МИНИСТЕРСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ
ПО ДЕЛАМ ГРАЖДАНСКОЙ ОБОРОНЫ, ЧРЕЗВЫЧАЙНЫМ
СИТУАЦИЯМ И ЛИКВИДАЦИИ ПОСЛЕДСТВИЙ
СТИХИЙНЫХ БЕДСТВИЙ

Академия Государственной противопожарной службы МЧС России

На правах рукописи

Рябцев Николай Алексеевич

АВТОМАТИЗАЦИЯ СБОРА И ОБРАБОТКИ ДАННЫХ В СИСТЕМЕ ОХРАННО-ПОЖАРНОЙ СИГНАЛИЗАЦИИ ПРОМЫШЛЕННОГО ОБЪЕКТА НА ОСНОВЕ КЛАССИФИЦИРОВАННЫХ ИЗВЕЩАТЕЛЕЙ

Специальность: 05.13.06 – Автоматизация и управление технологическими процессами и производствами (технические науки, отрасль – промышленность)

ДИССЕРТАЦИЯ
на соискание ученой степени
кандидата технических наук

Научный руководитель:
доктор технических наук, профессор,
заслуженный работник высшей школы
Российской Федерации
Членов Анатолий Николаевич

Москва – 2020

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Актуальность и степень проработанности темы исследования

Безопасность промышленных объектов нефтяной и газовой промышленности является одним из основных условий успешного функционирования и развития нефтегазового комплекса. Достижение безопасности предполагает, прежде всего, безаварийную работу технологического оборудования, пожарную безопасность, а также противокриминальную и антитеррористическую защиту промышленных объектов.

Важность формирования эффективной системы безопасности подтверждено Распоряжением Правительства Российской Федерации от 15 мая 2017 № 928-р (ред. от 10 сентября 2019 г.) [1], в котором утвержден перечень объектов, подлежащих обязательной охране войсками национальной гвардии Российской Федерации. В этом перечне в качестве приоритетных указаны промышленные объекты ОАО «Грознефтегаз» в Чеченской Республике и ОАО «РН Ингушнефть» в Республике Ингушетия.

К одним из наиболее уязвимых относятся потенциально опасные промышленные объекты нефтегазодобычи, особенность которых состоит не только в большом количестве технологических установок, представляющих повышенную опасность, но и в наличии значительной территории, где эксплуатируется такое оборудование. В связи с этим цехи добычи нефти и газа (ЦДНГ) и их комплексной подготовки подлежат надежной защите с помощью автоматизированных интегрированных систем на основе эффективных средств охранно-пожарной сигнализации.

Вместе с тем существенную проблему представляет формирование системы охранно-пожарной сигнализации, в полной мере соответствующей характеру технологического процесса и условиям его реализации на промышленном объекте. Особенность современного этапа развития техники состоит в том, что при видимом насыщении рынка охранными извещателями

и модулями, они зачастую не отвечают требованиям эффективности, надежности и живучести для применения на потенциально опасных и критически важных промышленных объектах.

С введением системы классификации автоматических средств обнаружения для охраны особо важных объектов необходимы извещатели, обладающие дополнительными специальными функциями и структурой формируемых ими извещений. Поскольку при этом неизбежно возрастают стоимостные параметры системы сбора и обработки данных, возникает проблема выбора составляющих ее технических средств.

Следовательно, в условиях значительного повышения технической оснащенности и подготовленности лиц, совершающих противоправные действия криминальной и террористической направленности, активно противодействующих нормальному функционированию систем охранно-пожарной сигнализации, требуются исследования, разработка и производство новых видов извещателей с повышенной эффективностью обнаружения, а также рекомендаций по выбору оптимального состава модульных структур сбора и обработки данных.

Информационной базой для исследований в данной области может служить вневедомственная охрана Росгвардии, имеющая возможность получения достоверных данных о функционировании систем централизованной охраны около 2-х миллионов объектов различного назначения. При этом более 95% объектов оборудовано системами охранно-пожарной сигнализации.

Вопросам повышения эффективности систем охраны и пожарной безопасности объектов посвящено значительное количество научных исследований. Широко известны в данной области работы Топольского Н. Г., Шепитько Г. Е., Бутузова С. Ю., Членова А. Н., Зарубина В. С., Волхонского Н. Н., Козьминых С. И., Крахмалева А. К., Зайцева А. Г., Климова А. В., Серезевского А. В., Буцынской Т. А., *Pigott S.*, *Walker Ph.* и ряда других ученых в России и за рубежом.

Вместе с тем интенсивное развитие электронной техники и технологий с учетом напряженной криминогенной обстановки требует постоянного совершенствования научно-технического обеспечения формирования систем безопасности объектов.

Таким образом, острая необходимость в совершенствовании системы охранно-пожарной сигнализации промышленного объекта на основе классифицированных извещателей с повышенной эффективностью обнаружения определяет актуальность темы диссертации.

Объект исследования – автоматизированные интегрированные системы безопасности потенциально опасных промышленных объектов на примере цехов добычи нефти и газа.

Предмет исследования – система охранно-пожарной сигнализации потенциально опасного промышленного объекта.

Цель – совершенствование автоматизации сбора и обработки данных в системе охранно-пожарной сигнализации потенциально опасного промышленного объекта на основе классифицированных извещателей с повышенной эффективностью обнаружения.

Практическая реализация данной цели вносит значительный вклад в повышение безопасности предприятий нефтяной и газовой промышленности.

Задачи исследования

1. Провести анализ современного состояния безопасности и основных задач совершенствования системы охраны и пожарной безопасности потенциально опасного промышленного объекта.

2. Провести анализ параметров эффективности обнаружения проникновения нарушителя, надежности и живучести централизованной охранно-пожарной сигнализации на этапе эксплуатации.

3. Разработать математическую модель и методику оценки эффективности обнаружения несанкционированного проникновения на охраняемый объект.

4. Разработать предложения по оптимальному проектированию модулей сбора и обработки данных, а также их эффективному применению в системе охранно-пожарной сигнализации потенциально опасного промышленного объекта.

Работа выполнена в соответствии с:

- Концепцией развития вневедомственной охраны войск национальной гвардии Российской Федерации на период 2018 – 2021 гг. и далее до 2025 года, утвержденной приказом Росгвардии от 7 марта 2018 года № 72 [2];

- Планами научно-исследовательских и опытно-конструкторских работ Академии ГПС МЧС России и ФКУ «НИЦ «Охрана» Росгвардии на 2015 – 2019 гг.

Методы исследований

Для решения поставленных задач использованы методы теории вероятностей и математической статистики, кластерный анализ, методы математического моделирования и анализа, эксперимент.

Научная новизна работы заключается в:

1. Разработке комплексного показателя, характеризующего уровень безопасности объекта от угроз криминального проникновения нарушителя, пожара и техногенной аварии, учитывающего взаимное влияние систем безопасности и управления технологическим процессом промышленного предприятия.

2. Разработке математической модели, определяющей риск несанкционированного проникновения на охраняемый промышленный объект, и методики ее применения при проектировании системы охранно-пожарной сигнализации для снижения опасности совершения противоправных действий и их последствий для людей, технологического оборудования и материальных ценностей.

3. Разработке методики оптимального проектирования модулей сбора и обработки данных на основе метода динамического программирования, обеспечивающего минимизацию затрат на расширение функциональных возможностей разрабатываемых технических средств.

Достоверность научных результатов и выводов, приведенных в диссертации, подтверждается применением современных апробированных методов исследования, значительным объемом данных для статистического анализа, практическими результатами испытаний и применения разработанных технических средств.

Апробация результатов работы

Основные результаты работы доложены и получили одобрение на 10 научно-практических конференциях:

Международной научно-технической конференции «Системы безопасности» – Москва, Академия ГПС МЧС России, 2015 – 2019 гг. [3-12];

Научно-практической конференции «Технические средства охраны для обеспечения комплексной безопасности объектов и территорий государства: проблемы и перспективы развития», Москва, «Интерполитех», 2016 – 2018 гг. [13, 14];

Одиннадцатой Всероссийской научно-технической конференции «Современные охранные технологии и средства обеспечения комплексной безопасности объектов», Пенза, НИКИРЭТ, 2016 г. [15];

Восьмой научно-технической конференции молодых ученых и специалистов «Проблемы техносферной безопасности» – Москва, Академия ГПС МЧС России, 2019 г. [16, 17].

Теоретическая значимость

Разработаны математические модели и предложены научно обоснованные методики, расширяющие методологическую основу проектирования систем охранно-пожарной сигнализации в составе автоматизированной системы управления промышленного производства.

Практическая ценность и значимость работы заключается в возможности использования полученных результатов на этапах разработки, проектирования и эксплуатации технических средств и систем охранно-пожарной сигнализации для оптимизации функциональной структуры, тактико-технических характеристик и стоимости, повышения их эффективности, надежности и живучести.

С целью формирования технического обеспечения сбора и обработки данных в автоматизированной системе охранно-пожарной сигнализации промышленного объекта:

1. Разработан и защищен патентом Российской Федерации на полезную модель [18] магнитоконтактный охранный извещатель с повышенной защитой от саботажа путем установки сторонних магнитов с внешней или внутренней стороны блокируемой строительной конструкции.

2. Разработан и внедрен в серийное производство комплекс модернизированных извещателей, обладающих повышенными тактико-техническими характеристиками для применения в составе систем охранно-пожарной сигнализации на потенциально опасных и критически важных промышленных объектах.

3. Разработаны нормативно-технические и методические документы по выбору и применению классифицированных технических средств сбора и обработки данных в системе охранно-пожарной сигнализации в зависимости от степени важности и уровня потенциальной опасности защищаемых объектов [19-24].

Реализация результатов работы

Результаты диссертационной работы использованы:

- в научных исследованиях ФКУ «НИЦ «Охрана» Росгвардии и Академии ГПС МЧС России по совершенствованию систем охраны и пожарной безопасности важных объектов;

- в учебном процессе Академии ГПС МЧС России при подготовке магистерских диссертаций, а также в ФКУ «НИЦ «Охрана» Росгвардии при организации дополнительного профессионального образования и повышении квалификации военнослужащих (сотрудников) Росгвардии;

- при разработке и внедрении в серийное производство на базе предприятия ЗАО «РИЭЛТА» извещателей с повышенной эффективностью обнаружения;

- при разработке нормативно-технических и методических документов, обеспечивающих качественное проектирование и эксплуатацию систем охранно-пожарной сигнализации объектов.

Положения, выносимые на защиту:

1. Комплексный показатель уровня безопасности объекта от угроз криминального проникновения нарушителя, пожара и техногенной аварии, учитывающее взаимное влияние систем безопасности и управления технологическим процессом промышленного предприятия.

2. Математическая модель, определяющая риск несанкционированного проникновения на охраняемый промышленный объект, и методика ее применения для снижения опасности совершения противоправных действий и их последствий для людей, технологического оборудования и материальных ценностей.

3. Методика оптимального проектирования модулей сбора и обработки данных на основе метода динамического программирования, обеспечивающая минимизацию затрат на расширение функциональных возможностей разрабатываемых технических средств.

Публикации

По тематике диссертации опубликовано 25 работ, в том числе 9 научных статей в рецензируемых журналах из перечня изданий, рекомендованных ВАК, 15 докладов на конференциях, 1 патент Российской Федерации на полезную модель, 6 работ опубликовано без соавторов.

Личный вклад автора

В работах, опубликованных в соавторстве в изданиях, рекомендованных ВАК, все результаты, составляющие научную новизну и выносимые на защиту, получены автором лично.

Структура и объем диссертации

Диссертация состоит из введения, четырех разделов, заключения, списка сокращений, списка литературы из 105 наименований и 4 приложений. Общий объем диссертации составляет 189 страниц машинописного текста, включая 29 таблиц и 39 рисунков.

1 СОСТОЯНИЕ И ОСНОВНЫЕ ЗАДАЧИ СОВЕРШЕНСТВОВАНИЯ СБОРА И ОБРАБОТКИ ДАННЫХ В АВТОМАТИЗИРОВАННОЙ СИСТЕМЕ ЦЕНТРАЛИЗОВАННОЙ ОХРАНЫ ПРОМЫШЛЕННОГО ОБЪЕКТА

1.1 Описание особенностей промышленного объекта и технологического процесса добычи и комплексной подготовки нефти

На территории Российской Федерации расположено более 300 тысяч опасных производственных объектов различного типа и различной формы собственности, в том числе более 8 000 взрывоопасных и пожароопасных объектов, к которым в соответствии с Федеральным законом от 21.07.1997 № 116-ФЗ «О промышленной безопасности опасных производственных объектов» [25] являются предприятия или их цехи, участки, площадки, а также иные производственные объекты, на которых получаются, используются, перерабатываются, образуются, хранятся, транспортируются, уничтожаются опасные воспламеняющиеся, окисляющиеся, горючие, взрывчатые, токсичные и высокотоксичные вещества, а также вещества, представляющие опасность для окружающей природной среды.

Особое внимание как объекты защиты представляют промышленные объекты нефтяной и газовой отрасли (НГК), в частности производственные объекты нефтедобычи, т. к. они расположены на значительной территории со сложной конфигурацией, на которой функционируют ЦДНГ с технологическими установками и оборудованием для разделения нефтепродуктов от примесей, резервуары для приема нефтепродуктов, а также административные здания (рисунок 1.1). Для обеспечения пропускного режима при транспортировке нефтепродуктов на территории охраняемого промышленного объекта, в частности ЦДНГ, необходимо наличие въездных ворот

для проезда автотранспорта и прохода сотрудников с оборудованным контрольно-пропускным пунктом (КПП). Периметр территории должен быть защищен каменным ограждением с колючей проволокой. Кроме того, на объекте должна быть сформирована система безопасности.

Рисунок 1.1 – Территория промышленного объекта НГК

При этом необходимо отметить, что к взрывоопасным производствам относятся объекты нефтегазового комплекса, химической, горнорудной и металлургической промышленностей, объекты оборонно-промышленного комплекса Российской Федерации и многие другие, т. к. опасность возгорания и взрыва несут в себе самые различные технологические процессы на производстве.

Для оценки уровня опасности ЦДНГ необходимо рассмотреть основы современного технологического процесса добычи и комплексной подготовки нефти (таблица 1.1) [26-29].

Таблица 1.1 – Основные этапы технологического процесса добычи и комплексной подготовки нефти

Наименование участка	Технологический процесс, происходящий на участке
Устье добывающих скважин – групповые замерные установки (ГЗУ)	Перекачка продукции скважин в виде трехфазной смеси (нефть, газ, вода) по отдельным трубопроводам до узла первичного замера и учета продукции
ГЗУ – дожимные насосные станций (ДНС)	Разделение продукции скважин на жидкую и газовую фазы (первая ступень сепарации)
ДНС – газосборная сеть (ГСС)	Отбор нефтяного газа из булитов (емкостей), являющихся первой ступенью сепарации, под давлением узла сепарации в газосборную сеть.
ДНС – установки комплексной подготовки нефти (УКПН)	Отбор и транспортировка продукта добычи
ДНС – установка предварительного сброса воды (УПСВ)	Доочистка воды до необходимого качества
УПСВ – кустовая насосная станция (КНС)	Подача силовыми насосами отделившейся воды необходимого качества и количества из емкостей УПСВ (отстойных аппаратов) на КНС для нагнетания в пласт
УКПН – узел подготовки воды	Отделение и очистка водной фазы на первой ступени, разделение и разрушение эмульсии промежуточного слоя, которая накапливается в резервуарах товарного парка – на второй
Узел подготовки воды – КНС	Транспортировка водной фазы с узла подготовки воды по отдельному трубопроводу до кустовой насосной станции
КНС – нагнетательная скважина (пласт)	Закачка очищенной от механических примесей и нефтепродуктов сточной воды силовыми насосами КНС в нагнетательную скважину и далее в пласт

На этапе комплексной подготовки нефти происходит разделение добытого сырья на нефть и газ в сепараторах нефти и газа, т. к. не переработанная

нефть, содержит различные примеси, например воду, соль, песок, частицы грунта, попутный нефтяной газ. Наличие в сырье механических примесей и воды мешает транспортированию нефти по нефтепродуктопроводам для ее дальнейшей переработки, вызывая образование отложений в теплообменных аппаратах и других емкостях.

На первой ступени сепарации на ДНС производится дегазация нефти с целью:

1. получения нефтяного газа, который используется как химическое сырье или как топливо;

2. уменьшения перемешивания нефтегазового потока и снижения за счет этого гидравлических сопротивлений;

3. уменьшения пенообразования;

4. уменьшения пульсаций давления в трубопроводах при дальнейшем транспорте нефти от сепараторов первой ступени до УКПН.

При этом сепарация газа от нефти начинается, как только внешнее давление снижается до давления насыщения, что может произойти в пласте, в стволе скважины или в трубопроводах. С уменьшением внешнего давления выделение газа из нефти увеличивается. Выделившийся газ стремится в сторону пониженного давления: в пласте – к забою скважины, в скважине – к ее устью и далее в нефтегазовый сепаратор.

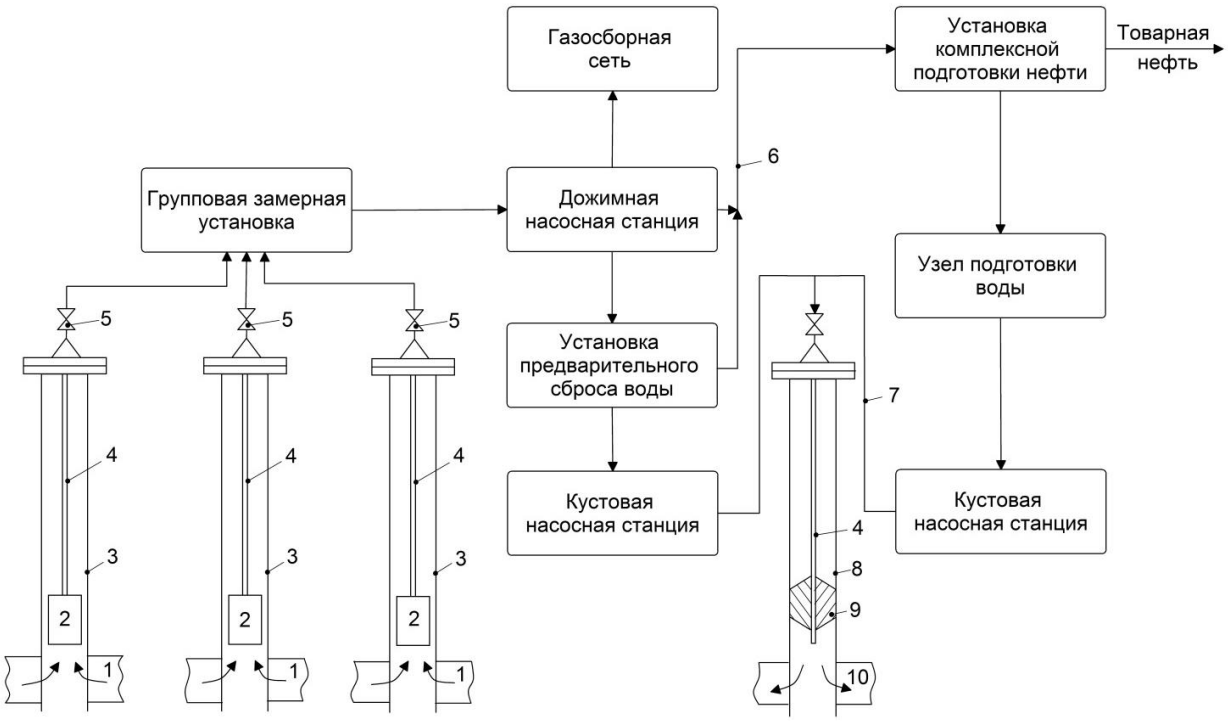
Зачастую нефть и вода образуют труднорастворимую гидрофильную или гидрофобную эмульсию, в которой мельчайшие капли одной жидкости распределены в другой во взвешенном состоянии.

На УПСВ для уменьшения коррозии трубопроводов и получения высоких показателей работы УКПН нефть, добываемая на месторождении, проходит сепарацию и предварительное обезвоживание с применением предварительного сброса пластовой воды. После сепараторов она поступает в отстойные аппараты, где происходит расслоение эмульсии. Затем частично обезвоженная нефть поступает на конечную сепарационную установку, где производится отбор газа в газосборную сеть при более низком давлении

и направляется на УКПН. Подготовленная вода направляется на КНС для закачки в пласт для поддержания пластового давления.

На УКПН нефть с целью защиты оборудования от воздействия комбинированной коррозии, предотвращения отложений в змеевиках печей и теплообменниках подвергают обессоливанию на специальных электрообессоливающих установках, в процессе которого из нефти удаляются хлористые соли, вода и механические примеси, а также металлоорганические соединения никеля, ванадия и других металлов. Вместе с ними удаляются, в частности, соединения мышьяка, отравляющего платиновый катализатор риформинга.

Структурная схема технологического процесса сбора и комплексной подготовки нефти представлена на рисунке 1.2.



1 – продуктивный пласт; 2 – насос; 3 – обсадная колонна; 4 – насосно-компрессорные трубы; 5 – устье добывающей скважины; 6 – нефтесборный коллектор; 7 – нагнетательный трубопровод; 8 – обсадная колонна нагнетательной скважины; 9 – пакер; 10 – пласт

Рисунок 1.2 – Структурная схема технологического процесса сбора и комплексной подготовки нефти

Дальнейшая обработка заключается в разделении подготовленной нефти, состоящей из смеси нафтеновых, парафиновых, ароматических углеводов с различным молекулярным весом и температурой кипения, сернистых, кислородных и азотистых органических соединений на фракции и группы углеводородов при первичной перегонке (ректификации, вакуумной дистилляции).

Рассмотрим основные особенности технологического процесса добычи и комплексной подготовки нефтепродуктов в ЦДНГ, а также объектов, находящихся на его территории и нуждающихся в комплексной охране и защите от несанкционированных проникновений и террористических атак, а также факторы, способствующие возникновению и развитию аварийных ситуаций при протекании данных технологических процессов:

- наличие большого количества нефтепродуктов, являющихся взрывопожароопасными веществами, а также веществами, опасными для окружающей среды;

- достаточно высокая упругость паров при рабочих температурах, которая может привести к значительной концентрации паров нефти в воздухе рабочей зоны при испарении;

- опасность разгерметизации трубопроводов в процессе транспортировки опасных веществ под давлением;

- возможное повышение давления в технологическом объекте выше допустимого, создающее дополнительную опасность разгерметизации системы;

- коррозионная активность нефти, создающая опасность разгерметизации системы;

- размещение насосов непосредственно под основным оборудованием – аппаратами воздушного охлаждения.

1.2 Комплексная оценка уровня безопасности промышленного объекта

Состав системы безопасности объекта может быть различным и зависит от характера функционирования объекта и требований, предъявляемых к уровню его защиты. Для критически важных промышленных объектов, имеющих сложную структуру, характерно ограничение доступа посторонних лиц и персонала в отдельные помещения, наличие телевизионных систем как внутреннего, так и наружного наблюдения, организация охраны и контроля пожарной обстановки.

Системы охраны, пожарной безопасности, контроля и управления доступа, телевизионного наблюдения должны иметь в своем составе собственные локальные сети передачи данных, собственные программно-технические средства, а также собственную структуру управления. Вместе с тем при комплексном проявлении угроз объекту существует необходимость взаимодействия отдельных систем [30]. Кроме того, в алгоритмах функционирования этих систем имеется много общего. В связи с этим целесообразным технически реализуемым вариантом является интеграция данных систем в системе безопасности [31].

Интеграция позволяет минимизировать капитальные затраты на оснащение объекта за счет уменьшения аппаратной части при исключении дублирующей аппаратуры в разных системах, а также текущие затраты за счет оптимизации штата охраны, снижения расходов на техническое обслуживание при эксплуатации. Расчеты показывают, что экономия может достигать 30% общих затрат. Кроме этого, интеграция позволяет улучшить тактико-технические характеристики всей системы за счет уменьшения времени поступления и увеличения полноты информации о состоянии объекта, увеличения защищенности самой системы от несанкционированного доступа к аппаратуре и базам данных, возможности создания гибких логических структур.

Следует отметить, что обеспечение безопасности объектов от преступных посягательств и пожара на основе эффективных средств сигнализации является одним из наиболее актуальных направлений развития автоматизированных интегрированных систем безопасности (ИСБ).

В настоящее время на крупном промышленном объекте формируются различные системы, обеспечивающие безопасность работы предприятия, которые могут функционировать самостоятельно или быть интегрированы в каких-либо частях, например организационной и (или) технической. Однако, учитывая в большинстве случаев комплексный характер возникающих угроз и их проявлений, как правило, существует взаимное влияние на качество функционирования систем безопасности и управления технологическим процессом [32, 33].

На рисунке 1.3 представлена структурная схема, характеризующая безопасность промышленного объекта от возможных характерных угроз, создаваемых в результате проникновения нарушителя, пожара и (или) техногенной аварии.

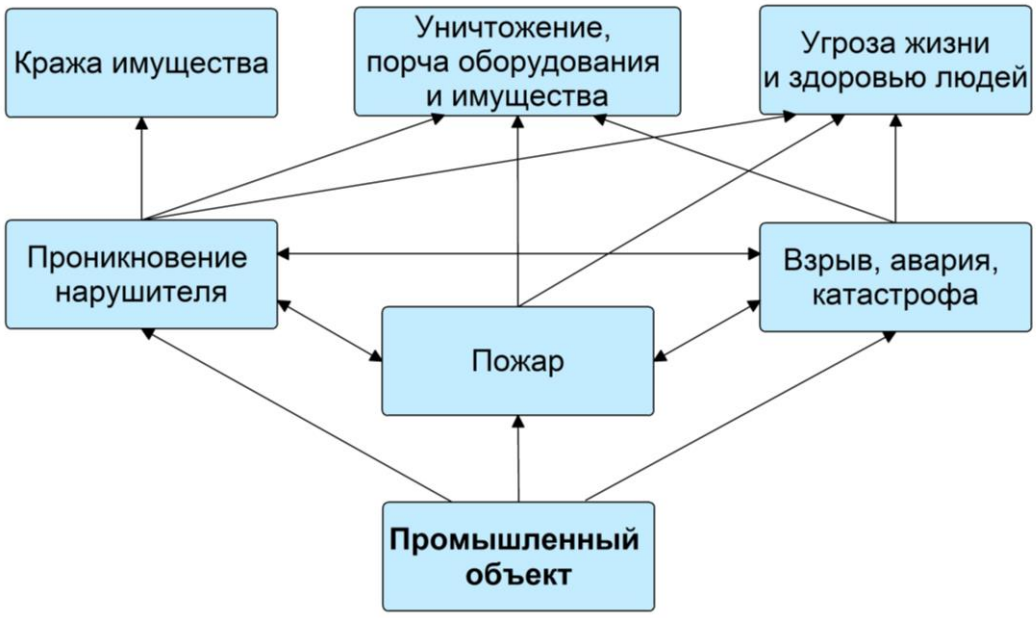


Рисунок 1.3 – Дерево вероятных угроз промышленному объекту

С учетом вышесказанного, представляет интерес комплексная оценка уровня безопасности промышленного объекта от возможных характерных угроз, создаваемых в результате проникновения нарушителя, пожара и (или) техногенной аварии [11, 34].

При формировании комплексного показателя необходимо иметь в виду следующее [35]:

- ни одна из прямых угроз не может иметь приоритет, то есть защита от каждой из них должна быть достаточной и ошибки в обеспечении безопасности объекта от одной угрозы не могут компенсироваться за счет избыточной защиты от другой;

- угрозы могут носить комплексный характер;

- показатель должен быть устойчив к небольшим изменениям параметров, вызванным погрешностью их определения или изменением условий с течением времени.

Сформированный комплексный показатель уровня безопасности промышленного объекта $U(B_i)$ имеет вид аддитивной свертки частных показателей безопасности B_i [5, 36-38].

$$U(B_i) = \sum_{i=1}^{3} \alpha_i B_i > 0, \quad \text{при} \quad B_i > 0. \qquad (1.1)$$

где i – вид опасности промышленному объекту (i = 1 – пожар; i = 2 – проникновение нарушителя; i = 3 – техногенная опасность); α_i – весовые коэффициенты.

На основе принципа справедливой компенсации абсолютных значений нормированных частных показателей комплексный показатель может быть представлен как взвешенная сумма частных показателей B_i в методе равномерной оптимизации. С учетом определенных выше условий весовые коэффициенты α_i должны быть равны друг другу и в сумме составлять единицу.

Уровень безопасности от каждой угрозы может быть определен как разница между допустимым и расчетным уровнем опасности с учетом коэффициента запаса на флуктуацию параметров.

$$B_i = K_{\text{зп}i} O_{\text{д}i} - O_i, \qquad (1.2)$$

где i – вид опасности промышленному объекту, i = 1 – пожар; i = 2 – проникновение нарушителя; i = 3 – техногенная опасность.

Для промышленного объекта в соответствии с рисунком 1.3 могут быть выделены следующие виды опасности:

$O_{\text{п}}$, $O_{\text{нп}}$, $O_{\text{т}}$ – уровень опасности пожара, проникновения нарушителя и техногенная опасность соответственно;

$O_{\text{пд}}$, $O_{\text{нпд}}$, $O_{\text{тд}}$ – допустимый уровень опасности пожара, проникновения нарушителя и техногенной опасности соответственно;

$K_{\text{зп}}$, $K_{\text{знп}}$, $K_{\text{зт}}$ – коэффициенты запаса допустимой опасности пожара и проникновения нарушителя соответственно.

$O_{\text{п}}$ может быть определена как отношение фактора пожарной опасности к фактору пожарной защиты объекта [35]:

$$O_{\text{п}} = F_{\text{п}} A_{\text{с}} A_{\text{п}} / F_{\text{з}}, \qquad (1.3)$$

где $F_{\text{п}}$ – фактор потенциальной пожарной опасности, определяемый наличием и количеством пожарной нагрузки, ее горючестью и способностью дымообразования, этажностью или высотой помещения, размерами и формой площади объекта;

$A_{\text{с}}$ – фактор случайной активации пожара, отражающий вероятность возникновения пожара, связанную с видом помещения и характером деятельности в нем;

$A_{\text{п}}$ – фактор умышленной активации пожара, отражающий возможность поджога;

$F_{\text{з}}$ – фактор пожарной защиты объекта, отражающий выполнение общих (нормативных), специальных (в том числе пожарная автоматика) и строительных защитных мероприятий.

Количественная оценка $O_{\text{п}}$ может быть получена на основе метода Гретенера, определяющего пожароопасность помещений различного назначения [39, 40]. Данный метод адаптирован специалистами к российским условиям с учетом действующих нормативов. Для определения численных значений факторов имеются соответствующие таблицы.

По аналогии $O_{нп}$ может быть определена как отношение фактора опасности несанкционированного проникновения к фактору защиты объекта:

$$O_{нп} = Q_к\, Q_и / Q_з, \qquad (1.4)$$

где $Q_к$ – криминогенный фактор, связанный с месторасположением объекта и его посещаемостью, а также уровнем криминальной обстановки;

$Q_и$ – фактор возможного использования нарушителем для проникновения на объект инициированного пожара, взрыва, аварии и т. п.

$Q_з$ – фактор защиты объекта, определяемый видом и способом организации охраны, наличием и количеством рубежей систем сигнализации и технических средств защиты, в том числе для активного противодействия проникновению, наличием дополнительных специальных систем безопасности (контроля и управления доступом, видеоконтроля и др.);

$O_{нпд}$ – максимальное допустимое значение фактора опасности проникновения, определяемое значимостью объекта и стоимостью постоянно или временно находящихся на нем оборудования и материальных ценностей.

$O_т$ может быть определена как отношение фактора опасности аварии к фактору технологической защиты промышленного объекта:

$$O_т = G_п\, C_с\, C_п / G_з, \qquad (1.5)$$

где $G_п$ – фактор потенциальной опасности аварии, определяемый характером технологического процесса, наличием и количеством обращающихся в нем взрывопожароопасных веществ, состоянием технологического оборудования;

$C_с$ – фактор случайного возникновения аварии, отражающий вероятность возникновения аварийной ситуации, связанную с технологическим процессом;

$C_п$ – фактор создания аварийной ситуации, связанной с внешними причинами, в том числе умышленными действиями нарушителя;

$G_з$ – фактор технологической защиты объекта, отражающий наличие и эффективное функционирование систем автоматического регулирования, противоаварийной защиты и взрывозащиты.

Коэффициенты запаса $K_{зп}$, $K_{знп}$, $K_{зт}$ определяют меру устойчивости комплексного показателя безопасности.

Исходя из выражений (1.2) – (1.4), коэффициенты $A_п$, $Q_и$, $C_п$ учитывают роль взаимного влияния систем безопасности и управления технологическим процессом промышленного предприятия на значение комплексного показателя безопасности.

Количественные значения факторов могут быть определены с помощью известных методик, в результате статистических исследований или экспертным путем.

В результате расчета определяют значение уровня безопасности объекта. Условие достаточной безопасности могут быть сформулированы в виде:

$$U(B_i) > 0, \text{ при } B_i > 0. \qquad (1.6)$$

Отрицательное значение любого слагаемого указывает на недостаточную защищенность объекта от одного из видов угроз. Отрицательное значение нескольких слагаемых также недопустимо.

Применение на практике предложенного критерия позволяет оценить реальное состояние объекта, определить потенциальную опасность проявления угроз, определить необходимые мероприятия для обеспечения защиты, оценить пригодность объекта для использования по новому назначению, а также определить тарифы для страхования от возможного ущерба.

Кроме этого, данный метод позволяет оценить влияние проводимых мероприятий на уровень безопасности объекта. Проведем такую оценку для случая выбора варианта применения различных систем охранной и пожарной сигнализации.

Из представленного выше описания видно, что влияние систем сигнализации на уровень безопасности учтено в коэффициентах $F_з$ и $Q_з$. Оно может быть представлено в явном виде следующим образом. Для пожарной составляющей:

$$F_з = H_п N_о T_{пт} S_{пс}, \qquad (1.7)$$

где $H_п$ – показатель, отражающий выполнение нормативных мероприятий

по обеспечению пожарной безопасности;

$N_о$ – показатель, отражающий исполнение строительных конструкций по огнестойкости;

$T_{пт}$ – показатель, характеризующий наличие и тип установок автоматического пожаротушения и систем дымоудаления, организацию, месторасположение, силы и средства пожарных подразделений, обслуживающих объект;

$S_{пс}$ – показатель, учитывающий наличие на объекте технических средств обнаружения пожара, наличие и виды средств передачи сигнала тревоги в пожарную службу.

Для охранной составляющей коэффициент $Q_з$ можно представить в виде:

$$Q_з = N_з\, T_з\, S_{ос}, \qquad (1.8)$$

где $N_з$ – параметр, отражающий вид и способ организации охраны;

$T_з$ – коэффициент, зависящий от применяемого комплекса технических защитных мероприятий;

$S_{ос}$ – параметр, отражающий вид используемой системы сигнализации.

В системах безопасности промышленных объектов возможно применение раздельных охранной, пожарной или совмещенной охранно-пожарной сигнализации.

Известно, что применение организационно-технических мер по обнаружению и сигнализации о пожаре повышает уровень пожарной безопасности объекта. Согласно этому значение коэффициента $S_{пс}$ в выражении (1.7), определенного по методике [40] находится в диапазоне 1,05-1,45. Значение коэффициента $T_{пт}$, характеризующего организацию, месторасположение, силы и средства пожарных подразделений, обслуживающих объект, для тех же условий – 1,05-1,2.

Значение показателя $C_п$ в соответствии с (1.5) определяется как произведение указанных выше коэффициентов. Таким образом, при обеспечении безопасности объектов централизованной охранно-пожарной сигнализации по оценкам [35] достигается увеличение пожарной безопасности объекта

в 1,1-1,74 раза.

Вместе с тем при совместном функционировании систем пожарной и охранной сигнализации, а также систем контроля технологических параметров АСУТП необходимо также учитывать особенности производства, виды и способы обнаружения проникновения и пожара, а также варианты организации безопасного функционирования защищаемого объекта [33].

Таким образом, качественный уровень системы охраны, влияя на уровень безопасности технологического процесса, пожарную безопасность объекта, непосредственно связан с качеством функционирования АСУТП предприятия. Поэтому можно утверждать, что система охраны, также как и противопожарной защиты, являются необходимыми элементами, обеспечивающими нормальное функционирование АСУТП промышленного объекта.

1.3 Состав и структура интегрированной АСУТП предприятий нефтегазового комплекса

Ввиду комплексного характера вероятных угроз ЦДНГ, увеличивающего сложность и многообразие функций управления производственной и хозяйственной деятельностью промышленного объекта, в основу для создания АСУ ЦДНГ может быть положена концепция интегрированной автоматизированной системы управления.

Следует отметить, что в общие функции управления производством входят также организация и управление предприятием, управление средствами инженерного обеспечения и жизнедеятельности и др. Поэтому задачи автоматизированного управления технологическим процессом, а также обеспечение безопасности являются частными, но наиболее важными (основными) для такого потенциально опасного объекта как ЦДНГ. Вместе с тем в настоящее время большинство существующих интегрированных АСУ

созданы на основе решений именно частных проблем, для решения которых совершенствование автоматизации управления позволит существенно облегчить достижение поставленных целей.

Для ЦДНГ основными являются производственные цели, которые требуют строгого соблюдения технологических регламентов, установленных планом сроков и объема выпуска продукции. При этом решение производственно-технологических задач должно производиться с обязательным выполнением требований охраны и пожарной безопасности производства.

Интеграция АСУ ЦДНГ должна основываться на следующих принципах, приведенных в таблице 1.2 [41-43].

Таблица 1.2 – Принцип синтеза интегрированной АСУ ЦДНГ

Принцип	Содержание
Интеграция	Решение задачи объединения системы управления технологическим процессом, охраны и пожарной безопасности в единую автоматизированную систему
Унификация	Рациональное ограничение номенклатуры технических средств и программного обеспечения, единый подход к автоматизации различных систем
Масштабируемость	Возможность добавления новых функций и технических средств для управления с сохранением единого подхода к системе управления
Комплексность	Учет всех требований к технологии производства и аспектов деятельности эксплуатирующих служб по обеспечению эффективного функционирования оборудования
Согласование частных критериев эффективности	Сочетание эффективности функционирования отдельных систем и их взаимодействия с глобальным критерием качества функционирования объекта в целом
Декомпозиция	Представление функциональной, организационно–технической и информационной структуры объекта в виде совокупности компонентов

В процессе функционирования АСУТП, интегрированной с системой

безопасности, решается ряд задач, которые можно объединить в три основные группы в соответствии с общими функциями, реализуемыми в системе (таблица 1.3).

Таблица 1.3 – Основные группы функций интегрированной АСУТП предприятий НГК и решаемые ей задачи

Основные группы функций	Решаемые задачи
Автоматизация сбора и обработки данных	- сбор и представление в произвольный момент времени значений параметров технологического процесса и состояния безопасности объекта; - анализ «предыстории» изменения параметров; - сигнализация отклонения параметров от заданных границ.
Разработка рекомендаций по обеспечению безопасности и оптимальному режиму управления ТП, осуществляемого оператором	- оперативное представление информации диспетчеру, позволяющее своевременно реагировать на тревожную ситуацию и эффективно проводить анализ технологического процесса и его корректировку; - глубокий анализ ситуации при возникновении угрозы, появлении случайного или принудительного возмущения и выработка стратегии управления (может производиться в подсистеме поддержки принятия решений по специально разработанным алгоритмам (программам))
Автоматическая реализация на объекте оптимальных рекомендаций (автоматический или комбинированный режим управления)	- сокращение продолжительности переходных процессов на объекте управления и уменьшение интервалов времени, в которых процесс ведется с отклонением от требуемых параметров, т. е. уменьшение производственных фактических или потенциальных потерь за счет снижения качества; - обеспечение рационального распределения нагрузок технологического оборудования при изменении номенклатуры выпускаемых изделий; - повышение безопасности технологического процесса и создание безопасных условий работы за счет предотвращения аварийных режимов работы технологического оборудования; - исключение вероятности пожаровзрывоопасных ситуаций и угроз от внешних воздействий

В соответствии с этим основными задачами, решаемыми АСУТП (в том числе извещателями, входящими в состав системы) предприятия НГК, в частности ЦДНГ, являются [44-47]: управление технологическим оборудованием; обеспечение качества продукции; обеспечение безопасности; материально-техническое обеспечение; информационная поддержка.

Сбор и обработка данных, а также формирование управленческих решений должны осуществляться центральным диспетчером.

Для решения указанных задач в состав интегрированной АСУТП должны входить следующие информационные подсистемы: контроля параметров технологического оборудования; контроля качества на этапах производства;

- охранно-пожарной (тревожной) сигнализации [48]; учета комплектующих и материалов; информационной поддержки.

Учитывая вышеизложенное, обобщенная структура интегрированной АСУТП предприятия нефтегазодобычи может быть представлена в виде, изображенном на рисунке 1.4.

Рисунок 1.4 – Обобщенная структура интегрированной АСУТП предприятий НГК

Необходимо отметить, что для крупных предприятий (с числом сотрудников более 200 человек и обширной территорией) с разветвленной инфраструктурой и спецификой производства такие структурные схемы должны разрабатываться индивидуально.

