**Содержание**

Введение

Глава 1. Сущность и содержание физической безопасности предприятия

1.1 Принципы, цели и задачи систем физической защиты предприятия

1.2 Анализ уязвимости предприятия

1.3 Разработка технико-экономического обоснования создания СФЗ

Глава 2. Особенности процессов планирования физической безопасности

2.1 Основы построения корпоративной системы физической защиты предприятия

2.2 Концептуальные принципы обеспечения и планирования физической безопасности объектов

Глава 3. Организация физической безопасности как составной части комплексной безопасности на примере Балаковской АЭС

3.1 Характеристика деятельности Балаковской АЭС

3.2 Организация производства на предприятии

3.3 Политика в области физической безопасности Балаковской АЭС

3.4 Требования к системам и органам управления обеспечения физической безопасности предприятия

Заключение

Список литературы

# Введение

Важным условием успешного функционирования любого предприятия на рынке является защита от возникающих угроз, среди которых особую опасность представляют незаконные действия физических лиц. Последствия их действий непредсказуемы от хищения имущества до создания чрезвычайных ситуаций на объекте. В этих условиях безопасность любого субъекта рынка осуществляется на основе принципов «разумной достаточности», «эффективность – стоимость», а также разработанной в теории и применяемой на практике концепции физической безопасности предприятия.

В рамках единой политики безопасности организации физическая безопасность является ее основным структурным элементом, направленным на сохранение собственности, жизни и здоровья персонала, финансовых ресурсов. Концепцией физической безопасности организации предусматривается:

- определение возможных угроз функционированию объектов Компании, вероятных исполнителей угроз (нарушителей); определение наиболее уязвимых мест на объекте, т.е. вероятных предметов защиты;

- оценка уязвимости предметов защиты Компании, т.е. соответствия существующей системы безопасности выявленным угрозам;

- разработка предложений и проведение необходимых мероприятий по обеспечению безопасности объекта.

Физическая безопасность (защиты) организации – это совокупность правовых норм, организационных мер и инженерно-технических решений, направленных на защиту важных интересов и ресурсов предприятия (объекта) от угроз злоумышленных противоправных действий физических лиц (нарушителей). Она включает в себя силы службы безопасности и охраны объекта, комплекс инженерно-технических средств охраны, режим, установленный на объекте. Система физической защиты не должна препятствовать нормальному функционированию организации, ее технологическим процессам.

В современных условиях сложной криминогенной обстановки в мире и РФ вопросы обеспечения безопасности населения и промышленных объектов приобретают особую актуальность. Особую опасность для крупных промышленных объектов представляют злоумышленные несанкционированные действия физических лиц (нарушителей): террористов, диверсантов, преступников, экстремистов. Результаты их действий не предсказуемы: от хищения имущества до создания чрезвычайной ситуации на объекте (пожар, разрушение, затопление, авария, и т.п.).

Одной из эффективных превентивных мер по обеспечению безопасности важных промышленных объектов является создание автоматизированной системы охраны от несанкционированного проникновения физических лиц - системы физической защиты (СФЗ).

Современные СФЗ в корне изменили тактику охраны объектов. В таких системах нет необходимости в организации постовой службы на периметре объекта; вместо этого создаются дежурные тревожные группы, которые начинают немедленные действия по нейтрализации нарушителей после получения сигнала тревоги на центральном пульте управления СФЗ. В них сведено до минимума влияние человеческого фактора и достигается высокая эффективность защиты объекта при минимальном количестве личного состава сил охраны.

Цель написания настоящей дипломной работы - изучение теоретических и практических основ обеспечения физической безопасности предприятия как составной части комплексной безопасности.

Цель работы обусловила постановку и решение следующих задач:

- рассмотреть сущность и содержание физической безопасности предприятия;

- изучить особенности процессов планирования физической безопасности;

- проанализировать организацию систем обеспечения физической безопасности на объекте исследования.

Объект исследования – Балаковская АЭС.

Предмет исследования – система обеспечения физической безопасности предприятия.

# Глава 1. Сущность и содержание физической безопасности предприятия

## 

## 1.1 Принципы, цели и задачи систем физической защиты предприятия

Безопасность объекта физическая - состояние защищенности жизненно-важных интересов (объекта) от угроз, источниками которых являются злоумышленные противоправные (несанкционированные) действия физических лиц (нарушителей).

Концепция безопасности - общий замысел обеспечения безопасности объекта от прогнозируемых угроз.

Уязвимость (объекта) - степень несоответствия принятых мер защиты (объекта) прогнозируемым угрозам или заданным требованиям безопасности.

Чрезвычайная ситуация (на объекте) - состояние, при котором (на объекте) нарушаются нормальные условия жизни и деятельности людей, возникает угроза их жизни и здоровью, наносится ущерб имуществу и окружающей природной среде.

Эффективность системы физической безопасности - вероятность выполнения системой своей основной целевой функции по обеспечению защиты объекта от угроз, источниками которых являются злоумышленные противоправные (несанкционированные) действия физических лиц (нарушителей).

"Система физической защиты" (СФЗ) представляет собой совокупность правовых норм, организационных мер и инженерно-технических решений, направленных на защиту жизненно-важных интересов и ресурсов предприятия (объекта) от угроз, источниками которых являются злоумышленные (несанкционированные) физические воздействия физических лиц - нарушителей (террористов, преступников, экстремистов и др.).

В этом едином комплексе задействованы и люди (служба безопасности, силы охраны), и техника - комплекс инженерно-технических средств охраны (ИТСО) или комплекс инженерно-технических средств физической защиты (ИТСФЗ). От их четкого взаимодействия зависит эффективность СФЗ.

Укрупненная структурная схема типовой СФЗ приведена на рисунке 1.

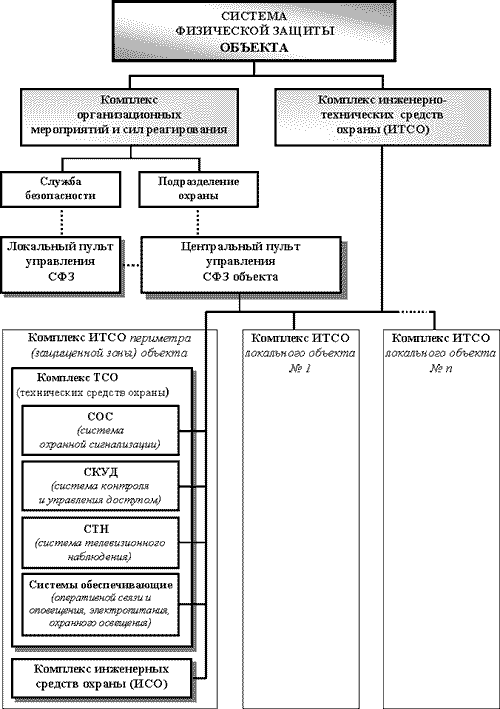


Рис. 1. Система физической безопасности предприятия

Современные СФЗ строятся на базе широкого применения инженерно-технических и программных средств и содержат следующие основные составные части (подсистемы):

- система контроля и управления доступом персонала (СКУД);

- система охранной сигнализации (СОС);

- система телевизионного наблюдения (СТН);

- система оперативной связи и оповещения;

- обеспечивающие системы (освещения, электропитания, охранного освещения и др.).

При создании современных СФЗ, как правило, ставится также и задача защиты жизненно важных центров и систем объекта от непреднамеренных, ошибочных или некомпетентных действий персонала, которые по характеру возможного ущерба приближаются к НСД внешних нарушителей.

Учитывая сложность решаемых задач, создание СФЗ важных объектов не может базироваться на довольно часто применяемом на практике принципе "разумной достаточности", а требует комплексного научного подхода. Такой подход подразумевает проектирование СФЗ важных объектов в две стадии:

а) концептуальное (системное) проектирование;

б) рабочее проектирование.

Основными этапами стадии концептуального проекта являются:

1) Анализ уязвимости объекта и существующей СФЗ;

2) Разработка принципов физической защиты объекта;

3) Разработка технико-экономического обоснования создания СФЗ и комплекса ИТСО.

