы для проверки его адекватности нет. Поэтому статистический анализ начинался с проверки значимости коэффициентов по t – критерию для уровня значимости 0,05.

По коэффициентам функции можно только определить направление движения базовой точки для уменьшения функции потерь, но оптимальные значения параметров нельзя определить, так как функция определена только в области варьирования параметров. Методологически данная задача решается следующим образом:

1. определяется градиент функции, и затем точка центра плана эксперимента перемещается в направлении антиградиента на границу области определения;

2. в данной точке вновь строится план проведения эксперимента и производится моделирование для получения нового уравнения регрессии.

Операция 1 и 2 повторяются до тех пор, пока градиент функции изменит знак на противоположный. Это и будет минимальное значение затрат на СФЗ. По мере приближения к оптимальному значению функции свободный член будет уменьшаться (затраты уменьшаются), коэффициенты уравнения также будут уменьшаться. С геометрической точки зрения это свидетельствует о приближении описываемой плоскости к впадине выпуклой поверхности**.**

На основе теоретического материала, с помощью программных средств, построена модель СФЗ. Входные экспериментальные данные следующие.

Начальную базовую точку выбрали: *Po*=0,6; *Kc*=0,4; *Kz*=0,6. После моделирования в каждой точке плана получили данные затрат на СФЗ, представленные на рисунке 4.3 – первая – третья колонки.

Определялись средние значения и дисперсии в каждой точке плана. Средние значения опытных данных представлены в четвертой колонке рисунка 4.3.

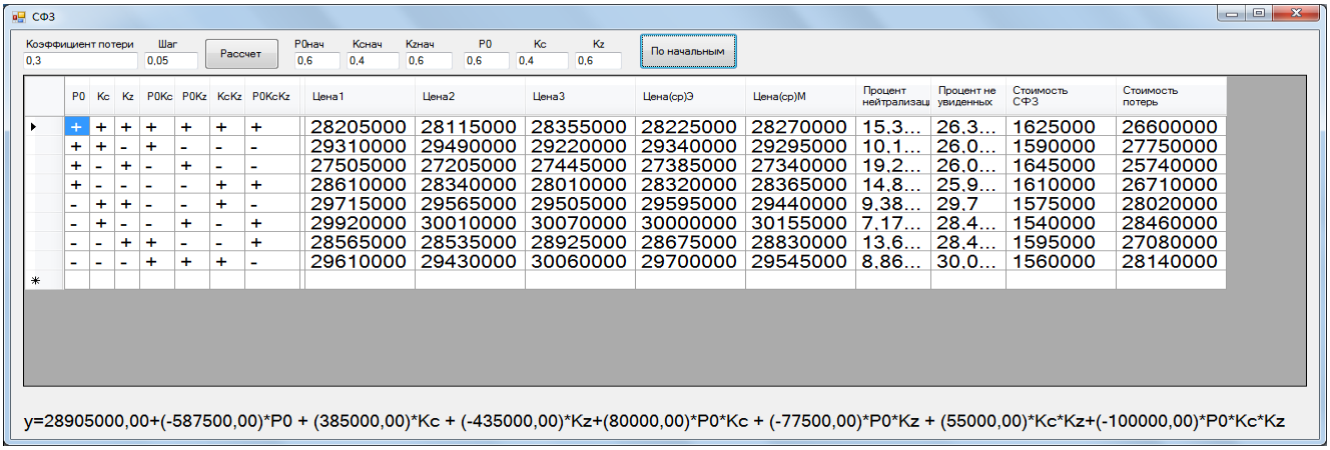


Рисунок 4.3 – Пример реализации модели СФЗ

Для оценки однородности дисперсий определялось расчетное значение G – критерия Кохрена по формуле:

$$G = \frac{S_j^2{}_{\max}}{\sum_{j=1}^{N} S_j^2} = 0{,}189. \tag{4.8}$$

Критическое значение G – критерия по таблице для уровня значимости α=0.05; числа степеней свободы f =3-1=2 и числа суммируемых оценок равно N:

$$G_{табл}(\alpha = 0{,}05; N = 8; f = 2) = 0{,}5127. \tag{4.9}$$

Расчетное значение меньше табличного значения, поэтому гипотеза об однородности ряда дисперсий выходного параметра не отвергается. В качестве оценки дисперсии воспроизводимости эксперимента определим среднюю дисперсию:

$$S^2_{воспр} = \frac{\sum_{j=1}^{N} S_j^2}{N} = 205500000000; \tag{4.10}$$

$$f_{воспр} = N \cdot (l - 1) = 16, \tag{4.11}$$

где l – число опытов в каждой точке плана.

Все предпосылки для проведения множественного регрессионного анализа выполняются, поэтому можно приступить к расчету коэффициентов уравнения регрессии.

Коэффициенты уравнения регрессии определялись по формуле:

$$b_i = \frac{1}{N}\sum_{j=1}^{N} x_{ji}\,\bar{y}_{iэ}. \qquad (4.12)$$

Таким образом, уравнение приближенной регрессии будет иметь вид:

$$\bar{y} = 28905000 - 587500Po + 385000Kc - 435000Kz + \\ +80000PoKc - 77500PoKz + 55000KcKz - 100000PoKcKz. \qquad (4.13)$$

В полученном уравнении число оцениваемых коэффициентов регрессии равно числу опытов *N* и степеней свободы для проверки его адекватности нет, поэтому статистический анализ начнем с проверки значимости коэффициентов.

Проверка значимости оценок коэффициентов регрессии:

$$t_i = \frac{|b_i|}{S_{b_i}}; \qquad (4.14),$$

$$S_{b_i} = \frac{S_{\bar{y}}}{\sqrt{N}} = \sqrt{\frac{S^2_{воспр}}{lN}}; \qquad (4.15)$$

$$S_{b_i} = 104208,32;$$

$$t_{0расч} = 37328; \qquad t_{1расч} = 9,5; \quad t_{2расч} = 6,2; \qquad t_{3расч} = 5,3;$$

$$t_{12расч} = 0,08; \qquad t_{13расч} = 1,02; \quad t_{23расч} = 0,01; \quad t_{123расч} = 0,5.$$

Проверка статистической гипотезы вида:

$$H_0 : b_i = 0; \quad H_1 : b_i \neq 0.$$

Определяем табличное значение критерия *t* - критерия:

$$f = f_{воспр} = 16; \; t_{табл}(0,05, \quad f = 16) = 1,75.$$

Коэффициенты, для которых выполняется условие

$$t_{расч} > t_{табл}, \qquad (4.16)$$

следует признать статистически значимыми и оставить в уравнении регрессии, а все остальные исключить.

Уравнение регрессии принимает вид:

$$\overline{y} = 28905000 - 587500Po + 385000Kc - 435000Kz, \qquad (4.17)$$

Проверка адекватности уравнения регрессии по результатам эксперимента. Определяем расчетное значение F - критерия:

$$F_{расч.S} = \frac{S^2_{ад}}{S^2_{воспр}};\ S^2_{воспр} = 205500000000;\ f_{воспр} = 16;$$

$$S^2_{ад} = \frac{l\sum_{j=1}^{N}(\overline{y}_{jэ} - \overline{y}_j)^2}{N-h}. \qquad (4.18)$$

где h – количество коэффициентов в уравнении.

Определим значения оценок выходного параметра $\overline{y}_j$ по результатам вычислений с использованием полученного уравнения приближенной регрессии. Результаты представлены в пятой колонке рисунка 4.3.

Вычисляем оценку дисперсии адекватности:

$$S^2_{ад} = 18037500000.$$

Вычисляем расчетное значение F - критерия:

$$F_{расч} = \frac{S^2_{ад}}{S^2_{воспр}} = 0{,}126.$$

Для проверки гипотезы об адекватности полученной модели определяем из таблицы критическое значение F - критерия для уровня значимости α = 0.05 и степеней свободы числителя:

$$f_1 = N - h = 4,$$

и знаменателя f_2 = 16; $F_{табл} = 4{,}68.$

Сравниваем расчетное и табличное значения F - критерия:

$$F_{расч} = 0{,}126 < F_{табл} = 4{,}68.$$

Следовательно, полученное уравнение регрессии адекватно описывает исследуемый процесс, то есть полином согласуется с экспериментальными данными моделирования.

4.3 Получение оптимальной величины уровня риска на основе градиентного метода оптимизации для задания рациональных требований безопасности

Получив уравнение регрессии со значимыми коэффициентами, перейдем к этапу определения оптимальных коэффициентов (показателей) СФЗ. Для этого будем варьировать входные параметры модели *Po, Kz* в сторону увеличения тех параметров, которые имеют отрицательный коэффициент, и уменьшение параметров с положительными коэффициентами *Kc* (4.19):

$$\overline{y} = 28905000 - 587500\,Po\uparrow + 385000\,Kc\downarrow - 435000\,Kz\uparrow . \qquad (4.19)$$

То есть план эксперимента (базовую точку) будем смещать в сторону минимума по антиградиенту функции (рисунок 4.4) и получать новые уравнения для очередной точки [95 - 99].

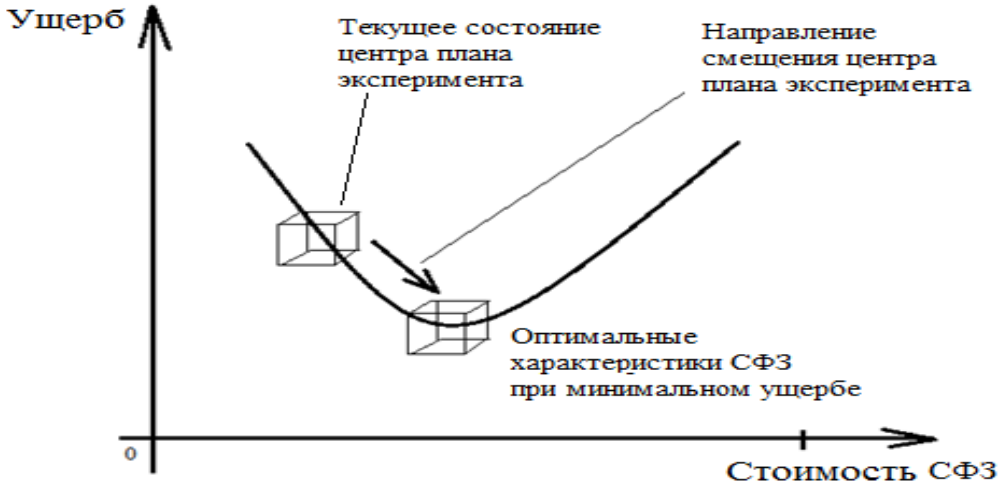


Рисунок 4.4 – Смещение плана эксперимента по функции риска

После нескольких итераций моделирования и перемещения базовой точки плана эксперимента получили уравнение регрессии с минимальными по модулю коэффициентами (рисунок 4.5). Из этого следует, что мы достигли минимальных параметров функции оценки ущерба (4.20). Представлено полное уравнение, чтобы оценить влияние взаимодействия факторов:

$$\overline{y} = 4068750 - 731250\,Po + 156250\,Kc - 76250\,Kz - \\ -96250\,Po\,Kc + 83750\,Po\,Kz - 98750\,Kc\,Kz + 13750\,PoKcKz\,. \quad (4.20)$$

В полученной области определения (в объеме куба) определялась точка с минимальным значением функции ущерба (риска).

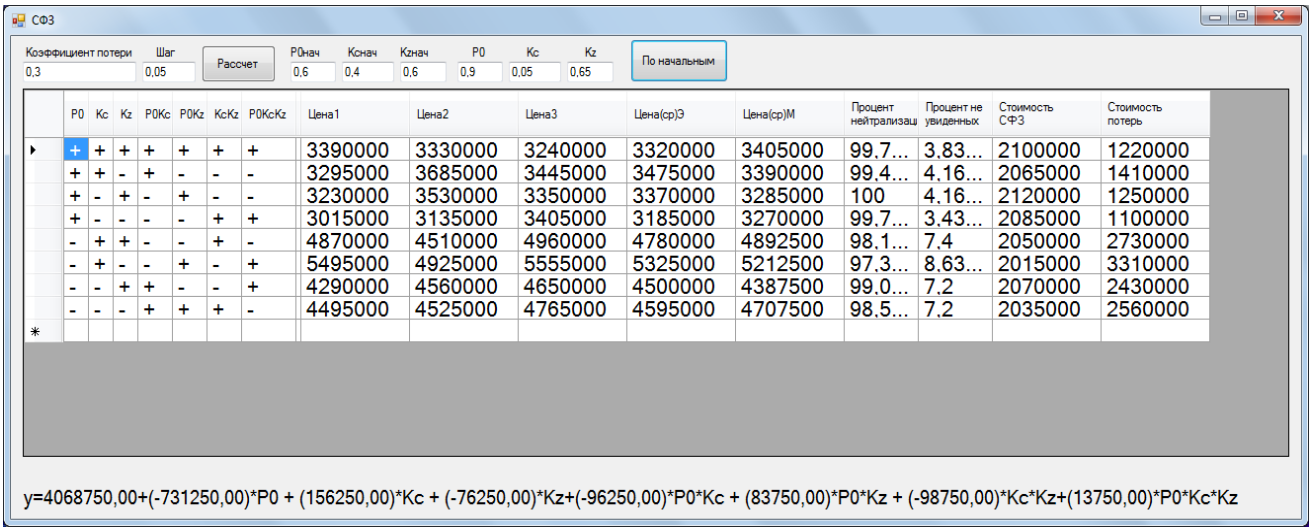


Рисунок 4.5 – модель СФЗ с оптимальными параметрами

Таким образом, при проектировании СФЗ для данного объекта необходимо задать следующие величины параметров СФЗ: вероятность обнаружения угрозы – 0,9; коэффициент задержки угрозы Kz – 0,6; коэффициент расположения сил реагирования Kc – 0,05.

Для вычисления величины вероятности своевременного прибытия в точку перехвата $P_{СВП}$ используется модель, отражающая рост вероятности своевременного прибытия сил реагирования по мере увеличения времени задержки нарушителей на физических барьерах и по мере сокращения времени перемещения сил реагирования на требуемое расстояние [43, 100]:

$$P_{СВП} = \exp[1,7(t_d - t_f)/\sigma]/[1+\exp[1,7(t_d - t_f)/\sigma]. \quad (4.21)$$

Вероятность $P_{СВП}$ является функцией средних значений времени t_d задержки нарушителей физическими барьерами, времени t_f занятия позиций силами реагирования и среднеквадратичных отклонений σ. Время занятия позиций подраз-

деляется на время сборов сил реагирования и на время ее прибытия к месту развертывания для встречи нарушения. Данные величины коэффициентов *Kz* и *Kc* обеспечивают вероятность своевременного прибытия сил реагирования $P_{СВП} = 0{,}8$.

Для реализации модели разработано программное средство на языке C#, свидетельство о государственной регистрации № 2018619550 [101].

Достоинства. В данной модели произведена декомпозиция общего показателя эффективности СФЗ на частные показатели, которые характеризуют эффективность функционирования подсистем СФЗ: обнаружения, задержки, реагирования и нейтрализации, то есть вероятности обнаружения, вероятности своевременного прибытия и вероятности нейтрализации и удержания. Эти показатели очень важны для проектировщика на следующем этапе проектирования [102].

Недостатки. Надежность и достоверность результатов моделирования существенно зависит от точности и обоснованности входных данных, а именно от зависимости показателей эффективности СФЗ от затрат для достижения этого уровня эффективности.

4.4 Обоснование требований к эффективности подсистем физической защиты критически важных объектов

Предложена методика декомпозиции общего показателя эффективности системы на частные показатели эффективности подсистем. Декомпозиция осуществляется на основе решения задачи нелинейного программирования с учетом минимизации затрат на построение подсистем СФЗ.

Постановка задачи. Используя критерий эффективности всей СФЗ ($P_З$ – вероятность защиты), необходимо определить наилучший вариант выбора частных показателей P_0 и $P_{СВП}$, обеспечивающий заданный уровень эффективности СФЗ при минимальной стоимости затрат на обеспечение безопасности КВО, то есть решить задачу декомпозиции общего показателя на частные.

Формализация задачи. Используя критерий «эффективность/стоимость» целевую функцию, отражающую минимизацию затрат на СФЗ при обеспечении не-

обходимой эффективности, можно записать в виде

$$Po / B_1 + P_{СВП} / B_2 \to \max \ , \tag{4.22}$$

где B_1 – стоимость подсистемы обнаружения;

B_2 – стоимость подсистем задержки, реагирования и нейтрализации.

Ограничением выступает обеспечение подсистемами необходимой эффективности всей СФЗ:

$$P_0 \cdot P_{СВП} = P_З \ , \ 0 \le P_0 \le 1, .. 0 \le P_{СВП} \le 1. \tag{4.23}$$

После преобразований целевая функция (4.22) примет вид:

$$(B_1 \cdot P_{СВП} + B_2 \cdot P_0) / P_0 \cdot P_{СВП} \to \min . \tag{4.24}$$

Знаменатель (4.24) представляет собой величину заданной эффективности $P_З$. Отсюда, для минимизации дроби необходимо минимизировать числитель, имеющий линейную форму (достоинство преобразований). Тогда целевая функция (4.24) примет вид (особенность постановки задачи):

$$(B_1 \cdot Pсв + B_2 \cdot Po) \to \min \ ,$$

при ограничениях (4.23).

Геометрическая интерпретация задачи представлена на рисунке 4.6.

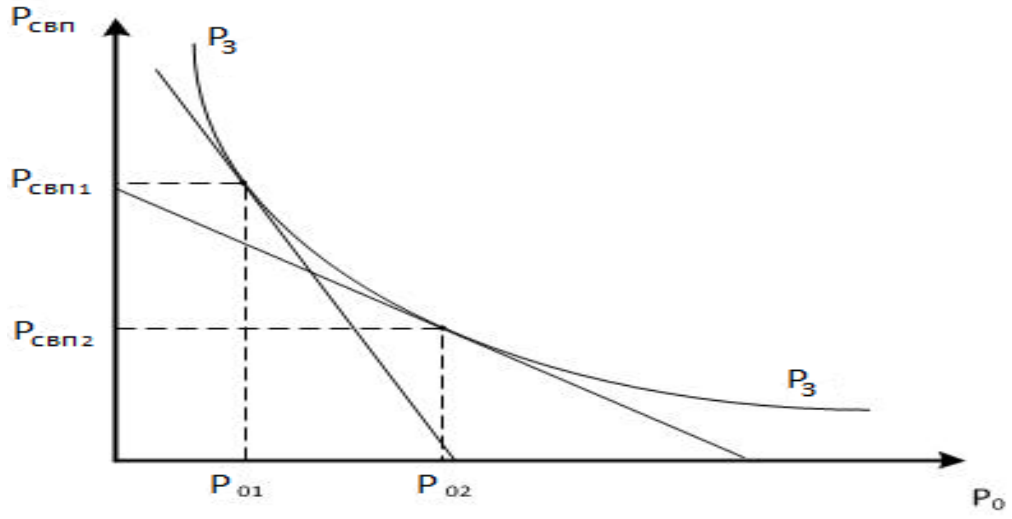


Рисунок 4.6 – Геометрическое представление постановки задачи

Таким образом, необходимо минимизировать стоимость затрат на СФЗ (ли-

нейная функция) при обеспечении необходимого значения *Рз,* как произведение частных показателей Po и $P_{СВП}$ (гипербола).

Методика решение задачи. Входными данными является величина эффективности СФЗ P_3, полученная в результате моделирования функционирования СФЗ или проведенных исследований главы 2.

Для определения требований к подсистемам СФЗ (декомпозиции общего показателя на частные) решена задача нелинейного программирования методом неопределенных множителей Лагранжа вида:

$$Z(x_1, x_2, ..., x_n, \lambda_1, \lambda_2, ..., \lambda_m) = f(x_1, x_2, ..., x_n) + \sum_{i=1}^{m} \lambda_i [b_i - q_i(x_1, x_2, ..., x_n)],$$

где $\lambda_1, \lambda_2, ..., \lambda_m$ – неопределенные множители Лагранжа;

$b_i - q_i(x_1, x_2, ..., x_n) = 0$ – ограничение в каноническом виде;

$f(x_1, x_2, ..., x_n)$ – целевая функция.

Для решения этой задачи использован пакет MathCad:

Целевая функция

$Z(b1, b2, P0, Pсв) := b2 \cdot P0 + b1 \cdot Pсв$

Функция Лагранжа

$L(b1, b2, C, P0, Pсв, \lambda1, \lambda2, \lambda3, u1, u2) := b2 \cdot P0 + b1 \cdot Pсв + \lambda1 \cdot (P0 \cdot Pсв - C) + \lambda2 \cdot (P0 + u1^2 - 1) + \lambda3 \cdot (Pсв + u2^2 - 1)$

Given

$\frac{d}{dP0} L(b1, b2, C, P0, Pсв, \lambda1, \lambda2, \lambda3, u1, u2) = 0$

$\frac{d}{dPсв} L(b1, b2, C, P0, Pсв, \lambda1, \lambda2, \lambda3, u1, u2) = 0$

$\frac{d}{d\lambda1} L(b1, b2, C, P0, Pсв, \lambda1, \lambda2, \lambda3, u1, u2) = 0$

$\frac{d}{d\lambda2} L(b1, b2, C, P0, Pсв, \lambda1, \lambda2, \lambda3, u1, u2) = 0$

$\frac{d}{d\lambda3} L(b1, b2, C, P0, Pсв, \lambda1, \lambda2, \lambda3, u1, u2) = 0$

$\frac{d}{d\lambda4} L(b1, b2, C, P0, Pсв, \lambda1, \lambda2, \lambda3, u1, u2) = 0$

$\frac{d}{du1} L(b1, b2, C, P0, Pсв, \lambda1, \lambda2, \lambda3, u1, u2) = 0$

$\frac{d}{du2} L(b1, b2, C, P0, Pсв, \lambda1, \lambda2, \lambda3, u1, u2) = 0$

$REZ(b1, b2, C) := Find(P0, Pсв, \lambda1, \lambda2, \lambda3, u1, u2)$

$$REZ(b1, b2, C)^{\langle 0 \rangle^T} \text{ simplify } \rightarrow \left(\frac{b1 \cdot \sqrt{\frac{C \cdot b2}{b1}}}{b2} \quad \sqrt{\frac{C \cdot b2}{b1}} \quad -\frac{b1 \cdot \sqrt{\frac{C \cdot b2}{b1}}}{C} \quad 0 \quad 0 \quad \sqrt{1 - \frac{b1 \cdot \sqrt{\frac{C \cdot b2}{b1}}}{b2}} \quad \sqrt{1 - \sqrt{\frac{C}{b1} \cdot b2}} \right)$$

Если задать расходы B_1, B_2 и требуемую величину *Рэ,* можно получить тре-

бования к подсистемам СФЗ *Ро* и $P_{СВП}$.

Функция Лагранжа

$L(b1, b2, P0, Pсв) := b2 \cdot P0 + b1 \cdot Pсв$

Given

$P0 \cdot Pсв = 0.81$

$P0 \le 1 \quad Pсв \le 1$

$REZ(b1, b2) := Minimize(L, P0, Pсв)$

$$REZ(5.5, 4.5) = \begin{pmatrix} 0.987 \\ 0.821 \end{pmatrix} \qquad REZ(4, 6) = \begin{pmatrix} 0.81 \\ 1 \end{pmatrix} \qquad REZ(6.5, 3.5) = \begin{pmatrix} 1 \\ 0.81 \end{pmatrix}$$

При проектировании СФЗ для типового объекта задана величина эффективности СФЗ: $P_З = 0{,}81$. Расчеты для *Ро* и $P_{СВП}$ при одинаковых затратах составляют 0,9, что подтверждает правильность вычислений.

Данные показатели важны для проектирования на следующих этапах разработки СФЗ при формировании инженерно-технических средств обнаружения и задержки нарушителя.

При изменении величины затрат B_1 и B_2 более 10 % от среднего значения, частные показатели принимают допустимо предельные значения, что говорит об узком диапазоне возможного изменения частных показателей.

Таким образом, предложена методика обоснования требований к эффективности подсистем СФЗ – средств обнаружения, задержки, реагирования и нейтрализации. Декомпозиция общего показателя эффективности СФЗ на показатели эффективности ее подсистем решена на основе решения задачи нелинейного программирования путем использования целевой функции в линейной форме и ограничений, заданных нелинейной функции эффективности СФЗ [103].

4.6 Выводы

1. При проектировании СФЗ в качестве показателя безопасного состояния КВО принят показатель – вероятность успешного функционирования системы по формуле (1.4).

2. При проектировании СФЗ для данного объекта необходимо задать следующие величины параметров СФЗ:

- вероятность обнаружения угрозы = 0,9;

- коэффициент задержки угрозы *Kz* = 0,6;

- коэффициент расположения сил реагирования и нейтрализации *Кс* = 0,05.

3. Данные величины коэффициентов *Kz* и *Кс* обеспечивают вероятность своевременного прибытия сил реагирования $P_{СВП}$=0,8.

4. Предложена методика декомпозиции комплексного показателя эффективности на частные на основе формализованной задачи нелинейного программирования.

ГЛАВА 5 ОПТИМИЗАЦИЯ РАЗМЕЩЕНИЯ ИНЖЕНЕРНО-ТЕХНИЧЕСКИХ СРЕДСТВ ОХРАНЫ СИСТЕМ ФИЗИЧЕСКОЙ ЗАЩИТЫ

5.1 Методика формирования оптимального размещения и выбора инженерно-технических средств охраны объекта

Важным этапом проектирования СФЗ является синтез оптимального варианта размещения ИТСО на объекте. При проектировании СФЗ используется классический принцип формирования последовательных зон и рубежей безопасности. Цель настоящего раздела – разработка методики формирования оптимального варианта размещения технических средств защиты на объекте.

Для решения этой задачи необходимо разработать методику формирования логических функций проникновения нарушителя, на основе которых осуществляется оптимизация размещения ИТСО. Данный подход рассматривался при оценке эффективности с использованием логико-вероятностного метода (ЛВМ) в статьях [37, 45], делался акцент на большую трудоемкость ЛВМ. Материал данного раздела является продолжением исследований формирования функций алгебры логики на основе системного анализа, методических вопросов оптимизации размещения ИТСО при проектировании СФЗ. Особенностью решения задачи является то, что необходимо обеспечить безопасность контролируемой зоны $R_{КЗ}$ для объектов КИИ для исключения утечки информации по техническим каналам, то есть вводится дополнительный показатель эффективности СФЗ.

Разработанная методика позволит получить всю совокупность маршрутов проникновения нарушителя на объект, которые представлены как логические функции проникновения в виде дизъюнкции и конъюнкции логических переменных в матрице инцидентности, для решения задачи оптимального размещения ИТСО СФЗ.

В качестве показателя эффективности СФЗ определим вероятность нахождения объекта охраны в безопасном состоянии $P_О \geq P_{О.зад}$, $P_{СВП} \geq P_{СВП.зад}$, $R_{КЗ} \geq R_{КЗ.зад}$, $C_{зат.СФЗ}(P_З) \to \min$.. То есть необходимо добиться заданной вероятности обна-

ружения нарушителя, вероятности своевременного прибытия сил реагирования в точку пресечения и обеспечить безопасность контролируемой зоны при минимальной стоимости затрат на ИТСО СФЗ.

Решение задачи рассмотрим на модельном примере. Охраняемый объект представляет собой сложную систему, состоящую из множества связанных зон (элементов) различной природы и назначения (рисунок 5.1). Вся территория объекта имеет двойное ограждение, периметровую охрану и контрольно-пропускной пункт (КПП). Каждая зона объекта характеризуется множеством параметров и имеет разный уровень важности (ценности). На объекте имеется ключевая система информационной инфраструктуры, подлежащая охране.

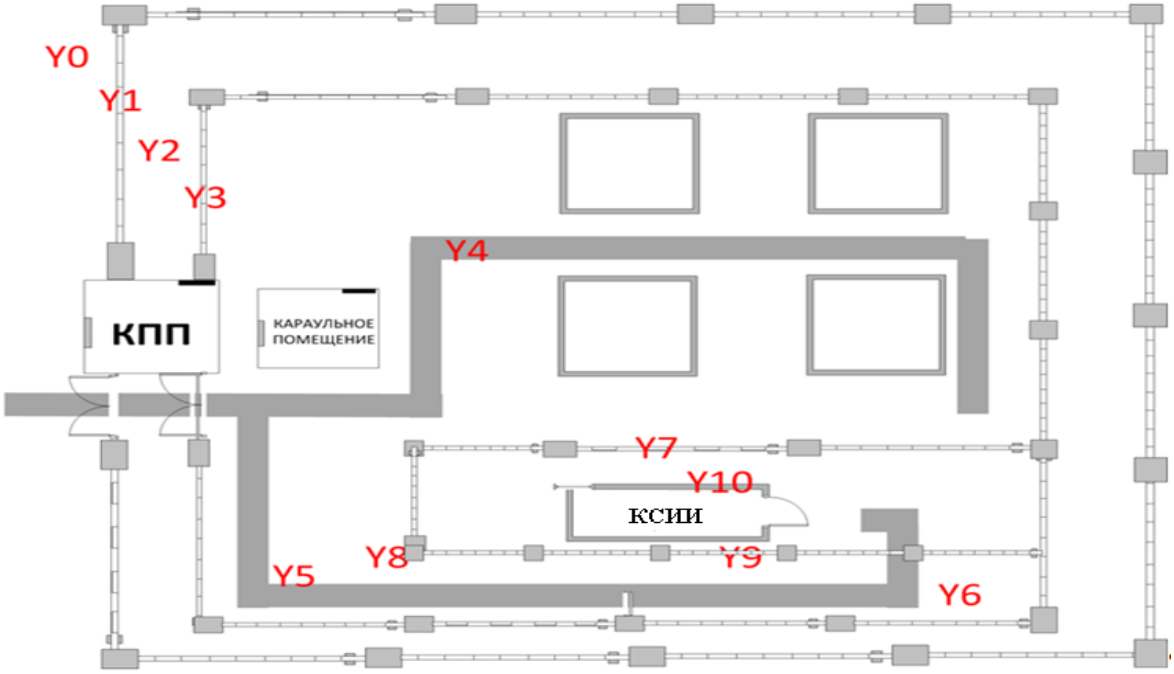


Рисунок 5.1 – План объекта охраны

Модель развития опасности – проникновения нарушителя – представлена в виде разветвленного ориентированного мультиграфа (рисунок 5.2). Вершины мультиграфа обозначены как рубежи достижения нарушителем определенного результата на пути к КСИИ. Ребра мультиграфа – это варианты перемещений (связей) нарушителя между рубежами, представленные как логические переменные функций. Ребра будем обозначать Xi, где i – номер ребра в графе (варианта перемещения). Полученный граф будем называть моделью достижимости нарушите-

лем своей цели. Всего будем определять n рубежей. Следовательно, граф будет иметь n вершин (событий). Инициирующему событию Yo присваивается значение 1. Наступление конечного события Yn означает факт проникновения нарушителя на объект, то есть нарушитель достиг своей цели (проведение диверсии и т. д.). Для данного графа вероятность нахождения Yn события в безопасном состоянии и будет показателем эффективности СФЗ.

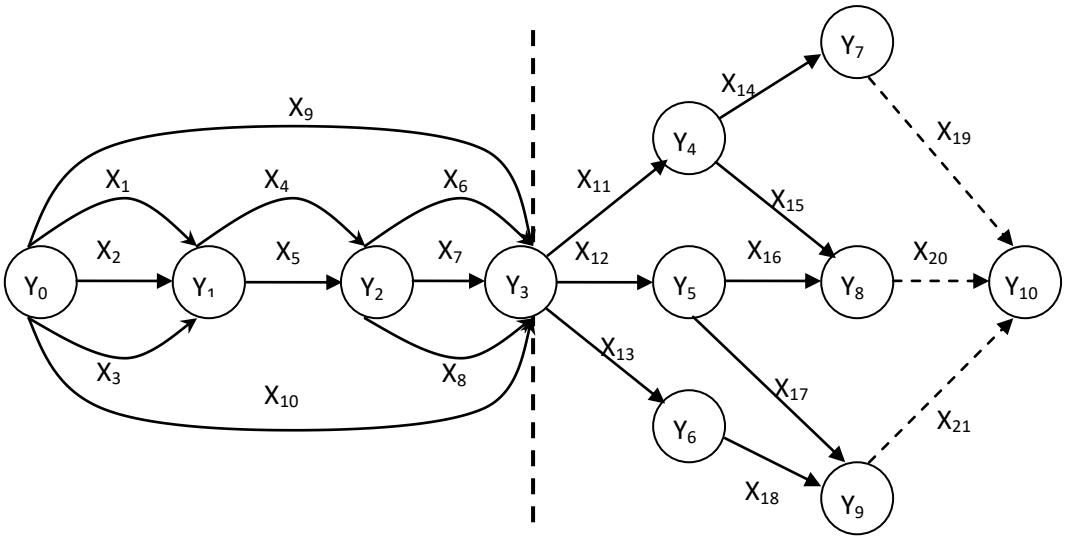


Рисунок 5.2 – Граф достижимости нарушителя своей цели

На рисунке 5.2 обозначено:

X_1 – преодоление ограждения через верх;

X_2 – преодоление через ограждение путем разрушения ограждения;

X_3 – подкоп ограждения для преодоления;

X_4 – вариант перемещения зоны бегом;

X_5 – преодоление зоны ползком (пластунским);

X_6 – преодоление второго ограждения через верх ограждения;

X_7 – разрушение второго ограждения;

X_8 – подкоп второго ограждения;

X_9 – проход через КПП путем подбора ПИН-кода;

X_{10} – проникновение через ворота путем подмены документов;

$X_{11} – X_{21}$ – вариант перемещения через зоны между рубежами внутри объекта.

Необходимо определить все пути перемещений из начальной вершины Y_0 в конечную вершину Y_{10}. Все варианты пути из одной смежной вершины в другую будем обозначать как дизъюнкцию логических переменных, которыми являются веса каждого ребра, принятые за единицу в данной задаче. Например, перемещение из вершины Y_0 в вершину Y_1 будем обозначать $X_1 v X_2 v X_3$.

Пути из одной вершины в другую определялись с помощью операции композиции матрицы смежности мультиграфа (рисунок 5.3). Для того чтобы найти пути, состоящие из k ребер, необходимо возвести матрицу смежности в степень k. При этом получим новую матрицу, в которой будут представлены все пути между событиями длинной от одного ребра до k ребер, откуда будут выбраны пути, состоящие из k ребер.

Таким образом, в полученной логической функции параллельные маршруты будут представлены как дизъюнкции, а последовательные – как конъюнкции. Также следует учесть, что умножаемые матрицы содержат логические переменные. Из этого следует, что к результатам умножения ячеек можно применить операции алгебры логики для сокращения результата умножения [46]. Применялись следующие операции:

1 правила для одной переменной – A v 1 = 1; Av 0 = A;

2 закон тавтологии – A v A v…A=A; - A $\wedge$ A $\wedge$ …A=A;

3 распределительный закон – A $\wedge$ (B v C) = (A $\wedge$ B) v (A $\wedge$ C).

Используя данные теоретические предпосылки, реализовано программное средство, позволяющее находить все пути заданной длинны из первого рубежа в последний, представленные как функции алгебры логики (ФАЛ) в виде конъюнкции весов ребер, по которым проходит путь проникновения [46].

Входные данные в программе представлены в виде матрицы смежности (рисунок 5.3). Для визуальной восприимчивости операцию конъюнкции двух переменных $X_1 \wedge X_2$ будем обозначать X_1X_2, а операцию дизъюнкции двух переменных X_1 v X_2 будем обозначать X_1+X_2.