Следует подчеркнуть, что система охранно-пожарной сигнализации в составе интегрированной АСУТП не только участвует в обеспечении общей безопасности объекта, но и играет важную роль в обеспечении безопасности процесса производства (предотвращение аварийных, пожароопасных ситуаций, нарушения технологии производства и т. п.).

Особенностью системы охранно-пожарной сигнализации является наличие различных режимов работы, связанных с особенностями функционирования производства предприятия нефтегазодобычи, что вызывает необходимость изменения структуры системы сигнализации и целесообразность ее модульного построения (контроль выделенных участков или помещений). Таким образом, возникает задача формирования оптимального по составу и структуре модуля сбора и обработки данных о состоянии объекта и целесообразность его аппаратной и программной интеграции.

В соответствии с общими задачами, стоящими перед интегрированными АСУТП, система безопасности должна обеспечивать защищенность объекта, представляющего собой промышленное предприятие с производственными и административными помещениями. По действующим нормам и правилам такой объект должен быть оборудован системой безопасности, включающей комплекс технических средств обнаружения, оповещения, устройства управления, специальное оборудование и средства, расположенные непосредственно в производственных помещениях, а также в специально выделенных помещениях (диспетчерский пункт, помещение службы охраны и др.). В общем случае в состав системы безопасности могут входить системы контроля и управления доступом, видеонаблюдения должны быть предусмотрены меры по технической укреплённости и физической защите объекта.

В общей интегрированной АСУТП систему безопасности можно рассматривать как часть общего технологического процесса предприятия, а используемые технические средства – как оборудование, функционирующее по соответствующим нормам и правилам этого технологического процесса [26].

Основными компонентами проектных решений, определяющих структуру построения, состав, организацию и взаимосвязь системы безопасности с другими системами интегрированной АСУТП, являются функциональная и организационная структуры, а также структура комплекса технических средств [42].

Основными функциями системы безопасности являются:

- наблюдение, обнаружение и оповещение об опасности проникновения и пожара;

- пассивное регулирование и предупреждение;

- обеспечение аварийной связи и передача информации;

- локализация и устранение опасности;

- управление эвакуационно-спасательными средствами, инженерными системами и системой аварийного жизнеобеспечения;

- управление системами активного противодействия пожару и проникновению;

- управление системами вентиляции и дымоудаления;

- организация мер по переводу объекта с рабочего режима в аварийный с привлечением дополнительных технических и людских резервов.

На рисунке 1.5 показана иерархия функций системы безопасности.

Рисунок 1.5 – Иерархия функций системы интегрированной АСУТП предприятий НГК

Главной целью создания системы безопасности является обнаружение пожара и несанкционированного проникновения, а также управление инженерными системами объекта с целью предотвращения и ликвидации этих угроз. Достижение данной цели осуществляется при выполнении системой безопасности своих функций в нормальном режиме работы и при появлении опасности (аварии, пожара и т. п.). Таким образом, в целом систему безопасности можно характеризовать как информационно-управляющую систему.

Функции и задачи системы безопасности представлены в таблице 1.4. Структура функций системы безопасности приведена на рисунке 1.6.

На рисунке 1.7 приведена организационная структура системы безопасности.

На рисунке 1.8 приведена обобщенная структура технических средств системы безопасности.

При формировании структуры технических средств системы безопасности возможен выбор из трех вариантов. В первом случае используется программная интеграция отдельных самостоятельных технических средств в составе системы. Преимуществом данного технического решения является то, что неполадки в работе автоматизированных рабочих мест (АРМ) в данном случае не влияют на полноценную работу системы, так как технические средства имеют самостоятельные органы контроля и управления.

Таблица 1.4 – Функции и задачи системы безопасности

Функции	Задачи
Охранно-пожарная сигнализация	
1. Контроль пожарной ситуации на объекте	1.1. Сбор данных от автоматических извещателей 1.2. Сбор данных от неавтоматических (ручных) извещателей
2. Контроль несанкционированного проникновения	2.1. Сбор данных от автоматических датчиков и модулей 2.2. Сбор данных, вводимых персоналом
3. Индикация и оповещение	3.1. Передача тревожных извещений 3.2. Световое и звуковое оповещение 3.3 Отображение состояний зон на планах помещений на мониторе 3.4. Индикация путей эвакуации 3.5. Формирование инструкций персоналу
Управление	
1. Управление системами противодействия угрозе	1.1. Управление работой технологического оборудования 1.2. Управление системой пожаротушения 1.3. Управление системой противодействия проникновению 1.4. Управление работой систем вентиляции, дымоудаления и инженерных систем

Функции	Задачи
2. Управление режимами работы системы	2.1. Изменение режимов работы технических средств 2.2. Ведение базы данных 2.3. Архивирование данных 2.4. Статистическая обработка данных 2.5. Ввод и постройка сценариев управления 2.6. Ограничение доступа к данным и распределение функций
Повышение надежности 1. Контроль работоспособности системы	1.1. Самотестирование работоспособности технических средств 1.2. Определение состояния линий связи и технических средств 1.3. Контроль работоспособности и чувствительности датчиков и модулей
2. Контроль проведения технического обслуживания и ремонта системы	2.1. Формирование указаний о необходимости технического осмотра и ремонта
Служебные функции 1. Формирование служебной информации	1.1. Обработка и архивация данных 1.2. Ведение протокола дежурства
2. Контроль диспетчера	2.1. Регистрация действий диспетчера, связанных с обработкой тревог

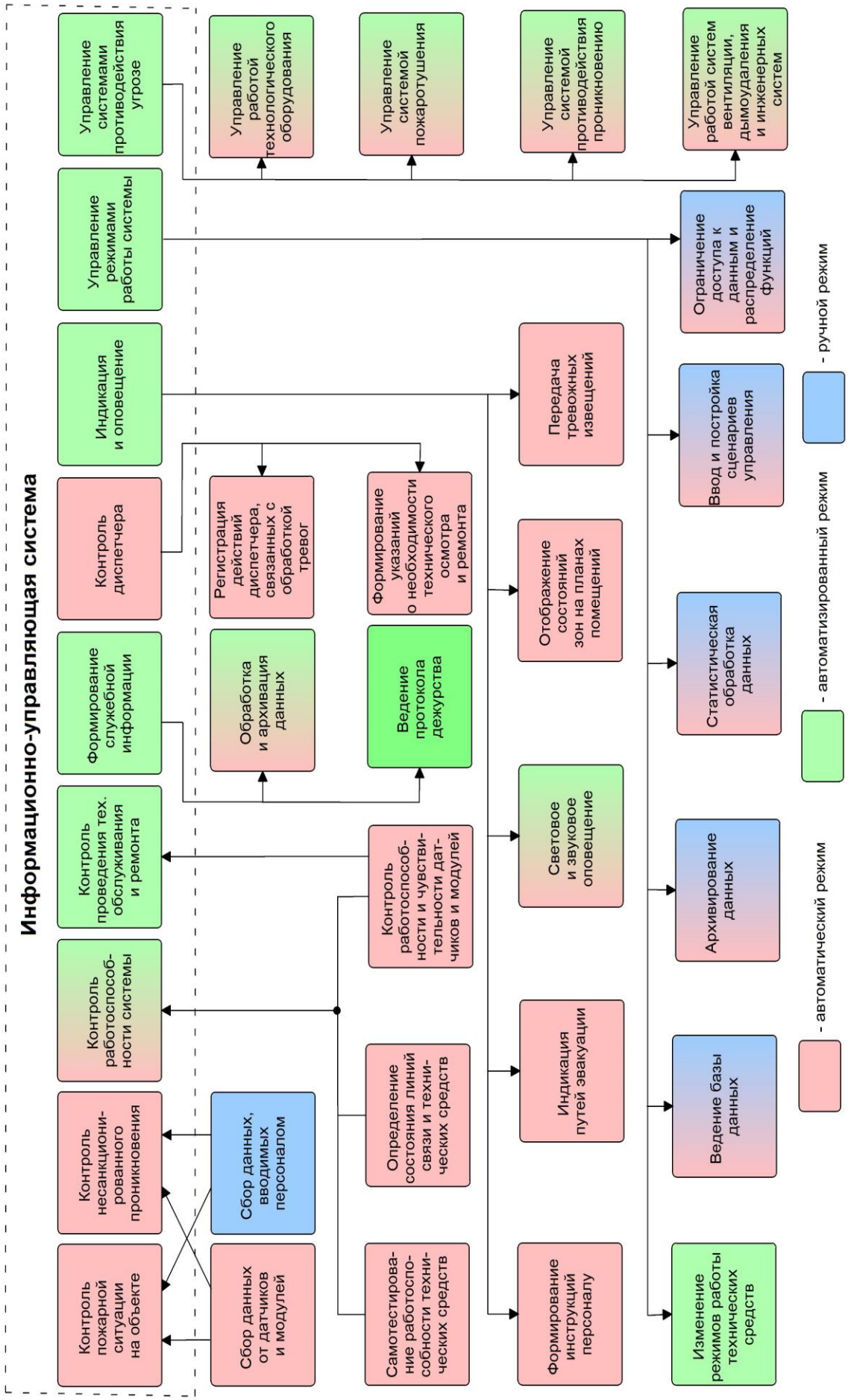


Рисунок 1.6 – Функциональная структура системы интегрированной АСУТП предприятий НГК

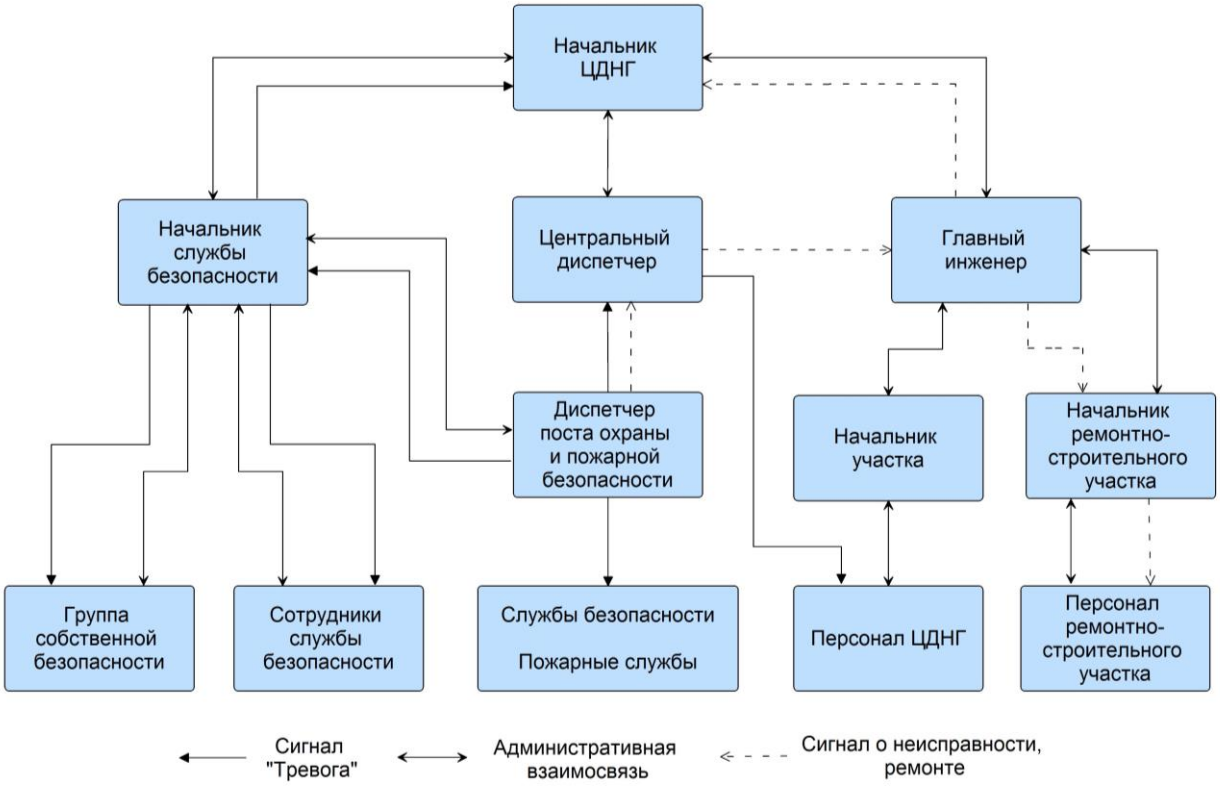
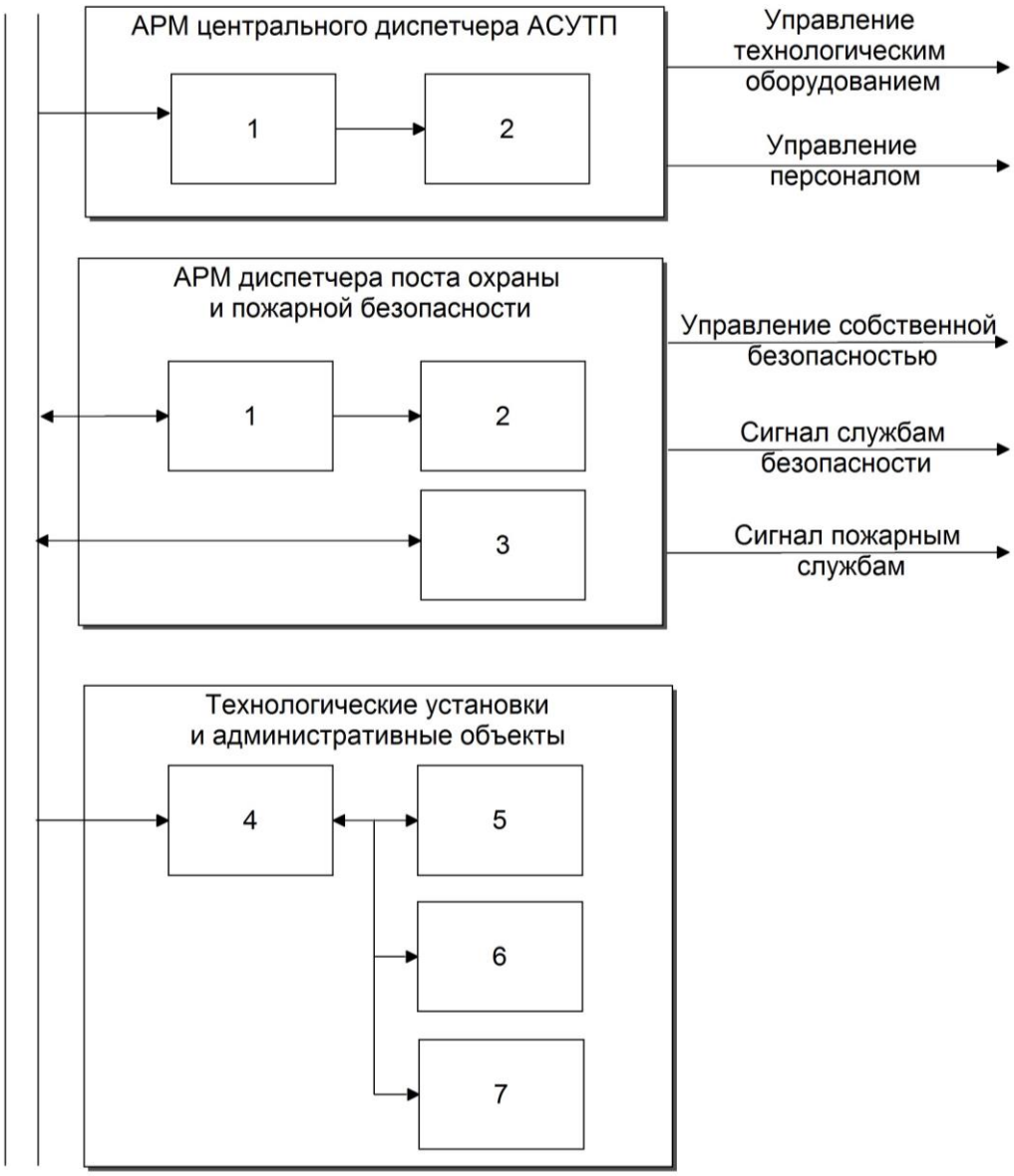


Рисунок 1.7 – Организационная структура интегрированной АСУТП предприятий НГК

Вторым вариантом является аппаратная интеграция, формируемая как на физическом уровне сопряжения самостоятельных средств, так и на уровне применения универсальных приборов. В таких системах отказ одного контроллера может вызвать сбои сразу во всей подсистеме.

Наиболее универсальной является аппаратно-программная интеграция, при которой одновременно присутствуют связи самостоятельных устройств как на программном, так и на физическом уровне.

С учетом указанного выше наибольший интерес для производственных объектов и комплексов представляет система, построенная с использованием программной и аппаратно-программной интеграции составляющих подсистем, выполненных на функционально законченных приборах, что позволяет повысить ее надежность при отказах как компьютеров, так и АРМ в целом.



1 – преобразователь интерфейсов; 2 – устройство отображения данных; 3 – блок контроля и управления; 4 – прибор приемно-контрольный; 5 – датчики (извещатели, модули обнаружения); 6 – оповещатели; 7 – технические средства активного противодействия

Рисунок 1.8 – Обобщенная структура технических средств интегрированной АСУТП предприятий НГК

1.4 Современное состояние системы безопасности промышленного объекта и классификация извещателей

В настоящее время требования к комплексным и интегрированным системам безопасности определяются национальными стандартами Российской Федерации ГОСТ Р 53704-2009 [49] и ГОСТ Р 57674-2017 [50], в соответствие с которыми ИСБ состоят из систем: охранной сигнализации (СОС), пожарной сигнализации, охранного телевидения (СОТ), контроля и управления доступом (СКУД), а также других вспомогательных и дополнительных систем обеспечения безопасности.

При этом важной задачей является возможность функционирования систем безопасности в обособленном режиме, а также при выходе по какой-то причине других систем из строя.

Нормальное функционирование АСУТП производства предприятий НГК, в частности ЦДНГ, должно быть обеспечено интегрированной централизованной системой, включающей, кроме охранной и пожарной сигнализации, видеонаблюдения, контроля и управления доступом, также дополнительные подсистемы [51].

Преимуществом данного способа организации ИСБ является независимость друг от друга и устойчивость отдельных подсистем, функционирующих по собственным каналам связи [52]. Модель данной системы безопасности приведена на рисунке 1.9.

Программное обеспечение (ПО) сервера ИСБ в этом случае состоит из следующих элементов:

1) драйвер, обеспечивающий прием информации от систем ИСБ;

2) система управления базой данных;

3) управляющий модуль, обеспечивающий классификацию и первичную обработку данных, осуществляющий регламентирование взаимодействия АРМ, системы управления базами данных и драйвера сети;

4) отдельные модули ПО на сервере ИСБ, обрабатывающие информацию по отдельным подсистемам.

Важно отметить, что вся передача информации на базу данных и АРМ осуществляется через управляющий модуль.

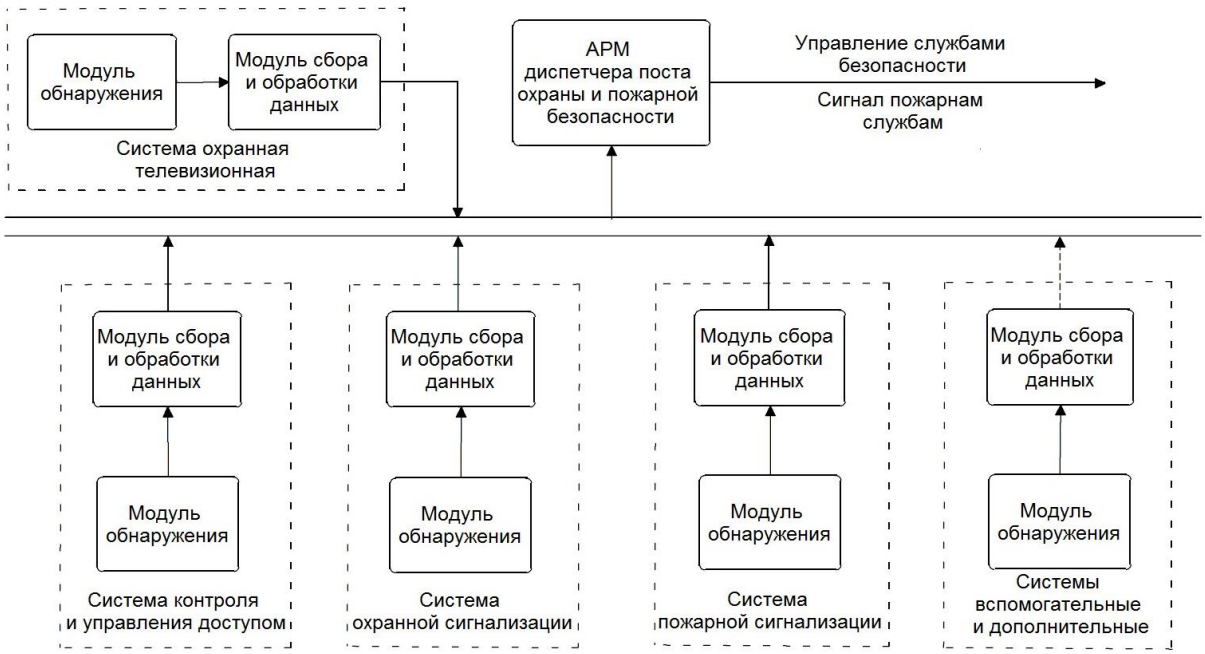


Рисунок 1.9 – Модель централизованной интегрированной системы безопасности

Основу централизованной ИСБ составляет модульная система охранно-пожарной сигнализации, включающая в себя технические средства сбора и обработки данных – датчики, извещатели и модули обнаружения, а также другие технические средства охраны (ТСО).

Структура сбора и обработки данных в системе централизованной охранно-пожарной сигнализации промышленного объекта представлена на рисунке 1.10.

К началу исследований была введена классификация автоматических охранных извещателей как по функциональной оснащенности [19], так и по уровню защиты от внешних факторов (рисунок 1.11) [53].

Однако требования к составу и значению технических характеристик для конкретных видов технических средств обнаружения отсутствовали. Анализ рынка показал, что при видимом насыщении рынка охранными извещателями и модулями они зачастую не отвечают требованиям эффективности, надежности и живучести для применения на потенциально опасных и критически важных промышленных объектах.

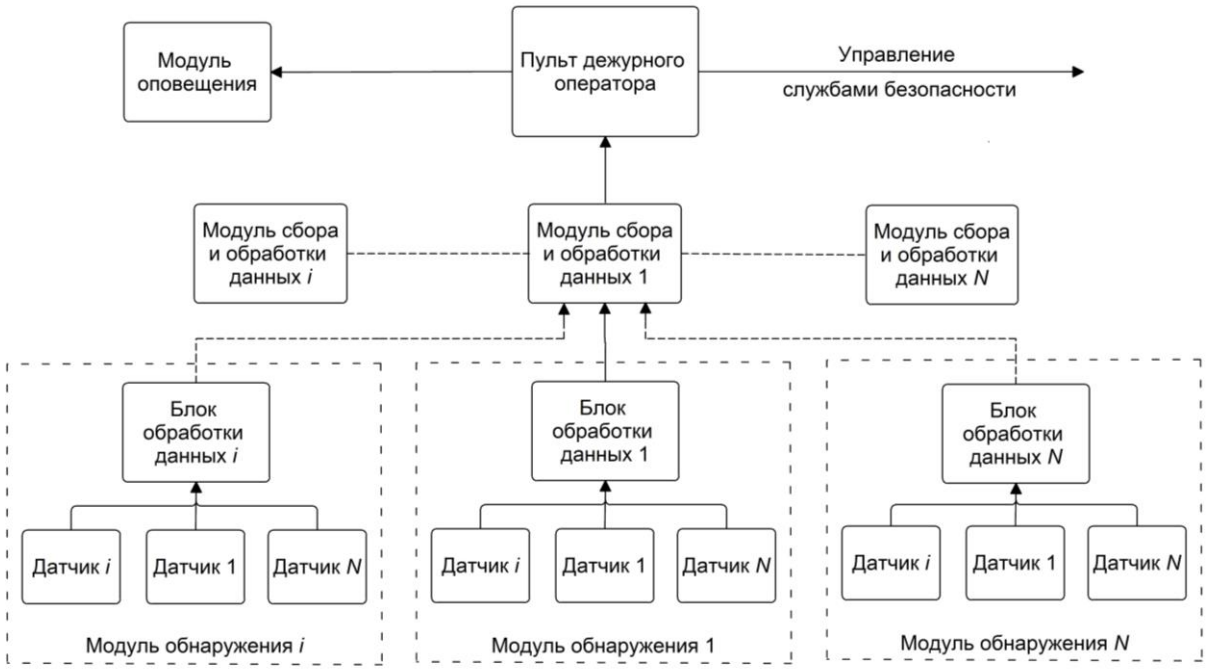


Рисунок 1.10 – Структура сбора и обработки данных в системе централизованной охранно-пожарной сигнализации

С введением системы классификации автоматических средств обнаружения для охраны особо важных объектов необходимы извещатели, обладающие дополнительными специальными функциями и структурой формируемых ими извещений. Поскольку при этом неизбежно возрастают стоимостные параметры системы сбора и обработки данных (ССОД), возникает проблема выбора составляющих ее технических средств.

Рисунок 1.11 – Классификация автоматических охранных извещателей

Следовательно, в условиях значительного повышения технической оснащенности и подготовленности лиц, совершающих противоправные действия криминальной и террористической направленности, активно противодействующих нормальному функционированию системы охранно-пожарной сигнализации, требуются исследования, разработка и производство новых видов извещателей с повышенной эффективностью обнаружения, а также рекомендаций по выбору оптимального состава модульных структур сбора и обработки данных.

Выводы по разделу 1

1. Современные предприятия нефтегазового комплекса являются потенциально опасными с точки зрения возможных последствий аварий и катастроф технологического оборудования, возникающих по различным причинам, в том числе из-за пожаров и террористических атак.

Поэтому нормальное функционирование автоматизированной системы управления технологическим процессом производства таких предприятий, в частности цехов по добыче и комплексной подготовке нефти и газа, должно быть обеспечено современной интегрированной системой безопасности, включающей модульную систему охранно-пожарной сигнализации.

2. На основе сформированного комплексного показателя безопасности промышленного объекта от угроз криминального проникновения нарушителя, пожара и техногенной аварии показана роль взаимного влияния систем безопасности и управления технологическим процессом промышленного предприятия. Предложенный метод позволяет оценить влияние проводимых мероприятий на уровень безопасности объекта.

3. В соответствии с основными задачами, решаемыми АСУТП предприятий НГК, сформирована обобщенная структура построения интегрированной АСУТП, которая включает ССОД.

4. Для рассматриваемых ЦДНГ сформулированы функциональная, организационная и техническая структуры, являющиеся основой для проектирования системы безопасности.

5. Анализ современного состояния системы охранно-пожарной сигнализации, а также составляющих ее технических средств определил необходимость дифференцированного подхода к задачам обеспечения противокриминальной и антитеррористической защиты объектов различных категорий значимости на основе введенной классификации автоматических охранных извещателей по их функциональной оснащенности и защищенности от несанкционированных внешних воздействий.

2 АНАЛИЗ ПОКАЗАТЕЛЕЙ ЭФФЕКТИВНОСТИ, НАДЕЖНОСТИ И ЖИВУЧЕСТИ ЦЕНТРАЛИЗОВАННОЙ ОХРАННО-ПОЖАРНОЙ СИГНАЛИЗАЦИИ НА ЭТАПЕ ЭКСПЛУАТАЦИИ

2.1 Предмет и область исследования показателей эксплуатации системы централизованной охранно-пожарной сигнализации

Понятия эффективность, надежность и живучесть должны рассматриваться применительно к автоматизированным техническим системам управления функционально максимально приближенным к решению задач диссертации. Следует отметить, что максимальное внимание данным показателям в справочной литературе уделено системам пожарной автоматики.

В соответствии с этим рассмотрены следующие определения [54-56], входящие в основные справочные базы:

Эффективность – «свойство системы выполнять поставленную цель в заданных условиях использования и с определенным качеством. Показатели эффективности характеризуют степень приспособленности системы к выполнению поставленных перед ней задач и являются обобщающими показателями оптимальности функционирования. Эффективность – свойство системы, характеризующее ее способность выполнять задачи по назначению».

Надежность – «свойство системы управления выполнять свои функции, сохраняя во времени показатели качества эксплуатации, соответствующие режимам и условиям их использования в условиях чрезвычайных ситуаций». «Надежность – комплексное свойство, которое в зависимости от назначения объекта и условий его эксплуатации может включать в себя свойства безотказности, долговечности, ремонтопригодности и сохраняемости, а также определенное сочетание этих свойств».

Живучесть – «способность технических систем и их компонентов сохранять или оперативно восстанавливать возможность выполнения заданных функций после повреждений в штатных и нештатных ситуациях, выходящих за пределы, установленные нормами и правилами». «Живучесть технической системы при возникновении чрезвычайной ситуации – свойство системы сохранять свою работоспособность в течение гарантированного времени в заданных условиях воздействий, в том числе при возникновении чрезвычайной ситуации, которая должна быть обеспечена применением специальных мер, технических мероприятий и проектных решений».

Учитывая достаточно широкую возможную трактовку данных понятий, рассмотрим их применительно к системе централизованной охранно-пожарной сигнализации.

Первоочередная задача системы охранной сигнализации – обеспечить своевременное обнаружение несанкционированного проникновения (НП) нарушителя на охраняемый объект. В связи с этим эффективность СОС напрямую зависит от применения в ней извещателей и модулей, максимально быстро и достоверно обнаруживающих попытки проникновения. Поэтому для повышения эффективности СОС необходимы исследование и анализ наиболее вероятных путей НП на охраняемые объекты. Это позволит определить классы извещателей, требующих первоочередного совершенствования.

В технической литературе понятие эффективности часто увязывают с требованиями надежности. Так для системы пожарной сигнализации в некоторых нормативных документах указывают: «Вероятность эффективной работы системы обнаружения пожара определяется как произведение вероятности выполнения функции основного назначения и вероятности безотказной работы технических средств этой системы».

В [54] в понятие надежности системы пожарной сигнализации (СПС) включают достоверное обнаружение пожара, учитывающее отсутствие ложных срабатываний.

Таким образом, расширяют понятие надежности, включая в него параметры эффективности и устойчивости обнаружения.

В некоторых случаях как главную характеристику СПС выделяют именно устойчивость, понимая надежность «как характеристику устойчивости по отношению к внутренним дестабилизирующим факторам», а живучесть «как характеристику устойчивости к внешним дестабилизирующим факторам».

Применительно к СОС живучесть следует понимать как параметр, характеризующий способность системы сигнализации функционировать в результате не только возможных экстремальных условий эксплуатации, но и активного противодействия нарушителя как во время НП, так и в период подготовки к нему.

Таким образом, для наиболее полного анализа показателей эксплуатации системы централизованной охранно-пожарной сигнализации должны быть рассмотрены следующие вопросы:

1. Надежность функционирования систем охранной сигнализации, характеризуемая безотказностью их работы.

2. Устойчивость функционирования систем охранной сигнализации, характеризуемая отсутствием ложных сигналов тревоги.

3. Живучесть как характеристика устойчивости СОС противодействию нарушителя эффективному функционированию системы охраны.

2.2 Способы проникновения нарушителей на категорированные объекты

В последние годы в связи с ростом технической оснащенности и подготовленности лиц, совершающих противоправные действия криминальной и террористической направленности, значительно возросла вероятность попыток осуществления квалифицированных преступных посяга-

тельств на охраняемые объекты [15]. Особенно опасно проникновение на промышленные объекты, преступные посягательства на которые могут привести к особо тяжким социальным и экономическим последствиям.

Например, для ЦДНГ, являющихся одной из основных составляющих НГК, выход из строя даже одного ЦДНГ при аварии, пожаре или диверсии затруднит деятельность всего НГК на длительное время. Главной задачей ЦДНГ является выполнение заданий по добыче нефти и газа с соблюдением установленных технологических режимов работы.

В соответствии с [22] объекты, охраняемые или подлежащие передаче под централизованную охрану в зависимости от значимости, концентрации материальных и иных ценностей, размещенных на объекте, последствий от возможных криминальных посягательств на них подразделяются на категории.

Объекты категорий А1, А2, и А3 – это критически важные объекты, особо важные объекты, потенциально опасные объекты и объекты жизнеобеспечения, государственные, а также коммерческие объекты, преступные посягательства на которые могут привести к особо крупному экономическому ущербу государству или собственнику имущества и иметь широкий общественный резонанс.

Объекты категорий Б1 и Б2 – это объекты организаций различных форм собственности, преступные посягательства на которые могут привести к крупному и значительному материальному ущербу предприятию или собственнику.

С целью повышения эффективности обнаружения для важных объектов система охранной сигнализации формируется как многорубежная [57-60]. Виды основных объектов блокировки и устанавливаемых на них извещателей по рубежам приведены в таблице 2.1.

Объекты категории А1 оборудуются тремя рубежами охранной сигнализации, А2 и Б1 – двумя рубежами охранной сигнализации [6, 8].

В случае необходимости объекты категории А2 и Б1 по согласованию с администрацией объекта допускается оборудовать третьим рубежом охранной сигнализации [61, 62].

Таблица 2.1 – Рубежи сигнализации

Рубеж	Объект блокировки	Виды применяемых извещателей
Первый	- оконные и дверные проемы по периметру здания или строения объекта; – места ввода коммуникаций, вентиляционные каналы; - выходы к пожарным лестницам; - некапитальные и капитальные стены.	- точечные магнитоконтактные [21]; - поверхностные звуковые [63, 64]; - поверхностные ударно-контактные; - вибрационные; - пассивные оптико-электронные с поверхностной зоной обнаружения; - активные оптико-электронные
Второй	- внутреннее пространство помещений.	- пассивные оптико-электронные [65]; - ультразвуковые; - радиоволновые; - комбинированные; - совмещенные
Третий	- сейфы, витрины, отдельные предметы или подходы к ним.	- поверхностные вибрационные или совмещенные с ними; - точечные магнитоконтактные; - поверхностные звуковые; - ультразвуковые

Рассматриваемые промышленные объекты НГК относятся к объектам категории А.

На рисунке 2.1 представлено относительное количество попыток проникновений на объекты различной категорий, охраняемые вневедомственной охраной Росгвардии.

На рисунке 2.2 представлено относительное количество попыток проникновения на объекты, обнаруживаемые системой сигнализации при преодолении нарушителем формируемых рубежей.

Основные способы проникновения на охраняемый объект представлены в таблице 2.2.

Из диаграммы рисунка 2.2 видно, что количество проникновений через первый рубеж охраны объекта значительно превышает количество проникновений через последующие рубежи. Учитывая, что многорубежной сигнализацией оборудуются объекты категории А1-А3, можно утверждать, что данные объекты относительно чаще, чем объекты категорий Б1 и Б2, подвергаются криминальным посягательствам.

Наиболее распространенным способом несанкционированного проникновения на охраняемую территорию вне зависимости от категории объекта по данным [16, 22] является преодоление ограждения путем перелаза. Относительная доля такого способа составляет около 32 % от общего количества попыток НП на территорию охраняемого объекта.

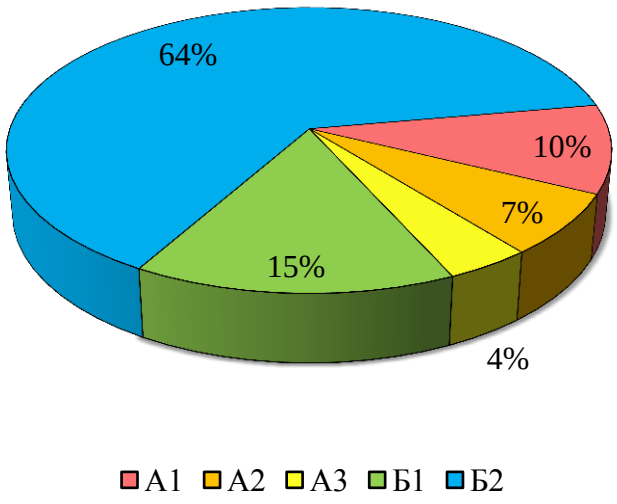


Рисунок 2.1 – Относительное количество попыток проникновений на объекты различной категории

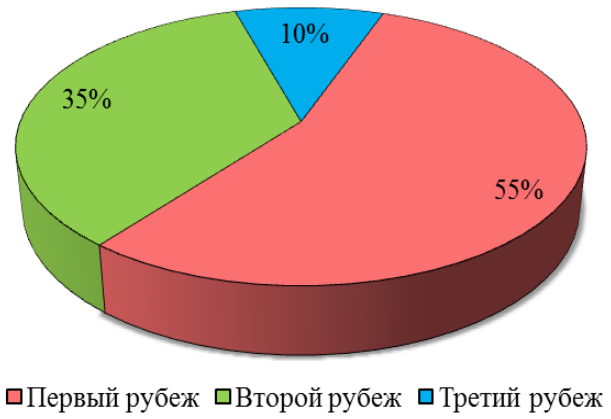


Рисунок 2.2 – Относительное количество попыток проникновения через рубежи сигнализации

Таблица 2.2 – Основные способы проникновения на охраняемый объект

Вид объекта	Виды проникновения	Относительное количество, %
1	2	3
Ограждение	Перелаз	32
	Разрушение полотна ограждения	15
	Отгиб полотна ограждения	2
	Подкоп	9
	Обход ограждения через водоспуски и т. д.	8
	Обход ограждения без механического контакта	25
	Другие виды	9
Территории и открытые площадки	Перемещение по охраняемой территории	9
	Подбор ключей и отмычек	3
Периметр охраняемого здания	Разрушение замка	12
	Разрушение части полотна двери	
	Выбывание двери	3
Помещения	Через окно путем разбития стекла	50
	Через окно без разбития стекла	12
	Через стену здания	8

Окончание таблицы 2.2.

1	2	3
	Через межэтажные перекрытия	3
	Через крышу	
	Путем подкопа	
	Через вентиляцию	
	Через люки	
	Через технологические каналы	
	Через лифтовую шахту	
	Через чердачные отверстия	
	Через подвальные отверстия	
	Через коммуникацию	
	Через другие технологические каналы	
Места хранения имущества	Разбитие остекленного ограждения	45
	Хищение сейфа или иного средства защиты целиком	11
	Вскрытие сейфа или иного средства защиты инструментальным способом на месте	28
	Посягательства на объекты дистанционного обслуживания, совершаемые как путем взлома на месте, так и кражи целиком	16

Способы, не связанные с механическим контактом при преодолении нарушителем полотна (козырька) ограждения, составляют также значительную долю – до 25%.

Для обнаружения такого способа НП эффективным является контроль территории охраняемого объекта с помощью СОТ по ГОСТ Р 51558-2014 [51, 66, 67] и (или) формирование второго рубежа системы сигнализации.

Следует отметить, что основное количество попыток проникновений на промышленные объекты составляют НП в здания или помещения. Как правило, более 50% случаев, они осуществляются через наиболее уязвимые места – окна или входные двери.

Окна и другие остекленные конструкции в основном подвергаются разрушению. Однако наряду с разбитием стекла значительное количество случаев НП, около 12%, сопровождается выдавливанием или извлечением стекла вместе с рамой.

НП через дверной проем осуществляются, как правило, в результате разрушения полотна двери или замка, значительно реже – выбиванием двери или дверной коробки целиком.

Представленные материалы позволяют выделить наиболее вероятные способы, используемые нарушителями для незаконного проникновения на охраняемые объекты с целью совершения противоправных действий, определить меры противодействия, в том числе направления разработки новых эффективных технических средств охранной сигнализации.

2.3 Надежность и устойчивость функционирования систем охранно-пожарной сигнализации

2.3.1 Причины отказов технических средств обнаружения систем охранно-пожарной сигнализации

Исследования проводились на основе анализа причин возврата на гарантийный ремонт технических средств, серийно производимых российскими фирмами и установленных на объекты, охраняемые вневедомственной охраной [9, 68, 69].

По результатам опроса выявлены основные виды неисправностей, приведенные на диаграмме рисунка 2.3, количественно характеризующие причины возвратов ТС.

К основным эксплуатационным дефектам могут быть отнесены:

- неисправности, возникшие в результате хранения или неправильной транспортировки;

- неисправности, возникшие при подключении или монтаже технических средств эксплуатирующей организацией;

- нарушения в процессе эксплуатации, приведшие к неисправности.

Неисправность в виде неустойчивой работы извещателя характеризовалась большим количеством ложных сигналов тревоги (ЛСТ) в процессе эксплуатации.

Относительное количество возвратов k-го вида D_k определялось за анализируемый период времени с 2010 по 2014 гг. (5 лет).

Общее количество неисправностей в период l-го года определяется как сумма всех возвратов по представленным на рисунке 2.3 причинам.