Основной задачей первых двух этапов стадии концептуального проекта является разработка руководства к действию по созданию СФЗ - "Концепции физической безопасности объекта".

Концепция безопасности определяет пути и методы решения основных задач по обеспечению безопасности объекта и должна отвечать на вопросы: "что защищать?", "от кого защищать?", "как защищать?".

## 1.2 Анализ уязвимости предприятия

Одной из главных задач начальной стадии концептуального проектирования является проведение анализа уязвимости объекта и существующей системы физической безопасности (защиты).

Целями и задачами проведения анализа уязвимости являются:

а) определение важных для жизнедеятельности объекта предметов защиты (наиболее вероятных целей злоумышленных акций нарушителей);

б) определение возможных угроз и моделей вероятных исполнителей угроз (нарушителей);

в) оценка возможного ущерба от реализации прогнозируемых угроз безопасности;

г) оценка уязвимости объекта и существующей системы безопасности;

д) разработка общих рекомендаций по обеспечению безопасности объекта.

Работы проводятся методом экспертных оценок комиссией, в состав которой входят специалисты НИКИРЭТ и специалисты соответствующих служб заказчика: безопасности, главного технолога, главного инженера, пожарной охраны.

Работы проводятся специалистами НИКИРЭТ с применением метода математического (компьютерного) моделирования. Результаты анализа могут оформляться отдельным отчетом. Гриф конфиденциальности определяется заказчиком. К материалам отчета допускается строго ограниченный круг лиц (только непосредственных исполнителей) по существующей на предприятии разрешительной системе. При необходимости, отчет выполняется в одном экземпляре (только для заказчика).

Реализацию жизненно-важных интересов любого предприятия обеспечивают его корпоративные ресурсы. Эти ресурсы должны быть надежно защищены от прогнозируемых угроз безопасности.

Для промышленного предприятия такими важными для жизнедеятельности ресурсами, а, следовательно, предметами защиты являются:

- люди (персонал предприятия);

- имущество:

- важное или дефицитное технологическое оборудование;

- секретная и конфиденциальная документация;

- материальные и финансовые ценности;

- готовая продукция;

- интеллектуальная собственность (ноу-хау);

- средства вычислительной техники (СВТ);

- контрольно-измерительные приборы (КИП) и др.;

- информация конфиденциальная:

- на материальных носителях, а также циркулирующая во внутренних коммуникационных каналах связи и информации, в кабинетах руководства предприятия, на совещаниях и заседаниях;

- финансово-экономические ресурсы, обеспечивающие эффективное и устойчивое развитие предприятия (капитал, коммерческие интересы, бизнес-планы, договорные документы и обязательства и т.п.).

Утрата перечисленных ресурсов может привести:

- к большому материальному ущербу;

- созданию угрозы для жизни и здоровья людей;

- разглашению конфиденциальной информации или сведений, содержащих Государственную тайну;

- банкротству предприятия.

Перечисленные предметы защиты размещаются на соответствующих производственных объектах (подобъектах) предприятия в зданиях и помещениях. Эти подобъекты и являются наиболее уязвимыми местами, выявление которых производится при обследовании объекта.

Таким образом, формулируется ответ на вопрос "что защищать?".

По результатам обследования оформляется специальный типовой "Протокол обследования...", который подписывается заинтересованными сторонами.

Основными угрозами безопасности, которые могут привести к утрате корпоративных ресурсов предприятия, являются:

- чрезвычайная ситуация (пожар, разрушение, затопление, авария, хищение опасных веществ и т.п.);

- хищение или порча имущества;

- несанкционированный съем конфиденциальной информации;

- ухудшение эффективности функционирования, устойчивости развития.

Самой опасной угрозой безопасности промышленного предприятия являются чрезвычайная ситуации (ЧС), которая может привести к большому материальному ущербу, вызвать угрозу для жизни и здоровья людей, а на потенциально опасных объектах - катастрофические последствия для окружающей среды и населения.

В современных условиях несанкционированные действия физических лиц: диверсантов, террористов, преступников, экстремистов представляют особую опасность, т. к. могут привести к возникновению большинства прогнозируемых угроз.

На этапе анализа угроз совместно со службой безопасности заказчика при предварительном обследовании объекта формируется модель вероятных исполнителей угроз (нарушителей), т. е. их количественные и качественные характеристики (оснащенность, тактика действий и т.п.).

В результате проведенной работы формулируется ответ на вопрос: от кого защищать?

Оценка уязвимости существующей СФЗ производится в два этапа:

На первом этапе (при обследовании объекта) методом экспертных оценок производится оценка уязвимости составных частей СФЗ:

- комплекса организационных мероприятий, проводимых администрацией и службой безопасности объекта;

- комплекса инженерно-технических средств охраны (по основным тактико-техническим характеристикам и степени оснащенности объекта);

- сил охраны (по организации, качеству, эффективности действий и др.)

На последующем этапе производится количественная оценка уязвимости существующей СФЗ.

Оценка возможного ущерба от реализации прогнозируемых угроз безопасности производится методом экспертных оценок совместно с представителями компетентных служб заказчика.

Оценка производится для каждого защищаемого подобъекта предприятия. При этом учитываются варианты прогнозируемых акций нарушителей и сценарии их реализации.

Количественная оценка уязвимости объекта и эффективности СФЗ, производится по имеющейся на предприятии компьютерной методике анализа уязвимости и оценки эффективности систем охраны особо важных объектов.

При анализе учитываются прогнозируемые угрозы и модель исполнителей угроз (нарушителей), вероятности обнаружения нарушителя с помощью технических средств, варианты тактики ответных действий сил охраны, временные параметры (времена задержки преодоления нарушителем физических барьеров, время ответных действий сил охраны и др.).

По этой методике в наглядной форме, путем моделирования на ПЭВМ процесса действий нарушителей и сил охраны, производится оценка основного показателя эффективности СФЗ объекта - вероятности перехвата нарушителя силами охраны, действующими по сигналу срабатывания комплекса ИТСО.

По результатам анализа уязвимости разрабатываются общие рекомендации по обеспечению безопасности объекта с ориентировочной оценкой стоимости создания предлагаемой СФЗ. При этом сравнивается ориентировочная стоимость предотвращаемого ущерба (Спу) и затрат на создание предлагаемой СФЗ (Cсфз).

Обязательным критерием целесообразности внедрения СФЗ в систему охраны объекта является выполнение условия неравенства:

Спу > Cсфз.

## 1.3 Разработка технико-экономического обоснования создания СФЗ

С целью достижения оптимального уровня защиты, защищаемые предметы и подобъекты классифицируются по важности (значимости) на категории безопасности. В качестве критерия классификации обычно используется характер или масштаб возможного ущерба в случае реализации основных угроз безопасности данному объекту.

Для подобъектов высшей категории безопасности должен быть установлен максимальный уровень защищенности. Основными последующими задачами концептуального проектирования являются:

Разработка структуры СФЗ и вариантов построения комплекса ИТСО объекта с оценкой стоимости их реализации.

Количественная оценка уязвимости предлагаемой СФЗ с различными вариантами структуры комплекса ИТСО и выбор оптимального варианта комплекса по критерию "эффективность - стоимость" (максимум эффективности при минимуме затрат).

От успешного проведения работ на стадии "Концептуального проекта" зависит оптимальность будущих проектно-технических решений. Именно на этой стадии с использованием методов системного анализа и моделирования происходит обоснование и выбор оптимальной структуры и состава СФЗ и комплекса ИТСО по критерию "эффективность - стоимость".

Сравнительная количественная оценка эффективности вариантов комплекса ИТСО позволяет на начальной (допроектной) стадии выбрать оптимальный вариант комплекса, обладающий достаточно высокой эффективностью при минимальных затратах на его создание и внедрение в систему охраны объекта.

Такой подход позволяет избежать серьезных ошибок в рабочем проекте, а следовательно, и излишних затрат на возможную доработку системы при ее эксплуатации.

