На правах рукописи

КОСТИН Владимир Николаевич

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

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

Автореферат
диссертации на соискание ученой степени
доктора технических наук

Оренбург – 2021

Работа выполнена на кафедре программного обеспечения вычислительной техники и автоматизированных систем федерального государственного бюджетного образовательного учреждения высшего образования «Оренбургский государственный университет».

Научный консультант – **Боровский Александр Сергеевич**, доктор технических наук, доцент, заведующий кафедрой «Управление и информатика в технических системах» федерального государственного бюджетного образовательного учреждения высшего образования «Оренбургский государственный университет»

Официальные оппоненты: **Еременко Владимир Тарасович,** доктор технических наук, профессор, федеральное государственное бюджетное образовательное учреждение высшего образования «Орловский государственный университет имени И.С. Тургенева», заведующий кафедрой «Информационная безопасность»

Алексеев Владимир Витальевич, доктор технических наук, профессор, федеральное государственное бюджетное образовательное учреждение высшего образования «Тамбовский государственный технический университет», заведующий кафедрой «Информационные системы и защита информации»

Истомин Андрей Леонидович, доктор технических наук, доцент, федеральное государственное бюджетное образовательное учреждение высшего образования «Ангарский государственный технический университет», факультет управления и бизнеса, декан

Ведущая организация – Федеральное государственное казенное образовательное учреждение высшего образования «Воронежский институт Министерства внутренних дел Российской Федерации»

Защита диссертации состоится 16 сентября 2021 г. в 14 часов на заседании диссертационного совета Д 212.065.06 в Ижевском государственном техническом университете имени М.Т. Калашникова по адресу 426033, г. Ижевск, ул. 30 лет Победы, 2, 5 корпус ИжГТУ имени М.Т. Калашникова.

С диссертацией и авторефератом диссертации можно ознакомиться в библиотеке ФГБОУ ВО «Ижевский государственный технический университет имени М.Т. Калашникова» и на сайте http://istu.ru.

Автореферат разослан «___» _____ 2021 г.

Отзывы на автореферат в двух экземплярах, заверенные гербовой печатью, просим направлять по адресу 426069, г. Ижевск, ул. Студенческая, д. 7, ИжГТУ имени М.Т. Калашникова

Ученый секретарь диссертационного совета,
кандидат технических наук, доцент Сяктерев Виктор Никонович

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования. В последнее время в связи с нарастающими угрозами международного терроризма намечается интенсивное развитие систем физической защиты (СФЗ) критически важных объектов (КВО). Актуальность данной проблемы обуславливается 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», в котором одним из приоритетных направлений развития науки обозначены безопасность и противодействие терроризму, а технологии обеспечения защиты и жизнедеятельности населения и опасных объектов при угрозах террористических проявлений включены в перечень критических технологий. Это выдвигает задачу обеспечения безопасности КВО в разряд первоочередных.

В соответствии с 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.

Согласно федеральному закону РФ 68–ФЗ от 21.12.1994 к КВО относятся: ядерно и химически опасные объекты: предприятия атомной и химической промышленности; биологически опасные объекты; техногенно опасные объекты: тепловые и гидроэлектростанции; центры управления работой ЕЭС; аэропорты; информационные вычислительные центры управления транспортом; морские порты; предприятия ракетно-космического и авиационного комплекса; плотины крупных водохранилищ, пожаро-взрывоопасные объекты: газоперерабатывающие заводы; нефтяные, газовые скважины и нефтеналивные терминалы, магистральные газо- и нефтепродуктопроводы; хранилища вооружения; объекты информационной инфраструктуры; предприятия по добыче и хранению драгоценных металлов; пункты государственного, военного управления; учреждения, обладающие уникальным оборудованием и информацией; комбинаты государственных резервов.

Особенность современных КВО – наличие ключевой системы информационной инфраструктуры (КСИИ), которая осуществляет управление или информационное обеспечение управления КВО. В результате деструктивных воздействий (внешних, внутренних угроз) против КСИИ может сложиться чрезвычайная ситуация (ЧС) или будут нарушены выполняемой системой функции управления со значительными негативными последствиями для обороны, безопасности, международных отношений, экономики или инфраструктуры страны.

Важность данной проблемы подчеркивается постановлениями правительства. Например, в постановлении правительства № 875 от 29.08.2014 «Об антитеррористической защищенности объектов ФСТЭК …» 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) минимизацию его последствий, которые обеспечивает СФЗ – 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.

Учитывая сложность решаемых задач, разработка СФЗ требует комплексного научного подхода, подразумевающего две стадии: предпроектных исследований и рабочего проектирования. Именно на стадии предпроектных исследований задаются и обеспечиваются необходимые требования к СФЗ, а качество этих исследований определяет риски ошибок и последствия рабочего проектирования.

В настоящее время при использовании методик, моделей и методов (например, методов оценки эффективности: критерия максимума среднегодового предотвращенного ущерба, предложенного Г. Е. Шепитько; критерия экономии от ущерба, представленного Э. И. Абалмазовым; критерия минимальных суммарных затрат на оснащение и эксплуатацию системы охранной сигнализации, разработанного в Академии ГПС МЧС России под руководством Н. Г. Топольского; критерия на основе модели потерь Lanchester; критерия «Эффективность – стоимость»; метода рисков и других) для разработки и оценки СФЗ обнаруживаются следующие недостатки: низкая математическая обоснованность и субъективизм принятия решений на этапах создания СФЗ; отсутствие методического аппарата формирования оптимального размещения инженерно-технических средств охраны (ИТСО) на объекте; отсутствие информационных показателей в задачах разработки СФЗ. В то же время существующие программные комплексы (например, Easi, Asses, SAFE – США; Спрут; Вега-2 – Россия) позволяют производить только оценку эффективности уже готовых СФЗ и не позволяют использовать их на всех этапах разработки СФЗ.

Существующий методологический аппарат при разработке и оценке СФЗ имеет принципиальные недостатки, главный из которых – игнорирование принципа комплексного научного подхода, предполагающего разработку и оценку СФЗ, как представлено выше, в два этапа и часто полное отсутствие именно системного проектирования, от успешного проведения которого зависит оптимальность будущих проектно-технических решений. Такой подход позволяет избежать серьезных ошибок в рабочем проекте, а следовательно, и излишних затрат на возможную доработку системы при ее эксплуатации.

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. Кроме того, рост технических возможностей нарушителей и активности террористических угроз также требует постоянного совершенствования СФЗ и соответствия возможностям средств нарушителя, а именно способности СФЗ к обеспечению своевременного обнаружения и нейтрализации нарушителей.

Степень разработанности темы исследования. Многие известные зарубежные и отечественные ученые посвятили свои труды исследованию проблем проектирования и оценки СФЗ, результаты которых нашли отражение в научных

изданиях: Джеймса Ф. Бродера, М. Гарсии, монографиях: А. В. Бояринцева, А. Н. Бражника, А. Г. Зуева, Р. Г. Магауенова, Ю. А. Оленина, Г. Е. Шепитько, трудах: Э. И. Абалмазова, В. А. Акимова, С. Ф. Алаухонова, А. В. Бочкова, Я. Д. Вишнякова, Н. Н. Радаева, Е. Т. Мишина, А. В. Измайлова, В. В. Лесных, А. В. Ничикова, А. М. Омельянчука, О. А. Панина, Д. Р. Резника, Н. Г. Топольского, К. И. Шестакова и др. При этом основное внимание уделялось отдельным этапам разработки СФЗ: категорированию КВО, вербальному описанию и оценке подготовленности нарушителей по отдельным характеристикам, сравнительной оценке развития ИТСО, обоснованию показателей и оценке эффективности СФЗ, модернизации существующих СФЗ.

Теоретические основы построения оптимальных технических систем, к которым относятся и СФЗ, крайне сложны и, несмотря на интенсивные исследования в данной области, далеки от совершенства. В литературных источниках не затрагивались вопросы комплексного подхода к разработке СФЗ, кроме того, отсутствуют критерии значимого различия категорий КВО, сравнительная оценка потенциальной опасности террористических угроз и КВО при возникновении ЧС, вопросы размещения ИТСО на объекте решаются без постановки задачи оптимизации, как этого требуют принципы системного анализа – с обоснованием целевой функции и ограничений. Не рассматриваются вопросы утечки (разглашения) информации о функционировании СФЗ, хотя в руководящих документах ФСТЭК определяются возможные каналы утечки информации, но показатели (критерии) и методы оценки показателей утечки информации не приводятся. Для решения задач оптимизации СФЗ в первую очередь необходима разработка способов структурного, а затем и параметрического синтеза СФЗ.

Несмотря на многочисленные исследования, средства анализа и оптимизации СФЗ в настоящее время развиваются медленно. Это обусловлено наличием ряда проблем. Основная проблема состоит в том, что СФЗ представляет собой сложную конфликтную систему, которая постоянно развивается, вследствие чего в процессе ее анализа и оптимизации присутствует элемент неопределенности. Данная проблема решается методами искусственного интеллекта, основанными на знаниях экспертов. В развитие данных методов значительный вклад внесли ученые А. С. Боровский, И. М. Янников и другие. Однако применение этих методов приводит к увеличению влияния субъективных факторов при формировании исходных данных и принятии управленческих решений на этапах разработки СФЗ.

Нормативные документы (федеральные законы, ГОСТ, приказы ФСТЭК и решения Совета безопасности Российской Федерации) регламентируют вопросы разработки СФЗ только в части выбора показателей оценки этапов проектирования и не предлагают критерии и методы их оценки для принятия решений.

На данный момент, несмотря на множество нормативных документов, методики предпроектных исследований СФЗ недостаточно разработаны и слабо объединены в единую структурную систему, хотя именно на этом этапе принимаются основные стратегические решения по вариантам построения системы, от которых зависит оптимальность проектно-технических решений, производится оценка ее будущей эффективности и закладываются количественные и качествен-

ные характеристики ИТСО. Ошибки предпроектных исследований приводят к увеличению затрат до 70 % на проведение рабочего проектирования. Существующие специализированные программные комплексы в основном используются только на этапе анализа эффективности уже спроектированных СФЗ, проектные решения на этапах проектирования не всегда математически обоснованны и не опираются на современные информационные технологии. Поэтому полноценное решение задачи повышения качества всех этапов проектирования СФЗ возможно с позиции единого системно-концептуального подхода.

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 методов оптимизации и современных форм обработки информации для обеспечения необходимой безопасности КВО.

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 динамиче-

ского 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 управления 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 выбора 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 безопас-

ного 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 структуры 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, теории 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.

Практическое использование результатов диссертационной работы подтверждено соответствующими документами о внедрении.

Основания для выполнения работы. Исследование проблемы – «безопасность 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», что отмечено в Указе 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».

Предлагаемые методологические основы в задачах проектирования СФЗ объектов были успешно применены в работах, выполняемых на ОАО «Концерн «Созвездие» г. Воронежа, ФГБУ «3 ЦНИИ» МО РФ ст. Донгузская, «Центр безопасности информации «ЦИНТУР» г. Оренбург, ООО Уральском центре систем безопасности «УЦСБ» г. Екатеренбург, предприятии корпорации «Ростех» АО «Радиозавод» г. Пенза. Разработанные методики, модели и методы выработки обоснованных решений в задачах разработки СФЗ объектов позволяют обоснованно строить на этапе предпроектных исследований структурную модель СФЗ, а также уменьшить ошибки рабочего проектирования.

Данное исследование выполнялось в рамках научно-исследовательской работы (НИР) о творческом содружестве «Шифр Охрана – 2011», договор № 572 от 11.06.2009 (г. Воронеж, ОАО Концерн «Созвездие»), ряд задач решался в рамках НИР шифр «Ясногорец-3» (ФГКУ «3 ЦНИИ» МО РФ) и госбюджетных НИР: И130621142522 от 26.07.2013, И130918174735 от 04.10.2014, И131210202925 от 12.12.2015, 01201000576 от 14.03.2017 (г. Оренбург, ОГУ).

Степень достоверности и апробация результатов. Основные положения и результаты диссертации докладывались, обсуждались и получили положительную оценку на научно-технических конференциях различного уровня по проблемам системного анализа, управления, информационных технологий.