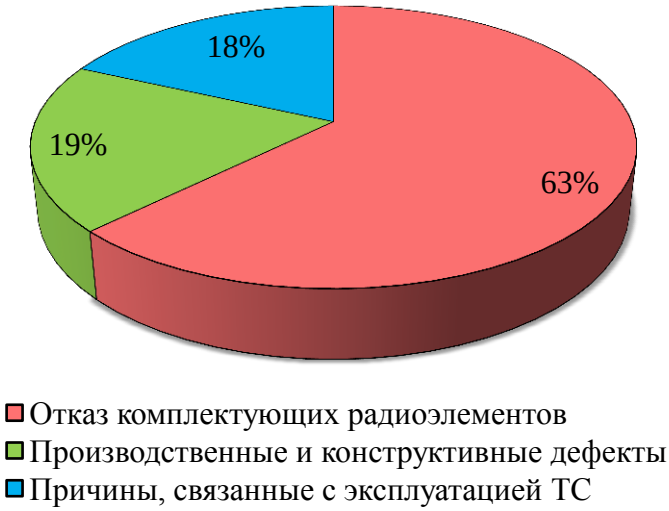


Рисунок 2.3 – Относительное количество причин возникновения неисправности в гарантийный период

Из рисунка 2.3 видно, что наиболее часто встречающаяся причина – отказ комплектующих радиоэлементов – 63%. Общая доля производственных и конструктивных дефектов составляет 19%. Значительную долю (18%) составляют причины, связанные с эксплуатацией ТС на охраняемых объектах.

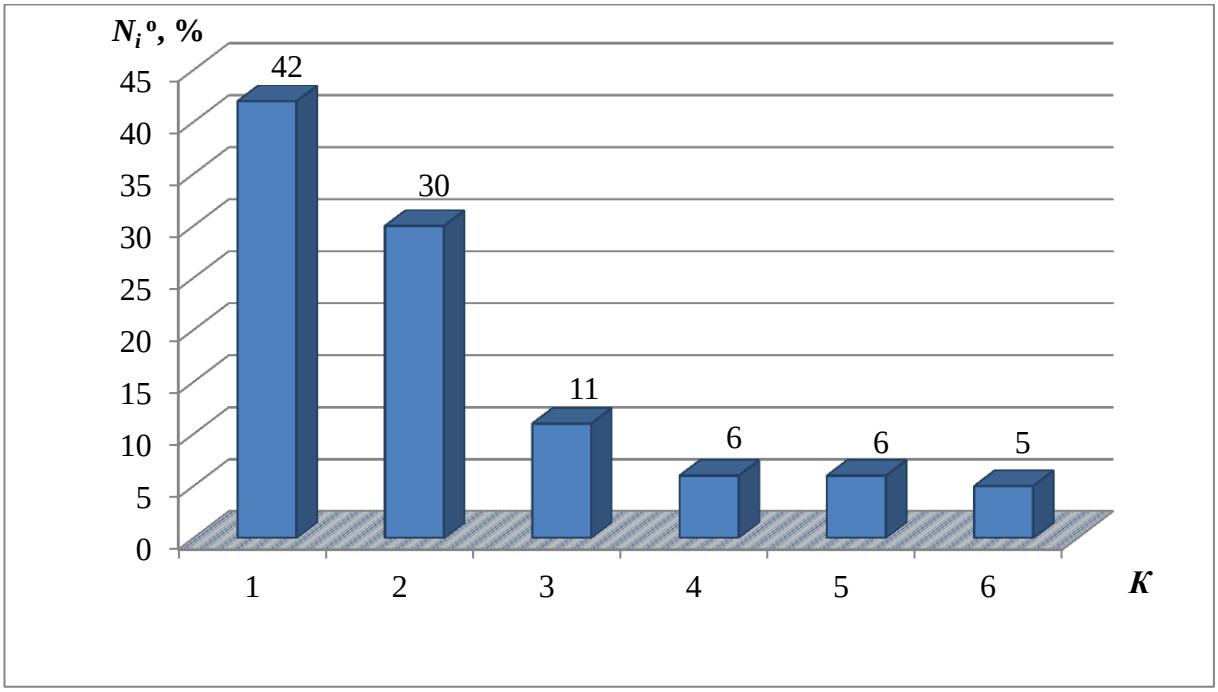
2.3.2 Причины ложных сигналов тревоги систем охранно-пожарной сигнализации

Рост технической оснащенности объектов средствами охраны может сопровождаться снижением устойчивости функционирования систем сигнализации, что проявляется прежде всего в увеличении количества ЛСТ. ЛСТ создают напряженность в работе органов охраны, наносят большой вред, как экономический, так и социальный, приводя вследствие их некачественной работы к допущению кражи, а иногда и к гибели сотрудников в схватках с преступником. Таким образом, большое количество ЛСТ является одним из основных сдерживающих факторов в развитии систем безопасности объектов.

Рост надежности охраны объектов на первом этапе интенсивного технического оснащения объектов ТСО отставал от прироста ложных сигналов тревоги. Их количество с 1982 г. по 1988 г. увеличилось более чем в 2 раза, с 1988 г. по 1993 г. – в 1,4 раза, к началу 90-х годов оно составляло в среднем около 2500 в год на 1000 задействованных пультовых номеров.

Результаты количественного анализа причин ЛСТ систем охранно-пожарной сигнализации, приведенные в [70], представлены на рисунке 2.4. Указанные причины были характерны и для зарубежных технических средств этого времени.

Выборочный анализ причин, указанных в статистической отчетности этого периода, проведен автором работы. Он показывает, что основными факторами, определяющими количество и динамику изменения ложных сигналов тревоги, являются действия человека, влияние погодных условий и помех различного рода. Однако целенаправленная работа Главного управления вневедомственной охраны Росгвардии совместно с ФКУ «НИЦ «Охрана» Росгвардии по повышению качества производимых и применяемых на объектах средств охранной и охранно-пожарной сигнализации, улучшению их тактико-технических характеристик (ТТХ) привело к существенному снижению ЛСТ уже в первом десятилетии 21-го века.



1 – некачественная установка и плохое техническое обслуживание; 2 – халатность и неправильные действия материально-ответственных лиц; 3 – неисправность телефонных линий и помехи в них; 4 – отказы аппаратуры; 5 – отклонения и провалы напряжения питания; 6 – прочие причины

Рисунок 2.4 – Причины неустойчивой работы систем охранно-пожарной сигнализации

Этому способствовало проведение эффективной технической политики, в частности введение специальных перечней ТСО, рекомендованных к применению на охраняемых объектах и отвечающих специально разрабатываемым единым тактико-техническим требованиям.

С 2004 г. началась работа по комплексному техническому перевооружению служб вневедомственной охраны (ВО). К настоящему времени ВО практически полностью перешла на использование автоматических систем передачи извещений (СПИ). Сегодня более 97% охраняемых ВО объектов оборудовано комплексами технических средств охранной и пожарной сигнализации, большинство из которых функционируют в составе систем централизованной охраны.

В связи с этим представляет несомненный интерес сравнительный анализ причин ЛСТ в предыдущий и настоящий периоды времени.

Анализ проводился по данным Главного управления вневедомственной охраны, приведенным в [9, 22, 68, 69]. Данные охватывали период 2014 года, включали 75 областей Российской Федерации, города из разных регионов России, в том числе такие крупные, как Москва, Санкт-Петербург, Нижний Новгород, а также Ленинградская область и др. Учитывая это, данную статистическую выборку можно считать представительной.

Среднее количество ЛСТ за этот период оценено примерно 400 на 1000 пультовых номеров, что почти в 6 раз меньше, чем полученное ранее [68]. Основные причины ЛСТ, выбранные для анализа, приведены в таблице 2.3.

Анализируемый массив с учетом особенностей организации охраны был разделен две группы: объекты различного назначения и формы собственности, а также группа охраняемых помещений (квартир) и мест хранения имущества граждан.

Параметры ЛСТ для статистического анализа представлены в таблице 2.4.

На рисунке 2.5 представлены сводные данные относительного количества ЛСТ N_i^{o}, $N_{\text{oio}}{}^{\text{o}}$, $N_{\text{oiк}}{}^{\text{o}}$ по причинам K, указанным в таблице 2.3.

Из рисунка 2.5 следует, что основными причинами ЛСТ являются помехи и неисправности в каналах передачи данных, в основном проводных абонентских линий связи, используемых для организации централизованной охраны.

Сравнивая с данными рисунка 2.4, можно отметить, что в настоящее время доля ЛСТ, поступающих непосредственно с объектов от технических средств обнаружения, существенно уменьшилась. Этому, очевидно, способствовало как улучшение характеристик применяемых извещателей и приемно-контрольных приборов (ППК), так и качество их обслуживания. Вместе с тем доля ЛСТ, вызванных недостатками электропитания, возросла.

Таблица 2.3 – Перечень причин ЛСТ для статистического анализа

Коды причин ЛСТ, *К*	Причины ЛСТ
1	Неисправность (неправильный монтаж) магнитоконтактных, ударноконтактных, омических датчиков, нарушение целостности или отклонение от заданных параметров шлейфов сигнализации
2	Неисправность (неправильная установка) извещателей оптико-электронного, емкостного, радиоволнового, ультразвукового, акустического, вибрационного принципа действия
3	Неисправность объектовых оконечных устройств СПИ, ППК, концентраторов / источников бесперебойного электропитания (в т. ч. аккумуляторных батарей в них)
4	Неисправность линейных модулей ретрансляционного и отказы каналообразующего оборудования
5	Отклонение от нормы параметров (отключение) абонентских линий связи, используемых для организации централизованной охраны
6	Отключение (отклонение параметров от нормы) электроэнергии на объекте
7	Неудовлетворительная инженерно-технической укреплённость объекта
8	Вина собственника
9	Прочие причины (установленные, но не относящиеся к перечисленным)

Несколько уменьшились, но по-прежнему значимую долю ЛСТ составляют ошибки хозоргана (собственника) при сдаче-снятии объектов с охраны.

Таблица 2.4 – Параметры ЛСТ для статистического анализа

Обозначение параметра	Наименование и размерность	Математическое выражение
N	Общее количество ЛСТ по всем причинам, ед	$N = N_o + N_к$
N_o	Количество ЛСТ по группе объектов по всем причинам, ед	$N_o = \sum_{i=1}^{9} N_{iо}$
$N_к$	Количество ЛСТ по группе помещений по всем причинам, ед	$N_к = \sum_{i=1}^{9} N_{iк}$
N_{io}	Количество ЛСТ по группе объектов по i-й причине, ед	-
$N_{iк}$	Количество ЛСТ по группе помещений по i-й причине, ед	-
$N_i^{о}$	Общее относительное количество ЛСТ по i-й причине, %	$N_i^{о} = N_{oiо}{}^{о} + N_{oiк}{}^{о}$
$N_{oiо}{}^{о}$	Общее относительное количество ЛСТ по группе объектов по i-й причине, %	$N_{oiо}{}^{о} = (N_{iо}/N)100$
$N_{oiк}{}^{о}$	Общее относительное количество ЛСТ по группе помещений по i-й причине, %	$N_{oiк}{}^{о} = (N_{iк}/N)100$
$N_{iо}{}^{о}$	Относительное количество ЛСТ по группе объектов по i-й причине, %	$N_{iо}{}^{о} = (N_{iо}/N_o)100$
$N_{iк}{}^{о}$	Относительное количество ЛСТ по группе помещений по i-й причине, %	$N_{iк}{}^{о} = (N_{iк}/N_к)100$

Следует отметить, что за последние два десятилетия значительно возросло количество охраняемых помещений. На рисунках 2.6, 2.7 представлены раздельно данные по относительному количеству ЛСТ по группам соответственно для объектов, а также помещений. В целом по данным распределения рисунка 2.5 количество ЛСТ для группы помещений существенно превышает их количество для группы объектов. Однако учет доли объектов и помещений в их общем количестве [9] показывает, что это отличие статистически незначимо. Соответствующая этому диаграмма представлена на рисунке 2.8.

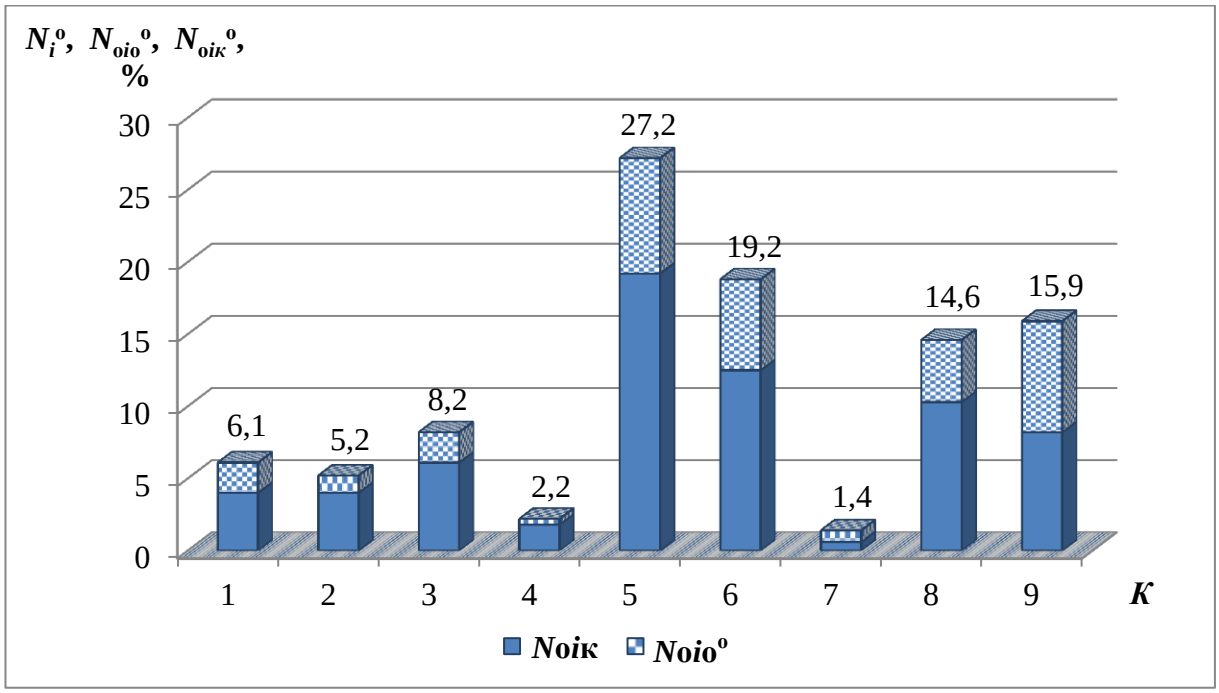


Рисунок 2.5 – Распределение общего относительного количества ЛСТ по основным причинам

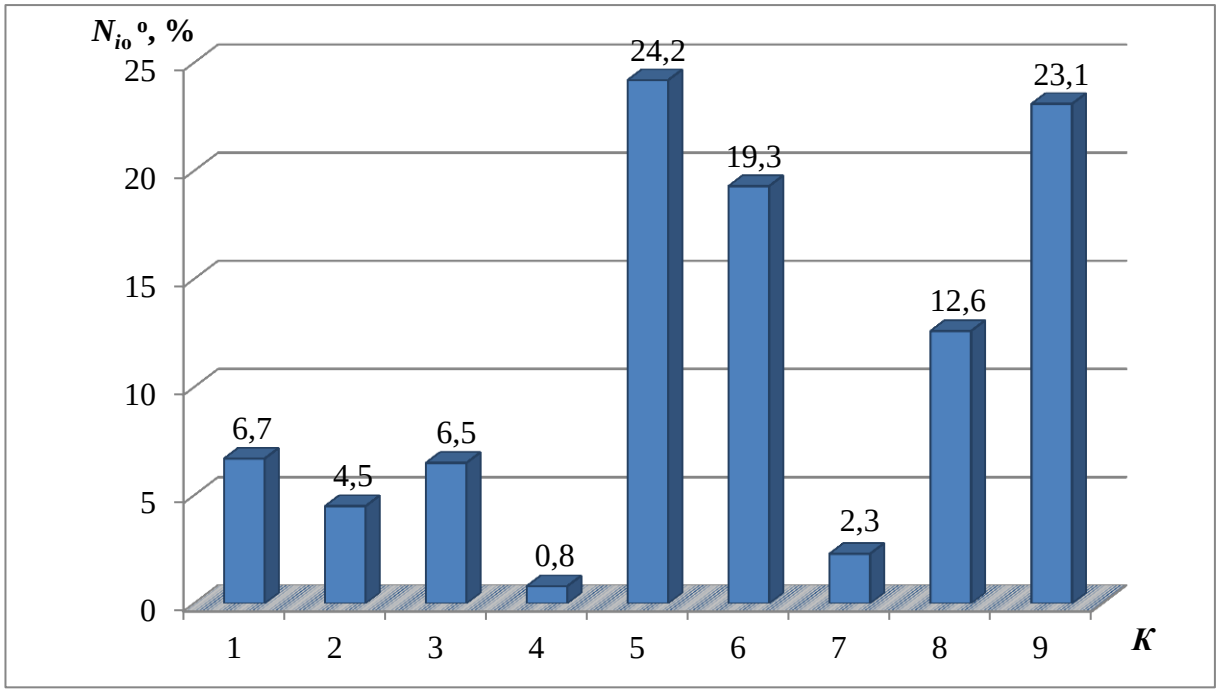


Рисунок 2.6 – Распределение относительного количества ЛСТ по основным причинам для группы объектов

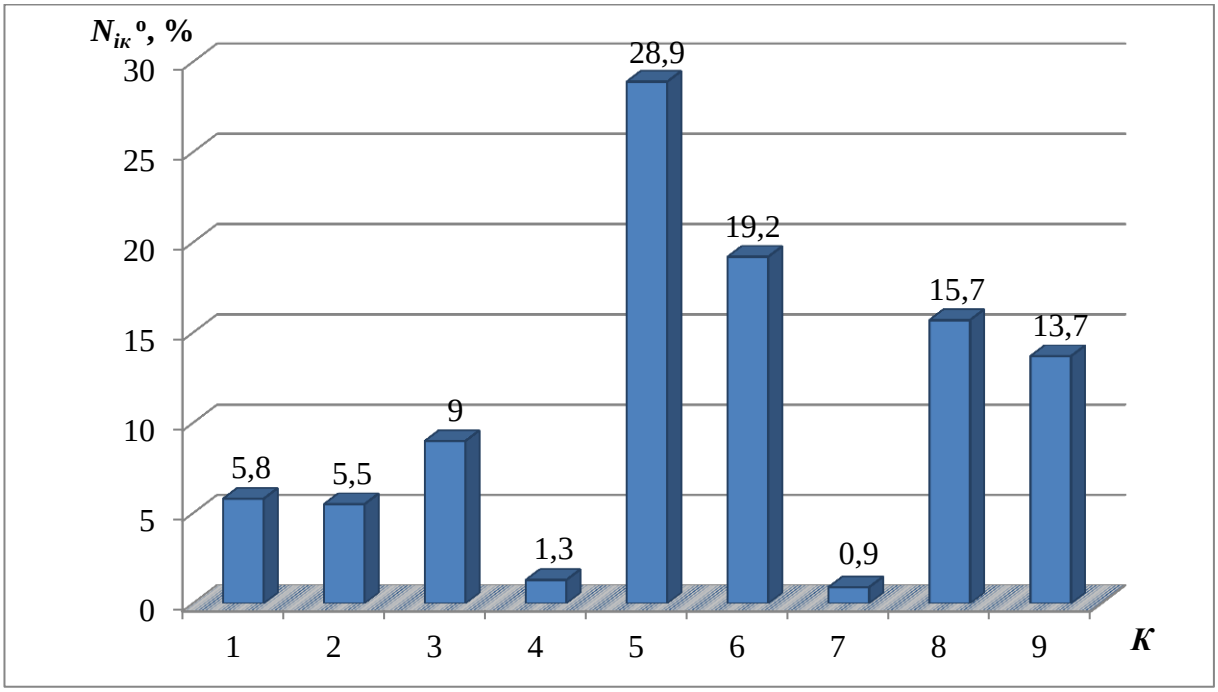


Рисунок 2.7 – Распределение относительного количества ЛСТ по основным причинам для группы помещений

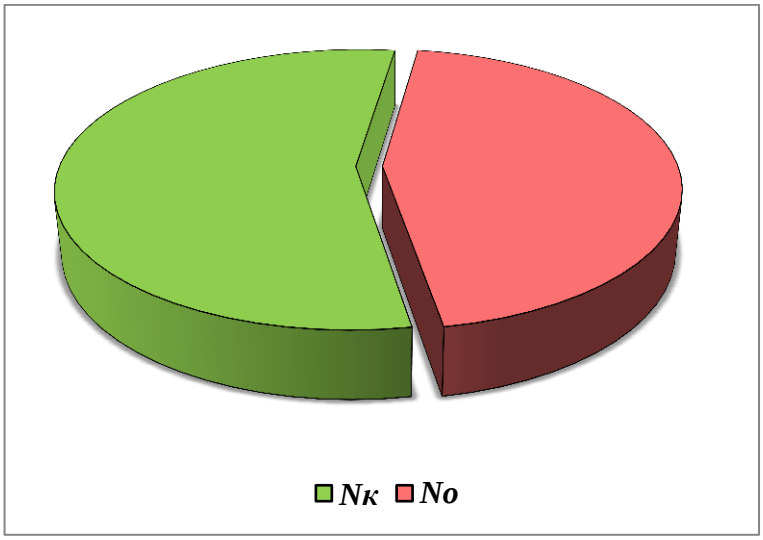


Рисунок 2.8 – Распределение доли ЛСТ по группам с учетом относительного количества субъектов

Проведенный анализ характеризует динамику изменения причин ЛСТ систем централизованной охранно-пожарной сигнализации и позволяет определить направления технической политики по повышению эффективности функционирования систем охраны объектов.

2.4 Способы противодействия нарушителя эффективному функционированию системы охраны категорированных объектов

2.4.1 Способы саботажа средств сбора и обработки данных

Под саботажем необходимо понимать действия, осуществляемые нарушителем на этапе подготовки и реализации несанкционированного проникновения, направленные на нарушение работоспособности ТСО и не обнаруживаемые системой сигнализации [69, 71-74].

Автором проведены обобщение и обработка статистических данных о способах саботажа ТСО, полученных от региональных подразделений вневедомственной охраны в период 2014 года.

В ходе работы также проведен анализ количества случаев саботажа ТСО в зависимости от его способа и категории охраняемого объекта (рисунок 2.9).

Анализ статистических данных свидетельствует, что случаи саботажа ТСО на объектах высоких категорий значимости (А1-А3) распространены практически в десять раз чаще, чем попытки саботажа на объектах низших категорий (Б1, Б2) [69, 75].

Исходя из результатов проведенного анализа распределения количества попыток саботажа ССОД, можно отметить относительное равенство количества случаев саботажа модулей обнаружения и средств передачи извещений.

Саботажу способствует то, что многие ТСО не могут устанавливаться скрытно, и в то время, когда объект не находится под охраной, к ним возможен доступ посторонних лиц. Таким образом, для успешного пресечения проникновения нарушителя необходимо обнаружение не только попытки проникновения, но и подготовки к нему путем саботажа.

Рисунок 2.9 – Относительное количество различных способов саботажа средств сбора и обработки данных в зависимости от категории охраняемого объекта

При более детальном рассмотрении случаев саботажа извещателей для помещений необходимо отметить, что их основную часть (54% от общего количества случаев саботажа извещателей для помещений) составляют случаи блокирования магнитоконтактного извещателя мощным магнитом и демонтаж извещателей (рисунок 2.10).

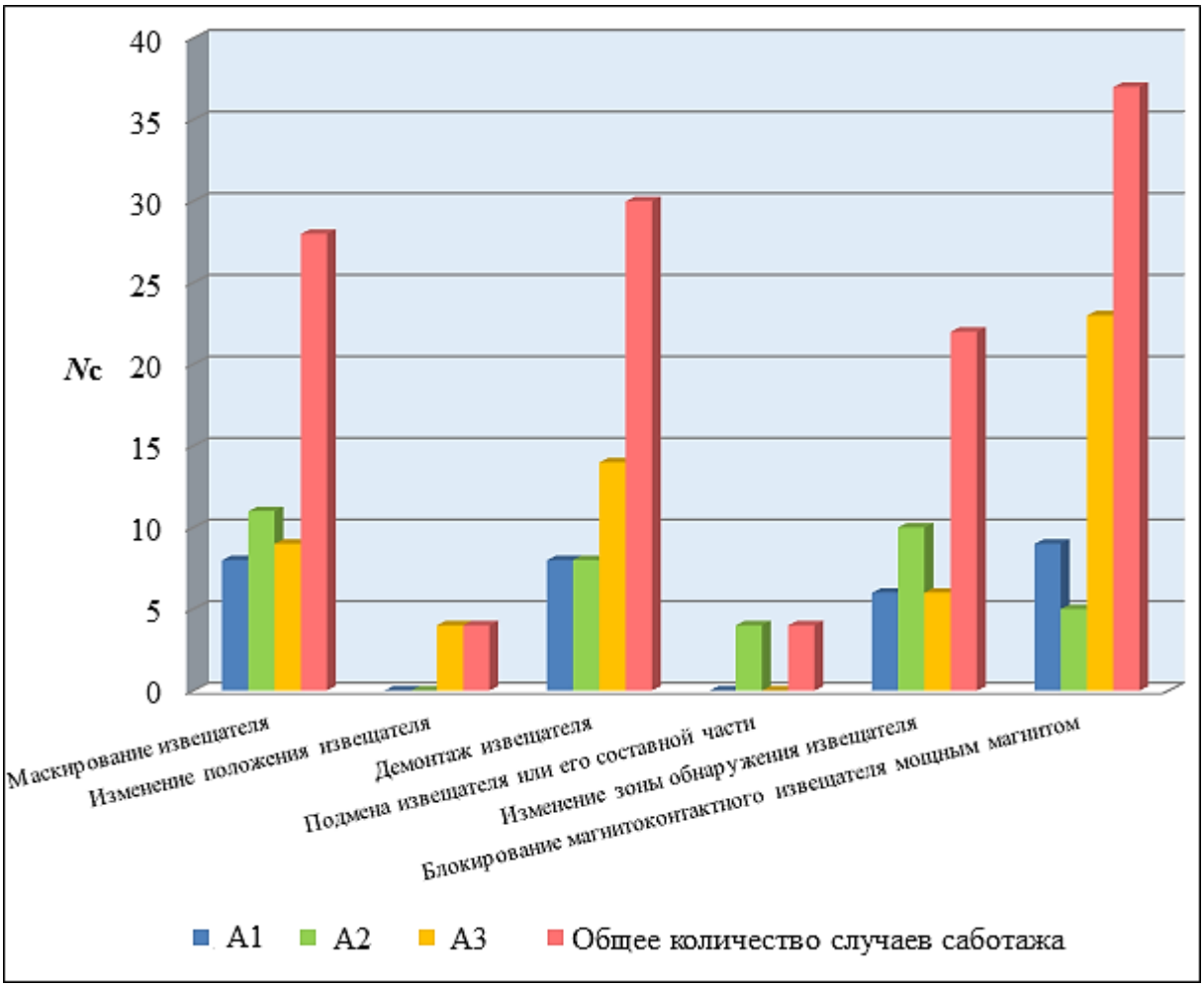


Рисунок 2.10 – Относительное количество случаев саботажа извещателей для помещений

Из вышеизложенного следует, что для повышения функциональных возможностей и увеличения надежности обнаружения проникновения на объектах высокой категории значимости необходимо использовать ТСО с функцией защиты от саботажа [4, 7, 13, 15]. Решение данной задачи воз-

можно при активном осуществлении разработки и внедрения в производство новых и модернизации имеющихся ТСО с введением данной функции, в частности извещателей охранных точечных магнитоконтактных, т. к. они являются одним из основных средств блокировки первого рубежа охраны объекта и на них, согласно приведенной статистике, направлено наибольшее количество воздействий с целью саботажа.

2.4.2 Влияние внешних криминальных воздействий на технические средства охраны и сигнализации

Защита от внешних угроз и несанкционированного проникновения является одной из приоритетных задач для таких промышленных объектов, как ЦДНГ. Как отмечалось выше, наиболее эффективной является ИСБ, включающая охранное телевидение и контроль доступа. Возникновение любой нештатной ситуации вследствие неправомерных действий злоумышленников на объекте может привести к серьезным, зачастую труднопреодолимым последствиям для персонала, производства и для окружающей среды в целом.

ИСБ должна непрерывно отслеживать перемещение людей на объекте, с высокой вероятностью и без ложных срабатываний обнаруживать незаконное проникновение на объект и идентифицировать возникающие угрозы в автоматическом режиме. В случае возникновения угроз контролируемому объекту система должна организовать своевременное оповещение персонала, обеспечить адекватную реакцию службы безопасности, информирование руководства объекта с использованием современных средств связи. В такой ИСБ скорость обработки информации, поступающей от всех подсистем, быстрый и правильно распределенный доступ к информации, надежность связи с пультом централизованного управления и мониторинга становятся определяющими параметрами.

Для электронного оборудования, используемого при создании ИСБ, определяющими становятся также критерии возможности работы во взрывоопасной среде и в экстремальных климатических условиях (например, ветровые и температурные нагрузки), а также в условиях криминального воздействия нарушителя.

В процессе функционирования технические средства систем безопасности могут подвергаться криминальным воздействиям, при этом наиболее вероятны внешние воздействия человека, находящегося вне зоны охраны объекта. К группе элементов ИСБ, с наибольшей вероятностью подверженным криминальным воздействиям, следует отнести ТСО периметровой СОС, а также СОТ, размещаемые на элементах ограждения объекта, стенах зданий, специальных опорных конструкциях, а также подходящие к ним кабели [66].

На рисунках 2.11-2.13 представлена структура возможных внешних криминальных воздействий на извещатели и видеокамеры СОТ с учетом особенностей их эксплуатации, находящихся вблизи границы охраняемой зоны. К основным видам возможных воздействий следует отнести: механическое, электрическое и оптическое (воздействие луча лазера). Экспериментальные исследования живучести ТСО проводились на примере оптических элементов СОТ (видеокамеры).

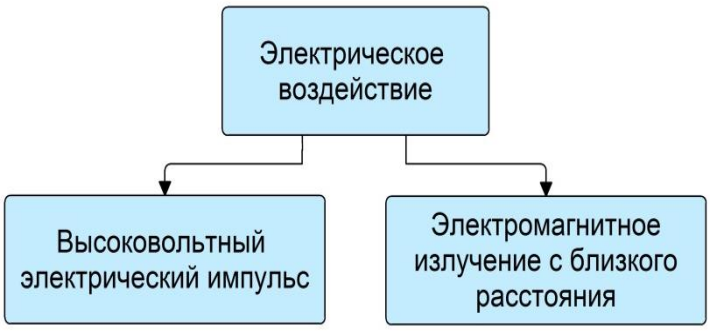


Рисунок 2.11 – Виды электрических криминальных воздействий

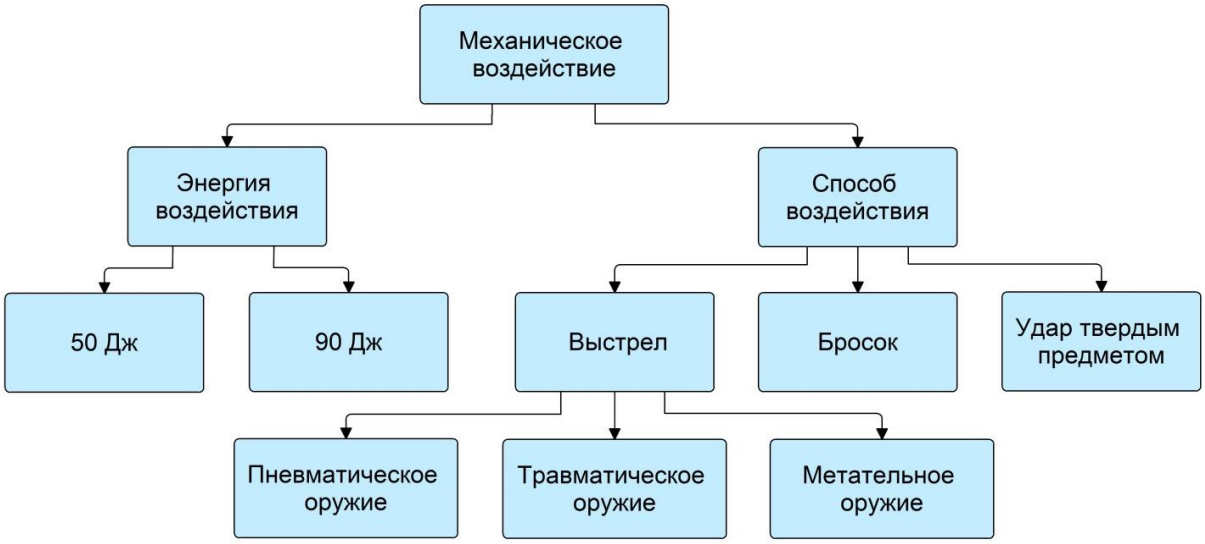


Рисунок 2.12 – Виды механических криминальных воздействий

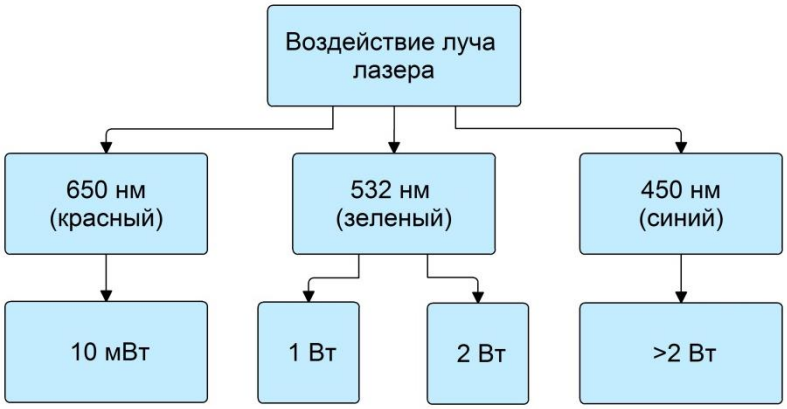


Рисунок 2.13 – Виды оптических криминальных воздействий

Для имитации нормированных воздействий использовались типовые инструменты и приспособления (таблица 2.5):

- для механического воздействия: пневматический и травматический пистолеты, рогатка, арбалет, грузы с различной массой;

- для электрического: электрошокер, носимая УКВ радиостанция;

- для оптического: лазеры различного вида и мощности.

Испытаниям подвергались типовые видеокамеры обычного, купольного и вандалозащищенного исполнения (таблица 2.6).

Таблица 2.5 – Средства криминальных воздействий

 Пневматический пистолет типа МР-53М	 Рогатка, доступная в точках розничной торговли	 Безлицензионный арбалет типа «Аспид»
 Травматический пистолет типа МР-79-9ТМ	 Электрошоковое устройство типа «ЭШУ-100»	 Носимая радиостанция типа Kenwood TK-248
 Лазерная указка мощностью 10 мВт, длина волны 650 нм (цвет излучения – красный)	 Лазерная указка мощностью 1 Вт, длина волны 532 нм (цвет излучения – зеленый)	 Лазерная указка мощностью 2 Вт, длина волны 450 нм (цвет излучения – синий)

В обобщенном виде средства и результаты испытаний представлены в таблицах 2.7 – 2.10.

Таблица 2.6 – Последствия механического и электрического внешнего криминального воздействия на СОТ

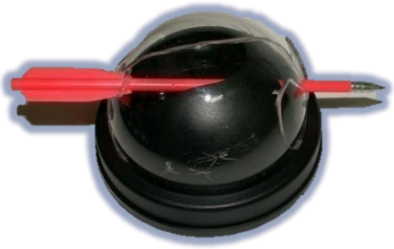
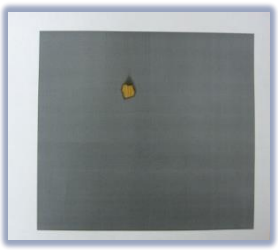
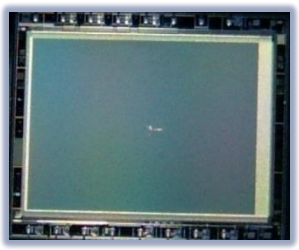
 Результат попадания в вандалозащищенную видеокамеру стальным шариком из рогатки	 Результат попадания в купольную видеокамеру дротиком из арбалета	 Результат попадания в вандалозащищенную видеокамеру пули из пистолета МР-79-9ТМ
 Результат попадания во внутреннюю видеокамеру пули из пистолета МР-79-9ТМ	 Результат механического воздействия на вандалозащищенную видеокамеру твердым предметом с энергией 90 Дж	 Результат воздействия на вандалозащищенную видеокамеру электрошокера
 Результат воздействия на матрицу видеокамеры лазерной указки мощностью 10 мВт, длина волны 650 нм (цвет – красный).	 Результат воздействия лазерной указки на лист бумаги 80 г/м^2 мощностью 2 Вт, длиной волны 450 нм (цвет – синий)	 Результат воздействия на матрицу видеокамеры лазерной указки мощностью 1-2 Вт, длиной волны 450 нм (цвет – синий)

Таблица 2.7 – Эффективность воздействия луча лазера

Длинна волны	Энергия воздействия	Тип видеокамеры	Степень воздействия
650 нм (красный)	до 10 мВт	обычного исполнения	низкая (возможна «засветка» изображения)
		купольная	низкая (возможна «засветка» изображения)
		вандало-защищенная	низкая (возможна «засветка» изображения), для отдельных видов камер «засветка» изображения прекращается при отклонении луча от оптической оси объектива на угол 30°
532 нм (зеленый)	до 1 Вт	обычного исполнения	средняя (возможна «засветка» изображения)
		купольная	средняя (возможна «засветка» изображения)
		вандало-защищенная	средняя (возможна «засветка» изображения), для отдельных видов камер «засветка» изображения прекращается при отклонении луча от оптической оси объектива на угол 45°
	до 2 Вт	обычного исполнения	высокая (возможна «засветка» изображения и выжигание отдельных пикселов матрицы)
		купольная	высокая (возможна «засветка» изображения и выжигание отдельных пикселов матрицы)
450 нм (синий)	более 2 Вт	обычного исполнения	высокая (возможна «засветка» изображения и выжигание отдельных пикселов матрицы)
		купольная	высокая (возможна «засветка» изображения и выжигание отдельных пикселов матрицы)
		вандало-защищенная	высокая (возможна «засветка» изображения и выжигание отдельных пикселов матрицы)
		Вероятность выжигания отдельных пикселов матрицы выше, чем у зеленого лазера	

Таблица 2.8 – Эффективность механического воздействия (свободно падающий груз)

Вид воздействия	Энергия воздействия	Тип видеокамеры	Разрушающий эффект
Удар грузом массой 5 кг, падающим с высоты 0,4 м	20 Дж	обычного исполнения	средний (по корпусу видеокамеры)
			высокий (по объективу)
		купольная	высокий (по корпусу видеокамеры)
			высокий (по объективу)
		вандало-защищенная	низкий (по корпусу видеокамеры)
			высокий (по объективу)
Удар грузом массой 5 кг, падающим с высоты 1 м	50 Дж	обычного исполнения	высокий (по корпусу видеокамеры)
			высокий (по объективу)
		купольная	высокий (по корпусу видеокамеры)
			высокий (по объективу)
		вандало-защищенная	низкий (по корпусу видеокамеры)
			высокий (по объективу)
Удар грузом массой 5 кг, падающим с высоты 1,8 м	90 Дж	обычного исполнения	высокий (по корпусу видеокамеры)
			высокий (по объективу)
		купольная	высокий (по корпусу видеокамеры)
			высокий (по объективу)
		вандало-защищенная	низкий (по корпусу видеокамеры)
			высокий (по объективу)

Таблица 2.9 – Эффективность механического воздействия (выстрел)

Вид воздействия	Энергия воздействия	Тип видеокамеры	Разрушающий эффект	Эффективная дистанция воздействия
1	2	3	4	5
Выстрел из пневматического пистолета	3 Дж	обычного исполнения	низкий	при любой дистанции воздействия эффективность низкая
		купольная	низкий	
		вандалозащищенная	низкий	
Выстрел из рогатки металлическим шариком весом 28 гр.	20 Дж	обычного исполнения	высокий	до 10 м (по корпусу видеокамеры)
				до 5 м (по объективу)
		купольная	высокий	до 15 м (по корпусу видеокамеры)
				до 5 м (по объективу)
		вандалозащищенная	низкий (по корпусу видеокамеры)	при любой дистанции воздействия эффективность низкая
			высокий (по объективу)	до 5 м (по объективу)
Выстрел из арбалета	20 Дж	обычного исполнения	высокий	до 10 м (по корпусу видеокамеры)
				до 5 м (по объективу)
		купольная	высокий	до 15 м (по корпусу видеокамеры)
				до 5 м (по объективу)
		вандалозащищенная	низкий (по корпусу видеокамеры)	при любой дистанции воздействия эффективность низкая
			высокий (по объективу)	до 5 м (по объективу)

Окончание таблицы 2.9

1	2	3	4	5
Выстрел из травматического пистолета типа МР-79-9ТМ	75 Дж	обычного исполнения	высокий	до 15 м (по корпусу видеокамеры)
				до 10 м (по объективу)
		купольная	высокий	до 15 м (по корпусу видеокамеры)
				до 10 м (по объективу)
		вандалозащищенная	низкий (по корпусу видеокамеры)	при любой дистанции воздействия эффективность низкая
			высокий (по объективу)	до 10 м (по объективу)

Таблица 2.10 – Эффективность воздействия излучения радиостанции и разряда электрошокера

Вид воздействия	Энергия воздействия	Тип видеокамеры	Степень воздействия
Разряд электрошокера	9 Дж	обычного исполнения	крайне низкая
		купольная	крайне низкая
		вандалозащищенная	крайне низкая
		Примечание: при пробое изоляции сигнального кабеля произошел выход из строя платы захвата видеорегистратора	
Излучение носимой УКВ радиостанции	5 Вт	обычного исполнения	крайне низкая
		купольная	крайне низкая
		вандалозащищенная	крайне низкая
		Примечание: воздействие не было зарегистрировано	

По результатам испытаний, можно сделать следующие выводы:

- механическое ударное воздействие с энергией от 20 Дж по объективу и выше выводит видеокамеры из строя в любом исполнении;

- воздействие носимых радиостанций не оказывает существенного влияния на функционирование;

- засветка объектива видеокамеры может привести к снижению качества изображения и некритичному нарушению работоспособности в виде выжигания отдельных пикселей матрицы.