Результаты работы этой стадии являются основной составной частью "Концепции..." или технико-экономического обоснование (ТЭО) создания комплекса ИТСО объекта (или группы объектов) и используются в качестве исходных данных для разработки технического задания на рабочее проектирование оборудования объектов комплексами ИТСО.

Результаты работы оформляются в виде ТЭО, которое содержит все необходимые сведения по концепции безопасности, структуре и составу СФЗ и комплекса ИТСО, количественной оценке уязвимости объекта и эффективности существующей и предлагаемой СФЗ, ожидаемые тактико-технико-экономические показатели комплекса ИТСО. В ТЭО приводятся также рекомендации по организации оперативных действий сил охраны с применением комплекса ИТСО, ориентировочный расчет необходимой численности технического персонала для обслуживания комплекса, необходимой численности сил охраны, а также стоимости всех этапов работ по оборудованию объекта предлагаемым комплексом ИТСО.

Этот документ может быть использован службой безопасности заказчика в качестве руководства по организации СФЗ и планированию работ по оборудованию объекта (объектов) комплексом ИТСО или его подсистемами.

Полный перечень основных этапов по созданию и внедрению комплекса ИТСО в эксплуатацию на охраняемом объекте приведен на рисунке 2.

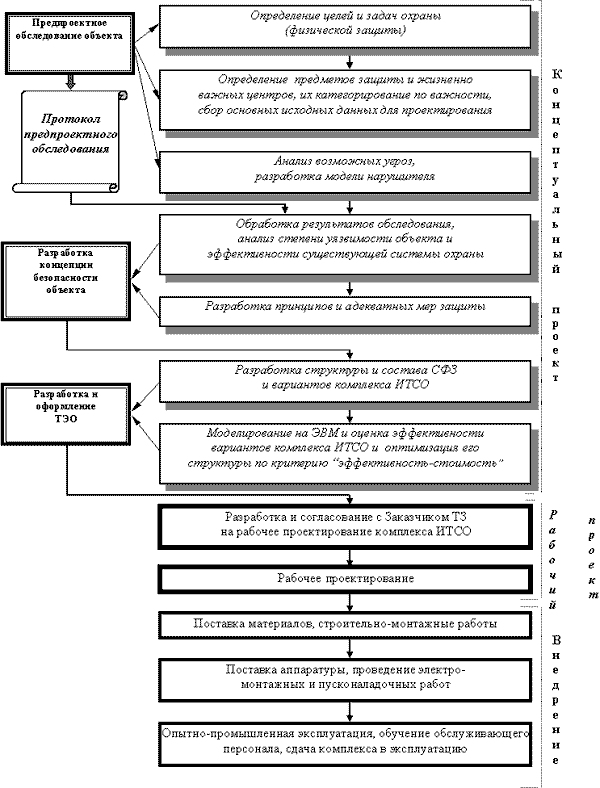


Рис. 2. Перечень основных этапов по созданию и внедрению комплекса ИТСО

Дальнейшим развитием в обеспечении безопасности объектов на современном этапе является создание комплексных (интегрированных) систем безопасности и управления системами жизнеобеспечения объектов (КИСБ). По современной терминологии такие системы называют "Автоматизированные системы управления зданиями" или "Автоматизированные системы управления для "интеллектуальных зданий".

Анализ показывает, что "интеллектуальные" системы могут быть созданы на базе автоматизированных СФЗ, а точнее комплексов ИТСО, имеющих в своем составе полный набор основных подсистем (СКУД, СОС, СТН).

Одним из примеров таких "базовых" систем может служить многоуровневя интегрированная система управления доступом и охранной сигнализацией (СУДОС) "Цирконий-С" разработки и производства НИКИРЭТ. Система выполнена на основе компьютерной сети и ПЭВМ IBM PC и содержит все необходимые компоненты для создания эффективной системы охраны от несанкционированного проникновения физических лиц объектов любой конфигурации и сложности.

В системе совмещены функции контроля и управления доступом персонала в охраняемые зоны и помещения с самыми "изощренными" процедурами входа-выхода и функции центрального пульта охранной сигнализации, приняты необходимые меры по защите информации от несанкционированных воздействий. Имеется возможность подключения и управления работой внешних устройств.

# Глава 2. Особенности процессов планирования физической безопасности

## 

## 2.1 Основы построения корпоративной системы физической защиты предприятия

Системы Физической Защиты (**СФЗ**) объектов представляют собой совокупность технических средств охраны (**ТСО**), средств инженерной укрепленности (**СИУ**) и антитеррористической защиты (**САЗ**), сил физической охраны, специальных мероприятий, направленных на обеспечение безопасности.

СФЗ объектов создаются с определенной целью - противостоять определенным угрозам, то есть снижать вероятность их реализации и возникновения, минимизировать потери в случае их возникновения. При этом к СФЗ предъявляется всего одно существенное требование - СФЗ должна быть эффективна относительно стоящих перед ней задач. Причем, под “эффективностью” следует понимать: оптимальность тактических характеристик противодействия основным угрозам, стратегическое влияние на снижение уровня глобальных рисков, сбалансированность экономических показателей системы. По всем указанным составляющим должна быть обеспечена как “проектируемая эффективность” (заложенная на этапе разработки СФЗ), так и “реальная эффективность” (достигаемая в процессе эксплуатации СФЗ).

Таким образом, для достижения основных целей создания СФЗ необходима система, регламентирующая основные процессы разработки, внедрения и эксплуатации СФЗ по основным критериям обеспечения эффективности. В противном случае целесообразность создания определенной модели СФЗ не может быть объективно обоснована. Когда речь идет о группе однотипных объектов, об объектах, принадлежащих единой производственной цепочке, либо о группе объектов одного предприятия, роль такой регламентирующей системы должна взять на себя Концепция Физической Защиты (КФЗ).

Осознавая необходимость концептуального подхода к решению проблем безопасности, многие крупные промышленные и коммерческие предприятия, группы и холдинги, самостоятельно, либо с привлечением специализированных организаций разрабатывают собственные Концепции безопасности.

При этом необходимо четко понимать, что разработка корпоративной Концепции является важнейшим, базовым моментом в обеспечении безопасности объектов предприятия. Любые ошибки, недочеты, пробелы Концепции, отсутствие в ней необходимых элементов, просчеты в организации процессов ее реализации будут негативным образом влиять на глобальное пространство рисков деятельности предприятия. В то же время, каких либо требований к концептуальным разработкам, их составу и содержанию практически не существует, не говоря уже о методах их оценки. Подобная ситуация чревата серьезными опасностями для предприятий, делающих абсолютно верный шаг в направлении корпоративной Концепции безопасности. Приведем несколько примеров:

Наиболее далеко в деле концептуальных разработок по физической защите объектов продвинулись зарубежные и отечественные институты и организации, работающие над проблемами обеспечения безопасности военных и ядерноопасных объектов, то есть, “объектов особой важности” (ООВ).

Зачастую подобные разработки ложатся в основу корпоративных концепций безопасности. При этом не учитывается, что базовым принципом КФЗ ООВ является “защита любой ценой”. Другими словами, задачей разработчика является определение необходимой конфигурации и состава СФЗ, которые с высокой степенью вероятности смогут противостоять анализируемым угрозам.

При формировании СФЗ эти требования должны быть выполнены. В случае корпоративной концепции ситуация иная. Основная группа угроз требует абсолютно другого подхода - оптимизации мер противодействия по критериям экономической целесообразности.

В то же время, существует группа угроз, требующая того же подхода, что и угрозы ООВ - “защита любой ценой”. Однако и здесь есть отличия - корпорация, в отличие от государства, может просто не располагать необходимыми возможностями для нейтрализации определенных угроз. Концепция должна предлагать иные варианты решения, помимо силового. Далее. Основные угрозы ООВ - внешние и комбинированные. Основные угрозы большинства корпораций - внутренние. Соответственно, если в первом случае акцент в построении СФЗ делается на системы обнаружения и силы физического реагирования, то во втором на первый план выходят системы контроля, детективно-аналитические и психологические методы в работе службы безопасности.