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

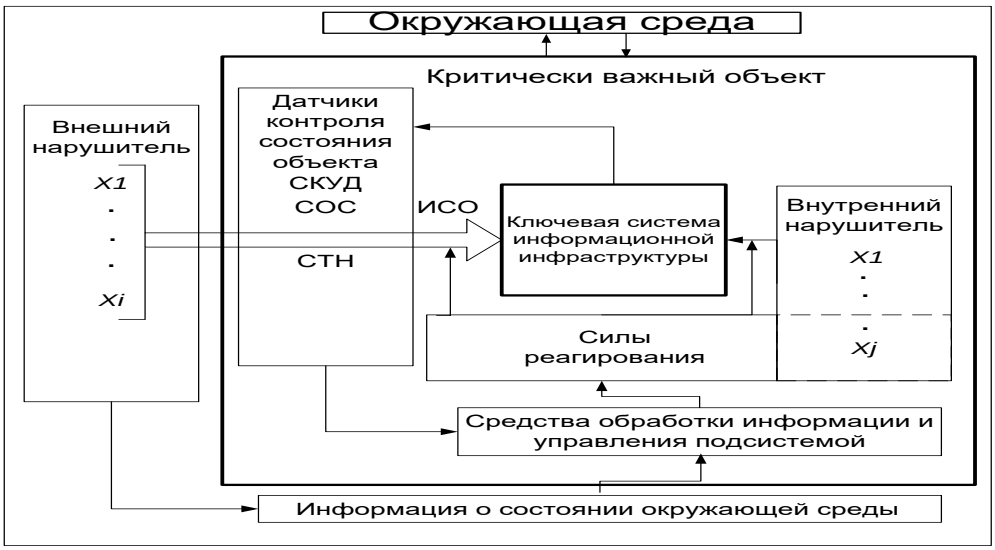
Личный вклад автора. Все основные результаты и положения, выносимые на защиту, получены лично автором. Основная часть публикаций выполнена лично автором, а часть в соавторстве с сотрудниками кафедры и научным консультантом, причем вклад диссертанта был определяющим.

Структура работы. Работа включает введение, 6 глав основного материала, заключение, библиографический список и приложения. Работа изложена на 249 страницах машинописного текста, кроме того, содержит 75 рисунков и 61 таблицу. Библиографический список содержит 138 наименований.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** рассмотрена актуальность работы, определена цель и решаемые задачи для ее достижения, сформулированы основные положения, выносимые на защиту, их научная новизна и практическая ценность. Представлены основания для выполнения работы, ее апробация и структура.

В **первой главе** изложены результаты анализа предметной области с системных позиций, состояния процесса разработки СФЗ объектов, обосновывается актуальность заявленных исследований. В рамках проводимых исследований была разработана модель предметной области (рис. 1), представленная в виде взаимодействия трех подсистем: подсистемы нарушителей, подсистемы объекта охраны и подсистемы СФЗ, включающей ИТСО, силы реагирования и организационные мероприятия. Подсистемы нарушителей и объекта охраны находятся в антагонистических отношениях, которые уравновешиваются СФЗ.



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

Рис. 1. Системный подход представления предметной области

Безопасность КВО определяется эффективность СФЗ. Для определения эффективности СФЗ введен функционал обеспечения безопасности КВО:

$$F = \Pi_{УГР}(P_З(K_i, \lambda_{ji})) + C_{СФЗ}(P_З(K_i, \lambda_{ji})) \to \min, \quad (1)$$

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

$P_З(K_i, \lambda_{ji})$ – эффективность СФЗ для K_i-ой категории объектов;

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

Соотношение зависимостей потерь категорируемых объектов от затрат на СФЗ и определение минимального суммарного ущерба, формирующего критерий обеспечения безопасности КВО, представлены на рисунке 2. Из рисунка видно – затраты на СФЗ увеличиваются с повышением категории объекта (точка F_2).

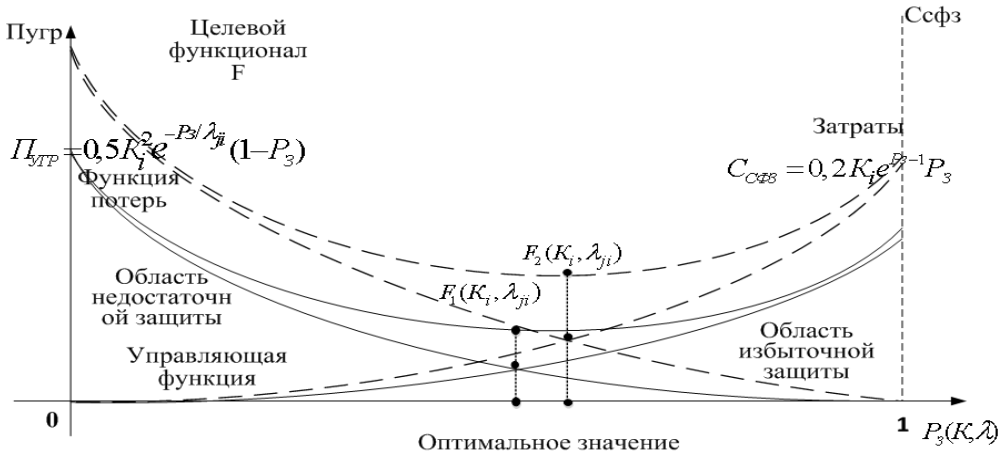


Рис. 2. Соотношение зависимостей потерь КВО и затрат на СФЗ

Из анализа рисунка 2, безопасность КВО обеспечивается СФЗ, эффективность которой определяется качеством управления технологии проектирования. Поэтому была разработана схема управления проектированием СФЗ (рис. 3).

W – нормативные документы; Q – ресурсы; U_i – управляющее решения (прямая связь); Y_i – выходная информация, определяет состояние объекта управления (обратная связь); Yсфз – выходные параметры модели; *b1, b2, b2* – параметры функции потерь; *Ро, $P_{СВП}$, Rкз* – показатели эффективности подсистем; *Рз* – показатель эффективности СФЗ; ε_i – ошибка; ε_{i3} – заданное значение

Рис. 3. Управление проектированием СФЗ (реализация функционала безопасности)

На рисунке 3 трехконтурная схема управления проектированием реализует задание критериев эффективности СФЗ; размещение и выбор ИТСО, обеспечи-

вающих заданные критерии эффективности; оценку эффективности СФЗ и ее повышение при неудовлетворительных результатах оценки.

Для оценки эффективности СФЗ выбран показатель – вероятность выполнения СФЗ своего функционального назначения – защиты объекта:

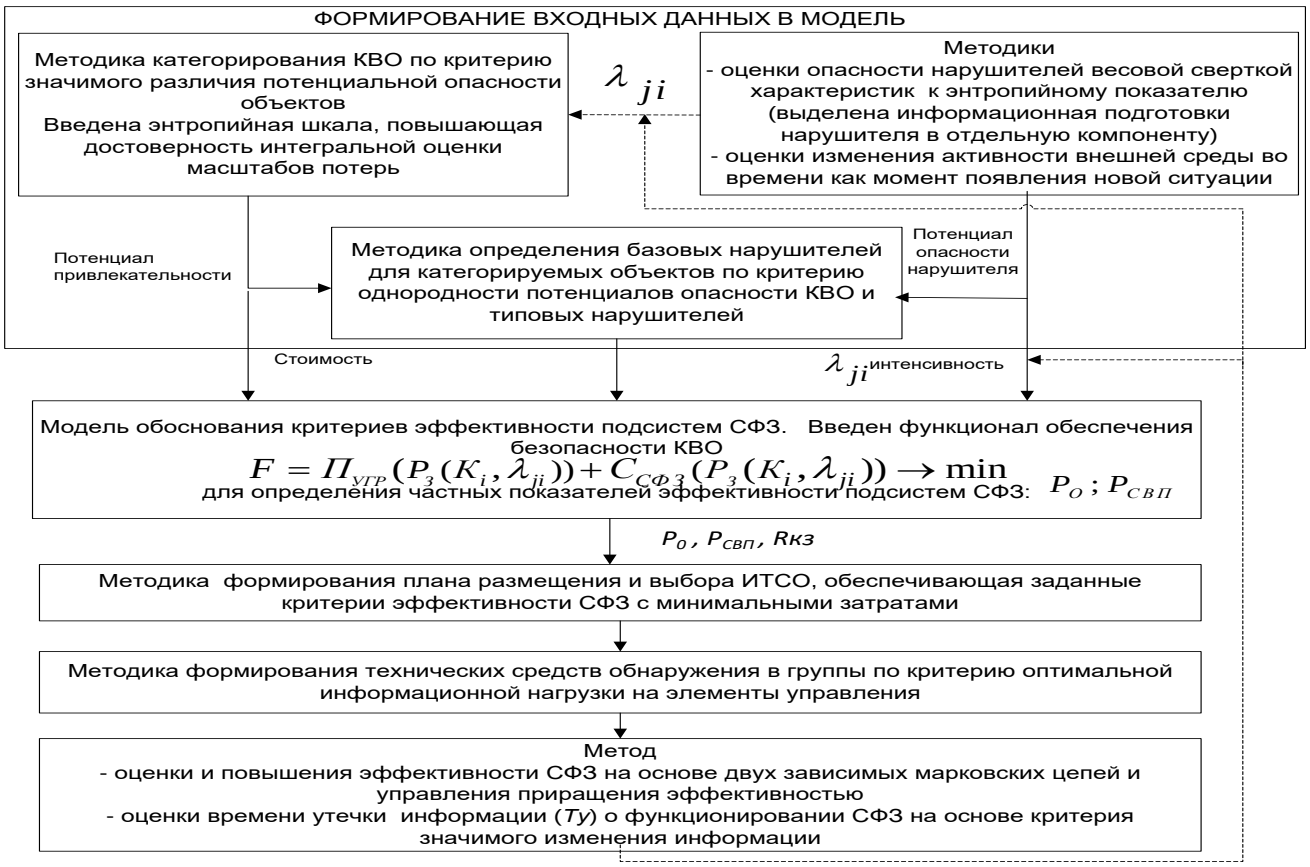
$$P_З = P_О \cdot P_{СВП} \cdot P_Н \,, \qquad (2)$$

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

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

$P_Н$ – вероятность нейтрализации нарушителя при условии своевременного развертывания сил реагирования.

Анализ состояния проектирования СФЗ выявил недостатки: категорирования КВО, обоснования критериев защищенности КВО, отсутствие методик оценки опасности типовых нарушителей. Это позволило сформулировать основные задачи и предложить методологические основы исследования в виде методик, моделей и методов в задачах проектирования СФЗ (рис. 4).



λ_{ji} – интенсивность действий *j*-го нарушителя против объекта *i*-ой категории;
$P_О$, $P_{СВП}$ – показатели эффективности подсистем СФЗ; *Rкз* – радиус контролируемой зоны.

Рис. 4. Методологические основы предпроектных исследований СФЗ

Новизна методологических основ состоит: во введенном формализованном критерии обеспечения безопасности КВО, который реализуется трехконтурной схемой управления проектированием (рис. 3); в новом информационном наполнении этапов предпроектных исследований; введенной методики объединения технических средств обнаружения в группы для формирования структуры организационного управления и методов оценки эффективности СФЗ и времени утечки информации о функционировании СФЗ – **решена задача №1.**

Для разработки СФЗ необходимо оценить степень опасности (важности) объекта защиты при возникновении ЧС (что защищать?) и определить потенциал возможностей нарушителей (от кого защищать?). Во **второй главе** на основе информационного показателя (оптимальности развития) систем разработана *методика категорирования КВО*, включающая следующие этапы:

А) введение энтропийной шкалы (вместо шестибалльной) оценки масштабов потерь при возникновении ЧС, повышающей адекватность и достоверность;

Б) формирование генеральной совокупности объектов по возрастанию опасности масштабов потерь при ЧС и оценка их опасности по энтропийной шкале;

В) декомпозиция спектра опасности на категории по информационному критерию значимого различия опасности объектов в одной категории;

Г) определение требований защищенности категорируемых объектов.

Этап А. При категорировании КВО для оценки масштабов потерь при ЧС используется, как правило, линейная шестибалльная шкала потерь, диапазон изменения которой не соответствует действительным потерям, поэтому введена нелинейная энтропийная шкала. Входными данными для получения энтропийной шкалы потерь является таблица 1 (постановление Правительства №304 от 21.05.2007 «О классификации ЧС …»), у которой столбцы ($i=1,n$) образованы масштабами ЧС $\{Ai\}$, а строки ($j=1,m$) – характеристики потерь, информационное поле таблицы – величина потерь (Xji).

Таблица 1 – Классификация ЧС природного и техногенного характера

Характеристики масштабов потерь при ЧС	Масштаб потерь при ЧС					
	Локального характера	Муниципального характера	Межмуниципального характера	Регионального характера	Межрегионального характера	Федерального характера
Пострадало и нарушены условия жизнедеятельности людей (человек)	не более 10	не более 50	не более 50	свыше 50, но не более 500	свыше 50, но не более 500	свыше 500
Размер материального ущерба (млн. руб.)	не более 0,1	не более 5	не более 5	свыше 5, но не более 500	свыше 5, но не более 500	свыше 500
Размер зоны ЧС	Не выходит за пределы территории объекта производственного или социального назначения	Не выходит за пределы одного поселения или внутригородской территории федерального значения	Не выходит за пределы двух или более поселений, внутригородских территорий федерального значения или межселенную территорию	Не выходит за пределы одного субъекта РФ	Затрагивает территорию двух и более субъектов РФ	Выходит за пределы территории РФ
Шестибалльная шкала оценки	1	2	3	4	5	6

Для оценки величины последствий ЧС в энтропийных шкалах автором использовался информационно-вероятностный метод. Алгоритм метода представлен на рисунке 5.