Результаты исследований в значительной степени могут быть распространены на ТСО, используемые в аналогичных условиях эксплуатации: расположенные вне зданий, на открытых площадках, имеющих оптическую систему или корпуса нежесткой конструкции.

Полученные результаты исследования живучести ТСО позволяют определить меры противодействия, в частности при разработке рекомендаций по повышению устойчивости и надежности функционирования систем охраны критически важных объектов.

Выводы по разделу 2

1. Из представленного анализа статистических данных о путях и способах несанкционированных проникновений на охраняемые объекты в зависимости от их категории и структуры формируемой системы тревожной сигнализации следует, что относительно более частыми являются попытки проникновения на объекты высоких категорий А1-А3, в том числе на потенциально опасные промышленные предприятия. При этом основное количество составляют попытки проникновений в здания или помещения через оконные и дверные проемы.

2. Представленные материалы позволяют выделить наиболее вероятные способы, используемые нарушителями для незаконного проникновения на охраняемые объекты с целью совершения противоправных действий; определить меры противодействия, заключающиеся, в совершенствовании средств сбора и обработки данных, а именно, разработке и модернизации извещателей первого рубежа системы охранной сигнализации – магнитоконтактных, звуковых для блокировки остекленных конструкций, вибрационных и оптико-электронных.

3. Известные результаты анализа надежности показывают, что наиболее часто встречающейся причиной неисправности технических средств обнаружения является отказ комплектующих радиоэлементов. Однако значительную долю составляют причины, связанные с эксплуатацией на охраняемых объектах.

Неисправность в виде неустойчивой работы извещателя характеризуется наличием ЛСТ в процессе эксплуатации.

Ретроспективный анализ показал, что, несмотря на существенное уменьшение за последние десятилетия количества ЛСТ, надежность функционирования средств сбора и обработки данных остается неудовлетворительной. В перечень основных причин входят:

- неисправность (неправильный монтаж) магнитоконтактных, ударно-контактных, омических датчиков, нарушение целостности или отклонение от заданных параметров шлейфов сигнализации;

- неисправность (неправильная установка) извещателей оптико-электронного, емкостного, радиоволнового, ультразвукового, акустического, вибрационного принципа действия.

Это подтверждает необходимость разработки и модернизации данных видов технических средств, а также рекомендаций по их оптимальной установке и эксплуатации.

4. Проведенный статистический анализ показал, что с течением времени, в связи с ростом технической оснащенности и подготовленности лиц, совершающих противоправные действия криминальной и террористической направленности, резко возрастает вероятность попыток осуществления преступных посягательств на объекты высокой категории значимости с предварительным воздействием на технические средства охранной сигнализации с целью нарушения их нормального функционирования (саботаж).

Для противодействия таким посягательствам необходимо постоянно развивать системы охраны и в первую очередь целесообразно совершенствовать тактико-технические характеристики охранных извещателей, являющихся основой данных систем. Одним из основных направлений совершенствования охранных извещателей должно быть введение функции защиты от саботажа.

5. К группе элементов ИСБ, с наибольшей вероятностью подверженным криминальным воздействиям, следует отнести ТСО периметровой СОС, а также СОТ, размещаемые на элементах ограждения объекта, стенах зданий, специальных опорных конструкциях, а также подходящие к ним кабели.

Полученные результаты испытаний позволяют определить меры противодействия, в частности при разработке рекомендаций по повышению устойчивости и надежности функционирования систем охраны критически важных объектов.

3 ФОРМАЛИЗОВАННЫЙ АНАЛИЗ МОДУЛЬНОЙ СИСТЕМЫ СБОРА И ОБРАБОТКИ ДАННЫХ

3.1 Разработка модели и критерия эффективности обнаружения несанкционированного проникновения на охраняемый объект

3.1.1 Риск проникновения нарушителя на охраняемый промышленный объект

Безопасность охраняемого объекта определяется возможностью НП нарушителя. После проникновения объекту может быть нанесен материальный ущерб в виде порчи имущества, поджога, террористического акта и других противоправных действий независимо от результата его задержания сотрудниками охраны.

Таким образом, потенциальный риск несанкционированного проникновения (далее – риск НП) можно определить как количественную меру возможности реализации опасности совершения противоправных действий на объекте защиты и их последствий для людей и материальных ценностей [63].

Опасность объекту может быть ликвидирована, если произойдет своевременное обнаружение попытки проникновения – менее чем за время, необходимое для НП. Это время, связанное с прибытием сил реагирования, устанавливается нормативно для каждого объекта с учетом места его размещения, а также условий охраны.

Результаты и выводы, полученные при определении риска НП, могут быть использованы при проектировании системы охраны для обоснования параметров применяемых технических средств (подсистем) и мер технической укреплённости (физической защиты).

Характеристикой соответствия риска НП требуемому является неравенство [63, 76].

$$Q_{\text{нп}} \leq Q_{\text{нп}}^{\text{н}}, \qquad (3.1)$$

где $Q_{\text{нп}}^{\text{н}}$ – нормативное значение риска НП,

$Q_{\text{нп}}$ – расчетная величина риска НП.

Расчетная величина риска НП $Q_{\text{нп}i}$ для i-го сценария проникновения на объекты различных категории может быть определена с помощью выражения:

$$Q_{\text{нп}i} = P_{\text{пп}i}\,(1 - P_{\text{эо}i})\,(1 - P_{\text{дп}i}), \qquad (3.2)$$

где $P_{\text{пп}i}$ – оценка вероятности попытки проникновения на охраняемый объект для i-го сценария, может быть определена на основании статистических данных как частота попыток проникновения на охраняемый объект данного вида (категории) в течение установленного времени [77];

$P_{\text{эо}i}$ – оценка вероятности эффективного обнаружения НП охранной сигнализацией для i-го сценария;

$P_{\text{дп}i}$ – оценка вероятности противодействия НП дополнительными подсистемами, входящими в ИСБ объекта, воздействующими на факторы НП, для i-го сценария.

Для типового состава ИСБ, соответствующего ГОСТ Р 53704-2009 «Системы безопасности комплексные и интегрированные. Общие технические требования» и ГОСТ Р 56102.1-2014 «Системы централизованного наблюдения. Часть 1. Общие положения» в качестве систем, дополнительно противодействующих НП и формирующих $P_{\text{дп}i}$ могут быть подсистемы видеонаблюдения, технической укреплённости и инженерной защиты, а также контроля доступом [77]. Не следует исключать и возможное положительное влияние на $P_{\text{дп}i}$ и других систем безопасности промышленного объекта.

Все возможные сценарии S_i НП составляют конечное множество H, состоящее из k членов:

$$H \subseteq (S_1, S_2, \ldots S_i, \ldots S_k), \qquad (3.3)$$

В общем случае случайные события реализации возможных сценариев НП являются независимыми, несовместными и образуют полную группу.

Для конкретного объекта M при учете его конструктивных особенно-

стей, а также имеющейся информации о вероятности реализации конкретных сценариев количество членов множества H может быть сокращено:

$$H_M \subseteq (S_1, S_2, \ldots S_i, \ldots S_l),\ L < K. \qquad (3.4)$$

При формировании системы охраны объекта M условие (3.1) должно быть выполнено для каждого возможного сценария НП

$$Q_{\text{нп}i} \le Q_{\text{нп}}{}^{\text{н}},\ i = 1, \ldots l. \qquad (3.5)$$

При расчете должен выбираться тот сценарий развития НП, при котором достигается худшее (максимальное) значение риска НП. Поэтому в дальнейшем индекс «i» можно не указывать.

Если для объекта M максимальное значение риска НП из всех возможных сценариев будет $Q_{\text{нп}}{}^{M}$, то условие (3.5) можно записать в виде:

$$Q_{\text{нп}}{}^{M} \le Q_{\text{нп}}{}^{\text{н}}. \qquad (3.6)$$

Таким образом, с учетом (3.2), условие эффективности системы обнаружения НП будет

$$P_{\text{пп}} (1 - P_{\text{эо}}) (1 - P_{\text{дп}}) \le Q_{\text{нп}}{}^{\text{н}}. \qquad (3.7)$$

Докажем, что неравенство

$$P_{\text{эо}} \ge (1 - Q_{\text{нп}}{}^{\text{н}}/P_{\text{пп}}) \qquad (3.8)$$

является необходимым и достаточным условием эффективности системы обнаружения НП [5, 7, 58, 78, 79].

Рассмотрим систему охранной сигнализации, функционирующую без дополнительных подсистем в составе ИСБ, то есть положим $P_{\text{дп}} = 0$. В этом случае, преобразуя (3.7) относительно $Q_{\text{нп}}{}^{\text{н}}$, получим (3.6), что подтверждает необходимость (3.8) для выполнения условия (6) эффективности системы обнаружения НП.

Поскольку при наличии дополнительных подсистем в составе ИСБ $P_{\text{дп}}$ в силу определения вероятности всегда ≥ 0, неравенство (3.8) независимо от вида используемых подсистем только усиливается, что подтверждает достаточность условия (3.8) эффективности системы обнаружения НП.

Для типового состава ИСБ $P_{\text{дп}}$ может быть представлена в виде:

$$P_{\text{дп}} = 1 - (1 - P_{\text{в}}) (1 - P_{\text{т}}) (1 - P_{\text{д}})(1 - P_{\text{б}}),\ \qquad (3.9)$$

где $P_в$, $P_т$, $P_д$ – оценка вероятности противодействия НП подсистемами видеонаблюдения, технической укреплённости и инженерной защиты, а также контроля доступом соответственно, действующими в составе системы охраны;

$P_б$ – оценка вероятности противодействия НП системами безопасности промышленного объекта.

Графическое представление реализации условия (3.7) для конкретных выбранных значений параметров показано на рисунке 3.1.

Из рисунка 3.1 следует, что практическое снижение уровня риска НП до нормативного значения может быть достигнуто увеличением вероятности эффективного обнаружения нарушителя охранной сигнализацией $P_{эо}$, а также усилением положительного влияния иных систем, входящих в ИСБ, таких как системы пожарной сигнализации, вспомогательные и дополнительные системы.

В случае, если при большом значении вероятности попытки проникновения на охраняемый объект $P_{ппi}$ это не представляется возможным, в состав ИСБ объекта могут быть включены (усилены) средства видеонаблюдения, технической укреплённости и инженерной защиты, контроля доступом, задействованные для защиты от НП.

Следует отметить, что в настоящее время официально принятого понятия риска НП как и его нормативного уровня не установлено.

Рассмотрим подробнее параметр $P_{эо}$, характеризующий вероятность эффективного обнаружения нарушителя охранной сигнализацией, и его составляющие.

Применительно к рассматриваемой задаче под модулем ТС обнаружения (охранной сигнализации) следует понимать комплекс взаимосвязанных ТС ОС, предназначенный для обнаружения нарушителя при *i*-м сценарии (варианте) проникновения его на объект. Минимальный состав модуля – один извещатель, максимальный – рубеж, объектовая подсистема.

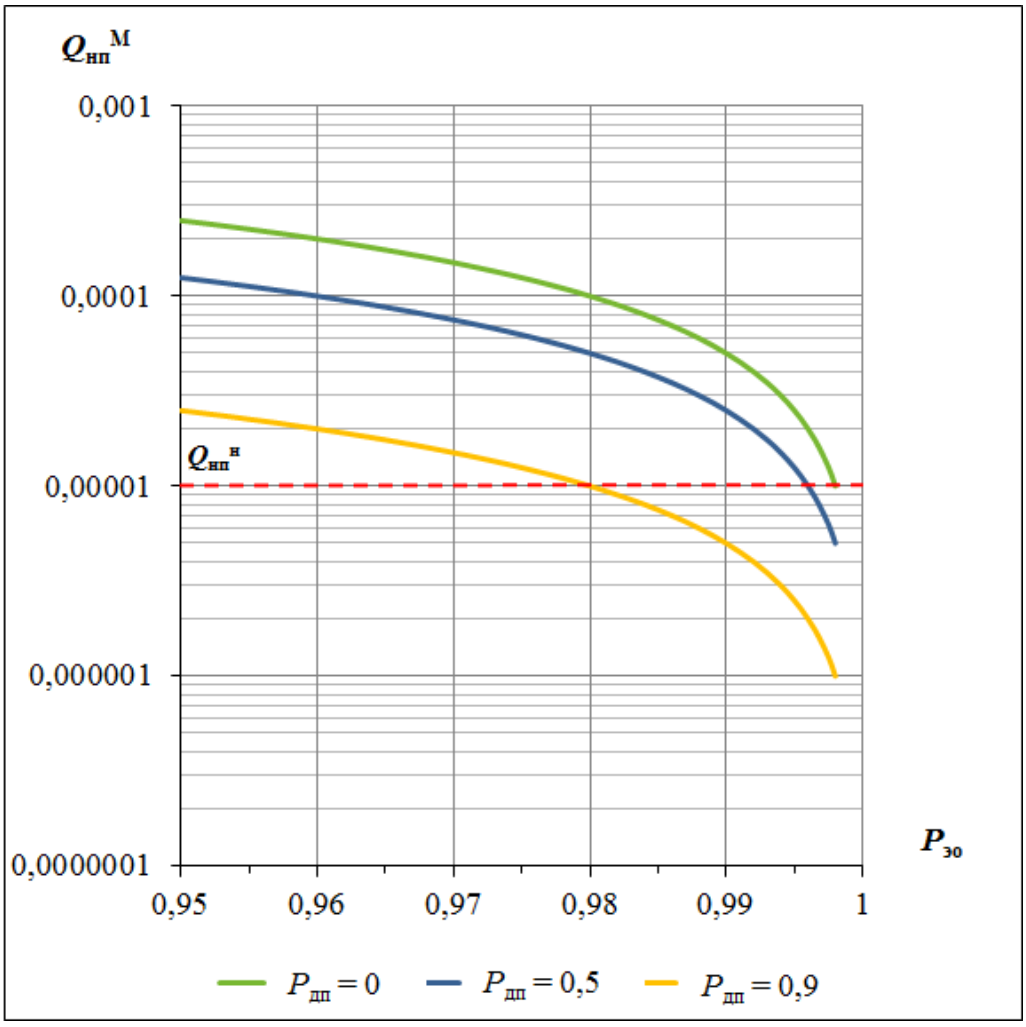


Рисунок 3.1 – Зависимость риска несанкционированного проникновения от вероятности эффективного обнаружения $P_{эо}$

Для $P_{эо}$ термин «эффективный» характеризует вероятность обнаружения с учетом комплекса воздействующих внутренних и внешних факторов.

В соответствии с этим выражение для $P_{эо}$ будет иметь вид:

$$P_{эо} = (1 - P_{от})\,(1 - P_{но})\,(1 - P_{с}), \qquad (3.10)$$

где $P_{от}$ – вероятность технического отказа ТС на период обнаружения;

$P_{но}$ – вероятность пропуска цели (не обнаружения);

$P_{с}$ – вероятность саботажа.

Под саботажем понимаем результат преднамеренных действий нарушителя, приводящий к нарушению функций обнаружения НП системой охраны.

Существующие на сегодняшний день теоретические и экспериментальные методы позволяют провести количественную оценку риска НП на этапе проектирования системы охраны.

$P_{пп}$ может быть определена на основании статистических данных как частота попыток проникновения на охраняемый объект данного вида (категории). Например, в [80] приводится методика и пример расчета вероятности появления нарушителя на объектах разной категории. Согласно оценкам профессора Шепитько Г. Е. вероятность появления нарушителя на объектах $P_{ц}$ составляла на период исследования от 0,005 (особо важные объекты), 0,05 (музеи и простые объекты) до 0,12 (важные объекты) в год.

Таким образом, введение параметра риска НП позволяет дать комплексную оценку опасности совершения противоправных действий на охраняемом объекте.

Полученные значения риска НП могут быть использованы при проектировании системы охраны для обоснования параметров применяемых подсистем (модулей, технических средств обнаружения), а также мер технической укреплённости и физической защиты объекта [81].

Рассмотрим методику применения параметра риска НП и критерия эффективности системы обнаружения (3.1) при проектировании системы охранно-пожарной сигнализации.

Обобщенный алгоритм последовательности реализуемых действий представлен на рисунке 3.2.

После задания параметров $P_{пп}$ и $Q_{нп}^{н}$ в соответствии с требованиями нормативных документов формируется структура и состав технических средств обнаружения на охраняемом объекте, определяется расчетное значение вероятности эффективного обнаружения НП, а затем – риска $Q_{нп}$.

Если полученное значение риска удовлетворяет условию $Q_{нп} \leq Q_{нп}^{н}$, принятые структура и состав технических средств системы сигнализации считаются удовлетворительным и данный этап проектирования заканчивается. Если неравенство не выполняется, в формируемую систему вносят изменения, направленные на увеличение $P_{эо}$.

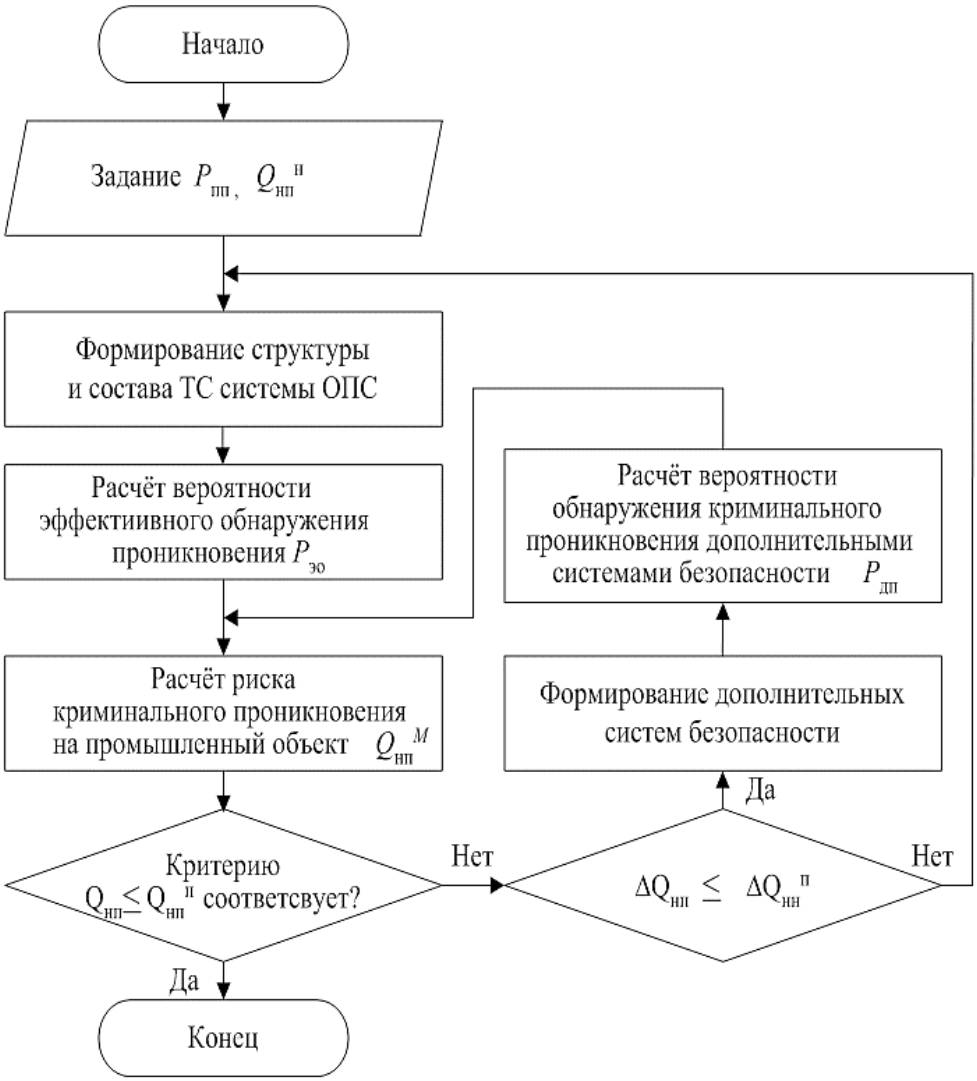


Рисунок 3.2 – Обобщенный алгоритм выбора оптимальной системы охранно-пожарной сигнализации

При этом фиксируется достигнутое приращение $\Delta Q_{нп}$. Процесс совершенствования проектируемой системы продолжается до тех пор, пока приращение $\Delta Q_{нп}$ не становится ниже установленного предельно допустимого уровня или оно становится экономически нецелесообразным. В этом случае рассматривается возможность увеличения $Q_{нп}$ за счет дополнительных подсистем, включаемых в систему безопасности.

Следует отметить, что для практической реализации данной методики необходимо получить более конкретные математические выражения для определения параметра $P_{эо}$.

3.1.2 Комплексный показатель эффективности обнаружения проникновения нарушителя на охраняемый объект

Одним из перспективных вариантов комплексной оценки эффективности системы сигнализации может быть оценка по интегральному показателю – вероятности эффективного обнаружения нарушителя охранной сигнализацией $P_{эо}$ [5].

Вероятность эффективного обнаружения НП $P_{эо}$ можно определить как свойство технических средств обнаружения или объектовой системы, характеризующее истинность выходного сигнала за заданный промежуток времени t при условии ее исправности на момент включения. Истинным выходным сигналом для системы является сигнал, правильно отражающий состояние охраняемого объекта (наличие или отсутствие на нем нарушителя), а также состояние самой системы (модуля) обнаружения – наличие или отсутствие в ней неисправности (саботажа), нарушающей функции контроля охраняемого объекта и передачу сигнала тревоги. Чем больше $P_{эо}$, то есть чем ближе она к единице, тем более качественно функционирует система охранной сигнализации.

При проектировании, в случае задания параметра риска НП, условие для требуемого значения $P_{эо}$ проектировании системы охраны можно записать в виде:

$$P_{эо} \geq (1 - Q_{нп}{}^{н}/P_{пп})\,(1 - P_{дп}). \qquad (3.11)$$

Условие (12) должно выполняться для любого сценария НП на охраняемый объект. В соответствии с (3.10) выражение для вероятности эффективного обнаружения НП $P_{эо}$ имеет вид:

$$P_{эо} = P_{бр}\,P_{до}\,P_{ос}. \qquad (3.12)$$

Получим выражения членов, входящих в (3.12) для количественной оценки $P_{эо}$.

Вероятность безотказной работы $P_{бр}$ характеризуется вероятностью работоспособного состояния к началу НП. Считая, что ССОД ИСБ является

обслуживаемой и восстанавливаемой, $P_{бр}$ можно представить в виде [5, 82]:

$$P_{бр} = \frac{T_{но}}{T_{но} + T_{в}} e^{-\frac{t_н}{T_{но}}}, \quad (3.13)$$

где $T_{но}$ – среднее время наработки на отказ;

$T_{в}$ – среднее время восстановления,

$t_{н}$ – время наблюдения.

При проектировании необходимо формирование ССОД из технических средств, обладающих максимальными значениями параметров надежности и удобных для технического обслуживания в процессе эксплуатации.

Эти же требования необходимо выполнять в отношении подсистем, дополнительно включаемых в состав ССОД, обеспечивающих безопасность и влияющих на обнаружение НП.

Вероятность достоверного обнаружения НП $P_{до}$ является основным параметром извещателя (модуля) при его работе в составе СОС, характеризует степень выполнения функции основного назначения, а именно эффективность работы ТС обнаружения.

$P_{до}$ определяется не только особенностями принципа действия самого извещателя, но и местом его размещения, ориентацией чувствительной зоны, установленной чувствительностью и т. п. [83].

В процессе обнаружения присутствуют два практически независимых и последовательных этапа: установление тактического и приборного контакта цели с извещателем [84]. Под тактическим контактом понимается процесс попадания цели в зону обнаружения извещателя. Приборный контакт характеризуется собственно процессом обнаружения.

Очевидно, что оба этих этапа являются функцией времени, как и соответствующие им вероятности.

$$P_{до}(t) = P_{тк}(t)\, P_{пк}(t), \quad (3.14)$$

где $P_{тк}(t)$ – вероятность тактического контакта;

$P_{пк}(t)$ – вероятность приборного контакта.

Значение $P_{тк}(t)$ определяется характеристиками движения цели относительно направления на извещатель. Если в процессе проникновения нарушитель может двигаться на объекте в N направлениях, только одно из которых может привести к приборному контакту, то $P_{тк}(t)$ можно определить по формуле:

$$P_{тк}(t) = P_{ткi}(t), \tag{3.15}$$

$$\sum_{i=1}^{N} P\text{тк}i(t) = 1. \tag{3.16}$$

Отсюда следует требование при формировании ССОД блокировки извещателями всех вероятных направлений движения нарушителя.

Считая, что извещатель расположен так, что нарушитель при движении на объекте обязательно попадет в зону обнаружения (N = 1), можно записать

$$P_{до}(t) = \begin{cases} 0\ , & \text{при } t < t_1; \\ P_{пк}(t), & \text{при } t \geq t_1, \end{cases} \tag{3.17}$$

где t_1 – интервал времени от начала проникновения, за которое нарушитель достигнет зоны обнаружения извещателя.

Очевидно, что t_1 в общем случае также величина случайная.

При наступлении приборного контакта возможны варианты:

1) цель сразу попадает в зону уверенного обнаружения извещателя;

2) цель при движении пересекает границу зоны обнаружения, характеризующуюся низкой чувствительностью.

Первый вариант характерен для извещателей, имеющих практически равномерную чувствительность в зоне обнаружения. Для извещателей с объемной или поверхностной зоной обнаружения это соответствует ситуации, когда зона обнаружения значительно превышает размеры объекта.

В этом случае если из эксперимента или статистических наблюдений известна мгновенная (элементарная) плотность вероятности обнаружения g_0, характеризующая вероятность обнаружения цели извещателем конкретного вида за элементарный промежуток времени, то функция плотности вероятности времени обнаружения будет определяться показательным законом (рисунок 3.3):

$$f(t_0)=\begin{cases} g_0 \mathrm{e}^{-g_0 \cdot t_0}, & \text{при } t_0 \geq 0 \\ 0, & \text{при } t_0 < 0. \end{cases} \qquad (3.18)$$

Второй вариант характерен для извещателей с поверхностной или объемной зоной обнаружения, расположенной внутри охраняемого пространства. В этом случае время обнаружения будет иметь нормальный закон распределения. При этом надо учитывать, что время как параметр не может быть отрицательным, поэтому диапазон возможных его значений ограничен полуинтервалом от 0 до ∞. Данным требованиям соответствует усеченный нормальный закон распределения, для которого плотность вероятности определяется выражением (рисунок 3.4):

$$f(t_i)=\begin{cases} 0, & \text{при } t_i \leq 0; \\ \dfrac{C_i}{\sigma_i\sqrt{2\pi}} e^{-(t_i-M(t_i))^2/2\sigma_i^2}, & \text{при } 0 < t_i < \infty, \end{cases} \qquad (3.19)$$

где C_i – нормирующий множитель, значение которого выбирают из условия равенства единице площади под кривой плотности вероятности $f(T_i)$.

$$C_i = \frac{\sigma_i\sqrt{2\pi}}{\int_0^{\infty} e^{-(t_i-M(t_i)^2/2\sigma_i^2}\mathrm{d}t_i}. \qquad (3.20)$$

Следует отметить, что для значений $t_i >> 0$ при относительно небольших соответствующих σ_i достаточную точность может дать использование и простого нормального (неусеченного) распределения. Это соответствует ситуации, когда зона обнаружения свободно размещена в охраняемом пространстве, не касаясь его границ.

Практический интерес представляет определение мгновенной плотности вероятности обнаружения g_0. Рассмотрим методику приближенной количественной оценки g_0, исходя из следующих соображений.

Определим вероятность обнаружения цели автоматическим извещателем за время $t_д$

$$t_о < t_д, \qquad (3.21)$$

где $t_д$ – время достоверного обнаружения цели исправным извещателем определенного вида.

$$P_{до}(t_о < t_д) = \int_0^{t_д} f(t_о)\mathrm{d}t_о = \begin{cases} 1-\mathrm{e}^{-g_0 t_д}, & \text{при } t_д \geq 0 \\ 0, & \text{при } t_0 < 0. \end{cases} \quad (3.22)$$

Время $t_д$ может быть определено из значений максимального времени обнаружения извещателем, установленного в технических условиях.

Это время подтверждается экспериментально при межведомственных и типовых испытаниях на заводе-изготовителе.

В таких исследованиях вероятность достоверной реализации случайного события $P_{до}(t_о < t_д)$ обычно принимается равной

$$P_{до}(t_о < t_д) \geq 0{,}95. \quad (3.23)$$

Подставляя выражение (3.22) в (3.21), получим неравенство, из которого определим область значений g_0.

$$1 - \mathrm{e}^{-g_o t_д} \geq 0{,}95. \quad (3.24)$$

Отсюда $g_0 \geq \ln 20/t_д = 2{,}996/t_д$.

Например, для ультразвукового извещателя «Эхо-5» максимальное время движения цели до ее достоверного обнаружения не должно превышать 3 с. Таким образом, минимальное нормативно установленное значение мгновенной плотности вероятности обнаружения g_0 для данного типа извещателя составляет примерно 1 $с^{-1}$. Данное значение пригодно и для тех ТСО, которые по чувствительности соответствуют стандарту.

Следует отметить, что в рассмотренном случае мгновенная плотность вероятности обнаружения g_0 определена для конкретных параметров движения цели, указанных в технических условиях. Для других условий обнаружения она может существенно отличаться и может быть определена в результате натурных испытаний извещателей.

Полученные таким образом значения мгновенной плотности вероятности обнаружения g_0 могут быть использованы в инженерных расчетах при оценке эффективности систем тревожной сигнализации.

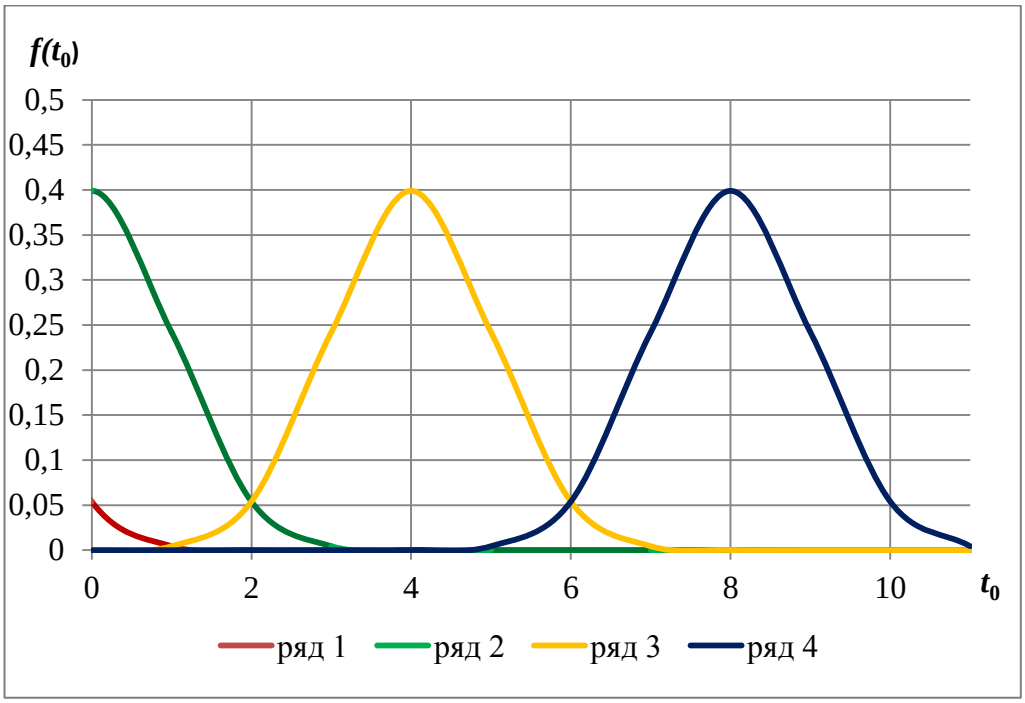


Рисунок 3.3 – Закон распределения случайной величины $f(t_o)$

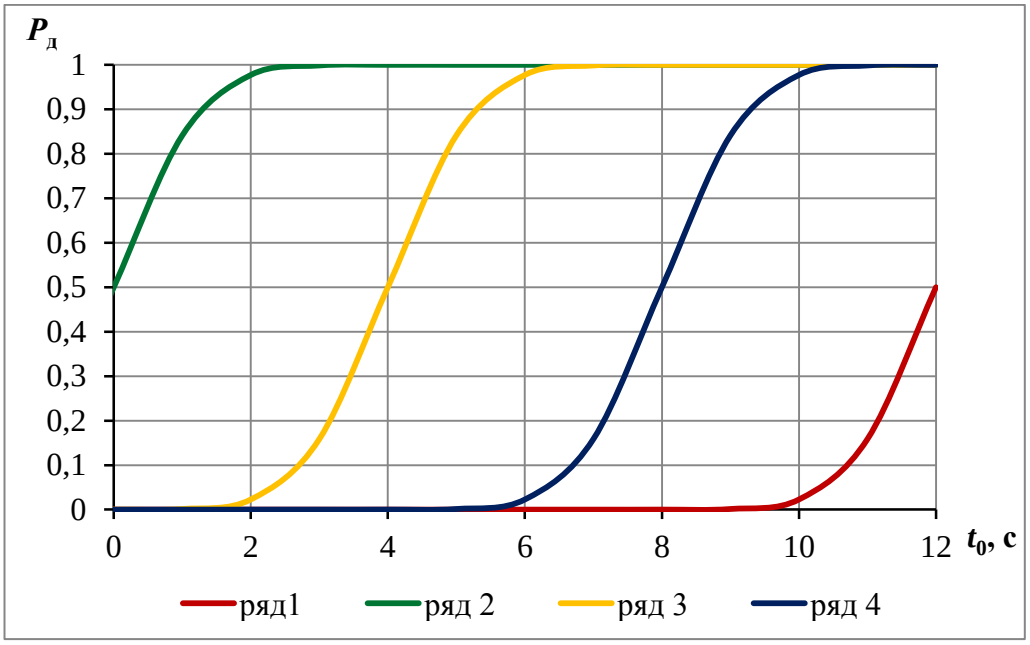


Рисунок 3.4 – Зависимость вероятности обнаружения цели $P_{до}$ от времени обнаружения $t_о$

Своевременное обнаружение гарантирует пресечение НП до совершения нарушителем действий, приносящим существенный материальный и (или) иной ущерб объекту.

Для квалифицированного нарушителя в общем случае можно определить следующие этапы его действий:

- подготовка к НП;

- преодоление технической укреплённости объекта и средств инженерной защиты;

- собственно НП;

- совершение противоправных действий на объекте.

Каждому этапу соответствует промежуток времени, зависящий от квалификации и цели нарушителя, характера объекта, а также комплекса мер, принятых для обеспечения безопасности.

Задача, решаемая ТСО в системе противокриминальной защиты, – достоверное обнаружение нарушителя или его действий, направленных на НП. При этом обнаружение может осуществляться на всех перечисленных выше этапах.

С целью повышения эффективности обнаружения для важных объектов система охранной сигнализации может формироваться как многорубежная. Первый рубеж, включающий ТСО, как правило устанавливаемые на внешней границе, «периметре» объекта, обнаруживает не только преодоление технической укреплённости и средств инженерной защиты, но и «попытку» проникновения – действия нарушителя, за которыми НП может и не последовать. К таким действиям относится разбитие стекла, разрушение ограждения и т. п. Особенность ТСО первого рубежа – раннее обнаружение нарушителя, что существенно увеличивает вероятность пресечения НП [3].

Вероятность обнаружения саботажа $P_{\text{ос}}$. На этапе подготовки НП нарушитель может совершать действия, направленные на нарушение работоспособности ТСО. Результат таких действий называют саботажем. Саботажу

способствует то, что многие ТСО не могут устанавливаться скрытно и к ним, когда объект не находится под охраной, возможен доступ посторонних лиц. Поэтому для успешного пресечения НП необходимо обнаружение не только попытки проникновения, но и подготовки к нему путем саботажа. Следовательно, можно определить обнаружение саботажа как «сверхраннее» обнаружение НП.

Проведенный анализ ТСО, используемых в современных системах охранной сигнализации, показал, что многие из них имеют функциональные возможности обнаружения как НП, так и саботажа (таблица 3.1). Анализ основан на имеющихся данных рынка ТСО и известных публикациях в данной области.

Следует отметить, что возможности обнаружения саботажа отдельными видами ТСО далеко не исчерпаны. Данное направление активно развивается, и именно с ним связано дальнейшее совершенствование систем охранной сигнализации.

При функционировании на отдельные элементы СОС воздействует большое число различных внешних и внутренних факторов, нарушающих устойчивое состояние системы. Результатом такого воздействия может быть ложное срабатывание СОС или нарушение работоспособности, в том числе не обнаруживаемое сразу же после своего возникновения.

Наиболее опасной внешней причиной, приводящей к потере контроля объекта или его части, является человеческий фактор – умышленный саботаж, так как именно после него наиболее вероятно несанкционированное проникновение на охраняемый объект с последующими противоправными действиями нарушителя.

Таблица 3.1 – Функциональные возможности раннего обнаружения извещателей разного вида

Вид извещателя	Функциональные возможности раннего обнаружения	
	Обнаружение попытки несанкционированного проникновения	Обнаружение саботажа ТСО
Электроконтактные	+	-
Магнитоконтактные	+	+
Ударно-контактные	+	+
Электромагнитные бесконтактные	+	+
Пьезоэлектрические	+	-
Емкостные	+	-
Звуковые	+	+
Инфразвуковые	-	-
Ультразвуковые	-	+
Вибрационные	+	-
Пассивные оптико-электронные	-	+
Активные оптико-электронные	+	+
Радиоволновые	-	+
Электростатические	+	-
Трибоэлектрические	+	-
Примечание: + возможность обнаружения имеется; – возможность обнаружения отсутствует.		

Эффективность функционирования СОС в значительной степени зависит от вероятности обнаружения саботажа. Считая события саботажа независимыми, целевая функция может быть представлена в виде [85]:

$$P_{oc} = \prod_{j=1}^{m} g_j, \tag{3.25}$$

где m – количество вариантов саботажа;

g_j – относительное количество обнаруженных попыток саботажа данного вида (вероятность обнаружения).

Основным условием для эффективного построения и функционирования ССОД является повышение вероятности обнаружения саботажа. Следовательно, задачей проектирования будет достижение максимума целевой функции:

$$P\text{oc}_{\max} = \max P\text{oc}(x),\ x \in X^*;\ P\text{oc}(x) \in P_{\text{ос}}^* , \qquad (3.26)$$

где X^* – множество допустимых вариантов построения СОС;

$P_{\text{ос}}^*$ – допустимая область изменений Pос.

Любой j-й вариант саботажа должен надежно обнаруживаться, то есть $g_j \to 1$. Кроме этого, при выборе варианта построении СОС следует учитывать необходимость выполнения принципа непрерывности, заключающегося в том, что не должно быть пропущено ни одного возможного варианта саботажа. При нарушении этого принципа, например, при $g_k = 0$, где k – необнаруживаемый вариант саботажа, $P_{\text{ос}} = 0$, то есть вся СОС становится неэффективной.