Как правило, концепции безопасности носят характер предписания - для обеспечения безопасности объекта следует реализовать то-то и то-то (определенную систему, схему организации охраны). Данный путь несет в себе ряд скрытых опасностей. Во-первых, подобный подход не позволяет в должной мере учесть индивидуальные особенности каждого отдельного объекта корпорации (типового объекта). Далее. После внедрения рекомендованных мер, само пространство угроз изменится, соответственно, “ответ” будет дан на “вопрос”, который уже не актуален, благодаря появлению “ответа”. Более того, в современном мире на уровне корпорации предсказать динамику изменения пространства угроз во времени практически невозможно. Таким образом, оценить период эффективной дееспособности предписываемых мер до момента их морального устаревания невозможно, хотя на практике корпоративные концепции безопасности “принимаются на вооружение” на значительные сроки - 10 лет и более.

Большинство корпоративных концепций безопасности не устанавливают четких однозначных требований к результатам внедрения предписываемых мер защиты, к организации внутренних и внешних информационных взаимодействий элементов СФЗ, не регламентируют основные процессы проектирования, внедрения и эксплуатации СФЗ по критериям необходимого уровня качества. Встречаются концепции, выставляющие определенные требования к мерам защиты вообще без анализа пространства угроз объекта. Очевидно, что такие подходы не могут дать четкого ответа на основной вопрос - “Какова будет эффективность внедрения предписываемых мер?”, что дискредитирует саму идею концептуального подхода к обеспечению безопасности.

В основе Корпоративной КФЗ должна лежать система (методика) анализа пространства угроз. Все меры защиты должны базироваться на результатах данного анализа. Построение эффективного комплекса защитных мер возможно только относительно определенного, характерного пространства угроз.

Корпоративная КФЗ должна базироваться на принципе классификации угроз по двум основополагающим категориям - материальные и нематериальные угрозы. Принципы и подходы к снижению нематериальной и материальной составляющей рисков принципиально различны. Методы противодействия угрозам материального характера оптимизируются по критериям экономической эффективности. Методы противодействия угрозам нематериального характера организуются по принципу “защита любой ценой в пределах имеющихся возможностей”. При очевидной недостаточности возможностей должны быть разработаны альтернативные варианты защиты. Таким образом, при выработке комплекса мер противодействия, каждая угроза должна быть изначально классифицирована по принципу разделения нематериальной и материальной составляющих.

Как уже отмечалось, основная часть пространства угроз Корпорации требует оптимизации мер защиты по критериям экономической эффективности, что требует учета финансово-экономических аспектов и аспектов страховой защиты. Преимущества комплексного подхода к обеспечению безопасности можно принять как аксиому. Таким образом, Корпоративная КФЗ должна рассматриваться не как отдельная, замкнутая система, а как часть Глобальной Концепции безопасности Корпорации. Глобальная Концепция безопасности должна включать также концепции экономической безопасности, информационной защиты, страховой защиты, защитных организационных мероприятий. Основой концепции глобальной безопасности должна стать технология управления рисками.

Корпоративная КФЗ должна содержать раздел, описывающий основные Концептуальные принципы и подходы к обеспечению безопасности объектов. Следование концептуальным принципам является важнейшим залогом создания эффективного комплекса мер защиты.

## 2.2 Концептуальные принципы обеспечения и планирования физической безопасности объектов являются

Основными концептуальными принципами обеспечения физической безопасности объектов являются:

* Приоритет превентивного подхода к обеспечению безопасности
* Принцип адекватности мер защиты пространству угроз
* Принципы адаптивности
  + Принцип долгосрочной адаптивности
  + Принцип краткосрочной адаптивности
* Принципы зональной (эшелонированной) защиты
  + Принцип концентрического построения рубежей вокруг целей защиты
  + Принцип концентрического усиления прочности рубежей
  + Принцип раннего обнаружения
  + Принцип распределения характеристик вдоль рубежа защиты
  + Принцип определения места расположения поста охраны

Принципы зональной защиты иллюстрирует диаграмма 1.

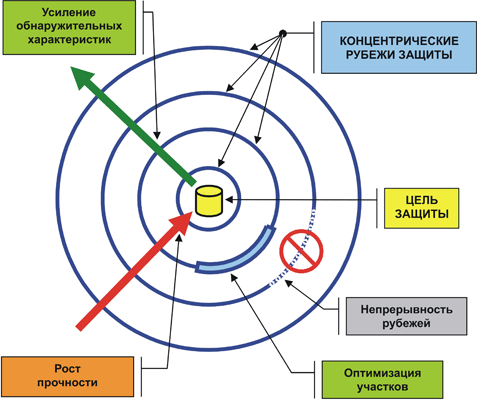


Диаграмма 1. Принципы зональной защиты

* Принципы постоянства уровня эффективности во времени
  + Принцип постоянства эффективности
  + Принцип тактической надежности (живучести)
  + Принцип самоконтроля эффективности СФЗ
* Принцип баланса превентивных и обнаружительных свойств СФЗ
* Принцип оптимизации синергетического взаимодействия
* Принцип приоритета применения комплексов ТСО, СИУ и САЗ
* Принцип необходимо достаточного уровня блокирующих свойств СФЗ
* Принципы оптимизации взаимодействий элементов СФЗ
* Принцип самоадаптации концептуальных подходов

Существует риск морального, тактического и технического устаревания любых, сколь бы то ни было грамотных и взвешенных решений. В сфере обеспечения безопасности, где идет постоянная “война” интеллектов и технологий между нарушителями и силами охраны, этот тезис дополняется риском утечки информации. Таким образом, любые, пусть самые современные и продуманные сегодня решения завтра могут оказаться малоэффективными.

По данной причине корпоративная КФЗ должна определять комплекс основных мер по обеспечению безопасности, на основании создания единого саморегулирующегося механизма. В основе данного механизма должна лежать внутрикорпоративная система нормативных документов, имеющих форму процессных стандартов качества.

Под термином “процессные стандарты качества” понимаются стандарты, устанавливающие требования к организации тех или иных процессов, процедур, к качеству их проведения и к конечным результатам.

Данный подход позволяет придать КФЗ вневременной, самоадаптирующийся под изменяющиеся во времени параметры пространства угроз, характер.

На основании процессных стандартов качества, корпоративная КФЗ регламентирует следующие основные процессы в обеспечении безопасности:

* Анализ предприятия и ее объектов с точки зрения основных подходов к обеспечению безопасности. На основании анализа формируются основные выводы.
* Категорирование угроз и моделей потенциальных нарушителей.
* Категорирование объектов как объектов охраны по критериям значимости, топологии и степени характерных рисков. Установление целевых показателей защищенности.
* Анализ угроз объекта, в том числе: идентификация угроз, выявление целей защиты на объекте, выявление наиболее опасных участков и направлений, сценарный анализ тактик нарушителей, выявление факторов мотивации и демотивации. Формирование результатов анализа, как целеполагающей системы условий для задачи построения комплекса мер противодействия.
* Анализ уязвимости объектов и оценки эффективности СФЗ по тактическим и экономическим критериям, в том числе, количественная оценка критерия “эффективность / стоимость”.
* Концептуальное проектирование СФЗ типовых и / или конкретных объектов, включая: анализ пространства угроз; выбор адекватных мер защиты; анализ их эффективности; оптимизацию по тактическим и экономическим критериям. Результатами концептуального проектирования являются:
  + набор требований к характеристикам СФЗ объекта, включая требования к организации охраны, построению комплексов ТСО, СИУ и САЗ;
  + система организационных мероприятий, обеспечивающих достижение заданных параметров;
  + прогноз изменения пространства угроз после внедрения предлагаемой СФЗ, анализ возможных негативных последствий и путей их снижения;
  + форвардная оценка стоимости внедрения и эксплуатации СФЗ.
* Тактическое проектирование СФЗ конкретных объектов. Тактическое проектирование производится при необходимости адаптации результатов концептуального проектирования под условия конкретного объекта. Результатом тактического проектирования является разработка технико-экономического обоснования, технического задания на СФЗ.
* Внедрение комплексов ИТСО и САЗ, включая циклы: рабочего проектирования, выбора подрядных организаций, поставки оборудования, проведения монтажно-наладочных работ и приемо-сдаточных испытаний, обеспечения надлежащего качества и гарантий.
* Организация физической охраны объектов, действий групп немедленного реагирования, взаимодействия с силовыми ведомствами. Работа с персоналом службы охраны. Взаимодействие с внешними организациями.
* Эксплуатация СФЗ. Организация эффективного взаимодействия между силами охраны, комплексами ТСО, СИУ и САЗ. Мониторинг эффективности СФЗ. Техническое обслуживание систем ТСО и САЗ.
* Организация мероприятий превентивного характера, работы детективно-аналитического отдела службы безопасности.