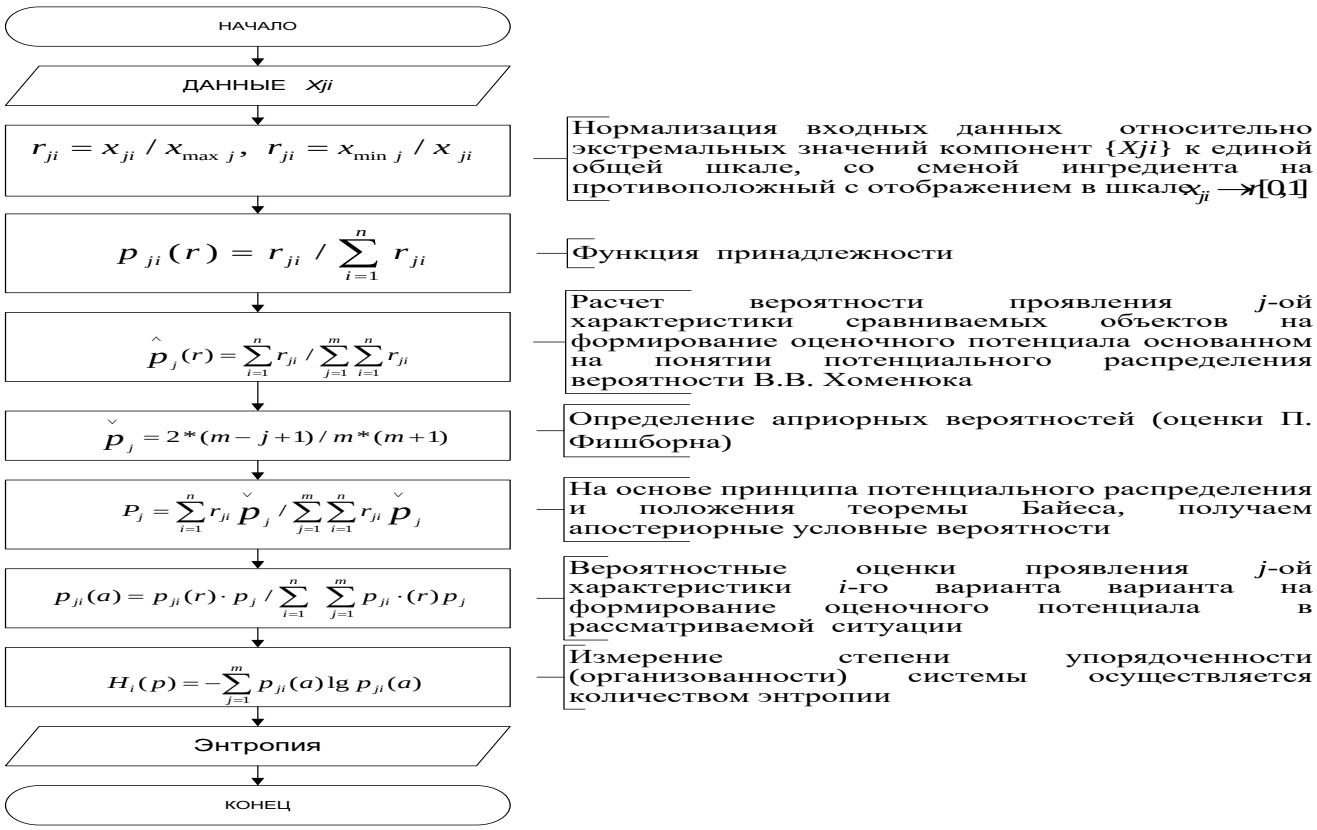


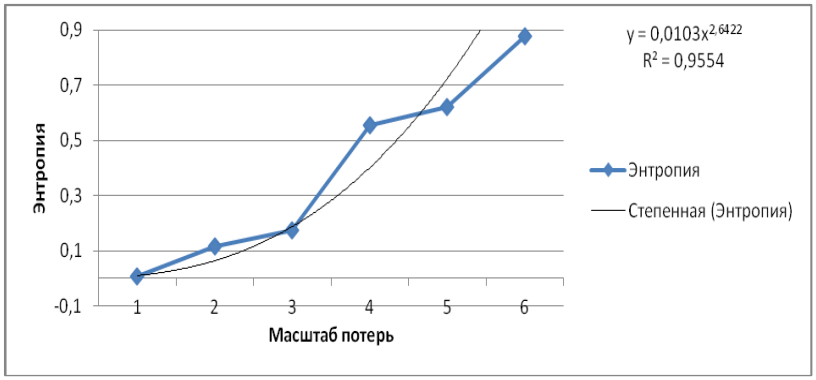
Рис. 5. Алгоритм расчета энтропии

В результате использования алгоритма ИВМ получено нелинейное распределение энтропийных потенциалов масштабов потерь при ЧС (табл. 2, рис. 6). Диапазон изменения масштаба потерь составляет сто раз, что соответствует диапазону действительных потерь (табл. 1), то есть введенная энтропийная шкала масштабов потерь повышает адекватность и достоверность оценки.

Таблица 2 – Потенциалы потерь 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 Н	0,0066	0,116	0,173	0,555	0,621	0,878

*- характера.



Анализ методик категорирования КВО выявил недостатки: категорирование происходит по перечневым классификаторам без математического обеспечения или критериальным оценкам, при этом количество категорий опасности математически не обосновано.

Рис. 6. Энтропийная шкала потерь

Этап Б. Генеральное множество опасных объектов представлено таблицей 3, у которой столбцы ($i=1,n$) образованы равномерным нарастанием опасности ге-

нерального множества объектов *{Ai}*, а строки (*j=1,m*) множеством характеристик частных видов потерь (табл. 3). Информационное поле таблицы – частные виды потери от 1 до 6 в зависимости от масштаба ЧС (табл. 1): 1 – локальный; 2 – местный; 3 – территориальный; 4 – региональный; 5 – государственный; 6 – межгосударственный.

Таблица 3 – Генеральное множество нарастания опасности объектов

Частные виды потерь	Генеральное множество опасных объектов													
	$\{A_1\}$	$\{A_2\}$	$\{A_3\}$	$\{A_4\}$	$\{A_5\}$	$\{A_6\}$	$\{A_7\}$	$\{A_8\}$	{Ai}	$\{A_{27}\}$	$\{A_{28}\}$	$\{A_{29}\}$	$\{A_{30}\}$	$\{A_{31}\}$
Политические	1	1	1	1	1	1	2	2	*X1i*	6	6	6	6	6
Людские	1	1	1	1	1	2	2	2	*Xji*	6	6	6	6	6
Финансовые	1	1	1	1	2	2	2	2	…	5	6	6	6	6
Экономические	1	1	1	2	2	2	2	2	…	5	5	6	6	6
Экологические	1	1	2	2	2	2	2	2	…	5	5	5	6	6
Информационные	1	2	2	2	2	2	2	3	*Xmi*	5	5	5	5	6

Исходные данные шестибалльной шкалы таблицы 3 заменили в соответствии с таблицей 2 энтропийной шкалой и с помощью разработанного автором программного средства (ПС № 2016616793), получили функцию нарастания энтропийной опасности генерального множества КВО, нелинейный характер изменения которой представлен на рисунке 7.

Рис. 7. Характер изменения потенциала опасности КВО по энтропийной шкале потерь

Этап В. Для построения решающего алгоритма формирования категорий используем статистические понятия ошибок первого и второго рода. Адаптация заключается в разной интерпретации использования ИВМ для решения следующих задач: категорирования объектов, прогнозирования развития внешней среды, объединения технических средств охраны в группы, оценки времени утечки информации о СФЗ как момент наступления новой ситуации в развитии системы, на основе впервые введенного информационного критерия. Алгоритм формирования категорий объектов представлен на рисунке 8.

Для декомпозиции генерального множества опасных объектов на значимо различные категории введен информационный критерий оптимальности развития систем – порция преемственности информации от предыдущей системы – $G_H^{ОПТ}$=0,27. Применяя изложенный алгоритм для данных рисунка 7, получили семь значимо различных по опасности категорий, которые сведены в таблицу 4.

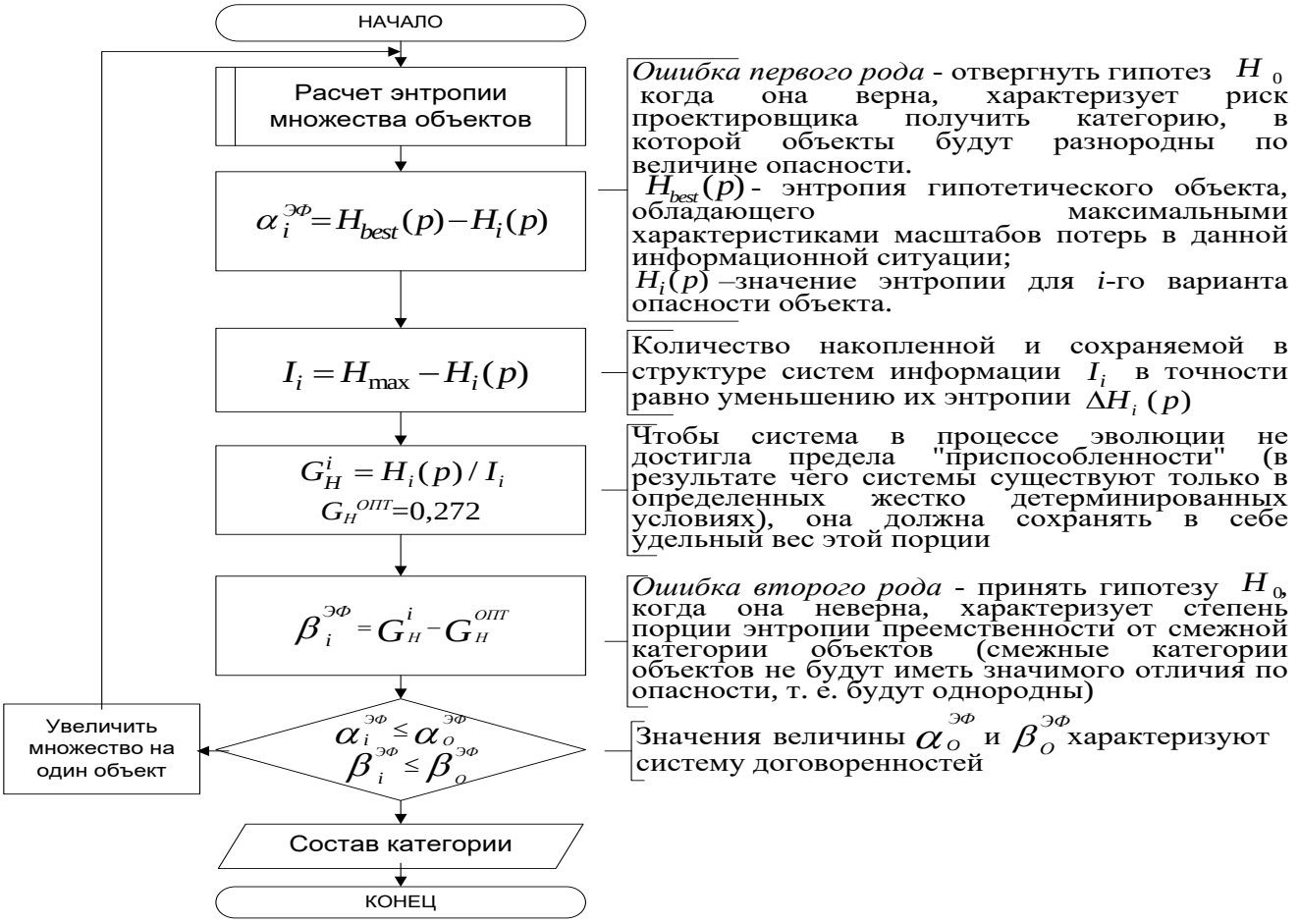


Рис. 8. Алгоритм формирования категорий объектов

Таблица 4 – Критерии категорирования по уровню потенциальных потерь

Характеристики категорий	Номер категории объектов						
	1-кат.	2-кат.	3-кат.	4-кат.	5-кат.	6-кат.	7-кат.
Порядковые номера совокупности объектов из таблицы рис. 6	A_{27}-A_{31}	A_{23}-A_{26}	A_{18}-A_{22}	A_{14}-A_{17}	A_{10}-A_{13}	A_6-A_9	A_1-A_5
Потенциал опасности энтропия Н	0,486	0,406	0,328	0,182	0,084	0,062	0,021

Выводы: 1 Распределение потенциалов опасности категорируемых объектов по энтропийной шкале носит нелинейный характер (рис. 7). 2 Методика категорирования рекомендует классифицировать КВО на семь значимо различимых по степени потенциальной опасности категорий.

Этап Г. Для определения критериев защищенности категорий КВО по данным таблицы 4 и рисунка 6 сформирована таблица 5 – характеристики опасности категорий объектов при ЧС. Анализ связи характеристик потерь таблицы 5 методом главных компонент (МГК) показал, что характеристики объединились в первую компоненту, которую интерпретировали как потенциал привлекательности категории, то есть потенциал опасности формирует потенциал привлекательности категории объектов.