	1	2	3	4	5	6	7	8	9	10	11
1	1	X1+X2+X3	0	X9+X10	0	0	0	0	0	0	0
2	0	1	X4+X5	0	0	0	0	0	0	0	0
3	0	0	1	X6+X7+X8	0	0	0	0	0	0	0
4	0	0	0	1	X11	X12	X13	0	0	0	0
5	0	0	0	0	1	0	0	X14	X15	0	0
6	0	0	0	0	0	1	0	0	X16	X17	0
7	0	0	0	0	0	0	1	0	0	X18	0
8	0	0	0	0	0	0	0	1	0	0	X19
9	0	0	0	0	0	0	0	0	1	0	X20
10	0	0	0	0	0	0	0	0	0	1	X21
11	0	0	0	0	0	0	0	0	0	0	1

Рисунок 5.3 – Матрица смежности графа

Будем увеличивать степень, в которую необходимо возвести данную матрицу, пока не получим все пути из начального события Y_0 в конечное Y_{10}. Всего получили сто логических функций проникновения нарушителя (таблица 5.1), из которых десять – длинной в четыре элемента, а девяносто – длинной в шесть элементов. Полученные логические функции сведены в матрицу инцидентности.

Таблица 5.1 – Матрица инцидентности

Функции угроз	Ребра графа																				
	X_1	X_2	X_3	X_4	X_5	X_6	X_7	X_8	X_9	X_{10}	X_{11}	X_{12}	X_{13}	X_{14}	X_{15}	X_{16}	X_{17}	X_{18}	X_{19}	X_{20}	X_{21}
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
1									1		1			1					1		
2									1		1				1					1	
3									1			1				1				1	
4									1			1					1				1
5									1				1					1			1
6										1	1			1					1		
7										1	1				1					1	
8										1		1				1				1	
9										1		1					1				1
10										1			1					1			1
11	1			1		1					1			1					1		
12	1			1		1					1				1					1	
13	1			1		1						1				1				1	
14	1			1		1						1					1				1
15	1			1		1							1					1			1
16	1			1			1				1			1					1		
17	1			1			1				1				1					1	
18	1			1			1					1				1				1	
19	1			1			1					1					1				1
20	1			1			1						1					1			1
21	1			1				1			1			1					1		
22	1			1				1			1				1					1	
23	1			1				1				1				1				1	
24	1			1				1				1					1				1
25	1			1				1					1					1			1
26	1				1	1					1			1					1		
27	1				1	1					1				1					1	
28	1				1	1						1				1				1	
29	1				1	1						1					1				1
30	1				1	1							1					1			1
31	1				1		1				1			1					1		
32	1				1		1				1				1					1	
33	1				1		1					1				1				1	

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
34	1				1		1					1					1				1
35	1				1		1						1					1			1
36	1				1			1			1			1					1		
37	1				1			1			1				1					1	
38	1				1			1				1				1				1	
39	1				1			1				1					1				1
40	1				1			1					1					1			1
41		1		1		1					1			1					1		
42		1		1		1					1				1					1	
43		1		1		1						1				1				1	
44		1		1		1						1					1				1
45		1		1		1							1					1			1
46		1		1			1				1			1					1		
47		1		1			1				1				1					1	
48		1		1			1					1				1				1	
49		1		1			1					1					1				1
50		1		1			1						1					1			1
51		1		1				1			1			1					1		
52		1		1				1			1				1					1	
53		1		1				1				1				1				1	
54		1		1				1				1					1				1
55		1		1				1					1					1			1
56		1			1	1					1			1					1		
57		1			1	1					1				1					1	
58		1			1	1						1				1				1	
59		1			1	1						1					1				1
60		1			1	1							1					1			1
61		1			1		1				1			1					1		
62		1			1		1				1				1					1	
63		1			1		1					1				1				1	
64		1			1		1					1					1				1
65		1			1		1						1					1			1
66		1			1			1			1			1					1		
67		1			1			1			1				1					1	
68		1			1			1				1				1				1	
69		1			1			1				1					1				1
70		1			1			1					1					1			1
71			1	1		1					1			1					1		
72			1	1		1					1				1					1	
73			1	1		1						1				1				1	
74			1	1		1						1					1				1
75			1	1		1							1					1			1
76			1	1			1				1			1					1		
77			1	1			1				1				1					1	
78			1	1			1					1				1				1	
79			1	1			1					1					1				1
80			1	1			1						1					1			1
81			1	1				1			1			1					1		
82			1	1				1			1				1					1	
83			1	1				1				1				1				1	
84			1	1				1				1					1				1
85			1	1				1					1					1			1
86			1		1	1					1			1					1		
87			1		1	1					1				1					1	
88			1		1	1						1				1				1	
89			1		1	1						1					1				1
90			1		1	1							1					1			1
91			1		1		1				1			1					1		
92			1		1		1				1				1					1	
93			1		1		1					1				1				1	
94			1		1		1					1					1				1
95			1		1		1						1					1			1
96			1		1			1			1			1					1		
97			1		1			1			1				1					1	
98			1		1			1				1				1				1	
99			1		1			1				1					1				1
100			1		1			1					1					1			1

Примечание: Элементы матрицы инцидентности булевы переменные: 1 – если путь проходит через *j*-ое ребро графа; 0 – в противном случае.

Строки в матрице – маршруты проникновения (функции), а столбцы – элементы объекта (ребра графа), на которых будет формироваться размещение ИТСО СФЗ. Элементы матрицы в строке связаны конъюнктивно, в столбцах – дизъюнктивно.

С точки зрения системного анализа процесс получение всех маршрутов проникновения (функций опасности) является задачей декомпозиции сложной задачи на более простые подзадачи. После этой задачи согласно теории системного анализа решается задача синтеза или оптимизации технических элементов СФЗ.

Следующий этап: синтез размещения технических средств защиты на основе задачи о покрытии на матрице вариантов проникновения нарушителя.

Количество функций определяет количество возможных вариантов проникновения нарушителя на объект. Причем каждая функция проникновения (угроза) предотвращается путем прерывания маршрута хотя бы в одном ребре графа. Необходимо исключить все сто маршрутов (функций) проникновения. Это задача о нахождении минимального сечения на графе, которая решается путем определения минимального покрытия на матрице инцидентности (таблица 5.1).

Задача о покрытии решалась методом ветвей и границ. Цель решения: минимальным количеством ребер покрыть все возможные маршруты проникновения на объект. Результат покрытия – это минимальный набор ребер (препятствий) для исключения проникновения на объект, то есть реализации угрозы.

Ребро в графе может ассоциироваться с каким-то типом варианта защиты объекта, который будет характеризоваться вероятностью защиты и стоимостью. Так как задача о покрытии решается на максимум эффективности, то в качестве показателя выберем количество перекрываемых маршрутов с минимальной (нулевой) избыточностью. Тогда результатом будет множество покрытий, каждое из которых перекрывает все маршруты проникновения.

Постановка задачи о покрытии – все пути проникновения покрыть минимальным количеством ребер [104, 105]:

$$\sum_{j=1}^{n} X_j \to \min, \tag{5.1}$$

где $x_j = \begin{cases} 1 - \text{если j-е ребро графа входит в состав покрытия;} \\ 0 - \text{в противном случае.} \end{cases}$

При этом избыточность нереализованных возможностей покрывающих ребер графа стремится к минимуму:

$$\sum_{j=1}^{n} a_{ij} x_j \to \min,\ i = \overline{1,m}. \tag{5.2}$$

При ограничении: каждое ребро покрывает хотя бы один путь проникновения:

$$\sum a_{ij} x_j \geq 1. \tag{5.3}$$

Исходные данные задаются с помощью матрицы инцидентности:

$$A = \left\| a_{ij} \right\|, \tag{5.4}$$

где i =1 - m – номер пути проникновения;

j = 1 - n – номер ребра графа;

$a_{ij} = \begin{cases} 1, \text{ если } j \text{ ребро входит в } i \text{ путь проникновения;} \\ 0, \text{ в противном случае.} \end{cases}$

Данная задача решается методом ветвей и границ. Для ее решения указать два момента: во-первых, необходимо определить способ ветвления дерева решений; во-вторых, определить способ вычисления границ решения задачи. Для оценки границ решения необходимо определить мощность каждого ребра:

$$W(j) = E'(j) - S(j), \tag{5.5}$$

где $E'(j) -$ потенциал j-го ребра:

$$E'(j) = \sum_{\forall i \in I} a_{ij},\ j \in J, i \in I, \tag{5.6}$$

где I – множество маршрутов, которые не покрыты ребрами.

$$S(j) = \sum_{\forall i \in I'} a_{ij}, j = (J / J_1), \tag{5.7}$$

где I' – множество маршрутов, которые покрыты ребрами;

$S(j)$ – избыточность или неиспользованные возможности *j*-го ребра.

Задача модернизирована. Чтобы задача о покрытии быстро сходилась к конечному результату, введена оценка перспективной мощности *j*-го ребра:

$$\widetilde{W}(j) = W(i) - S(j), \tag{5.8}$$

где $W(i)$ – мощность *i*-го ребра, из которого производится ветвление;

$S(j)$ – избыточность ребра, претендующего на включение в покрытие;

$\widetilde{W}(j)$ – перспективная мощность *j*-го ребра.

Процесс решения задачи о покрытии автоматизирован с помощью программного средства на языке C#, свидетельство о государственной регистрации № 2018619865 [107].

В результате решения задачи о покрытии для каждого ребра графа (столбца матрицы) получили 22 покрытия (сечения), (таблица 5.2).

Таблица 5.2 – Таблица покрытий

Номер покрытия	Ребра покрытия
1	X_1, X_2, X_3, X_9, X_{10}
2	X_4, X_5, X_9, X_{10}
3	X_6, X_7, X_8, X_9, X_{10}
4	X_{11}, X_{12}, X_{13}
5	X_{12}, X_{13}, X_{14}, X_{15}
6	X_{12}, X_{13}, X_{15}, X_{19}
7	X_{11}, X_{16}, X_{21}
8	X_{11}, X_{16}, X_{17}, X_{18}
9	X_{12}, X_{14}, X_{15}, X_{18}
10	X_{11}, X_{16}, X_{17}, X_{13}
11	X_{14}, X_{15}, X_{16}, X_{21}
12	X_{14}, X_{15}, X_{16}, X_{17}, X_{13}
13	X_{13}, X_{17}, X_{19}, X_{20}
14	X_{12}, X_{15}, X_{18}, X_{19}
15	X_{14}, X_{20}, X_{21}
16	X_{14}, X_{20}, X_{17}, X_{18}
17	X_{19}, X_{20}, X_{21}
18	X_{15}, X_{16}, X_{19}, X_{21}
19	X_{17}, X_{18}, X_{19}, X_{20}
20	X_{13}, X_{14}, X_{17}, X_{20}
21	X_{11}, X_{12}, X_{18}
22	X_{14}, X_{15}, X_{16}, X_{17}, X_{18}

Каждое покрытие позволяет контролировать все маршруты проникновения нарушителя в КСИИ. Таким образом, на этих элементах (ребрах покрытий) и предполагается проектировать варианты построения элементов СФЗ.

Проведем оптимизацию размещения технических средств защиты СФЗ по критерию стоимости.

После формирования таблицы покрытий для обеспечения защиты объекта необходимо сформировать систему рубежей, удовлетворяющих заданным требованиям и ограничениям, на которых будут располагаться элементы СФЗ.

Возможны две постановки задачи оптимизации СФЗ:

– минимизировать стоимость затрат на реализацию СФЗ при заданной вероятности противодействия типовому нарушителю (эффективности СФЗ);

– максимизировать вероятность защиты объекта от воздействия угрозы (эффективность СФЗ) при заданной величине стоимости, затрачиваемой на обеспечение СФЗ.

Учитывая то, что вероятности обнаружения и вероятность перехвата (своевременного прибытия для нейтрализации) нарушителя обоснованы и заданы на предыдущих этапах проектирования СФЗ (рисунок 5.1), будем решать первую задачу.

Критерии эффективности СФЗ определены в четвертом разделе диссертации:

– вероятность обнаружения нарушителя на каждом маршруте проникновения не менее – 0,9;

– вероятность своевременного прибытия в точку пресечения сил реагирования на каждом маршруте не менее – 0,8.

Кроме того, на объекте имеются контролируемые зоны. В этих зонах для обеспечения безопасности объекта и исключения утечки конфиденциальной информации не допускается несанкционированное нахождение посторонних лиц. Контроль этих зон обеспечивается ИТСО СФЗ. Размеры контролируемых зон, в зависимости от типа средств разведки, определяются руководящими документа-

ми, то есть размер контролируемой зоны $R_{КЗ}$ – выбирался в соответствии с требованиями заказчика.

В этой постановке необходимо на полученном множестве вариантов покрытий оценить стоимость и эффективность комбинаций покрытий. Логично считать, что стоимость покрытия прямо пропорционально зависит от протяженности покрытия, то есть стоимость $C=K*L$, где L – протяженность покрытия; K – коэффициент пересчета. Кроме того, каждое покрытие еще характеризуется расположением на местности, то есть его удалением от охраняемого элемента объекта. Этот параметр вводится для оценки временной возможности противодействия и нейтрализации нарушителя силами реагирования и обеспечения безопасности контролируемой зоны $R_{КЗ}$. Для этого выделяется критическая зона и контролируемая зона – минимальное расстояние от элемента охраны, после которой при обнаружении нарушителя противодействие из-за недостатка времени невозможно. Все покрытия, которые попадают в эти зоны, исключаются из процесса оптимизации.

Из двадцати двух результирующих покрытий выбраны десять покрытий (1, 2, 3, 4, 5, 8, 9, 10, 12, 21). Двенадцать покрытий (6, 7, 12, 13, 14, 15, 16, 17, 18, 19, 20, 22) исключены из рассмотрения, так как они попадают в критическую или контролируемую зону.

Определив длину каждого покрытия, необходимо построить возрастающий ряд. В первую очередь в оптимальное множество сечений включаются покрытия с минимальной протяженностью и необходимым удалением от охраняемого элемента. Оптимизация заключается в получении минимальной длины покрытий (стоимости) при обеспечении заданной вероятности обнаружения проникновения нарушителя. Каждое дополнительное покрытие будет повышать вероятность обнаружения и вероятность распознать ситуацию поведения нарушителя (конкретный маршрут движения) для принятия решения его эффективной нейтрализации. Формирование множества покрытий заканчивается при достижении заданной вероятности обнаружения. Построение элементов обнаружения на данных покрытиях позволит получить СФЗ с заданной вероятностью обнаружения при минимальной стоимости.

Данная задача решается методом динамического программирования (ДП). Формализованная постановка задачи имеет вид – на основании принципа оптимальности Беллмана можно записать следующее [106]:

$$\Lambda_n(b_n) = \min_X (\max)\left[f_n(x_n) + \Lambda_{n-1}(b_{n-1}) \right], \tag{5.9}$$

где $$X = \left\{ \sum_{j=1}^{n} a_j x_j \le b_n;\ a_j;\ b_n \ge 0;\ x_j \ge 0 \right\}.$$

В свою очередь, $$\Lambda_n(b_n) = \min_{X_n} (\max)\left[f_n(x_n) + \Lambda_{n-2}(b_{n-2}) \right], \tag{5.10}$$

$$b_{n\text{-}1} = b_n - a_n x_n,$$

$$\Lambda_{n-1}(b_{n-1}) = \min_{x_{n-1}} (\max)\left[f_{n-1}(x_{n-1}) + \Lambda_{n-2}(b_{n-2}) \right], \tag{5.11}$$

$$b_{n\text{-}2} = b_{n\text{-}1} - a_{n\text{-}1} x_{n\text{-}1}.$$

Продолжая, получим

$$\Lambda_{n-2}(b_{n-2}) = \min_{x_{n-2}} (\max)\left[f_{n-2}(x_{n-2}) + \Lambda_{n-3}(b_{n-3}) \right], \tag{5.12}$$

$$b_{n\text{-}3} = b_{n\text{-}2} - a_{n\text{-}2} x_{n\text{-}2}. \tag{5.13}$$

На последнем шаге $\Lambda_1(b_1) = \min_{x_1} (\max)\left[f_1(x_1) \right]$, при $b_1 = b_2 - a_2 x_2$.

Эти соотношения называются функциональными уравнениями Беллмана. Обычно известно, да и то не всегда, только b_n, а b_1, …, $b_{n\text{-}1}$ заранее неизвестны, поэтому ДП является, по существу, организованным перебором с последовательным отсечением промежуточных результатов. При этом значения b_1, …, b_n берутся из всего возможного диапазона их изменений от 0 до b_n включительно. Для каждого значения b_j рассматриваются все значения переменных x_j и находят то x^*_j, которое доставляет экстремум $\Lambda_j(b_j)$. На последнем этапе определяется x^*_n, доставляющее экстремум $\Lambda_n(b_n)$. При этом сначала просматривается все от x_1 до x_n. Затем начинается движение в обратном направлении. Далее, на последнем этапе находится $b_1 = b_2 - a_2 x^*_2$, по которому определяется x^*_1.

Иллюстрация решения представлена на рисунке 5.4.

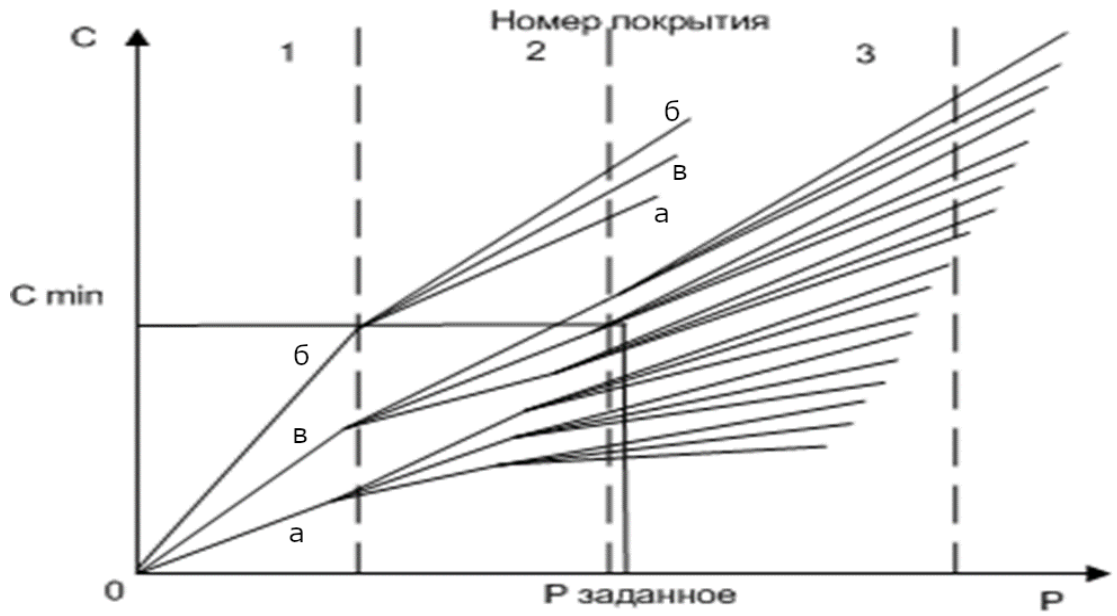


Рисунок 5.4 – Схема решения задачи динамического программирования

На рисунке 5.4 обозначено: Р – вероятность обнаружения нарушителя; С – стоимость технических средств защиты СФЗ, размещенных на покрытии – №; а, б, в – варианты установки на покрытие средств обнаружения первого, второго, третьего типа соответственно.

Таким образом, при достижении заданной границы вероятности обнаружения нарушителя выбирается вариант покрытий для размещения технических элементов защиты с минимальной стоимостью.

После определения величины затрат (Cmin) на обеспечение защиты объекта необходимо определить рубежи (зоны) охраны объекта, на которых будут располагаться технические средства защиты, удовлетворяющие заданным ограничениям.

Длина каждого покрытия определялась как сумма протяженности ребер графа на местности:

X_1 – 2500 м; X_2 – 2500 м; X_3 – 2500 м; X_4 – 2400 м; X_5 – 2400 м; X_6 – 2300 м; X_7 – 2300 м; X_8 – 2400 м; X_9 – 5 м; X_{10} – 5 м;

X_{11} – вариант перемещения через зоны между рубежами Y_3-Y_4 – 450 м;

X_{12} – вариант перемещения через зоны между рубежами Y_3-Y_5 – 320 м;

X_{13} – вариант перемещения через зоны между рубежами Y_3-Y_6 – 220 м;

X_{14} – вариант перемещения через зоны между рубежами Y_4-Y_7 – 180 м;

X_{15} – вариант перемещения через зоны между рубежами Y_4-Y_8 – 50 м;

X_{16} – вариант перемещения через зоны между рубежами Y_5-Y_8 – 160 м;

X_{17} – вариант перемещения через зоны между рубежами Y_5-Y_9 – 50 м;

X_{18} – вариант перемещения через зоны между рубежами Y_6-Y_9 – 120 м;

X_{19} – вариант перемещения через зоны между рубежами Y_7-Y_{10} – 60 м;

X_{20} – вариант перемещения через зоны между рубежами Y_8-Y_{10} – 70 м;

X_{21} – вариант перемещения через зоны между рубежами Y_9-Y_{10} – 50 м.

Запишем номера покрытий по возрастанию их протяженности: 12 – 660 м, 9 – 670 м, 5 – 770 м, 8 – 780 м, 10 – 880 м, 21 – 890 м, 4 – 9м90 , 3 – 2310 м, 2 – 2410 м, 1 – 2510 м. Все множество покрытий делится на две группы, которые находятся внутри объекта (12, 9, 5, 8, 10, 21, 4) и за пределами (3, 2, 1). Как правило, на внешние покрытия устанавливают датчики движения – это будет короткое покрытие номер 3. На внутренние покрытия устанавливают ИТСО (камеры наблюдения) [108, 109].

Для каждого покрытия определим удаление от КСИИ и по этой величине определим вероятность перехвата нарушителя. Удаление КСИИ от караульного помещения составляет 300 м. Удаление покрытий от КСИИ составляет: 12 – 280 м, 9 – 300 м, 8 – 320 м, 5 – 350 м, 10 – 450 м, 21 – 400 м, 4 – 460 м – удовлетворяют требованию обеспечения безопасности контролируемой зоны *Rкз*.

Для вычисления величины вероятности своевременного прибытия сил реагирования в точку перехвата $P_{СВП}$ используется модель [43, 111]:

$$P_{СВП} = \exp[1,7(t_d - t_f)/\sigma]/[1+\exp[1,7(t_d - t_f)/\sigma]. \qquad (5.14)$$

Принимаем ограничения, что скорость движения нарушителя по данному объекту составляет 3 м/с, а скорость движения сил реагирования 4,4 м/с, и их среднеквадратичные отклонения соизмеримы со скоростями движения сил реагирования и нейтрализации. Поэтому по расстояниям можно оценить время движения к цели и по формуле (5.14) определить вероятность своевременного прибытия сил реагирования и нейтрализации.

Покрытие 12 не удовлетворяет требованиям вероятности своевременного пресечения нарушителя, то есть значение вероятности меньше 0,8.

Для оставшихся покрытий 9, 5, 8, 10, 21, 4 проведем операцию дискретной разности множеств с целью исключения одинаковых ребер в покрытиях. Пятое покрытие объединяется с девятым в пользу пятого, восьмое покрытие объединяется с десятым в пользу восьмого по меньшей длине покрытий. Так как 21 и 4 покрытия пересекаются с 8 и 5 покрытием, то необходимо их исключить в соответствии с постановкой задачи.

Очевидно, что для обеспечения вероятности обнаружения 0,92 необходимо не более, чем двукратное дублирование камер. Получаем два варианта покрытий: пятое – протяженностью 770 м и восьмое –протяженностью 780 м или девятое – протяженностью 670 м и десятое –протяженностью 880 м с одинаковой общей длинной покрытий – протяженностью 1550 метров.

Поэтому будем решать два разных варианта задачи динамического программирования и выберем наилучший вариант установки технических средств наблюдения.

На основе метода иерархий определены наиболее приемлемые ИТСО, характеристики которых представлены в таблице 5.3.

Таблица 5.3 – Характеристики инженерно-технических средств охраны

Тип ИТСО	Относительная стоимость за штуку, руб.	Вероятность обнаружения	Угол обзора, град.	Дальность, м
1тип (CNB-WFL-21S)	4800	0,60	70 – 90	60
2 тип (SCANALL)	7000	0,80	70 – 90	70

Данная задача автоматизирована на языке программирования C#, свидетельство о государственной регистрации №2018661409 [112]. Вводится количество покрытий и их протяженности. Оконная форма, реализации алгоритма динамического программирования, представлена на рисунках 5.5, 5.6.

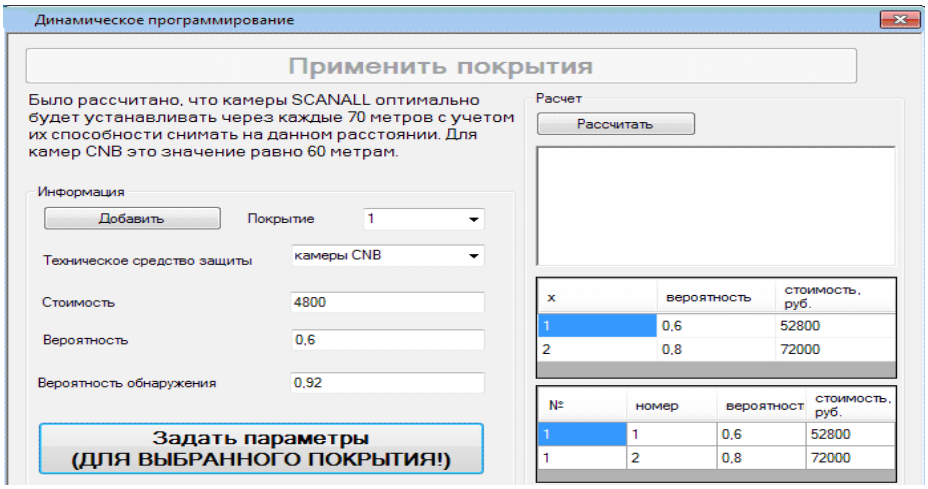


Рисунок 5.5 – Результаты ввода данных

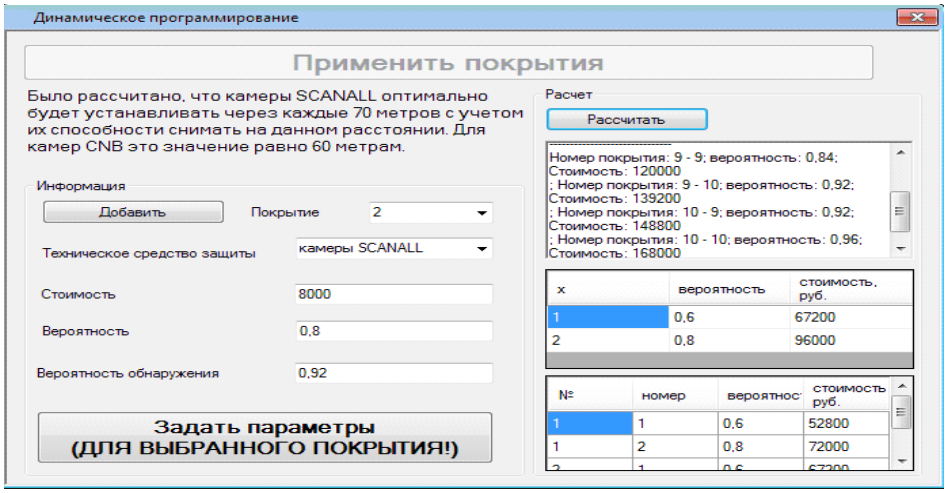
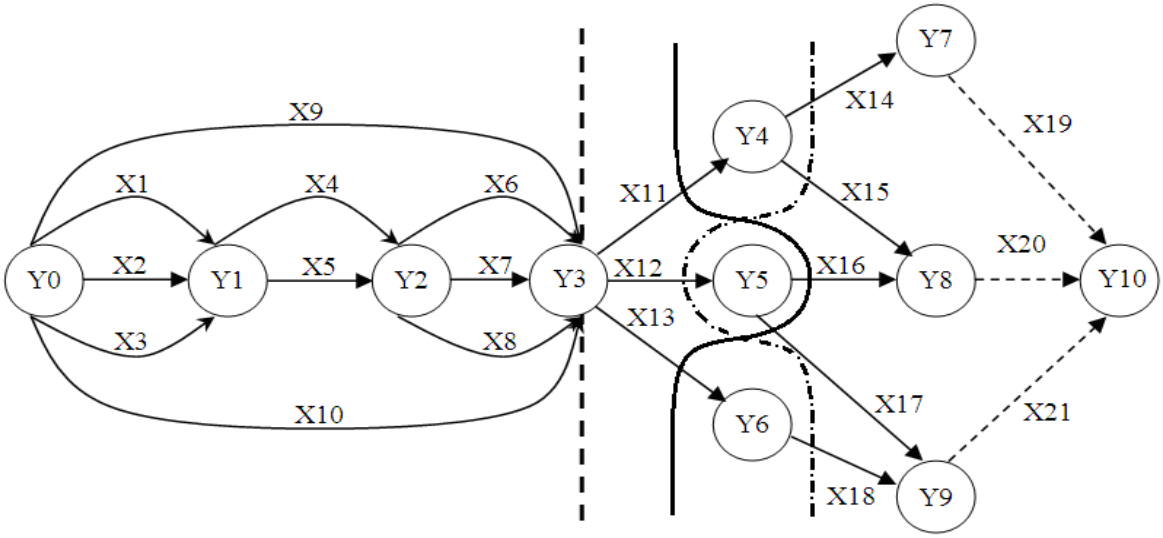


Рисунок 5.6 – Результаты выполнения модуля

Оптимальным по выбранному критерию является второй вариант: на девятое покрытие устанавливаются камеры с вероятностью обнаружения 0,8, на десятое – с вероятность обнаружения – 0,6. Таким образом, каждый маршрут проникновения имеет одинаковое значение вероятности обнаружения – 0,92 (не больше и не меньше, что очень важно) – это позволит выполнить важный принцип проектирования СФЗ – равнопрочности [111]. Любое другое расположение камер на покрытиях приводит к увеличению стоимости СФЗ. На рисунке 5.7 представлен граф с изображением девятого и десятого покрытий (маршрутов проникновения нарушителя), на которых необходимо разместить ИТСО объекта.



--- граница объекта; -.- 9 покрытие; - 10 покрытие.

Рисунок 5.7 – Покрытия пресечения маршрутов проникновения

На рисунке 5.8 показано расположение ИТСО на объекте, которое является оптимальным по выбранному критерию эффективности.

Таким образом, разработанный метод позволяет решать задачу декомпозиции сложной задачи на простые подзадачи – получение всех возможных маршрутов проникновения нарушителя в виде логических функций.

Результаты декомпозиции являются входными данными для решения следующей задачи системного анализа – синтеза размещения ИТСО СФЗ. Данная задача решалась путем задачи о покрытии на матрице логических функций. На полученных покрытиях решалась задача динамического программирования, выбирался оптимальный набор покрытий, на которых формировались ИТСО СФЗ (типовые датчики, камеры видеонаблюдения, точки контроля и т. д.) [113].

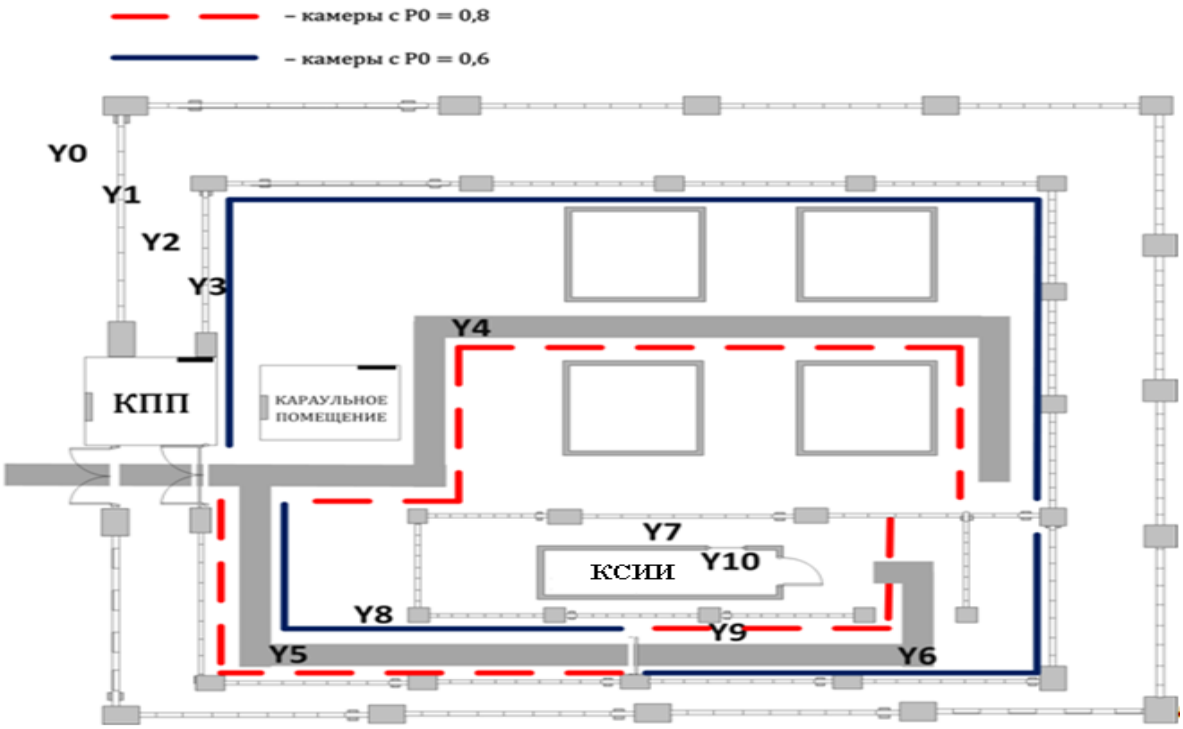


Рисунок 5.8 – Оптимальное расположение ИТСО

5.2 Синтез оптимального размещения инженерно-технических средств охраны для обеспечения безопасности разных по важности критических элементов объекта

Для решения задачи синтеза размещения ИТСО для разных по важности КЭ необходимо разработать метод оптимального размещения ИТСО на основе формирования логических функций проникновения нарушителя на объект, которые представлены как функции условий проникновения в виде конъюнкции логических переменных – аргументов. Аргументы функции – ребра графа проникновения, представленные как булевы переменные. Логические функции необходимо сформировать в матрицу инцидентности, на основе которой с помощью задач оптимизации о покрытии и динамического программирования произвести синтез оптимального размещения ИТСО, удовлетворяющий заданным требованиям эффективности СФЗ.

В качестве показателя эффективности СФЗ определим тот же самый показатель. Критерием эффективности СФЗ будем считать: $P_O \geq P_{O3}$ –

вероятность обнаружения нарушителя не менее заданной $P_{ОЗ}$; $P_{СВП} \geq P_{СВПЗ}$ – вероятность своевременного прибытия сил реагирования и нейтрализации в точку перехвата при условии обнаружения не менее заданной $P_{СВПЗ}$. При этом стоимость затрат на ИТСО стремится к минимуму: $C_{СТЗ} \to \min$. Считаем, что стоимость ИТСО прямо пропорционально зависит от протяженности их размещения, то есть стоимость определяется $C_{СТЗ} = K \cdot L,$ где $L-$ протяженность размещения ИТСО на рубежах зон охраны; $K-$ коэффициент пропорциональности.

Особенностью данной задачи является то, что из-за разной степени важности КЭ объекта, им задаются разные требования безопасности. Поэтому для КЭ с большей степенью важности необходимо формирование дополнительных покрытий для получения приращения показателя безопасности.