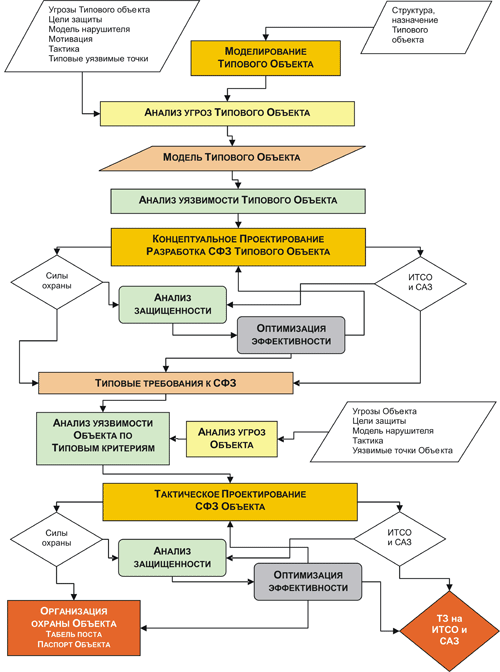


Диаграмма 2. Концепция физической защиты

* Перманентный мониторинг и анализ “среды безопасности объекта” с целью модифицирования и актуализации самой КФЗ относительно текущего момента времени, включая: внешнее и внутреннее пространство рисков объекта; современные методы и средства, применяемые злоумышленниками; рынок средств и услуг обеспечения безопасности; правовую и нормативную базу, регулирующую правоотношения в сфере обеспечения безопасности объектов предприятия.

Результатом внедрения корпоративной КФЗ, как продуманной и сбалансированной системы защиты, должен стать качественный рост уровня защищенности объектов промышленного и коммерческого назначения от основных характерных угроз, глобальное снижение уровня рисков деятельности предприятия.

# Глава 3. Организация физической безопасности как составной части комплексной безопасности на примере Балаковской АЭС

## 

## 3.1 Характеристика деятельности Балаковской АЭС

История Балаковской АЭС — крупнейшего производителя электроэнергии в России — уходит в 70-е годы, когда в Поволжье начались работы по выбору территории для будущей мощной атомной станции, первоначально именовавшейся Приволжской. Необходимость в строительстве АЭС диктовалась обозначившимся в регионе дефицитом электроэнергии, что было обусловлено интенсивным ростом промышленности.

Технико-экономическое обоснование строительства будущей АЭС по заданию Минэнерго СССР выполняло Уральское отделение института «Теплоэлектропроект». Размещение станции прорабатывалось на территории объединенной энергосистемы Среднего Поволжья. Площадка выбиралась с учетом таких факторов, как необходимость покрытия дефицита электроэнергии в регионе Средней Волги и в центре России, приемлемые гидрогеологические и сейсмические условия, отсутствие смерчей.

Приказом Минэнерго № 6р от 13 января 1977 года, подписанным заместителем министра П.П. Фалалеевым, была создана Государственная межведомственная комиссия для выбора площадки строительства АЭС в Саратовской области. Ее председателем назначили заместителя начальника Главатомэнерго В.Н. Кондратенко. В конце января комиссия, рассмотрев материалы, подготовленные Уральским отделением института «Теплоэлектропроект», и побывав на месте, подписала акт, которым определила площадку возле села Натальино Балаковского района в качестве места будущего строительства. Данный акт 26 марта 1977 г. согласовал председатель исполкома Саратовского областного Совета депутатов трудящихся Н. С. Александров, а утвердил 12 мая того же года министр энергетики и электрификации СССР П.С. Непорожний.

Выбор места строительства Балаковской АЭС осуществлялся в полном соответствии с действовавшим тогда законодательством, строительными и санитарными нормами и правилами. Главный государственный санитарный врач СССР А.И. Бурназян согласовал размещение АЭС мощностью 4-6 млн. кВт в районе г. Балаково при условии обеспечения расстояния между атомной станцией и границей застройки города не менее 8 км. Это требование было соблюдено.

Сам город Балаково — второй по значению промышленный центр Саратовской области — расположен на левом берегу Волги, на границе Среднего и Нижнего Поволжья, в 180 км от г. Саратова и 260 км от г. Самары. Первое промышленное предприятие Балакова — специальный завод нефтяных двигателей братьев Маминых (впоследствии машиностроительный завод имени Ф.Э. Дзержинского, затем «Волгодизельмаш») — было основано еще в 1899 году. Однако бурное промышленное строительство в Балакове началось только в 50-е годы прошлого века. Именно с этим связано и развитие самого города. В 60-80-е годы население Балакова увеличилось на 180 тысяч человек (в настоящее время оно превышает 200 тыс. человек). Благодаря пяти Всесоюзным стройкам в Балакове создан крупный индустриальный комплекс, насчитывающий более двух десятков предприятий химии, машиностроения, энергетики, промышленного и жилищного строительства. Среди крупнейших предприятий, уже существовавших к моменту начала строительства АЭС, следует отметить Саратовскую ГЭС, производственные объединения «Балаковское химволокно», «Балаковорезинотехника», «Балаковские минеральные удобрения», управление «Саратовгэсстрой».

В соответствии с указанием Минэнерго № Ф-9520 от 1 августа 1977 г. Главниипроект, институт «Теплоэлектропроект» и его Уральское отделение приступили к разработке рабочих чертежей для подготовительного этапа строительства АЭС. Дирекция строящейся Приволжской атомной станции с местом нахождения в г. Балаково была создана приказом Минэнерго 26 октября 1977 г. Директором строящейся станции 15 ноября 1977 г. был назначен Д.Т. Шутюк.

Официально строящаяся АЭС стала называться Балаковской только летом 1978 года — после того, как министр П. С. Непорожний подписал 19 июня соответствующий приказ.

Балаковская АЭС расположена в 8 км от города Балаково Саратовской области, на левом берегу Саратовского водохранилища. Она является филиалом ОАО «Концерн Росэнергоатом».

Балаковская АЭС – крупнейший в России производитель электроэнергии. Ежегодно она вырабатывает более 30 миллиардов кВт. час электроэнергии (больше, чем любая другая атомная, тепловая и гидроэлектростанция страны). Она обеспечивает четверть производства электроэнергии в Приволжском федеральном округе и пятую часть выработки всех атомных станций страны. Ее электроэнергией надежно обеспечиваются потребители Поволжья (76 % поставляемой ею электроэнергии), Центра (13 %), Урала (8 %) и Сибири (3 %). Коэффициент использования установленной мощности (КИУМ) на Балаковской АЭС составляет около 90 процентов (в 2009 г. – 89,32 %).

Пуски блоков состоялись:

• первого – 28 декабря 1985 г.,

• второго – 10 октября 1987 г.,

• третьего – 28 декабря 1988 г.,

• четвертого – 12 мая 1993 г.

Четвертый энергоблок Балаковской АЭС стал первым российским энергоблоком, пущенным в эксплуатацию после распада СССР.

На станции трудятся около 4 000 человек, более 60 % из которых имеют высшее и среднее профессиональное образование.