Применяя алгоритм расчета энтропии к данным таблицы 5, оценивали величину опасности каждой категории объектов при ЧС в виде энтропийного потенциала опасности. Результаты оценки каждой категории представлены в нижней строке таблицы 5.

Таблица 5 – Характеристики опасности категорий объектов по энтропийной шкале

Частные виды потерь категорий КВО Характеристики оценок	Масштаб потерь категорий 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
Вероятность безопасного состояния	**0,999**	0,95	0,90	0,77	0,69	0,65	**0,60**

На основе установленных потенциалов опасности категорируемых КВО определены критерии их защищенности – вероятности безопасного состояния. Изменению энтропийного потенциала опасности категорий объектов сопоставили требуемую величину вероятности безопасного состояния первой категории (принято предельное значение вероятности защиты 0,999) и седьмой категории (чувствительность датчика обнаружения – 0,6). Характер изменения энтропии опасности категорий объектов и вероятности их безопасного состояния приведен на рисунке 9 и в таблице 5.

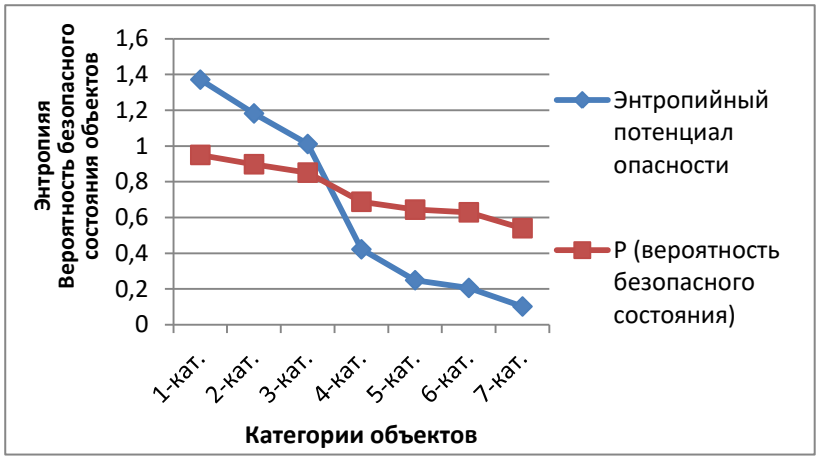


Рис. 9. Показатели опасности и защищенности объектов

Выводы: 1 Анализ характеристик масштабов частных видов потерь КВО при возникновении ЧС показал, что интегральной характеристикой категорируемых объектов является потенциал опасности объекта при ЧС, формирующий его привлекательность. 2 Распределение потенциалов опасности категорий КВО и показателей их защищенности носит нелинейный характер. Полученные результаты будут использоваться при обосновании требований к безопасности категорируемых объектов – **решена задача № 2.1**.

В **третьей главе** разработаны методики оценки потенциалов опасности типовых нарушителей; определения базовых нарушителей для категорий объектов и прогнозирования интервала времени значимого изменения активности нарушителей. В настоящее время используется вербальное описание модели нарушителя, сравнительный анализ нарушителей производится только по отдельным характеристикам, определение базовых нарушителей решается экспертными методами, а вопросы прогнозирования активности нарушителей при проектировании СФЗ не рассматриваются.

Методика оценки потенциалов опасности нарушителей включает этапы:

А) анализ структуры связей характеристик опасности нарушителей и определение энтропийных потенциалов опасности нарушителей МГК и ИВМ (табл. 7);

Б) анализ структуры связей характеристик последствий потерь от действий нарушителей (табл. 10) и определение энтропийных потенциалов последствий действий нарушителей МГК и ИВМ;

В) определение потенциалов опасности нарушителей ИВМ по характеристикам их опасности (табл. 7) и характеристикам последствий масштабов потерь их действий (табл. 10);

Г) оценка однородности энтропийных потенциалов опасности и потенциалов последствий их действий, полученных в А, Б, В по разнородным характеристикам опасности и последствий действий нарушителей. Если однородность не выполняется, то корректируются данные таблицы 10, полученные экспертным путем, в направлении обеспечения однородности энтропийных потенциалов;

Д) определение требований к показателям эффективности СФЗ для противодействия типовым нарушителям.

Этап А. Анализ структуры связей характеристик типовых нарушителей и оценка их потенциалов опасности осуществлялась соответственно МГК и ИВМ.

Постановлением правительства № 875 от 29.08.2014 «Об антитеррористической защищенности объектов ФСТЭК...» определены типы нарушителей (табл. 6).

Таблица 6 – Характеристики типовых нарушителей

Характеристики опасности 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	теракт	теракт	теракт	хищение	Хищение	хищ-е, теракт
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 (0,6)	низкий уровень 0,3	низкий уровень 0,3	высокий уровень (0,9)	высокий уровень (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 р>0,8	высокий уровень подготовки	высокий уровень подготовки	низкий уровень подготовки	низкий уровень подготовки	средний уровень подготовки

От качественных характеристик нарушителей таблицы 6 на основании методических разработок ФСТЭК перешли к количественным (табл. 7).

Таблица 7 – Количественные характеристики типовых нарушителей

Тип нарушителя	Характеристики нарушителей					
	Численность	Цель действ.	Последствия действий	Уровень информационной осведомленности	Холодное и огнестрельное оружие (оснащенность)	Уровень физической подготовки
X_1	11	10	0,878	0,7	0,9	1
X_2	4	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

Характеристика «*последствия действий нарушителя*» заменена соответствующим энтропийным потенциалом масштаба потерь из таблицы 2.

Применяя МГК к характеристикам нарушителей (табл. 7) получена новая структура связей характеристик (табл. 8): F_1 – интерпретировали «степень мотивации: физическая, техническая подготовка»; F_2 – как «информированность».

Таблица 8 – Факторные нагрузки нарушителей

Характеристики нарушителей	Факторные нагрузки	
	F_1 Степень мотивации к ТА	F_2 информированность
Численность	***0,843***	0,101
Цель действий	**0,95**	0,179
Последствия действий	***0,94***	0,031
Информационная осведомленность	0,116	**-0,975**
Оружие (техническая оснащенность)	**0,8**	-0,368
Уровень физической подготовки	***0,952***	0,128

То есть информационная (интеллектуальная) подготовка выделяется в самостоятельную компоненту. От матрицы факторных нагрузок перешли к оценке типовых нарушителей посредством главных компонент (табл. 9).

Таблица 9 – Оценка типовых нарушителей

Тип нарушителя	Факторные нагрузки		Энтропийный потенциал нарушителя
	F_1 Степень мотивации к ТА	F_2 информированность	
X1	1,631	0,131	**0,607**
X2	0,75	0,303	0,525
X3	0,037	0,905	0,377
X4	-1,25	1,203	**0,040**
X5	-1,099	-0,829	0,298
X6	-0,069	-1,714	0,550

Анализ таблицы 9 показал, что наиболее мотивированными к проведению ТА является первый тип нарушителя, менее мотивирован четвертый тип нарушителя, так как он обычный похититель. По информированности (компонента F_2) шестой и пятый тип нарушителя имеет наибольшую информированность, так как это внутренние нарушители. Менее информированы третий и четвертый тип нарушителя, так как они одиночные нарушители и не вступают в сговор с внутренними нарушителями.

Применяя ИВМ к первым двум компонентам, впервые введен энтропийный потенциал опасности типовых нарушителей (табл. 9 и рис. 10). Первый тип нарушителя превосходит четвертый тип нарушителя по энтропийному потенциалу опасности (мотивации и информированности) в 15 раз.

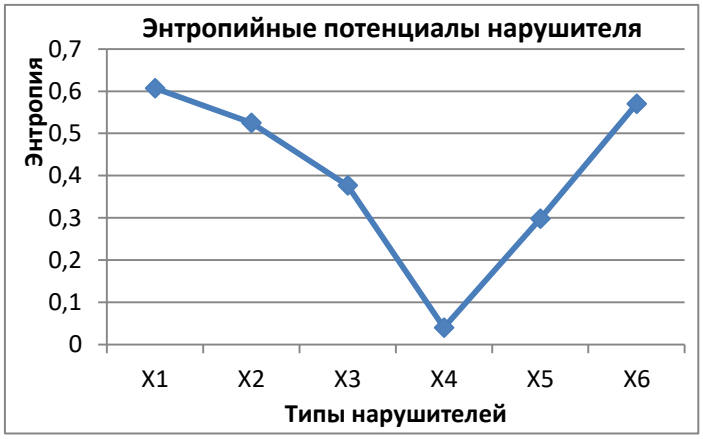


Рис. 10. Потенциалы опасности нарушителей

Этап Б. На этом этапе впервые применялся МГК для исследования связи характеристик нарушителей с использованием энтропийной шкалы формирования категорий объектов (табл. 5) на основе общей характеристики «последствия действия нарушителя» (табл. 7), связывающей между собой множество категорий опасности объектов и им соответствующих типовых нарушителей.

Для оценки типовых нарушителей в энтропийных шкалах масштабов потерь от их действий сформировали таблицу 10. Оценки характеристик подбирались так, чтобы обеспечивалась однородность характеристик опасности типовых на-

рушителей таблицы 7 с характеристиками масштабов потерь после их действия (табл. 10). Обработка характеристик потерь от действий нарушителей (табл. 10) МГК показала, что они также описываются двумя компонентами (табл. 11).

Таблица 10 – Оценки масштабов потерь от действий нарушителей

Частные виды потерь от действий нарушителя по энтропийной шкале	Масштабы потерь от действий типовых 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	0,0066	0,116	0,555	0,555

Таблица 11 – Факторные нагрузки нарушителей

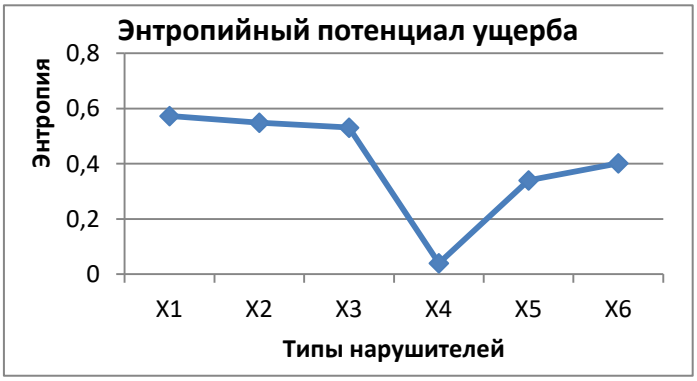
Частные виды потерь от действий нарушителя	Факторные нагрузки	
	F_1 Подрыв автор. власти.	F_2 информационные.
Политические	**- 0,989**	0,013
Людские	**- 0,985**	0,013
Финансовые	***+ 0,672***	-0,557
Экономические	**- 0,971**	-0,061
Экологические	**- 0,988**	0,061
Информационные	+ 0,473	**+0,805**

Все характеристики, кроме «информационных», объединились в первую компоненту. Базовой характеристикой в первой компоненте является «политические» потери, то есть целью является политическая мотивация, ее интерпретировали как «подрыв авторитета власти». В эту компоненту объединились такие характеристики: политические, экономические, экологические последствия и людские потери. Вторую компоненту интерпретировали как «информационные» потери последствий ТА. По таблице 11 определили характеристики нарушителей, выраженные через факторные нагрузки (табл. 12).

Таблица 12 – Характеристики нарушителей

Типы нарушителей	Факторные нагрузки		Энтропийный потенциал ущерба
	F_1-подрыв авторитета власти	F_2- информационные	
X_1	**-1,31**	***-0,245***	**0,573**
X_2	**-0,816**	0,002	0,549
X_3	**-0,772**	-0,151	0,531
X_4	***1,331***	-1,549	**0,040**
X_5	0,733	***0,069***	0,340
X_6	0,84	1,874	0,402

В компоненте F_1 «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. В компоненте F_2 наибольший вес имеют пятый, шестой тип нарушителя, так как они являются внутренними нарушителями (информированы) и будут оказывать деструктивное воздействие на информацию.



Применяя ИВМ к двум информационным компонентам, получили энтропийные потенциалы последствий (ущерб) от действий нарушителей (табл. 12, рис. 11). Первый тип нарушителя превосходит по энтропийному потенциалу ущерба четвертый тип нарушителя в 14 раз.

Рис. 11. Потенциал ущерба от нарушителей

Этап В. К данным таблиц 7, 10 применялся алгоритм расчета энтропии. В результате получили энтропийные потенциалы опасности по характеристикам нарушителей и характеристикам последствий их действий, которые представлены в таблицах 13, 14.

Таблица 13 – Энтропийные потенциалы опасности нарушителей

Характеристики нарушителей	Типы нарушителей					
	X_1	X_2	X_3	X_4	X_5	X_6
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 14 – Энтропийные потенциалы последствий реализации цели нарушителей

Частные виды потерь от действий нарушителей	Типы нарушителей					
	X_1	X_2	X_3	X_4	X_5	X_6
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

Этап Г. Анализ рисунков 10 и 11 показывает, что характер изменения потенциалов опасности типовых нарушителей и потенциал наносимого ими ущерба, согласуются по критериям хи-квадрат Пирсона, знаков Фишера.