Решение поставленной задачи укладывается в последовательность этапов:

- на основе графовой модели проникновения нарушителя сформировать все пути проникновения нарушителя в виде логических функций, представленных матрицей инцидентности;

- сформировать множество вариантов размещения ИТСО с помощью задачи о покрытии на матрице инцидентности;

- провести синтез вариантов оптимального размещения ИТСО на основе задачи ДП;

- сформировать дополнительные варианты покрытий для повышения показателя безопасности более важных КЭ;

- провести синтез дополнительных вариантов размещения ИТСО, обеспечивающих повышение показателя безопасности более важных КЭ.

Решение задачи рассмотрим на типовом примере (рисунок 5.9). Охраняемый объект представляет собой сложную систему, состоящую из множества связанных зон разной важности и назначения [114].

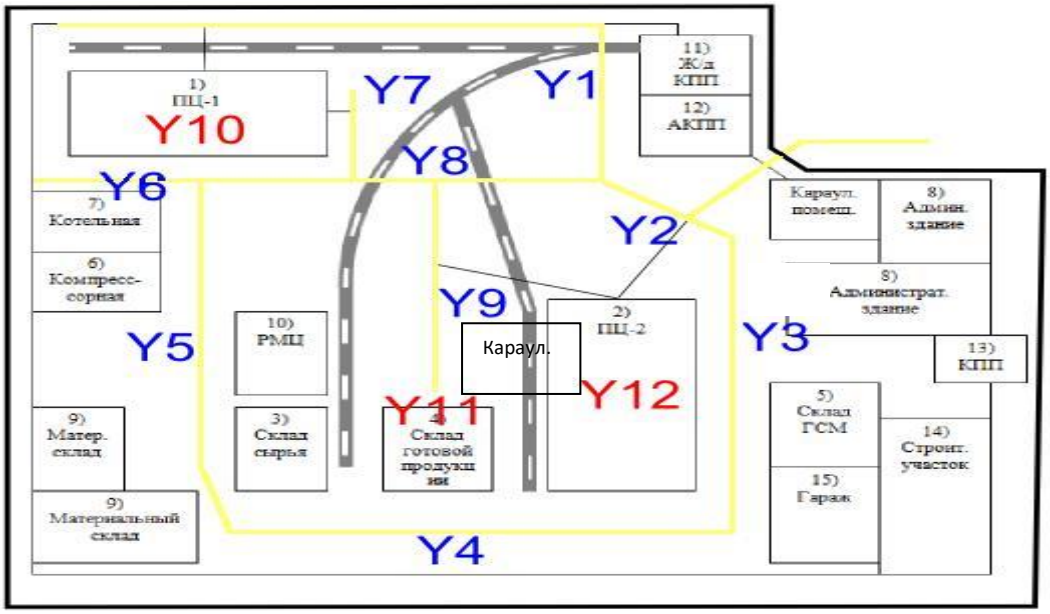


Рисунок 5.9 – План объекта

Вся территория объекта имеет ограждение, контрольно-пропускной пункт (КПП), автомобильный КПП (АКПП), железнодорожный КПП (ЖКПП). Объект имеет зоны и рубежи охраны. На объекте имеется три критических элемента, подлежащих охране: цех 1 (Y10), цех 2 (Y12), склад готовой продукции (Y11) и административное здание. Цель посягательства – проникнуть в цех 1, цех 2 или склад готовой продукции и произвести диверсионно-террористическое действие.

Первый этап. Представим сценарий проникновения нарушителя в виде разветвленного ориентированного графа (рисунок 5.10).

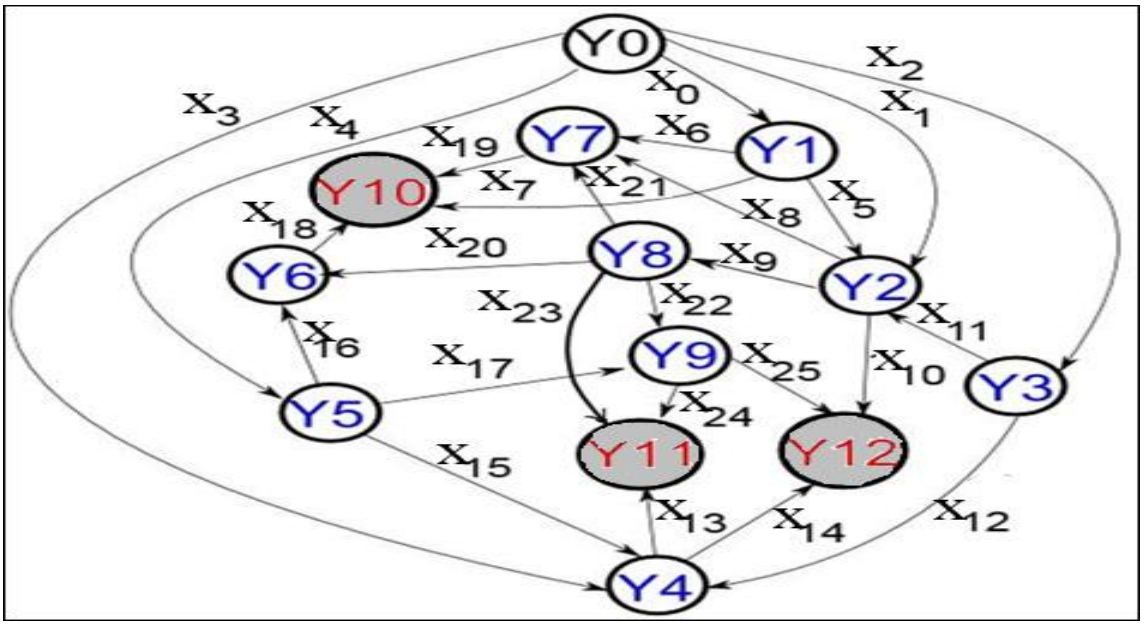


Рисунок 5.10 – Граф достижимости нарушителя своей цели

Вершины графа (Y_K) – рубежи, ребра – варианты возможных перемещений между рубежами, представленные как логические аргументы функций проникновения. Ребра обозначим X*j*, где *j* – номер ребра в графе, $X_0 – X_{25}$ – варианты перемещения через зоны между рубежами. Полученный граф назовем моделью достижимости нарушителем цели (модель развития опасности). Граф имеет k событий, начальное событие Y0 является инициирующим. Наступление хотя бы одного конечного события Y10, Y11,Y12 означает факт достижения нарушителем цели. Вероятность нахождения событий Y10, Y11, Y12 в безопасном состоянии и будет показателем эффективности СФЗ. Наступление промежуточных событий является условием логических комбинаций двух и более ребер графа на пути проникновения нарушителя.

Необходимо определить все пути проникновения из начальной вершины Y0 в конечные вершины графа Y10, Y11, Y12. Пути определяются с помощью операции композиции матрицы смежности графа. При этом получаем матрицу (таблица 5.4), в которой будут представлены все пути различного состава ребер из начального события – в конечные.

Каждый путь проникновения описывается логической функцией, аргументами которой является множество упорядоченных ребер графа. Аргументы функции – булевы переменные: 1 – если ребро входит в путь проникновения, 0 – не входит. Всего получаем тридцать две логических функции проникновения, сведенные в матрицу инцидентности (таблица 5.4).

Строки в матрице – пути проникновения (номера логических функций), а столбцы – упорядоченные ребра графа. Элементы матрицы в строке связаны конъюнктивно, а множество функций проникновения – дизъюнктивно (совершенная дизъюнктивная нормальная форма). Полученные логические функции позволяют оценить вероятность реализации цели нарушителем на каждом пути проникновения, то есть оценить эффективность СФЗ. В вероятностном смысле эффективность СФЗ будет определяться вероятностью нереализации ни одной функции проникновения.

Таблица 5.4 – Матрица инцидентности

N функции проникновения	Ребра графа																								
	X_0	X_1	X_2	X_3	X_4	X_5	X_6	X_7	X_8	X_9	X_{10}	X_{11}	X_{12}	X_{13}	X_{14}	X_{15}	X_{16}	X_{17}	X_{18}	X_{19}	X_{20}	X_{21}	X_{22}	X_{23}	X_{24}	X_{25}
1	1	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0
2	1	0	0	0	0	1	0	0	0	1	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0
3	1	0	0	0	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0
4	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0
5	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0
7	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0
8	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0
9	0	0	1	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0
10	0	0	1	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	1	0	1	0	0	0	0	0
11	0	0	1	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	1	0	1	0	0	0	0
12	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0
13	1	0	0	0	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0
14	1	0	0	0	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
15	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0
16	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
17	0	0	1	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	1	0	1	0
18	0	0	1	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0
19	0	0	1	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0
20	0	0	0	1	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0
21	0	0	0	0	1	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0
22	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0
23	1	0	0	0	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1
24	1	0	0	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
25	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1
26	0	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
27	0	0	1	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	1
28	0	0	1	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
29	0	0	1	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0
30	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
31	0	0	0	0	1	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0
32	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1

С точки зрения системного анализа процесс получения всех маршрутов проникновения (функций опасности) является задачей декомпозиции сложной задачи на более простые подзадачи. После этой задачи согласно теории системного анализа решается задача оптимизации размещения ИТСО СФЗ.

Второй этап. Количество функций проникновения определяет количество вариантов доступа нарушителя на объект. Необходимо исключить все пути проникновения. Это задача нахождения минимального сечения на графе. Она решается путем определения минимального покрытия на матрице инцидентности.

Постановка задачи о покрытии – все пути проникновения покрыть минимальным количеством ребер.

Решая задачу о покрытии для каждого ребра графа (столбца матрицы) получили десять покрытий, которые представлены в таблице 5.5. Причем, каждое покрытие позволяет контролировать все пути проникновения при размещении на них ИТСО. То есть покрытие может ассоциироваться с каким-то вариантом размещения ИТСО, который будет характеризоваться вероятностью обнаружения и стоимостью.

Таблица 5.5 – Таблица покрытий

N покрытия	Ребра покрытий	Длина покрытия, м	Номер протяжен.	Удаление от КЭ, м	Примечание
1	$X_3X_4\,X_6X_7X_8X_9X_{10}X_{12}$	1560	2	190	Близко к КЭ
2	$\mathbf{X_0X_1X_2X_3X_4}$	3000	10	460	Подходит
3	$X_1X_2X_3X_4X_5\,X_6X_7$	2690	9	190	Близко к КЭ
4	$\mathbf{X_0X_1X_3X_4}\,X_{11}X_{12}$	2500	6	400	Подходит
5	$X_3X_4\;\;X_7X_9X_{10}X_{12}X_{19}$	1410	1	240	Близко к КЭ
6	$X_3X_4\;X_7X_{10}X_{12}X_{19}X_{20}X_{22}X_{23}$	2540	7	240	Близко к КЭ
7	$\mathbf{X_6X_7X_8X_9X_{10}X_{13}X_{14}}X_{17}X_{18}$	2300	4	250	Подходит
8	$X_4\;X_6X_7X_8X_9X_{10}X_{13}X_{14}$	1860	3	190	Близко к КЭ
9	$\mathbf{X_6X_7X_8X_9X_{10}X_{13}X_{14}}X_{16}X_{17}$	2350	5	260	Подходит
10	$X_3X_6X_7X_8X_9X_{10}X_{12}X_{15}X_{16}X_{17}$	2680	8	240	Близко к КЭ

Третий этап. Возможны две постановки задачи оптимизации размещения ИТСО:

- минимизировать стоимость затрат на реализацию СФЗ при заданной вероятности противодействия нарушителям;

- максимизировать вероятность защиты объекта от воздействия нарушителей при заданной величине стоимости, затрачиваемой на обеспечение защиты.

Учитывая то, что вероятности обнаружения и вероятность перехвата (своевременного прибытия для нейтрализации) угрозы обоснованы и заданы на предыдущих этапах проектирования СФЗ и с учетом выбранного критерия эффективности СФЗ, решаем первую задачу.

По результатам четвертой главы диссертации зададим критерии эффективности к СФЗ:

- вероятность обнаружения нарушителя $P_O \geq 0,9$;

- вероятность своевременного прибытия сил реагирования для нейтрализации нарушителя $P_{СВП} \geq 0,8$.

В этой постановке необходимо на множестве комбинаций покрытий сформировать размещение ИТСО, обеспечивающее заданные критерии эффективности с минимальной стоимостью ИТСО, их монтаж и эксплуатацию. Стоимость ($C_{СТЗ}$) размещения ИТСО на покрытии пропорционально (K) зависит от его длины (L). Определив длину (стоимость) каждого покрытия необходимо сформировать возрастающий ряд. Обычно при проектировании формируют несколько рубежей обнаружения и задержки продвижения нарушителя. В первую очередь в оптимальное множество включаются покрытия с минимальной длиной и необходимым удалением от КЭ. Каждое дополнительное покрытие будет повышать вероятность обнаружения и вероятность распознать поведение нарушителя (конкретный путь движения) для принятия решения его нейтрализации. Формирование множества покрытий заканчивается при достижении заданной вероятности обнаружения. Кроме того, каждое покрытие еще характеризуется удалением от КЭ. Этот параметр вводится для оценки вероятности своевременного прибытия сил реагирования для нейтрализации нарушителя. Для этого выделяется критическая зона – минимальное расстояние от КЭ, после которой противодействие из-за недостатка времени невозможно. Покрытия, попавшие в эту зону, исключаются из процесса оптимизации. Оптимизация заключается в минимизации общей длины покрытий (стоимости) при обеспечении заданной вероятности обнаружения нарушителя и своевременного прибытия сил реагирования и нейтрализации.

Для обеспечения заданного критерия эффективности СФЗ рассмотрим покрытия минимальной протяженности и минимальным количеством общих ребер. Из десяти результирующих покрытий выбраны четыре покрытия (2, 4, 7, 9), причем второе и четвертое покрытия имеют общие ребра (пересекаются), седьмое и девятое покрытия также пересекаются. Остальные покрытия или попадают в критическую зону, или имеют большую длину, а значит стоимость размеще-

ния ИТСО. Таким образом, получили два множества непересекающихся покрытий, из которых выбираем наиболее короткие: четвертое и седьмое.

Четвертое покрытие короче второго покрытия на 500 м, но расположение второго покрытия дополнительно защищает административное здание и склад горюче-смазочных материалов (ГСМ). В этом случае выбор покрытия определяет вышестоящее руководство. На рисунке 5.11 данные покрытия показаны соответственно сплошной, пунктирной и штрихпунктирной линией.

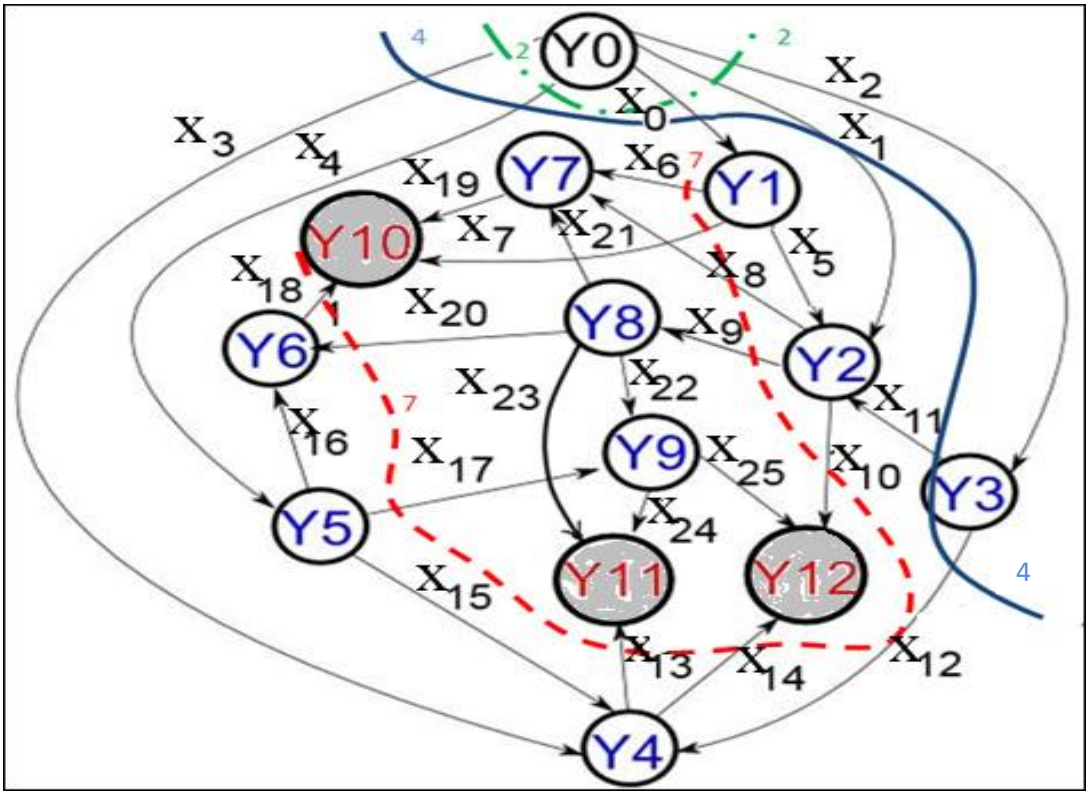


Рисунок 5.11 – Результирующие покрытия

Для каждого покрытия определили удаление от критических элементов объекта и по этой величине определим вероятность своевременного прибытия сил реагирования и нейтрализации. Удаление КЭ от караула составляет: Y10 – 240 м. Y11 – 200 м, Y12 – 90 м. Удаление покрытий от ближайших КЭ охраны составляет: седьмое – 250 м, четвертое – 400 м, второе – 460 м.

Для вычисления величины вероятности своевременного прибытия $P_{СВП}$ используется модель - формула (5.14) [43, с. 23].

При переходе от пространственных характеристик к временным параметрам перемещений для уровня оснащенности нашего объекта физическими барьерами считаем, что скорости движения составляют: сил реагирования – 4,4 м/с, нарушителя – 3 м/с, а их среднеквадратичные отклонения одинаковы [43, с. 22]. Покрытия 2, 4, и 7 удовлетворяют требованиям вероятности своевременного прибытия, т. к. $P_{СВП} \geq 0{,}8$.

Запишем покрытия в порядке увеличения длины: семь – 2300 м, четыре – 2500 м, два – 3000 м. Учитывая, что второе покрытие обеспечивает охрану склада ГСМ и административного здания, имеет смысл четвертое покрытие заменить вторым (ограждение объекта).

Для покрытий четыре и семь на основе решения задачи ДП определим наилучший вариант выбора типов ИТСО.

Для формирования исходных данных задачи из большого множества ИТСО на основе метода анализа иерархий определены наиболее приемлемые типы ИТСО, характеристики которых представлены в таблице 5.6.

Таблица 5.6 – Характеристики инженерно-технических средств охраны

Тип ИТСО	Относительная стоимость за штуку, руб.	Относительная стоимость покрытия 7 тыс. руб.	Относительная стоимость покрытия 2 тыс. руб.	Вероятность обнаружения, *Ро*	Угол обзора, град	Дальность, м
Первый тип (CNBWFL21S)	4800	184	240	0,60	70-90	60
Второй тип (SCANALL)	7000	203	266	0,80	70-90	80
Третий тип (IWPC22ZW)	6000	198	258	0,70	70-90	70

Проведем решение задачи синтеза элементов СФЗ с использованием аппарата динамического программирования. Для решения задачи ДП используется табличный алгоритм. Оконная форма результатов реализации алгоритма программы для вероятности обнаружения 0,9 представлена на рисунке 5.12.

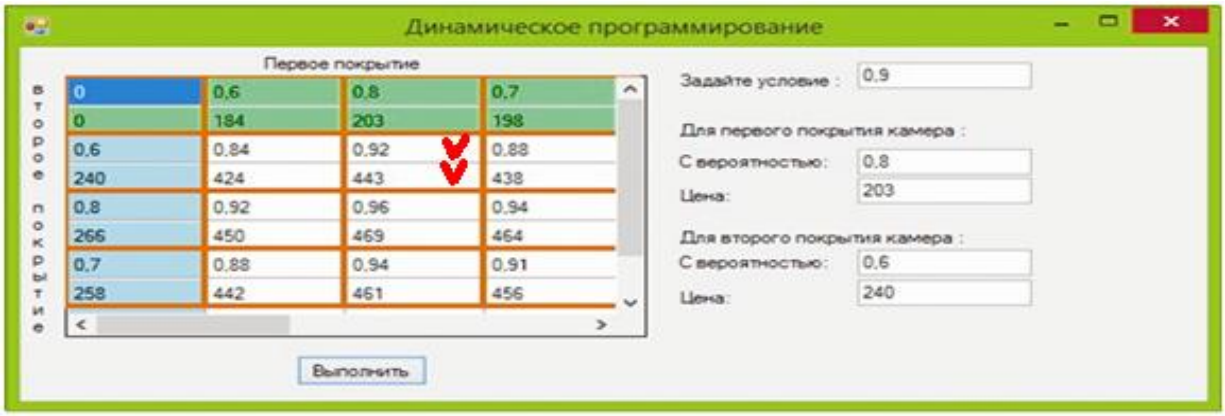


Рисунок 5.12 – Результаты выполнения модуля

Таким образом, на покрытии два располагать ИТСО первого типа с вероятностью обнаружения 0,6, а на покрытии семь – ИТСО второго типа с вероятностью обнаружения 0,8. Такое расположение ИТСО обеспечит P_o=0,92 нарушителя на каждом маршруте проникновения при минимуме стоимости – 443 тыс. руб. (рисунок 5.12).

Результат размещения ИТСО представлен на рисунке 5.13.

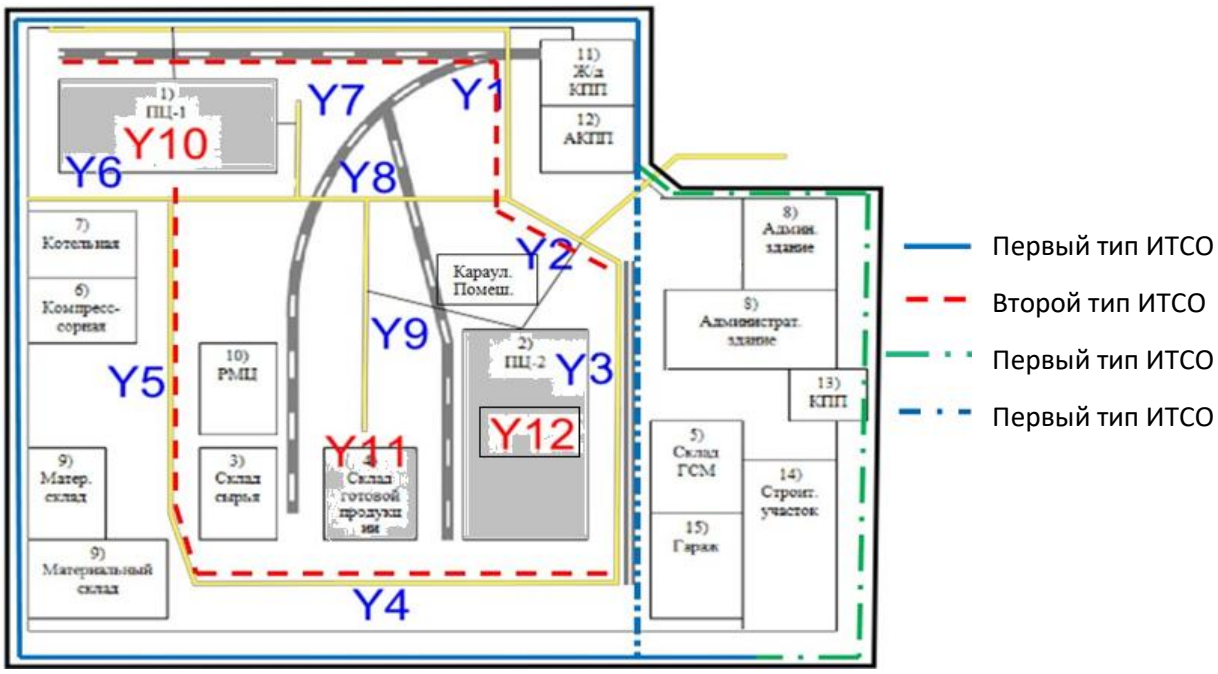


Рисунок 5.13 – План размещения камер наблюдения на объекте

Следующий этап решения задачи – обеспечение разного уровня безопасности критических элементов на основе задачи динамического программирования.

Для обеспечения повышения уровня безопасности КЭ объекта рассмотрим пересекающие покрытия с выделением путей проникновения нарушителя к КЭ повышенной опасности. Например, для цеха 1 (Y10) необходимо обеспечить вероятность обнаружения не 0,9, а $P_O \geq 0,95$. В этом случае на графе проникновения нарушителя (рисунок 5.11) с помощью алгоритма обхода графа в ширину определим маршруты (функции) проникновения только на Y10 [115, с. 659]. Результаты решения сведем в матрицу инцидентности.

Постановка задачи. Необходимо найти дополнительное покрытие, которое не пересекалось с ранее выделенными покрытиями, или выявить такие покрытия, которые пересекались незначительно по протяженности с назначенными покрытиями и имели возможность увеличения вероятности обнаружения. При этом полученные покрытия должны иметь минимальную протяженность (стоимость) и достаточное удаление от Y10 для своевременного реагирования сил реагирования на проникновение. Ребра, вошедшие в покрытия при решении предыдущей задачи, на которых уже размещены ИТСО, необходимо не исключать из рассмотрения. В результате решения получаем двенадцать функций проникновения, представленных в виде матрицы инцидентности (таблица 5.7).

Таблица 5.7 – Матрица инцидентности

Номер функции проникновения	Ребра графа																					
	X_0	X_1	X_2	X_3	X_4	X_5	X_6	X_7	X_8	X_9	X_{10}	X_{11}	X_{12}	X_{13}	X_{14}	X_{15}	X_{16}	X_{17}	X_{18}	X_{19}	X_{20}	X_{21}
1	1	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0
2	1	0	0	0	0	1	0	0	0	1	0	0	0	0	0	0	0	0	1	0	1	0
3	1	0	0	0	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	1	0	1
4	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
5	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0
7	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1	0	1	0
8	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	1	0	1
9	0	0	1	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	1	0	0
10	0	0	1	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	1	0	1	0
11	0	0	1	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	1	0	1
12	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0

Решив задачу о покрытии, получаем дополнительное множество покрытий. Из этого множества по изложенной выше методике выберем покрытия, которые

минимальны по протяженности, и их расположение обеспечивает своевременное прибытие сил реагирования. Характеристики полученных покрытий приведены в таблице 5.8.

Таблица 5.8 – Таблица покрытий

Номер покрытия	Ребра покрытия	Длина покрытия, м	Номер протяженности	Удаление от Y_{10}, м	Примечание
1	$X_7X_{18}X_{19}$	640	1	110	Близко к Y_{10}
2	$X_4X_6X_7X_8X_9$	1860	9	420	Пересекает
3	$X_6X_7X_8X_9X_{16}$	1320	5	220	Пересекает
4	$X_0X_1X_2X_4$	2600	14	510	Длинное
5	$X_0X_1X_2X_{16}$	2100	11	260	Длинное
6	$X_0X_1X_4X_{11}$	2110	12	250	Длинное
7	$\mathbf{X_0X_1X_{11}X_{16}}$	1600	7	250	Удовлетворяет
8	$X_1X_2X_4X_6X_7$	2340	13	210	Пересекает
9	$X_1X_2X_5X_6X_7X_{16}$	1890	10	220	Пересекает
10	$X_1X_4X_5X_6X_7X_{12}$	1790	8	230	Пересекает
11	$X_1X_5X_6X_7X_{11}X_{16}$	1390	6	220	Пересекает
12	$X_4X_7X_{19}X_{20}$	1240	4	150	Близко, пересекает
13	$X_7X_{16}X_{19}X_{20}$	730	2	150	Близко, пересекает
14	$\mathbf{X_6X_7X_8X_{18}X_{21}}$	1210	3	230	Пересекает

Анализ содержания покрытий. Очевидно, что формировать новое покрытие (рубеж обнаружения) для установки ИТСО будет затратным решением, поэтому необходимо на максимально объединяющихся покрытиях предыдущей задачи обеспечить требуемую вероятность обнаружения для Y10. Для решения этой задачи выбираем покрытия, которые не пересекаются с покрытием семь предыдущей задачи и пересекаются со вторым покрытием и одновременно имеют наименьшую длину.

Из четырнадцати покрытий выбираем наиболее приемлемые. Для первого, двенадцатого и тринадцатого покрытия не выполняется условие своевременного прибытия (5.14). Покрытия 2, 3, 8, 9, 10, 11 и 14 частично пересекаются с покрытием семь предыдущей задачи оптимизации. На этих покрытиях было сделано размещение ИТСО второго типа с P_o=0,8, то есть нет возможности наращивать показатель вероятности обнаружения. Поэтому выберем наиболее короткие по протяженности покрытия, которые не имеют общих ребер с седьмым покрытием

предыдущей задачи. Получаем покрытия: четыре ($X_0X_1X_2X_4$), пять ($X_0X_1X_2X_{16}$), шесть ($X_0X_1X_4X_{11}$), семь ($X_0X_1X_{11}X_{16}$). Для обеспечения вероятности 0,95 достаточно одного самого короткого по протяженности покрытия – номер семь ($X_0X_1X_{11}X_{16}$) протяженностью 1600 м.

Пятый этап. Решим задачу ДП для покрытий семь и четырнадцать для обеспечения вероятности обнаружения 0,95 КЭ Y10. В результате решения получили: на оба покрытия необходимо устанавливать ИТСО второго типа. На покрытие четырнадцать уже установлены ИТСО второго типа, чтобы получить вероятность не менее 0,95, надо на покрытии семь установить ИТСО второго типа, на ребрах X_0, X_1, X_{11} ИТСО первого типа заменить вторым, а на ребре X_{16} дополнительно установить ИТСО второго типа. То есть на втором покрытии предыдущей задачи частично ИТСО первого типа заменить вторым. Дополнительное покрытие показано пунктиром на рисунке 5.14 и на плане объекта рисунка 5.15.

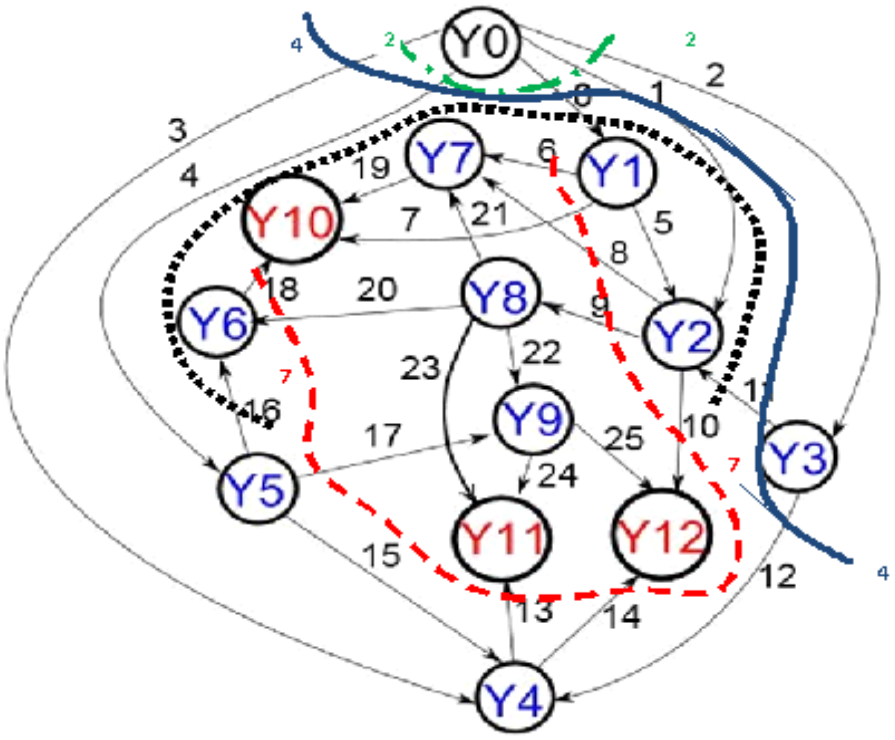


Рисунок 5.14 – Результирующие покрытия

Получаем избыток вероятности обнаружения в первой задаче по всем путям, проходящим через ребра X_0, X_1 и X_{11} при движении в направлении КЭ Y11 и Y12. На схеме видно, что имеется избыток вероятности обнаружения путей, похо-

дящих через ребро X_{16}, поэтому на этом ребре можно рекомендовать установить менее дорогие камеры первого типа с P_o=0,6 (ИТСО первого типа на X_{16}) [116].

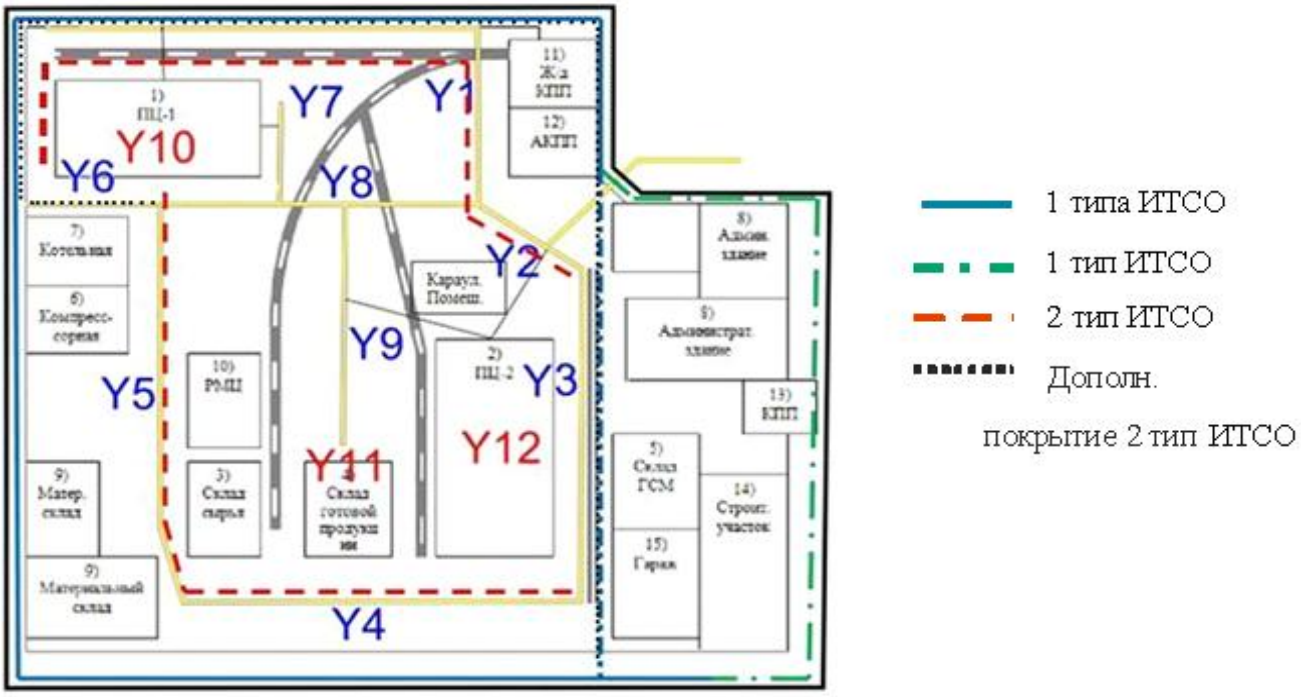


Рисунок 5.15 – План размещения ИТСО на объекте

5.3 Методика формирования элементов организационного управления системы физической защиты на основе информационного подхода

После проведения всех этапов концептуального проектирования СФЗ КВО, необходимо сформировать структуру организационного управления СФЗ, которая обеспечит эффективное выполнение ее функционального назначения. Вопросы формирования структур организационного управления мало исследованы. Одной из причин такого положения является трудная формализация математического описания процессов взаимодействия элементов структуры организационного управления и возможности ее оптимизации. В настоящее время, как правило, структуры организационного управления формируются решением руководителей без использования математических методов, опираясь на предыдущий опыт построения организационных структур.