Балаковская АЭС – признанный лидер атомной энергетики России – неоднократно удостаивалась почетных званий и наград:

– «Лучшая АЭС России» по итогам работы в 1995, 1999, 2000, 2003, 2005, 2006, 2007, 2008 и 2009 гг.;

– лауреат XIV Международного конкурса «Золотая медаль «Европейское качество» в 2008 г.;

– победитель Всероссийских конкурсов «Российская организация высокой социальной эффективности» в 2001, 2004, 2005, 2006 и 2007 годах;

– лучшая станция в области культуры безопасности по результатам работы концерна «Росэнергоатом» в области соблюдения принципов культуры безопасности – 2006, 2007 и 2009 годы;

– почетное звание «Лидер природоохранной деятельности в России» по итогам 2007, 2008, 2009 годов.

Главным в деятельности руководства АЭС является обеспечение и повышение безопасности при эксплуатации, защита окружающей среды от влияния технологического процесса, снижение издержек при производстве электроэнергии, улучшение социальной защищенности персонала, увеличение вклада станции в социально-экономическое развитие региона.

## 3.2 Организация производства на предприятии

Компоновка и расположение энергоблоков.

Каждый из унифицированных энергоблоков Балаковской АЭС представляет собой отдельно расположенное сооружение, состоящее из реакторного отделения, машинного зала, деаэраторной этажерки и помещения электротехнических устройств. Все, что относится к первому, радиоактивному контуру, располагается вместе с реактором в герметичной железобетонной оболочке, облицованной изнутри стальным листом — контейнменте.

Главные корпуса энергоблоков ориентированы к водоему-охладителю — источнику циркуляционного водоснабжения АЭС. Между водоемом-охладителем и главными корпусами энергоблоков размещены блочные насосные станции, трубопроводы технического водоснабжения и дороги. Общая площадь, занимаемая сооружениями Балаковской АЭС, составляет 487,4 га.

Технологическая схема энергоблоков.

Тепловая схема каждого блока Балаковской АЭС двухконтурная. Первый контур — радиоактивный. Он состоит из одного водо-водяного энергетического реактора ВВЭР-1000 тепловой мощностью 3000 МВт и четырех циркуляционных петель охлаждения.

Теплоносителем и одновременно замедлителем нейтронов служит обыкновенная вода с некоторым содержанием бора. Вода первого контура прокачивается главными циркуляционными насосами через активную зону реактора и нагревается.

Давление воды в корпусе реактора составляет 16 МПа (160 атмосфер), и ее кипения не происходит.

Температура воды на входе в реактор равна 289°С, а на выходе из реактора 320°С.

Циркуляционный расход воды через реактор 84000 т/ч. Нагретая в реакторе вода направляется по четырем трубопроводам в парогенераторы. Давление и уровень теплоносителя первого контура поддерживаются при помощи парового компенсатора давления, подключенного к общей части контура.

Второй контур — нерадиоактивный. Он состоит из испарительной и водопитательной установок, блочной обессоливающей установки и турбоагрегата электрической мощностью 1000 МВт. Предусмотрена эффективная система регенерации питательной воды.

Теплоноситель первого контура охлаждается в парогенераторах и отдает тепло воде второго контура. Насыщенный пар, производимый в парогенераторе, под давлением 6,4 МПа (64 атмосферы) подается в сборный паропровод и направляется к турбоустановке, приводящей во вращение электрогенератор. Кроме того, второй контур включает в себя конденсатные насосы первой и второй ступеней, подогреватели высокого и низкого давления, деаэратор, турбопитательные насосы.

Энергоблок выполнен с полной автоматизацией контроля и управления технологическими процессами.

Таблица 1

**Основные технические характеристики энергоблоков Балаковской АЭС**

Энергоблоки(4 унифицированных блока, введены в эксплуатацию в 1985-1993гг.)

|  |  |
| --- | --- |
| Электрическая мощность энергоблока, МВт | 1000 |
| Тепловая мощность, МВт | 3000 |
| КПД, % | 33 |
| Количество циркуляционных петель (насосов, парогенераторов), шт | 4 |
| Расход теплоносителя через реактор, м 3/ч | 84000 |
| Рабочее давление теплоносителя, МПа (атмосфер) | 16 (160) |
| **Реактор (водо-водяной энергетический ВВЭР-1000 проекта В-320)** |  |
| Максимальная температура теплоносителя на входе в реактор, оС | 289 |
| Средний подогрев телоносителя, оС | 30,3 |
| Масса диоксида урана в активной зоне, т | 80 |
| Количество топливных сборок, шт | 163 |
| Количество органов механической системы регулирования реактивности реактора, шт | 61 |
| Высота корпуса реактора (без верхнего блока), м | 10,89 |
| Максимальный диаметр корпуса, м | 4,58 |
| Внутренний диаметр главных циркуляционных трубопроводов, мм | 850 |
| Обогащение топлива (макс), % | 3,3 |
| **Парогенератор (горизонтального расположения)** |  |
| Производительность, т/ч | 1470 |
| **Турбогенератор** |  |
| Давление насыщенного пара перед турбиной, МПа (атмосфер) | 6 (60) |
| Давление в конденсаторе турбины, МПа | 0,004 |
| Мощность электрического генератора, МВт | 1000 |
| Напряжение на клеммах, В | 24000 |

Реакторная установка.

На Балаковской АЭС используются реакторные установки типа ВВЭР-1000 конструкции ОКБ "Гидропресс", изготовленные ПО «Ижорский завод» и ПО "Атоммаш".

Конструкция реакторной установки предусматривает:

- автоматическую остановку реактора при отклонениях параметров выше допустимых в работе основного оборудования;

- трехканальное построение систем безопасности, каждая из которых функционирует независимо и автономно с полным обеспечением всех функций;

- наличие герметичной оболочки, в которой расположено все реакторное оборудование (эта оболочка рассчитана на удержание радиоактивных веществ, которые теоретически могут выделиться при разгерметизации первого контура);

- способность реакторной установки к саморегуляции (т.е. при повышении параметров активной зоны происходит самопроизвольное снижение интенсивности цепной реакции).

Реактор состоит из корпуса, верхнего блока, приводов и органов регулирования системы управления и защиты, внутрикорпусных устройств и активной зоны.

Реактор конструктивно представляет собой вертикальный цилиндрический сосуд, выполненный из высокопрочной теплоустойчивой хромомолибденовой стали с нержавеющей наплавкой (плакировкой).

Активная зона реактора помещена в корпус и собрана из шестигранных тепловыделяющих сборок (ТВС), содержащих тепловыделяющие элементы (ТВЭЛ) стержневого типа с сердечником из диоксида урана в виде таблеток, находящихся в оболочке из циркониевого сплава.

Нижние цилиндрические части ТВС входят в отверстия в днище внутри корпусной шахты реактора, верхние — в дистанционирующую прижимную решетку защитных труб. В верхней части корпуса имеются два ряда патрубков.

Через 4 нижних патрубка вода (теплоноситель) поступает в реактор, опускается по кольцевому зазору в нижний смесительный объем, проходит снизу вверх через активную зону, нагревается за счет тепла ядерной реакции и, охлаждая тепловыделяющие элементы, выходит из реактора через верхний ряд патрубков.

Внутри реактора находится цилиндрическая шахта, предназначенная для размещения в ней активной зоны и организации потока теплоносителя. Над активной зоной расположен блок защитных труб, который обеспечивает дистанционирование топливных кассет активной зоны и удерживает кассеты от всплытия.

На блоке смонтированы каналы для установки датчиков контроля температуры воды на выходе из кассет и приборов для замера нейтронного потока по высоте активной зоны.

Для создания замкнутого объема в реакторе и размещения приводов системы управления и защиты на корпусе реактора устанавливается верхний блок.

Реактор установлен в бетонной шахте, обеспечивающей надежное крепление реактора и биологическую защиту.

Конструкция реактора и способ его закрепления, а также системы управления и защиты (СУЗ) и аварийного охлаждения зоны (САОЗ) обеспечивают безопасную остановку и расхолаживание реактора, в том числе при максимальном расчетном землетрясении.

Турбина.