Между энтропийными потенциалами опасности нарушителей и энтропийными потенциалами последствий их действий (табл. 13, 14) также нет значимого различия по критериям Вилкоксона, знаков Фишера (они однородны). Поэтому энтропийные характеристики нарушителей (табл.10) и КВО (табл. 5) можно объединить в одно информационное поле для определения базовых нарушителей.

Этап Д. Каждому потенциалу опасности типового нарушителя поставлен соответствующий потенциал защиты – эффективность СФЗ (вероятность защиты объекта). Иначе говоря, характер изменения зависимостей потенциалов опасности нарушителей и эффективности СФЗ должны быть подобными функциями. Функция изменения энтропийных потенциалов типовых нарушителей согласована с требуемой величиной эффективности СФЗ по аналогии с КВО. Результаты приведены в таблицах 13, 14 и на рисунке 12.

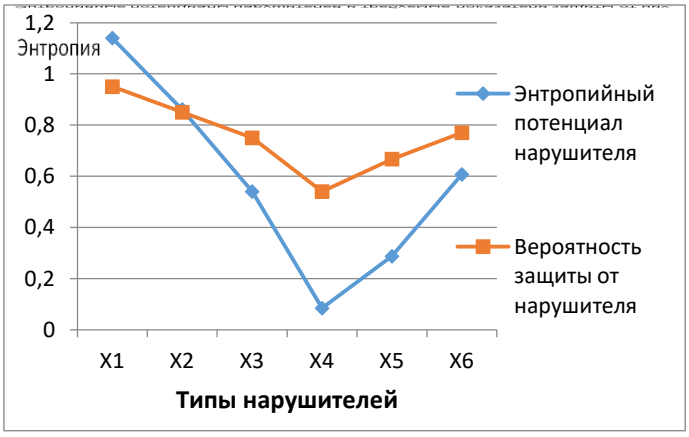


Рис. 12. Потенциал нарушителя и вероятность защиты от него

Вывод: 1 Разработана методика оценки энтропийных потенциалов опасности нарушителей и последствий реализации их цели. Полученные оценки согласованы. 2 Комплексной характеристикой типовых нарушителей является мотивация к действию, которая влечет за собой оснащенность, подготовленность и степень последствий реализации цели. 3 Информационная (интеллектуальная) подготовка нарушителей является важной составляющей, так как выделяется в самостоятельную компоненту – **решена задача № 2.2.**

Далее разработана *методика определения базовых нарушителей*. Очевидно, что каждой категории КВО должен соответствовать определенный базовый нарушитель из типовых нарушителей, то есть должно существовать соответствие, которое базируется на основе общего информационного поля категорируемых объектов и типовых нарушителей в виде энтропийной шкалы масштабов потерь.

Объединив таблицы 5 и 10 в таблицу 15, получили характеристики типовых нарушителей и категорируемых объектов в однородных энтропийных шкалах. Используя алгоритм расчета энтропии, получили энтропийные потенциалы опасности категорий объектов и типовых нарушителей.

Таблица 15 – 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-к	2-к	3-к	4-к	5-к	6-к	7-к
Политические	,878	,621	,555	,0066	,116	,173	,621	,555	,173	,173	,116	,116	0,0066
Людские	,878	,621	,555	,0066	,116	,173	,621	,555	,555	,173	,116	,116	0,0066
Финансовые	,555	,116	,116	,116	,621	,555	,621	,621	,555	,173	,116	,116	0,0066
Экономические	,878	,621	,555	,116	,116	,173	,878	,621	,555	,173	,173	,116	0,0066
Экологические	,878	,621	,555	,0066	,173	,116	,878	,621	,555	,173	,173	,116	0,116
Информационные	,555	,116	,007	,116	,621	,621	,878	,621	,555	,173	,173	,116	0,116
Энтропийный потенциал	,633	,497	,446	,160	,368	,375	,733	,629	,547	,269	,219	,210	0,122

Решив задачу объединения однородных потенциалов в кластеры ИВМ и МГК для данных табл. 15, получили результаты объединения типовых нарушителей и КВО в кластеры (табл. 16, рис. 13). Результаты согласуются с методом кластерного анализа.

Таблица 16 - Базовые нарушители

Типовые нарушители	Категория объекта	Энтропия H
$X_1+(X_6+X_5)$	1 – категория	0,733
X_1	2 – категория	0,633
$X_2,X_3+(X_6+X_5)$	3 – категория	0,497
X_3 , X_5, X_6	4– категория	0,280
X_3 , X_5, X_6	5 – категория	0,239
X_3 , X_5, X_6	6– категория	0,200
X_4	7– категория	0,122

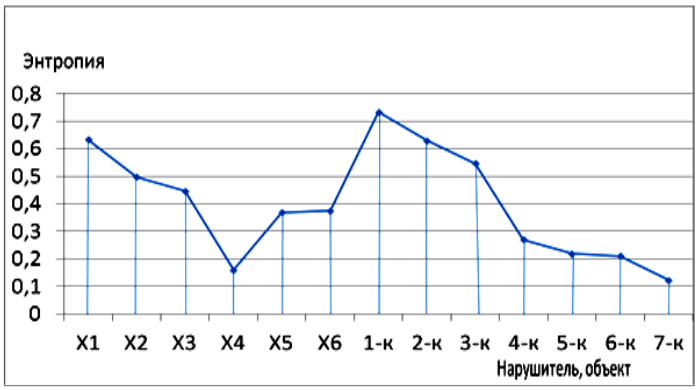


Рис.13. График энтропийного потенциала

Вывод: определены базовые типовые нарушители для каждой категории объектов – **решена задача № 2.3.**

Так как создание СФЗ осуществляется на перспективу, в разделе разработана методика прогнозирования оценки интервала времени значимого изменения внешней среды с позиции развития системы для определения времени модернизации СФЗ. В качестве меры эволюции системы выступает удельный вес порции энтропии ИВМ (рис. 8), то есть имеется оптимальное время прогнозирования активности нарушителей.

Прогнозирование характеристик интенсивности действий типовых нарушителей по статистическим данным осуществлялось на основе метода наименьших квадратов с использованием полинома третьей степени $P^3(x_i)$ (рис. 14), так как

данный полином описывает статистические результаты с наименьшей ошибкой согласования с исходными статистическими данными.

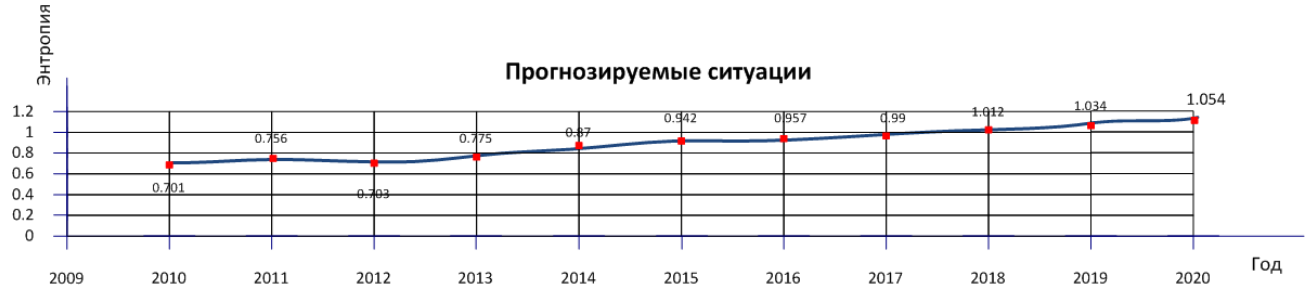


Рис. 14. Прогнозирование развития активности нарушителей

Последовательно с помощью аппроксимирующей функции получали прогнозируемые результаты активности нарушителей (рис. 14) и с использованием ИВМ оценивали $\beta_i^{ЭФ} = G_H^i - G_H^{ОПТ}$ пока $\beta_i^{ЭФ}$ не достигнет заданного минимума.

Вывод: полученные результаты (рис. 14) показывают, что разработанный метод оценки изменения активности внешней среды позволяет определить интервал времени будущей модернизации СФЗ – **решена задача № 2.4.**

В **четвертой главе** разработана модель определения требований эффективности к подсистемам СФЗ на основе эксперимента на имитационной модели функционирования СФЗ (рис. 15) и градиентного спуска в минимум функции потерь, реализующая функционал обеспечения безопасности КВО $F = П_{УГР}(P_З(K_i, \lambda_{ji})) + C_{СФЗ}(P_З(K_i, \lambda_{ji})) \to \min$.

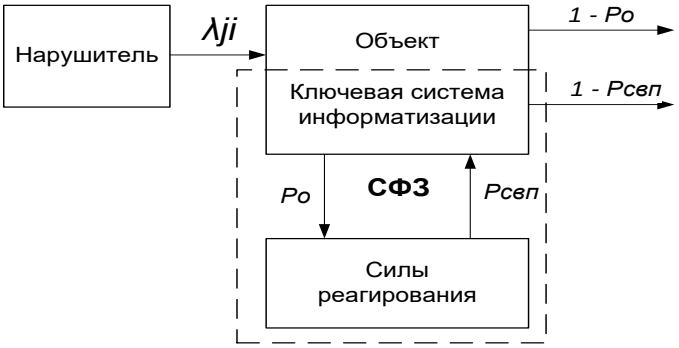


Рис. 15. Модель функционирования СФЗ

λ_{ji} – прогнозируемая интенсивность действий базового нарушителя;

P_O – вероятность обнаружения нарушителя;

$P_{СВП}$ – вероятность своевременного прибытия сил реагирования;

1- Ро – вероятность потерь ресурсов объекта от необнаружения нарушителя;

1- $P_{СВП}$ – вероятность потерь несвоевременного прибытия сил реагирования.

Учитывая принцип зональности построения СФЗ, пространственно-временная диаграмма противодействия нарушителя и СФЗ представлена на рисунке 16.

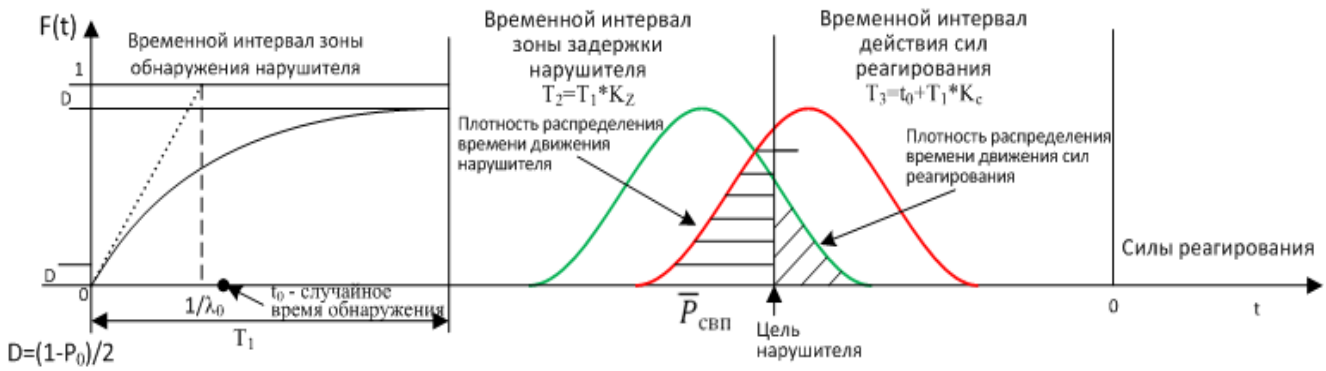


Рис. 16. Пространственно-временная диаграмма противодействия нарушителя и СФЗ

Моделировались две величины: время проникновения нарушителя и время реакции СФЗ на проникновение. Время проникновения состоит из случайного времени преодоления зоны обнаружения T_1 и случайного времени преодоления зоны задержки T_2. Интервал времени T_2 связан с интервалом T_1 коэффициентом Kz, учитывающим степень задержки нарушителя в зоне задержки объекта. Вероятность обнаружения нарушителя зависит от времени его движения в зоне обнаружения:

$$Po = 1 - e^{-\lambda_o t}. \quad (3)$$

Выразим из формулы 3 величину λ_0 и применяя нормализацию при t= 1. Тогда интенсивность будет зависеть только от вероятности обнаружения:

$$\lambda o = -\ln(1 - Po), \quad (4)$$

где P_0 – заданная вероятность обнаружения проникновения. В соответствии с заданной интенсивностью λ_0 случайное время обнаружения определяется:

$$to = -1/\lambda o \cdot \ln(1 - R), \quad (5)$$

где ~~R~~ – случайная величина, равномерно распределенная в интервале [0 - 1]. После подстановки формул получаем случайное время обнаружения:

$$t_o = \ln(1 - R)/\ln(1 - Po) \cdot t, \ при \ t = 1. \quad (6)$$

Годовая цена потерь от реализации угроз и затрат на СФЗ определялась эмпирической формулой:

$$Ц = C \cdot (M \cdot 0,3 + 0,1 \cdot Po + 0,04 \cdot (1 - Kc) + 0,07 \cdot Kz) + Co, \quad (7).$$

где M – математическое ожидание количества реализованных угроз в год; C – стоимость объекта; C_0 – стоимость обеспечения СФЗ в год (расходы эксплуатации); Kc – коэффициент стоимости СФЗ, связанный удаленностью критического элемента (КЭ) от караула (при Kc =0, караул находится в непосредственной близости от КЭ); Kz – коэффициент стоимости СФЗ, связанный со степенью оснащенности объекта заградительными средствами.