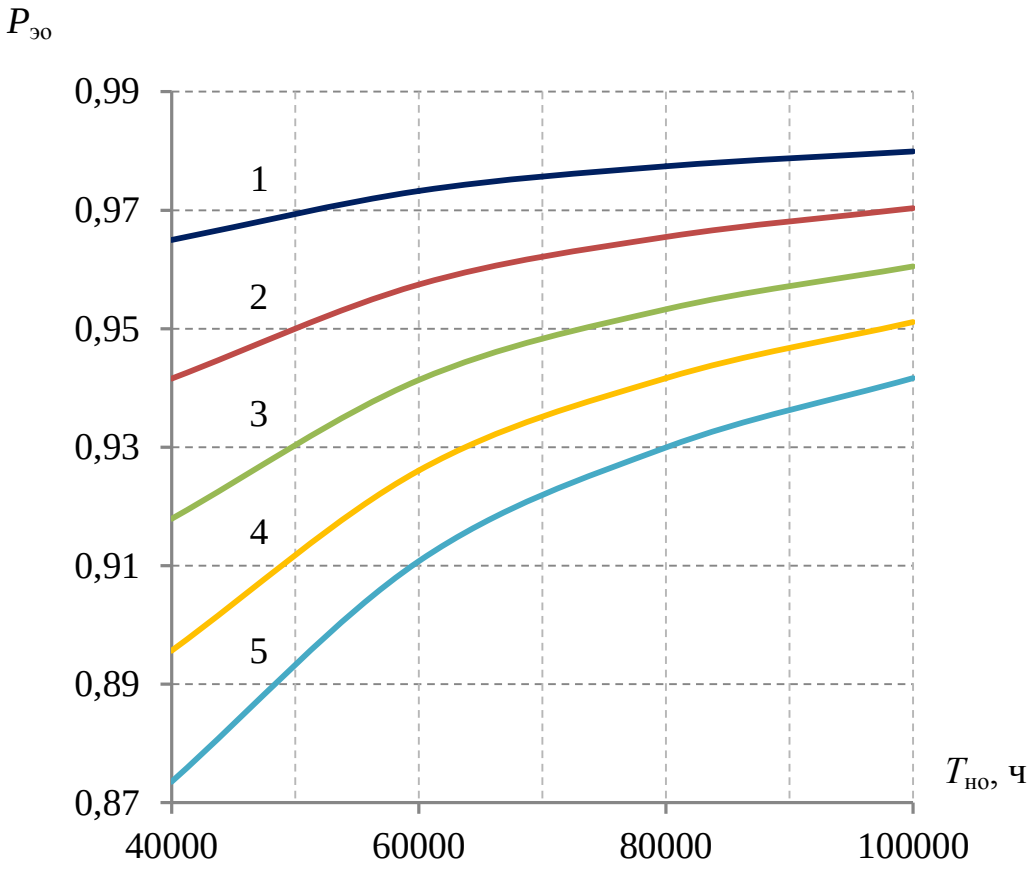
Таким образом, необходимым дополнительным условием формирования эффективной СОС является требование полноты системы обнаружения случайных попыток саботажа. Для повышения значения Pос необходимо совершенствование технических средств обнаружения, при котором они будут обнаруживать практически любое нарушение своей работоспособности и формировать соответствующие извещения в СОС.

Подставив в формулу (3.12) математические выражения для входящих в него членов, получим расчетное выражение для вероятности эффективного обнаружения $P_{\text{эо}}$:

$$P_{\text{эо}} = P_{\text{бр}} P_{\text{до}} P_{\text{ос}} = \frac{T_{\text{но}}}{T_{\text{но}} + T_{\text{в}}} e^{-\frac{t_н}{T_{\text{но}}}} (1 - e^{-g_o t_д}) \prod_{j=1}^{m} g_j , \qquad (3.27)$$

$P_{эо}$ определяет вероятность, с которой система сигнализации за заданный промежуток времени $t_н$ формирует достоверный сигнал о наличии несанкционированного проникновения нарушителя на охраняемый промышленный объект с учетом состояния средства обнаружения и наличия внешних мешающих факторов различной природы.

На рисунке 3.5 в качестве примера показаны графики зависимости $P_{эо}$ от времени наработки на отказ $T_{но}$ для конкретных значений остальных параметров.



$t_н$: 1 – 1000 ч.; 2 – 2000 ч.; 3 – 3000 ч.; 4 – 4000 ч.; 5 – 5000 ч;

$(1 - e^{-g_0 t_д}) = 0{,}09$; $\prod_{j=1}^{m} g_j = 1{,}0$; $T_в = 24$ час

Рисунок 3.5 – График зависимости вероятности эффективного обнаружения от параметров надежности

Количественное значение $P_{эо}$ может быть использовано при проектировании системы охранно-пожарной сигнализации в соответствии с методикой раздела 3.1.1 по критерию соответствия риска НП установленного значения.

3.2 Оптимизация проектирования охранно-пожарной сигнализации на основе показателя вероятности эффективности обнаружения проникновения нарушителя

Формирование оптимальной системы охранно-пожарной сигнализации может быть реализовано по критерию достижения максимума вероятности эффективного обнаружения [5]:

$$P_{эоi}(t) \to \max, \qquad i = 1, \ldots, r, \tag{3.28}$$

где r – количество рассматриваемых вариантов выбираемого модуля обнаружения.

Для данного критерия единственным требованием является получение значения $P_{эо}$, соответствующего условию формирования эффективной системы обнаружения. Затраты на достижение результата проектирования при этом не учитывается.

На практике для проектировщика возникают ограничения, связанные с необходимостью учета затрат на изготовление и техническую эксплуатацию средств обнаружения.

Рассмотрим в этом случае процесс проектирования оптимального модуля обнаружения (извещателя) по вероятности $P_{эо}$.

Пусть для некоторого «исходного» модуля может быть определено значение $P_{эо}(t)$ и его стоимость $S_о$. Пусть существует конечное число $M_с$ возможных способов увеличения вероятности эффективного обнаружения им нарушителя. Каждый из них может увеличить $P_{эо}(t)$ исходного варианта на $\Delta P_{эо}(t)_{i,j}$.

$$\Delta P_{эо}(t)_{i,j} = P_{эо}(t)_{i,j} - P_{эо}(t)_{(i\text{-}1),(j\text{-}1)}, \tag{3.29}$$

где $P_{эо}(t)_{(i\text{-}1),(j\text{-}1)}$, – вероятность эффективного обнаружения «исходного» модуля;

$P_{эо}(t)_{i,j}$ – вероятность эффективного обнаружения модуля, использующего i-й способ повышения $P_{ЭО}(t)$.

При использовании *i*-го способа увеличивается стоимость технического средства на величину $\Delta S_{i,j}$

$$\Delta S_{i,j} = S_{i,j-1} - S_{i,j}. \quad (3.30)$$

Индекс «*j*» означает порядковый номер, под которым рассматривается применение *i*-го способа при проектировании модуля. Это связано с тем, что величина приращения $\Delta P_{ЭО}(t)_i$, так же как и ΔS_i, в общем случае зависит от исходных значений $\Delta P_{ЭО}(t)_{(j-1)}$ и $\Delta S_{(j-1)}$. Кроме того, величина каждого последующего приращения $\Delta P_{ЭО}(t)_i$ и ΔS_i может зависеть также от того, какие способы применялись ранее.

Задача выбора варианта модуля с максимальной эффективностью обнаружения может быть сформулирована следующим образом:

требуется найти max $P_{ЭО}(t)$ $[S_{i,j}]$ при ограничении на общую стоимость модуля $S_{уст}$

$$S_{i,j} = S_o + \sum_{i=1}^{N_c} \Delta S_{i,j} \le S_{уст}. \quad (3.31)$$

При необходимости число ограничений может быть увеличено, например, введением ограничения на вероятность обнаружения и т. п.

Количество N_c используемых способов повышения $P_{ЭО}(t)$ при проектировании определяется условием достижения стоимости заданного или близкого к нему установленного значения

$$S_{уст}(N_c) \le M_c. \quad (3.32)$$

В общем виде решение задачи может быть получено при рассмотрении всех возможных вариантов и выборе одного варианта с максимальной $P_{ЭО}(t)$, удовлетворяющей условию (3.32).

Вполне очевидно, что при больших M_c и N_c количество вариантов может быть значительным, что существенно затруднит практическое решение задачи. Гораздо быстрее это решение может быть получено при использовании метода динамического программирования [86, 87].

Определим суммарную удельную стоимость модуля $S_{\text{у}}$, характеризующую затраты на приращение вероятности эффективного обнаружения, достигаемую при модернизации. При этом предполагаем, что использование различных схемотехнических способов можно производить в любом порядке и достигаемое при этом приращение $\Delta P_{\text{ЭО}i}(t)$ не зависит от порядка применения способа.

Очевидно, что последовательность используемых способов будет оптимальной, если суммарные удельные затраты на модернизацию модуля будут минимальными.

$$S_y = \frac{S_0}{P_{\text{ЭО}0}(t)} + \frac{\Delta S_1}{\Delta P_{\text{ЭО}1}(t)} + \cdots + \frac{S_i + S_{i,\ i-1}}{\Delta P_{\text{ЭО}i}(t)} \rightarrow \min, \quad (3.33)$$

где S_0, $P_{\text{ЭО}0}(t)$ – соответственно начальное значение затрат и вероятность эффективного обнаружения «исходного» технического средства;

S_i, $\Delta P_{\text{ЭО}i}(t)$ – соответственно затраты на использование в «исходном» техническом средстве i-го способа повышения вероятности эффективного обнаружения и достигаемое при этом приращение этой вероятности.

$$S_{i,\ i\text{-}1} = \Delta S_{i,\ 1} + \Delta S_{i,\ 2} + \Delta S_{i,\ i\text{-}1}, \quad (3.34)$$

где $\Delta S_{i,\ i\text{-}1}$ – дополнительные к S_i затраты на использование в модуле i-го способа повышения вероятности эффективного обнаружения, если до этого был использован $(i - 1)$ способ, $i = 1, 2, \ldots$

Из выражения (3.34) видно, что полученное значение параметра S является аддитивным, при этом перестановкой элементов последовательности может быть достигнуто его экстремальное (минимальное) значение, то есть для данной задачи справедлив принцип оптимальности Беллмана [86, 87].

Оптимальная последовательность вида (3.33) должна предусматривать применение способов повышения вероятности эффективного обнаружения в порядке невозрастания удельного приращения стоимости применения i-го способа при условии использования предыдущего $(i - 1)$ способа.

Вполне очевидно, что в случае взаимной независимости применяемых способов соответствующие приращения будут равны нулю, в случае незави-

симости порядка их применения – одинаковы, что является следствиями рассматриваемого принципа оптимальности.

При применении данного метода размещают полученные в результате расчетов члены последовательности (3.33) в порядке уменьшения удельного приращения стоимости применения *i*-го способа при условии использования предыдущего (*i* – 1) способа. Процесс синтеза модуля будет закончен при достижении суммарной величины вероятности эффективного обнаружения модуля (или его суммарной стоимости) с установленной точностью требуемого (предельного) значения. Алгоритм оптимизации проектирования системы охранно-пожарной сигнализации представлен на рисунке 3.6.

Рассмотрим в качестве примера вариант использования данного метода при модернизации звуковых охранных извещателей серии «Стекло», предназначенных для обнаружения разрушения остекленных конструкций [63, 64]. В качестве «исходного» технического средства выбираем извещатель – аналог «Стекло-1», обладающий недостаточно высокими значением основных ТТХ и имеющий $P_{ЭО}(1000) = 0{,}9$. В соответствии с техническим заданием себестоимость модернизированного звукового извещателя не должна превышать себестоимость аналога более чем в 1,3 раза.

В таблице 3.2 приведены рассмотренные при проектировании способы увеличения вероятности эффективного обнаружения $P_{ЭО}(t)$ и результат их применения в «исходном» звуковом извещателе. Данные методы апробированы и уже использованы в извещателях «Стекло-2» – «Стекло-4» [23, 88-90].

Для выявления взаимодействия способов может быть построена матрица, диагональными элементами которой являются величины приращений стоимости к минимальному звуковому извещателю S_i, а остальными элементами – добавка к этому приращению в результате использования ранее другого способа.

Анализ показывает, что способы 1 и 4 являются зависимыми и применение первым 4-го способа, а вторым – 1-го более выгодно.

С учетом затрат на реализацию данных способов оптимальная последовательность будет 4, 1, 2, 3, 5.

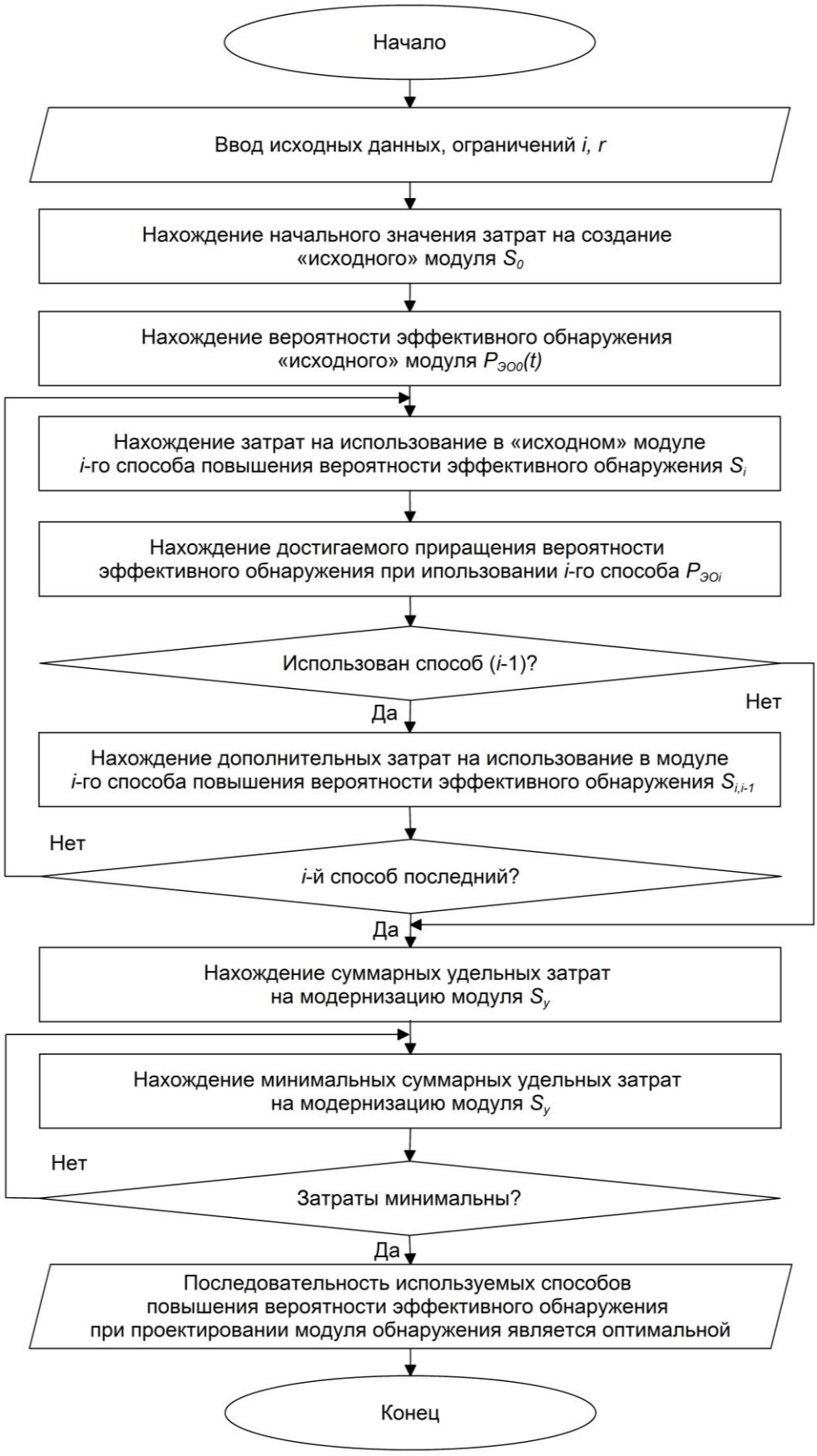


Рисунок 3.6 – Алгоритм оптимизации проектирования системы охранно-пожарной сигнализации

Расчет показывает, что 3-й и 5-й способы при их достаточно большой эффективности не удовлетворяют условию ограничения на себестоимость модернизируемого модуля, поэтому не могут быть применены. Таким образом, в новом звуковом извещателе могут быть использованы способы 4, 1, 2. Вероятность эффективного обнаружения при этом возрастает на 0,034 и составит $P_{ЭО}(1000) = 0{,}934$.

Таблица 3.2 – Способы повышения вероятности эффективного обнаружения звукового извещателя

№ п/п	Наименование способа	На какой параметр $P_{ЭО}$ влияет	$\Delta P_{ЭО}$ (1000)
1	Селекция сигнала в двух спектральных областях с логическим объединением «2И»	$P_{до}$, $P_{бр}$	0,013
2	Применение имитатора звукового сигнала разрушения стекла	$P_{до}$, $P_{ур}$	0,005
3	Введение периодического контроля функционирования и защиты от саботажа	$P_{бр}$, $P_{ос}$	0,018
4	Анализ непрерывности и длительности сигнала	$P_{до}$	0,016
5	Применение единого протокола обмена данными в системе охранной сигнализации	$P_{бр}$, $P_{ос}$	0,08

Следует отметить, что практическое применение данного метода показывает значительное влияние конкретной схемной реализации применяемого способа на $P_{ЭО}(t)$. Это придает большое значение совершенствованию схемотехнических и технологических приемов применения различных способов улучшения параметров проектируемого модуля.

Таким образом, рассмотренный метод решения задачи оптимизации, учитывающий как основные характеристики обнаружения, так и затраты на их реализацию, может быть использован при проектировании эффективной системы охранно-пожарной сигнализации промышленного объекта.

3.3 Оптимизация состава автоматизированной системы централизованной охраны промышленного предприятия

Для обеспечения оптимального состава ТС ССОД необходимо обеспечить соответствие категории охраняемого объекта степени функциональной оснащенности ТС ССОД. Наиболее часто такую задачу решают, используя методы экспертных оценок [91, 92], нечетких множеств [93-95], кластерного анализа [12, 96, 97].

Возможность использования экспертных оценок и обоснование их объективности основаны на том, что неизвестная характеристика исследуемого явления трактуется как случайная величина, отражением закона распределения которой является индивидуальная оценка специалиста-эксперта достоверности и значимости того или иного события. При этом предполагается, что истинное значение исследуемой характеристики находится внутри диапазона экспертных оценок $p \in P$ (где $P = (p_1, p_2, \ldots, p_i, \ldots, p_n)$, − репрезентативная выборка), получаемых от группы экспертов, и что обобщенное коллективное мнение является достоверным.

Необходимо отметить, что экспертные оценки наряду с достоинствами имеют и ограничения, основные из которых представлены в таблице 3.3.

На основе механизма теории нечетких множеств создано несколько методов многокритериального выбора альтернатив: отношения предпочтения, нечеткий вывод, аддитивная свертка, максиминная свертка.

Достоинства и недостатки перечисленных методов приведены в таблице 3.4.

Все методы, основанные на теории нечетких множеств, имеют общие свойства. Однако методы, базирующиеся на разных подходах, дают различные результаты. Их общим недостатком является слабая устойчивость результатов относительно исходных данных.

Таблица 3.3 – Достоинства и недостатки экспертных оценок

Достоинства	Недостатки	Способы повышения истинности результата
1. Синтез опыта и интуиции для получения нового знания	1. Достоверность и надежность результатов исследования зависят от компетентности эксперта	1. Применение специальных как индивидуальных, так и коллективных процедур сбора информации.
2. Возможность получения количественных оценок в случаях, когда отсутствуют статистические сведения или показатель имеет качественную природу	2. Субъективность метода	2. Применение методов обсуждения, предполагающих личное взаимодействие экспертов при рассмотрении проблемы
3. Относительная быстрота получения результатов	3. Трудоемкость процедуры сбора информации и потребность в высококвалифицированных специалистах для проведения опроса	3. Применение методов, сочетающих творческий подход к решению проблемы и статистические методы обработки полученных данных (например, Дельфи)

Наиболее применим для решения поставленной задачи кластерный анализ, под которым понимают совокупность методов классификации многомерных наблюдений или объектов, основанных на определении понятия расстояния между объектами с последующим выделением из них групп наблюдений (кластеров) [96-98].

Таблица 3.4 – Достоинства и недостатки методов нечетких множеств

Достоинства	Недостатки
1. Возможность оперировать нечеткими входными данными: например, непрерывно изменяющиеся во времени значения (динамические задачи), значения, которые невозможно задать однозначно (результаты статистических опросов)	1. Отсутствие стандартной методики конструирования нечетких систем
2. Возможность нечеткой формализации критериев оценки и сравнения: оперирование критериями «большинство», «возможно», преимущественно» и т. д.	2. Невозможность математического анализа нечетких систем существующими методами
3. Возможность проведения качественных оценок как входных данных, так и выходных результатов: оперирование не только значениями данных, но и их степенью достоверности и ее распределением	3. Применение нечеткого подхода по сравнению с вероятностным не приводит к повышению точности вычислений

Основные наиболее распространенные алгоритмы кластерного анализа приведены на рисунке 3.7.

Рисунок 3.7 – Основные методы кластерного анализа

Основные достоинства и недостатки вышеупомянутых методов приведены в таблице 3.5.

Таблица 3.5– Достоинства и недостатки алгоритмов кластерного анализа

Алгоритм кластеризации	Достоинства	Недостатки
k-средних	Простота использования, возможность останавливать работу алгоритма, если на шаге 2 не было объектов, переместившихся из кластера в кластер	Необходимость задавать количество кластеров для разбиения, невозможность применения при пересекающихся кластерах
Иерархический алгоритм	Простота использования, наглядность	Наличие системы полных разбиений, которая может являться излишней в контексте решаемой задачи
c-средних	Нечеткость определения объекта в кластер позволяет определить объекты, которые находятся на границе кластеров	Необходимость задавать количество кластеров для разбиения либо необходимость однозначно отнести каждый объект к одному кластеру
Графовые алгоритмы	Наглядность, относительная простота реализации и возможность внесения различных усовершенствований, основанных на геометрических соображениях. Возможность создания как плоского разбиения данных, так и иерархического.	Ограниченная применимость, плохая управляемость числом кластеров.

Проведя анализ вышеуказанных методов, можно сделать вывод, что для решения конкретной задачи оптимизации наиболее применим метод иерархической кластеризации со способом обработки данных агломеративным алгоритмом. Сущность алгоритма заключается в том, что на первом шаге каждый объект выборки рассматривается как отдельный кластер. Процесс

объединения кластеров произведем последовательно методом одиночной связи (ближнего соседа) на основании матрицы расстояний.

Обычной формой представления исходных данных в задачах кластерного анализа служит матрица вида:

$$X = \begin{pmatrix} x_{11} & x_{12} & x_{13} & x_{14} \\ x_{21} & x_{22} & x_{23} & x_{24} \\ \dots & \dots & \dots & \dots \\ x_{i1} & x_{i2} & x_{i3} & x_{i4} \\ \dots & \dots & \dots & \dots \\ x_{n1} & x_{n2} & x_{n3} & x_{n4} \end{pmatrix}. \qquad (3.35)$$

Каждая строка матрицы представляет результат измерений n, рассматриваемых признаков на одном из обследованных объектов. В задачах кластерного анализа часто используют расстояния Чебышева, Минковского, Евклидово, Хемингово и др. Для решения конкретной задачи в качестве расстояния между объектами примем обычное Евклидово расстояние, определяемое по формуле:

$$\rho_E(x_i, x_j) = \sqrt{\sum_{l=1}^{k} (x_{il} - x_{jl})^2}, \qquad (3.36)$$

где x_{il}, x_{jl} – значения l-го признака у i-го (j-го) объекта (l = 1, 2, ..., k; i, j = 1, 2, ... n).

В таблице 3.6 представлены параметры технических средств ССОД, полученные на основе анализа репрезентативной выборки, исходя из состояния рынка ТСО в Российской Федерации на период исследования, их коэффициенты значимости и удельные стоимости.

Таблица 3.6 – Параметры технических средств ССОД

№ п/п	Дополнительные требования к основной функции назначения ТС ССОД	Параметр ТС ССОД	Коэффициент значимости	Удельная стоимость, тыс. руб.
1	Требование к формированию извещения о несанкционированном доступе	Обнаружение попытки нарушения нормального функционирования путем отрыва от монтажной поверхности, изменения положения в пространстве или иного внешнего воздействия (маскирования)	3	6
2		Обнаружение попытки несанкционированного доступа путем вскрытия корпуса	1	2
3	Требование к формированию извещения о неисправности	Обнаружение неисправности в виде полного отсутствия напряжения электропитания	1	1
4		Обнаружение снижения напряжения электропитания	2	3
5		Обеспечение удаленного контроля функционирования	4	10
6		Обеспечение автоматического контроля параметров окружающей среды, влияющих на параметры обнаружения	3	5
7	Требования к интерфейсу	Наличие не менее трех информационных выходов для формирования не менее четырех видов извещений	3	6
8		Наличие не менее двух информационных выходов для формирования не менее трех видов извещений	2	4
9		Наличие не менее одного информационного выхода для формирования не менее двух видов извещений	1	1

На основании представленных данных сформирована матрица Евклидовых расстояний для проведения кластерного анализа (таблица 3.7).

Таблица 3.7 – Матрица Евклидовых расстояний

№ п/п	1	2	3	4	5	6	7	8	9
x_1	3	1	1	2	4	3	3	2	1
x_2	6	2	1	3	10	5	6	4	1

Определяем расстояния между объектами и представляем полученные данные в матрице расстояний, проанализировав которую наиболее близкие по расстоянию объекты объединим в один кластер. С учетом наименьшего значения объединенных объектов формируем новую матрицу и алгоритм повторяем до формирования необходимого количества кластеров (см. приложение 4). В результате имеем 4 кластера: $S_{(5)}$, $S_{(4, 8)}$, $S_{(2, 3, 9)}$, $S_{(1, 7, 6)}$ (см. таблицу 3.8).

Таблица 3.8 – Матрица расстояний для кластеров $S_{(5)}$, $S_{(4, 8)}$, $S_{(2, 3, 9)}$, $S_{(1, 7, 6)}$

№ п/п	1, 7, 6	2, 3, 9	4, 8	5
1, 7, 6	0	3,606	1,414	4,123
2, 3, 9	3,606	0	1,414	8,544
4, 8	1,414	1,414	0	6,325
5	4,123	8,544	6,325	0

На основе полученных результатов кластеризации ТС ССОД формируем дендрограмму, на которой отражаем взаимные связи между кластерами (рисунок 3.8).

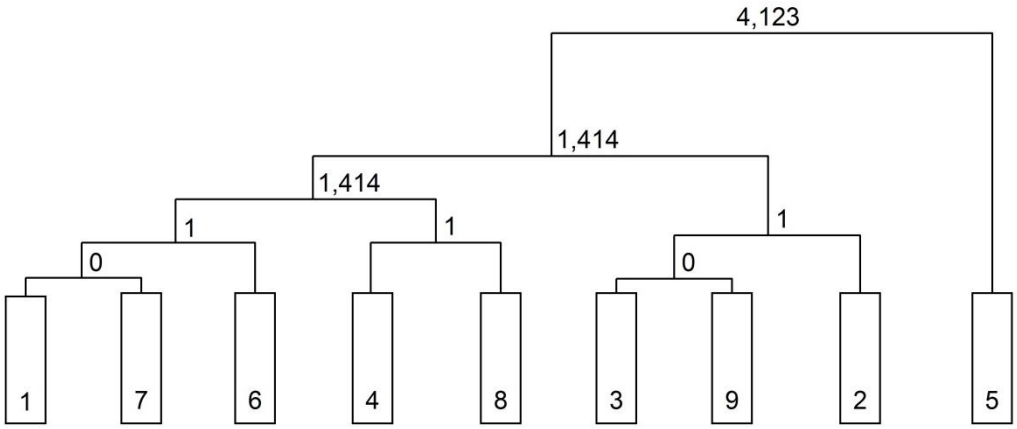


Рисунок 3.8 – Дендрограмма кластеризации ТС ССОД

Для проведения кластерного анализа объектов, принимаемых под централизованную охрану, применим агломеративный алгоритм метода иерархической кластеризации. Обработку данных проведем методом одиночной связи.

На основе репрезентативной выборки определены коэффициенты значимости и прогнозируемые ущербы от возможных проникновений нарушителей (таблица 3.9) на охраняемые объекты.

Таблица 3.9 – Коэффициенты значимости и прогнозируемые ущербы

№ п/п	Группа объектов	Наименование объекта	Коэффициент значимости	Прогнозируемый ущерб, млн. руб.
1	2	3	4	5
1	Особо важные, критически важные и потенциально опасные объекты	Специальные помещения, расположенные на территории (в зданиях, сооружениях) особо важных объектов инфраструктуры Российской Федерации, объектов, подлежащих обязательной охране [1], определенных перечнями, утвержденными Правительством Российской Федерации (помещения с оборотом сведений, составляющих государственную тайну; хранилища взрывчатых и токсичных веществ, денежных и валютных средств; фондохранилища объектов культуры и т. п.).	11	1
2		Государственные и коммерческие объекты, преступные посягательства на которые могут иметь широкий международный и общественный резонанс и (или) привести к особо крупному экономическому ущербу государству или собственнику имущества (обособленные помещения критически важных объектов, особо важных и потенциально опасных объектов инфраструктуры Российской Федерации, помещения для хранения наличных денежных средств предприятий, помещения с хранением документов строгой отчетности или специальной продукции и т. п.).	10	1
3		Критически важные и потенциально опасные объекты, а также объекты, подлежащие обязательной охране, в соответствии с перечнями, утверждаемыми Правительством Российской Федерации, особо важные объекты, объекты жизнеобеспечения, а также объекты с массовым пребыванием граждан, на которых охрана обеспечивается постами физической охраны и выводом тревожной сигнализации на ПЦО подразделений вневедомственной охраны (контрольно-пропускные пункты охраны объекта, служебные помещения и посты охраны и т. п.).	9	0,9

Окончание таблицы 3.9

1	2	3	4	5
4	Государственные и коммерческие объекты	Объекты организаций различных форм собственности с сосредоточением материальных ценностей, преступные посягательства на которые могут привести к крупному или значительному ущербу собственнику имущества (объекты потребительского рынка и т. п.).	7	0,9
5		Государственные и коммерческие объекты, на которых установлена система тревожной сигнализации (служебные помещения охраны и т. п.).	2	0,9
6	Жилые помещения и индивидуальные постройки	Квартиры (антикваров, коллекционеров, деятелей науки, культуры и искусства) со стоимостью имущества, не имеющего денежного эквивалента.	8	1
7		Квартиры со стоимостью имущества, превышающей 1 млн. руб.	6	1
8		Квартиры со стоимостью имущества от 250 тыс. руб. до 1 млн. руб.	4	0,9
9		Места хранения имущества граждан со стоимостью имущества, превышающей 1 млн. руб.	5	1
10		Места хранения имущества граждан со стоимостью имущества от 250 тыс. руб. до 1 млн. руб.	3	0,9
11		Отдельно стоящие места хранения имущества граждан (индивидуальные постройки хозяйственного назначения)	1	0,25

На основании данных таблицы 3.9 сформирована матрица расстояний для проведения кластерного анализа (таблица 3.10).

Таблица 3.10 – Матрица расстояний

№ п/п	1	2	3	4	5	6	7	8	9	10	11
x_1	11	10	9	7	2	8	6	4	5	3	1
x_2	1	1	0,9	0,9	0,9	1	1	0,9	1	0,9	0,25

Определим расстояния между объектами и полученные данные поместим в матрицу расстояний, проанализировав которую наиболее близкие по расстоянию объекты объединим в один кластер. С учетом наименьшего значения объединенных объектов формируем новую матрицу и алгоритм повторяем необходимое количество раз (см. приложение 4). В результате имеем 4 кластера: $S_{(1, 2, 3, 6, 4)}$, $S_{(5, 10, 8)}$, $S_{(7, 9)}$, $S_{(11)}$ (таблица 3.11).

Таблица 3.11 – Итоговая матрица расстояний

№ п/п	1, 2, 3, 6, 4	5, 10, 8	7, 9	11
1, 2, 3, 6, 4	0	3	1,005	6,035
5, 10, 8	3	0	1,005	1,193
7, 9	1,005	1,005	0	4,07
11	6,035	1,193	4,07	0

На основе полученных результатов кластеризации объектов, принимаемых под централизованную охрану, строим дендрограмму, на которой отражаем взаимные связи между кластерами (рисунок 3.9).

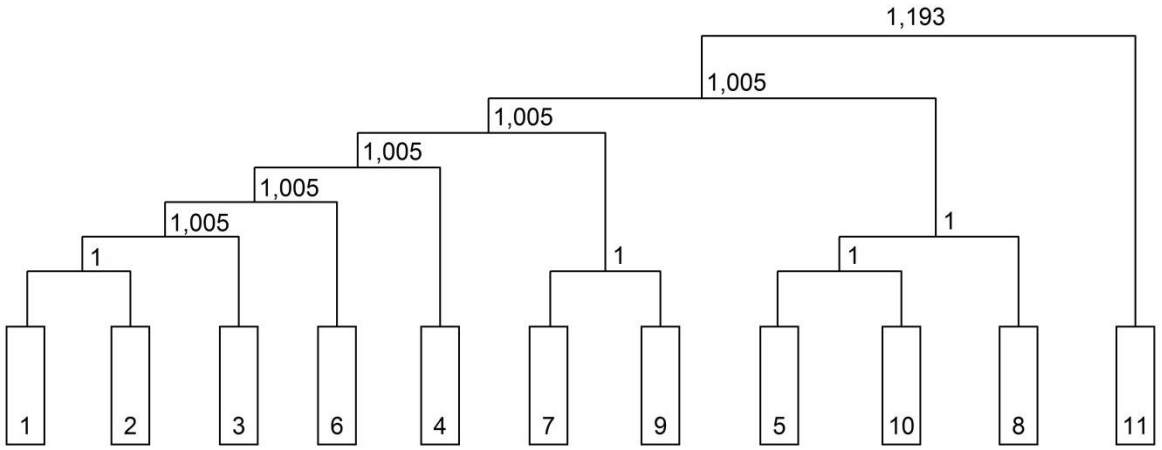


Рисунок 3.9 – Дендрограмма кластеризации объектов

На основе анализа проведенных кластеризаций строим сводную таблицу, отражающую взаимосвязь между объектами, принимаемыми под централизованную охрану, и функциональной оснащенностью ТС ССОД (таблица 3.12).

Таблица 3.12 – Соответствие степени функциональной оснащенности категории охраняемого объекта

Порядковый номер объекта, принимаемого под централизованную охрану	Набор функциональных параметров ТС ССОД
1, 2, 3, 6, 4	1, 2, 3, 4, 5, 6
5, 10, 8	1, 2, 3, 4, 6, 7
7, 9	2, 3, 4, 8
11	2, 3, 9

Выводы по разделу 3

1. В диссертации введен новый параметр – риск несанкционированного проникновения, который представляет собой количественную меру возможности реализации опасности совершения противоправных действий на объекте защиты и их последствий для людей и материальных ценностей.

Рассмотрены вопросы проектирования системы охраны, обеспечивающей гарантированную защиту объекта по критерию соответствия риска несанкционированного проникновения нормативно установленному.

2. Рассмотрены существующие теоретические и экспериментальные методы, позволяющие провести количественную оценку риска несанкционированного проникновения на этапе проектирования системы охраны.

Полученные значения риска несанкционированного проникновения могут быть использованы при проектировании охранно-пожарной сигнализации для обоснования параметров применяемых технических средств обнаружения, а также мер технической укреплённости и физической защиты объекта.

3.Предложено использование нового комплексного показателя – вероятности эффективного обнаружения несанкционированного проникновения нарушителя на охраняемый промышленный объект при проектировании системы охранно-пожарной сигнализации. Показано, что он достоверно характеризует уровень безопасности объекта от угроз криминального и террористического характера.

Получены выражения для составляющих данный параметр членов: вероятности работоспособного состояния на период обнаружения, вероятности достоверного обнаружения проникновения и вероятности обнаружения саботажа.

4. В связи с ограничениями для проектирования, связанными с необходимостью учета затрат на изготовление и техническую эксплуатацию средств

обнаружения, предложено для нахождения оптимального варианта последовательности применяемых средств использовать метод динамического программирования.

Оптимальная последовательность в соответствии с принципом Беллмана должна предусматривать применение способов повышения вероятности эффективного обнаружения в порядке невозрастания удельного приращения стоимости применения *i*-го способа при условии использования предыдущего (i – 1) способа.

Практическая возможность применения метода оптимизации подтверждена на примере модернизации охранного звукового извещателя обнаружения разрушения остекленных конструкций серии «Стекло».

5. Предложено формирование системы сбора и обработки данных на основе использования классифицированных охранных извещателей в соответствии с характеристикой важности и уровня потенциальной опасности объекта.

Для рассматриваемой группы промышленных объектов определены классы средств обнаружения, необходимые для формирования модулей сбора и обработки данных системы охранно-пожарной сигнализации.

4 НАУЧНО-ТЕХНИЧЕСКОЕ И МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ СБОРА И ОБРАБОТКИ ДАННЫХ В АВТОМАТИЗИРОВАННОЙ СИСТЕМЕ ОХРАННО-ПОЖАРНОЙ СИГНАЛИЗАЦИИ ПРОМЫШЛЕННОГО ОБЪЕКТА

4.1 Разработка извещателей охранно-пожарной сигнализации для потенциально опасных промышленных объектов

Ущерб, возникающий в результате преступных посягательств на различные объекты, может иметь как материальный, так и иной характер и может быть причинен как самому объекту, так и находящимся на нем ценностям. Как правило, чем выше категория объекта или стоимость имущества, находящегося на объекте, тем выше вероятность того, что криминальные посягательства будут совершаться более подготовленными и «квалифицированными» нарушителями. Наблюдаемый в последнее время рост технической оснащенности и информированности нарушителей, связанный с развитием и массовым распространением информационных и других технологий, приводит к росту количества успешных попыток преступных посягательств.

Необходимо отметить, что преступные посягательства на объекты высоких категорий значимости, могут привести не только к материальному ущербу, но и к гибели людей или причинению вреда их здоровью, повреждению критически важной инфраструктуры, другим чрезвычайным ситуациям общегосударственного, регионального или муниципального масштаба.

Учитывая это, можно сделать вывод о необходимости дифференцированного подхода к задачам обеспечения противокриминальной и антитеррористической защиты объектов различных категорий значимости, в том числе в части оснащения их ТСО. Очевидно, что чем выше категория значимости охраняемого объекта, тем совершеннее и выше должны быть характеристики

комплекса ТСО (системы охранной сигнализации), применяемого для его защиты [58, 99, 100].

Среди проблем обеспечения противокриминальной и антитеррористической защиты объектов и имущества можно выделить два основных аспекта: технический и экономический.

Технический аспект организации защиты заключается в обеспечении надежности и эффективности ТСО, соответствии их ТТХ и функциональных возможностей определенным видам криминальных воздействий, которые потенциально могут возникать на охраняемом объекте, архитектурным и иным особенностям объекта [7].

Экономический – в обеспечении оптимального баланса между надежностью, эффективностью, информативностью СОС и затратами на оборудование объекта входящими в нее ТСО.

СОС, предназначенная для защиты объектов высоких категорий значимости, должна обеспечивать:

- блокировку всех возможных путей и способов НП нарушителя на охраняемый объект;

- своевременное обнаружение всех вероятных преступных воздействий, совершаемых нарушителями, обладающими высоким уровнем подготовки, осведомленности и технической оснащенности;

- обнаружение преступных (несанкционированных) воздействий на ТСО;

- стабильное функционирование при наличии на охраняемом объекте внешних воздействующих факторов и помех;

- высокую информативность, позволяющую оперативно получать детальную информацию о событиях, происходящих на охраняемом объекте и о текущем состоянии ТСО;

- высокую криптостойкость и имитостойкость, позволяющие безопасно осуществлять обмен информацией между элементами ТСО.

Наиболее полного решения указанных задач СОС можно достичь путем применения ТСО, обладающих высокими ТТХ, обеспечивающими расширенные параметры основной функции назначения, помехоустойчивости, устойчивости к воздействию климатических и механических факторов, а также комплексом дополнительных функций, позволяющих обнаруживать умышленные воздействия и неблагоприятные факторы, нарушающие нормальное (в соответствии с назначением и проектной документацией) функционирование ТСО.

В части средств обнаружения (охранных извещателей), являющихся важнейшей составной частью СОС, решение перечисленных задач достигается применением извещателей классов 3 и 4 по ГОСТ Р 52435-2015 [19] (либо в соответствии с требованиями стандартов на извещатели конкретных типов, содержащих их классификацию, например ГОСТ Р 50777-2014 [65] или ГОСТ 34025-2016 [20]).

Извещатели указанных классов обеспечивают:

- расширенные параметры основной функции назначения и помехоустойчивости;
- обнаружение умышленных попыток нарушения нормального функционирования (несанкционированного доступа) путем вскрытия корпуса, отрыва от монтажной поверхности, изменения положения в пространстве или иного внешнего воздействия;
- обнаружение наиболее вероятных неблагоприятных параметров окружающей среды и техногенных внешних воздействующих факторов, приводящих к нарушению нормального функционирования;
- автоматический контроль работоспособности;
- дистанционный контроль работоспособности (для извещателей класса 4);
- высокую информативность, позволяющую формировать не менее четырех видов извещений (о нормальном состоянии, о тревоге в соответствии с основной функцией назначения, о несанкционированном доступе, о неисправности).

Кроме того, в целях обеспечения высокой вероятности обнаружения нарушителя на объектах высокой категории указанные средства обнаружения (в сочетании с соответствующими средствами инженерно-технической укреплённости) должны быть использованы для организации многорубежной охраны [79]. Количество и виды рубежей охраны на конкретном объекте определяются в соответствии с указаниями, приведенными в соответствующей нормативной документации [22].

Для надежной и эффективной охраны помещений на объектах высоких категорий значимости необходимо блокировать все возможные пути и способы проникновения нарушителя. Так, например, блокировка оконного или дверного проема в охраняемом помещении должна осуществляться извещателями двух типов, один из которых обнаруживает открытие или разрушение дверного полотна (створок оконной конструкции или стекол), а второй – проникновение нарушителя через проем, внутренний объем помещения при этом блокируется третьим извещателем, обнаруживающим перемещение нарушителя в охраняемом помещении. Для решения этих задач необходимо использовать извещатели с различными видами охраняемых зон (точечные, объемные, поверхностные, линейные), основанные на различных физических принципах (магнитоконтактные, звуковые, оптико-электронные, вибрационные и др.).