В последнее время все больше вводятся информационные показатели для определения эффективности функционирования систем, оценки их сложности, организованности и т.д. То есть, информационные критерии и методы их оценки проникают в новые сферы математического анализа систем. Рассмотрим формирование структур организационного управления с помощью информационного подхода на основе введения понятия энтропии с точки зрения анализа упорядоченности и организованности любой системы, в том числе и СФЗ.

По мнению автора Седова Е. А. [90], степень организованности и упорядоченности любой системы можно описать с помощью энтропии, при этом система достигает своей оптимальности при определенной степени неопределенности. В этом случае система, как организованная структура, будет наиболее приспособлена к решению технологических задач в условиях неопределенности ситуаций изменения внешней среды.

Для реализации функционального назначения формируется функциональная и организационная структура СФЗ.

Организационная структура СФЗ представлена в виде древовидного графа подчиненности (рисунок 5.16).

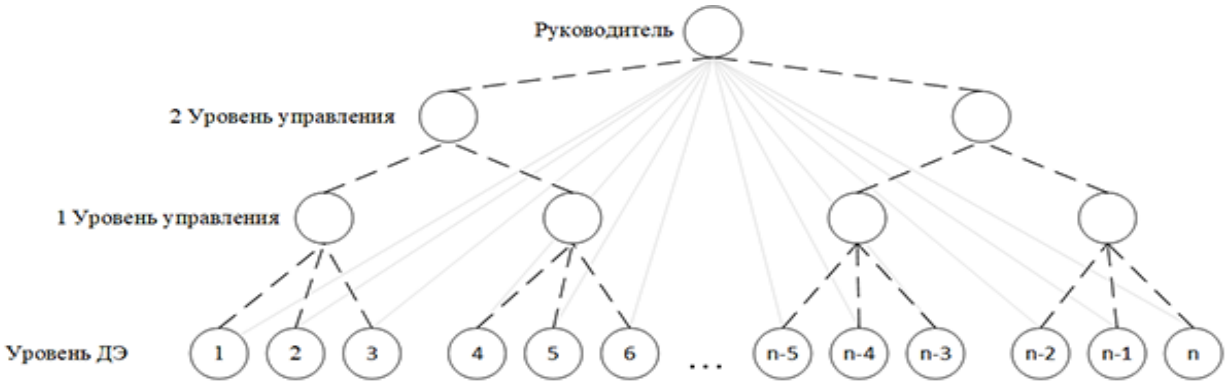


Рисунок 5.16 – Иерархическая структура организационного управления

В общем виде структура организационного управления СФЗ представляет древовидный граф подчиненности, который имеет определенную ширину (количество отдельных функций) и глубину (количество уровней управления). Структура организационного управления отражает логические взаимосвязи между

уровнями управления и функциональными областями, позволяющими организации максимально эффективно достигать своих целей [117].

При формировании организационных структур с увеличением количества управляющих элементов растут расходы управленческого аппарата и время процесса управления, при этом уменьшается информационная нагрузка на элементы управления (рисунок 5.17). При уменьшении количества управляющих звеньев увеличивается информационная нагрузка (снижая стоимость) на элементы управления, что может привести к возникновению задержек и ошибок в управлении от информационной перегрузки исполнителей. В данном случае должна быть золотая середина между двумя тенденциями, это и будет оптимальной информационной нагрузкой (нормой управляемости) в структуре организации [117].

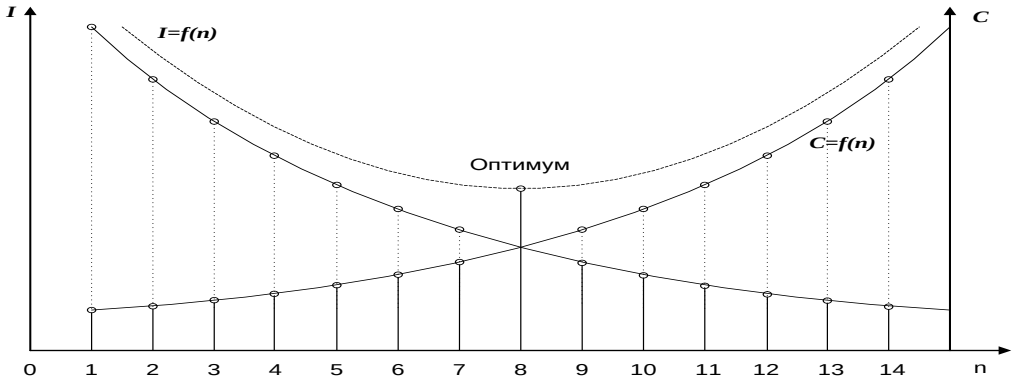


Рисунок 5.17 – Информационно-стоимостные зависимости от n элементов организационного управления

Постановка задачи. Будем считать структуру организационного управления оптимальной, если информационная нагрузка на все элементы организационного управления стремится к оптимальному значению. Показатель информационной нагрузки – количество информации на элемент управления $Iэу$. Тогда критерий оптимальности опишем в виде: $Iэу \to opt$. То есть, информационная нагрузка на элементы управления в ширину и глубину графа структуры организации стремится к оптимальному значению [68].

Процесс формирования элементов управления с оптимальной нагрузкой рассматривается как развитие (эволюция) системы – включаются дополнительные элементы в систему (средства наблюдения), система расширяется (увеличивается

контролируемая зона ответственности и т. д.) и, следовательно, увеличивается количество информации в системе. Согласно источникам [68, 90], при развитии систем значение величины оптимальности информационной нагрузки $Iэу \to opt$ на элементы структуры управления достигается при обеспечении порции преемственности энтропии развития системы от предыдущей системы (степени структурной упорядоченности системы) в виде критерия оптимальности $G_H^{ОПТ} = 0,27.$ Наилучшее соотношение порции преемственности энтропии порождает оптимальную величину структурной информации.

Порция преемственности энтропии G_H^K – это количество энтропии в новой системе от начальной (предыдущей) системы (начального состояния). Если в полученной системе количество энтропии мало отличается от начальной системы $(G_H^K < 0,27)$, то это лишь модернизация системы (т. е. система не совершенна). Если в полученной системе количество энтропии значимо отличается от начальной системы $(G_H^K > 0,27)$, то в этом случае большой риск, что система будет не приспособлена к новым условиям. Это баланс старого и нового в перспективной системе.

В приложении к данной предметной области – порция преемственности энтропии системы контроля – количество энтропии начального элемента (состояния) представленная в новой системе контроля (зоне ответственности).

Решение задачи. Формирование организационного управления начинается с нижнего уровня организации (снизу вверх).

Первый этап. На самом нижнем уровне (первом) организационной структуры исполнителей определяются все технологические операции (ТО), которые выполняются при функционировании СФЗ. Степень детализации ТО: каждую операцию выполняет отдельный исполнитель самостоятельно или с использованием определенного вида ИТСО. Всех исполнителей ТО и ИТСО будем называть действующими элементами (ДЭ). Исходные данные о ДЭ представляются в виде матрицы. Строки – совокупность ДЭ по назначению, уровню специализации и т. д. Столбцы – ТО, или информация, получаемая при

выполнении ТО. Поле матрицы – степень участия ДЭ при реализации ТО или получении информации, оценивается дискретной величиной от нуля до двух: 0 – не участвует в выполнении ТО; 1 – готовит и (или) обеспечивает выполнение ТО; 2 – выполняет или контролирует выполнение ТО.

Обработав данную информационную МГК, получим объединение ДЭ в компоненты. Иными словами, получаем структуру ДЭ в виде их декомпозиции по ортогональным компонентам (информационным темам). Каждая компонента рассматривается как принадлежность связанных ДЭ по определенному информационному признаку. Таким образом, построение организационной структуры основано на выделении множества отдельных функций или задач организации в виде групп ДЭ, объединенных в компоненты, которые и формируют слепок структуры организации первого уровня управления (рисунок 5.16).

Второй этап. Используя информационно-вероятностный метод для каждой компоненты, оценивался информационный потенциал действующих элементов в виде энтропии. Исходными данными для оценки информационного потенциала являлась матрица признаков ДЭ.

Затем в каждой компоненте ДЭ формируются в группы (структурные единицы) оптимального информационного размера, используя критерий оптимальной порции преемственности энтропии развития систем $G_H^{ОПТ}$. Полученные группы (структурные единицы) по величине сосредоточенной информации должны быть однородны, т.е. их информационная нагрузка (не зависимо от количества ДЭ) в виде порции преемственности энтропии составляет $G_H^{ОПТ}$ [68]. Результат решения – структурные единицы первого уровня организационного управления (рисунок 5.16).

Третьим этапом построения является формирование по информационному признаку структур более высокого уровня организационного управления (второго и т.д.). Когда сформирован самый низший (первый) уровень управления, необходимо каждую структурную единицу информационно сжать, то есть охарактеризо-

вать значимой информацией назначения, функции, операции или характеристики. Это набор семантических и количественных характеристик (в виде интерпретации компонент) функционального назначения структурной единицы. Определялись средние характеристики по каждой структурной единице, которые сводились в таблицу. Далее необходимо обработать таблицу МГК и определить объединения структурных единиц первого уровня в компоненты, то есть осуществляется композиция элементов назначения в целое назначение на основе семантических определений назначения путем использования МГК. Таким образом, на данной матрице проводится МГК анализ объединения элементов в компоненты по информационному признаку, и на их основе формировался соответствующий (второй) уровень организационного управления. Если это разные компоненты, то эти разнородные несвязанные элементы отдельно связываются с более высоким (третьим) уровнем управления по информационной компоненте.

Четвертый этап. Проверяется однородность информационной нагрузки на элементы каждого уровня управления путем оценки величины энтропийного потенциала (информационной нагрузки) каждого элемента управления. При возникновении неоднородности проводятся различные варианты декомпозиции и (или) композиции структурных элементов организации для достижения однородности, при необходимости, в крайнем случае, может возникать дополнительная ветвь управления.

Информационный потенциал каждого ИТСО описывался в виде значения величины энтропии. Имеется n ИТСО, претендующих на включение в структурную единицу; каждому ИТСО поставлена в соответствие совокупность m признаков, определяющих его информационный потенциал.

Декомпозиции множества ИТСО на значимо различные классы (структурные единицы) характеризуется таблицей 5.9.

Для данных таблицы 5.9 использовались расчеты ИВМ по формулам 2.5 – 2.10.

Таблица 5.9 – Модифицированная морфологическая матрица

Наименование признаков ИТСО	Множество ИТСО				
	$\{A_1\}$	...	$\{A_i\}$	…	$\{A_n\}$
X_1	X_{11}	…	X_{1i}	…	X_{1n}
X_j	X_{j1}	…	X_{ji}	…	X_{in}
...	…	…	…	…	…
X_m	X_{m1}	…	X_{mi}	…	X_{mn}

Если рассматривать организационную структуру как развитие, т.е. как расширение за счет включения дополнительных ИТСО в организацию, то это приводит к увеличению информации, а следовательно нагрузки на оператора. Количество информации в *k*-ой структурной единице определим как увеличение энтропии относительно начальной энтропии $H_1(p)$:

$$H_K(p) = \sum_{i=1}^{i=q} H_i(p) - H_1(p) \tag{5.15}$$

где q – количество ИТСО в к- ой структурной единице.

Количество информации $I_к$, накопленной в данной структуре определяется $I_k = H_{\max} - H_k(p)$. Удельный вес этой порции определяется: $G_H^k = H_k(p) / I_k$.

В результате анализа работ из различных научных областей доказано существование оптимального значения величины $G_H^{ОПТ}$, характеризующей удельный вес порции энтропии [68, 90]. Получено оптимальное значение порции энтропии $G_H^{ОПТ}$=0,272 – это наилучшее соотношение непредсказуемости и детерминированности системы (структурной единицы). Поэтому оценка ошибки мощности критерия (удельного веса порции энтропии) определяется:

$$\beta_i^{ЭФ} = G_H^K - G_H^{ОПТ}. \tag{5.16}$$

То есть при включении очередного *i*-го ИТСО в структурную единицу информация возрастает, это приводит к увеличению информационной нагрузки на оператора. И когда будет выполнено условие $G_H^K = G_H^{ОПТ}$, наступает момент оптимального развития системы. Если $G_H^K > G_H^{ОПТ}$, то расширение количества элементов приведет к большой неоднородности элементов системы внутри структурной единицы, т. е. получим информационную избыточность или перегруз – структур-

ная единица будет трудно управляема. Если $G_H^K < G_H^{ОПТ}$, то получим структурные единицы, информационно не достаточно нагруженные (система не развита).

Рассмотрим решение задачи на модельном примере. Исходные данные: результаты размещения технических средств обнаружения (ТСО) СФЗ, которые представлены на рисунках 5.18, 5.19 и в таблице 5.10 [113].

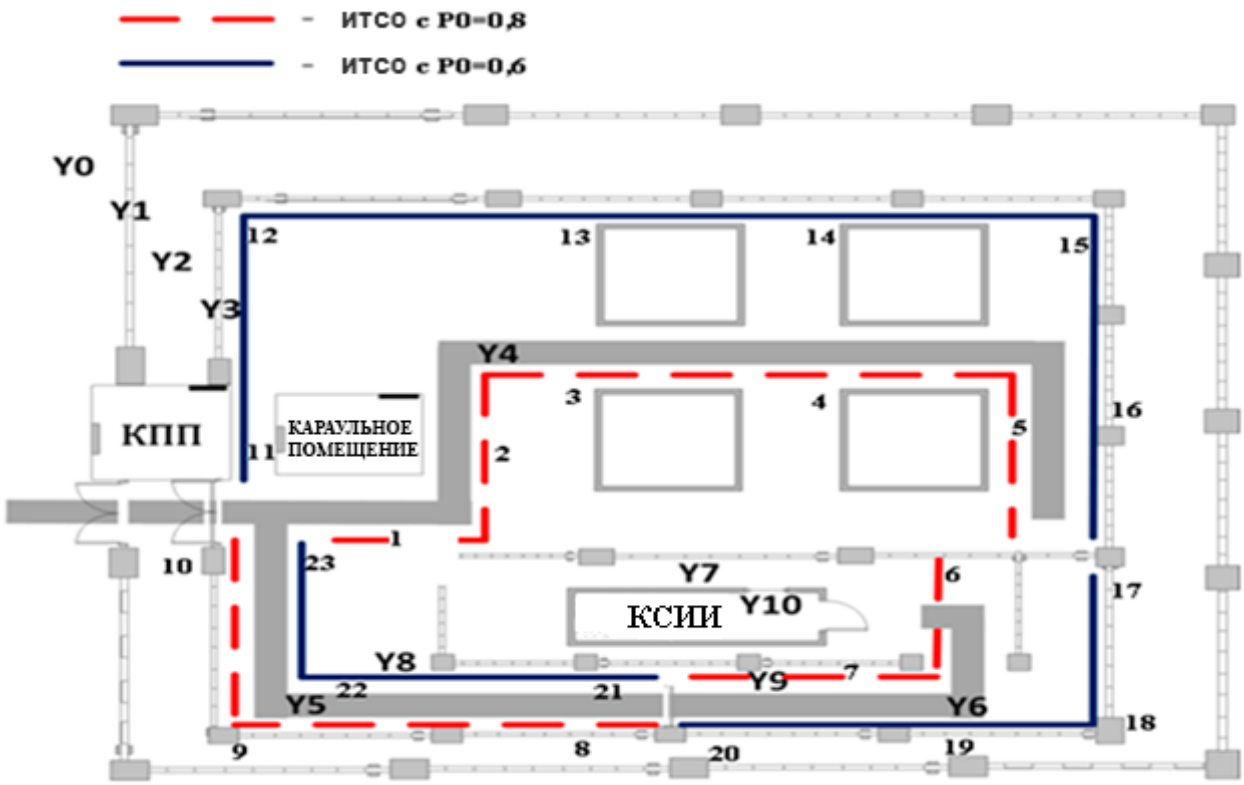


Рисунок 5.18 – Объект с рубежами расположения ИТСО

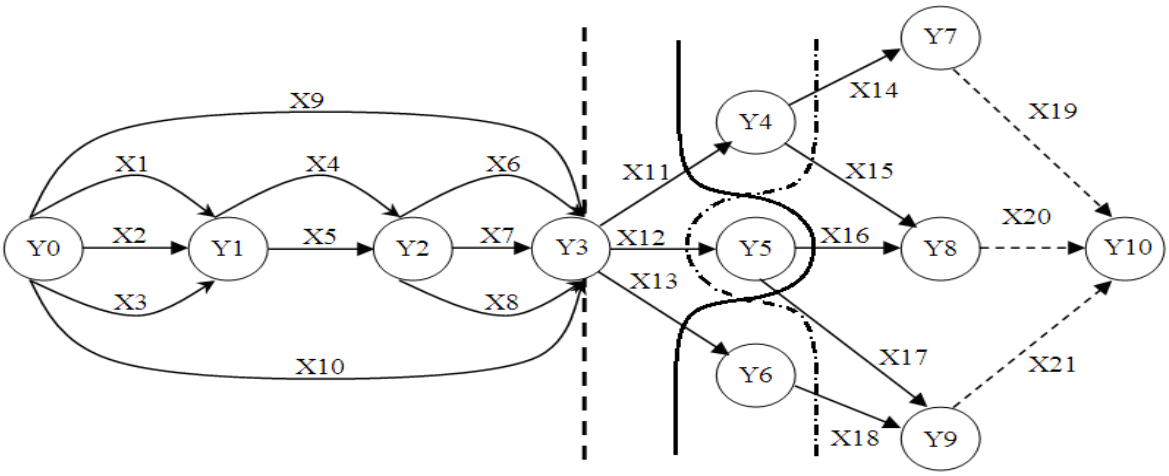


Рисунок 5.19 – Прерывание нарушителей на графе проникновения

Таблица 5.10 - Характеристики инженерно-технических средств обнаружения

Тип ТСО, точки контроля	Наименование ребер на графе проникновения	Вероятность обнаружения	Количество ТСО	Протяженность, м. - номер покрытия	Удаление от КСИИ, м	Угол обзора, град	Дальность, м
1 тип ТСО	X_{11}, X_{13}, X_{16},X_{17}	0,6	13	880 – 10	450	70 – 90	60
2 тип ТСО	X_{12}, X_{14}, X_{15}, X_{18}	0,8	10	670 – 9	300	70 – 90	70

Необходимо сформировать на нижнем уровне организационного управления структурные единицы ТСО. По результатам исследования функционального назначения ТСО и ТО методом главных компонент все технические средства обнаружения объединились в первую компоненту. Далее необходимо определить оптимальный информационный размер структурных единиц. Каждое средство определяется характеристиками расположения (опасность контролируемой зоны, удаление от КСИИ, интенсивности движения в зоне ТСО и т. д.), которые сведены в таблице 5.11.

Таблица 5.11 – Характеристики расположения ТСО

№ ТСО	Характеристики расположения ТСО						Энтропийная важность ТСО H_i	Энтропия преемственности G_H^K
	Опасность направления +	Вероятность движения нарушителя+	Вероятность обнаружения +	Номер эшелона расположения ТСО	Интенсивность движения в зоне ТСО +	удаление от КСИИ		
1	1	0,5	0,8	2	8	300	0,207	**0,009**
2	1	0,5	0,8	2	7	280	0,197	**0,029**
3	1	0,6	0,8	2	6	370	0,223	**0,069**
4	2	0,7	0,8	2	6	350	0,280	**0,109**
5	2	0,6	0,8	2	5	320	0,254	**0,159**
6	4	0,6	0,8	2	6	300	0,319	**0,211**
7	4	0,5	0,8	2	5	280	0,292	**0,280**
8	3	0,5	0,8	1	3	300	0,315	0,359
9	3	0,6	0,8	1	6	340	0,359	0,053
10	3	0,7	0,8	1	9	360	0,394	0,119
11	1	0,7	0,6	1	9	330	0,242	0,162
12	1	0,5	0,6	1	4	420	0,192	0,201
13	1	0,3	0,6	1	2	410	0,133	0,229
14	2	0,3	0,6	1	2	450	0,183	0,268
15	2	0,3	0,6	1	2	460	0,185	0,311
16	2	0,6	0,6	1	6	400	0,264	0,379
17	4	0,7	0,6	1	7	350	0,341	0,051
18	4	0,7	0,6	1	4	370	0,325	0,103
19	4	0,8	0,6	1	7	350	0,356	0,168
20	4	0,8	0,6	1	7	340	0,354	0,240
21	3	0,6	0,6	2	7	280	0,223	0,290
22	3	0,6	0,6	2	7	300	0,227	0,330
23	3	0,7	0,6	2	9	320	0,257	0,325

Одним входом информационного поля (столбцы) являются характеристики, а другой – носители этой информации – номера технических средств защиты. Элементы матрицы – соответствующие количественные характеристики ТСО. Вероятность движения нарушителя через зону расположения ТСО и интенсивности движения в зонах объекта определены экспертным путем (таблица 5.11).

Величина опасности зоны охраны определена экспертным методом с помощью качественной шкалы относительной важности по аналогии шкалы Саати [118]. Номера зон расположения ТСО и величина опасности направления объекта приведена на макете объекта в виде рисунка 5.20.

Рисунок 5.20 – Номера зон расположения ТСО и опасности направлений

По результатам анализа данных все ТСО объединились в первую компоненту. Следующим шагом будет оценка информационной нагрузки, а именно декомпозиция целого на информационные группы.

Для оценки энтропийного потенциала важности каждого ТСО используется ИВМ. На основе этих характеристик определялся информационный потенциал каждого ТСО. Все ТСО последовательно пронумерованы по месту расположения на объекте (рисунок 5.18).

Анализ результатов расчета показывает, что технические средства защиты имеют разные информационные потенциалы важности, поэтому при формировании информационных структур необходимо объединять в группы, разные по количественному составу, но однородные по информационной нагрузке на элементы организационного управления (оператора, охранника, начальника караула и т. д.).

Вся совокупность ТСО (таблица 5.11) декомпозировалась на три группы: 1 – 7; 8 – 16; 17 – 23, что соответствует оптимальной порции преемственности энтропии в данной информационной ситуации. Если порция энтропии больше оптимальной величины, то увеличивается нагрузка на элемент управления. Иначе говоря, если количество ТСО в группе будет больше, то теряется их однородность как системы элементов, возникает новая информационная ситуация, то есть нарушается оптимальное соотношение одноразовой порции энтропии по отношению к максимальной энтропии информационной ситуации. Если порция будет меньше требуемой величины, то оператор будет информационно не догружен.

Алгоритм. Структурные элементы формируются, выбирая последовательно объекты из таблицы 5.11. Применяя расчетные формулы для выбранных ТСО, определяли значения мощности критерия G_H^k. По условиям решения задачи задавалась величина $\beta_0^{ЭФ}$ =0,03 Если расчетное значение $\beta_i^{ЭФ}$ превышало требуемые, то в множество выбранных ТСО включали очередной объект защиты и расчеты (2.5 – 2.14) повторялись. Итерация повторялась, пока $\beta_0^{ЭФ}$ не удовлетворяла заданным требованиям. Аналогично формировались последующие элементы структуры. Результаты формирования групп представлены в таблице 5.12 и показаны на рисунке 5.21.

Таблица 5.12 – Объединение групп ТСО

Характеристика	Номера сформированных групп ТСО		
	1	2	3
Номер из таблицы 5.12	1 – 7	8 – 16	17 – 23
Опасность направления	1	2	1,5
Номер эшелона	2	1,5	1
Информационная нагрузка	0,320	0,328	0,311

Таким образом, получили оптимальное объединение в группы ТСО, то есть максимум однородности информационной нагрузки в группах на элементы управления, что обеспечит приспособленность системы управления в условиях неопределенности изменения внешних условий. При меньшей нагрузке оператор будет информационно не догружен, при большей – перегружен.

Формируем следующий уровень управления. От таблицы 5.11 перейдем к параметрам, связывающим операторов в единую систему (таблица 5.13). Применим МГК, определим связь операторов и затем – информационную наполняемость.

Таблица 5.13 – Характеристики важности контролируемых зон операторами

Операторы	Количество ТСО +	Опасность направления +	Р движения нарушителя +	Вероятность обнаружения +	Номер эшелона расположения ТСО -	Интенсивность движения в зоне ТСО +	Удаление от КСИИ +	Энтропийный потенциал оператора H_i	Порция энтропии преемственности
1	7	2,3	0,6	0,8	2	7	320	0,691	0,07
2	9	2,0	0,5	0,65	1	8	450	0,945	0,155
3	7	3,5	0,8	0,7	1,5	5	360	0,940	0,297

Проведя корреляционный, компонентный, кластерный, а также информационный анализ можно сделать вывод о том, что три оператора объединяются в одну компоненту с единой информационной нагрузкой. Полученный элемент структуры организационного управления представлен на рисунке 5.21, а характеристики распределения информационных нагрузок – в таблице 5.13.

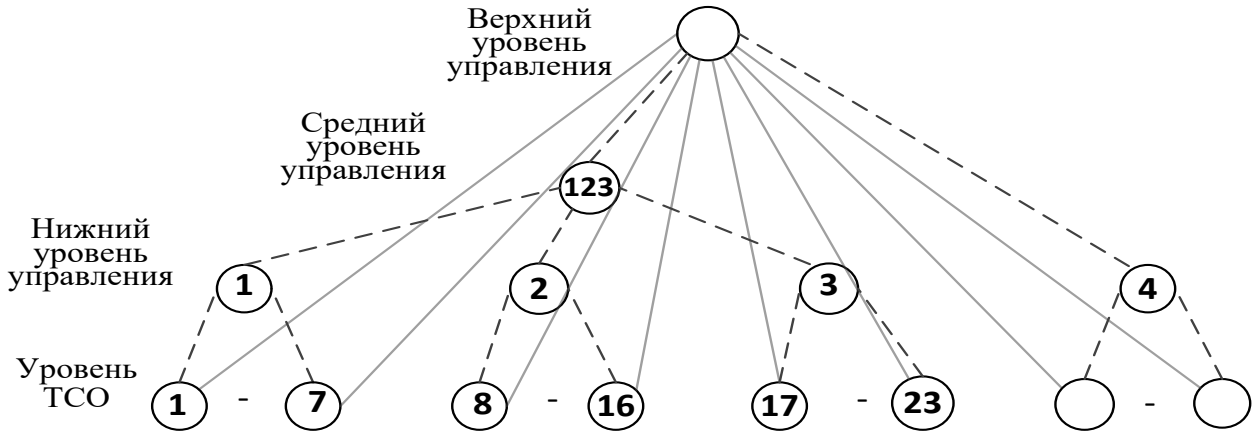


Рисунок 5.21 – Схема объединений ТСО в группы организационного управления уровня операторов

Таким образом, рассмотрена методика формирования организационных структур элементов СФЗ на основе информационного подхода. На типовом примере приведен фрагмент решения задачи формирования структуры организационного управления нижнего уровня.

5.4 Выводы

1. Разработана методика оптимального размещения ИТСО, которая была апробирована на типовых КВО. На основе формирования множества логических функций проникновения и решения задач о покрытии и ДП произведен синтез оптимального размещения ИТСО СФЗ, удовлетворяющий заданным требованиям безопасности для одного КЭ и разных по степени важности КЭ объекта.

2. Вероятность обнаружения нарушителя на путях проникновения к цеху №2 и складу готовой продукции составила $P_O \geq 0,9$, а к цеху №1 – $P_O \geq 0,95$. Это удовлетворяет заданным требованиям при минимальной стоимости размещения ИТСО. Кроме того, расположение ИТСО на путях проникновения нарушителя соответствует заданным требованиям вероятности своевременного прибытия сил реагирования $P_{СВП} \geq 0,8$. Таким образом, размещение ИТСО обеспечивает заданные требования безопасности критически важного объекта [116].

3. Рассмотрен информационный подход к формированию элементов управления организационных структур технических средств обнаружения СФЗ. На типовом примере приведен фрагмент решения задачи формирования структур организационного управления нижнего уровня (объединения ТСО в структуру).

ГЛАВА 6 КОМПЛЕКСНАЯ ОЦЕНКА И ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ СИСТЕМЫ ФИЗИЧЕСКОЙ ЗАЩИТЫ

6.1 Оценка эффективности системы физической защиты критически важных объектов на основе марковской модели

Завершающим и важным этапом разработки СФЗ является оценка ее эффективности. Материал данного раздела является продолжением исследований вопросов оценки эффективности СФЗ на основе системного анализа. Для оценки функционирования СФЗ необходимо определить показатель эффективности. В первом разделе диссертации проведен анализ системы показателей оценки эффективности СФЗ.

По мнению автора, наиболее полно характеризующим показателем эффективности функционирования СФЗ является вероятность нахождения КВО в безопасном состоянии. Данный критерий определяется двумя связанными показателями – вероятностью обнаружения нарушителя и вероятностью своевременного прибытия сил реагирования и нейтрализации нарушителя – и был представлен зависимостью (1.4). В этой зависимости два показателя: P_O – вероятности обнаружения нарушителя и $P_{СВП}$ – вероятности своевременного прибытия сил реагирования и нейтрализации нарушителя, которые в совокупности определяют величину эффективности СФЗ.

Решение задачи рассмотрим на модельном примере. КВО представляет собой сложную систему, состоящую из множества связанных зон охраны, различной природы назначения, важности и уровня защищенности (рисунок 6.1).

Вся территория объекта имеет двойное ограждение, периметровую охрану и контрольно-пропускной пункт (КПП). На КВО имеется ключевая система информационной инфраструктуры, подлежащая охране. На рубежах зон охраны располагаются ИТСО. Цель нарушителя – проникнуть в КСИИ и вывести из строя АСУ технологическим процессом КВО для создания ЧС.

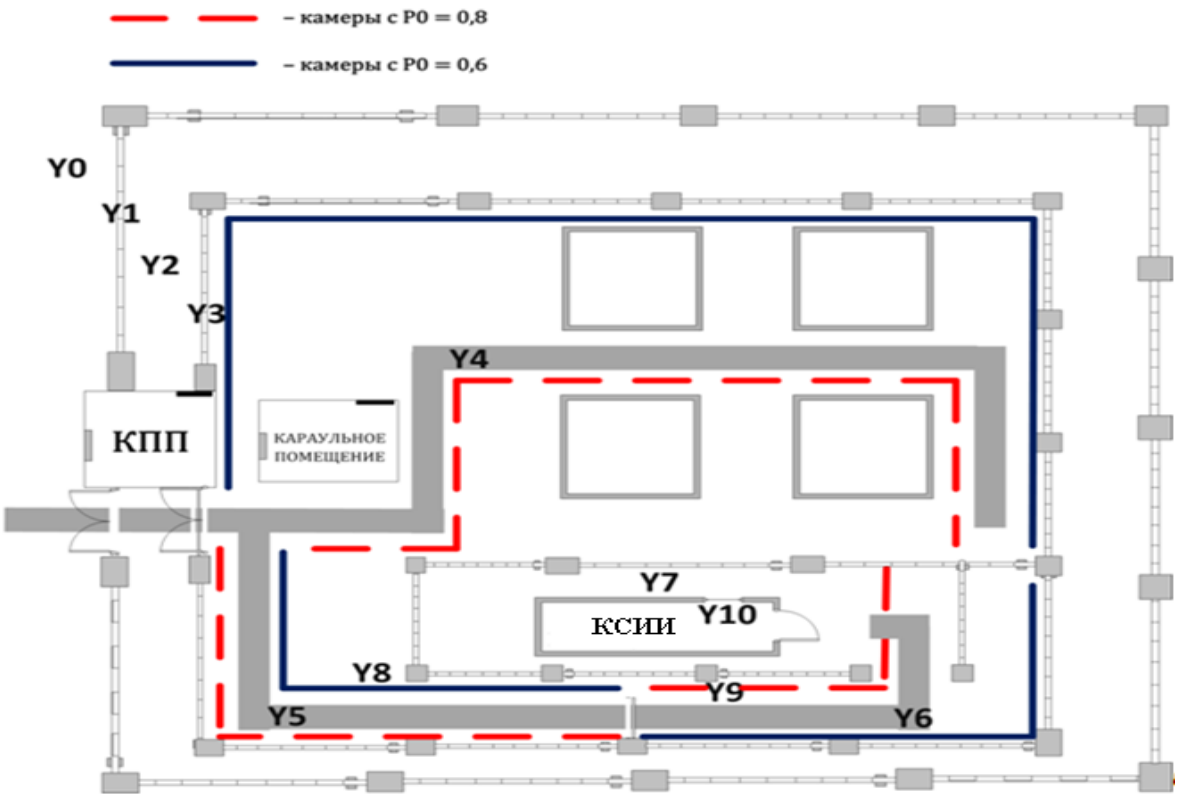
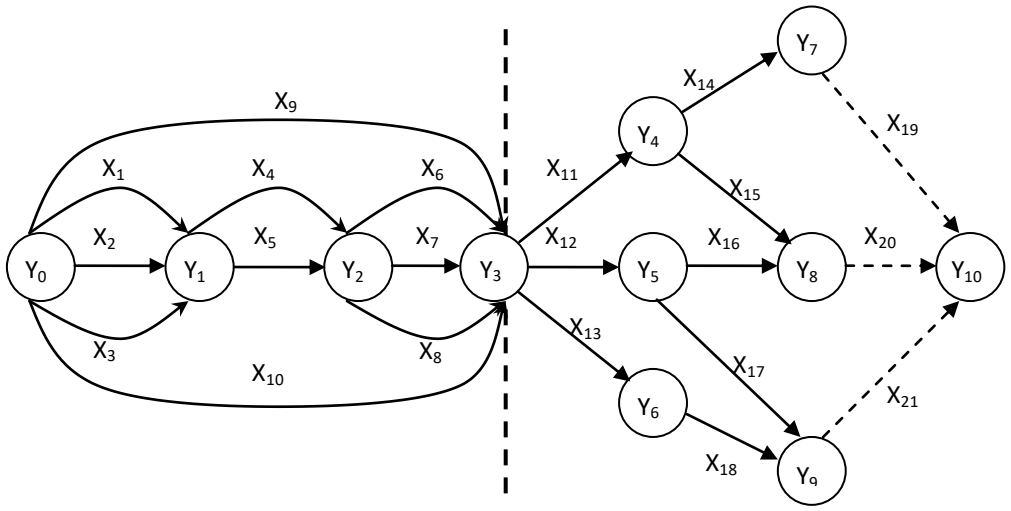


Рисунок 6.1 – Расположение ИТСО на объекте

Модель проникновения нарушителя представлена в виде разветвленного ориентированного мультиграфа (рисунок 6.2). Мультиграф – это сценарий проникновения нарушителя на охраняемый объект. Вершины графа обозначим как рубежи зон охраны при достижении нарушителем определенного результата на пути к цели. Ребра графа – варианты перемещений нарушителя между рубежами охраны. Ребра обозначим Xi, где i – номер ребра (варианта перемещения) в графе. Всего определим n рубежей зон охраны. Следовательно, граф имеет n вершин (событий). Первая вершина – Yo, последняя – Yn. Событию Yo присваивается единица – это вероятность нахождения нарушителя в нулевом событии в начальный момент времени.

Наступление события Yn означает факт проникновения нарушителя на объект, то есть нарушитель достиг цели (хищение и т. д.). Вероятность нахождения события Yn в безопасном состоянии и будет показателем эффективности СФЗ.