Для получения уравнения регрессии затрат на СФЗ и потерь от проникновения угроз формировалась полная матрица планирования эксперимента. По результатам эксперимента центральную точку плана эксперимента смещали в сторону антиградиента функции потерь (рис. 17):

$$y = b_0 - b_1 Po \uparrow + b_2 Kc \downarrow - b_3 Kz \uparrow - b_{12} PoKc + b_{13} PoKz - b_{23} KcKz + b_{123} PoKcKz.$$

Процесс моделирования автоматизирован с помощью разработанного автором программного средства (ПС № 2018619550).

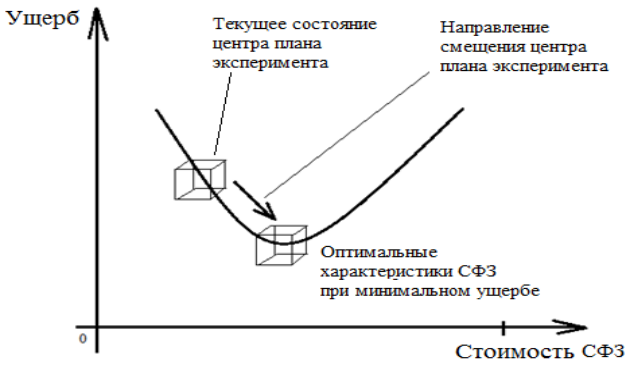


Рис. 17. Смещение в минимум потерь

Получено уравнение в точке минимума функции потерь при минимальных значениях коэффициентов, которое позволяет задать показатели эффективности подсистем СФЗ: Po, Kc и Kz. По значениям Kz и Kc определяли значения $t_н$, t_o и вероятность своевременного прибытия сил реагирования $P_{СВП}$:

$$P_{СВП} = \exp(1,7(t_H - t_0)/\sigma)/(1 + \exp(1,7(t_H - t_0)/\sigma), \quad (8)$$

где $t_н$ и t_0 – время задержки нарушителя и время прибытия сил реагирования – **решена задача № 3.**

В **пятой главе** разработана методика оптимального размещения и выбора ИТСО для типового объекта на основе формирования логических функций проникновения нарушителя на объект, которые представлены как функции условий наступления опасности в виде конъюнкции логических переменных – аргументов. Аргументы функции – ребра графа проникновения, представленные как булевы переменные, которые формировались в матрицу инцидентности, на основе которой с помощью задач о покрытии и динамического программирования (ДП) производилось оптимальное размещение ИТСО, удовлетворяющее заданным требованиям эффективности СФЗ $P_O \geq P_{O.зад}$, $P_{СВП} \geq P_{СВП.зад}$, $R_{КЗ} \geq R_{КЗ.зад}$ при минимуме затрат $C_{зат.СФЗ}(P_З) \to \min$.

Особенностью задачи является то, что необходимо обеспечить безопасность контролируемой зоны $R_{кз}$ КСИИ для исключения утечки информации по техническим каналам.

Решение задачи укладывается в последовательность этапов:

- на основе графовой модели проникновения нарушителя формировались все пути достижения цели в виде логических функций, представленных матрицей инцидентности;
- формировалось множество вариантов размещения ИТСО с помощью задачи о покрытии на матрице инцидентности;
- проводился синтез вариантов оптимального размещения ИТСО на основе задачи ДП;
- формировались дополнительные варианты покрытий для повышения показателя безопасности более важных КЭ;
- проводился синтез дополнительных вариантов размещения ИТСО, обеспечивающих повышение показателя безопасности более важных КЭ.

На первом этапе формировался сценарий проникновения нарушителя в виде разветвленного ориентированного графа (рис. 18). Цель нарушителя – достижение КЭ Y10, Y11, Y12 для совершения теракта (диверсии).

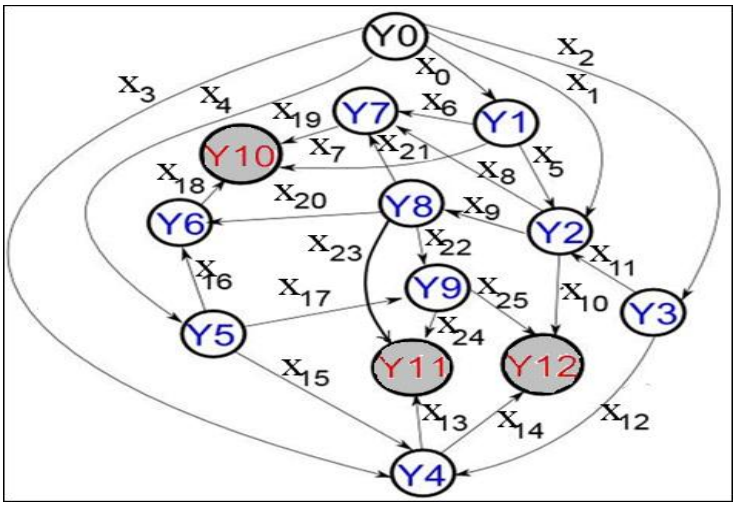


Рис. 18. Граф достижимости нарушителем цели

Пути проникновения из начальной вершины Y0 в конечные вершины Y10, Y11, Y12 определялись операцией обхода графа в глубину. Каждый путь проникновения описывается логической функцией, аргументы булевы переменные: 1 – если ребро входит в путь проникновения, 0 – не входит. Функции проникновения, сведены в матрицу инцидентности (табл. 17).

Таблица 17 – 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}	X_{22}	X_{23}	X_{24}	Xn
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
i																										
m	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

После этого решается задача оптимизации размещения ИТСО. Необходимо исключить возможность проникновения по каждому пути. Это задача нахождения минимального сечения на графе путем определения минимального покрытия на матрице инцидентности (табл. 17).

Постановка задачи о покрытии – все пути проникновения покрыть минимальным количеством ребер:

$$\sum_{j=1}^{n} X_j \to \min, \tag{9}$$

где $X_j = \begin{cases} 1 - \text{если j-е ребро входит в состав покрытия;} \\ 0 - \text{не входит.} \end{cases}$

При этом избыточность нереализованных возможностей покрывающих ребер графа стремится к минимуму:

$$\sum_{j=1}^{n} a_{ij} x_j \to \min,\ i = \overline{1,m}. \tag{10}$$

Исходные данные задаются с помощью матрицы инцидентности: $A = \|a_{ij}\|$,

где $a_{ij} = \begin{cases} 1, \text{ если } j = 1 \div n \text{ ребро входит в } i = 1 \div m \text{ путь проникновения;} \\ 0, \text{ в противном случае.} \end{cases}$

Данная задача решается методом ветвей и границ, модернизированным автором. Для оценки границ необходимо определить мощность каждого ребра:

$$W(j) = E'(j) - S(j), \tag{11}$$

где $E'(j)-$ потенциал j-го ребра:

$$E'(j) = \sum_{\forall i \in I} a_{ij},\ j \in J,\ i \in I, \tag{12}$$

где I – множество маршрутов, непокрытые ребрами,

$$S(j) = \sum_{\forall i \in I'} a_{ij}, j = (J / J_1), \tag{13}$$

где $S(j)$ – избыточность или неиспользованные возможности j-го ребра.

Модернизация заключается во введении оценки перспективной мощности j- го ребра, чтобы решение задачи быстро сходилось к конечному результату:

$$\tilde{W}(j) = W(i) - S(j), \tag{14}$$

где $W(i)$ – мощность i-го ребра, из которого производится ветвление; $S(j)$ – избыточность ребра; $\tilde{W}(j)$ – перспективная мощность j-го ребра.

Процесс решения задачи о покрытии автоматизирован с помощью разработанного автором программного средства (ПС № 2018619865).

Каждое покрытие контролирует все пути проникновения при размещении на них ИТСО и характеризуется вероятностью обнаружения, временем задержки (удаленностью) и протяженностью (затратами). Далее решается задача синтеза покрытий для оптимального размещения ИТСО, то есть необходимо на множест-

ве комбинаций покрытий определить вариант размещения, обеспечивающий заданную вероятность обнаружения с минимальной стоимостью ИТСО, которая зависит от длины покрытия. Кроме того, каждое покрытие характеризуется удалением от КЭ. Этот параметр определяет вероятность своевременного прибытия сил реагирования и обеспечения безопасности контролируемой зоны. Оптимизация заключается в минимизации общей длины (стоимости) покрытий при обеспечении заданной вероятности обнаружения и своевременного прибытия сил реагирования.

Для размещения ИТСО методом анализа иерархий определяли наиболее приемлемые типы средств охраны.

Обычно формируют два – три рубежа обнаружения и задержки продвижения нарушителя. В первую очередь в множество вариантов включаются покрытия с минимальной длиной и необходимым удалением от КЭ и КСИИ, обеспечивая $P_{СВП} \geq P_{СВП.зад}$ и $R_{КЗ} \geq R_{КЗ.зад}$. На основе решения задачи ДП определили наилучший вариант размещения ИТСО на соответствующих покрытиях (ПС № 2018661409).

Для обеспечения повышения безопасности КЭ, например, для цеха 1 (Y10) на графе проникновения нарушителя (рис. 18) с помощью алгоритма обхода графа в ширину определим маршруты (функции) проникновения только к Y10. Результаты решения сводились в матрицу инцидентности для определения дополнительного покрытия, которое не пересекалось с ранее выделенными покрытиями или 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 своевременной реакции сил реагирования и обеспечения контроля зоны $R_{КЗ}$. Решая задачу ДП для покрытий, обеспечили увеличение вероятности обнаружения КЭ Y10. Размещение покрытий показано на рис. 19 – **решена задача № 4.**

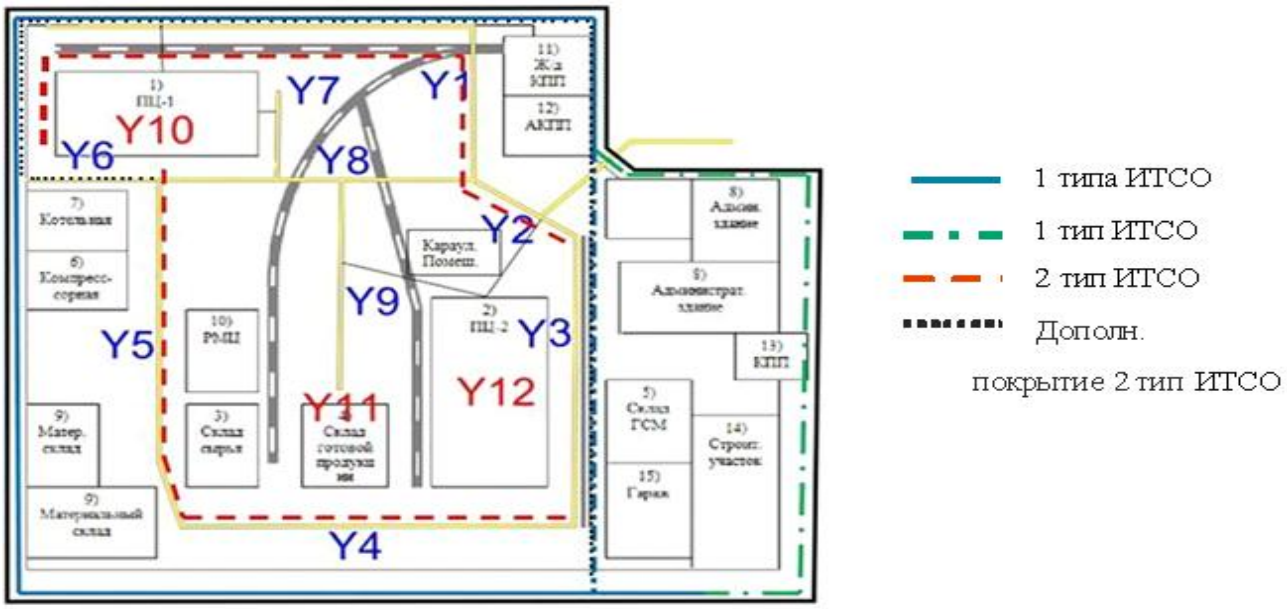


Рис. 19. Результирующие покрытия типового объекта

Разработана *методика объединения технических средств обнаружения (ТСО) в группы* для формирования структуры организационного управления с оптималь-

ной информационной нагрузкой на ее элементы. В настоящее время эта задача решается без использования критериев оптимальной информационной нагрузки.

С увеличением количества управляющих элементов организационного управления увеличиваются расходы управленческого аппарата, при этом уменьшается информационная нагрузка на ее элементы, при уменьшении управляющих элементов наоборот. То есть существует оптимальная информационная нагрузка. Величина оптимальности информационной нагрузки на элементы организационного управления определена по информационному критерию оптимальности развития систем $G_н$=0,27.