Специфика обеспечения безопасности многих объектов высоких категорий значимости, в отличие от обычных объектов, зачастую предполагает необходимость организации дополнительных рубежей охраны для блокировки не только внутреннего объема охраняемых отдельных помещений, но и находящихся в них ценностей, а также, при необходимости, и всего здания и прилегающей к нему территории, что приводит к необходимости применения специализированных средств обнаружения, предназначенных для охраны периметра и отдельных предметов.

Организацию рубежа охраны для блокировки отдельных предметов (ценностей) можно осуществлять как извещателями общего назначения,

так и специализированными, предназначенными для решения задачи охраны конкретного вида предметов (ценностей) от конкретных видов воздействий.

Обеспечение эффективной охраны периметров и открытых площадок объектов высоких категорий значимости заключается в проведении тщательного анализа функциональных и иных особенностей объекта, примененных средств инженерно-технической укреплённости, и в выборе на основе проведенного анализа типа извещателей, обеспечивающих оптимальные характеристики обнаружительной способности и помехозащищенности. Рекомендуется при прочих равных условиях использовать активные и многоканальные (комбинированные) извещатели, как более устойчивые к умышленным попыткам несанкционированного доступа и воздействию некоторых помех и внешних факторов. При необходимости должна быть проведена и модернизация средств инженерной укреплённости. Эксплуатация и техническое обслуживание извещателей должны осуществляться с учетом влияния сезонных климатических факторов.

Еще одной важнейшей проблемой повышения эффективности охраны объектов высоких категорий значимости является обеспечение возможности оперативного получения дежурным на пульте централизованной охраны (сотрудниками группы реагирования или техническими специалистами на объекте) детальной информации о событиях, происходящих на охраняемом объекте, текущем состоянии ТСО, входящих в состав СОС, что достигается повышением информативности ТСО.

Информативность СОС определяется количеством информации (извещений, сообщений), предоставляемой персоналу организации, осуществляющей охрану объекта, и зависит от функциональной оснащенности ТСО и типа применяемого способа передачи и обмена информацией (интерфейса) между составными частями СОС. Очевидно, что чем выше функциональная оснащенность ТСО и чем больше информации может передать используемый интерфейс, тем выше будет информативность.

На сегодняшний день существует два типа интерфейса, отвечающих условиям применения на объектах высоких категорий значимости: релейный, в котором информация передается размыканием и замыканием выходных контактов, и адресный, в котором информация передается в виде кодовых комбинаций электрических сигналов.

Необходимо отметить, что в настоящее время наиболее распространенными на российском рынке ТСО являются извещатели, в которых для формирования извещений применяется релейный интерфейс, следовательно, для формирования всех типов извещений (о тревоге, несанкционированном доступе, неисправности) в конструкции извещателя должны быть предусмотрены три информационных выхода (реле). Данный интерфейс не обладает технической сложностью (следовательно, обеспечивает низкую стоимость ТСО), хорошо освоен и прост в эксплуатации, но при этом не обеспечивает двустороннего обмена информацией между извещателем и объектовым средством сбора и обработки информации, а также подробной детализации формируемых извещений. Возможности повышения информативности ТСО, использующих данный интерфейс, практически исчерпаны по причине невозможности дальнейшего увеличения количества информационных выходов и подключаемых шлейфов сигнализации.

Для качественного повышения информативности СОС, предназначенных для защиты объектов высоких категорий значимости, требуется применение адресных ТСО, обеспечивающих:

- предоставление детальной служебной информации о типах ТСО и их текущем состоянии;

- предоставление детальной тревожной информации о виде воздействия, вызвавшего формирование ТСО извещений о тревоге, несанкционированном доступе, неисправности;

- двусторонний обмен информацией, позволяющий оперативно производить диагностику состояния адресных ТСО и осуществлять при необходимости их конфигурирование.

Еще одним достоинством применения адресных ТСО (по сравнению с ТСО, имеющим релейный интерфейс) является повышение криптостойкости и имитостойкости СОС, которая достигается использованием современных защищенных протоколов обмена информацией. Использование адресных ТСО, имеющих уникальную идентификационную информацию, позволяет обнаруживать подмену установленных на охраняемом объекте устройств.

Необходимо отметить, что финансовые затраты на оснащение СОС объекта высокой категории значимости будут значительно выше, чем на оснащение объекта более низкой категории. Экономические вопросы организации охраны такого объекта не должны превалировать над вопросами безопасности, которая обеспечивается высокой надежностью и эффективностью СОС, особенно в части, касающейся обеспечения нормального функционирования особо и критически важных объектов, объектов, связанных с массовым пребыванием людей, а также имеющих огромное культурное и историческое значение.

Снижения затрат на оснащение СОС объекта высокой категории значимости можно добиться путем тщательного анализа всех особенностей и характеристик объекта, осуществлением на его основе определения оптимального состава СОС, обеспечивающего требуемый уровень безопасности, обоснованным выбором ТСО, обладающих высокими технико-экономическими показателями.

Необходимо отметить, что на сегодняшний день в связи с ростом криминальных и террористических проявлений задача обеспечения безопасности объектов высоких категорий значимости приобретает все большую актуальность. Добиться решения этой задачи можно путем применения на таких объектах ТСО, обладающих самыми высокими ТТХ и функциональными возможностями, достаточными для обеспечения требуемого уровня надежности и эффективности СОС.

В целях противодействия современным угрозам необходимо совершенствование существующих ТСО, разработка и применение новых перспектив-

ных путей обнаружения и нейтрализации различных преступных воздействий, широкое внедрение их в охране промышленных объектов, а также структур различной ведомственной принадлежности [101].

В предыдущих разделах доказано, что наиболее актуальна разработка и модернизация технических средств обнаружения (извещателей и модулей) первого рубежа сигнализации, устанавливаемых на пути наиболее вероятного проникновения нарушителей. К одному из видов таких средств относятся магнитоконтактные извещатели (МКИ).

МКИ широко применяются в системах охранно-пожарной сигнализации. На рынке присутствует более 30 их конструктивных типов. Вместе с тем необходима разработка новых ТСО данного вида.

Стоит отметить, что подавляющее большинство имеющихся на российском рынке в настоящее время МКИ удовлетворяют лишь требованиям первого и второго классов. На объектах особой важности или повышенной опасности целесообразно применять ТСО третьего и четвертого класса, обладающие встроенными средствами защиты от несанкционированных воздействий, осуществляемых с целью нарушения их работоспособности и контролем функционирования ТСО.

МКИ третьего и четвертого класса в дополнение к основной функции назначения должны:

- обнаруживать попытку несанкционированного доступа путем вскрытия корпуса на величину, обеспечивающую доступ к органам управления, подключения, регулировки, индикации и монтажным элементам;

- формировать извещение о несанкционированном доступе и/или извещение о тревоге при попытке саботажа их исполнительного блока внешним магнитным полем.

Кроме того, МКИ третьего и четвертого класса (при наличии процессора) должны формировать извещение о неисправности или о тревоге при полном отсутствии и снижении напряжения электропитания.

Четвертый класс дополнительно предусматривает формирование извещений о несанкционированном доступе после превышения допустимого зазора между основанием исполнительного блока и монтажной поверхностью.

Данные нововведения позволят применять ТСО высоких классов с повышенными тактико-техническими характеристиками на особо важных объектах, на которых возможны попытки криминальных посягательств, совершаемых подготовленными нарушителями.

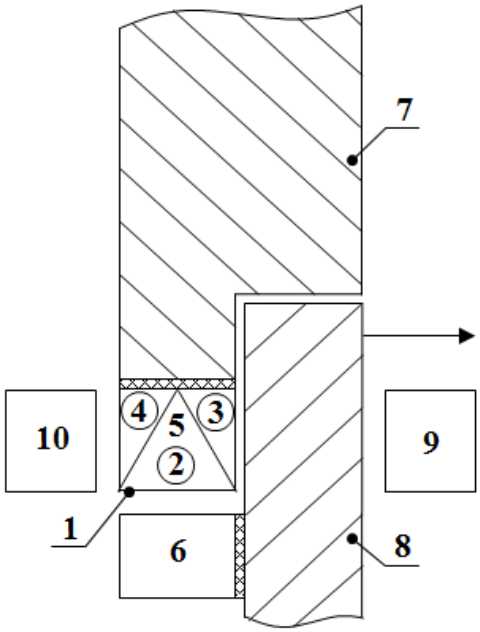
МКИ предназначены для обнаружения открывания дверных (оконных) конструкций и хранилищ ценностей, а также перемещения отдельных предметов с выдачей в шлейф сигнализации приемно-контрольного прибора тревожного извещения путем замыкания или размыкания электрических герметичных контактов.

Общим недостатком таких извещателей является возможность их саботажа внешним магнитным полем, создаваемым сторонним магнитом, при котором происходит потеря работоспособности извещателя, не обнаруживаемая системой сигнализации. Такой способ саботажа известен и уже применялся на охраняемых объектах при совершении крупных краж. Это существенно снижает надежность функционирования охранного МКИ.

Разработанная нами конструкция МКИ предусматривает размещение в корпусе исполнительного элемента первого и второго антисаботажных магнитоуправляемых датчиков и магнитного экрана. Это позволяет обнаружить магнитное поле, создаваемое сторонним магнитом, установленным как с внутренней, так и с внешней стороны охраняемой строительной конструкции, и сформировать в систему сигнализации тревожное извещение [17].

Вариант установки предлагаемого устройства на дверной конструкции показан (в разрезе) на рисунке 4.1. МКИ устанавливается со стороны охраняемого помещения, при этом исполнительный элемент 1 устанавливается на неподвижной части строительной конструкции 7, управляющий элемент 6 устанавливается на подвижной части строительной конструкции 8. Стрелкой показано направление перемещения строительной конструкции 8 при откры-

вании. На рисунке 4.1 условно показано возможное размещение с целью саботажа внешнего стороннего магнита 9 и внутреннего стороннего магнита 10.



1 – исполнительный элемент; 2 – рабочий магнитоуправляемый датчик; 3 – первый антисаботажный магнитоуправляемый датчик; 4 – второй антисаботажный магнитоуправляемый датчик; 5 – магнитный экран; 6 – управляющий элемент; 7 – неподвижная часть строительной конструкции; 8 – подвижная часть строительной конструкции; 9 – внешний сторонний магнит; 10 – внутренний сторонний магнит

Рисунок 4.1 – Вариант установки магнитоконтактного извещателя и варианты обнаруживаемого саботажа

Устройство работает следующим образом.

В рабочем состоянии извещателя при небольшом расстоянии между исполнительным элементом 1 и управляющим элементом 6 магнитное поле, формируемое постоянным магнитом 9 управляющего элемента 6 воздействует на рабочий магнитоуправляемый датчик 2, при этом за счет магнитного экрана 5 воздействие данного поля на первый 3 и второй 4 антисаботажные магнитоуправляемые датчики практически отсутствует. В рабочем состоянии электрические контакты 10 рабочего магнитоуправляемого датчика 2 замкнуты, выходные электрические контакты 11, 12 разомкнуты, что соответствует сигналу «норма», передаваемому в шлейф сигнализации приемно-

контрольного прибора.

При перемещении строительной конструкции 8 и удалении управляющего элемента 6 от исполнительного элемента 1 воздействие поля постоянного магнита 9 на рабочий магнитоуправляемый датчик 2 практически прекращается. При этом электрические контакты 10 рабочего магнитоуправляемого датчика 2 размыкаются, что соответствует формированию в шлейф сигнализации приемно-контрольного прибора тревожного извещения.

При перемещении строительной конструкции 8 и удалении управляющего элемента 6 от исполнительного элемента 1 воздействие поля постоянного магнита 9 на рабочий магнитоуправляемый датчик 2 практически прекращается. При этом электрические контакты 10 рабочего магнитоуправляемого датчика 2 размыкаются, что соответствует формированию в шлейф сигнализации приемно-контрольного прибора тревожного извещения.

При попытке саботажа извещателя внешним магнитным полем стороннего магнита 9 с внешней стороны блокируемой строительной конструкции происходит замыкание электрических контактов 11 первого антисаботажного магнитоуправляемого датчика 3, что приводит к формированию в шлейф сигнализации приемно-контрольного прибора тревожного извещения.

При попытке саботажа извещателя магнитным полем стороннего магнита 10 с внутренней стороны блокируемой строительной конструкции происходит замыкание электрических контактов 12 второго антисаботажного магнитоуправляемого датчика 4, что приводит к формированию в шлейф сигнализации приемно-контрольного прибора тревожного извещения.

В случае подключения антисаботажных датчиков в отдельный шлейф приемно-контрольного прибора, используемого для контроля самих охранных извещателей, саботаж заявляемого магнитоконтактного извещателя сторонним магнитом будет обнаружен сразу же после его реализации. Для реализации указанной тактики работы магнитоконтактного извещателя используются варианты подключения электрических контактов датчиков,

указанные в эксплуатационных документах на соответствующие приемно-контрольные приборы.

Дополнительным преимуществом МКИ является возможность формирования с помощью антисаботажных датчиков раздельных извещений о саботаже.

Таким образом, предлагаемый МКИ не допускает возможность его саботажа магнитным полем стороннего магнита с внешней или внутренней стороны блокируемой строительной конструкции, полностью решая задачу повышения надежности функционирования.

В настоящее время изготовлен макетный образец описанного извещателя и проведены с положительным результатом его испытания. Конструкция устройства МКИ защищена патентом Российской Федерации на полезную модель [18].

На основе обоснованных направлений повышения эффективности, надежности и живучести СОС при непосредственном участии автора разработан и модернизирован ряд ТСО СОС для применения на потенциально опасных и критически важных промышленных объектах. Сводная характеристика данных извещателей приведена в таблице 4.1.

Основными улучшенными характеристиками являются:

- повышенная устойчивость к внешним воздействующим факторам, прежде всего к возможным вариантам саботажа;

- повышенная информативность и надежность передачи извещений, достигаемая применением специально разработанного защищенного протокола передачи информации.

Технические характеристики разработанных в результате исследований извещателей с повышенной эффективностью обнаружения для применения на потенциально опасных промышленных объектах, приведенных в таблице 4.1, представлены в приложении 4.

Таблица 4.1 – Извещатели для применения на потенциально опасных и критически важных промышленных объектах, разработанные при непосредственном участии соискателя

№ п/п	Условное обозначение, год начала серийного выпуска и внешний вид	Физический принцип и зона обнаружения	Основная улучшенная характеристика
1	ИО102-55 «Кенар», 2014 ИО102-55/1 «Кенар-М», 2017 	Магнитоконтактный точечный	Устойчивость к внешним воздействующим факторам
2	ИО102-49, 2018 	Магнитоуправляемый точечный	Повышенная информативность и надежность передачи извещений
3	ИО329-19 «Астра-618», 2017 	Звуковой поверхностный	Повышенная информативность и надежность передачи извещений
4	ИО329-18 «Стекло-5», 2017 	Звуковой поверхностный	Повышенная информативность и надежность передачи извещений
5	ИО329-10 «Стекло-4», 2018 	Звуковой поверхностный	Устойчивость к внешним воздействующим факторам
6	ИО409-30 «Фотон-16», 2017 ИО209-27 «Фотон-16А», 2017 ИО309-14 «Фотон-16Б», 2017 	Оптико-электронный Объемный Оптико-электронный линейный Оптико-электронный поверхностный	Устойчивость к внешним воздействующим факторам

4.2 Оценка уровня автоматизации сбора и обработки данных системы охранно-пожарной сигнализации предприятий нефтегазового комплекса

Уровень автоматизации характеризует долю автоматического труда по управлению технологическим объектом, производимую без участия человека [102, 103]. Данный показатель используется для анализа текущего состояния автоматизации с целью определения планируемых работ, являясь оценкой технико-экономической эффективности автоматизации предприятия. Как правило, количественная оценка уровня автоматизации осуществляется с помощью показателя (коэффициента) K_A, максимальное значение которого составляет 1 [102] или выраженное в процентах – 100 %.

Для нефтегазодобывающей отрасли разработана и опробована методика моделирования и оценки степени автоматизации АСУТП [103]. В соответствии с данной методикой расчет показателя $К_А$ основывался на стандарте компании АСУТП нефтегазодобычи, который учитывался при разработке плановой программы развития ЦДНГ.

Для расчета использовался иерархический принцип определения показателя K_A как по уровням построения системы автоматизации (нулевой уровень – контрольно-измерительные приборы локальной автоматики, первый уровень – программно-логические контроллеры, второй уровень – SCADA, третий уровень – управление производством), так и по уровням технологического/административного деления (технологический элемент, объект, предприятие).

Показатель рассчитывался для соответствующей технологической/административной единицы в структуре. Рассчитанные коэффициенты со своим весом использовались для определения интегрального показателя по каждому уровню построения системы автоматизации. Следует отметить, что указанная методика и рассмотренная модель весовых коэффициентов

может быть использована для оценки состояния и динамики уровня автоматизации в любых иерархических структурах [102], в частности в системе охранно-пожарной сигнализации, входящей в интегрированную АСУ ЦДНГ.

В нашем случае нулевой уровень построения автоматизации соответствует подсистеме сбора и обработки данных, включающей извещатели и модули контроля состоянии защищаемого объекта. Для этого уровня в соответствии с [103] определяется значение расчетного коэффициента полноты автоматизации $К_{ПА}$ с учетом уровня функциональности $К_{Ф}$, характеризующего «интеллектуальность» используемых технических средств обнаружения.

$$К_{А0} = К_{ПА} \cdot К_{Ф} = К_{ПА}(Ч_{ДФ} / Ч_{МДФ}), \quad (4.1)$$

где $Ч_{ДФ}$ – действительное число контролируемых/формируемых сигналов одним извещателем (модулем);

$Ч_{МДФ}$ – максимальное возможное число контролируемых/формируемых сигналов одним извещателем (модулем).

$К_{ПА}$ для этого уровня учитывает наличие «интеллектуальных» извещателей класса 3,4, необходимых для применения в соответствии с разработанными рекомендациями. Значение $К_{ПА}$ в соответствии с [102] приведено в таблице 4.2.

Отношение $Ч_{ДФ}/Ч_{МДФ}$ определяется фактической технической реализацией требований стандарта по функциональной оснащенности в соответствии с рекомендуемыми классами извещателей. Максимальное значение $К_{Ф} = 1$, однако, как и в [103] в нашем случае может быть принято его базовое значение $К_{Ф} = 0{,}75$.

Таблица 4.2 – Значения $К_{ПА}$

Значение коэффициента полноты автоматизации $К_{ПА}$	Относительное количество «интеллектуальных» извещателей
0	<20
0,5	от более 20 до менее 50
0,75	от более 50 до менее 75
1	>75

Следует отметить, что для нулевого уровня весовой коэффициент K_{B0} при определении интегрального коэффициента автоматизации K_A всей системы сигнализации, определенный по методике [102], составляет примерно 0,54. Это подчеркивает оцениваемую экспертами важность технических средств сбора данных для качественного функционирования всей системы автоматизации.

Подставляя значения параметров в формулу (4.1) с учетом весового коэффициента K_{B0} получим значение интегрального коэффициента автоматизации K_A всей системы охранной сигнализации:

$$K_A = K_{B0} \cdot K_{ПА} \cdot K_Ф = 0{,}54 \cdot 0{,}75 \cdot 1{,}0 \cdot 100\% \cong 40\%. \quad (4.2)$$

Для системы охранно-пожарной сигнализации при расчете K_A необходимо учитывать долю охранных извещателей в общем количестве средств сбора данных. Если считать количество охранных и пожарных извещателей примерно равным, получаем значение K_A = 20 %.

С учетом этого, получим увеличение коэффициента автоматизации K_A, достигаемое за счет внедрения разработанных в диссертации способов совершенствования технических средств сбора и обработки данных в системе охранно-пожарной сигнализации (20-40) %.

4.3 Разработка нормативного обеспечения проектирования модульных систем сбора и обработки данных для систем охранно-пожарной сигнализации

На особо важных объектах необходимо применение средств охранной сигнализации, в частности ТСО с высоким уровнем функциональной надежности, позволяющим на ранней стадии обнаруживать различные виды несанкционированных воздействий, совершаемых подготовленными нарушителями. В свою очередь повышение технических характеристик и функциональной надежности ТСО (охранных извещателей и модулей) приводит к увеличению их стоимости. Введение системы классификации ТСО дает возможность применять на объектах конкретной категории значимости ТСО с определенным набором функций, позволяет избежать как недостаточности функциональной надежности, так и ее избыточности, которая негативно влияет на стоимостные показатели ТСО.

В национальных стандартах Российской Федерации классификация ТСО введена в 2014 году в зависимости от наличия в них, помимо основной функции назначения, дополнительных специальных функций, определяющих уровень функциональной надежности и устойчивости к несанкционированному вмешательству и неблагоприятным внешним воздействующим факторам.

В процессе выполнения диссертационной работы возникла необходимость введения классификации в стандарты на конкретные типы ТСО как при пересмотре существующих стандартов, так и при разработке новых.

При непосредственном участии соискателя проведена подготовка нормативно-технических и методических документов (НТД) по разработке и применению классифицированных извещателей в модульных СОС (таблица 4.3).

В таблице 4.3 представлены основные виды НТД, их краткая характеристика и доля участия соискателя в их разработке. Конкретно для различных документов она состояла в следующем.

Внесение изменения в национальный стандарт Российской Федерации (п. 1 таблицы 4.3) обусловлено появлением и распространением новых методов несанкционированных воздействий на охраняемые объекты и потребовало корректировки отдельных положений стандарта в части классификации извещателей, внесения соответствующих изменений и дополнений в технические требования к извещателям, актуализации нормативной базы, корректировки терминов и определений.

Учитывая вышеизложенное, изменением стандарта введены новые виды охранных извещателей, проведена корректировка их классификации.

Таблица 4.3 – Нормативно-технические и методических документы по разработке и применению средств сбора и обработки данных охранно-пожарной сигнализации, разработанные при непосредственном участии соискателя

п/п	Наименование	Краткая характеристика
1	2	3
1	ГОСТ Р 52435-2015 Технические средства охранной сигнализации. Классификация. Общие технические требования и методы испытаний. (Разработка изменений)	Стандарт устанавливает классификацию основных видов ТСО, общие технические требования и методы испытаний ТСО, предназначенных для работы в системах охранно-пожарной, тревожной и охранной сигнализации, интегрированных системах безопасности [104].
2	ГОСТ 34025-2016 Извещатели охранные поверхностные звуковые для блокировки остекленных конструкций помещений. Общие технические требования и методы испытаний. (Разработка документа)	Стандарт устанавливает классификацию, функциональные требования к извещателям, требования, обеспечивающие безопасную эксплуатацию и совместимость извещателей с другими ТСО, а также методы испытаний на соответствие установленным требованиям.

Окончание таблицы 4.3

1	2	3
3	ГОСТ Р 54832-2011 Извещатели охранные точечные магнито-контактные. Общие технические требования и методы испытаний. (Разработка изменений)	Стандарт распространяется на вновь разрабатываемые и модернизируемые извещатели охранные точечные магнитоконтактные, предназначенные для работы в системах тревожной сигнализации, устанавливаемые в помещениях, в т. ч. хранилищах ценностей.
4	Р 78.36.044-2014 Методическое пособие по выбору и применению охранных поверхностных звуковых извещателей для блокировки остекленных конструкций закрытых помещений. (Разработка документа)	В пособии раскрыты вопросы выбора, приобретения, проектирования, монтажа, эксплуатации и обслуживания ТСО тревожной и охранной сигнализации, средств инженерно-технической укреплённости на объектах, охраняемых или передаваемых под охрану подразделениям вневедомственной охраны Росгвардии.
5	Р 069-2017 Рекомендации по выбору и применению средств обнаружения проникновения в зависимости от степени важности и опасности охраняемых объектов. (Разработка документа)	В документе приведены обоснованные рекомендации по выбору конкретных видов, классов и типов ТСО, в зависимости от степени важности, значимости и потенциальной опасности охраняемых объектов. Даны предложения по эффективному применению ТСО, выбору режимов функционирования, регулировке, защите от несанкционированного вмешательства и внешних воздействий.
6	Единые требования к системам передачи извещений, объектовым техническим средствам охраны и охранным сигнально-противоугонным устройствам автотранспортных средств, предназначенным для применения в подразделениях вневедомственной охраны Росгвардии. (Разработка изменений)	В документе определены технические требования к ТСО и сигнально-противоугонным устройствам, предназначенным для применения в пунктах централизованной охраны, на охраняемых или принимаемых под централизованную охрану объектах, местах хранения имущества граждан, а также на автотранспортных средствах.

Кроме того, с учетом развития нормативной базы в области охранной сигнализации обновлены нормативные ссылки, проведена корректировка терминов и соответствующих им определений, актуализирован ряд технических требований и методов испытаний.

В частности, стандарт дополнен терминами с соответствующими определениями, такими как: «извещатель активный», «извещатель магнитоконтактный», «извещатель магнитоуправляемый», «извещатель газовый (охранный)», «извещатель пассивный», «извещатель оптико-электронный инфракрасный», «извещение о несанкционированном доступе», «извещение о тревоге», «основная функция назначения извещателя» и др.

Разработка межгосударственного стандарта (п. 2 таблицы 4.3) была обусловлена отсутствием межгосударственного стандарта, устанавливающего общие технические требования и методы испытаний технических средств охранной сигнализации, относящихся к классу охранных поверхностных звуковых извещателей, предназначенных для блокировки остекленных конструкций в помещениях.

Данным межгосударственным стандартом предусматривается:

- определение области применения стандарта (раздел 1);

- перечень стандартов, других нормативных документов и информационных источников, на которые даются ссылки в стандарте (раздел 2, библиография);

- установление необходимых терминов с соответствующими определениями (раздел 3);

- установление классификации извещателей по функциональной оснащенности и техническим характеристикам (раздел 4);

- формирование общих требований к изготовлению звуковых извещателей и технических требований к ним (раздел 5), а именно: функциональных требований, требований к электропитанию, требований защиты от несанкционированных воздействий и контроля функционирования, требований к интерфейсу, устойчивости извещателей к воздействию внешних факторов, тре-

бований к конструкции, материалам и комплектующим изделиям, требований электромагнитной совместимости, надежности, безопасности, требований к эксплуатационным документам, маркировке и упаковке извещателей;

- установление методов испытаний звуковых извещателей (раздел 6) на соответствие установленным в разделе 5 техническим требованиям, а также формирование требований к помещениям для проведения испытаний, испытательному оборудованию, измерительным приборам и общему порядку проведения испытаний.

Внесение изменения в национальный стандарт Российской Федерации (п. 3 таблицы 4.3) обусловлено необходимостью введения классификации извещателей, повышения и конкретизации требований по устойчивости извещателей к нарушению функционирования при воздействии внешнего магнитного поля, а также введения дополнительных требований по формированию адресных извещений повышенной информативности в извещателях соответствующих классов.

Учитывая вышеизложенное, изменением введена классификация МКИ по степени защищенности от несанкционированных воздействий, а также устанавлены соответствующие технические требования и методы испытаний.

Кроме того, с учетом развития нормативной базы в области охранной сигнализации обновлены нормативные ссылки и актуализирован ряд технических требований и методов испытаний.

В методическом пособии (п. 4 таблицы 4.3) приведены описания конструктивных особенностей, функциональных возможностей и основных тактико-технических характеристик различных типов и модификаций звуковых и совмещенных с ними извещателей, предназначенных для блокировки остекленных конструкций закрытых помещений и хранилищ ценностей на объектах различных видов и категорий, различающихся степенью материальной или социальной значимости, государственной важности или потенциальной опасности, охраняемых подразделениями вневедомственной охраны полиции.

В процессе научных исследований при подготовке пособия проведены:

- анализ физического принципа обнаружения разрушения стеклянных конструкций, применяемый в извещателях;

- классификация извещателей, применяемых для блокировки остекленных конструкций помещений;

- анализ характеристик охранных звуковых и совмещенных извещателей (звуковых с оптико-электронными);

- классификация основных видов и категорий охраняемых объектов, квартир и мест хранения имущества граждан, обуславливающих выбор извещателей;

- анализ характерных помех в работе извещателей и организационно-технических методов защиты от помех;

- разработка рекомендаций по выбору и установке извещателей.

В процессе работы материалы методического пособия приводились в соответствие с современными техническими разработками, внедряемыми в практическую деятельность подразделений вневедомственной охраны, новыми условиями их эксплуатации и техническими характеристиками, а также в соответствии с изменениями в тактике применения извещателей данного типа при охране квартир и других объектов, охраняемых подразделениями вневедомственной охраны.

В рекомендациях (п. 5 таблицы 4.3) рассмотрены особенности применения технических средств обнаружения на объектах различных форм собственности и ведомственной принадлежности. В документе приведены обоснованные рекомендации по выбору конкретных видов, классов и типов средств обнаружения проникновения и тревожной сигнализации, в зависимости от степени важности, материальной, культурной, научной или иной значимости охраняемых объектов либо их потенциальной опасности. Даны рекомендации по эффективному применению средств обнаружения при оборудовании объектов системами охранной сигнализации, по оптимальному выбору места установки, правильному монтажу, подключению, выбору режи-

мов функционирования, регулировке, защите от несанкционированного вмешательства, внешних воздействий и т. п., что является важнейшими составляющими комплекса мероприятий по обеспечению высокой надежности охраны объектов, охраняемых или принимаемых под охрану подразделениями вневедомственной охраны войск национальной гвардии Российской Федерации.

Рекомендации включают в себя восемь основных глав.

В первой главе приведены термины с соответствующими определениями и принятые в рекомендациях сокращения.

Вторая глава посвящена классификации объектов, охраняемых или принимаемых под централизованную охрану подразделениями вневедомственной охраны.

В ней приведено подразделение объектов, охраняемых или подлежащих передаче под централизованную охрану подразделениями вневедомственной охраны на классы зависимости от значимости, концентрации материальных, художественных, исторических и культурных ценностей, размещенных на объекте, последствий от возможных криминальных посягательств на них.

В третьей рассматривается классификация средств обнаружения проникновения на охраняемые объекты и средства тревожной сигнализации, включающая как общие принципы классификации средств обнаружения и тревожной сигнализации, так и особенности классификации средств обнаружения по функциональной оснащенности и защищенности от несанкционированных воздействий. Приведены общие принципы классификации средств обнаружения и тревожной сигнализации и особенности классификации средств обнаружения по функциональной оснащенности и защищенности от несанкционированных воздействий.

В четвертой главе уделено внимание функциональным особенностям и тактико-техническим характеристикам средств обнаружения и тревожной сигнализации различных классов.

В данной главе подробно рассмотрены основные типы извещателей, особенности их конструкции, физические принципы работы и области применения, а также тактика и особенности применения, даны рекомендации по выбору места установки, монтажу и регулировке, отражены стоимостные особенности извещателей.

В пятой рассматриваются особенности выбора и применения средств обнаружения в зависимости от видов и классов охраняемых объектов. Представлены возможные пути и способы проникновения нарушителя на охраняемый объект и рекомендации по применению средств обнаружения проникновения в зависимости от класса охраняемого объекта

В шестой – функциональные особенности, технические характеристики и требования к монтажу средств обнаружения, предназначенных для применения на взрывоопасных объектах. Рассмотрены виды взрывозащиты в области охранной и пожарной сигнализации – способы обеспечения взрывобезопасности электротехнического оборудования, особенности их организации и присущие недостатки, приведен ряд конкретных типов извещателей во взрывозащищенном исполнении.

В седьмой представлен анализ основных путей и способов несанкционированного проникновения на охраняемые объекты. В частности, способы несанкционированного проникновения через охраняемое ограждение периметра объекта, способы несанкционированного проникновения в охраняемое здание (помещение) и особенности несанкционированных действий по отношению к отдельно охраняемым предметам (ценностей).

В заключительной главе приведены основные виды несанкционированных воздействий на технические средства охранной сигнализации и способы защиты.

Единые требования (п. 6 таблицы 4.3) переработаны во исполнение решения расширенного заседания Технического совета Главного управления вневедомственной охраны Росгвардии.

Переработка включила введение требований к средствам активной защиты и охранным сигнально-противоугонным устройствам автотранспортных средств, а также корректировку общих требований, требований к системам передачи извещений и объектовым техническим средствам охраны, в частности, к средствам обнаружения проникновения таким, как оптико-электронные инфракрасные пассивные извещатели для охраны помещений и открытых площадок, звуковые извещатели для блокировки остекленных конструкций помещений, магнитоконтактные (магнитоуправляемые) извещатели и др.

На основе данных, приведенных в таблице 4.3, построена диаграмма, отражающая работу по подготовке НТД (рисунок 4.2).

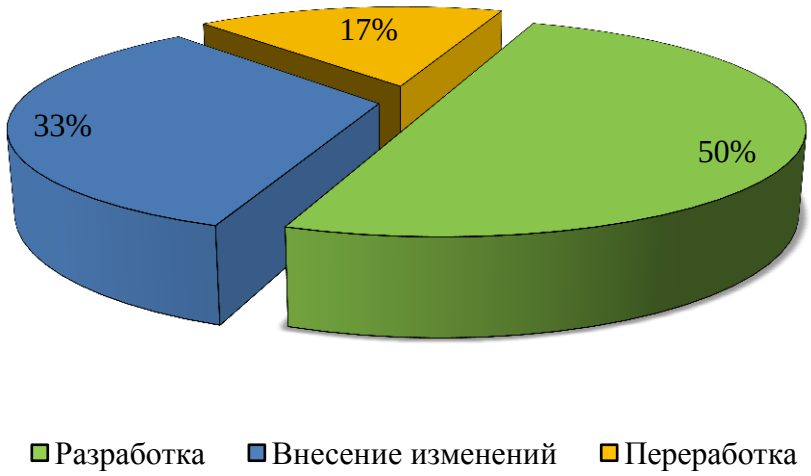


Рисунок 4.2 – Формирование новой системы классификации ТСО

Проанализировав процесс формирования новой системы классификации ТСО, следует отметить, что в настоящее время они составляют основу НТД для проектирования и применения ТСО в системе охранно-пожарной сигнализации потенциально опасных и критически важных объектов.

Однако в целом работа работ по актуализации стандартов с учетом их востребованности должна быть продолжена.

4.4 Разработка предложений по формированию системы охраны цеха добычи нефти и газа

В процессе исследований и проектной деятельности автором разработаны предложения по формированию системы охраны периметра цехов добычи нефти и газа, подверженных террористической опасности. В основе функционирования системы находится сбор и обработка данных НП и криминальных действиях нарушителя.

ЦДНГ как объект защиты представляет собой территорию со сложной конфигурацией, на которой располагаются административные здания, здание диспетчерской, резервуары для приема нефтепродуктов, технологические установки и оборудование для разделения от примесей нефтепродуктов и их транспортировки. Для обеспечения пропускного режима на территорию охраняемого объекта имеются: въездные ворота для проезда автотранспорта и прохода сотрудников с оборудованным КПП. Как правило, периметр территории защищен ограждением из колючей проволоки и каменным забором со стороны КПП.

Однако это не обеспечивает в полной мере решения задачи защиты оборудования, материальных ценностей, сотрудников ЦДНГ и сотрудников охраны, находящихся на защищаемой территории.

С этой целью на объекте должна быть сформирована техническая система охраны периметра. В соответствии с современной концепцией обеспечения защиты она должна включать в себя следующие основные элементы:

- систему технической укреплённости объекта;
- систему охранно-пожарной сигнализации;
- систему тревожно-вызывной сигнализации.

На основании современного состояния развития техники с учетом применяемой тактики охраны могут быть сформированы следующие предложения по реализации перечисленных систем.

Система технической укреплённости объекта.

Для защиты от проникновения преступных элементов и посторонних лиц необходимо обнести территорию ограждениями. Наиболее дешевыми и простыми являются ограждения из колючей проволоки, которые не требуют для своего устройства дефицитных строительных материалов и привлечения значительных сил и средств. При сооружении таких ограждений следует придерживаться следующих правил:

- Ограждения должны быть выполнены в виде прямоугольных участков, с минимальным количеством изгибов, ограничивающих наблюдение и затрудняющих применение технических средств охраны.

- Высота ограждения должна быть не менее 2 м. Колючая проволока прокладывается в два «слоя» – по внешней и внутренней части деревянных, металлических или бетонных столбов. Расстояние между рядами проволоки не должно превышать 10 см. Кроме этого, в каждой секции ограждения прокладывают диагональные ряды колючей проволоки, которые в местах пересечения с основными рядами крепятся к последним с помощью стальной проволоки.

- Для усиления ограждение рекомендуется оборудовать козырьками из 3-4-х рядов колючей проволоки или средств защиты, выполненных в виде «спирали-путанки», которые крепятся на кронштейнах под наклоном к столбам ограждения.

Периметр караульного помещения следует оборудовать двойным ограждением с расстоянием между рядами, достаточным для установки средств периметральной сигнализации и охранного освещения либо прокладки других коммуникаций. Между рядами в один или несколько слоев по земле укладывают «спирали-путанки».

Для нормального функционирования службы в ограждениях, там, где это необходимо, устраивают ворота или калитки, которые должны запираться на засовы и замки. Ворота и калитки, находящиеся за пределами зоны постоянного наблюдения, следует дополнительно запирать на запорно-

пломбировочные устройства, которые позволяют зафиксировать факт проникновения или попытки проникновения на территорию объекта. С внешней стороны ворот желательно устанавливать преграды типа «лежачий полицейский» либо противотаранные устройства.

На ограждении вывешивают запрещающие таблички «Не подходить! Запретная зона» или аналогичного содержания. Текст табличек должен быть выполнен водостойкой краской на 2-х языках – русском и национальном и должен читаться с расстояния 15-20 м.

Для осуществления визуального контроля за прилегающей к охраняемому объекту территорией необходимо установить смотровые вышки. Количество вышек определяется формой периметра ЦДНГ.

Примерное конструктивное исполнение вышки наблюдения представлено на рисунке 4.3.

Вышки должны:

1) быть утеплены;

2) иметь вращающийся прожектор для обеспечения освещения прилегающей к охраняемому объекту территории;

3) обеспечивать защищенность от обстрела стрелковым оружием;

4) быть подняты над поверхностью земли не менее чем на 3 м.

Система охранно-пожарной сигнализации.

Для построения системы охранной сигнализации периметра могут быть применены ППК.

Информация о состоянии охраняемых шлейфов (зон) выводится на переднюю панель ППК.

В каждый шлейф ППК включают извещатели, защищающие один участок периметра. Управление взятием на охрану и снятием с охраны осуществляется с ППК, установленного на посту дежурного в караульном помещении.

Могут быть рекомендованы следующие технические средства обнаружения для защиты территории:

- для въездных ворот на открывание и проход (проезд) через них – оптико-электронные извещатели;

- ограждение на проникновение – извещатели радиоволновые.

Извещателями пожарной сигнализации оборудуются караульное помещение и КПП.

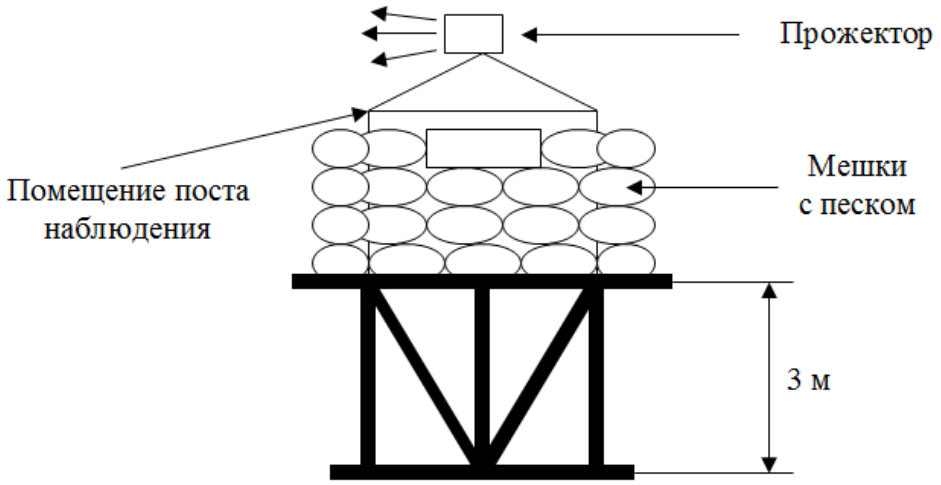


Рисунок 4.3 – Примерное конструктивное исполнение вышки наблюдения

Система тревожно-вызывной сигнализации.

Для построения системы тревожной сигнализации могут быть применены радиосистемы тревожной сигнализации «Радиокнопка», которой оборудуются посты охраны.

Сигнал тревоги на центральный пост охраны передается по радиоканалу. Информация о состоянии охраняемых шлейфов (зон) выводится на панели визуального контроля. Малогабаритное передающее устройство, оборудованное датчиком падения, устанавливается на стене или находится у постового.