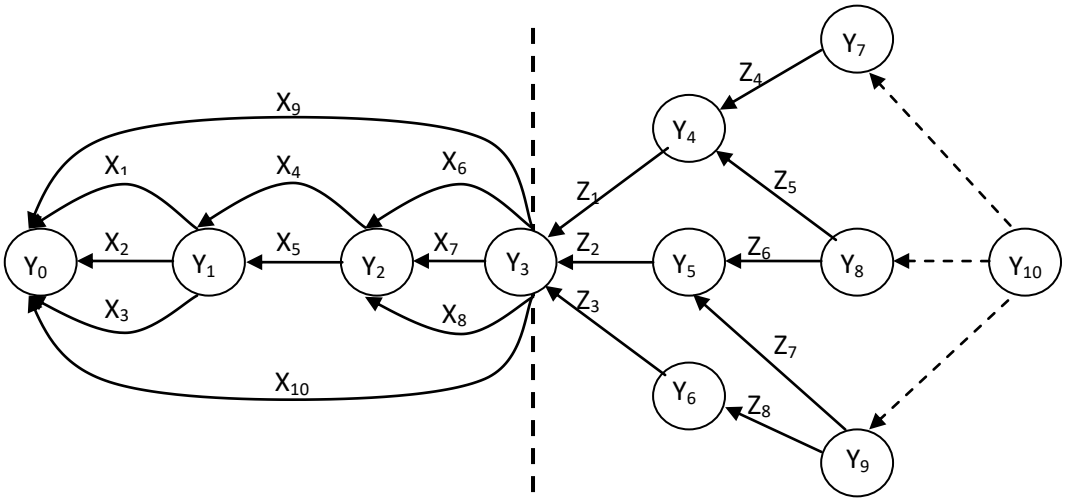


граница объекта

Рисунок 6.2 – Граф достижимости нарушителем цели

На рисунке 6.2 обозначено: X_1 – преодоление ограждения через верх; X_2 – через ограждение путем разрушения ограждения; X_3 – подкоп ограждения для преодоления; X_4 – преодоление зоны бегом; X_5 – преодоление зоны ползком; X_6 – преодоление второго ограждения через верх ограждения; X_7 – разрушение второго ограждения; X_8 – подкоп второго ограждения; X_9 – проход через КПП путем подбора ПИН -кода; X_{10} – проникновение через ворота путем подмены документов; X_{11} – X_{21} – варианты перемещения через зоны между рубежами Y_3 – Y_{10} внутри объекта.

Для отображения противодействия СФЗ введем еще один ориентированный граф (рисунок 6.3).



граница объекта

Рисунок 6.3 – Граф противодействия СФЗ проникновению нарушителя

Вершины графа обозначаются как рубежи противодействия системы защиты на нарушителя. Ребро в графе ассоциируется с каким-то типом варианта защиты объекта, который будет характеризоваться вероятностью защиты. Ребро – вероятность того, что СФЗ обнаружит нарушителя и окажет противодействие при переходе между рубежами. Ребра так же будем обозначать Zi, где i – номер ребра (вариант противодействия) в графе. Полученный граф назовем графом противодействия. Всего будем определять n рубежей, как и в предыдущем графе, то есть граф имеет n вершин. Первая вершина – Yn, последняя – Yo. Событию Yn присваивается значение 1. Ребра будут направлены от вершины Yn к Yo.

Марковская модель позволяет оценить вероятности состояний двух противоборствующих систем: нарушителя и СФЗ, то есть оценить вероятность реализации угрозы. Исходными данными являются вектор начальных состояний нарушителя, матрица смежности вероятностей преодоления рубежей защиты за время Δt и матрица смежности вероятностей противодействия (нейтрализации нарушителя) СФЗ. Исходные данные определяются расчетным путем и методом экспертных оценок, а также проведением натурного эксперимента на реальном объекте защиты. В процессе моделирования определяется вектор предельных вероятностей состояний каждого события графа (рубежа), в том числе и конечного, как вероятность безопасного состояния объекта.

Таким образом, имеем модель марковской цепи с дискретными состояниями, представленную в виде ориентированного взвешенного графа. Переход системы из состояния в состояние будем рассматривать в дискретные моменты времени Δt.

Система задана, если определены два условия [104].

1. Вероятности состояний системы $P_i(t)$:

$$P^{(0)}{}_i = (P_{01}, P_{02}, ..., P_{0n}). \qquad (6.1)$$

2. Вероятности переходов $P_{ik}(\Delta t)$ из i-го в k-ое состояние за время Δt . Вероятности переходов задаются с помощью квадратной матрицы:

$$P_{ik}(\Delta t) = \begin{vmatrix} P_{11}(\Delta t) & P_{12}(\Delta t) & \dots & P_{1n}(\Delta t) \\ P_{21}(\Delta t) & P_{22}(\Delta t) & \dots & P_{2n}(\Delta t) \\ \dots & \dots & \dots & \dots \\ P_{n1}(\Delta t) & P_{n2}(\Delta t) & \dots & P_{nn}(\Delta t) \end{vmatrix}. \quad (6.2)$$

Тогда вероятность нахождения системы в k-ом состоянии, в момент времени $t + \Delta t$, будет определяться по формуле полной вероятности:

$$P_K(t+\Delta t) = P_1(t) \cdot P_{1K} + P_2(t) \cdot P_{2K} + \dots + P_K(t) \cdot P_{KK} + \dots + P_n(t) \cdot P_{nK}, \quad (6.3)$$

или можно записать в следующем виде:

$$P(t+\Delta t) = P(t) \cdot P_{ij}(t+\Delta t), \quad (6.4)$$

где $P(t) = \{ P_1(t), P_2(t), и\ P_n(t) \}$ – вектор начальных состояний системы;

P_{ij} – матрица вероятности переходов уравнения Маркова.

При этом сумма вероятностей:

$$\sum_{i=1}^{n} P_i = 1. \quad (6.5)$$

Так как математический аппарат марковских моделей не позволяет моделировать работу мультиграфов, поэтому путем стягивания весов ребер к одному ребру перешли к обычному графу. Так как граф достижимости нарушителем цели и граф противодействия отличаются только направлением ребер, то графы можно совместить, при этом матрица смежности вероятностей переходов между вершинами за время Δt результирующего графа получится путем объединения матриц смежности исходных графов с нормированием вероятностей переходов (рисунок 6.4).

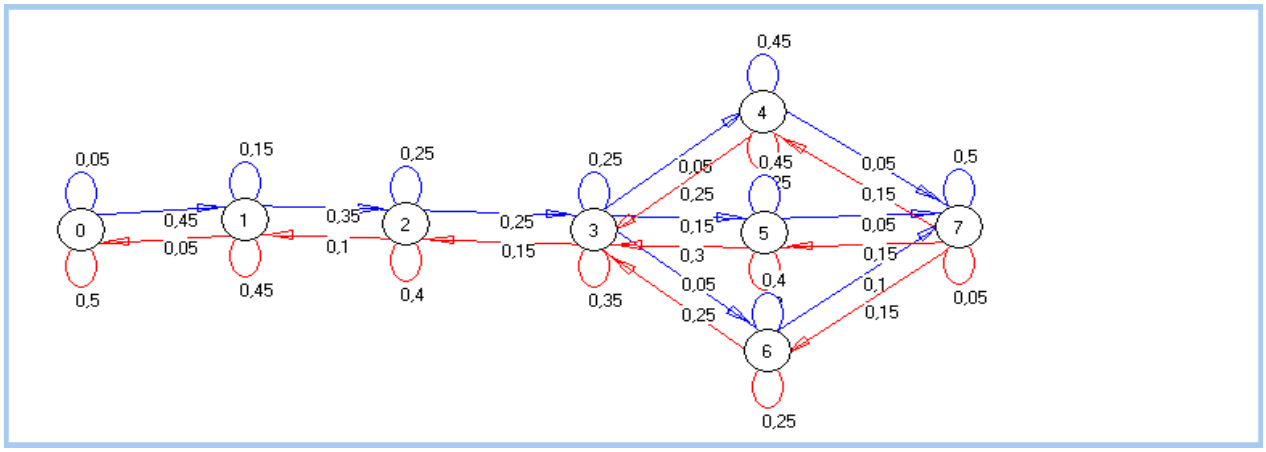


Рисунок 6.4 – Граф проникновения нарушителя и противодействия СФЗ

Ребра синего цвета обозначают вероятности переходов нарушителя между рубежами за время Δt, а ребра красного цвета – вероятности противодействия СФЗ проникновению. Вектор исходного состояния нарушителя представлен в виде вектора строки. Умножая вектор вероятности состояний на матрицу смежности вероятностей, получаем установившийся результат на определенной итерации. Вероятность конечного n-го события и будет вероятностью безопасного состояния объекта. С использованием данных теоретических предпосылок разработано программное средство на языке программирования C#, реализующее оценку эффективности СФЗ. Матрица смежности вероятностей переходов представлена таблицей 6.1.

Таблица 6.1 – Матрица смежности

Номер вершины	0	1	2	3	4	5	6	7
0	0,55	0,45	0	0	0	0	0	0
1	0,05	0,6	0,35	0	0	0	0	0
2	0	0,1	0,65	0,25	0	0	0	0
3	0	0	0,15	0,6	0,05	0,15	0,05	0
4	0	0	0	0,25	0,7	0	0	0,05
5	0	0	0	0,3	0	0,65	0	0,05
6	0	0	0	0,25	0	0	0,65	0,1
7	0	0	0	0	0,15	0,15	0,15	0,55

Вектор исходного состояния нарушителя и системы нейтрализации нарушителя представлены в виде одномерной матрицы строки с обязательным выполнением условия нормировки. Исходный вектор начальных вероятностей состояний представлен в таблице 6.2.

Таблица 6.2 – Исходный вектор начальных вероятностей вершин

Номера событий и начальные вероятности состояний							
0	1	2	3	4	5	6	7
1	0	0	0	0	0	0	0

Будем умножать вектор вероятности состояний на матрицу вероятностей смежности, пока вероятности событий не достигнут предельных состояний.

Получили следующие итерации:

1) 0,275 0,225 0 0 0,075 0,075 0,075 0,275;
2) 0,1625 0,2587 0,0787 0,06 0,0937 0,09 0,09 0,1662;
3) 0,1023 0,2362 0,1507 0,1286 0,0935 0,0924 0,0864 0,1096;
4) 0,0680 0,2028 0,1999 0,1875 0,0883 0,0958 0,0790 0,0782;
5) 0,0475 0,1723 0,2291 0,2331 0,0829 0,1021 0,0725 0,0601;
6) 0,0347 0,1477 0,2442 0,2666 0,0787 0,1103 0,0678 0,0495;
7) 0,0265 0,1287 0,2504 0,2908 0,0759 0,1192 0,0648 0,0435;
8) 0,0210 0,1142 0,2514 0,3080 0,0742 0,1276 0,0632 0,0401;
9) 0,0172 0,1031 0,2496 0,3203 0,0733 0,1351 0,0625 0,0385;
10) 0,0146 0,0946 0,2464 **0,3291** 0,0731 0,1417 0,0624 0,0378.

Таким образом, на 10-й итерации программа завершает свое выполнение, т.е. спустя период времени десять Δt система перешла в установившиеся финальные (предельные) вероятности. Результатами моделирования являются вероятности проникновения нарушителя для реализации цели. По результирующему вектору видно, что наибольшая вероятность установившегося состояния системы находится в третьем рубеже защиты.

Разработанная вероятностная модель Маркова не позволяет корректно оценить эффективность функционирования СФЗ. Недостатком вероятностной модели является то, что вероятности переходов из состояния в состояние трудно достоверно рассчитать. Кроме того, проблема состоит в обеспечении нормализации вероятностей вектора исходного состояния нарушителя и сил реагирования на одном векторе исходных данных и нормализацию вероятностей переходов нарушителя и сил реагирования на одной исходной матрице вероятности переходов [122].

Решение задачи оценки эффективности с помощью марковской модели в такой постановке составило непреодолимую трудность по следующим причинам: сложность проведения нормировки графа на совместной матрице переходов при взаимодействии противодействующих сторон и трудности принятия решений в случае невыполнения требований эффективности СФЗ. По этой причине перешли к синтезу марковских моделей оценки эффективности СФЗ.

6.2 Метод оценки эффективности системы физической защиты критически важных объектов на основе марковских цепей

Целью является разработка метода оценки эффективности СФЗ (оценки варианта размещения ИТСО) на основе марковских цепей. Для решения этой задачи необходимо разработать метод формирования логических функций проникновения, на основе которых с помощью марковских цепей осуществляется оценка эффективности СФЗ.

Разработанный метод позволяет получить совокупность всех путей проникновения нарушителя на объект, представленных как логические функции проникновения в виде дизъюнкции и конъюнкции логических переменных – ребер графа, которые сформированы в информационную матрицу инцидентности для решения задачи оценки эффективности СФЗ.

Достоинства метода: 1) сложная задача оценки вероятности безопасного состояния объекта представлена как оценка надежности системы в виде мультиграфа, который декомпозируется на множество простых графов проникновения нарушителя; 2) вероятность проникновения нарушителя по каждому маршруту оценивается с помощью синтеза двух взаимно связанных марковских цепей.

Для решения задачи оценки вероятности реализации угрозы проведем декомпозицию мультиграфа проникновения нарушителя. Определим все пути перемещений из начальной вершины Y_0 в конечную Y_{10}. Все варианты пути из одной смежной вершины в другую будем обозначать как дизъюнкцию логических переменных, которые являются весом каждого ребра, принятые за единицу в данной задаче. Например, перемещение из вершины Y_0 в вершину Y_1 будем обозначать $X_1 \vee X_2 \vee X_3$.

Пути из одной вершины в другую определяются с помощью операции композиции матрицы смежности мультиграфа. Чтобы найти пути из k ребер необходимо возвести матрицу смежности в степень k. При этом получим новую матрицу, в которой будут представлены все пути между событиями длиной от одного ребра до k ребер. Таким образом, в полученной логической функции проникнове-

ния параллельные маршруты будут представлены как дизъюнкции ребер, а последовательные как их конъюнкции. Также следует учесть, что умножаемые матрицы смежности содержат логические переменные. Из этого следует, что к результатам умножения ячеек можно применить операции алгебры логики для сокращения результата умножения [46, 123].

Используя данные теоретические предпосылки, определим все возможные пути из первого рубежа в последний, представленные как функция алгебры логики (ФАЛ) в виде конъюнкции весов ребер, по которым проходит путь. Для удобства операцию конъюнкции $X_1 \wedge X_2$ будем обозначать X_1X_2, а операцию дизъюнкции $X_1 \vee X_2$ будем обозначать X_1+X_2. Матрица смежности имеет вид (рисунок 6.5).

	1	2	3	4	5	6	7	8	9	10	11
1	1	×1+×2+×3	0	×9+×10	0	0	0	0	0	0	0
2	0	1	×4+×5	0	0	0	0	0	0	0	0
3	0	0	1	×6+×7+×8	0	0	0	0	0	0	0
4	0	0	0	1	×11	×12	×13	0	0	0	0
5	0	0	0	0	1	0	0	×14	×15	0	0
6	0	0	0	0	0	1	0	0	×16	×17	0
7	0	0	0	0	0	0	1	0	0	×18	0
8	0	0	0	0	0	0	0	1	0	0	×19
9	0	0	0	0	0	0	0	0	1	0	×20
10	0	0	0	0	0	0	0	0	0	1	×21
11	0	0	0	0	0	0	0	0	0	0	1

Рисунок 6.5 – Матрица смежности графа

Всего получили сто логических функций проникновения нарушителя, из которых десять длиной в четыре ребра, а девяносто длиной в шесть ребер. Полученные ФАЛ сведены в матрицу инцидентности (таблицу 6.3): строки в матрице – маршруты проникновения в виде логических функций, а столбцы – ребра графа между рубежами объекта, на которых расположены ИТСО СФЗ с характеристиками, представленными в таблице 6.4.

Таблица 6.3 – Матрица инцидентности

Номер функции проник	Номера ребер графа																				
	X_1	X_2	X_3	X_4	X_5	X_6	X_7	X_8	X_9	X_{10}	$\mathbf{X_{11}}$	X_{12}	$\mathbf{X_{13}}$	X_{14}	X_{15}	$\mathbf{X_{16}}$	$\mathbf{X_{17}}$	X_{18}	X_{19}	X_{20}	X_{21}
1									1		1			1					1		
…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…
100			1		1			1					1					1			1

Таблица 6.4 – Характеристики инженерно-технических средств охраны

Тип ИТСО	Расположение на графе проникновения	Р- обнаружения	Протяженность, м, номер покрытия	Удаление от КСИИ, м
CNB- WFL-21S	X_{11}, X_{16}, X_{17}, X_{13}	0,60	880 - 10	450
SCANALL	X_{12}, X_{14}, X_{15}, X_{18}	0,80	670 - 9	300

Элементы матрицы инцидентности в строке связаны конъюнктивно, а сами строки – дизъюнктивно. Полученные логические функции проникновения позволяют оценить вероятность проникновения и противодействия на каждом маршруте, то есть оценить эффективность СФЗ. В вероятностном смысле эффективность СФЗ будет определяться вероятностью не реализации ни одной из ста функций проникновения.

Вероятности обнаружения и перехвата (своевременного прибытия для нейтрализации) нарушителя обоснованы и заданы на предыдущих этапах проектирования СФЗ [111]. Определим требования к СФЗ: вероятность обнаружения нарушителя на каждом пути проникновения не менее ≥0,9; вероятность своевременного прибытия в точку пресечения сил реагирования на каждом пути не менее ≥0,8, т. е. вероятность безопасного состояния объекта не меньше $P_З \geq 0{,}72$.

На основе протяженности ребер графа на местности определим протяженность пути проникновения как их сумма в соответствии с таблицей 6.3: X_1 - 25 м; X_2 - 15 м; X_3 - 35 м; X_4 - 14м; X_5 - 24 м; X_6 - 20 м; X_7 - 15 м; X_8 - 24 м; X_9 и X_{10} - 13 м; X_{11} - перемещение между рубежами Y_3 - Y_4 – 450 м; X_{12} - перемещение между рубежами Y_3- Y_5 – 320 м; X_{13} - между рубежами Y_3- Y_6 – 220 м; X_{14} - между рубежами Y_4 - Y_7 – 180 м; X_{15} - между рубежами Y_4 - Y_8 – 50 м; X_{16}- между рубежами Y_5 - Y_8 – 160 м; X_{17} - между рубежами Y_5-Y_9 – 50 м; X_{18} - между рубежами Y_6 - Y_9 – 120 м; X_{19} - между рубежами Y_7 - Y_{10} – 60 м; X_{20} - между рубежами Y_8- Y_{10} – 70 м; X_{21} - между рубежами Y_9 - Y_{10} – 50 м. Расстояние от караула до КСИИ - 310 м.

Для решения задачи оценки вероятности проникновения нарушителя по порядку моделировались все пути проникновения нарушителя из матрицы инцидентности (таблица 6.3) в виде последовательных событий перемещения нарушителя между рубежами охраны и одновременно моделировалось противодействие

СФЗ как реакция на проникновение. Данная последовательность описывалась двумя простыми связанными марковскими цепями переходов событий.

Таким образом, произвели декомпозицию сложного графа проникновения на множество простых графов. На основе каждого маршрута моделировались два связанных процесса – проникновения нарушителя и противодействия СФЗ. Это является достоинством данного метода.

Сформированы две взаимно связанные марковские цепи. Первая – модель перемещения нарушителя, вторая – модель перемещения сил реагирования и нейтрализации нарушителя после его обнаружения. Обе модели описываются с помощью последовательного графа переходов событий. Модели взаимосвязаны и работают синхронно. Процесс движения x(t) считаем как поток независимых приращений расстояний с интенсивностью (скоростью) λ(t). Так как приращения на любом участке времени t, $t+\Delta t$ независимы, то процесс приращения расстояния при движении x(t) является процессом Пуассона с ограниченным числом состояний x(t)≤L, где L – расстояние от начального события в конечное [111]. Вероятности переходов между событиями за время Δt определяются по экспоненциальному закону исходя из значения величины скорости перемещения между рубежами охраны. Графы проникновения и противодействия представлены на рисунке 6.6.

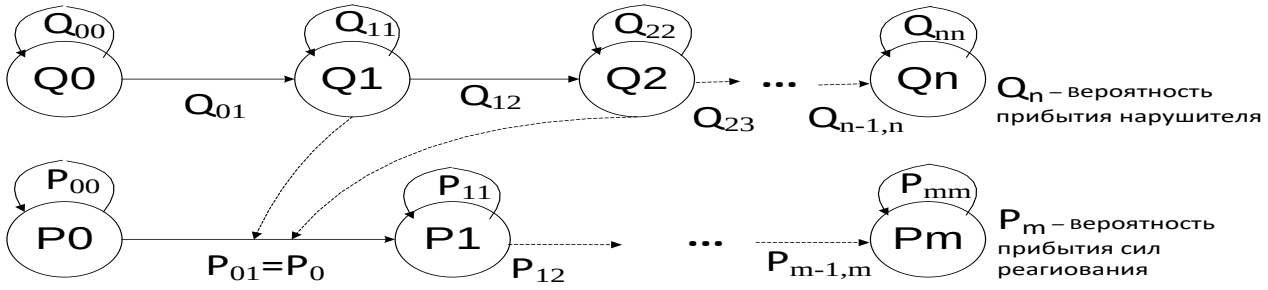


Рисунок 6.6 – Синхронизация графов проникновения и противодействия СФЗ

Вершины графов – рубежи перемещений нарушителя и сил реагирования и нейтрализации. Особенностью второго графа переходов является то, что он информационно связан с первым графом (на рисунке пунктирные ребра). Матрица вероятностей переходов изменяется динамически, в зависимости от вероятности состояния событий Q1 и Q2 модели движения нарушителя. Марковская модель

реакции на проникновение нарушителя группой нейтрализации не стационарна – матрица вероятности переходов меняется. По мере перемещения нарушителя вероятность состояний Q1 и Q2 увеличивается и, следовательно, увеличивается вероятность обнаружения. То есть из состояний Q1 и Q2, где находятся средства технического контроля, информация передается в ребро 0 - 1 на второй марковский граф в виде величины вероятности обнаружения, то есть содержание матрицы переходов вероятностей динамически изменяется. Эта информация в виде возрастающей вероятности передается во второй граф (матрицу переходов), и, следовательно, вероятность начала перемещения сил реагирования увеличивается. Во второй модели графа сил реагирования переход из нулевого состояния в первое состояние – это и есть вероятность обнаружения нарушителя ТСО в виде логической связи. Таким образом, движение сил реагирования начинается с первого события при получении информации (обнаружении нарушителя) с двух рубежей расположения технических средств обнаружения. Последние вершины обоих графов имеют одно и то же физическое положение на местности – КСИИ.

Величина вероятности перехода из нулевого события в первое (вероятность обнаружения) определяется по формуле умножения вероятностей последовательных событий, так как нарушитель последовательно пересекает рубежи, на которых расположены ТСО. Результирующее действие оценивает вероятность перехода на графе из нулевого события в первое, как произведение вероятностей не обнаружения на каждом рубеже:

$$P_{01} = 1 - \left[\left(1 - P^1_{mco} \cdot Q_1\right) \cdot \left(1 - P^2_{mco} \cdot Q_2\right) \right], \qquad (6.6)$$

где P^1_{mco}, P^2_{mco} вероятности обнаружения ТСО, расположенных на графе в вершинах событий Q_1 и Q_2 соответственно;

Q_1, Q_2 – вероятности нахождения нарушителя в зоне обнаружения ТСО на рубежах вершин графа один и два соответственно.

Функционирование графов синхронизировано по времени с шагом продолжительности $\Delta t = 1c$. В результате моделирования определялись значения вероятности обнаружения, которые передавались во вторую модель противодействия.

Во второй модели на графе с помощью марковской цепи определяется вероятность своевременного прибытия сил реагирования, т. е. вероятность наступления события два (2).

Выходными значениями марковских цепей являются вероятности наступления конечных событий, т.е. реализация целей нарушителя и сил реагирования. По соотношению вероятностей конечных событий можно сделать вывод о величине безопасного состояния объекта [120, 121, 123].

Процесс моделирования автоматизирован при помощи программы на языке программирования C#, свидетельство о государственной регистрации № 2016661765 [124]. Исходные данные представлены в виде характеристик: протяженности и скорости перемещения нарушителя в соответствующих зонах охраны объекта. Результаты решения и динамика изменения вероятности состояний конечных событий представлены рисунками 6.7, 6.8.

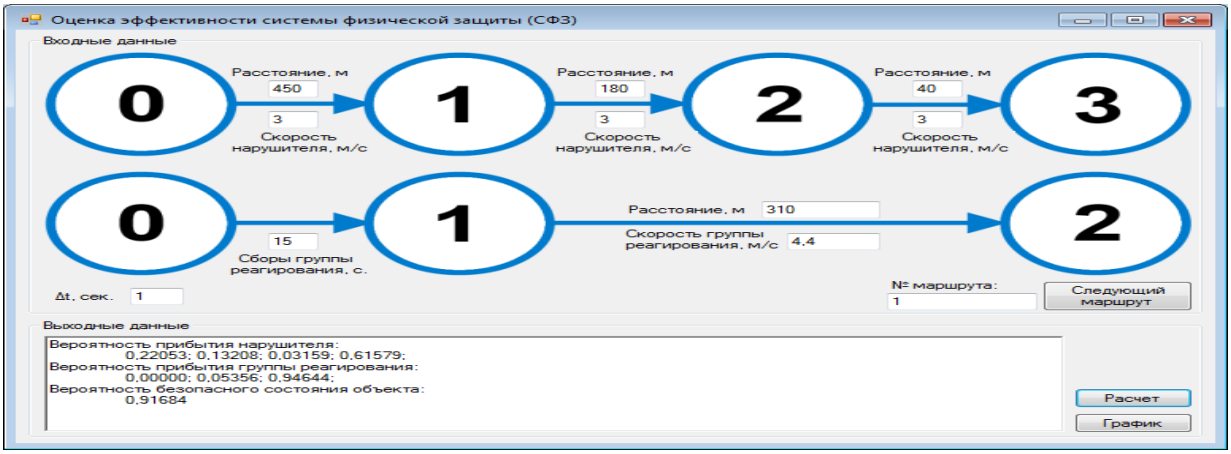


Рисунок 6.7 – Входные данные и результаты вычислений

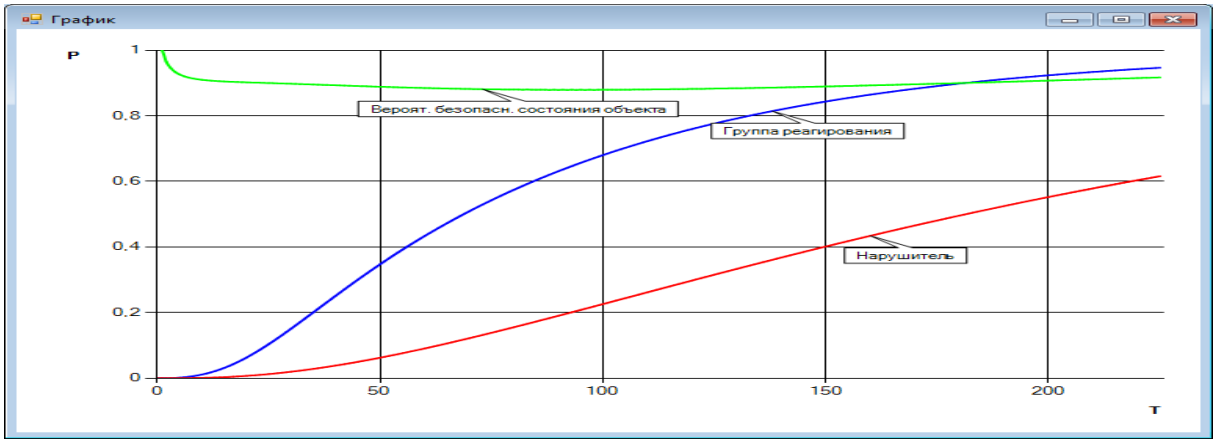


Рисунок 6.8 – Динамика изменения вероятности конечных событий

Достоверность результатов определяется корректностью задаваемых исходных данных, которые определяются путем экспертных оценок и согласовываются с экспериментальными данными [120, 121]. На основе входных данных формируется матрица вероятностей переходов. Данные вероятности определяются расчетным путем как элемент вероятности: $\Delta P_{ij} = \lambda_{ij} \cdot \Delta t$, где λ_{ij} интенсивность (скорость) движения нарушителя между рубежами и сил реагирования к месту расположения объекта информатизации.

Оценка вероятности нахождения объекта в безопасном состоянии по вероятностям двух конечных событий определяется по формуле гипотез. Оценивается первая гипотеза, что силы реагирования опередят нарушителя, и вторая гипотеза, что нарушитель опередит силы реагирования. Условная вероятность появления первой гипотезы определялась по формуле [120 стр. 64]:

$$P(H1/A) = PH1/(PH1 + PH2), \quad (6.7)$$

где $PH_1 = P_m \cdot (1 - Q_n)$ – вероятность первой гипотезы;

$PH_2 = (1 - P_m) \cdot Q_n$ – вероятность второй гипотезы;

P_m, Q_n – вероятности прибытия к месту развертывания сил реагирования и нарушителя соответственно.

Данная задача решается для каждого из ста маршрутов проникновения матрицы инцидентности (таблица 6.3). В результате анализа всех путей проникновения с учетом расположения ТСО получили матрицу инцидентности всего пять уникальных функций проникновения без путей до границы объекта (таблица 6.5)

Таблица 6.5 – Инцидентности уникальных маршрутов в границах объекта

№ функции проникновения	Номер ребра графа										
	X_{11}	X_{12}	X_{13}	X_{14}	X_{15}	X_{16}	X_{17}	X_{18}	X_{19}	X_{20}	X_{21}
1	1			1					1		
2	1				1					1	
3		1				1				1	
4		1					1				1
5			1					1			1

Результаты вычислений вероятностей безопасного состояния сведены в таблицу 6.6. Анализ результатов таблицы 6.6 показывает, что требования к эффек-

тивности СФЗ выполнены [113, 116]. Программное средство адекватно реагирует на вводимые изменения в структуру модели, что говорит о чувствительности модели к входным данным.

Таблица 6.6 – Результаты моделирования марковских процессов

№ функции проникновения	Вероятность прибытия сил реагирования PH_1	Вероятность прибытия нарушителя PH_2	Вероятность безопасного состояния объекта $P(H1/A)$
1	0,951	0,615	0,924
2	0,912	0,633	0,857
3	0,912	0,608	0,870
4	0,837	0,635	0,747
5	0,815	0,612	0,736

Таким образом, разработанный метод на основе синтеза марковских цепей позволяет оценить эффективность функционирования СФЗ. Применение разработанного математического аппарата автоматизировано. Программное средство адекватно реагирует на вводимые изменения в структуру модели, что говорит о чувствительности модели к входным данным. Результатами моделирования являются вероятности безопасного состояния КСИИ при попытке нарушителя проникнуть на объект по каждому маршруту. Каждый путь проникновения обеспечивает безопасное состояние объекта на уровне не меньше заданных требований.

6.3 Модернизация структуры системы физической защиты критически важных объектов на основе выбора эффективных решений

Постановка задачи. Разработать метод повышения эффективности СФЗ (оценки вариантов структуры размещения инженерно-технических средств охраны) на основе градиентного движения по функции отклика эффективности, полученной моделированием функционирования СФЗ марковскими цепями. Для решения этой задачи необходимо провести эксперимент на марковской модели, получить функцию эффективности от параметров структуры СФЗ, на основе которой осуществляется принятие оптимального решения по изменению структуры СФЗ для повышения эффективности.

Решение задачи. Допустим, при анализе результатов таблицы 6.6 требования к эффективности СФЗ по маршруту пять не выполнены.

Модернизацию СФЗ за счет повышения вероятности обнаружения считаем нецелесообразной по экономическим соображениям (обеспечение стандартизации и унификации средств обнаружения). Поэтому повышение эффективности СФЗ рассмотрим только за счет частного показателя – вероятности своевременного прибытия сил реагирования. Для этого можно произвести следующие структурные изменения СФЗ (факторы):

- увеличить расстояние *L(Po)* обнаружения между точкой обнаружения движения нарушителя и элементом защиты объекта за счет переноса средств обнаружения в сторону внешнего периметра. Первый фактор;

- уменьшить скорость (увеличить время) движения нарушителя за счет введения и модернизации заградительных средств *Vo.* Второй фактор;

- уменьшить расстояние движения сил реагирования за счет создания коротких путей перемещения *Lo.* Третий фактор;

- увеличить скорость движения сил реагирования по территории объекта за счет использования подвижных средств. Четвертый фактор.

Последний фактор в наших условиях не может быть реализован в силу особенностей объекта охраны, поэтому будем рассматривать первые три фактора.

Любые изменения структуры СФЗ связаны с затратами, поэтому рассматривалось соотношение эффективности и затрат для каждого фактора (рисунок 6.9).

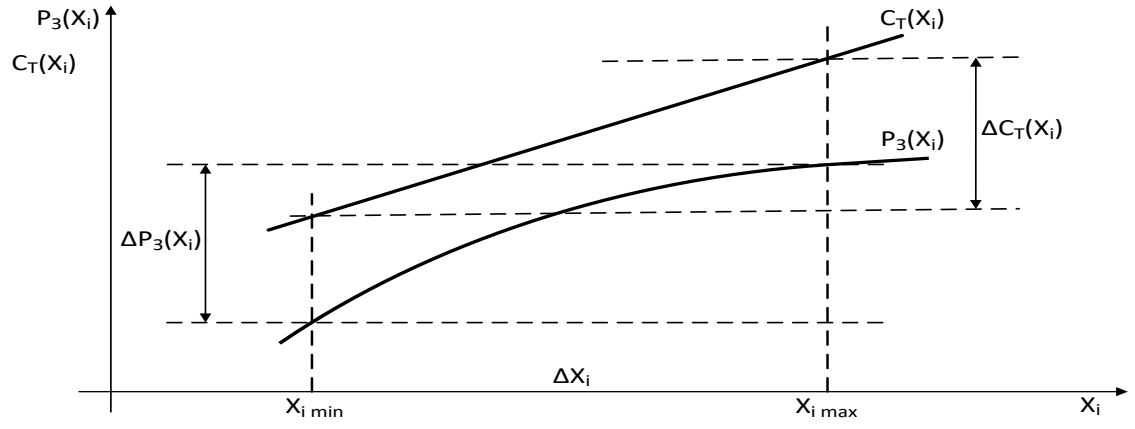


Рисунок 6.9 – Изменение эффективности и затрат реализации при структурных изменениях СФЗ (*Xi* - факторов)

В этой связи воспользуемся функцией отношения эффективности к стоимости. Для получения функции регрессии «эффективность/стоимость» СФЗ формировалась полная матрица планирования эксперимента (таблица 6.7), в которой x_1, x_2, x_3 – соответствующие факторы *L(Po), Vo, Lo* [11].

Уравнение регрессии имеет вид:

$$\overline{y} = b_0 x_0 + b_1 x_1 + b_2 x_2 + b_3 x_3 .$$

По коэффициентам функции можно определить направление изменения определяющего фактора для увеличения функции «эффективность/стоимость» до граничного значения параметра области варьирования, так как функция определена только в области варьирования параметров.

Таблица 6.7 – Матрица планирования эксперимента

№ опыта	Кодированные входные факторы				Эффективность ($P_З$)/затраты (%)		
	X_0	X_1	X_2	X_3			
1	+	-	-	-	0,646/7,5	0,646/7,6	0,646/7,7
2	+	+	-	-	0,704/9,5	0,704/9,6	0,704/9,7
3	+	-	+	-	0,709/8,5	0,709/8,6	0,709/8,7
4	+	+	+	-	0,749/10,5	0,749/10,6	0,749/10,7
5	+	-	-	+	0,816/10,5	0,816/10,6	0,816/10,7
6	+	+	-	+	0,849/12,5	0,849/12,6	0,849/12,7
7	+	-	+	+	0,883/11,5	0,883/11,6	0,883/11,7
8	+	+	+	+	0,961/13,5	0,961/13,6	0,961/13,7

Методически данная задача решается следующим образом:

1) определяется фактор с наибольшим коэффициентом функции «эффективность/стоимость», и точка центра плана эксперимента перемещается в направлении этого фактора на границу области определения. Оценивается эффективность СФЗ в данной точке – если удовлетворяет требованиям, то процесс заканчивается. В противном случае переходят к пункту 2.