Второй контур включает паровую турбину, конденсатные насосы первой и второй ступеней, подогреватели высокого и низкого давления, деаэратор, турбопитательные насосы, блочную обессоливающую установку.

Насыщенный пар, производимый в парогенераторах, под давлением 6 Мпа (60 атмосфер) с температурой 274,3°С подается в паровую конденсационную одновальную четырехцилиндровую (ЦВД + 3 ЦНД) турбину К-1000-60/1500-2 с номинальной мощностью 1030МВт и частотой вращения 25 Гц (1500 об/мин). Турбина является приводом электрического генератора переменного тока типа ТВВ-1000-4 мощностью 1000МВт, напряжением 24000В.

## 3.3 Политика в области физической безопасности Балаковской АЭС

Руководство филиала ОАО «Концерн Росэнергоатом» «Балаковская атомная станция» заявляет, что безопасность АС на всех этапах жизненного цикла пользуется самым высоким приоритетом, превосходящим, при необходимости, факторы производства электроэнергии и соблюдения графика работ.

Ответственность за проведение политики в области безопасности и организацию системы обеспечения безопасности несёт директор Балаковской АЭС.

Безопасность АЭС – это свойство АС ограничивать радиационное воздействие на персонал, население и окружающую среду установленными пределами при нормальной эксплуатации и нарушениях нормальной эксплуатации, включая аварии.

Безопасность АС должна обеспечиваться за счёт реализации концепции глубоко эшелонированной защиты, основанной на применении:

1. системы физических барьеров на пути распространения ионизирующего излучения и радиоактивных веществ в окружающую среду;

2. системы технических и организационных мер по защите барьеров и сохранению их эффективности, а также по защите персонала, населения и окружающей среды.

Основные цели обеспечения безопасности на всех этапах жизненного цикла АС:

1. защитить отдельные лица, общество и окружающую среду от радиологической опасности;

2. обеспечить такой уровень эксплуатации, чтобы дозы облучения персонала на АС находились ниже установленных пределов;

3. предотвратить аварии на атомной станции и обеспечить, чтобы вероятность больших радиологических последствий тяжёлых аварий была чрезвычайно мала.

Основные задачи обеспечения безопасности:

1. эксплуатация АС в соответствии с требованиями нормативных документов, технологических регламентов и инструкций по эксплуатации;

2. поддержание в исправном состоянии систем, оборудования, путём своевременного выявления дефектов, принятия профилактических мер, замены выработавшего ресурс оборудования;

3. обеспечение требуемого качества систем АС и выполняемых работ;

4. подбор персонала и обеспечение необходимого уровня квалификации персонала;

5. формирование культуры безопасности, которая должна обеспечиваться:

а) структурой управления и контроля деятельности по безопасной эксплуатации АС;

б) высоким уровнем ответственности персонала при выполнении им своих обязанностей.

6. выявление отклонений от нормальной эксплуатации и их устранение;

7. предотвращение, с применением систем безопасности; перерастания отклонений в работе в проектные аварии, а проектных аварий в запроектные.

8. подготовка и осуществление, при необходимости, планов противоаварийных мероприятий на площадке АС и за её пределами;

9. использование внешнего и внутреннего опыта эксплуатации;

10. проведение регулярной работы по самооценке эксплуатационной безопасности Руководство Балаковской АЭС гарантирует, что любые инициативы работников АС, направленные на обеспечение и повышение безопасности в рамках заявленной политики, будут поддержаны руководством и по достоинству оценены.

## 3.4 Требования к системам и органам управления обеспечения физической безопасности предприятия

Для выполнения задач физической защиты на каждом ядерном объекте должно быть проведено категорирование:

- предметов физической защиты;

- помещений, в которых размещаются предметы физической защиты, а также зданий, сооружений, отдельных территорий ядерного объекта, на которых используется или хранится ядерный материал либо размещается и (или) эксплуатируется ядерная установка или пункт хранения (далее - промышленные площадки);

- ядерного объекта.

Категорирование предметов физической защиты, помещений (при необходимости зданий, сооружений, промышленных площадок) и ядерного объекта используется для разработки требований к системе физической защиты и обеспечения ее адекватности угрозам и моделям нарушителей.

В качестве показателей категорирования предметов физической защиты должны рассматриваться:

- категория ядерных материалов;

- степень секретности предметов физической защиты;

- категория последствий несанкционированных действий в отношении предметов физической защиты;

- наличие значимого количества ядерного материала прямого использования.

Категория ядерных материалов должна определяться видом, содержанием изотопов, степенью облучения и массой ядерных материалов согласно приложению N 1 к "Правилам физической защиты ядерных материалов, ядерных установок и пунктов хранения ядерных материалов".

Категории последствий несанкционированных действий в отношении предметов физической защиты должны определяться согласно приложению N 2 к "Правилам физической защиты ядерных материалов, ядерных установок и пунктов хранения ядерных материалов".

Результатом категорирования предметов физической защиты, помещений, зданий, сооружений, промышленных площадок и ядерного объекта должно быть отнесение их к одной из категорий.

Требования к размещению предметов физической защиты в соответствующих охраняемых зонах и зонах ограниченного доступа должны определяться согласно приложению № 3 к "Правилам физической защиты ядерных материалов, ядерных установок и пунктов хранения ядерных материалов".

На ядерном объекте должно быть проведено категорирование помещений, в которых размещаются предметы физической защиты (при необходимости категорирование зданий, сооружений, промышленных площадок). Категория помещения, здания, сооружения и промышленной площадки должна определяться исходя из максимальной категории находящихся в них отдельных ядерных материалов, ядерных материалов, входящих в состав ядерных установок, с учетом степени их секретности и последствий несанкционированных действий в отношении предметов физической защиты.

Результаты категорирования предметов физической защиты, помещений, зданий, сооружений, промышленных площадок и отнесение их к охраняемым зонам должны оформляться отдельным документом.

С учетом категории предметов физической защиты устанавливаются следующие категории ядерных объектов:

- I категория - ядерные объекты, на которых имеются предметы физической защиты категории А;

- II категория - ядерные объекты, не отнесенные к I категории, на которых имеются предметы физической защиты категории Б;

- III категория - ядерные объекты, не отнесенные к I и II категориям, на которых имеются предметы физической защиты категории В или Г;

- IV категория - ядерные объекты, не отнесенные к I - III категориям, на которых имеются предметы физической защиты категории Д.

Порядок создания, совершенствования и функционирования системы физической защиты.

При создании (совершенствовании) системы физической защиты необходимо:

а) учитывать особенности ядерного объекта и действующие на нем меры ядерной, радиационной, экологической, пожарной, технической безопасности, безопасности информации и безопасности иных видов;

б) ограничивать число лиц, имеющих доступ к предметам физической защиты, к элементам и системам, важным для обеспечения безопасности ядерного объекта или его системы физической защиты, к информации об организации, составе и функционировании системы физической защиты;

в) обеспечивать соответствие системы физической защиты требованиям, установленным к ядерному объекту;

г) устанавливать требования к организационно-техническим мерам по обеспечению физической защиты в зависимости от категории предметов физической защиты.

В целях обеспечения физической защиты должны приниматься меры по защите информации об организации и функционировании системы физической защиты, определяемые в соответствии с федеральными и ведомственными нормативными актами.

Технические и программные средства систем физической защиты, используемые при обработке информации, составляющей государственную и служебную тайны, подлежат обязательной сертификации на соответствие требованиям безопасности информации, а созданные и реконструированные системы физической защиты подлежат аттестации по требованиям безопасности информации.

Этапы и конкретные работы по созданию (совершенствованию) системы физической защиты должны устанавливаться в техническом задании на создание (совершенствование) системы физической защиты (в частных технических заданиях).

Предпроектная стадия.

Создание (совершенствование) системы физической защиты должно проводиться на основе результатов анализа уязвимости ядерного объекта и оценки эффективности системы физической защиты.

При создании (совершенствовании) системы физической защиты должны учитываться категории предметов физической защиты, помещений, зданий, сооружений и промышленных площадок, а также особенности расположения и функционирования ядерных установок и пунктов хранения.