Таким образом, представленная техническая система периметровой сигнализации обеспечивает выполнение следующих функций:

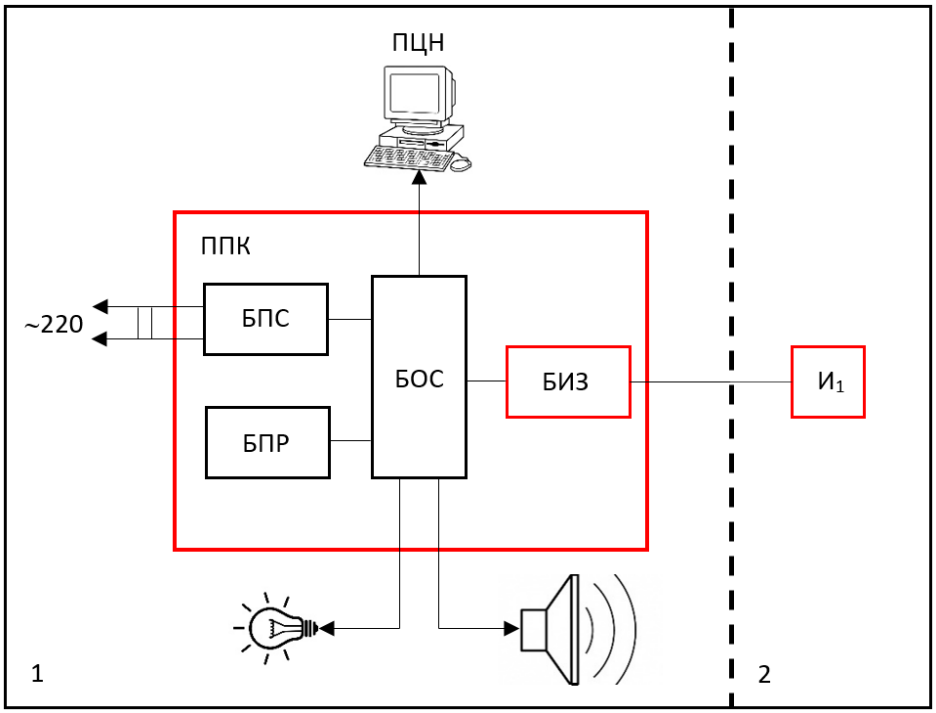
- выявление (автоматически и персоналом) тревожных ситуаций, формирование сигналов тревог, выдачу информации о наличии и месте возникновения тревожной ситуации на пост охраны объекта;

- автоматический и полуавтоматический (по сигналам оператора) контроль состояния элементов системы и ее составных частей.

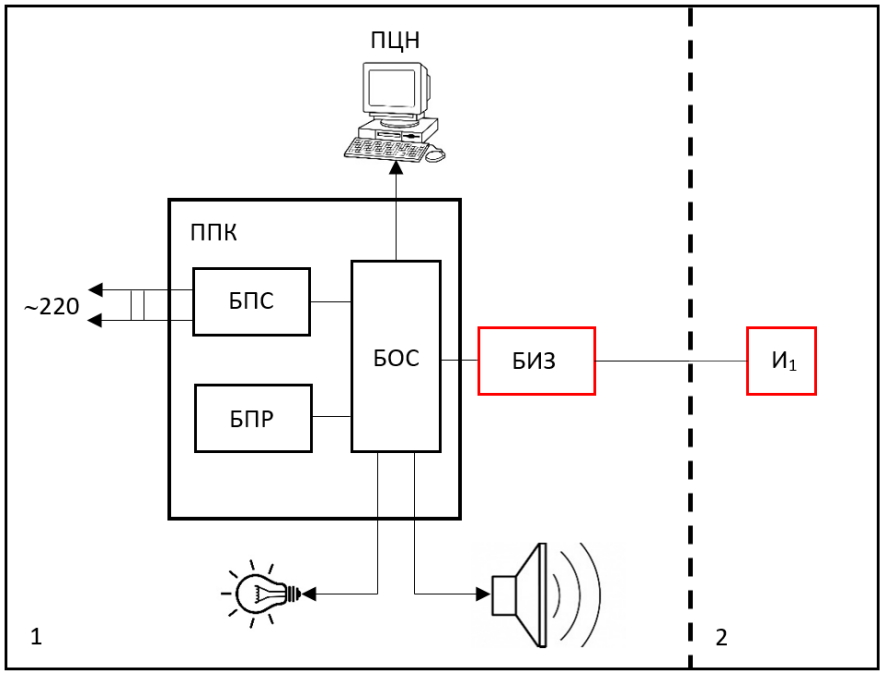
Учитывая потенциальную пожаро-взрывоопасность предприятия ЦДНГ при организации сбора и обработки данных, должно быть обеспечено специальное конструктивное исполнение технических средств.

В области охранно-пожарной сигнализации применяют в основном два вида взрывозащиты: искробезопасная электрическая цепь и взрывонепроницаемая оболочка [105].

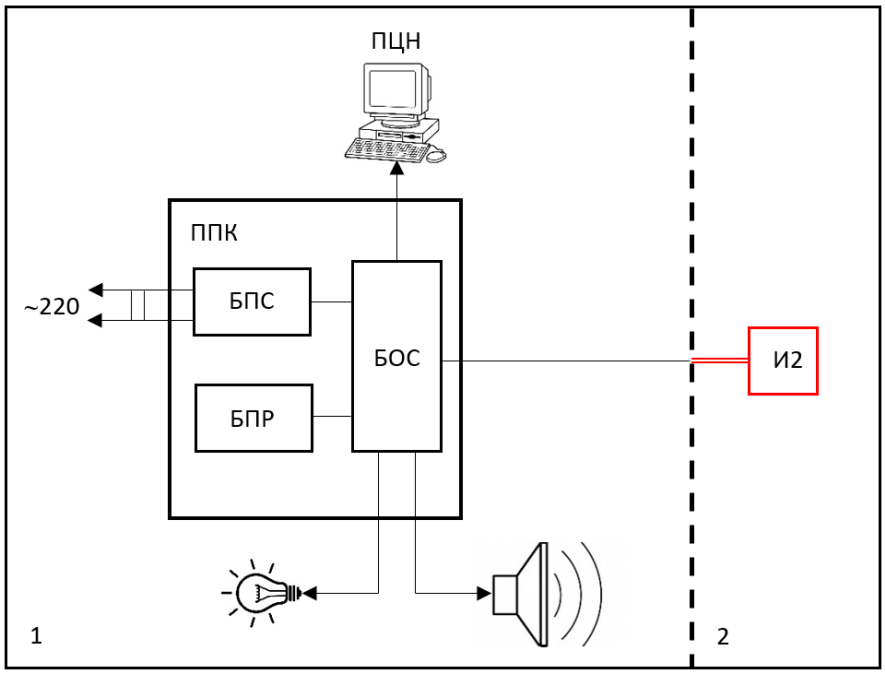
Организация защиты вида «искробезопасная электрическая цепь» построена на принципе исключения возможности вызвать воспламенение взрывоопасной смеси при возникновения искры или нагреве цепи за счет ограничения выделяемой энергии. В случае обрыва или короткого замыкания электрической цепи, связывающей извещатель и ППК, искрообразование практически исключается. С этой целью устанавливают специальные блоки взрывозащиты, снижающие мощность электрических цепей, которые могут входить в состав ППК или быть выполнены в виде обособленного модуля, установленного между ППК и искробезопасными цепями (рисунок 4.4 а, б).



а) Схема подключения извещателей к ППК с встроенным БИЗ



б) Схема подключения извещателей к ППК через обособленный БИЗ



в) Схема подключения извещателей к ППК через бронекабель:

1 – взрывобезопасная зона; 2 – взрывоопасная зона; ПЦН – пульт централизованного наблюдения; ППК – прибор приемно-контрольный; БПС – блок питания сетевой; БОС – блок обработки сигналов; БПР – блок питания резервный; БИЗ – блок искрозащиты; И1 – извещатель с искробезопасной электрической цепью; И2 – извещатель во взрывонепроницаемой оболочке.

Рисунок 4.4 – Схемы формирования системы тревожной сигнализации на взрывоопасном промышленном объекте

Второй вид «взрывонепроницаемая» оболочка» характеризуется отсутствием возможности распространения взрыва вне извещателя.

Таким образом, конструкция допускает возможность возникновения взрыва внутри оболочки, но гарантирует невозможность его распространения в окружающую среду. Корпуса таких извещателей имеют повышенную прочность, но отличаются относительно большими габаритами и массой.

Линии сигнализации и питания для практической реализации данного вида взрывозащиты необходимо прокладывать в бронекабеле или в стальных трубах (рисунок 4.4 в).

Достоинством такого метода является отсутствие ограничения потребляемой мощности электропитания, недостатком – высокая стоимость оборудования и монтажа, а также повышенные требования к обслуживанию системы.

Рассмотрим конкретные варианты взрывозащищенного исполнения извещателя, а именно блок искрозащиты (рисунок 4.5), а также взрывонепроницаемую оболочку (рисунок 4.6).

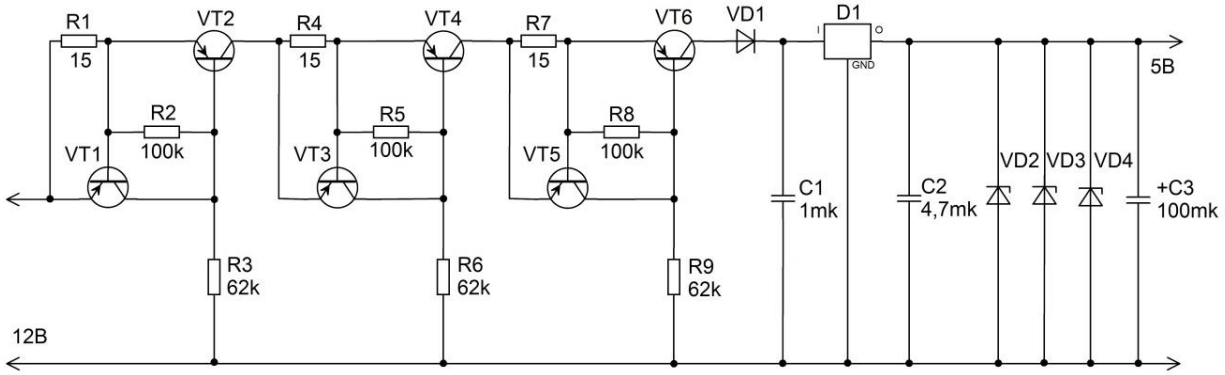
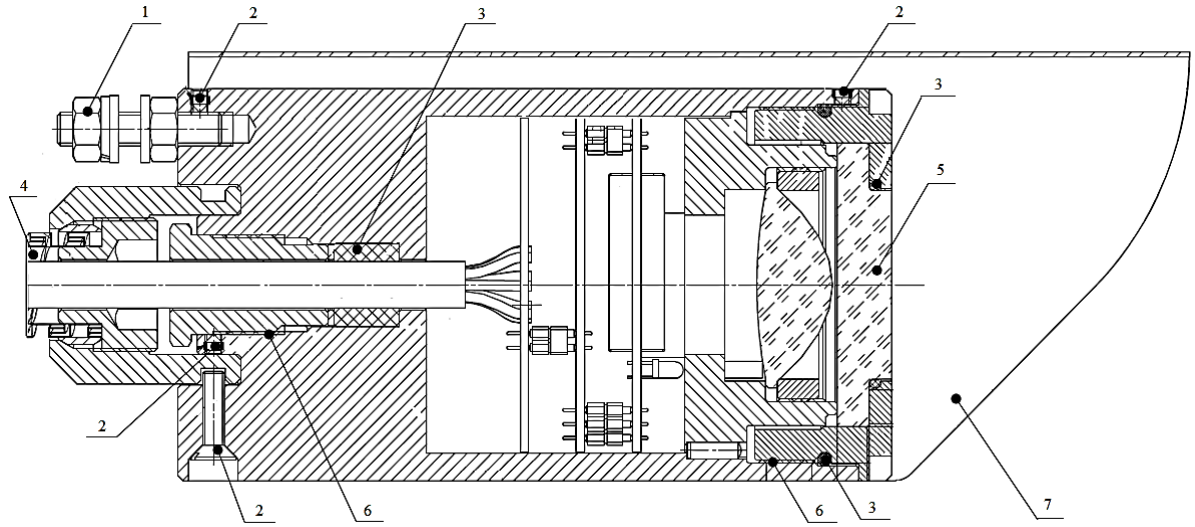


Рисунок 4.5 – Схема электрическая принципиальная блока искрозащиты

Для реализации представленной схемы использован диодный барьер безопасности – сборка элементов, состоящая из шунтирующих диодов (цепи диодов, в том числе стабилитронов), защищенных предохранителями или резисторами (их сочетанием), осуществлена герметизация элементов заливочным компаундом, а также обеспечено необходимое значение электрических

зазоров между неизолированными токопроводящими частями внешних соединительных средств раздельных искробезопасных цепей.



1 – шпилька заземления; 2 – винт контровочный; 3 – кольцо уплотнительное; 4 – металлорукав (бронекабель); 5 – стекло защитное (полиметилметакрилат); 6 – взрывонепроницаемое соединение; 7 – козырек защитный

Рисунок 4.6 – Схема конструкции корпуса блока извещателя охранного активного линейного оптико-электронного

Для создания взрывонепроницаемой оболочки в конструкции корпуса блока извещателя применены следующие основные меры:

- выдержаны минимальные длины соединений и максимальные зазоры между поверхностями соединений оболочки в соответствии с видом взрывонепроницаемого элемента и ее объемом;

- обеспечена регламентированная шероховатость поверхности и параметры зубчатых соединений (шаг, вид, класс, осевая длина резьбы, число ее полных непрерывных ниток);

- для защиты от доступа влаги и пыли применены прокладки из пластичного материала, выполнено заземление, использованы бронекабель и защитное стекло.

Таким образом, развитие технологий и требований по обеспечению безопасности промышленных предприятий привело к расширению номен-

клатуры и повышению качественных характеристик оборудования тревожной сигнализации во взрывозащищенном исполнении.

Оборудование современными системами обнаружения пожара и проникновения нарушителя позволяют снизить количество чрезвычайных ситуаций на взрывоопасных объектах на них и в итоге спасти человеческие жизни.

Рассмотренные предложения могут быть использованы для формирования системы охраны периметра ЦДНГ, подверженных потенциальной террористической опасности.

Выводы по разделу 4

1. На основе обоснованных задач совершенствования технических средств обнаружения системы охранной сигнализации разработан и модернизирован ряд извещателей, внедренных в серийное производство для применения на потенциально опасных и критически важных промышленных предприятиях.

2. Разработаны научно-обоснованные предложения по оптимальному проектированию модулей сбора и обработки данных и их эффективному применению в составе системы охранной сигнализации промышленного объекта. Данные предложения включены в состав нормативно-технических и методических документов, официально утвержденных для использования в практической деятельности вневедомственной охраны Росгвардии.

3. Таким образом, в результате комплекса теоретических и научно-технических работ, выполненных в рамках диссертации, обеспечено достижение поставленной цели – совершенствование автоматизации сбора и обработки данных в системе охранной сигнализации на основе классифицированных извещателей с повышенной эффективностью обнаружения несанкционированного проникновения нарушителя на охраняемый промышленный объект.

4. Практическая реализация данной цели на основе научно обоснованных технических разработок позволяет решить важную для экономики задачу – повышение безопасности промышленных объектов нефтегазовой отрасли Российской Федерации.

ЗАКЛЮЧЕНИЕ

Основные научные результаты, выводы и предложения, полученные в диссертационной работе, сводятся к следующему:

1. Проведен анализ современного состояния безопасности и основных задач совершенствования системы охраны и пожарной безопасности потенциально опасного промышленного объекта на примере цеха добычи нефти и газа.

Сформирован комплексный показатель безопасности промышленного объекта от угроз криминального проникновения нарушителя, пожара и техногенной аварии. Особенностью данного показателя является учет комплексного характера возникающих угроз и их проявлений, а также степень взаимодействия систем безопасности и управления технологическим процессом.

Использование полученной математической модели позволяет планировать и проводить оценку влияния проводимых мероприятий на уровень безопасности объекта.

2. В результате проведенного статистического и экспериментального исследований параметров эффективности обнаружения, надежности и живучести автоматизированной системы централизованной охранно-пожарной сигнализации на этапе эксплуатации определены задачи совершенствования сбора и обработки данных, учитывающие необходимость дифференцированного подхода для обеспечения противокриминальной и антитеррористической защиты объектов различных категорий значимости.

3. Разработана математическая модель, определяющая риск несанкционированного проникновения на охраняемый промышленный объект.

Разработана методика проектирования системы сигнализации по критерию соответствия риска несанкционированного проникновения нормативно установленному.

Получено математическое выражение для количественной оценки вероятности эффективного обнаружения несанкционированного проникновения, обеспечивающее практическую реализацию разработанной методики.

4. С целью достижения максимальной вероятности эффективного обнаружения разработана методика оптимального проектирования модулей сбора и обработки данных на основе метода динамического программирования, обеспечивающая минимизацию затрат на расширение функциональных возможностей разрабатываемых технических средств.

5. Разработаны научно-обоснованные предложения по выбору модулей обнаружения при формировании системы охранно-пожарной сигнализации, которые являются основой для практических рекомендаций по оборудованию промышленных объектов нефтегазового комплекса классифицированными извещателями.

6. Разработан и модернизирован ряд извещателей, внедренных в серийное производство для применения на потенциально опасных и критически важных промышленных предприятиях.

7. Разработаны нормативно-технические и методические документы по производству классифицированных извещателей, составляющие основу для их применения в модульных системах охранно-пожарной сигнализации на потенциально опасных и критически важных объектах.

Таким образом, в результате комплекса теоретических и научно-технических работ, выполненных в рамках диссертации, обеспечено достижение поставленной цели – совершенствование автоматизации сбора и обработки данных в системе охранно-пожарной сигнализации потенциально опасного промышленного объекта на основе классифицированных извещателей с повышенной эффективностью обнаружения.

Практическая реализация данной цели вносит значительный вклад в повышение безопасности предприятий нефтяной и газовой промышленности.

СПИСОК СОКРАЩЕНИЙ

АРМ – автоматизированное рабочее место

АСУ – автоматизированная система управления

АСУТП – автоматизированная система управления технологическим процессом

ВАК – Высшая аттестационная комиссия при Министерстве образования и науки Российской Федерации

ВО – вневедомственная охрана

ГОСТ – межгосударственный стандарт

ГОСТ Р – национальный стандарт Российской Федерации

ГЗУ – групповые замерные установки

ГСС – газосборная сеть

ДНС – дожимные насосные станций

ИСБ – интегрированная система безопасности

КНС – кустовая насосная станция

КПП – контрольно-пропускной пункт

ЛСТ – ложный сигнал тревоги

МКИ – магнитоконтактный извещатель

НГК – нефтяная и газовая отрасли

НИЦ – научно-исследовательский центр

НП – несанкционированное проникновение

НТД – нормативно-технический докумен

ОАО – открытое акционерное общество

ПО – программное обеспечение

ППК – прибор приемно-контрольный

ПЦО – пульт централизованной охраны

ССОД – система сбора и обработки данных

СОС – система охранной сигнализации

СОТ – система охранная телевизионная

СКУД – система контроля и управления доступом

СПИ – система передачи извещений

СПС – система пожарной сигнализации

ТС – техническое средство

ТСО – техническое средство охраны

ТТХ – тактико-технические характеристики

УКПН – установки комплексной подготовки нефти

УПВ – узел подготовки воды

УПСВ – установка предварительного сброса воды

ЦДНГ – цех по добыче и комплексной подготовке нефти

СПИСОК ЛИТЕРАТУРЫ

1. Распоряжение Правительства Российской Федерации от 15 мая 2017 года № 928-р «Об утверждении перечня объектов, подлежащих обязательной охране войсками национальной гвардии Российской Федерации» (с изменениями на 10 сентября 2019 года).

2. Приказ Федеральной службы войск национальной гвардии Российской Федерации от 7 марта 2018 г. № 72 «Об утверждении концепции развития вневедомственной охраны войск национальной гвардии Российской Федерации на период 2018-2021 годов и далее до 2025 года».

3. Рябцев, Н.А. Раннее обнаружение нарушителя системой охранной сигнализации / А.Н. Членов, Н.А. Рябцев // Материалы двадцать четвертой международной научно-технической конференции «Системы безопасности – 2015». – М.: Академия ГПС МЧС России, 2015. – С. 276-278.

4. Рябцев, Н.А. Основные тенденции развития охранных извещателей для защиты объектов особой важности / А.Р. Фамильнов, Н.А. Рябцев, А.Н. Федин, О.Г. Точилова, В.А. Козлов // Материалы двадцать пятой международной научно-технической конференции «Системы безопасности – 2016». – М.: Академия ГПС МЧС России, 2016. – С. 368-371.

5. Рябцев, Н.А. Комплексный показатель технической эффективности системы тревожной сигнализации / Т.А. Буцынская, В.А. Николаев, Н.А. Рябцев // Материалы двадцать пятой международной научно-технической конференции «Системы безопасности – 2016». – М.: Академия ГПС МЧС России, 2016. – С. 386-387.

6. Рябцев, Н.А. Условие повышения надежности системы тревожной сигнализации объекта особой важности / В.А. Николаев, Н.А. Рябцев // Материалы двадцать пятой международной научно-технической конференции «Системы безопасности – 2016». – М.: Академия ГПС МЧС России, 2016. – С. 390-391.

7. Рябцев, Н.А. Оптимизация формирования системы безопасности критически важного объекта / Н.А. Рябцев // Материалы двадцать шестой международной научно-технической конференции «Системы безопасности – 2017». – М.: Академия ГПС МЧС России, 2017. – С. 342-345.

8. Рябцев, Н.А. Пути повышения функциональной надежности технических средств тревожной сигнализации для объектов высокой категории значимости / А.Н. Членов, А.В. Климов, Н.А. Рябцев // Материалы двадцать шестой международной научно-технической конференции «Системы безопасности – 2017». – М.: Академия ГПС МЧС России, 2017. – С. 311-314.

9. Рябцев, Н.А. Анализ причин неустойчивой работы систем охранно-пожарной сигнализации / Т.А. Буцынская, Н.А. Рябцев // Материалы двадцать седьмой международной научно-технической конференции «Системы безопасности – 2018». – М.: Академия ГПС МЧС России, 2018. – С. 212-215.

10. Рябцев, Н.А. Особенности формирования систем тревожной сигнализации потенциально опасных объектов / Н.А. Рябцев // Материалы двадцать седьмой международной научно-технической конференции «Системы безопасности – 2018». – М.: Академия ГПС МЧС России, 2018. – С. 216-219.

11. Рябцев, Н.А. Оценка эффективности обнаружения тревожной ситуации на охраняемом объекте / Н.А. Рябцев, Т.А. Буцынская // Материалы двадцать восьмой международной научно-технической конференции «Системы безопасности – 2019». – М.: Академия ГПС МЧС России, 2019. - С. 262-264.

12. Рябцев, Н.А. Оптимизация состава технических средств охранной сигнализации на основе кластерного анализа / Н.А. Рябцев // Материалы двадцать восьмой международной научно-технической конференции «Системы безопасности – 2019». – М.: Академия ГПС МЧС России. – 2019. – С. 265-269.

13. Рябцев, Н.А. Основные направления развития и новейшие разработки средств обнаружения проникновения для противокриминальной защи-

ты объектов и имущества / Н.А. Рябцев // В кн.: Сборник материалов деловой программы XX международной выставки средств обеспечения безопасности государства «Интерполитех-2016»: материалы научно-практической конференции «Технические средства охраны для обеспечения комплексной безопасности объектов и территорий государства: проблемы и перспективы развития». – М., 2016. – С. 334-336.

14. Рябцев, Н.А. Тенденции повышения функциональной надежности средств обнаружения проникновения, предназначенных для блокировки инженерных средств физической защиты критически важных объектов / Н.А. Рябцев // В кн.: Сборник материалов деловой программы XXI международной выставки средств обеспечения безопасности государства «Интерполитех-2017»: материалы научно-практической конференции «Технические средства охраны для обеспечения комплексной безопасности объектов и территорий государства: проблемы и перспективы развития». – М., 2017. – С. 147-148.

15. Рябцев, Н.А. Основные факторы, определяющие направления развития средств обнаружения несанкционированного проникновения на объекты высоких категорий значимости / А.Г. Зайцев, А.В. Климов, Н.А. Рябцев // Современные охранные технологии и средства обеспечения комплексной безопасности объектов: Материалы одиннадцатой Всероссийской научно-технической конференции. – Пенза: Изд-во «Март», 2016. – С. 55-59.

16. Рябцев, Н.А. Способы проникновения нарушителей на промышленные объекты / Н.А. Рябцев // Материалы VIII-й международной научно-практической конференции молодых ученых и специалистов «Проблемы техносферной безопасности – 2019». – М.: Академия ГПС МЧС России., 2019. – С. 137-140.

17. Рябцев, Н.А. Магнитоконтактный извещатель / Н.А. Рябцев, Т.А. Буцынская // Материалы VIII-й международной научно-практической

конференции молодых ученых и специалистов «Проблемы техносферной безопасности – 2019». – М.: Академия ГПС МЧС России, 2019. – С. 175-179.

18. Рябцев, Н.А. Охранный магнитоконтактный извещатель: МПК G08B 13/08. Патент на полезную модель № 189504 Рос. Федерация; заявл. 26.11.2018; опубл. 24.05.2019 / А.Н. Членов, Н.А. Рябцев, Т.А. Буцынская.

19. ГОСТ Р 52435-2015. Технические средства охранной сигнализации. Классификация. Общие технические требования и методы испытаний (с Изменением №1).

20. ГОСТ 34025-2016. Извещатели охранные поверхностные звуковые для блокировки остекленных конструкций помещений. Общие технические требования и методы испытаний.

21. ГОСТ Р 54832-2011. Извещатели охранные точечные магнитоконтактные. Общие технические требования и методы испытаний.

22. Рябцев, Н.А. Р 069-2017. Рекомендации по выбору и применению средств обнаружения проникновения в зависимости от степени важности и опасности охраняемых объектов / А.В. Климов, Н.А. Рябцев, В.А. Николаев и др. – М.: ФКУ «НИЦ «Охрана» Росгвардии, 2017. – 160 с.

23. Рябцев, Н.А. Р 78.36.044-2014. Методическое пособие по выбору и применению охранных поверхностных звуковых извещателей для блокировки остекленных конструкций закрытых помещений / А.В. Климов, Н.А. Рябцев, А.Н. Членов и др. – М.: ФКУ НИЦ «Охрана» МВД России, 2014. – 92 с.

24. Единые требования к системам передачи извещений, объектовым техническим средствам охраны и охранным сигнально-противоугонным устройствам автотранспортных средств, предназначенным для применения в подразделениях вневедомственной охраны Росгвардии.

25. О промышленной безопасности опасных производственных объектов: Федеральный закон № 116-ФЗ от 21 июля 1997 г.

26. Глазунов, А.М. Сбор и подготовка скважинной продукции [Электронный ресурс]. – Режим доступа: https://studopedia.su/6_38363_ustanovki-podgotovki-nefti-upn.html (дата обращения: 28.02.2020).

27. Коршак, А.А. Основы нефтегазового дела: учебник для вузов / А.А. Коршак, А.М. Шаммазов. – Уфа: ООО «Дизайн Полиграф Сервис», 2001. – 544 с.

28. Андоськин, В.А. Нефть: от шахты до потребителя / В.А. Андоськин, Ю.В. Маркова // Международный студенческий научный вестник. – 2015. – № 5-1. – С. 61.

29. Писаная, Е.А. Установка комплексной подготовки нефти / Е.А. Писаная, О.В. Кохан // Международный студенческий научный вестник. – 2016. – № 5-3. С. 473-473b.

30. Козьминых, С.И. Обеспечение комплексной безопасности автозаправочных комплексов / С.А. Качанов, С.И. Козьминых // Технологии гражданской безопасности. – 2009. – Т. 6. – № 1-2. – С. 94-96.

31. Козьминых, С.И. Методические основы проектирования и внедрения интегрированных систем безопасности на объектах информатизации топливно-энергетического комплекса / С.И. Козьминых // Информационные ресурсы России. – 2018. – № 2 (162). – С. 2-7.

32. Буцынская, Т.А. Особенности совместного функционирования систем пожарной и охранной сигнализации / Т.А. Буцынская // Материалы двадцать шестой научно-технической конференции «Системы безопасности – 2017». – М.: Академия ГПС МЧС России, 2017. – С. 319-321.

33. Надеждин, Ю.М. Безопасность АСУ ТП критически важных объектов / Ю.М. Надеждин // Системы безопасности. – 2014. – №2. – С. 34-39.

34. Рябцев, Н.А. Обобщенная оценка уровня безопасности промышленного объекта / А.Н. Членов, Т.А. Буцынская, Н.А. Рябцев // Пожары и чрезвычайные ситуации: предотвращение, ликвидация. – 2019. – № 2. – С. 5-8.

35. Членов, А.Н. Комплексная оценка уровня безопасности объекта от угроз пожара и проникновения нарушителя / А.Н. Членов // Материалы научно-практической конференции «Современные проблемы тушения пожаров». Ч.2. – М.: ГУГПС-МИПБ МВД России. – 2000. – С.145-152.

36. Горбунов, В.М. Теория принятия решений: Учебное пособие / В.М. Горбунов. – Томск: Национальный исследовательский томский политехнический университет, 2010. – 67 с.

37. Гончаров, В.А. Методы оптимизации: Учебное пособие для вузов. – Люберцы: Юрайт, 2016. – 191 с.

38. Пантелеев, А.В. Методы оптимизации в примерах и задачах: Учебное пособие / А.В. Пантелеев, Т.А. Летова. – СПб.: Лань, 2015. – 512 с.

39. Осипова, М.Н. Методическое пособие по оценке пожароопасности помещений различного назначения методом Гретенера. – М.: НОУ «Такир», 1998. – 68 с.

40. Костерин, И.В. Экспертный метод оценки пожарной опасности многофункциональных общественных зданий [Электронный ресурс] // Технологии техносферной безопасности». – 2011. – Вып. 2 (36). – Режим доступа: http://agps-2006.narod.ru/ttb/2011-2/12-02-11.ttb.pdf (дата обращения: 28.02.2020).

41. Членов, А.Н. Разработка методов и технических средств повышения эффективности охранно-пожарной сигнализации в интегрированных системах управления безопасностью объектов: дис. … д-ра техн. наук: 05.13.10 / Членов Анатолий Николаевич. – М.: Академия ГПС МЧС России, 2001. – 487 с.

42. Буцынская, Т.А. Автоматизация охранно-пожарной сигнализации интегрированной АСУТП предприятия электронного приборостроения на основе ультразвукового модуля: дис. … канд. техн. наук: 05.13.06 / Буцынская Татьяна Анатольевна. – М.: Академия ГПС МЧС России, 2009. – 168 с.

43. Шакирова, А.Ф. Автоматизированная интегрированная система охраны и противопожарной защиты предприятий электронного приборостроения: дис. … канд. техн. наук: 05.13.06 / Шакирова Анастасия Фатековна. – М.: Академия ГПС МЧС России, 2013. – 217 с.

44. Членов, А.Н. Оценка качества систем охранно-пожарной сигнализации на этапах жизненного цикла / А.Н. Членов // Материалы седьмой международной конференции "Системы безопасности" – СБ-98. – М.: МИПБ МВД России, 1998. С. 228, 229.

45. Буцынская, Т.А. Роль этапа проектирования в жизненном цикле системы тревожной сигнализации / Буцынская Т.А., Шакирова А.Ф. // Материалы науч.-практ. конф. – Иваново: Ивановский институт Государственной противопожарной службы МЧС России, 2010.

46. Шакирова, А.Ф. Структурированная база данных для систем охраны и пожарной безопасности объектов / А.Ф. Шакирова // Материалы научно-технической конференции молодых ученых и специалистов «Проблемы техносферной безопасности». – М.: Академия ГПС МЧС России, 2013.

47. Шакирова А.Ф. Современное состояние системы охраны и безопасности предприятия электронного приборостроения и задачи ее совершенствования / Шакирова А.Ф. // Материалы научно-технической конференции молодых ученых и специалистов «Проблемы техносферной безопасности». – М.: Академия ГПС МЧС России, 2013.

48. IEC 62642-8:2011. Alarm systems – Intrusion and hold-up systems – Part 8: Security fog device/systems. – М.: Стандартинформ, 2011. – 50 с.

49. ГОСТ Р 53704-2009. Системы безопасности комплексные и интегрированные. Общие технические требования.

50. ГОСТ Р 57674-2017. Интегрированные системы безопасности. Общие положения.

51. Серезевский, А.В. Вопросы обеспечения централизованной охраны с точки зрения информационных процессов / А.В. Серезевский, С.П. Борисов // Безопасность. – 4/2014. – С. 46-47.

52. Серезевский, А.В. Сравнительный анализ и перспективы развития использования средств фото и видео-фиксации совместно с системами централизованного наблюдения / А.В. Серезевский, И.А. Баринов, С.П. Борисов, Е.Н. Кузьмина // Алгоритм безопасности. – 2016. – №2. – С. 62-65.

53. ГОСТ Р 54455-2011 (МЭК 62599-1:2010). Системы охранной сигнализации. Методы испытаний на устойчивость к внешним воздействующим факторам.

54. Членов, А.Н. Повышение эффективности систем централизованной охраны на основе совершенствования объектовых комплексов технических средств: дис. канд. техн. наук: 05.13.10 / Членов Анатолий Николаевич. – М.: Академия МВД СССР, 1996.

55. Членов, А.Н. Современное состояние разработки и производства технических средств тревожной сигнализации в России [Электронный ресурс] / А.Н. Членов, Е.В. Самышкина, Б.Г. Новосельцев, М.Е. Канзафарова // Технологии техносферной безопасности. – 2015. – Вып. 1 (59). С. 51-54. – Режим доступа: http://agps-2006.narod.ru/ttb/2015-1/20-01-15.ttb.pdf (дата обращения: 28.02.2020).

56. Антоненко, А.А. Нормативное обеспечение систем комплексной безопасности объектов [Электронный ресурс] / А.А. Антоненко, Т.А. Буцынская, А.Н. Членов // Технологии техносферной безопасности. – 2010. – Вып. 2 (30). – Режим доступа: http://agps-2006.narod.ru/ttb/2010-2/11-02-10.ttb.pdf (дата обращения: 28.02.2020).

57. Рябцев, Н.А. Риск проникновения нарушителя на охраняемый промышленный объект [Электронный ресурс] / А.Н. Членов, Н.А. Рябцев, Т.А. Буцынская // Технологии техносферной безопасности. – 2019. – Вып. 2 (84). – С. 132-137. DOI: 10.25257/TTS.2019.2.84.132-137. – Режим

доступа: http://agps-2006.narod.ru/ttb/ 2019-2/06-02-19.ttb.pdf (дата обращения: 28.02.2020).

58. Рябцев, Н.А. О вероятности обнаружения нарушителя системой тревожной сигнализации [Электронный ресурс] / Н.А. Рябцев, Т.А. Буцынская // Технологии техносферной безопасности. – 2017. – Вып. 1 (71). – С. 312-316. – Режим доступа: http://agps-2006.narod.ru/ttb/2017-1/28-01-17.ttb.pdf (дата обращения: 28.02.2020).

59. Рябцев, Н.А. Оптимизация проектирования охранной сигнализации на основе показателя вероятности эффективного обнаружения проникновения нарушителя [Электронный ресурс] / А.Н. Членов, Н.А. Рябцев, Т.А. Буцынская // Технологии техносферной безопасности. – 2019. – Вып. 3 (85). – С. 86-92. DOI: 10.25257/TTS.2019.3.85.86-92. – Режим доступа: http://agps-2006.narod.ru/ttb/2019-3/03-03-19.ttb.pdf (дата обращения: 28.02.2020).

60. Рябцев, Н.А. Защита систем охранного телевидения от внешнего криминального воздействия [Электронный ресурс] / А.А. Михайлов, А.В. Котельников, Н.А. Рябцев, Ю.И. Дронов, Л.В. Паникова // Технологии техносферной безопасности. – 2016. – Вып. 3 (67). – С. 296-302. – Режим доступа: http://agps-2006.narod.ru/ttb/2016-3/04-03-16.ttb.pdf (дата обращения: 28.02.2020).

61. Волхонский, В.В. Методы оценки эффективности функционирования систем безопасности / В.В. Волхонский // Безопасность, достоверность, информация. – 2002. – № 5. – С. 44-46.

62. Топольский, Н.Г. Оценка эффективности систем безопасности и жизнеобеспечения / Н.Г. Топольский, А.Н. Членов // Сб. тезисов докл. международной конференции «Информатизация правоохранительных систем». – М.: Академия МВД России, 1996.

63. IEC 62642-2-71:2015. Alarm systems – Intrusion and hold-up systems – Part 2-71: Intrusion detectors – Glass break detectors (acoustic). – М.: Стандартинформ, 2015. – 98 с.

64. IEC 62642-2-72:2015. Alarm systems – Intrusion and hold-up systems – Part 2-72: Intrusion detectors – Glass break detectors (passive). – М.: Стандартинформ, 2015. – 94 с.

65. ГОСТ Р 50777-2014. Извещатели пассивные оптико-электронные инфракрасные для закрытых помещений и открытых площадок. Общие технические требования и методы испытаний.

66. ГОСТ Р 51558-2014. Средства и системы охранные телевизионные. Классификация. Общие технические требования. Методы испытаний (с Изменением №1).

67. Членов, А.Н. Новые направления применения видеотехнологий в системах безопасности / А.Н. Членов, Ф.В. Демёхин, Т.А. Буцынская, И.Г. Дровникова // Вестник Московского энергетического института. – 2009. – № 3. – С. 88-93.

68. Синилов, В.Г. Результаты анализа и обработки данных о ложных срабатываниях ТС ОПС / В.Г. Синилов, А.А. Антоненко, Л.И. Савчук // Охранные извещатели, приемно-контрольные приборы и системы передачи извещений: Сб. научн. тр. – М.: ВНИИПО МВД СССР, 1991. – С. 123-128.

69. Рябцев, Н.А. Анализ способов нейтрализации тревожной сигнализации систем охраны категорированных объектов [Электронный ресурс] / А.Н. Членов, Н.А. Рябцев, А.Н. Федин // Технологии техносферной безопасности. – 2017. – Вып. 3 (73). – С. 271-279. – Режим доступа: http://agps-2006.narod.ru/ ttb/2017-3/34-03-17.ttb.pdf (дата обращения: 28.02.2020).

70. Пиготт, С. Выводы инспекции – в кн.: Проблемы ложных срабатываний и меры английской полиции по борьбе с ними. / Пиготт С. / Пер. с англ. – М.: ВЦП НТЛ и Д, 1981. – 43 с.

71. Шепитько, Г.Е. Проблемы охранной безопасности объектов. Часть 1. / Г.Е. Шепитько; под ред. проф. В.А. Минаева. – М.: Русское слово, 1995. – 352 с.

72. Шепитько, Г.Е. Проблемы безопасности объектов: Учебное пособие / Г.Е. Шепитько, И.И. Медведев. – М.: Академия экономической безопасности МВД России, 2006. – 199 с.

73. ГОСТ Р 56102.1-2014. Системы централизованного наблюдения. Часть 1.Общие положения.

74. ГОСТ Р 56102.2-2015. Системы централизованного наблюдения. Часть 2. Подсистема объектовая. Общие технические требования и методы испытаний.

75. Рябцев, Н.А. Особенности применения технических средств безопасности на объектах высоких категорий / Н.А. Рябцев, А.Н. Федин, Н.Г. Метелева // Алгоритм безопасности. – 2018. – № 5. – С. 32-34.

76. Королев, В.Ю. Математические основы теории риска: Учебное пособие / В.Ю. Королев, С.Я. Шоргин, В.Е. Бенинг. – М.: Физматлит, 2011. – 620 с.

77. Гмурман, В.Е. Теория вероятностей и математическая статистика: Учебник для СПО. 12-е изд. – М.: Юрайт. 2016. – 480 с.

78. Волхонский, В.В. Особенности разработки структуры средств обнаружения угроз охраняемому объекту / В.В. Волхонский, А.Г. Крупнов // Научно-технический вестник Санкт-Петербургского государственного университета информационных технологий, механики и оптики. – 2011. – № 4(74). – С. 131-136.

79. Волхонский, В.В. Способ оценки вероятности пресечения проникновения на объект / В.В. Волхонский // Сборник трудов IX международной конференции «Информатизация правоохранительных органов» – М.: МВД России, 2000. – С. 113-119.

80. Шепитько, Г.Е. Исследование характеристик модели нарушителя / Г.Е. Шепитько // Технические средства охраны: Сб. научн. тр. – М.: ВНИИПО МВД России. – 1992. – С. 41-49.

81. Мокшанцев А.В. Модели, методы и алгоритмы поддержки принятия управленческих решений при поиске и обнаружении пострадавших под завалами, образующимися в результате чрезвычайных ситуаций, аварий, пожаров и взрывов [Электронный ресурс] / А.В. Мокшанцев, И.М. Тетерин, Н.Г. Топольский // Технологии техносферной безопасности. – 2013. – Вып. 5 (51). – Режим доступа: http://agps-2006.narod.ru/ttb/2013-5/19-05-13.ttb.pdf (дата обращения: 28.02.2020).

82. Шаровар, Ф.И. Пожаропредупредительная автоматика / Ф.И. Шаровар. – М.: Специнформатика-СИ. – 2013. – 556 с.

83. Членов, А.Н. Групповой извещатель для тревожной сигнализации / А.Н. Членов, Т.А. Буцынская, А.Ф. Шакирова, В.Ю. Фёдоров // Пожары и чрезвычайные ситуации: предотвращение, ликвидация. – 2011. – № 1. – С. 42-46.