2) в данной точке вновь строится план проведения эксперимента и производится моделирование для получения нового уравнения регрессии – функции «эффективность/стоимость» СФЗ и переходят к пункту 1.

Операция 1 и 2 повторяется до тех пор, пока требования к СФЗ будут выполнены. Это и будет оптимальное значение параметров структуры СФЗ.

Для проведения эксперимента использовалась марковская цепь, описывающая функционирование СФЗ, представленная в п. 6.2.

Входные данные: нижний уровень параметров: *L(Po)=220 м, 90 м, 50 м, Vo=3 м/с, Lo=310 м*; верхний уровень параметров: *L(Po)=200 м, 110 м, 70 м, Vo=2,7 м/с, Lo=210 м*. Центр плана: *L(Po)=210 м, 100 м, 60 м, Vo=2,85 м/с, Lo=260 м.* Этим изменениям факторов соответствует увеличение затрат на СФЗ как процент величины стоимости объекта охраны. Увеличение в процентах составило соответственно 2 %, 1 %, 3 %. Затраты определялись по примерным сметам расходов экспертным путем. После моделирования в каждой точке плана получили данные увеличения эффективности СФЗ, ее отношение к затратам на реализацию фактора и будет целевой функцией исследования.

Результаты моделирования представлены в таблице 6.7.

Для оценки однородности дисперсий определялось расчетное значения G-критерия Кохрена:

$$G = \frac{S^2_{j\,\max}}{\sum_{j=1}^{N} S^2_j} = 0{,}15806.$$

Критическое значение G-критерия для уровня значимости α=0,05; числа степеней свободы f = l - 1 = 2 и числа суммируемых оценок, равного N:

$$G_{табл}(\alpha = 0{,}05;\ N = 8;\ f = 3-1) = 0{,}5127.$$

Расчетное значение меньше табличного значения - гипотеза об однородности ряда выборочных дисперсий выходного параметра не отвергается. В качестве оценки дисперсии воспроизводимости эксперимента определим среднюю дисперсию:

$$S^2_{воспр} = \frac{\sum_{j=1}^{N} S^2_j}{N} = 0{,}0343; \qquad f_{воспр} = N(l-1) = 16,$$

где l — число опытов в каждой точке плана.

Предпосылки регрессионного анализа выполняются, приступим к расчету коэффициентов уравнения регрессии:

$$b_i = \frac{1}{N}\sum_{j=1}^{N} x_{ji}\,\overline{y}_{iэ}.$$

Уравнение приближенной регрессии имеет вид:

$$\overline{y} = 0,07538 - 0,004754\ L(Po) - 0,00029\ Vo - 0,00251\ Lo.$$

Отрицательные знаки при коэффициентах уравнения регрессии свидетельствуют, что затраты на структурные изменения растут быстрее, чем эффективность СФЗ. Для проверки адекватности уравнения регрессии определим расчетное значение *F*-критерия:

$$F_{расч.S} = \frac{S^2_{ад}}{S^2_{воспр}};\ S^2_{воспр} = 0,0343;\ f_{воспр} = 16;\quad S^2_{ад} = \frac{l\sum_{j=1}^{N}(\overline{y}_{jэ} - \overline{y}_j)^2}{N - h},$$

где $h -$ количество коэффициентов в уравнении.

Определим значения оценок выходного параметра $\overline{y}_j$ по результатам вычислений с использованием полученного уравнения регрессии. Определяем оценку дисперсии адекватности: $S^2_{ад} = 0,0144.$

Определяем расчетное значение *F*-критерия: $F_{расч} = \frac{S^2_{ад}}{S^2_{воспр}} = 0,4219.$

Для проверки гипотезы об адекватности уравнения определяем из таблицы критическое значение *F*-критерия для значимости α =0,05 и степеней свободы числителя: $f_1 = N - h = 4$ и знаменателя f_2 = 16; $F_{табл} = 4,68.$

Соизмеряем расчетное и табличное значения *F* - критерия:

$$F_{расч} = 0,4219 < F_{табл} = 4,68.$$

Уравнение приближенной регрессии адекватно описывает исследуемый процесс, то есть модель согласуется с полученными данными моделирования.

Определим наибольший коэффициент показателя «эффективность/стоимость» СФЗ. Для этого будем варьировать входным параметром модели *Vo* в сторону увеличения эффективности до границы области определения функции:

$$\overline{y} = 0,07538 - 0,004754\,L(Po) - 0,00029\,Vo\uparrow - 0,00251\,Lo, \qquad (6.8)$$

то есть центр плана эксперимента будем смещать в сторону увеличения функции эффективности и получать новые уравнения для очередной области определения. В таблице 6.7 точка опыта № 3 показывает, что показатель эффективности выполняется с наименьшими затратами.

Таким образом, после одной итерации моделирования получили уравнение регрессии - структурные параметры СФЗ, при которых выполняются требования к СФЗ. Из этого следует, что достигли оптимальных параметров функции оценки эффективность/стоимость путем установки дополнительных заградительных средств задержки нарушителя, уменьшающих его скорость перемещения до *Vo=2,7 м/с*.

Таким образом, разработанный метод позволяет принимать оптимальное решение по структурной модернизации СФЗ, направленное на повышение ее эффективности. Результаты моделирования – предложения по изменению структуры СФЗ. Недостаток метода – достоверность результатов определяется корректностью задаваемых входных данных, которые определяются экспертным путем и согласовываются с экспериментальными данными натурного эксперимента. Кроме того, экспертные оценки увеличения сметной стоимости затрат на структурные изменения в СФЗ являются приближенными и носят субъективный характер.

6.4 Метод оценки времени утечки информации о системе физической защиты критически важных объектов

Главная особенность КСИИ КВО – наличие специализированных АСУ функционированием объекта. Это определяет задачу их защиты от дестабилизирующих воздействий как внутренних, так и внешних, и в первую очередь защиту от утечки информации об организации и порядке функционирования СФЗ [64, 66].

В сфере информационной безопасности основными рисками считаются внешние угрозы. Однако исследования аналитического центра ЗАО InfoWatch (Россия) [129] показали, что до 80 % утечек информации происходит за счет не-

соблюдения сотрудниками компании режима обеспечения конфиденциальности. В настоящее время этот режим обеспечивается в основном комплексом организационно-правовых мер. Однако анализ вопросов, касающихся количественной оценки утечки информации и соответственно инструментальных средств ее анализа и контроля, раскрыт не в полной мере.

В разделе рассмотрен метод оценки времени утечки информации, имеющий сходство с оценкой утечки электрической энергии во время переходных процессов в электрической цепи. Расчет переходных процессов электрических цепей является одной из частых задач, решаемых в рамках теоретических основ электротехники. Используемые в теоретических основах электротехники величины сопоставляются с понятиями защиты информации, а именно: величина заряда емкости соответствует количеству определенного вида информации; время заряда емкости – времени накопления информации; величина электродвижущей силы – максимально возможному количеству информации, под которым понимается первоначальные знания об организации и порядке функционирования СФЗ.

Достоинство метода – замещение графовой модели утечки информации эквивалентной электрической схеме с переходными процессами.

Постановка задачи. Информационный показатель защищенности КВО опишем в виде критерия: – $I_{СФЗ}(t) \rightarrow \min$ – информация о функционировании системы физической защиты стремится к минимуму. На рисунке 6.10 показана графическая интерпретация информационной постановки задачи оптимизации в общем виде.

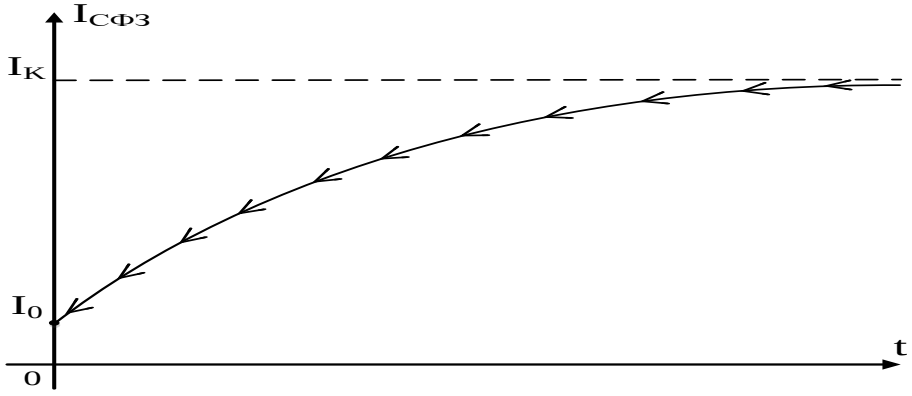


Рисунок 6.10 – Графическая интерпретация информационной постановки задачи оптимизации в общем виде

На основе анализа информационной деятельности исполнителей технологических процессов на объекте необходимо произвести оценку временно́го интервала утечки информации о СФЗ как количественную меру наступления момента однородности информированности исполнителей и на этой основе выработать оптимальную (рациональную) политику организационных мер по уменьшению утечки информации о СФЗ, т.е. сформировать политику безопасности.

Формирование входных данных. В качестве примера рассмотрим модельный объект, структура которого полностью соответствует реальному объекту. Для анализа информационных процессов, происходящих на КВО, представим информационное поле в виде двухмерной матрицы (таблица 6.8).

Таблица 6.8 – Информационное поле в виде двухмерной матрицы

Код ДЭ	Код типа информации											
	101	201	102	202	103	301	302	503	500	401	501	502
10	6	3	6	2	6	2	1	2	1	2	1	1
20	3	6	2	6	6	2	1	2	1	2	1	1
30	3	2	1	1	3	6	6	2	1	2	1	1
11	5	2	6	2	5	2	1	1	1	2	1	1
21	3	6	1	5	4	4	3	1	1	2	1	1
31	3	2	1	1	3	6	6	1	1	2	1	1
22	1	2	1	2	2	2	2	1	1	1	0	1
23	1	2	0	1	1	1	1	1	1	1	0	1
81	1	1	2	1	1	1	1	1	1	1	1	1
61	2	2	1	2	2	2	1	1	0	1	1	1
71	1	1	1	1	2	1	1	1	2	1	1	1
70	2	1	2	1	3	2	1	1	2	2	2	1
50	1	1	1	1	2	1	1	6	6	5	6	6
51	1	1	1	1	1	3	1	6	4	3	3	3
52	1	1	1	2	1	1	1	3	4	3	6	6
53	1	1	1	1	1	1	1	3	3	3	3	6
54	0	1	0	0	0	0	0	2	3	2	6	4
40	1	1	0	0	2	1	0	3	3	6	3	4

Один вход матрицы (столбцы) – тип информации (содержание), другой (строки) – исполнители, т.е. носители данной информации, которыми могут быть специалисты различных уровней специализации. Назовем строки – коды действующих элементов (ДЭ), а столбцы – коды типа информации.

На пересечении столбцов и строк в поле матрицы определяется уровень владения содержанием информации о КВО, которое задается экспертно на осно-

вании инструкций о должностных обязанностях по следующей шкале: 6 – анализирует и работает с информацией; 4 – просто владеет информацией; 2 – имеет представление об информации; 0 – не владеет информацией; 5, 3, 1 – промежуточные значения. Данная шкала определена по аналогии со шкалой Саати [118].

Для удобства работы с информационной матрицей ДЭ и им соответствующие типы информации закодированы следующим образом: при кодировании ДЭ использовались двузначные номера, при кодировании типов информации – трехзначные. Первая цифра во всех кодах означает принадлежность к родовому типу информации. Вторая цифра для ДЭ – порядковый номер важности исполнителя, связанный с данным типом информации – первой цифрой. Вторая цифра в коде типа – информации ноль, а третья детализирует и уточняет родовую информацию. Рассмотрим пример для первой цифры 3 (выделено шрифтом, таблица 6.8) – информации о «специальной части» изделия. Код ДЭ: 30 – руководитель работ по оценке качества «специальной части» изделия; 31 – исполнитель работ по оценке качества «специальной части» изделия; код типа информации: 301 – информация о разработчике «специальной части» изделия; 302 – результаты оценки качества «специальной части» изделия.

СФЗ объекта позволяет исключить утечку конфиденциальной информации о разработке и характеристиках «специальной части» изделия путем несанкционированного доступа нарушителей. Для эффективного решения данной задачи СФЗ должна уменьшить утечку информации о технических средствах защиты и порядке доступа к элементам объекта и т.д.

В рассматриваемом примере СФЗ обеспечивает защиту типа информации с кодовыми номерами 301, 302 (конфиденциальная информация). Прямыми носителями данной информации являются ДЭ с кодовыми номерами 30, 31. Информация о СФЗ, характеристиках типовых средств защиты, режимах доступа и пропускном режиме заключена в кодах информации 503, 500, 401, 501, 502, а ее носителями являются соответственно кодовые номера ДЭ 50, 51, 52, 53, 54, 40.

Формирование структуры связей информации. Обработав данную матрицу МГК (при решении задачи использован стандартный пакет прикладных программ

(ППП) Statistica 6.0), получим объединение типов информации в ортогональные компоненты – такой процесс называется структурированием [77]. В таблице 6.9 показаны связи компонент после варимаксного вращения, где в столбцах представлены четыре значимые компоненты F1 – F4, в которых сосредоточено 90 % информационной нагрузки. Определим, как объединяются коды 301, 302 с кодами 503, 500, 401, 501, 502.

Проведем анализ результатов. В первой компоненте F1 – информация о функционировании СФЗ (код 500) как базовый параметр связана со следующими сведениями: режим доступа к объекту информатизации; время несение смен; характеристики технических средств защиты. Следовательно, через них есть риск утечки информации о функционировании СФЗ.

Таблица 6.9 – Связи компонент после варимаксного вращения

Код типа информации	Компоненты типов информации			
	F1 – 500, 503, 501, 502, 401	F2 – 102, 101, 103	F3 – 302, 301	F4 – 202, 201
101	**0,198**	0,892	**–0,267**	**0,263**
201	**0,225**	**0,174**	**–0,154**	0,917
102	**0,129**	*0,956*	**0,125**	**0,044**
202	**0,094**	**0,196**	**–0,029**	*0,922*
103	**0,212**	0,729	**–0,141**	**0,543**
301	**0,173**	**0,109**	–0,949	**0,136**
302	**0,168**	**0,012**	*–0,953*	**0,045**
503	–0,895	**–0,075**	**0,034**	**–0,075**
500	*–0,907*	**–0,229**	**0,210**	**–0,209**
401	–0,795	**–0,011**	**0,052**	**–0,071**
501	–0,805	**–0,209**	**0,240**	**–0,163**
502	–0,831	**–0,249**	**0,236**	**–0,171**

Вторая компонента F2 объединила типы информации 102, 101, 103; F3 – 302, 301; F4 – 201, 201. Таким образом, конфиденциальная информация 301, 302 находится только в третьей компоненте F3, что исключает ее функциональное представление через другие типы информации, т. е. риск утечки конфиденциальной информации через другие типы информации минимален.

В таблице 6.10 представим транспонированную двухмерную матрицу таблицы 6.8 и аналогичный образом проведем анализ информационной связи действующих элементов.

Таблица 6.10 – Транспонированная двухмерная матрица

Код типа информации	Код ДЭ																	
	10	20	30	11	21	31	22	23	81	61	71	70	50	51	52	53	54	40
101	6	3	3	5	3	3	1	1	1	2	1	2	1	1	1	1	0	1
201	3	6	2	2	6	2	2	2	1	2	1	1	1	1	1	1	1	1
102	6	2	1	6	1	1	1	0	2	1	1	2	1	1	1	1	0	0
202	2	6	1	2	5	1	2	0	1	2	1	1	1	1	2	1	0	0
103	6	6	3	5	4	3	2	1	1	2	2	3	2	1	1	1	0	2
301	2	2	6	2	4	6	2	1	1	2	1	2	1	3	1	1	0	1
302	1	1	6	1	3	6	2	1	1	1	1	1	1	1	1	1	0	0
503	2	2	2	1	1	1	1	1	1	1	1	1	6	6	3	3	2	3
500	1	1	1	1	1	1	1	1	1	0	2	2	6	4	4	3	3	3
401	2	2	2	2	2	2	1	1	1	1	1	2	5	3	3	3	2	6
501	1	1	1	1	1	1	0	0	1	1	1	2	6	3	6	3	6	3
502	1	1	1	1	1	1	1	1	1	1	1	1	6	3	6	6	4	4

Обработав данную информационную матрицу МГК, получим объединение ДЭ в ортогональные компоненты по информационному признаку. Получим шесть значимых компонент, содержащих более 95 % информационной нагрузки, т. е. ДЭ структурно классифицировались в шесть компонент F1 – F6 (таблица 6.11).

Таблица 6.11 – Связи компонент ДЭ

Код ДЭ	Компоненты ДЭ					
	F1 - 30, 31, 23	**F2- 10, 11, 81,**52	**F3 - 71, 70**	**F4- 20, 21, 22, 61,** 50, 51	F5 – 54	F6 – 53, 40
10	0,022	**–0,917**	0,114	0,223	0,032	0,106
20	0,182	–0,215	0,094	**0,874**	0,168	0,091
30	**–0,951**	0,031	–0,032	0,079	0,081	0,121
11	0,024	**–0,940**	0,113	0,123	0,044	0,145
21	–0,253	0,012	–0,071	**0,902**	0,106	0,163
31	**–0,952**	0,013	–0,001	0,104	0,046	0,127
22	–0,436	0,039	0,072	**0,619**	0,522	0,215
23	**–0,534**	–0,005	0,277	0,438	0,116	–0,312
81	0,234	**–0,594**	–0,138	–0,368	0,166	0,348
61	–0,215	–0,248	0,053	**0,854**	–0,062	0,146
71	0,069	–0,052	**0,867**	0,057	0,089	–0,052
70	–0,126	–0,535	**0,656**	–0,035	–0,266	–0,158
50	0,396	0,4216	0,184	**–0,496**	–0,184	–0,491
51	0,124	0,405	0,055	**–0,421**	–0,031	–0,336
52	0,451	**0,482**	0,034	–0,417	–0,382	–0,336
53	0,3429	0,379	–0,053	–0,436	–0,098	**–0,539**
54	0,404	0,454	0,054	–0,393	**–0,532**	–0,314
40	0,207	0,221	0,137	–0,281	–0,135	**–0,798**

В компонентах F2 и F4 ДЭ (F2 – 52, F4 – 50, 51) имеют противоположные знаки связи (выделено шрифтом), поэтому получаем восемь категорий ДЭ. В первой компоненте объединились ДЭ 30, 31, обладающие конфиденциальной инфор-

мацией 301, 302 и ДЭ 23 (обладает информацией с кодом 201 – характеристики изделия №2). Поэтому утечка информации может произойти в компоненте F1 через ДЭ 23, который неявно связан с ДЭ 30, 31. F2 объединяет ДЭ 10, 11, 81, 52; F3 – 71, 70; F4 – 20, 21, 22, 61, 50, 51, F5 – 54; F6 – 53, 40. Таким образом, ДЭ 50, 51, 52, 53, 54, 40, связанные с функционированием СФЗ, объединились с другими разнородными ДЭ в разных компонентах, т. е. возникает риск утечки информации о СФЗ через ДЭ в данных компонентах.

Формирование структуры исполнителей и информации. Результаты анализа таблиц 6.9, 6.11 представим в виде двудольного графа связей ДЭ и типов информации (графа Кенига) на рисунке 6.11, где коды заменены на действительные названия исполнителей и типов информации.

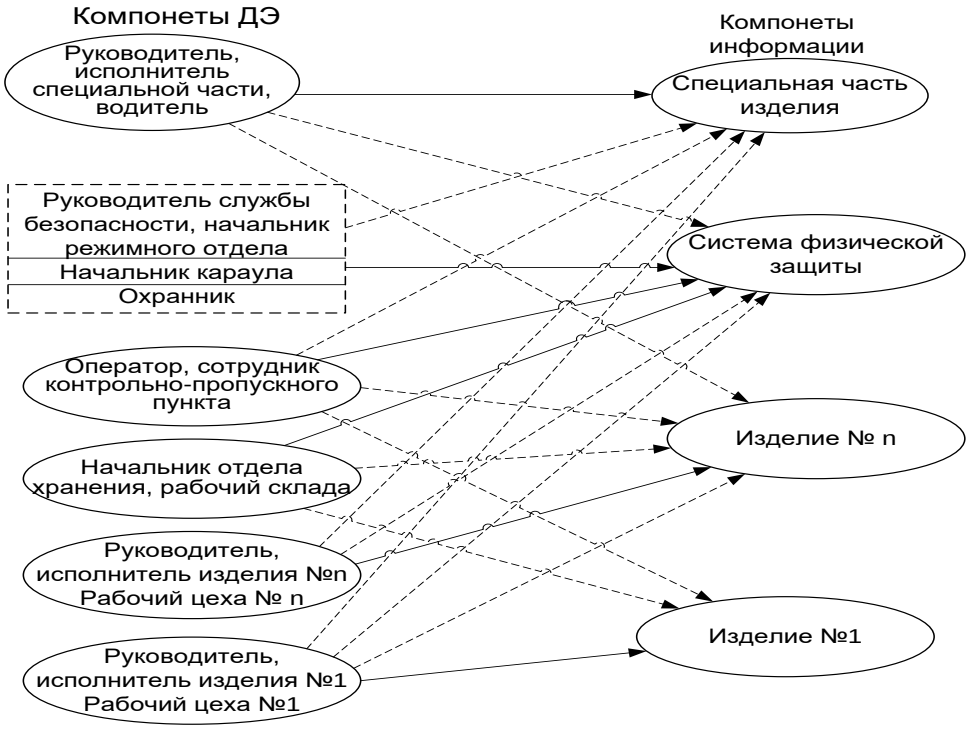


Рисунок 6.11 – Двудольный граф связей ДЭ и типов информации

Нас интересует в двудольном графе утечка информации о системе физической защиты как результат взаимодействия действующих элементов в компонентах при выполнении технологических процессов производства и своих функциональных обязанностей. На основе анализа двудольного графа и технологических

процессов функционирования организации построим граф утечки информации о системе защиты (рисунок 6.12).

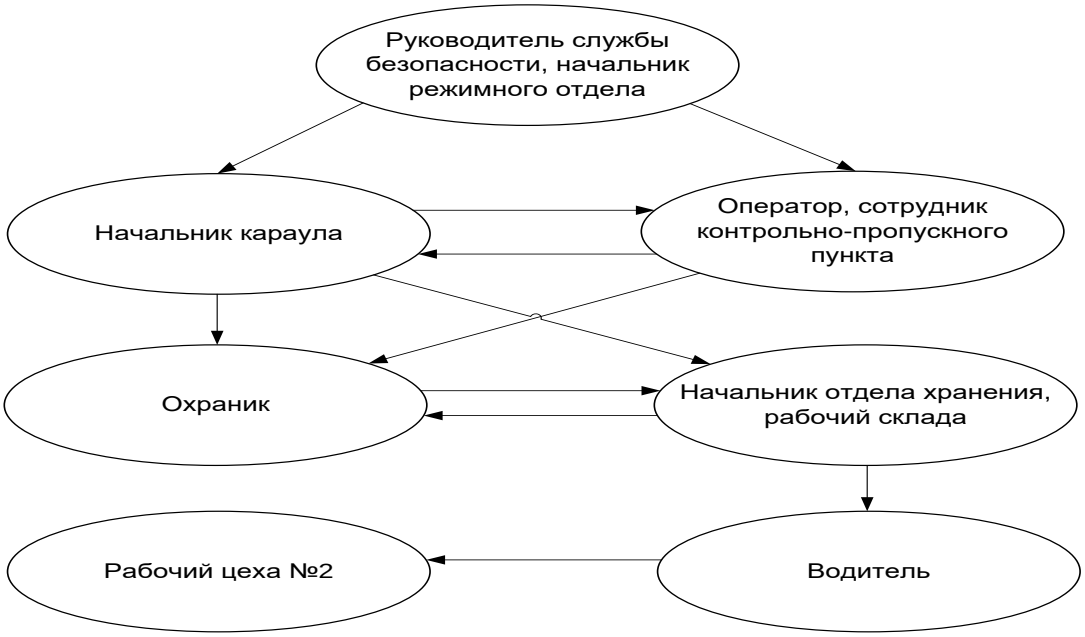


Рисунок 6.12 – Граф утечки информации о СФЗ

Временно́й интервал утечки информации (обмена информацией) между ДЭ на графе в результате их взаимодействия при выполнении технологических процессов определяется экспериментальным или экспертным путем. К полученному графу приведем соответствующую эквивалентную электрическую схему переходных процессов с *RC* цепями (рисунок 6.13).

На схеме установлено следующее соответствие графу утечки информации (рисунок 6.13): вершины графа – накопительные емкости *C*, ребра графа – резистивные сопротивления *R*.

Начальный заряд каждой емкости (В) – уровень владения содержанием информации о СФЗ по шестибалльной шкале (таблица 6.8), но в единицах напряжения (таблица 6.12). Величина сопротивления и емкости характеризует скорость обмена (утечки) информации между вершинами графа и определяет длительность переходного процесса $\tau = R \cdot C$ – время заряда емкости до 63 % приложенного напряжения. Заряд емкости ассоциируется с накоплением конфиденциальной информации в графе. Определим параметры *R* и *C* для переходного электрического процесса соответствующего аналогичного – утечки информации.

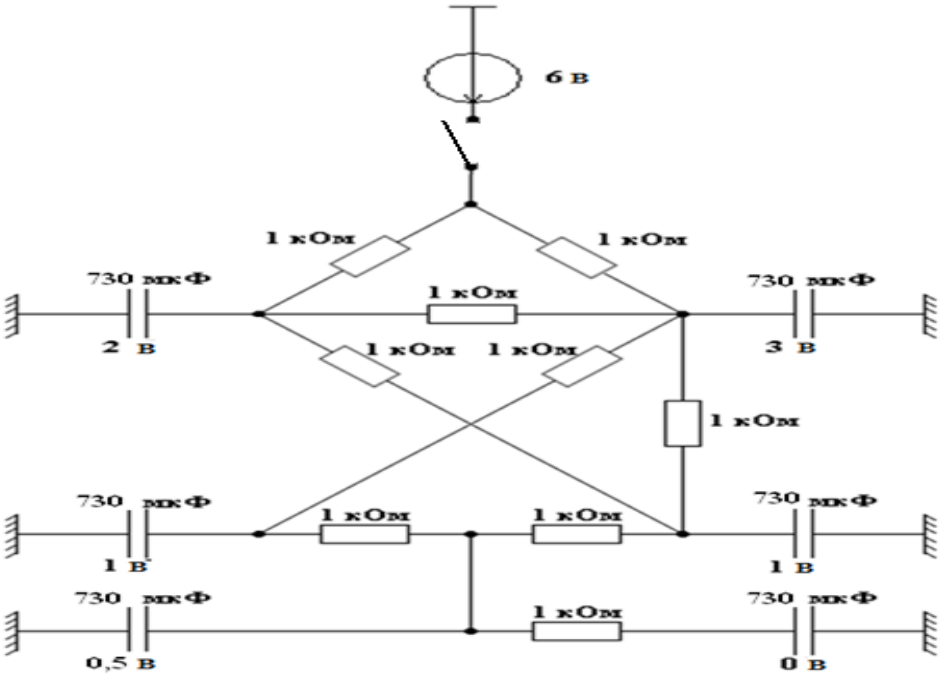


Рисунок 6.13 – Эквивалентная электрическая схема переходных процессов

Из-за отсутствия априорных сведений о скорости утечки нет оснований полагать, что скорости обмена информацией между вершинами графа будут разными – поэтому в схеме параметры емкостных и резистивных сопротивлений одинаковы. Время утечки информации на графе при взаимодействии ДЭ определим – 365 дней. При переходе к электрической схеме необходимо время утечки информации оценить в секундах, поэтому проведем масштабирование: 1 день – 0,01 с, следовательно, 365 дней – 3,65 с. Время полного заряда емкости составляет $5 \cdot \tau$, т.е. $5 \cdot \tau = 3{,}65$, поэтому $\tau = 0{,}730$ с. Для такой длительности переходного процесса сопротивление будет $R = 1$ кОм, а емкость – С = 730 мкФ.

При моделировании переходного процесса с помощью ППП *Proteus* 8.0 получена динамика заряда конденсаторов как аналог накопления информации (т.е. утечки информации) о СФЗ объекта информатизации. Результаты моделирования переходных процессов на электрической схеме показаны в таблице 6.12.

Время утечки информации о системе защиты определяется в момент наступления однородности в информационной системе, т. е. данная ситуация соответствует однородным параметрам информированности ДЭ в графовой модели (принадлежность к одной генеральной совокупности).

Таблица 6.12 – Результаты моделирования переходных процессов на электрической схеме

Коды ДЭ	Начальные условия B	Время переходного процесса, с													
		0,5	1	1,5	2	2,5	3	3,5	4	4,5	5	5,5	6	6,5	7
Руководитель службы безопасности, начальник режимного отдела	**6**	**6**	**6**	**6**	**6**	**6**	**6**	**6**	**6**	**6**	**6**	**6**	**6**	**6**	**6**
Начальник караула	**3**	**3,1**	**3,5**	**3,9**	**4,3**	**4,5**	**4,8**	**4,9**	**5,0**	**5,2**	**5,3**	**5,4**	**5,5**	**5,6**	**5,7**
Оператор, сотрудник контрольно-пропускного пункта	**2**	**2,9**	**3,4**	**3,8**	**4,2**	**4,5**	**4,7**	**4,9**	**5,0**	**5,2**	**5,3**	**5,4**	**5,5**	**5,6**	**5,7**
Охранник	**1**	**2**	**2,9**	**3,4**	**3,8**	**4,1**	**4,4**	**4,6**	**4,9**	**5,2**	**5,2**	**5,4**	**5,5**	**5,6**	**5,7**
Начальник отдела хранения, рабочий склада	**1**	**1,5**	**2,5**	**3,3**	**3,7**	**4,0**	**4,2,**	**4,6**	**4,8**	**5,0**	**5,2**	**5,4**	**5,5**	**5,6**	**5,7**
Водитель	**0,5**	**1,4**	**2**	**2,6**	**3,1**	**3,5**	**3,9**	**4,2**	**4,5**	**4,7**	**4,9**	**5,0**	**5,2**	**5,3**	**5,4**
Рабочий цеха №2	**0**	**0,5**	**1,2**	**1,8**	**2,3**	**2,8**	**3,3**	**3,6**	**4**	**4,3**	**4,5**	**4,7**	**4,9**	**5**	**5,2**
Энтропия ситуации	**0,01**	**0,12**	**0,21**	**0,28**	**0,34**	**0,37**	**0,41**	**0,44**	**0,46**	**0,48**	**0,50**	**0,51**	**0,52**	**0,53**	**0,54**

В момент наступления однородности (в таблице 6.12 выделенный столбец) необходимо произвести обновление или реконфигурацию параметров системы защиты, например: сменить все пароли, изменить режимы доступа, поменять замки, ключи и т. д.

Оценка однородности зарядов конденсаторов (или значимого различия ситуации информированности ДЭ) проводилась по критериям Вилкоксона и знаков Фишера при уровне доверительной вероятности $\alpha = 0{,}05$ [130]. Анализ динамики изменения параметров заряда емкостей на электрической схеме свидетельствует о том, что время утечки информации $T_у$ о СФЗ соответствует шести – восьми месяцам. Дополнительно величина $T_у$ оценивалась с помощью ИВМ по критерию оптимальной глубины эволюции развития энтропии любой технической системы с использованием разработанной программы [133, 74]. Графическая интерпретация

информационной постановки задачи оптимизации представлена на рисунке 6.14. Результат работы ИВМ приведен на рисунке 6.15.

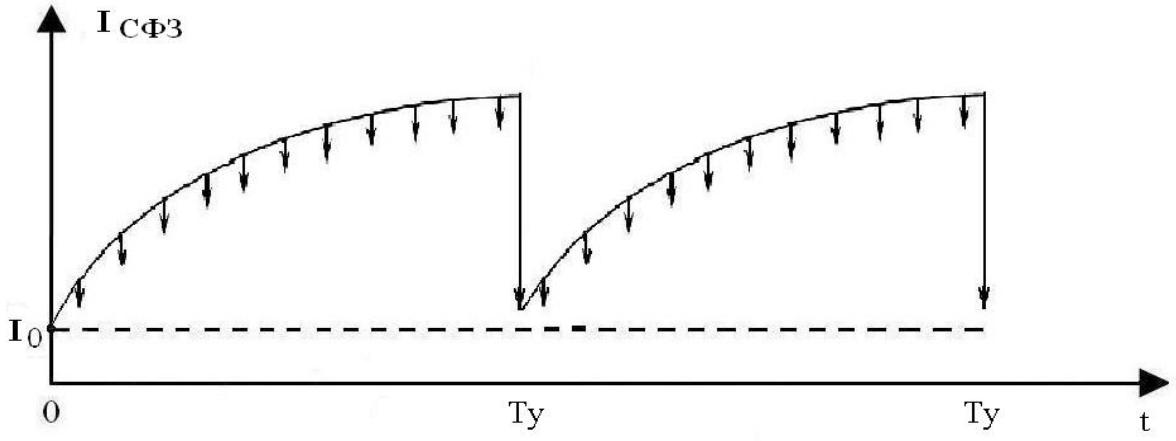


Рисунок 6.14 – Графическая интерпретация информационной постановки задачи оптимизации (I_0 – начальный уровень информированности исполнителей)

p2	p3	p4	p5	p6	p7	Энтропия
6	6	6	6	6	6	0,5901847...
3	2	1	1	0,5	0,1	0,0135945...
3,1	2,9	2	1,5	1,4	0,5	0,1206347...
3,5	3,4	2,9	2,5	2	1,2	0,2175490...
3,9	3,8	3,4	3,3	2,6	1,8	0,2878484...
4,3	4,2	3,8	3,7	3,1	2,3	0,3409468...
4,5	4,5	4,1	4	3,5	2,8	0,3783141...
4,8	4,7	4,4	4,2	3,9	3,3	0,4135293...
4,9	4,9	4,6	4,6	4,2	3,6	0,4393225...
5	5	4,9	4,8	4,5	4	0,4623672...
5,2	5,2	5,2	5	4,7	4,3	0,4867933...
5,3	5,3	5,2	5,2	4,9	4,5	0,5001841...
5,4	5,4	5,4	5,4	5	4,7	0,5150690...
5,5	5,5	5,5	5,5	5,2	4,9	0,5281535...
5,6	5,6	5,6	5,6	5,3	5	0,5383908...
5,7	5,7	5,7	5,7	5,4	5,2	0,5498538...

Рисунок 6.15 – Результаты работы информационно-вероятностного метода

На рисунке 6.15 p2 – p6 – значения величины напряжения на емкостных элементах эквивалентной электрической схемы.

Оптимальная порция преемственности энтропии наступает через шесть – семь месяцев, т.е. полученные результаты согласуются разными методами. Следовательно, необходимо менять информацию (ключи, шифры, пароли) через шесть – семь месяцев, что соответствует лучшему состоянию развития информационной системы.

Таким образом, при концептуальном проектировании системы защиты необходимо задавать параметр времени $T_{\text{у}}$. Введение данного критерия позволяет повысить эффективность СФЗ за счет снижения потенциала опасности нарушителя путем лишения нарушителя информационной компоненты, рассмотренной в третьей главе диссертации. Снижение информационного потенциала подготовки нарушителя составляет 13 %, так как информационный вес второй компоненты определяется величиной в 26 %.