Для типового объекта проведен фрагмент формирования структуры организационного управления. Исходные данные: результаты размещения ТСО, представленные на рис. 21. Каждое ТСО имеет характеристики: опасность контролируемой зоны, удаление от КЭ, интенсивности движения в зоне ТСО, вероятность обнаружения, номер эшелона расположения ТСО и т. д., то есть имеет информационные признаки (нагрузку).

Необходимо на нижнем уровне организационного управления объединить ТСО в группы для формирования элементов организационного управления (уровень операторов). В результате объединения ТСО в группы по информационному критерию получили элементы организационного управления (рис. 20) – **решена задача № 5.**

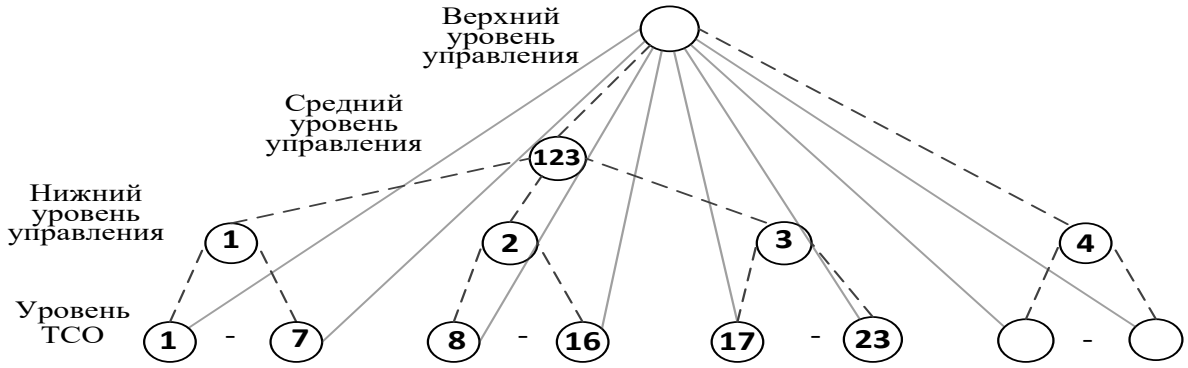


Рис. 20. Объединение ТСО в группы организационного управления операторов

В **шестой главе** разработан *метод оценки эффективности СФЗ* (оценки варианта размещения ИТСО) на основе взаимосвязанных марковских цепей, который позволяет вырабатывать решения по оптимальному изменению структуры СФЗ для повышения эффективности.

Задача оценки вероятности безопасного состояния объекта, представленная как оценка надежности системы безопасности в виде мультиграфа, декомпозируется на множество простых графов проникновения. Вероятность проникновения нарушителя по каждому маршруту оценивается с помощью двух зависимых марковских цепей.

Имеется план размещения ИТСО на объекте (рис. 21). Цель нарушителя – проникнуть в КСИИ для совершения теракта (деструктивных действий). Модель проникновения нарушителя и расположение на графе ИТСО представлена в виде разветвленного ориентированного мультиграфа (рис. 22).

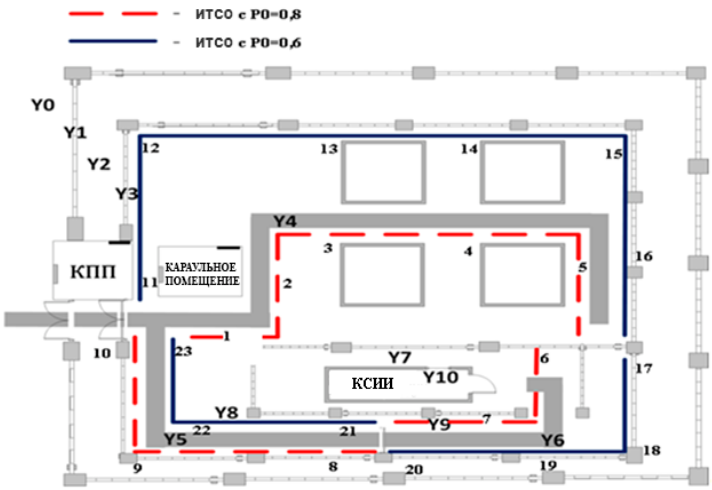
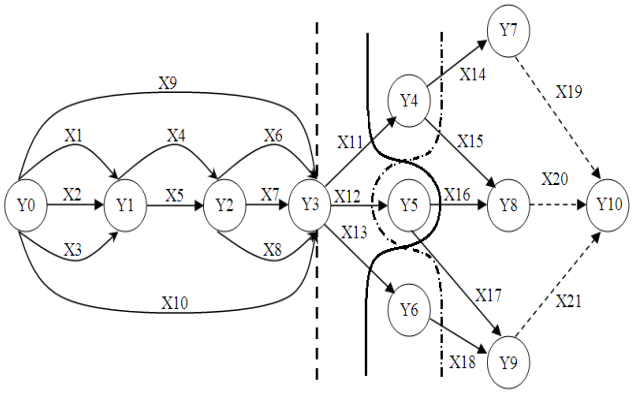


Рис. 21. Расположение ИТСО на объекте



--- граница объекта; -.- P_0=0,6; — P_0=0,8.

Рис. 22. Граф реализации цели нарушителем

Для решения задачи оценки вероятности проникновения определили с помощью композиции матрицы смежности мультиграфа все пути перемещений нарушителя из начальной вершины Y_0 в конечную Y_{10}. В результате анализа путей проникновения с учетом расположения ИТСО на графе получили матрицу инцидентности функций проникновения (табл. 18).

Таблица 18 – Инцидентность маршрутов в объекте

№ 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	0	0	1	0	0	0	0	1	0	0
2	1	0	0	0	1	0	0	0	0	1	0
3	0	1	0	0	0	1	0	0	0	1	0
4	0	1	0	0	0	0	1	0	0	0	1
5	0	0	1	0	0	0	0	1	0	0	1

Для оценки эффективности СФЗ моделировались все пути проникновения из матрицы инцидентности (таб. 18). Функционирование СФЗ описывалось двумя зависимыми марковскими цепями с дискретным состоянием и временем перехода (рис. 23).

Исходные данные: два вектора начальных состояний и две матрицы вероятностей переходов, которые формировались по результатам натурных оценок параметров перемещений типового нарушителя и сил реагирования на объекте.

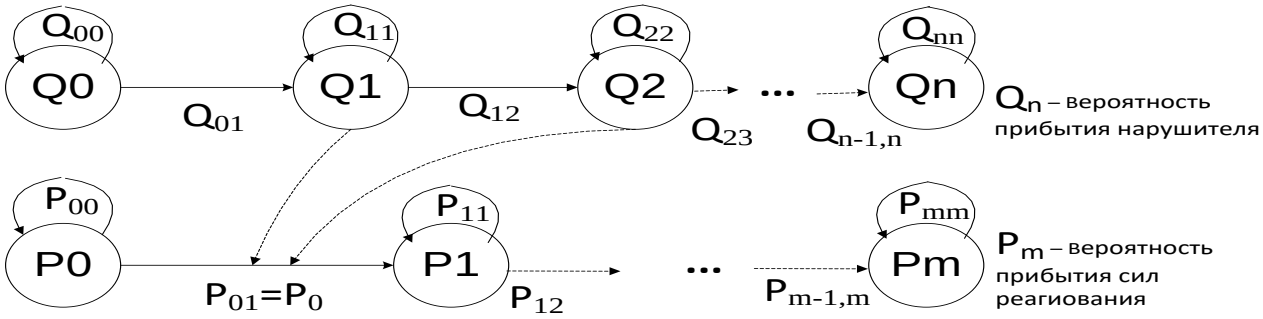


Рис. 23. Марковские цепи проникновения нарушителя и противодействия СФЗ

Первая цепь моделирует проникновение нарушителя, вторая – реакции сил реагирования на проникновение. При перемещении нарушителя вероятность вершин Q1 и Q2 увеличивается и, следовательно, динамически изменялась матрица вероятности переходов реакции СФЗ. Вероятность обнаружения P_0 определялась:

$$P_0 = 1 - \left[\left(1 - P_{1\,mco} \cdot Q_1\right) \cdot \left(1 - P_{2\,mco} \cdot Q_2\right) \right], \quad (15)$$

где $P_{1\,mco}, P_{2\,mco}$ – вероятности обнаружения техническими средствами, расположенными в вершинах Q1 и Q2 соответственно; Q_1, Q_2 – вероятности нахождения нарушителя в зоне обнаружения вершин Q1 и Q2.

Выходными данными являются вероятности наступления конечных событий Qn и Pm. Оценка вероятности защиты объекта определялась:

$$P_З = PH1 / (PH1 + PH2), \quad (16),$$

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. Процесс моделирования автоматизирован с помощью разработанного автором программного средства (ПС № 2016661765).

При неудовлетворительных оценках повышение эффективности СФЗ рассматривалось за счет структурных изменений СФЗ: увеличить расстояние обнаружения между точкой обнаружения движения нарушителя и КЭ объекта; уменьшить скорость (увеличить время) движения нарушителя за счет модернизации заградительных средств; уменьшить расстояние движения сил реагирования за счет создания коротких путей перемещения. Любые изменения структуры СФЗ связаны с затратами, поэтому использовали критерий «эффективность/стоимость». Для получения уравнения регрессии «эффективность/стоимость» проводился эксперимент на модели по перечисленным структурным изменениям и по функции отклика определяли направление изменения определяющего фактора для увеличения функции эффективность/стоимость до тех пор пока не получали уравнение регрессии (структурные параметры СФЗ), при которых выполняются требования эффективности СФЗ – **решена задача № 6.1.**

Впервые введен показатель эффективности СФЗ **–** время утечки конфиденциальной информации о функционировании СФЗ (*Ту)* и разработан метод ее оценки. Исходные данные метода **–** информационная матрица (табл. 19), в которой столбцы – коды типов информации, строки – коды носителей (исполнителей) этой информации – действующие элементы (ДЭ), поле таблицы – уровень владения информацией по семибалльной шкале: 0 – не владеет информацией, 6 – анализирует информацию, 1…5 – промежуточные значения. На основе обработки прямой и транспонированной матрицы МГК сформирована структура информации и структура ДЭ, представленная компонентами.

Таблица 19 – Информационная матрица

Код ДЭ		Код типа информации							
	101	201	202	103	-		401	501	502
10	6	3	2	6	-		2	1	1
20	3	6	6	6	-		2	1	1
-	-	-	-	-	-		-	-	-
70	2	1	2	3	-		2	2	1
50	1	1	1	2	-		5	6	6
40	1	1	0	2	-		6	3	4

Для удобства анализа от компонент перешли к двудольному графу связей ДЭ и типов информации (рис. 24), где коды заменены на действительные названия исполнителей и типов информации. На основе анализа двудольного графа сформировали граф утечки информации о функционировании СФЗ (рис. 25).

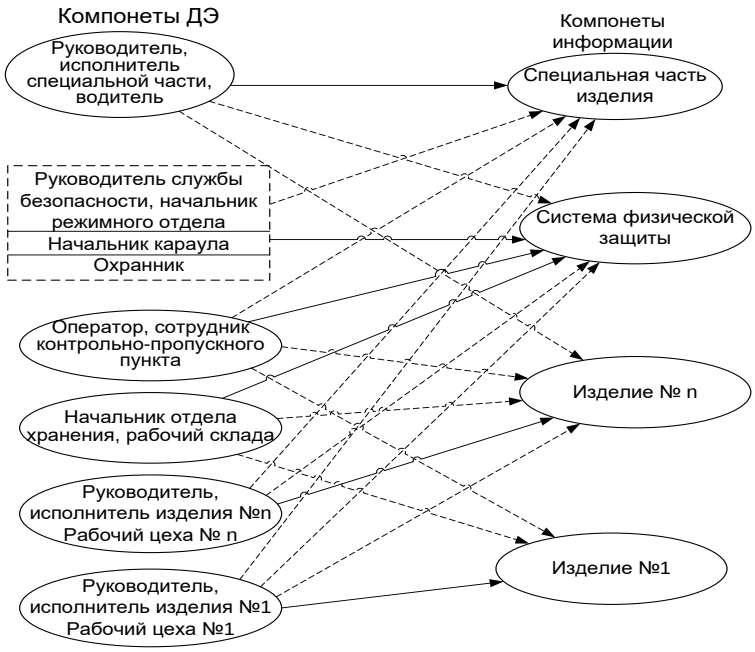


Рис. 24. Граф связей ДЭ и типов информации

Рис. 25. Граф утечки информации о СФЗ

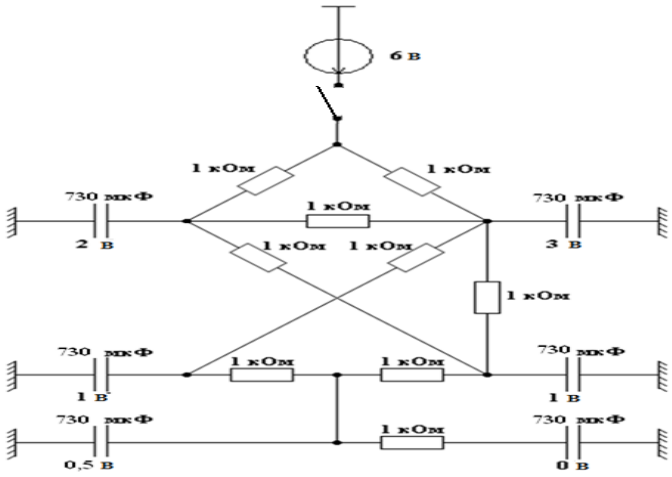


Рис. 26. Схема переходных процессов

Из-за невозможности описать марковской моделью граф утечки информации перешли к эквивалентной электрической схеме (рис. 26), на которой установлено следующее соответствие графу: вершины графа – накопительные емкости *C*, ребра графа – резистивные сопротивления *R*. Начальный заряд каждой емкости (В) – уровень владения содержанием информации о СФЗ по семибалльной шкале (табл. 19), но в единицах напряжения.