84. Горбунов, В.А. Эффективность обнаружения целей. / В.А. Горбунов. – М.: Воениздат. – 1979. – 160 с.

85. Вентцель, Е.С. Теория вероятностей: учебник / Е.С. Вентцель. – 12-е изд., стер. – М.: ЮСТИЦИЯ, 2018. – 658 с.

86. Лежнёв, А.В. Динамическое программирование в экономических задачах / А.В. Лежнёв: Учебное пособие. – М.: Бином, 2010. – 176 с.

87. Юденков, А.В. Математическое программирование в экономике: Учебное пособие / А.В. Юденков. – М.: Финансы и статистика, 2010. – 240 с.

88. Никитин, А.А. Современные модификации акустических извещателей / А.А. Никитин, А.В. Климов // Охрана: служба, технические средства, экономика. – М.: НИЦ «Охрана» МВД России. – 2010. – № 3. – С. 74-78.

89. Рябцев, Н.А. Новый межгосударственный стандарт на акустические извещатели разбития стекла. Что в нем нового для производителей и потребителей? / А.В. Климов, Н.А. Рябцев, С.В. Климова, В.А. Козлов // Алгоритм безопасности. – 2017. – № 4. – С. 46-49.

90. Рябцев, Н.А. Новая система классификации средств обнаружения для особо важных объектов / Н.А. Рябцев, О.Г. Точилова, В.А. Козлов // Алгоритм безопасности. – № 3. – 2018. – С. 70-71.

91. Дивина, Т.В. Основные методы анализа экспертных оценок / Т.В. Дивина, Е.А. Петракова, М.С. Вишневский // Экономика и бизнес: теория и практика. – 2019. – № 7. – С. 42-44.

92. Cooke, R.M. Procedures guide for structured expert judgement, s. l. / R. M. Cooke, L. H. J. Gossens. – University of Technology Delft. – 1999.

93. Дилигенский, Н.В. Нечеткое моделирование и многокритериальная оптимизация производственных систем в условиях неопределенности: технология, экономика, экология / Н.В. Дилигенский, Л.Г. Дымова, П.В. Севастьянов. – М.: Изд-во «Машиностроение − 1», 2004.

94. Gupta, N.M. Fuzzy sets theory and its applications: a survey / N.M. Gupta, R.K. Ragade // Multivariable Technol. Syst.Proc.4th IFAC Int. Symp.1977. – Oxford, 1978. – Pp. 247-259.

95. Hung, T. Theoretical aspects of fuzzy control / T. Hung, M. Sugeno, R. Tong, R.R. Yager. New York: John Wiley and Sons Inc. – 1995. – 267 p.

96. Tryon, R.C. Cluster analysis / R.C. Tryon. – London: Ann Arbor Edwards Bros, 1939. – 139 p.

97. Олдендерфер, М.С. Кластерный анализ: в кн. Факторный, дискриминантный и кластерный анализ / М.С. Олдендерфер, Р.К. Блэшфилд / пер. с англ. под. ред. И.С. Енюкова. – М.: Финансы и статистика, 1989. – 215 с.

98. Айвазян С.А. Прикладная статистика: Классификация и снижение размерности / С.А. Айвазян, В.М. Бухштабер, И.С. Енюков, Л.Д. Мешалкин. – М.: Финансы и статистика, 1989. – 607 с.

99. Рябцев, Н.А. Современные аспекты организации охраны объектов и имущества различных категорий [Электронный ресурс] / А.В. Климов, Н.А. Рябцев, А.Н. Федин, С.В. Климова, О.Г. Точилова // Технологии техносферной безопасности. – 2017. – Вып. 2 (72). – С. 336-343. – Режим доступа:

http://agps-2006.narod.ru/ttb/2017-2/22-02-17.ttb.pdf (дата обращения: 28.02.2020).

100. Рябцев, Н.А. Влияние особенностей охраняемого объекта на выбор конкретного типа акустического извещателя / Н.А. Рябцев // ИнформОхрана. – 2015. – № 9. – С. 21-24. – Режим доступа: http://www.nicohrana.ru/informohrana.html (дата обращения: 28.02.2020).

101. Рябцев, Н.А. Перспективы развития средств обнаружения несанкционированного проникновения в помещения и хранилища ценностей [Электронный ресурс] / А.В. Климов, Н.А. Рябцев, А.Н. Федин // Технологии техносферной безопасности. – 2016. – Вып. 4 (68). – С. 288-294. – Режим доступа: http://agps-2006.narod.ru/ttb/2016-4/29-04-16.ttb.pdf (дата обращения: 28.02.2020).

102. Кузьмин, Ю.Б. Оценка уровня автоматизации предприятия / Ю.Б. Кузьмин // Нефтяное хозяйство. – 2009. – № 10. – С. 104-107.

103. Определение уровня автоматизации технологических объектов [Электронный ресурс]. – 2015. – Режим доступа: https://helpiks.org/4-44750.html (дата обращения: 28.02.2020).

104. ГОСТ 31817.1.1-2012. Системы тревожной сигнализации. Часть 1. Общие требования. Раздел 1. Общие положения (IEC 60839-1-1:1998 Alarm systems. Part 1: General requirements. Section one: General).

105. Рябцев, Н.А. Взрывобезопасные извещатели тревожной сигнализации [Электронный ресурс] / А.Н. Членов, А.В. Климов, Н.А. Рябцев, Т.А. Буцынская // Технологии техносферной безопасности». – 2017. – Вып. 3 (73). – С. 266-270. – Режим доступа: http://agps-2006.narod.ru/ttb/2017-3/33-03-17.ttb.pdf (дата обращения: 28.02.2020).

ПРИЛОЖЕНИЕ А

Акты внедрения
результатов диссертационной работы

УТВЕРЖДАЮ
Заместитель начальника
Академии ГПС МЧС России
по научной работе
доктор технических наук,
профессор

М.В. Алешков
"__" _____ 2019 г.

А К Т
о внедрении результатов диссертации
на соискание ученой степени кандидата
технических наук Рябцева Николая Алексеевича,
подготовленной в Академии ГПС МЧС России

Мы, нижеподписавшиеся, начальник кафедры пожарной автоматики доктор технических наук, доцент Холостов Александр Львович, профессор кафедры пожарной автоматики доктор технических наук, профессор Федоров Андрей Владимирович, кандидат технических наук старший преподаватель Мальцев Алексей Сергеевич составили настоящий акт в том, что результаты кандидатской диссертации Рябцева Н.А. использованы при проведении научно-исследовательской работы по теме: «Применение технических средств тревожной сигнализации на взрывопожароопасных объектах» (план научной работы Академии ГПС на 2019 г., раздел 2.3, п. 77).

Результаты кандидатской диссертации Рябцева Н.А. используются в учебном процессе при преподавании дисциплины «Производственная и пожарная автоматика» курсантам и слушателям, а также для подготовки магистерских диссертаций в Академии ГПС МЧС России.

Начальник кафедры пожарной автоматики
д.т.н., доцент А.Л. Холостов

Профессор кафедры пожарной автоматики
д.т.н., профессор А.В. Федоров

Старший преподаватель кафедры пожарной автоматики
к.т.н. А.С. Мальцев

Разработка, производство и продажа приборов
охранно-пожарной сигнализации, устройств для
видеонаблюдения, а также систем энергосбережения.

УТВЕРЖДАЮ
Генеральный директор
ЗАО «РИЭЛТА»
кандидат технических наук
_____ В.И. Перчуков
«___» ноября 2019 г.

А К Т

о внедрении результатов диссертационной работы Рябцева Николая Алексеевича, представленной на соискание ученой степени кандидата технических наук по специальности 05.13.06 – «Автоматизация и управление технологическими процессами и производствами» (технические науки, отрасль – промышленность)

Комиссия в составе председателя – заместителя генерального директора кандидата технических наук Т.М. Рахматуллиной и членов комиссии: директора по развитию С.В. Образцова и главного технического специалиста Р.Ф. Кутейникова, подтверждает, что результаты диссертационной работы Рябцева Н.А., связанные с совершенствованием средств обнаружения проникновения для охраны особо важных объектов, использованы ЗАО «РИЭЛТА» при разработке, модернизации и серийном производстве извещателей, обладающих повышенными тактико-техническими характеристиками и предназначенными для применения в составе систем охранно-пожарной сигнализации, точечного магнитоуправляемого извещателя ИО102-49, поверхностных звуковых извещателей ИО329-10 «Стекло-4» и ИО329-18 «Стекло-5», а также оптико-электронных извещателей ИО409-30 «Фотон-16», ИО209-27 «Фотон-16А», ИО309-14 «Фотон-16Б».

В соответствии с разработанными в рамках диссертационной работы Рябцева Н.А. нормативно-техническими и методическими документами на предприятии осуществляется контроль качества серийно выпускаемых технических средств охранно-пожарной сигнализации, а также подтверждение их соответствия установленным требованиям в области технического регулирования.

Председатель комиссии: Т.М. Рахматуллина

Члены комиссии: С.В. Образцов

Р.Ф. Кутейников

РОССИЯ, 197101, Санкт-Петербург, ул.Чапаева, 17
Тел./факс: (812) 498-19-71, 233-03-02, 703-13-63
www.rielta.ru, e-mail: rielta@rielta.ru

УТВЕРЖДАЮ
Начальник
ФКУ «НИЦ «Охрана» Росгвардии
полковник полиции
_____ А.И. Кротов
«15» 11 2019 г.

А К Т
о внедрении результатов диссертационной работы
Рябцева Николая Алексеевича, представленной на соискание
ученой степени кандидата технических наук по специальности
05.13.06 – «Автоматизация и управление технологическими процессами
и производствами» (технические науки, отрасль – промышленность)

Комиссия в составе председателя – заместителя начальника ФКУ «НИЦ «Охрана» Росгвардии кандидата технических наук, полковника полиции А.Р. Фамильнова и членов комиссии: начальника отдела развития объектовых систем охраны кандидата технических наук, полковника полиции А.В. Климова, старшего научного сотрудника отдела развития централизованной охраны кандидата технических наук С.В. Петрушкова, подтверждает, что результаты диссертационной работы Рябцева Н.А. связанные с автоматизацией сбора и обработки данных в системе охранно-пожарной сигнализации для применения на объектах высоких категорий значимости, в том числе потенциально опасных и критически важных промышленных объектах, использованы:

1. При выполнении следующих научно-исследовательских и опытно-конструкторских работ:

- К.5.И.05.2014 «Создание и освоение в серийном производстве магнитоконтактного извещателя, устойчивого к саботажу внешним магнитным полем»;
- К.2.И.01.2017 «Создание звукового охранного извещателя, обеспечивающего взаимодействие с устройством оконечным объектовым систем централизованного наблюдения по единому специализированному объектовому протоколу (ЕСОП)»;
- К.2.И.02.2017 «Модернизация серийно выпускаемых объектовых технических средств охранной сигнализации»;
- К.2.И.02.2018 «Создание и освоение в промышленном производстве охранного точечного извещателя, предназначенного для обнаружения несанкционированного открывания дверных и оконных конструкций, обеспечивающего взаимодействие с устройством оконечным объектовым системы централизованного наблюдения по Единому специализированному объектовому протоколу обмена информацией (ЕСОП)»;

- К.2.И.03.2018 «Модернизация серийно выпускаемых объектовых технических средств охранной сигнализации»;

2. В учебном процессе ФКУ «НИЦ «Охрана» Росгвардии при организации дополнительного профессионального образования и повышении квалификации военнослужащих (сотрудников) войск национальной гвардии Российской Федерации;

3. При разработке и актуализации (внесении изменений) нормативно-технической и методической документации:

- межгосударственного стандарта ГОСТ 34025-2016;

- национальных стандартов Российской Федерации ГОСТ Р 52435-2015 и ГОСТ Р 54832-2011;

- Р 069-2017 Рекомендаций по выбору и применению средств обнаружения проникновения в зависимости от степени важности и опасности охраняемых объектов;

- Р 78.36.044-2014 Методического пособия по выбору и применению охранных поверхностных звуковых извещателей для блокировки остекленных конструкций закрытых помещений;

- Единых требований к системам передачи извещений, объектовым техническим средствам охраны и охранным сигнально-противоугонным устройствам автотранспортных средств, предназначенным для применения в подразделениях вневедомственной охраны войск национальной гвардии Российской Федерации;

4. При разработке и модернизации извещателей с повышенной эффективностью обнаружения, внедренных в серийное производство: магнитоконтактных ИО102-55 «Кенар» и ИО102-55/1 «Кенар-М», магнитоуправляемого ИО102-49, звуковых ИО329-19 «Астра-618», ИО329-10 «Стекло-4», ИО329-18 «Стекло-5», а также оптико-электронных ИО409-30 «Фотон-16», ИО209-27 «Фотон-16А», ИО309-14 «Фотон-16Б».

Председатель комиссии:

Заместитель начальника
ФКУ «НИЦ «Охрана» Росгвардии,
полковник полиции, к.т.н. А.Р. Фамильнов

Члены комиссии:

Начальник отдела развития объектовых систем охраны
ФКУ «НИЦ «Охрана» Росгвардии
полковник полиции, к.т.н. А.В. Климов

Старший научный сотрудник
отдела развития централизованной охраны
ФКУ «НИЦ «Охрана» Росгвардии, к.т.н. С.В. Петрушков

ПРИЛОЖЕНИЕ Б
Патент на полезную модель

РОССИЙСКАЯ ФЕДЕРАЦИЯ

ПАТЕНТ

НА ПОЛЕЗНУЮ МОДЕЛЬ

№ 189504

Охранный магнитоконтактный извещатель

Патентообладатель: ***Членов Анатолий Николаевич (RU)***

Авторы: ***Членов Анатолий Николаевич (RU), Рябцев Николай Алексеевич (RU), Буцынская Татьяна Анатольевна (RU)***

Заявка № **2018141434**
Приоритет полезной модели **26 ноября 2018 г.**
Дата государственной регистрации в Государственном реестре полезных моделей Российской Федерации **24 мая 2019 г.**
Срок действия исключительного права на полезную модель истекает **26 ноября 2028 г.**

Руководитель Федеральной службы по интеллектуальной собственности

Г.П. Ивлиев

ПРИЛОЖЕНИЕ В

Расчетные материалы кластерного анализа параметров технических средств систем охранно-пожарной сигнализации и объектов, принимаемых под централизованную охрану

1. Кластерный анализ параметров технических средств систем охранно-пожарной сигнализации

Матрица Евклидовых расстояний для проведения кластерного анализа параметров технических средств систем охранно-пожарной сигнализации.

№ п/п	1	2	3	4	5	6	7	8	9
x_1	3	1	1	2	4	3	3	2	1
x_2	6	2	1	3	10	5	6	4	1

Агломеративным иерархическим алгоритмом классификации определяем расстояния между объектами и представляем полученные данные в матрице расстояний. Процесс объединения кластеров производим последовательно методом одиночной связи.

№ п/п	1	2	3	4	5	6	7	8	9
1	0	4,472	5,385	3,162	4,123	1	0	2,236	5,385
2	4,472	0	1	1,414	8,544	3,606	4,472	2,236	1
3	5,385	1	0	2,236	9,487	4,472	5,385	3,162	0
4	3,162	1,414	2,236	0	7,28	2,236	3,162	1	2,236
5	4,123	8,544	9,487	7,28	0	5,099	4,123	6,325	9,487
6	1	3,606	4,472	2,236	5,099	0	1	1,414	4,472
7	0	4,472	5,385	3,162	4,123	1	0	2,236	5,385
8	2,236	2,236	3,162	1	6,325	1,414	2,236	0	3,162
9	5,385	1	0	2,236	9,487	4,472	5,385	3,162	0

Из матрицы расстояний следует, что объекты № 1 и № 7 наиболее близки $P_{1;7} = 0$ и поэтому объединяются в один кластер.

№ п/п	**[1]**	2	3	4	5	6	**[7]**	8	9
[1]	0	4,472	5,385	3,162	4,123	1	0	2,236	5,385
2	4,472	0	1	1,414	8,544	3,606	4,472	2,236	1
3	5,385	1	0	2,236	9,487	4,472	5,385	3,162	0
4	3,162	1,414	2,236	0	7,28	2,236	3,162	1	2,236
5	4,123	8,544	9,487	7,28	0	5,099	4,123	6,325	9,487
6	1	3,606	4,472	2,236	5,099	0	1	1,414	4,472
[7]	0	4,472	5,385	3,162	4,123	1	0	2,236	5,385
8	2,236	2,236	3,162	1	6,325	1,414	2,236	0	3,162
9	5,385	1	0	2,236	9,487	4,472	5,385	3,162	0

При формировании новой матрицы расстояний выбираем наименьшее значение из значений объектов № 1 и № 7. В результате имеем 8 кластеров: $S_{(1, 7)}$, $S_{(2)}$, $S_{(3)}$, $S_{(4)}$, $S_{(5)}$, $S_{(6)}$, $S_{(8)}$, $S_{(9)}$.

Из матрицы расстояний следует, что объекты № 3 и № 9 наиболее близки $P_{3; 9} = 0$ и поэтому объединяются в один кластер.

№ п/п	1, 7	2	**[3]**	4	5	6	8	**[9]**
1, 7	0	4,472	5,385	3,162	4,123	1	2,236	5,385
2	4,472	0	1	1,414	8,544	3,606	2,236	1
[3]	5,385	1	0	2,236	9,487	4,472	3,162	0
4	3,162	1,414	2,236	0	7,28	2,236	1	2,236
5	4,123	8,544	9,487	7,28	0	5,099	6,325	9,487
6	1	3,606	4,472	2,236	5,099	0	1,414	4,472
8	2,236	2,236	3,162	1	6,325	1,414	0	3,162
[9]	5,385	1	0	2,236	9,487	4,472	3,162	0

При формировании новой матрицы расстояний выбираем наименьшее значение из значений объектов №3 и №9. В результате имеем 7 кластеров: $S_{(1, 7)}$, $S_{(2)}$, $S_{(3, 9)}$, $S_{(4)}$, $S_{(5)}$, $S_{(6)}$, $S_{(8)}$.

Из матрицы расстояний следует, что объекты № 1, 7 и № 6 наиболее близки $P_{1, 7; 6} = 1$ и поэтому объединяются в один кластер.

№ п/п	**[1, 7]**	2	3, 9	4	5	**[6]**	8
[1, 7]	0	4,472	5,385	3,162	4,123	1	2,236
2	4,472	0	1	1,414	8,544	3,606	2,236
3, 9	5,385	1	0	2,236	9,487	4,472	3,162
4	3,162	1,414	2,236	0	7,28	2,236	1
5	4,123	8,544	9,487	7,28	0	5,099	6,325
[6]	1	3,606	4,472	2,236	5,099	0	1,414
8	2,236	2,236	3,162	1	6,325	1,414	0

При формировании новой матрицы расстояний выбираем наименьшее значение из значений объектов № 1, 7 и № 6. В результате имеем 6 кластеров: $S_{(1, 7, 6)}$, $S_{(2)}$, $S_{(3, 9)}$, $S_{(4)}$, $S_{(5)}$, $S_{(8)}$.

Из матрицы расстояний следует, что объекты № 2 и № 3, 9 наиболее близки $P_{2; 3, 9} = 1$ и поэтому объединяются в один кластер.

№ п/п	1, 7, 6	**[2]**	**[3, 9]**	4	5	8
1, 7, 6	0	3,606	4,472	2,236	4,123	1,414
[2]	3,606	0	1	1,414	8,544	2,236
[3, 9]	4,472	1	0	2,236	9,487	3,162
4	2,236	1,414	2,236	0	7,28	1
5	4,123	8,544	9,487	7,28	0	6,325
8	1,414	2,236	3,162	1	6,325	0

При формировании новой матрицы расстояний выбираем наименьшее значение из значений объектов № 2 и № 3, 9. В результате имеем 5 кластеров: $S_{(1, 7, 6)}$, $S_{(2, 3, 9)}$, $S_{(4)}$, $S_{(5)}$, $S_{(8)}$.

Из матрицы расстояний следует, что объекты № 4 и № 8 наиболее близки $P_{4; 8} = 1$ и поэтому объединяются в один кластер.

№ п/п	1, 7, 6	2, 3, 9	**[4]**	5	**[8]**
1, 7, 6	0	3,606	2,236	4,123	1,414
2, 3, 9	3,606	0	1,414	8,544	2,236
[4]	2,236	1,414	0	7,28	1
5	4,123	8,544	7,28	0	6,325
[8]	1,414	2,236	1	6,325	0

При формировании новой матрицы расстояний выбираем наименьшее значение из значений объектов № 4 и № 8. В результате имеем 4 кластера: $S_{(1, 7, 6)}$, $S_{(2, 3, 9)}$, $S_{(4, 8)}$, $S_{(5)}$.

Из матрицы расстояний следует, что объекты № 1, 7, 6 и № 4, 8 наиболее близки $P_{1, 7, 6; 4, 8} = 1{,}414$ и поэтому объединяются в один кластер.

№ п/п	**[1, 7, 6]**	2,3,9	**[4, 8]**	5
[1, 7, 6]	0	3,606	1,414	4,123
2, 3, 9	3,606	0	1,414	8,544
[4, 8]	1,414	1,414	0	6,325
5	4,123	8,544	6,325	0

При формировании новой матрицы расстояний выбираем наименьшее значение из значений объектов № 1, 7, 6 и № 4, 8. В результате имеем 3 кластера: $S_{(1, 7, 6, 4, 8)}$, $S_{(2, 3, 9)}$, $S_{(5)}$. Из матрицы расстояний следует, что объекты № 1, 7, 6, 4, 8 и № 2, 3, 9 наиболее близки $P_{1, 7, 6, 4, 8; 2, 3, 9} = 1{,}414$ и поэтому объединяются в один кластер.

№ п/п	**[1, 7, 6, 4, 8]**	**[2, 3, 9]**	5
[1, 7, 6, 4, 8]	0	1,414	4,123
[2, 3, 9]	1,414	0	8,544
5	4,123	8,544	0

При формировании новой матрицы расстояний выбираем наименьшее значение из значений объектов № 1, 7, 6, 4, 8 и № 2, 3, 9. В результате имеем 2 кластера: $S_{(1, 7, 6, 4, 8, 2, 3, 9)}$, $S_{(5)}$.

№ п/п	1, 7, 6, 4, 8, 2, 3, 9	5
1, 7, 6, 4, 8, 2, 3, 9	0	4,123
5	4,123	0

Таким образом, при проведении кластерного анализа получили два кластера, расстояние между которыми равно P = 4,123.

2. Кластерный анализ объектов, принимаемых под централизованную охрану

Матрица Евклидовых расстояний для проведения кластерного анализа объектов, принимаемых под централизованную охрану

№ п/п	1	2	3	4	5	6	7	8	9	10	11
x_1	11	10	9	7	2	8	6	4	5	3	1
x_2	1	1	0,9	0,9	0,9	1	1	0,9	1	0,9	0,25

Агломеративным иерархическим алгоритмом классификации определяем расстояния между объектами и представляем полученные данные в матрице расстояний. Процесс объединения кластеров производим последовательно методом одиночной связи.

№ п/п	1	2	3	4	5	6	7	8	9	10	11
1	0	1	2,002	4,001	9,001	3	5	7,001	6	8,001	10,028
2	1	0	1,005	3,002	8,001	2	4	6,001	5	7,001	9,031
3	2,002	1,005	0	2	7	1,005	3,002	5	4,001	6	8,026
4	4,001	3,002	2	0	5	1,005	1,005	3	2,002	4	6,035
5	9,001	8,001	7	5	0	6,001	4,001	2	3,002	1	1,193
6	3	2	1,005	1,005	6,001	0	2	4,001	3	5,001	7,04
7	5	4	3,002	1,005	4,001	2	0	2,002	1	3,002	5,056
8	7,001	6,001	5	3	2	4,001	2,002	0	1,005	1	3,07
9	6	5	4,001	2,002	3,002	3	1	1,005	0	2,002	4,07
10	8,001	7,001	6	4	1	5,001	3,002	1	2,002	0	2,103
11	10,028	9,031	8,026	6,035	1,193	7,04	5,056	3,07	4,07	2,103	0

Из матрицы расстояний следует, что объекты № 1 и № 2 наиболее близки $P_{1;2} = 1$ и поэтому объединяются в один кластер.

№ п/п	**[1]**	**[2]**	3	4	5	6	7	8	9	10	11
[1]	0	1	2,002	4,001	9,001	3	5	7,001	6	8,001	10,028
[2]	1	0	1,005	3,002	8,001	2	4	6,001	5	7,001	9,031
3	2,002	1,005	0	2	7	1,005	3,002	5	4,001	6	8,026
4	4,001	3,002	2	0	5	1,005	1,005	3	2,002	4	6,035
5	9,001	8,001	7	5	0	6,001	4,001	2	3,002	1	1,193
6	3	2	1,005	1,005	6,001	0	2	4,001	3	5,001	7,04
7	5	4	3,002	1,005	4,001	2	0	2,002	1	3,002	5,056
8	7,001	6,001	5	3	2	4,001	2,002	0	1,005	1	3,07
9	6	5	4,001	2,002	3,002	3	1	1,005	0	2,002	4,07
10	8,001	7,001	6	4	1	5,001	3,002	1	2,002	0	2,103
11	10,028	9,031	8,026	6,035	1,193	7,04	5,056	3,07	4,07	2,103	0

При формировании новой матрицы расстояний выбираем наименьшее значение из значений объектов № 1 и № 2. В результате имеем 10 кластеров: $S_{(1, 2)}$, $S_{(3)}$, $S_{(4)}$, $S_{(5)}$, $S_{(6)}$, $S_{(7)}$, $S_{(8)}$, $S_{(9)}$, $S_{(10)}$, $S_{(11)}$.

Из матрицы расстояний следует, что объекты № 5 и № 10 наиболее близки $P_{5; 10} = 1$ и поэтому объединяются в один кластер.

№ п/п	1, 2	3	4	**[5]**	6	7	8	9	**[10]**	11
1, 2	0	1,005	3,002	8,001	2	4	6,001	5	7,001	9,031
3	1,005	0	2	7	1,005	3,002	5	4,001	6	8,026
4	3,002	2	0	5	1,005	1,005	3	2,002	4	6,035
[5]	8,001	7	5	0	6,001	4,001	2	3,002	1	1,193
6	2	1,005	1,005	6,001	0	2	4,001	3	5,001	7,04
7	4	3,002	1,005	4,001	2	0	2,002	1	3,002	5,056
8	6,001	5	3	2	4,001	2,002	0	1,005	1	3,07
9	5	4,001	2,002	3,002	3	1	1,005	0	2,002	4,07
[10]	7,001	6	4	1	5,001	3,002	1	2,002	0	2,103
11	9,031	8,026	6,035	1,193	7,04	5,056	3,07	4,07	2,103	0

При формировании новой матрицы расстояний выбираем наименьшее значение из значений объектов № 5 и № 10. В результате имеем 9 кластеров: $S_{(1, 2)}$, $S_{(3)}$, $S_{(4)}$, $S_{(5, 10)}$, $S_{(6)}$, $S_{(7)}$, $S_{(8)}$, $S_{(9)}$, $S_{(11)}$.

Из матрицы расстояний следует, что объекты № 5, 10 и № 8 наиболее близки $P_{5, 10; 8} = 1$ и поэтому объединяются в один кластер.

№ п/п	1,2	3	4	**[5, 10]**	6	7	**[8]**	9	11
1,2	0	1,005	3,002	7,001	2	4	6,001	5	9,031
3	1,005	0	2	6	1,005	3,002	5	4,001	8,026
4	3,002	2	0	4	1,005	1,005	3	2,002	6,035
[5, 10]	7,001	6	4	0	5,001	3,002	1	2,002	1,193

№ п/п	1,2	3	4	**[5, 10]**	6	7	**[8]**	9	11
6	2	1,005	1,005	5,001	0	2	4,001	3	7,04
7	4	3,002	1,005	3,002	2	0	2,002	1	5,056
[8]	6,001	5	3	1	4,001	2,002	0	1,005	3,07
9	5	4,001	2,002	2,002	3	1	1,005	0	4,07
11	9,031	8,026	6,035	1,193	7,04	5,056	3,07	4,07	0

При формировании новой матрицы расстояний выбираем наименьшее значение из значений объектов № 5, 10 и № 8. В результате имеем 8 кластеров: $S_{(1, 2)}$, $S_{(3)}$, $S_{(4)}$, $S_{(5, 10, 8)}$, $S_{(6)}$, $S_{(7)}$, $S_{(9)}$, $S_{(11)}$.

Из матрицы расстояний следует, что объекты № 7 и № 9 наиболее близки $P_{7; 9} = 1$ и поэтому объединяются в один кластер.

№ п/п	1, 2	3	4	5, 10, 8	6	**[7]**	**[9]**	11
1, 2	0	1,005	3,002	6,001	2	4	5	9,031
3	1,005	0	2	5	1,005	3,002	4,001	8,026
4	3,002	2	0	3	1,005	1,005	2,002	6,035
5, 10, 8	6,001	5	3	0	4,001	2,002	1,005	1,193
6	2	1,005	1,005	4,001	0	2	3	7,04
[7]	4	3,002	1,005	2,002	2	0	1	5,056
[9]	5	4,001	2,002	1,005	3	1	0	4,07
11	9,031	8,026	6,035	1,193	7,04	5,056	4,07	0

При формировании новой матрицы расстояний выбираем наименьшее значение из значений объектов № 7 и № 9. В результате имеем 7 кластеров: $S_{(1, 2)}$, $S_{(3)}$, $S_{(4)}$, $S_{(5, 10, 8)}$, $S_{(6)}$, $S_{(7, 9)}$, $S_{(11)}$.

Из матрицы расстояний следует, что объекты № 1, 2 и № 3 наиболее близки $P_{1, 2; 3} = 1{,}005$ и поэтому объединяются в один кластер.

№ п/п	**[1, 2]**	**[3]**	4	5, 10, 8	6	7,9	11
[1, 2]	0	1,005	3,002	6,001	2	4	9,031
[3]	1,005	0	2	5	1,005	3,002	8,026
4	3,002	2	0	3	1,005	1,005	6,035
5, 10, 8	6,001	5	3	0	4,001	1,005	1,193
6	2	1,005	1,005	4,001	0	2	7,04
7,9	4	3,002	1,005	1,005	2	0	4,07
11	9,031	8,026	6,035	1,193	7,04	4,07	0

При формировании новой матрицы расстояний выбираем наименьшее значение из значений объектов № 1, 2 и № 3. В результате имеем 6 кластеров: $S_{(1, 2, 3)}$, $S_{(4)}$, $S_{(5, 10, 8)}$, $S_{(6)}$, $S_{(7, 9)}$, $S_{(11)}$.

Из матрицы расстояний следует, что объекты № 1, 2, 3 и № 6 наиболее близки $P_{1, 2, 3; 6} = 1{,}005$ и поэтому объединяются в один кластер.

№ п/п	**[1, 2, 3]**	4	5, 10, 8	**[6]**	7,9	11
[1, 2, 3]	0	2	5	1,005	3,002	8,026
4	2	0	3	1,005	1,005	6,035
5, 10, 8	5	3	0	4,001	1,005	1,193
[6]	1,005	1,005	4,001	0	2	7,04
7,9	3,002	1,005	1,005	2	0	4,07
11	8,026	6,035	1,193	7,04	4,07	0

При формировании новой матрицы расстояний выбираем наименьшее значение из значений объектов № 1, 2, 3 и № 6. В результате имеем 5 кластеров: $S_{(1, 2, 3, 6)}$, $S_{(4)}$, $S_{(5, 10, 8)}$, $S_{(7, 9)}$, $S_{(11)}$.

Из матрицы расстояний следует, что объекты № 1, 2, 3, 6 и № 4 наиболее близки $P_{1, 2, 3, 6; 4} = 1{,}005$ и поэтому объединяются в один кластер.

№ п/п	**[1, 2, 3, 6]**	**[4]**	5, 10, 8	7, 9	11
[1, 2, 3, 6]	0	1,005	4,001	2	7,04
[4]	1,005	0	3	1,005	6,035
5, 10, 8	4,001	3	0	1,005	1,193
7, 9	2	1,005	1,005	0	4,07
11	7,04	6,035	1,193	4,07	0

При формировании новой матрицы расстояний выбираем наименьшее значение из значений объектов № 1, 2, 3, 6 и № 4. В результате имеем 4 кластера: $S_{(1, 2, 3, 6, 4)}$, $S_{(5, 10, 8)}$, $S_{(7, 9)}$, $S_{(11)}$.

Из матрицы расстояний следует, что объекты № 1, 2, 3, 6, 4 и № 7, 9 наиболее близки $P_{1, 2, 3, 6, 4; 7, 9} = 1{,}005$ и поэтому объединяются в один кластер.

№ п/п	**[1, 2, 3, 6, 4]**	5, 10, 8	**[7, 9]**	11
[1, 2, 3, 6, 4]	0	3	1,005	6,035
5, 10, 8	3	0	1,005	1,193
[7, 9]	1,005	1,005	0	4,07
11	6,035	1,193	4,07	0

При формировании новой матрицы расстояний выбираем наименьшее значение из значений объектов № 1, 2, 3, 6, 4 и № 7, 9. В результате имеем 3 кластера: $S_{(1, 2, 3, 6, 4, 7, 9)}$, $S_{(5, 10, 8)}$, $S_{(11)}$.

Из матрицы расстояний следует, что объекты № 1, 2, 3, 6, 4, 7, 9 и № 5, 10, 8 наиболее близки $P_{1, 2, 3, 6, 4, 7, 9; 5, 10, 8} = 1{,}005$ и поэтому объединяются в один кластер.

№ п/п	**[1, 2, 3, 6, 4, 7, 9]**	**[5, 10, 8]**	11
[1, 2, 3, 6, 4, 7, 9]	0	1,005	4,07
[5, 10, 8]	1,005	0	1,193
11	4,07	1,193	0

При формировании новой матрицы расстояний выбираем наименьшее значение из значений объектов № 1, 2, 3, 6, 4, 7, 9 и № 5, 10, 8. В результате имеем 2 кластера: $S_{(1, 2, 3, 6, 4, 7, 9, 5, 10, 8)}$, $S_{(11)}$.

№ п/п	1, 2, 3, 6, 4, 7, 9, 5, 10, 8	11
1, 2, 3, 6, 4, 7, 9, 5, 10, 8	0	1,193
11	1,193	0

Таким образом, при проведении кластерного анализа получили два кластера, расстояние между которыми равно P = 1,193.

ПРИЛОЖЕНИЕ Г

Технические характеристики
разработанных в результате исследований извещателей
с повышенной эффективностью обнаружения для применения
на потенциально опасных промышленных объектах

Извещатели точечные магнитоконтактные ИО102-55 «Кенар», ИО102-55/1 «Кенар-М»

Предназначены для блокировки дверных и оконных проемов, других строительных конструктивных элементов зданий, сооружений на открывание или смещение.

Коммутируемое напряжение, В	от 0,05 до 50
Максимальный коммутируемый ток, мА	0,05
Коммутируемая мощность, макс., Вт	10
Наработка в указанных диапазонах, количество срабатываний, не менее	10^6
Диапазон рабочих температур, °С	от минус 50 до +50 (+55)*
Габаритные размеры, не более, мм: - исполнительного блока - задающего блока	 80×24×21 (76×24×15)* 80×24×15 (38×15×11)*
Степень защиты, обеспечиваемая оболочкой	IP40 (IP57)*
*для извещателя ИО102-55/1 «Кенар-М»	

Замыкание электрической цепи происходит при расположении исполнительного и задающего блоков извещателя на расстоянии 12 мм и менее между ними, размыкание – на расстоянии 45 мм и более.

Обладает функцией защиты от попытки умышленного нарушения функционирования при помощи внешнего магнитного поля.

Извещатель точечный магнитоуправляемый ИО102-49

Предназначен для обнаружения несанкционированного открывания подвижной части дверных и оконных конструкций или перемещения отдельно стоящих предметов, выполненных из немагнитного материала (пластика, дерева, цветного металла).

Диапазон напряжений электропитания, В	от 9 до 17
Потребляемый ток, мА, не более	15
Габаритные размеры, мм: - исполнительного блока; - задающего блока	 100 × 25 × 21 60 × 15 × 15
Диапазон рабочих температур, °С	от минус 30 до +55
Степень защиты, обеспечиваемая оболочкой	IP41

По функциональной оснащенности и техническим характеристикам относится к классу 3 по ГОСТ Р 52435-2015, по условиям эксплуатации к классу II по ГОСТ Р 54455-2011.

Формирует извещения путем посылки на средство сбора и обработки информации кодовых комбинаций в соответствии с техническим описанием ЕСОП.

Обладает функцией защиты от маскирования.

Извещатель поверхностный звуковой ИО329-19 «Астра-618»

Предназначен для обнаружения разрушения листовых стекол (остекленных строительных конструкций и элементов интерьера помещения).

Максимальная дальность действия, м	6
Минимальная контролируемая площадь стекла, $м^2$	0,1
Диапазон напряжений электропитания, В	от 9 до 17
Потребляемый ток, мА, не более	35
Габаритные размеры, мм	80×80×35
Диапазон рабочих температур, °С	от минус 20 до +55
Степень защиты, обеспечиваемая оболочкой	IP30

По функциональной оснащенности и техническим характеристикам относится к классу 3 по ГОСТ 34025-2016, по условиям эксплуатации к классу II по ГОСТ Р 54455-2011.

Формирует пять видов извещений путем посылки на средство сбора и обработки информации кодовых комбинаций в соответствии с техническим описанием ЕСОП и передает их по двухпроводной линии связи стандарта RS-485.

В извещателе предусмотрены: защита от несанкционированного вскрытия корпуса, возможность регулировки чувствительности, выбор алгоритма работы, выбор режима тестирования.

Извещатель поверхностный звуковой ИО329-18 «Стекло-5»

Предназначен для обнаружения разрушения листовых стекол (остекленных строительных конструкций и элементов интерьера помещения).

Максимальная дальность действия, м	6
Минимальная контролируемая площадь стекла, $м^2$	0,1
Диапазон напряжений электропитания, В	от 9 до 17
Потребляемый ток, мА, не более	35
Габаритные размеры, мм	87 × 55 × 27
Диапазон рабочих температур, °С	от минус 20 до +55
Степень защиты, обеспечиваемая оболочкой	IP30

По функциональной оснащенности и техническим характеристикам относится к классу 3 по ГОСТ 34025-2016, по условиям эксплуатации к классу II по ГОСТ Р 54455-2011.

Формирует семь видов извещений путем посылки на средство сбора и обработки информации кодовых комбинаций в соответствии с техническим описанием ЕСОП и передает их по двухпроводной линии связи стандарта RS-485.

В извещателе предусмотрены: возможность регулировки чувствительности, световая индикация состояния извещателя и помеховой обстановки внутри охраняемого помещения с возможностью отключения индикации.

Извещатель поверхностный звуковой ИО329-10 «Стекло-4»

Предназначен для обнаружения разрушения листовых стекол (остекленных строительных конструкций и элементов интерьера помещения).

Максимальная дальность действия, м	6
Минимальная контролируемая площадь стекла, $м^2$	0,1
Диапазон напряжений электропитания, В	от 9 до 17
Потребляемый ток, мА, не более	35
Габаритные размеры, мм	80×80×35
Диапазон рабочих температур, °С	от минус 20 до +55
Степень защиты, обеспечиваемая оболочкой	IP30

По функциональной оснащенности и техническим характеристикам относится к классу 3 по ГОСТ 34025-2016, по условиям эксплуатации к классу II по ГОСТ Р 54455-2011.

В извещателе предусмотрены:

- защита от несанкционированного вскрытия корпуса;
- возможность регулировки чувствительности;
- выбор алгоритма работы в зависимости от вида охраняемых стекол и принятой тактики охраны на объекте;
- световая индикация состояния и опознавания извещателя, а также помеховой обстановки внутри охраняемого помещения с возможностью отключения индикации;
- выбор режима тестирования.

Извещатели оптико-электронные ИО409-30 «Фотон-16», ИО209-27 «Фотон-16А», ИО309-14 «Фотон-16Б»

Предназначены для обнаружения проникновения в охраняемое пространство закрытого помещения и формирования извещения о тревоге (блокировка объема коридоров, проходов и иных узких помещений).

Максимальная дальность действия, м - объемного ИО409-30 «Фотон-16» - линейного ИО209-27 «Фотон-16А» - поверхностного ИО309-14 «Фотон-16Б»	 12 20 15
Диапазон напряжения электропитания, В	от 9 до 15
Потребляемый ток, мА	35
Степень защиты, обеспечиваемая оболочкой	IP41
Габаритные размеры, мм	126×70×55
Диапазон рабочих температур, °С	от минус 30 до + 55

По функциональной оснащенности и техническим характеристикам относится к классу 3 по ГОСТ Р 50777-2014, по условиям эксплуатации к классу II по ГОСТ Р 54455-2011.

Имеет три информационных выхода для передачи извещений о тревоге, о неисправности и о несанкционированном доступе. Извещения формирует путем размыкания электрической цепи соответствующего информационного выхода.

Обладает возможностью регулировки чувствительности, температурной компенсацией обнаружительной способности, функцией «память тревоги» и тестовым режимом для регулировки на объекте.