6.5 Выводы

1. Разработанный метод на основе синтеза марковских цепей позволяет оценить эффективность функционирования СФЗ. Применение разработанного математического аппарата автоматизировано. Программное средство адекватно реагирует на вводимые изменения в структуру модели, что говорит о чувствительности модели к входным данным. Результатами моделирования являются вероятности безопасного состояния КСИИ при попытке нарушителя проникнуть на объект по каждому маршруту. Каждый путь проникновения обеспечивает безопасное состояние объекта на уровне не меньше заданных требований.

2. Разработан метод оптимального повышения эффективности СФЗ на основе планирования эксперимента для выработки рациональных управленческих решений.

3. По результатам моделирования процесса утечки информации, с помощью разработанной графовой модели аналогично приведенному анализу переходных процессов утечки тока, на основе критерия Хотеллинга и ИВМ оценки возникновения новой ситуации предложен оптимальный период времени обновления или регенерации новых параметров системы защиты КВО. Установлено, что необходимо вводить к таким объектам показатель времени утечки информации о системе защиты, который влияет информационный потенциал подготовки нарушителя и на время подготовки типового нарушителя к проникновению и, следовательно, интенсивность угроз.

Заключение

Нестабильность международной обстановки в связи с обострением терроризма, радикальные изменения в принципах и методах защиты объектов в целом обуславливают необходимость повышения роли СФЗ в обеспечении безопасности КВО. Уровень безопасности КВО закладывается при проектировании СФЗ, поэтому в качестве основного направления обеспечения безопасности КВО выбрано управление проектированием СФЗ на основе методов системного анализа, наиболее значимой стороной которого является системный подход к исследованию предметной области.

Современные КВО в своем составе, как правило, имеют ключевую систему информационной инфраструктуры, которая осуществляет управление КВО или информационное обеспечение управления КВО. Деструктивные действия нарушителей в отношении КСИИ могут привести к возникновению чрезвычайной ситуации. Это накладывает дополнительные требования при разработке СФЗ по обеспечению не только антитеррористической, но и информационной безопасности КВО.

Главным результатом диссертационной работы является разработка новых научно-технических и технологических решений в задачах проектирования СФЗ для обеспечения необходимой антитеррористической и информационной безопасности КВО, направленных на построение методик, моделей и методов выработки обоснованных управленческих решений.

Основные выводы по работе представлены следующими положениями:

1. В результате проведенного системного анализа технологии проектирования СФЗ объектов, имеющих распределенную структуру, и обзора существующих подходов к решению данной проблемы можно сделать следующие выводы.

В настоящее время при проектировании СФЗ КВО остаются мало исследованными вопросы обоснования принятия управленческих решений, основанных на методах системного анализа, формализованных моделей функционирования

СФЗ, методик на базе информационных критериев оптимальности, разных методов обработки одной и той же информации и формализации полученной информации как новых знаний для проектирования СФЗ.

Используемые специализированные программные комплексы (EASI, ASSESS, SAFE, СПРУТ, Вега-2) в основном применяются только на этапе анализа эффективности уже существующих СФЗ и не позволяют использовать их на всех этапах технологии проектирования новой СФЗ.

Самым сложным и плохо формализуемым этапом, требующим математических процедур, являются предпроектные исследования, под которым понимается разработка принципов и структуры СФЗ, выбор варианта и состава ИТСО. Ошибки на этапе предпроектных исследований приводят к увеличению затрат на проектирование СФЗ до 70 %.

Данная научно-техническая проблема проектирования СФЗ объектов связана с отсутствием развитого целостного теоретического подхода к проектированию, моделированию и оптимизации, собственно методологических основ – интегрирующей методики, модели и методы проектирования.

Для решения этой проблемы поставлена задача разработки теоретического обоснованного подхода к системному анализу процесса проектирования СФЗ на основе современных информационных технологий и методов синтеза сложных систем.

Следовательно, проблема разработки методик, моделей и методов в виде методологических основ выработки управленческих решений при проектировании СФЗ является актуальной.

Сформировано системное представление предметной области – «безопасность КВО» – в виде противоборства нарушителя и СФЗ для обеспечения безопасности объекта. С системных позиций рассмотрен технологический процесс проектирования СФЗ в виде последовательных связанных этапов. Проведен анализ этапов проектирования, выявлены проблемы и недостатки построения СФЗ:

- математически не обосновано количество категорий опасности объектов;

- линейная шкала оценки масштабов потерь имеет узкий диапазон и не соответствует действительности масштабов потерь;

- при определении интегрального показателя нарушителя – потенциала опасности – возникает проблема сведения множества разнородных характеристик к единому оценочному потенциалу. В настоящее время сравнительная оценка типовых нарушителей проводится только по отдельным характеристикам: по скорости перемещения, по времени преодоления физических барьеров, по вероятности обнаружения и т.д.;

- в основном технологии принятия решений при проектировании опираются на экспертные оценки специалистов в данной области, это вносит элемент субъективизма в процесс принятия решений при проектировании СФЗ из-за трудности привлечь достаточное количество специалистов и обеспечить согласованность их оценок. Целесообразно экспертные оценки использовать с минимальным привлечением и вмешательством человеческого фактора в процесс принятия решений [131, 62];

- мало разработаны вопросы применения математических методов, основанных на современных информационных технологиях и критериях.

Введен критерий обеспечения безопасности КВО и схема управления проектированием СФЗ, реализующая данный критерий. Предложена схема проведения предпроектных исследований в виде методологических основ, применяемых на всех этапах проектирования СФЗ.

2. Проведена сравнительная оценка энтропийного потенциала опасности каждой чрезвычайной ситуации, выявлен нелинейный характер изменения шкалы масштабов потерь, причем диапазон изменения энтропийного потенциала опасности ЧС составил сто раз.

На основе информационно-вероятностного метода предложена методика категорирования объектов, которая описывает каждую категорию КВО в виде порции энтропийнного потенциала опасности. Методика позволяет проводить декомпозицию спектра опасности объектов на группы (классы), т.е. формирует ка-

тегории объектов значимо различающиеся по энтропийному потенциалу опасности. Сформировано семь значимо отличных по опасности категорий.

3. Определены подходы к формированию модели нарушителя: произведена оценка интенсивности действий каждого типа нарушителей на определенный момент времени как прогнозирование момента возникновения новой террористической ситуации. С помощью ИВМ был определен потенциал опасности (подготовленности) типовых нарушителей.

На основе МГК интерпретированы главные компоненты характеристик объектов и модели нарушителя. Основной характеристикой объекта является его привлекательность, а характеристикой нарушителя – степень его технической, физической и информационной подготовленности (мотивации).

4. На основе сформированного общего информационного поля масштабов потерь КВО при возникновении ЧС и потерь после действия типовых нарушителей определены базовые нарушители для каждой категории объектов.

Для решения одной и той же задачи использовался ИВМ как основной метод определения потенциала опасности, а МГК и кластерный анализ – для подтверждения полученных результатов.

5. Выбран показатель оценки эффективности СФЗ – вероятность защиты (безопасного состояния) объекта. Вероятность выполнения ИТСО и силами реагирования своего функционального назначения обоснована как основной критерий оценки защищенности объекта.

Разработана имитационная модель функционирования СФЗ. На основе планирования эксперимента на имитационной модели определена функция потерь (риска) объекта от показателей эффективности подсистем СФЗ. Методом градиентного спуска в минимум функции потерь определены оптимальные требования к подсистемам СФЗ.

6. На типовых объектах на основе теории графов построен план размещения ИТСО, соответствующий заданным критериям эффективности СФЗ.

С помощью графа (мультиграфа) сформирована модель проникновения на объект, которая представлена в виде логических функций в матрице инцидентно-

сти. На основе решения задачи о покрытии на матрице инцидентности получены наборы покрытий для решения задачи динамического программирования для оптимального размещения и выбора ИТСО по критерию минимума стоимости при заданной вероятности обнаружения нарушителя. Таким образом, на основе методов целочисленного линейного и динамического программирования разработана методика для определения оптимального варианта размещения и выбора ИТСО на объекте. Предложен путь решения задачи, когда КЭ объекта имеют разный уровень важности.

7. Представлен метод оценки эффективности СФЗ, позволяющий оценить уровень защищенности объекта от террористических угроз. Проведен анализ защищенности типового объекта (оценка эффективности СФЗ) на основе марковских цепей. Основное достоинство метода заключается в том, что он дает обоснованный количественный показатель эффективности СФЗ по каждому маршруту проникновения нарушителя.

Оценка уровня защищенности объекта с помощью марковских цепей обладает следующим достоинством – в качестве исходных данных используется экспериментальная информация о защищенности каждой зоны объекта, что позволяет повысить достоверность оценки уровня физической защиты каждой зоны объекта в зависимости от степени подготовленности нарушителей и сил реагирования.

При разработке СФЗ могут использоваться несколько типов исходных данных, полученных проведением натурного эксперимента на объекте защиты, а именно:

- вероятность обнаружения нарушителя;

- характеристики, описывающие возможности нарушителя по преодолению физических барьеров между рубежами защиты: скорость перемещения; время преодоления барьеров (по результатам испытаний или аналитических оценок);

- характеристики, описывающие возможности сил реагирования по перемещению для нейтрализации нарушителя.

8. Рассмотрен информационный подход к формированию элементов организационного управления СФЗ на примере методики объединения технических средств обнаружения в группы, обеспечивающий равномерную и оптимальную информационную нагрузку на элементы организационного управления.

9. Впервые введен показатель оценки эффективности СФЗ – «время утечки информации о функционировании СФЗ», направленный на повышение ее эффективности. Реализован математический метод оценки данного показателя, по результатам которого принимается решение о смене паролей, шифров, замков и т.д., то есть регенерация новых установок и условий доступа к критическим элементам КВО.

Применение разработанного математического аппарата предлагаемых методов автоматизировано.

Новизна научных решений проблемы разработки СФЗ КВО состоит:

1. Введен формализованный критерий обеспечения безопасности КВО и схема управления проектированием СФЗ. Предложен комплекс методик, моделей и методов повышения достоверности и обоснованности проектирования в виде методологических основ проведения исследования технологического процесса проектирования СФЗ с использованием нового информационного подхода и добавлением методики формирования элементов организационного управления и методов оценки эффективности и времени утечки информации о функционировании СФЗ, направленные на повышение эффективности СФЗ.

2. Впервые использованы информационные показатели для оценки потенциалов опасности нарушителей и КВО при возникновении ЧС и критерии оптимальности развития систем, позволяющие обоснованно производить категорирование объектов, формировать элементы организационного управления и прогнозировать временной интервал значимого изменения активности террористических угроз.

3. Разработан комплекс методик в задачах поэтапного проектирования СФЗ на основе ИВМ и методов многомерного анализа, имеющих существенные отличия, основанные на впервые введенных информационных критериях:

- введение нелинейной энтропийной шкалы оценки масштаба видов потерь, позволяющей сформировать методику декомпозиции спектра опасности на значимо отличные категории КВО по информационному критерию оптимальности, проведение сравнительной оценки потенциалов опасности КВО и на этой основе обосновать необходимые требования вероятности безопасного состояния КВО;

- проведение оценки энтропийного потенциала опасности типовых нарушителей, а также прогнозируемого интервала времени значимого изменения активности террористических угроз для определения периода модернизации СФЗ;

- определение базовых нарушителей для КВО на основе обработки однородной информации о типовых нарушителях и категорируемых объектах.

4. Предложена модель обоснования требований эффективности к подсистемам СФЗ на основе планирования эксперимента на имитационной модели функционирования СФЗ с применением градиентного спуска в минимум функции потерь, новизна которого обоснована получением критериев эффективности подсистем СФЗ: обнаружения, задержки, реагирования и нейтрализации нарушителя.

5. Разработана методика размещения и выбора ИТСО объекта, удовлетворяющего заданным критериям эффективности СФЗ на основе декомпозиции графа (мультиграфа) проникновения нарушителя в матрицу логических функций и на последующем решении задач о покрытии и задачи динамического программирования. В основу разработки методики положены требования руководящих документов ФСТЭК. Введен показатель для обеспечения информационной безопасности ключевой системы информационной инфраструктуры – граница контролируемой зоны *Rкз.* Методика адаптирована для КЭ разной величины важности.

6. Разработана методика объединения технических средств обнаружения в группы для формирования элементов организационной структуры СФЗ. Предложен вариант формирования структуры СФЗ с равномерной и оптимальной информационной нагрузкой на элементы организационного управления СФЗ.

7. Разработан метод оценки эффективности СФЗ на основе противодействующих систем – нарушителя и СФЗ в виде марковских цепей, дающий обоснованный количественный показатель оценки эффективности СФЗ, позволяющий

вырабатывать оптимальные управленческие решения по структурной модернизации СФЗ для повышения ее эффективности.

8. Впервые введен показатель, повышающий эффективность СФЗ – «время утечки информации о функционировании СФЗ». Предложен метод определения времени утечки информации на основе формирования структуры семантики (содержания) информации МГК, теории графов и формирования эквивалентной аналоговой электрической схемы переходных процессов *RC* цепочек для моделирования процесса утечки информации. Метод позволяет определять момент наступления утечки информации о функционировании СФЗ для выработки управленческих решений по обновлению информационной среды СФЗ с целью уменьшения потенциала подготовки нарушителя.

Практическая ценность работы и внедрение результатов:

1. Разработаны методологические основы исследования процесса проектирования СФЗ, практическая ценность которых определяется повышением достоверности исходных данных: внешней среды и категории КВО, наличием критерия оптимальности безопасного состояния КВО для обоснования эффективности подсистем СФЗ, введением в процесс проектирования СФЗ методики объединения технических средств обнаружения в группы и методов оценки эффективности и времени утечки информации о функционировании СФЗ для выработки обоснованных решений, направленных на повышение ее эффективности.

2. При оценке опасности КВО от линейной шкалы определения масштабов потерь произведен переход к нелинейной энтропийной шкале, позволяющей повысить правдоподобность полученных результатов оценки потенциала опасности категорируемых КВО при возникновении ЧС и на этой основе определять требования к эффективности СФЗ. На основе ИВМ обосновано семь значимо различимых категорий опасности КВО.

3. Проведена сравнительная оценка потенциалов опасности (подготовленности) типовых нарушителей на основе обработки их характеристик МГК и ИВМ. Потенциал опасности внутреннего нарушителя соизмерим потенциалом группо-

вого нарушителя. Предложены уровни требований к эффективности СФЗ по защите объектов от типовых нарушителей.

4. На основе ИВМ и МГК сформированы базовые нарушители для каждой категории КВО.

5. Определен интервал времени прогнозирования значимого изменения активности террористических угроз для оценки интенсивности их действий на момент модернизации СФЗ.

6. Предложена и реализована модель обоснования требований к эффективности подсистем физической защиты (систем обнаружения, задержки, реагирования и нейтрализации нарушителя), так как именно эти требования необходимы проектировщику.

7. Разработаны и реализованы технические предложения в виде методик:

- методики оптимального размещения и выбора ИТСО, позволяющей формировать план размещения ИТСО на объекте защиты, обеспечивающий заданные требования безопасности КВО с минимальными затратами;

- методики объединения технических средств обнаружения в группы для формирования структуры организационного управления СФЗ, обеспечивающей равномерную и оптимальную информационную нагрузку на элементы управления.

8. Предложен и реализован метод оценки эффективности СФЗ на основе декомпозиции графа проникновения и моделирования противодействия СФЗ и нарушителя с помощью марковских цепей, позволяющий количественно оценить эффективность СФЗ по каждому маршруту проникновения и возможностью оптимально изменять структуру СФЗ для повышения ее эффективности.

9. Введен показатель оценки эффективности СФЗ - «время утечки информации о функционировании СФЗ», направленный на повышение эффективности СФЗ. Применение метода позволило уменьшить потенциал опасности нарушителя на 13 %, то есть повысить эффективность СФЗ.

Практическая значимость решенной проблемы заключается в том, что полученные в работе научные результаты являются методологической основой для

обоснования и разработки принятия решений в задачах управления проектированием СФЗ и позволяют обеспечить необходимую безопасность КВО. Предлагаемые методики, модели и методы обоснования решений в задачах управления проектированием СФЗ объектов были успешно применены в работах, выполняемых на ОАО «Концерн «Созвездие» г. Воронеж [134], ФГБУ «3 ЦНИИ» министерства обороны РФ ст. Донгузская, Оренбургской обл., ЗАО «Центр безопасности информации «ЦИНТУР» г. Оренбург, ООО «Уральский центр систем безопасности «УЦСБ» г. Екатеринбург, предприятие корпорации «Ростех» АО «Радиозавод» г. Пенза, в учебном процессе ФГБОУ ВО Оренбургский государственный университет и ФГБОУ ВО Пензенский государственный университет.

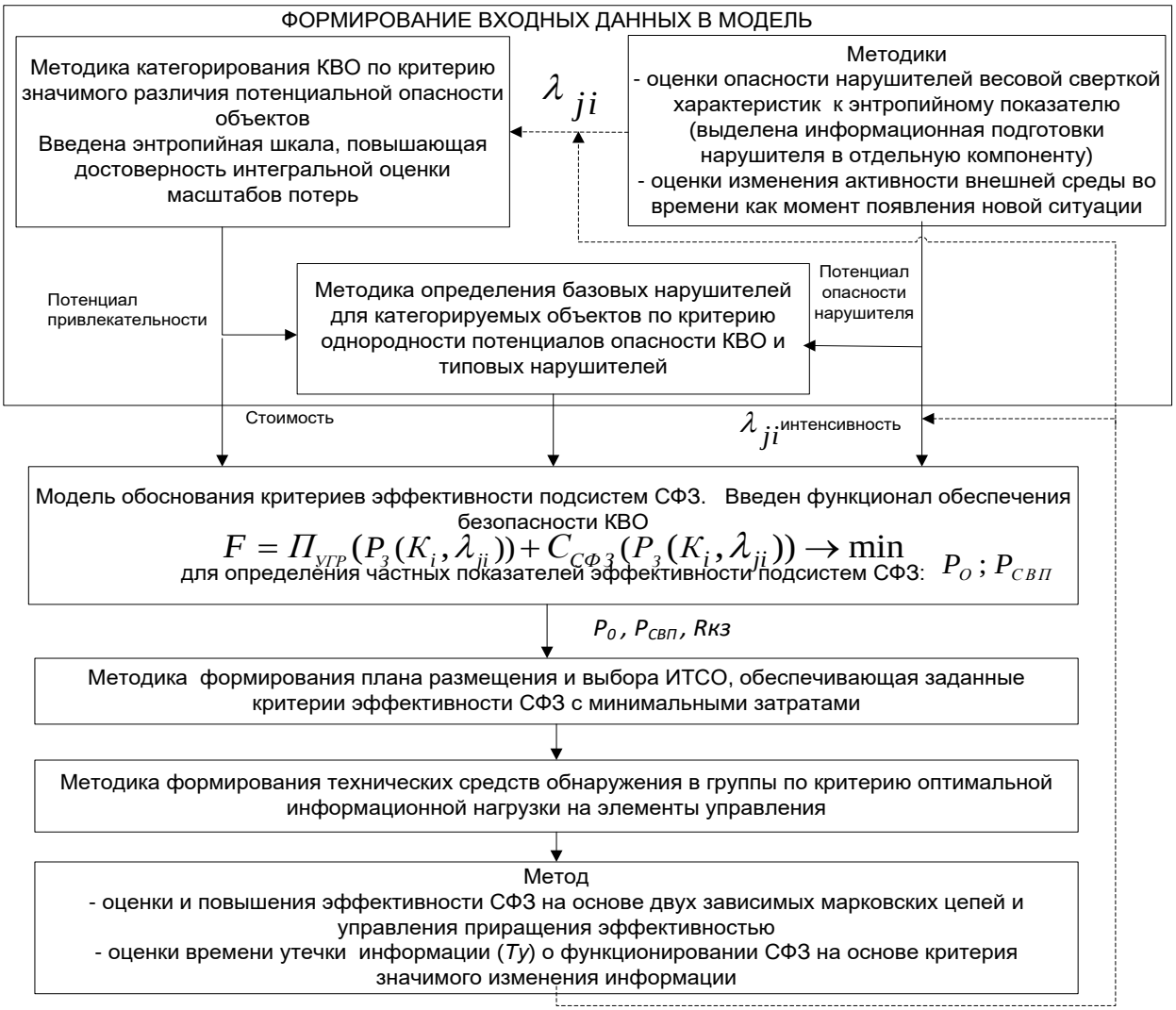
Таким образом, разработаны новые научно-технические и технологические решения в задачах проектирования СФЗ КВО, направленные на создание методик, моделей и методов повышения уровня обоснованности принимаемых управленческих решений, позволяющие на этапе концептуального проектирования строить оптимальную структурную модель СФЗ, обеспечивающую необходимую безопасность КВО.

Использование результатов диссертационной работы подтверждено документами о внедрении.

Все методики, модели и методы сведены в единую системно-логическую схему в виде методологических основ исследований, направленных на увеличение эффективности СФЗ, представленную на рисунке 1.

Рекомендации и перспективы дальнейшей разработки темы.

Работа представляет законченное научное исследование. Однако может быть продолжена в области разработки комплекса методов, моделей и алгоритмов обоснования и разработки СФЗ КВО на основе агентно-ориентированного подхода, байесовских сетей доверия, а также с использованием сочетания совокупности интеллектуальных методов поддержки принятия решений в задачах обоснования и разработки интеллектуальных СФЗ.



λ_{ji} – интенсивность действий *j*-го нарушителя против объекта *i*-ой категории; $P_О$, $P_{СВП}$ – частные показатели эффективности подсистем СФЗ; *Rкз* – граница контролируемой зоны.

Рисунок 1 – Методологические основы предпроектных исследований СФЗ

Список сокращений и условных обозначений

АСУ – Автоматизированная система управления

ДП – Динамическое программирование

ИК – Интегральный комплекс

ИТСО – Инженерно-технические средства охраны

ИСО – Инженерные средства охраны

ИВМ – Информационно-вероятностный метод

ИУС – Информационно-управляющая система

ИТС – Информационно-телекоммуникационная система

КВО – Критически важный объект

КИТСО Комплекс инженерно-технических средств охраны,

КИИ – Критическая информационная инфраструктура

КПП – Контрольно-пропускной пункт

КЗ – Контролируемая зона

КСИИ – Ключевая система информационной инфраструктуры

КЭ – Критический элемент

МГК – Метод главных компонент

ОКИИ – Объект критической информационной инфраструктуры

СФЗ – Система физической защиты

СОС – Система охранной сигнализации

СКУД – Система контроля и управления доступом

СТН – Система телевизионного наблюдения

ТА – Террористический акт

ТН – Типовой нарушитель

ТСО – Технические средства обнаружения

ФСТЭК – Федеральная служба технического экспертного контроля

ФАЛ – Функция алгебры логики

ЧС – Чрезвычайная ситуация

Список использованных источников

1 ГОСТ Р 22.2.06-2016**.** Безопасность в чрезвычайных ситуациях. Менеджмент риска чрезвычайной ситуации. Оценка риска чрезвычайных ситуаций при разработке паспорта безопасности критически важного объекта и потенциально опасного объекта : нац. стандарт Рос. Федерации : изд. офиц. – Введ. 2017-06-01. – Москва : Стандартинформ, 2016. – III, 8 с.

2 Об утверждении требований к антитеррористической защищенности объектов (территорий) Федеральной службы по техническому и экспортному контролю, ее территориальных органов и подведомственных организаций и формы паспорта безопасности этих объектов (территорий) [Электронный ресурс] : постановление Правительства РФ от 29 авг. 2014 г. N 875 // Гарант.ру : информ.-правовое обеспечение : [офиц. сайт] / ООО НПП «Гарант-Сервис-Университет». – Москва, 1990-2020. – Электрон. дан. – Режим доступа: https://base.garant.ru/70731274/ (дата обращения: 08.09.2020).

3 О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера (с изм. и доп.) [Электронный ресурс] : федер. закон от 21 декабря 1994 г. N 68-ФЗ // Гарант.ру : информ.-правовое обеспечение : [офиц. сайт] / ООО НПП «Гарант-Сервис-Университет». – Москва, 1990-2020. – Электрон. дан. – Режим доступа: https://base.garant.ru/10107960/ (дата обращения: 08.09.2020).

4 Совет Безопасности 08.11.2005 «Система признаков критически важных объектов и критериев отнесения функционирующих в их составе информационно-телекоммуникационных систем к числу защищаемых от деструктивных информационных воздействий».

5 ГОСТ Р 53114-2008. Защита информации. Обеспечение информационной безопасности в организации : : нац. стандарт Рос. Федерации : изд. офиц. – Введ. 2009-10-01. – Москва : Стандартинформ, 2009. – IV, 16 с.

6 Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими

процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды [Электронный ресурс] : приказ ФСТЭК России от 14.03.2014 № 31. // КонсультантПлюс : справочно-правовая система : [офиц. сайт] / ЗАО «Консультант Плюс». – Москва, 1997-2020. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_165503/ (дата обращения 09.09.2020).

7 О безопасности критической информационной инфраструктуры [Электронный ресурс] : федер. закон от 26.07.2017 № 187-ФЗ (послед. ред.) // КонсультантПлюс : справочно-правовая система : [офиц. сайт] / ЗАО «Консультант Плюс». – Москва, 1997-2020. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_220885/ (дата обращения 09.09.2020).

8 ГОСТ Р 50922-2006. Защита информации. Основные термины и определения : нац. стандарт Рос. Федерации : изд. офиц. – Взамен ГОСТ Р 50922—96 ; введ. 2008-02-01. – Москва : Стандартинформ, 2008. – IV, 8 с.

9 ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения : нац. стандарт Рос. Федерации : изд. офиц. – Взамен ГОСТ Р 51275-99 ; введ. 2008-02-01. – Москва : Стандартинформ, 2018. – III, 8 с.

10 ГОСТ Р 52069.0-2013. Защита информации. Система стандартов. Основные положения : нац. стандарт Рос. Федерации : изд. офиц. – Взамен ГОСТ Р 52069.0-2003 ; введ. 2013-09-01. – Москва : Стандартинформ, 2018. – III, 12 с.

11 ГОСТ Р 22.1.12-2005. Безопасность в чрезвычайных ситуациях. Структурированная система мониторинга и управления инженерными системами зданий и сооружений. Общие требования : нац. стандарт Рос. Федерации : изд. офиц. – Введ. 2005-06-15 ; изм. 2018-09-12. – Москва : Стандартинформ, 2005. – II, 23 с.

12 Об утверждении приоритетных направлений развития науки, технологий и техники в Российской Федерации и перечня критических технологий Российской Федерации : указ Президента Рос. Федерации от 7 июля 2011 г. № 899 (с

изм. и доп.) // Гарант.ру : информ.-правовое обеспечение : [офиц. сайт] / ООО НПП «Гарант-Сервис-Университет». – Москва, 1990-2020. – Электрон. дан. – Режим доступа: https://base.garant.ru/55171684/ (дата обращения: 08.09.2020).

13 Об утверждении Доктрины информационной безопасности Российской Федерации : указ Президента Рос. Федерации от 5 дек. 2016 г. № 646 // Гарант.ру : информ.-правовое обеспечение : [офиц. сайт] / ООО НПП «Гарант-Сервис-Университет». – Москва, 1990-2020. – Электрон. дан. – Режим доступа: https://base.garant.ru/71556224/ (дата обращения: 08.09.2020).

14 О внесении изменений в Федеральный закон "О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера : федер. закон от 08.03.2015 N 38-ФЗ (послед. ред.) // КонсультантПлюс : справочно-правовая система : [офиц. сайт] / ЗАО «Консультант Плюс». – Москва, 1997-2020. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_176157/ (дата обращения: 08.09.2020).

15 Волхонский, В. В. К вопросу единства терминологии в задачах физической защиты объектов / В. В. Волхонский, С. Л. Малышкин // Информационно-управляющие системы. – 2013. – № 5 (66). – С. 61–68.

16 Гарсиа, М. Проектирование и оценка систем физической защиты / М. Гарсиа ; пер. с англ. В. И. Воропаева [и др.]. – Москва : Мир : АСТ, 2002. – 386 с.

17 Garcia, M. L. Vulnerability Assessment of Physical Protection Systems / M. L. Garcia. – Butterworth-Heinemann, 2005. – 400 p.

18 Broder, J. F. Risk Analysis and the Security Survey / J. F. Broder. – Butterworth-Heinemann, 2006. – 393 p.

19 Классификации чрезвычайных ситуаций природного и техногенного характера : постановление Правительства Рос. Федерации от 21 мая 2007 г. № 304 (с изм. и доп.) // Гарант.ру : информ.-правовое обеспечение : [офиц. сайт] / ООО НПП «Гарант-Сервис-Университет». – Москва, 1990-2020. – Электрон. дан. – Режим доступа: https://base.garant.ru/12153609/ (дата обращения: 08.09.2020).

20 Бояринцев, А. В. Проблемы антитеррористического: Категорирование и анализ уязвимости объектов / А. В. Бояринцев, А. Н. Бражник, А. Г. Зуев. – Санкт-

Петербург : ИСТА-Системс, 2006. – 252 с.

21 Боровский, А. С. Автоматизированное проектирование и оценка систем физической защиты потенциально-опасных (структурно-сложных) объектов : монография / А. С. Боровский, А. Д. Тарасов. – Самара : Сам ГУПС ; Оренбург : ОрИПС – филиал Сам ГУПС, 2012. – Ч. 1 : Системный анализ проблемы проектирования и оценки систем физической защиты. – 163 с.

22 О безопасности : закон РФ от 05.03.1992 №4246 (послед. ред.) // КонсультантПлюс : справочно-правовая система : [офиц. сайт] / ЗАО «Консультант Плюс». – Москва, 1997-2020. – Электрон. дан. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_376/ (дата обращения: 08.09.2020).

23 Ярочкин, В. И. Теория безопасности / В. И. Ярочкин, Я. В. Бузанова. – Москва : Акад. Проект : Мир, 2005. – 174 с.

24 Шепитько, Г. Е. Проблемы охранной безопасности объектов / Г. Е. Шепитько ; под ред. проф. В. А. Минаева. – Москва : Рус. слово, 1995. – Ч. 1. – 352 с.

25 Магауенов, Р. Г. Охранная сигнализация и другие элементы систем физической защиты. Краткий толковый словарь / Р. Г. Магауенов. – Москва : Горячая линия – Телеком, 2007. – 97 с.

26 Магауенов, Р. Г. Системы охранной сигнализации: основы теории и принципы построения / Р. Г. Магауенов. – Москва : Горячая линия – Телеком, 2004. – 368 с.

27 Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации : руководящий документ Гостехкомиссии России. – Москва : ГТК РФ, 1992. – 39 с.

28 Панин, О. А. Категорирование объектов для создания эффективных систем физической защиты / О. А. Панин // Безопасность. Достоверность. Информация. – 2007. – № 1 (70). – С. 20–24.

29 Зуев, А. Г. Категорирование потенциально опасных объектов как основа создания эффективных систем обеспечения безопасности / А. Г. Зуев // Системы безопасности. – 2002. – № 3 (45). – С. 46–47.

30 Приказ Минпромнауки России от 25 мая 2002 года № 145 «Методические рекомендации по категорированию объектов науки, промышленности, энергетики и жизнеобеспечения по степени их потенциальной опасности и диверсионно-террористической уязвимости».

31 Вишняков, С. М. Функциональная опасность, безопасность и значимость объектов / С. М. Вишняков // Системы безопасности. – 2006. – № 2. – С. 29–32.

32 Шепитько, Г. Е. Проблемы безопасности объектов : учеб. пособие / Г. Е. Шепитько, И. И. Медведев. – Москва : Акад. экон. безопасности МВД России, 2006. – 199 с.

33 Алаухов, С. Ф. Концепция безопасности и принципы создания систем физической защиты важных промышленных объектов / С. Ф. Алаухов, С. Ф. Коцеруба. – НИКИРЭТ, 2005. – 96 с.

34 Об утверждении рекомендаций по антитеррористической защищенности объектов промышленности и энергетики : приказ министра промышленности и энергетики РФ от 04.05.2007 №150. – 2007. – 72 с.

35 О внесении изменений в требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды : приказ Федеральной службы по техническому и экспортному контролю от 9 августа 2018 г. № 138 // Гарант.ру : информ.-правовое обеспечение : [офиц. сайт] / ООО НПП «Гарант-Сервис-Университет». – Москва, 1990-2020. – Электрон. дан. – Режим доступа: https://www.garant.ru/products/ipo/prime/doc/71938866/ (дата обращения: 08.09.2020).

36 Грибунин, В. Г. Комплексная система защиты информации на предприятии : учеб. пособие для студентов высш. учеб. заведений / В. Г. Грибунин, В. В. Чудовский. – Москва : Академия, 2009. – 416 с.

37 Панин, О. А. Проблемы оценки эффективности функционирования систем физической защиты объектов / О. А. Панин // Безопасность. Достоверность. Информация. – 2007. – № 3 (72). – С. 22–27.

38 Алаухов, С. Ф. Вопросы создания систем физической защиты для крупных промышленных объектов / С. Ф. Алаухов, В. Я. Коцеруба // Системы безопасности. – 2001. – № 41. – С. 93–95.

39 Вентцель, Е. С. Исследование операций. Задачи, принципы, методология / Е. С. Вентцель. – 2-е изд., стер. –Москва : Наука, 1988. – 208 с.

40 Костин, В. Н. Проектирование систем физической защиты потенциально опасных объектов на основе развития современных информационных технологий и методов синтеза сложных систем [Электронный ресурс] : монография / В. Н. Костин, С. Н. Шевченко, Н. В. Гарнова. – Оренбург : ОГУ, 2013. – 202 с.

41 Оленин, Ю. А. Системы и средства управления физической защитой объектов / Ю. А. Оленин. – Пенза : ПГУ, 2002. – Кн. 1. – 212 с. ; 2003. – Кн. 2. – 256 с.

42 Радаев, Н. Н. Моделируя повадки нарушителя. Формализация нарушителя в задаче оценки эффективности системы физической защиты объекта / Н. Н. Радаев // Безопасность. Достоверность. Информация. – 2008. – № 1 (76). – С. 16–22.

43 Никитин, В. В. Телевидение в системах физической защиты : учеб. пособие / В. В. Никитин, А. К. Цыцулин. – Санкт-Петербург : Изд-во СПбГЭТУ "ЛЭТИ", 2001. – 132 с.

44 Вержбицкий, В. М. Основы численных методов : учебник для вузов / В. М. Вержбицкий. – Москва : Высш. шк., 2002. – 840 с.

45 Панин, О. А. Как измерить эффективность? Логико-вероятностное моделирование в задачах оценки систем физической защиты / О. А. Панин // Безопасность. Достоверность. Информация. – 2008. – № 2 (77). – С. 20–24.

46 Рябинин, И. А. Надежность и безопасность структурно-сложных систем / И. А. Рябинин. – Санкт-Петербург : Изд-во Санкт-Петерб. ун-та, 2007. – 275 с.

47 Можаев, А. С. Общий логико-вероятностный метод анализа надежности структурно сложных систем : учеб. пособие / А. С. Можаев. – Ленинград : ВМА, 1988. – 68 с.

48 Тулупьев, А. Л. Байесовские сети = Bayesian networks: логико-вероятностный подход / А. Л. Тулупьев, С. И. Николенко, А. В. Сироткин ; под ред. Р. М. Юсупова. – Санкт-Петербург : Наука, 2006. – 607 с.

49 Панин, О. А. Анализ безопасности интегрированных систем защиты: логико-вероятностный подход / О. А. Панин // Специальная техника. – 2004. – № 5 – С. 23–27.