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 62 % приложенного напряжения. Заряд емкости ассоциируется с накоплением конфиденциальной информации ДЭ в графе о СФЗ. Временной интервал утечки информации (обмена информацией) между ДЭ на графе в результате их взаимодействия при выполнении технологических процессов определяется экспериментальным или экспертным путем и задается параметрами *R* и *C* переходного электрического процесса соответствующего аналогии утечки информации.

При моделировании переходного процесса с помощью ППП Proteus 8.0 получена динамика изменения заряда конденсаторов как аналог накопления информации (то есть утечки информации) о функционировании СФЗ. По результатам моделирования с помощью ИВМ, критериев Вилкоксона, знаков Фишера определялся момент наступления однородности информации в системе, то есть утечки

информации, после которого необходимо изменить информационную среду СФЗ (коды, пароли, замки и так далее). Таким образом, происходит повышение эффективности СФЗ за счет снижения потенциала опасности нарушителя из-за лишения его информированности о СФЗ (второй компоненты) – **решена задача №6.2.**

В **заключение** приведены основные итоги диссертационного исследования. В приложении приведены акты внедрения программных продуктов для ЭВМ.

ЗАКЛЮЧЕНИЕ

Главным итогом 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.

1. Проведен системный анализ технологии проектирования СФЗ и на этой основе предложены методики, модели и методы, повышающие достоверность и обоснованность принимаемых решений. Разработана формализованная постановка задачи обеспечения безопасности КВО при управлении проектированием СФЗ и методологические основы предпроектных исследований процесса разработки СФЗ с использованием нового информационного подхода и добавлением методики формирования технических средств обнаружения в группы структур организационного управления, а также методов оценки эффективности и времени утечки информации о функционировании СФЗ, направленные на повышение ее эффективности.

2. Впервые использованы информационные показатели для оценки потенциалов опасности типовых нарушителей и КВО при возникновении ЧС, а также критерий оптимального развития систем, позволяющие обоснованно производить категорирование КВО, формировать элементы организационного управления и прогнозировать временной интервал модернизации СФЗ из-за значимого изменения внешней среды.

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, а именно:

- методика категорирования КВО с использованием нелинейной энтропийной шкалы, повышающей достоверность оценки масштаба потерь и информационного критерия оптимальности развития систем, позволяющего обоснованно производить декомпозицию спектра опасности объектов на значимо отличные по энтропийному потенциалу опасности категории КВО и на этой основе определять необходимые требования безопасности для категорий КВО. Обосновано семь значимо различных по опасности категорий КВО и требования к их защищенности. На основе обработки характеристик КВО МГК интерпретировали основную компоненту – привлекательность объекта;

- оценки энтропийного потенциала опасности типовых нарушителей. Потенциал опасности внутреннего нарушителя соизмерим с потенциалом группового нарушителя. Структуру характеристик нарушителя интерпретировали двумя компонентами: физическая (техническая) и информационная подготовка;

- определения базовых нарушителей для КВО на основе формирования информации о типовых нарушителях и категорируемых объектов в единых энтропийных шкалах. Определены базовые нарушители для семи категорий КВО;

- оценки временного интервала значимого изменения активности внешней среды (нарушителей) по информационному критерию для прогнозирования периода модернизации СФЗ.

4. Предложена модель обоснования требований эффективности к подсистемам СФЗ на основе планирования эксперимента на имитационной модели функционирования СФЗ с применением градиентного метода спуска в минимум функции потерь обеспечения безопасности, новизна которой определяется обоснованием требований к критериям эффективности подсистем СФЗ: обнаружения, задержки, реагирования и нейтрализации нарушителя, так как именно эти критерии необходимы проектировщику.

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 решении задач о покрытии и динамического программирования. Метод адаптирован для критических элементов разной важности (опасности).

6. Разработана методика объединения технических средств обнаружения в группы для формирования элементов структуры 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. Метод позволяет вырабатывать оптимальные 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 информации и структуры носителей этой информации с использованием МГК и теории графов, и формирования эквивалентной аналоговой электрической схемы переходных процессов *RC* цепочек для моделирования процесса утечки информации. Метод позволяет определить момент наступления утечки информации о СФЗ для выработки решений по обновлению ее информационной среды, что способствует уменьшению информационного потенциала опасности нарушителя на 13 %.

9. По всем методам проведены вычислительные эксперименты по проектированию и исследованию эффективности СФЗ типовых объектов.

Рекомендации и перспективы дальнейшей разработки темы.

Можно рекомендовать как дальнейшее развитие темы продолжить исследования в области разработки комплекса методов, моделей и алгоритмов обоснования и разработки СФЗ КВО на основе агентно-ориентированного подхода, байесовских сетей доверия, а также использования сочетания совокупности интеллектуальных методов поддержки принятия решений в задачах построения интеллектуальных СФЗ.

ОСНОВНЫЕ ПУБЛИКАЦИИ ПО ТЕМЕ ДИССЕРТАЦИИ

Монографии.

1. 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.

Публикации в изданиях, рекомендованных ВАК РФ

2. 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.

3. 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.

4. 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.

5. 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.

6. 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.

7. 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.

8. 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.

9. 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.

10. 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.

11. 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.

12. Костин, В. Н. Методика формирования элементов структуры организационного управления систем физической защиты на основе

информационного подхода / В. Н. Костин // Труды Ин-та систем. анализа Рос. Акад. наук. – 2020. – Т. 70, № 1. – С. 30–39.

13. 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.

14. 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.

Публикации в журналах, индексируемых *в Scopus*

15. 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.

Публикации в других изданиях

16. Костин, В. Н. Вопросы математического моделирования боевых действий войсковой ПВО / В. Н. Костин // Сборник материалов военной научной конференции. – Смоленск, 1998. – С. 18–19.

17. Костин, В. Н. Разработка методического аппарата оптимизации технологических структур процесса натурной обработки сложного технического комплекса / В. Н. Костин // Тезисы докладов региональной конференции молодых ученых и специалистов. – Оренбург : Изд. центр ОГАУ, 1998. – Ч. III. – С. 101.

18. Костин, В. Н. Математическая модель функционирования войсковой ПВО / В. Н. Костин // Материалы 14-го межвузовского научно-практического семинара. – Оренбург, ФВУ ВПВО ВС РФ, 1999. – С. 13–14.

19. Костин, В. Н. Построение организационных структур предприятий / В. Н. Костин // Региональная научно-практическая конференция молодых ученых и специалистов : [тез. докл.], 12-13 окт. 1999 г., – Оренбург : Изд. центр ОГАУ, 1999. – Ч. 3. – С. 15–16.

20. Костин, В. Н. Повышение эффективности отработки сложных технических комплексов / В. Н. Костин // Современные информационные технологии в науке, образовании и практике : материалы регион. науч.-практ. конф. (с междунар. участием). – Оренбург : ГОУ ОГУ, 2003. – С. 54–56.

21. Костин, В. Н. Оптимизация технологического процесса натурной обработки сложного технического комплекса / В. Н. Костин // Перспективные информационные технологии в научных исследованиях, проектировании и обучении «ПИТ-2006» : тр. науч.-техн. конф. с междунар. участием, 29-30 июня 2006 г./ Федер. агентство по образованию Рос. Федерации [и др.]. – Самара, 2006. – Т. 1. – С. 97–101.

22. Костин, В. Н. Формирование технологических структур и упорядочение видов испытаний сложных технических комплексов / В. Н. Костин // Инновации в науке, бизнесе и образовании : сб. материалов Междунар. науч.-практ. конф. 30 окт. 2008 г., Оренбург. — Оренбург : ОГИМ, 2008. – С. 95–99.

23. Костин, В. Н. Синтез элементов системы физической защиты / В. Н. Костин // Современные информационные технологии в науке, образовании и практике: материалы IX Всерос. Науч.-практ. конф. С междунар. участием, посвящ. 55-летию Оренбург. Гос. Ун-та. – Оренбург : ОГУ, 2010. – С. 36–39.

24. Костин, В. Н. Методика формирования оптимального размещения элементов СФЗ охраняемого объекта / В. Н. Костин // Современные информационные технологии в науке, образовании и практике : материалы X Всерос. Науч.-практ. конф., 7-9 нояб. 2012 г., Оренбург. – Оренбург : Университет, 2012. – С. 60–69.

25. Костин, В. Н. Информационная оптимизация технологических процессов / В. Н. Костин // Современные информационные технологии в науке, образовании и практике : материалы XI Всерос. Науч.-практ. конф., посвящ. 80-летию Оренбург. Обл. – Оренбург : Университет, 2014. – С. 37–38.

26. Чепасов, В. Базовые параметры в многопараметрических исследованиях / В. Чепасов, М. Токарева, В. Костин. – Saarbruecken : LAP Lambert Academic Publishing. – 2014. – 328 с.

27. Костин, В. Н. Оптимизация организационной структуры систем физической защиты (СФЗ) на основе информационного подхода / В. Н. Костин, А. С. Боровский, А. Д. Тарасов // Информационные технологи и системы : тр. Пятой Междунар. науч. конф., 24-28 февр. 2016 г. – Челябинск : Изд-во Челяб. гос. ун-та, 2016. – С. 181–185.

28. Костин, В. Н. Проблемы и задачи концептуального проектирования систем физической защиты критически важных объектов / В. Н. Костин, А. С. Боровский, А. Д. Тарасов // Новые информационные технологии и системы : сб. науч. ст. XIII Междунар. науч.-техн. конф., 23-25 нояб. 2016 г., Пенза. – Пенза : Изд-во ПГУ, 2016. – С. 215–217.

29. Тарасов, А. Д. Адаптивный генетический алгоритм в задаче проектирования систем физической защиты / А. Д. Тарасов, А. С. Боровский, В. Н. Костин // Новые информационные технологии и системы: сб. науч. ст. XIII Междунар. науч.-техн. конф., 23-25 нояб. 2016 г., Пенза. – Пенза : Изд-во ПГУ, 2016. – С. 226–228.

30. Черепенин, А. Ю. Системный анализ информационных потоков оценки эффективности систем физической защиты критически важных объектов / А. Ю. Черепенин, В. Н. Костин // Материалы IV научно-практической международной конференции (школы-семинара) молодых ученых: в 2 частях, Тольятти, 23-25 апреля 2018, С. 594-600.

31. Черепенин, А. Ю. Повышение эффективности систем физической защиты по результатам ее оценки / А. Ю. Черепенин, В. Н. Костин // Сборник материалов Международной молодежной научной конференции: Оренбург, 31 октября-02 ноября 2018, С. 350-355.

32. 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.

33. Костин, В. Н. Модели и методы разработки комплексов информационной безопасности критической информационной инфраструктуры Российской Федерации / В. Н. Костин, А. С. Боровский // Информационные технологии интеллектуальной поддержки принятия решений (ITIDS 2019): тр. VII Всерос. научн. конф. (с приглашением зарубеж. ученых), 28-30 мая 2019 г., Уфа: в 3 т. – Уфа: Уфим. гос. авиац. техн. ун-т, 2019. – Т. 2. – С. 210–213.

34. 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.

35. 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.

Свидетельства о регистрации программ для ЭВМ

36. 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.

37. Программное средство синтеза Марковских моделей оценки эффективности систем физической защиты потенциально опасных объектов : свидетельство 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.

38. Прикладная программа. Оценка эффективности системы физической защиты на основе Марковских моделей. / С.А. Щелоков, В.Н. Костин, С.А. Черепенин // Министерство образования и науки РФ, ФГБО ВО «Оренбургский государственный университет». – Оренбург: ОГУ. – 2017. – 7с. № 1367 от 03.04.2017.

39. Имитационная модель функционирования системы физической защиты: свидетельство 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.

40. Решение задачи о покрытии на графе вариантов проникновения системы физической защиты: свидетельство 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.

41. 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». –№ 2018661409; заявлено 03.08.2018; зарегистрировано в Реестре программ для ЭВМ 07.09.2018. – 1 с.