50 ASSESS: справочное руководство : пер. с англ. / Министерство энергетики США, 1993.

51 Программный комплекс «Вега – 2» [Электронный ресурс] / АО "ФЦНИВТ "СНПО "Элерон" : [офиц. сайт], 2005-2020. – Электрон. дан. – Режим доступа: https://www.eleron.ru/production/special-programs/vega-2 (дата обращения: 09.09.2020).

52 Волков, И. А. Инструкция пользователю программы СПРУТ / И. А. Волков. – Санкт-Петербург : ИСТА-Системс, 2002. – 135 с.

53 Программный комплекс «СПРУТ» [Электронный ресурс] / Интернет – портал ГК «ИСТА» : сайт, 2005. – Режим доступа: https://ista.ru/.

54 Леус, А. В. Математическая модель оценки эффективности систем физической защиты / А. В. Леус // T–Comm – Телекоммуникации и транспорт. – 2010. – Т. 4, № 6. – С. 46–49.

55 Корчагин, С. И. Оценка эффективности ИК СФЗ в рамках вероятностного подхода / С. И. Корчагин // T–Comm – Телекоммуникации и транспорт. – 2010. – Т. 4, № 4. – С. 46–47.

56 Оценка функциональной эффективности охранной сигнализации малых объектов / С. С. Звежинский, Г. В. Голубков, В. А. Иванов, С. М. Сизов // Спецтехника и связь. – 2008. – № 3. – С. 13–20.

57 Домарев, В. В. Безопасность информационных технологий. Методология создания систем защиты / В. В. Домарев. – 2-е изд., перераб. – Киев : ТИД «ДС», 2008. – 286 с.

58 Порядок проведения оптимизации структуры интегрированного комплекса системы физической защиты на основе выбора наиболее эффективных альтернативных вариантов / С. Корчагин, А. Леус, А. Филимонов, Г. Шанаев // Безопасность. Достоверность. Информация. – 2010. – № 3 (89). – С. 6–9.

59 Звежинский, С. Победа любой ценой? Эффективность и результативность средств обнаружения / С. Звежинский, В. Иванов // Безопасность. Достоверность. Информация. – 2005. – №5 (62). – С. 64–70.

60 Вишняков, С. М. Функциональная безопасность объекта / С. М. Вишняков // Системы безопасности. – 2006. – № 3. – С. 96.

61 Звежинский, С. Объект защиты – вся страна. Средства обнаружения для территориально распределенных систем охраны / С. Звежинский, В. Иванов, А. Гомонов // Безопасность. Достоверность. Информация. – 2006. – №3 (66). – С. 54–57.

62 Завгородний, В. И. Вопросы создания систем физической защиты для крупных промышленных объектов / В. И. Завгородний, В. Я. Коцеруба // Системы безопасности. – 2001. – № 41. – С. 93–96.

63 Завгородний, В. И. Комплексная защита информации в компьютерных системах: учеб. пособие / В. И. Завгородний. – Москва : Логос, 2001. – 264 с.

64 Боровский, А. С. Обобщенная модель системы физической защиты как объект автоматизированного проектирования / А. С. Боровский // Вестник компьютерных и информационных технологий. – 2014. – № 10. – С. 45–52.

65 Костин, В. Н. Задачи концептуального проектирования систем физической защиты критически важных объектов / В. Н. Костин // Проблемы

информационной безопасности. Компьютерные системы. – 2020. – № 1. – С. 58–67.

66 Боровский, А. С. Автоматизированное проектирование и оценка систем физической защиты потенциально опасных (структурно-сложных) объектов : монография : в 3 ч. / А. С. Боровский, А. С. Тарасов. – Москва : Омега-Л ; Оренбург : Издат. центр ОГАУ, 2013. – Ч. 2 : Модели нечетких систем принятия решений в задачах проектирования систем физической защиты. – 247 с.

67 Фишборн, П. С. Теория полезности для принятия решений / П. С. Фишборн ; пер. с англ. В. Н. Воробьевой, А. Я. Кируты ; под ред. Н. Н. Воробьева. – Москва : Наука, 1978. – 352 с.

68 Мушков, А. Ю. Модели и методы стратегического управления сложными экономическими и технологическими системами: монография / А. Ю. Мушков, В. А. Тихомиров, В. А. Тихомиров. – Тверь : ВУ ПВО, 2003. – 244 с.

69 Оценка интеллектуальной собственности : учеб. пособие / под ред. С. А. Смирнова. – Москва : Финансы и статистика, 2002. – 352 с.

70 Рамбо, Дж. UML 2.0. Объектно-ориентированное моделирование и разработка / Дж. Рамбо, М. Блаха. – 2-е изд.– Санкт-Петербург : Питер, 2007. – 544 с.

71 Кантор, М. Управление программными проектами: практ. рук. по разраб. успеш. прогр. обеспечения : пер с англ. / М. Кантор. – Москва ; Санкт-Петербург ; Киев : Вильямс, 2002. – 173 с.

72 Крутько, П. Д. Алгоритмы и программы проектирования автоматических систем / П. Д. Крутько, А. И. Максимов, Л. М. Скворцов ; под ред. П. Д. Крутько. – Москва : Радио и связь, 1988. – 303 с.

73 Окулов, С. О. Программирование в алгоритмах / С. О. Окулов. – Москва : Бином. Лаборатория знаний, 2004. – 341 с.

74 Программное средство оценки развития ситуаций в системах физической защиты : свидетельство о гос. регистрации программы для ЭВМ / В. Н. Костин, А. А. Паршков ; заявитель и правообладатель федер. гос. бюджет. образоват.

учреждение высш. образования «Оренбург. гос. ун-т». – № 2016616793 ; заявл. 04.05.2016 ; зарегистрировано 20.06.2016 в Реестре программ для ЭВМ. – 1 с.

75 Костин, В. Н. Оценка величины значимости чрезвычайных ситуаций на основе информационно-вероятностного метода / В. Н. Костин // Проблемы информационной безопасности. Компьютерные системы. – 2019. – № 3. – С. 17–23.

76 Костин, В. Н. Информационно-вероятностный метод формирования категорий потенциально опасных объектов / В. Н. Костин, А. К. Пономарев // Вестник компьютерных и информационных технологий. – 2015. – № 6 (132). – С. 34–42.

77 Харман, Г. Современный факторный анализ / Г. Харман ; пер. с англ. В. Я. Лумельского. – Москва : Статистика, 1972. – 485 с.

78 Чепасов, В. Базовые параметры в многопараметрических исследованиях / В. Чепасов, М. Токарева, В. Костин. – Saarbruecken : LAP Lambert Academic Publishing. – 2014. – 328 с.

79 Чепасов, В. И. Детерминированные и статистические методы в повышении надежности несущих конструкций сельскохозяйственных машин: метод. пособие / В. И. Чепасов. – Москва : Колос–Пресс, 2002. – 88 с.

80 Костин, В. Н. Оценка потенциала опасности критически важных объектов при возникновении чрезвычайных ситуаций на основе информационно вероятностного метода и метода главных компонент / В. Н. Костин // Информационные технологии. – 2020. – Т. 26, № 5. – С. 297–301.

81 Медведев, И. И. Вероятностная модель действий нарушителей при проникновении на объект / И. И. Медведев, Г. Е. Шепитько // Современные технологии безопасности. – 2003. – №2 (5). – С. 4–7.

82 Ротштейн, А. П. Интеллектуальные технологии идентификации: нечеткие множества, нейронные сети, генетические алгоритмы / А. П. Ротштейн. – Винница : Универсум-Винница, 1999. – 320 с.

83 Лбов, Г. С. Методы обработки разнотипных экспериментальных данных / Г. С. Лбов ; отв. ред. Л. А. Растригин. – Новосибирск : Наука. Сиб. отд-ние, 1981. – 160 с.

84 Костин, В. Н. Оценка потенциала опасности нарушителей на основе информационного метода и метода главных компонент / В. Н. Костин // Информационные технологии и вычислительные системы. – 2016. – № 3. – С. 74–81.

85 Костин, В. Н. Оценка значимости частных видов потерь критически важных объектов при возникновении чрезвычайной ситуации / В. Н. Костин, А. С. Боровский // Научно-технический вестник Поволжья. – 2020. – № 8. – С. 8–11.

86 Дубров, А. М. Многомерные статистические методы / А. М. Дубров, В. С. Мхитарян, Л. И. Трошин. – Москва : Финансы и статистика, 1998. – 352 с.

87 Kostin, V. N. Definition of basic violators for critically important objects using the information probability method and cluster analysis / V. N. Kostin, A. S. Borovsky // Информационные технологии и нанотехнологии (ИТНТ-2020) : сб. тр. по материалам VI Междунар. конф. и молодеж. шк., 26-29 мая 2020 г. Самара : в 4 т. / [под ред. В. А. Фурсова]. – Самара : Изд-во Самар. ун-та, 2020. – Т. 4 : Науки о данных. – С. 943–947.

88 Положение о Реестре КСИИ : утверждено приказом ФСТЭК России от 4 марта 2009 г. № 74.

89 Gutlin, L. L. Information Theory and the Living System / L. L. Gutlin. – New York : Columbia University Press, 1972. – 210 p.

90 Седов, Е. А. Эволюция и информация / Е. А. Седов. – Москва : Наука, 1976. – 232 с.

91 Костин, В. Н. Метод оценки глубины прогноза развития (эволюции) характеристик сложных систем на основе энтропийного подхода / В. Н. Костин, Д. В. Даньшин // Информационные технологии. – 2015. – Т. 21, № 1. – С. 62–67.

92 Справочник офицера противовоздушной обороны / [Г. В. Зимин и др.]; под ред. Г. В. Зимина, С. К. Бурмистрова. – [2-е изд., перераб. и доп]. – Москва : Воениздат, 1987. – 511 с.

93 Вентцель, А. Д. Курс теории случайных процессов : учеб. пособие для студентов мех.-мат. фак. ун-тов/ А. Д. Вентцель. – Москва : Наука, 1975. – 319 с.

94 Костин, В. Н. Статистические методы и модели : учеб. пособие для вузов / В. Н. Костин, Н. А. Тишина. – Оренбург : ОГУ, 2004. – 138 с.

95 Адлер, Ю. П. Планирование эксперимента при поиске оптимальных условий / Ю. П. Адлер, Е. В. Маркова, Ю. В. Грановский. – Москва : Наука, 1976. – 279 с.

96 Куватов, В. И. Исследование операций / В. И. Куватов, Г. А. Величко. – Петродворец : ВМИРЭ, 2000. – 374 с.

97 Емельянов, С. В. Многокритериальные методы принятия решений / С. В. Емельянов, О. И. Ларичев. – Москва : Знание, 1985. – 32 с.

98 Шикин, Е. В. Математические методы и модели в управлении : учеб. пособие / Е. В. Шикин, А. Г. Чхартишвили. – Москва : Дело, 2000. – 440 с.

99 Мильнер, Б. З. Системный подход к организации управления / Б. З. Мильнер, Л. И. Евенко, В. С. Рапопорт. – Москва : Экономика, 1983. – 224 с.

100 Вентцель, Е. С. Прикладные задачи теории вероятностей / Е. С. Вентцель, Л. А. Овчаров – Москва : Радио и связь, 1983. – 416 с.

101 Имитационная модель функционирования системы физической защиты : свидетельство о гос. регистрации программы для ЭВМ / В. Н. Костин, А. А. Ларионов ; заявитель и правообладатель федер. гос. бюджет. образоват. учреждение высш. образования «Оренбург. гос. ун-т». – № 2018619550 ; заявл. 05.04.2018 ; зарегистрировано в Реестре программ для ЭВМ 08.08.2018. – 1 с.

102 Костин, В. Н. Методика формирования требований к системе физической защиты на основе концептуальной имитационной модели / В. Н. Костин, С. Н. Шевченко // Инфокоммуникационные технологии. – 2013. – Т. 11, № 2. – С. 91–98.

103 Костин, В. Н. Обоснование требований к эффективности подсистем физической защиты объектов информатизации / В. Н. Костин, Н. А. Соловьев, Н. А. Тишина // Научно-технический вестник Поволжья. – 2018. – № 4. – С. 125–128.

104 Костин, В. Н. Методы оптимизации в примерах и задачах : учеб. пособие / В. Н. Костин, А. Н. Калинин. – Оренбург : ОГУ, 2008. – 154 с.

105 Гуткин, Л. С. Оптимизация радиоэлектронных устройств по совокупности показателей качества / Л. С. Гуткин. – Москва : Совет. радио, 1975. – 367 с.

106 Беллман, Р. Прикладные задачи динамического программирования / Р. Беллман, С. Дрейфус ; пер. с англ. Н. М. Митрофановой [и др.] ; под ред. А. А. Первозванского. – Москва, 1965. – 458 с.

107 Решение задачи о покрытии на графе вариантов проникновения системы физической защиты : свидетельство о гос. регистрации программы для ЭВМ / В. Н. Костин, И. Д. Михайлов, И. Д. Михайлов ; заявитель и правообладатель федер. гос. бюджет. образоват. учреждение высш. образования « Оренбург. гос. ун-т». – № 2018619865 ; заявл. 06.04.2018 ; зарегистрировано в Реестре программ для ЭВМ 18.08.2018. – 1 с.

108 Мост безопасности [Электронный ресурс] : информ. сайт. – Режим доступа: http://www.security-bridge.com (дата обращения: 09.09.2020).

109 Боровский, А. С. Автоматизированное проектирование и оценка систем физической защиты потенциально опасных (структурно-сложных) объектов : монография : в 3 ч. / А. С. Боровский, А. С. Тарасов. – Москва : Омега-Л ; Оренбург : Изд. центр ОГАУ, 2013. – Ч. 2 : Модели нечетких систем принятия решений в задачах проектирования систем физической защиты. – 247 с.

110 Саати, Т. Принятие решений. Метод анализа иерархий / Т. Саати ; . пер. с англ. Р. Г. Вачнадзе. – Москва : Радио и связь, 1993. – 278 с.

111 Мишин, Е. Т. Построение систем физической защиты потенциально опасных объектов / Е. Т. Мишин, Е. Е. Соколов. – Москва : Радио и связь, 2005. – 200 с.

112 Динамическое программирование : свидетельство о гос. регистрации программы для ЭВМ / В. Н. Костин, И. Д. Михайлов, И. Д. Михайлов ; заявитель и правообладатель федер. гос. бюджет образоват. учреждение высш. образования «Оренбург. гос. ун-т». – № 201866140 ; заявл. 03.08.2018 ; зарегистрировано в Реестре программ для ЭВМ 07.09.2018. – 1 с.

113 Гарнова, Н. В. Методика формирования оптимального размещения элементов системы физической защиты (СФЗ) охраняемого объекта / Н. В. Гарнова, В. Н. Костин // Инфокоммуникационные технологии. – 2013. – Т. 11, № 4. – С. 91–95.

114 Бабиков, В. Г. Защита объектов нефтяной промышленности : справ. пособие / В. Г. Бабиков. – Москва : НОУ ШО «Баярд», 2005. – 512 с.

115 Андерсон, Джеймс А. Дискретная математика и комбинаторика : пер. с англ. / Джеймс А. Андерсон. – Москва ; Санкт-Петербург ; Киев : Вильямс, 2004. – 960 с.

116 Костин, В. Н. Синтез оптимального размещения технических средств систем физической защиты критически важных объектов / В. Н. Костин // Информационные технологии. – 2017. – Т. 23, № 1. – С. 41–49.

117 Новиков, Д. А. Модели и методы организационного управления инновационным развитием фирмы: монография / Д. А. Новиков, А. А. Иващенко. – Москва : КомКнига, 2006. – 336 с.

118 Саати, Т Л. Взаимодействие в иерархических системах / Т. Л. Саати // Техническая кибернетика. – 1979. – № 1. – С. 68–84.

119 Костин, В. Н. Методика формирования элементов структуры организационного управления системы физической защиты на основе информационного подхода / В. Н. Костин // Труды Ин-та систем. анализа Рос. Акад. наук. – 2020. – Т. 70, № 1. – С. 30–39.

120 Вентцель, Е. С. Теория случайных процессов и ее инженерные приложения : учеб. пособие для вузов / Е. С. Вентцель, Л. А. Овчаров. – 3-е изд., перераб. и доп. – Москва : Академия, 2003. – 432 с.

121 Вентцель, Е. С. Теория вероятностей : учебник / Е. В. Вентцель. – 11-е изд., стер. – Москва : КНОРУС, 2013. – 664 с.

122 Вишнякова, Т. О. Анализ эффективности систем физической защиты при помощи марковской сетевой модели / Т. О. Вишнякова, В. И. Васильев // Вестник УГАТУ. – 2007. – Т. 9, № 7. – С. 11–19.

123 Киреев, В. И. Численные методы в примерах и задачах : учеб. пособие для студентов вузов / В. И. Киреев, А. В. Пантелеев. – 4-е изд., испр. – Санкт-Петербург : Лань, 2015. – 448 с.

124 Программное средство синтеза Марковских моделей оценки эффективности систем физической защиты потенциально опасных объектов : свидетельст-

во о гос. регистрации программы для ЭВМ / В. Н. Костин, С. В. Пышкин ; заявитель и правообладатель федер. гос. бюджет образоват. учреждение высш. образования «Оренбург. гос. ун-т». – № 2016661765 ; заявл. 01.07.2016 ; зарегистрировано в Реестре программ для ЭВМ 20.10.2016. – 1 с.

125 Костин, В. Н. Оценка эффективности физической защиты информации критически важных объектов на основе марковских цепей / В. Н. Костин // Информационные технологии. – 2019. – Т. 25, № 12. – С. 757–765.

126 Крылов, А. К. Роль модельного эксперимента и фрактального анализа данных в психологическом исследовании / А. К. Крылов // Экспериментальная психология в России: традиции и перспективы // под ред. В. А. Барабанщикова. – Москва : Ин-т психологии РАН, 2010. – С. 106–110.

127 Абомелик, Т. П. Методология планирования эксперимента : метод. указ. к лаб. работам / сост. Т. П. Абомелик. – Ульяновск : УлГТУ, 2011. – 38 с.

128 Костин, В. Н. Модернизация структуры физической защиты критически важных объектов информатизации на основе выбора эффективных решений // Вестник компьютерных технологий. – 2019. – № 12 (186). – С. 27–39.

129 InfoWatch [Электронный ресурс] : офиц. сайт. – Режим доступа: https://www.infowatch.ru/ (дата обращения: 09.09.2020).

130 Morrison, D. F. Multivariate Statistical Methods / D. F. Morrison. – 2nd ed. – New York : McGraw Hill, 1976. – 415 p.

131 Лаборатория Касперского – антивирус kaspersky.lab.ru [Электронный ресурс] : сайт / АО «Лаборатория Касперского». – Москва, 2020. – Режим доступа: https://www.kaspersky.ru (дата обращения: 09.09.2020).

132 Костин, В. Н. Метод оценки утечки конфиденциальной информации о функционировании системы защиты объекта информатизации по информационному критерию // В. Н. Костин, А. С. Боровский // Вестник компьютерных и информационных технологий. – 2016. – № 8 (146). – С. 34–43.

133 Kostin, V. Definition of basic violators for critically important objects using the information probability method and cluster analysis : [Электронный ресурс] / V. Kostin, A. Borovsky // CEUR Workshop Proceedings. – 2020. – Vol. 2667 : 6th

International Conference Information Technology and Nanotechnology. Session Data Science, ITNT-DS 2020, 26-29 May 2020, Samara, Russian Federation. – P. 343–347.

134 Поддержка принятия решений в задаче проектирования и анализа систем физической защиты при охране больших открытых территорий (особо важных объектов) – Системный анализ проблемы проектирования систем физической защиты больших открытых территорий (особо важных объектов) : отчет о НИР (промежуточ.) / исполн. А. С. Боровский, В. Н. Костин, Г. Б. Волобуев.– Воронеж : Созвездие, 2009. – 126 с.

135 Развитие информационных технологий и методов принятия решений в автоматизированных системах. – Логико-вероятностная модель оценки эффективности систем физической защиты : отчет о НИР (промежуточ.) / исполн. В. Н. Костин. – Зарегистрирован в ВНТИЦ № И120315124936, 18.05.2012. – Оренбург : ОГУ – 104 с.

136 Развитие информационных технологий и методов принятия решений в автоматизированных системах. – Системный анализ проблемы проектирования и оценки систем физической защиты распределенных объектов (потенциально опасных объектов) : отчет о НИР (промежуточ.) / исполн. В. Н. Костин. – Зарегистрирован в ВНТИЦ № И130228153148, 01.03.2013. – Оренбург : ОГУ – 201 с.

137 Развитие информационных технологий и методов принятия решений в автоматизированных системах. – Модели опасных объектов отчет о НИР (промежуточ.) / исполн. В. Н. Костин. – Зарегистрирован в ВНТИЦ № И140609113555, 10.06.2014. – Оренбург : ОГУ – 130 с.

138 Развитие информационных технологий и методов принятия решений в автоматизированных системах. – Оценка потенциала опасности нарушителей на основе информационного метода и метода главных компонент : отчет о НИР (промежуточ.) / исполн. В. Н. Костин. – Зарегистрирован в ИКРБС № АААА-Б17-217031440025-9, 14.03.2017. – Оренбург, ОГУ – 118 с.

ПРИЛОЖЕНИЕ А

Свидетельства о государственной регистрации программ для ЭВМ

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2016616793

«Программное средство оценки развития ситуаций в системах физической защиты»

Правообладатель: *федеральное государственное бюджетное образовательное учреждение высшего образования «Оренбургский государственный университет» (RU)*

Авторы: *Костин Владимир Николаевич (RU), Паршков Алексей Александрович (RU)*

Заявка № 2016614555
Дата поступления 04 мая 2016 г.
Дата государственной регистрации в Реестре программ для ЭВМ *20 июня 2016 г.*

Руководитель Федеральной службы по интеллектуальной собственности

Г.П. Ивлиев

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2016661765

«Программное средство синтеза Марковских моделей оценки эффективности систем физической защиты потенциально опасных объектов»

Правообладатель: ***федеральное государственное бюджетное образовательное учреждение высшего образования «Оренбургский государственный университет» (RU)***

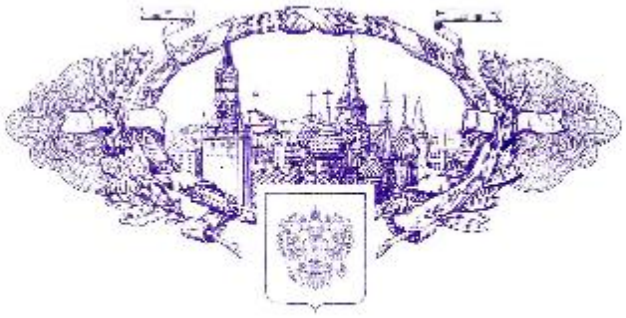
Авторы: ***Костин Владимир Николаевич (RU),***
Пышкин Сергей Витальевич (KZ)

Заявка № **2016617018**
Дата поступления **01 июля 2016 г.**
Дата государственной регистрации
в Реестре программ для ЭВМ ***20 октября 2016 г.***

Руководитель Федеральной службы
по интеллектуальной собственности

Г.П. Ивлиев

РОССИЙСКАЯ ФЕДЕРАЦИЯ



СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2018619550

Имитационная модель функционирования системы физической защиты

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

Авторы: ***Костин Владимир Николаевич (RU),***
Ларионов Андрей Александрович (RU)

Заявка № **2018613298**
Дата поступления **05 апреля 2018 г.**
Дата государственной регистрации
в Реестре программ для ЭВМ ***08 августа 2018 г.***

Руководитель Федеральной службы
по интеллектуальной собственности

Г.П. Ивлиев

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2018619865

Решение задачи о покрытии на графе вариантов проникновения системы физической защиты

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

Авторы: ***Костин Владимир Николаевич (RU), Михайлов Игорь Дмитриевич (RU), Михайлов Илья Дмитриевич (RU)***

Заявка № **2018613370**

Дата поступления **06 апреля 2018 г.**

Дата государственной регистрации в Реестре программ для ЭВМ ***14 августа 2018 г.***

Руководитель Федеральной службы по интеллектуальной собственности

Г.П. Ивлиев

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2018661409

Динамическое программирование

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

Авторы: ***Костин Владимир Николаевич (RU), Михайлов Игорь Дмитриевич (RU), Михайлов Илья Дмитриевич (RU)***

Заявка № **2018618239**
Дата поступления **03 августа 2018 г.**
Дата государственной регистрации
в Реестре программ для ЭВМ ***07 сентября 2018 г.***

Руководитель Федеральной службы по интеллектуальной собственности

Г.П. Ивлиев

ПРИЛОЖЕНИЕ Б

Акты о внедрении результатов диссертации

Утверждаю

Генеральный директор
ЗАО «ЦБИ «ЦИНТУР»
_____ В.А. Чекрыжов
«___» июня 2020 г.

Настоящим актом подтверждается, что закрытым акционерным обществом «Центр безопасности информации «ЦИНТУР» в процессе оказания услуг по информационной безопасности были применены результаты диссертационной работы Костина Владимира Николаевича «Методики, модели и методы обоснования и разработки систем физической защиты критически важных объектов» на соискание ученой степени доктора технических наук на тему.

В частности, это относится к нижеследующему – результаты научных исследований в части использования комплекса методик и методов поддержки принятия решений при разработке систем физической защиты (СФЗ), а именно:

– методика категорирования критически важных объектов (КВО) с использованием энтропийной шкалы оценки масштаба видов потерь при ЧС и информационного критерия в интерпретации значимого различия

– методика размещения и выбора инженерно-технических средств охраны (ИТСО) объекта, как совокупность методов: метод модернизированной задачи о покрытии и метод синтеза вариантов назначения ИТСО на покрытия с использованием динамического программирования, обеспечивающая заданные критерии эффективности СФЗ;

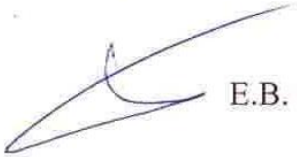
– метод оценки и повышения эффективности СФЗ на основе двух зависимых марковских цепей, позволяющий вырабатывать рациональные решения структурных изменений СФЗ для повышения ее эффективности;

были апробированы при выполнении работ по аттестации объектов информатизации по требованиям безопасности информации в следующих организациях г. Оренбурга и Оренбургской области:

- АО "Оренбургнефть";
- ООО "Оренбург Водоканал";
- Филиал ФГУП «Всероссийская государственная телевизионная и радиовещательная компания «Государственная телевизионная и радиовещательная компания «Оренбург»;
- Оренбургский локомотиворемонтный завод – филиал ОАО «Желдорреммаш»;
- ОАО «Орский машиностроительный завод»;
- Управление Федеральной службы исполнения наказаний по Оренбургской области.

Комиссия в составе:

Председатель –
заместитель генерального
директора – начальник отдела технической
защиты информации  А.П. Васильев

Члены:
Заместитель начальника отдела
технической защиты информации  Е.В. Костин

Главный специалист отдела
технической защиты информации  С.А. Осипов

УТВЕРЖДАЮ
Заместитель начальника полигона по НИИР

Д.И. Гурин

«__» июля 2020 г.

Акт реализации

Настоящим актом подтверждается использование результатов диссертационной работы Костина В.Н. на соискание ученой степени доктора технических наук на тему «Методики, модели и методы обоснования и разработки систем физической защиты критически важных объектов» при разработке и внедрении системы безопасности для объектов военного значения. Так при разработке общей структуры системы безопасности, оценки защищенности объекта военного значения была использована разработанная им методика размещения инженерно технических средств охраны и оценки их эффективности, которая используется при анализе защищенности объекта от угроз с целью выработки стратегических решений при организации его защиты.

Положения диссертационной работы тов. Костина В.Н. на тему «Методики, модели и методы обоснования и разработки систем физической защиты критически важных объектов» использованы на испытательном полигоне при проведении НИР «Ясногорец-3».

Использование результатов научных работ Костина В.Н., а также разработанные методики, модели и методы, реализованные в форме программных систем поддержки принятия решений, нашедшие отражение в его публикациях, позволили обеспечить высокую эффективность разрабатываемых систем безопасности объектов военного значения.

Начальник отдела
к.т.н. А.М. Серегин

Заместитель начальника отдела-начальник лаборатории
И.Н. Чивилёв

УТВЕРЖДАЮ
Директор департамента
организации работ
ООО «УЦСБ»

_____ /А.А. Макаров

_____ 2020г.

АКТ
рассмотрения результатов диссертационной работы
«Методики, модели и методы обоснования и разработки систем физической защиты критически важных объектов» Костина Владимира Николаевича на соискание ученой степени доктора технических наук

Комиссия в составе: председателя – Начальника отдела, Сидельникова Антона Юрьевича, руководителя направления систем безопасности, Торопова Александра Валерьевича, составила этот акт о нижеследующем.

С методиками оценки систем физической защиты (СФЗ) приходится сталкиваться при рассмотрении проектирования инженерно-технических средств охраны (ИТСО) для объектов топливно-энергетического комплекса. Действительно существующие программные продукты решают задачу оценки эффективности уже после выполнения проектирования, но никак не в процессе проектирования. С этой точки зрения предлагаемая методика размещения и выбора ИТСО с учётом заданной эффективности, считаем, очень актуальна.

В диссертационной работе представляет практический интерес метод оценки эффективности СФЗ, т.к. позволяет на основе расчетов показать насколько эффективны имеющиеся средства СФЗ, что в свою очередь необходимо для принятия управленческих решений.

Указанные выше методика и метод используются предприятием ООО «УЦСБ» при проектировании ИТСО объектов ГРЭС.

Результаты использования указанной выше методики и метода позволяют улучшить параметры проектирования систем физической защиты критически важных объектов.

Председатель комиссии:
Начальник отдела — А.Ю. Сидельников

Члены комиссии:
руководитель направления систем безопасности — А.В. Торопов

УТВЕРЖДАЮ
Проректор по учебной работе
ФГБОУ ВО «Оренбургский
государственный университет»
профессор
Т.А. Ольховая
“____” сентября 2020 г.

АКТ

внедрения результатов диссертационной работы
«Методики, модели и методы обоснования и разработки систем физической защиты критически важных объектов» Костина Владимира Николаевича на соискание ученой степени доктора технических наук

Мы, нижеподписавшиеся, заведующая кафедрой компьютерной безопасности и математического обеспечения информационных систем к.т.н., доцент Влацкая Ирина Валерьевна, и секретарь кафедры доцент Полищук Юрий Владимирович настоящим актом подтверждаем, что результаты диссертационной работы Костина В.Н. используются в учебном процессе ФГБОУ ВО «Оренбургский государственный университет».

Результаты научных исследований, полученных Костиным В.Н., используются преподавателями кафедры компьютерной безопасности и математического обеспечения информационных систем при чтении лекций по дисциплинам образовательной программы специалитета 10.05.01 «Компьютерная безопасность» специализации – разработка защищенного программного обеспечения: «Защита программ и данных», «Основы информационной безопасности», «Техническая защита информации».

Разработанное программное средство «Имитационная модель функционирования системы физической защиты», используется при проведении практических занятий по дисциплине «Технология построения защищенных автоматизированных систем».

Разработанные математические подходы построения моделей и методов обработки информации, представленные в монографии Костина В.Н. «Проектирование систем физической защиты потенциально опасных объектов на основе развития современных информационных технологий и методов синтеза сложных систем» используются преподавателями и студентами при проведении научных исследований.

Успешный опыт длительного использования результатов научных и методических работ Костина В.Н. в учебном процессе ФГБОУ ВО «Оренбургский государственный университет» подтверждает практическую значимость результатов его научных исследований.

Заведующая кафедрой
компьютерной безопасности и
математического обеспечения
информационных систем,
к.т.н., доцент — Влацкая И.В.

Секретарь кафедры,
к.т.н., доцент — Полищук Ю.В.

МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Пензенский государственный университет»
(ФГБОУ ВО «ПГУ»)
ул. Красная, д. 40, г. Пенза, Россия, 440026
Тел/факс: (841-2) 56-51-22, e-mail: cnit@pnzgu.ru, http://www.pnzgu.ru
ОКПО 02069042, ОГРН 1025801440620, ИНН/КПП 5837003736/583701001

Утверждаю
Проректор по научной работе
и инновационной деятельности
д.э.н., профессор
С.М. Васин
"___"сентября 2020 г.

АКТ

о внедрении результатов диссертации на соискание ученой степени доктора технических наук Костина Владимира Николаевича

Комиссия в составе: председателя - заведующего кафедрой «Технические средства информационной безопасности» (ТСИБ) ФГБОУ ВО «Пензенский государственный университет», к.т.н., доцента Иванова А.П., членов комиссии: профессора кафедры ТСИБ, д.т.н., доцента Иванова А.И., доцента кафедры ТСИБ, к.т.н. Хворостухина С.П., составила настоящий акт о том, что основные результаты диссертационной работы Костина В.Н.:

- методика оценки опасности угроз по интегральному энтропийному показателю;
- методика определения базовых нарушителей для категорируемых объектов;
- метод оценки эффективности системы защиты на основе моделирования процессов проникновения нарушителя и противодействия системы защиты с использованием двух зависимых марковских цепей, используются в учебном процессе кафедры «Технические средства информационной безопасности» при чтении лекций, проведении лабораторных и практических работ по дисциплинам «Специальные исследования технических средств защищенных автоматизированных систем управления», «Специальные исследования технических средств защищенных телекоммуникационных систем», «Биометрия и защита информации» специальностей 10.05.02 «Информационная безопасность телекоммуникационных систем» и 10.05.03 «Информационная безопасность автоматизированных систем», а также в научной работе кафедры по направлению развития методов и средств обеспечения информационной безопасности автоматизированных систем управления и связи в условиях информационного конфликта.

Председатель комиссии:
к.т.н., доцент А.П. Иванов

Члены комиссии:
д.т.н., доцент А.И. Иванов
к.т.н. С.П. Хворостухин

ГОСУДАРСТВЕННАЯ КОРПОРАЦИЯ
«Ростех»
АКЦИОНЕРНОЕ ОБЩЕСТВО
«Российская электроника»
АКЦИОНЕРНОЕ ОБЩЕСТВО
РАДИОЗАВОД
Ул. Байдукова, 1, Пенза, 440039, Россия
тел.: (841-2) 928096 факс.: (841-2) 496024
ИНН 5835049799 ОГРН 1045802500336
телетайп 155261"Волна" e-mail:radio@rf58.ru

УТВЕРЖДАЮ

Заместитель генерального директора
по научно-техническому развитию
АО «Радиозавод»

П.Е. Майоров
«__» _____ 2020 г.

АКТ ВНЕДРЕНИЯ
результатов диссертационной работы «Методики, модели и методы обоснования и разработки систем физической защиты критически важных объектов» Костина Владимира Николаевича на соискание ученой степени доктора технических наук

Комиссия в составе:
председателя комиссии – Денисова А.А. – начальника НИО-1 НТЦ;
членов комиссии:
- Бондарука Р.И., заместителя главного инженера НТЦ;
- Комарова А.А. – начальника конструкторского отделения НТЦ,

составила настоящий акт о том, что следующие результаты диссертационной работы Костина В.Н. внедрены на АО «Радиозавод» при выполнении инвестиционного проекта «Разработка и изготовление опытного образца командно-штабной машины береговых ракетно-артиллерийских войск ВМФ»:

1. Методика размещения и выбора инженерно-технических средств охраны объекта, позволяющая формировать план их размещения на объекте защиты и обеспечивающая заданные требования эффективности системы физической защиты (СФЗ).

2. Метод оценки и повышения эффективности СФЗ, позволяющий количественно оценить эффективности СФЗ по каждому маршруту проникновения нарушителя и вырабатывать рекомендации по оптимальному изменению структуры СФЗ для обеспечения заданной эффективности.

Достигнутые в результате использования указанных выше методик и методов позволили улучшить параметры проектирования систем физической защиты критически важных объектов.

Председатель комиссии Денисов А.А.

Члены комиссии: Бондарук Р.И.

Комаров А.А.