На этапе концептуального проектирования системы физической защиты в качестве исходных данных должны использоваться материалы анализа уязвимости и категорирования помещений, зданий, сооружений и промышленных площадок.

На этом этапе проводятся предпроектное обследование ядерного объекта и системы физической защиты, разработка и выбор варианта построения системы физической защиты на основе оценок эффективности и стоимости различных вариантов системы физической защиты.

Техническое задание на создание (совершенствование) системы физической защиты должно разрабатываться с целью формирования и детализации требований к системе физической защиты на основе результатов концептуального проектирования, а также определения состава, содержания и порядка работ по вводу в действие системы физической защиты.

Техническое задание на разработку проектной документации составляется на основе исходных данных и результатов предпроектной стадии создания (совершенствования) системы физической защиты и должно содержать требования к разработке обоснования инвестиций и проектной документации на систему физической защиты при строительстве, реконструкции, техническом перевооружении ядерного объекта, а также к разработке обоснования инвестиций и проектной документации при реконструкции и техническом перевооружении системы физической защиты на действующем ядерном объекте.

Технические задания на проектирование и проекты комплексов ИТСФЗ подлежат согласованию с вышестоящими организациями подразделений охраны в части, касающейся инженерно-технических средств, используемых для охраны ядерных объектов.

Стадия проектирования.

Проектные работы по созданию системы физической защиты осуществляются при строительстве новых ядерных установок и пунктов хранения, а на действующих ядерных установках, в пунктах хранения осуществляется совершенствование (реконструкция, техническое перевооружение) системы физической защиты.

При строительстве новых ядерных установок и пунктов хранения должна разрабатываться проектная документация на систему физической защиты и включаться отдельным разделом в проектную документацию на их строительство.

При реконструкции, техническом перевооружении только системы физической защиты должно разрабатываться технико-экономическое обоснование (проект) системы физической защиты, или рабочий проект (утверждаемая часть и рабочая документация), или рабочая документация.

Проектные, технические и организационные решения по системе физической защиты ядерных установок, пунктов хранения должны разрабатываться на основании требований, норм и правил, а также с использованием типовых проектных решений.

Стадия ввода в действие системы физической защиты.

Стадия ввода в действие системы физической защиты должна включать:

- организационные мероприятия, в том числе подготовку ядерного объекта и персонала физической защиты к вводу в действие системы физической защиты, организацию комплекса режимных, инженерно-технических и иных мероприятий, проводимых силами и средствами подразделений охраны при непосредственном участии руководства ядерных объектов и других взаимодействующих органов с целью недопущения несанкционированного проникновения нарушителей на ядерный объект и их нейтрализации (далее - охрана), разработку объектовых документов по физической защите, организацию контроля;

- оборудование ядерного объекта совокупностью инженерных и технических средств, предназначенных для решения задач физической защиты (далее - ИТСФЗ), в том числе комплектование, строительно-монтажные и пусконаладочные работы;

- испытания и приемку в эксплуатацию комплекса ИТСФЗ;

- аттестацию по требованиям безопасности информации и приемку системы физической защиты приемочными комиссиями.

При усовершенствовании отдельных элементов действующей системы физической защиты допускается не проводить приемку системы физической защиты.

Оценка эффективности системы физической защиты.

Качество создания и функционирования системы физической защиты должно подтверждаться оценкой ее эффективности.

Эффективность системы физической защиты должна оцениваться экспериментально (на учениях), аналитически или с помощью моделирования на различных стадиях и этапах создания системы физической защиты, а также в процессе ее функционирования. Оценка эффективности системы физической защиты должна использоваться для определения путей ее совершенствования.

Для каждого ядерного объекта должно быть установлено минимально допустимое значение показателя эффективности системы физической защиты.

Оценка эффективности системы физической защиты на ядерном объекте должна проводиться периодически.

При изменении угроз и моделей нарушителей, изменении технологических процессов использования и хранения ядерных материалов должна быть проведена оценка эффективности системы физической защиты.

Требования к системе физической защиты на ядерном объекте.

Общие требования к системе физической защиты.

Функционирование системы физической защиты должно быть обеспечено к моменту поставки ядерных материалов на ядерный объект.

На этапе вывода из эксплуатации ядерной установки, пункта хранения должно быть обеспечено функционирование системы физической защиты до изъятия ядерных материалов из ядерной установки, пункта хранения.

Система физической защиты должна выполнять задачи в штатных ситуациях и в состояниях ядерного объекта, при которых в результате несанкционированного действия на нем нарушаются нормальные условия его работы, возможно нанесение ущерба здоровью персонала (населения), возникает угроза жизни персонала (населения), а также возможно нанесение ущерба окружающей среде (далее - чрезвычайные ситуации).

В системе физической защиты должна быть обеспечена защита информации, в том числе секретность (конфиденциальность) информации об организации, составе и функционировании системы физической защиты, ее целостность и санкционированная доступность, нарушение которых может приводить к снижению эффективности функционирования системы физической защиты в целом или ее отдельных элементов.

На ядерном объекте должна быть обеспечена защита не относящихся к ядерной установке или пункту хранения систем, элементов и коммуникаций ядерного объекта, в отношении которых в процессе анализа уязвимости выявлена необходимость предотвращения несанкционированных действий.

В исключительных случаях при невозможности выполнения в полном объеме требований к системе физической защиты на ядерном объекте, установленных настоящими федеральными нормами и правилами, должны быть приняты компенсирующие организационно-технические меры. Достаточность принятых мер должна подтверждаться оценкой эффективности системы физической защиты.

Требования к составным частям системы физической защиты.

Требования к организационным мероприятиям системы физической защиты.

Организационные мероприятия системы физической защиты должны включать в себя комплекс мер на всех этапах создания (совершенствования) и функционирования системы физической защиты и регламентирующие эти меры нормативные документы по вопросам организации и функционирования системы физической защиты.

Комплекс мер, проводимых на стадиях создания (совершенствования) системы физической защиты, установлен в разделе 4 настоящих федеральных норм и правил.

Комплекс мер по обеспечению функционирования системы физической защиты должен предусматривать:

- управление функционированием системы физической защиты, в том числе планирование работ, организацию взаимодействия, объектовый контроль за состоянием системы физической защиты;

- организацию допуска и доступа лиц к ядерным материалам, ядерным установкам, пунктам хранения и информации о функционировании системы физической защиты;

- организацию пропускного и внутриобъектового режимов;

- защиту циркулирующей информации в системе физической защиты;

- проведение аналитической работы, в том числе анализ уязвимости ядерного объекта, оценку эффективности системы физической защиты и подготовку предложений по ее совершенствованию.

На ядерном объекте должны быть разработаны организационные мероприятия и изданы нормативные акты по физической защите.

Охрана ядерных объектов должна осуществляться на основании актов межведомственных (ведомственных, внутренних) комиссий по организации их охраны.

В категорированных зданиях, сооружениях и помещениях, где проводятся работы с ядерными материалами, должен выполняться комплекс организационно-технических мероприятий, проводимых в рабочее время работниками (персоналом) ядерного объекта, находящимися в них, с целью своевременного сообщения дежурным службам и подразделениям охраны о проникновении на их территорию лиц, не имеющих на это права, или с нарушением установленного порядка и обеспечения сохранности ядерных материалов (далее - самоохрана):

- порядок организации самоохраны должен определяться инструкцией по самоохране;

- в категорированных зданиях, сооружениях и помещениях, находящихся под самоохраной, должно быть установлено дежурство персонала и должен вестись журнал учета посетителей;

- действия персонала в зданиях, сооружениях и помещениях, находящихся под самоохраной, должны быть направлены на обеспечение защиты ядерных материалов, ядерных установок и пунктов хранения от несанкционированных действий (обнаружение несанкционированных действий и своевременное сообщение о них дежурным службам и подразделениям охраны).

К отбору и подготовке персонала физической защиты предъявляются следующие требования:

- квалификационные и медицинские требования к персоналу физической защиты должны определяться федеральными и ведомственными нормативными актами;

- должны быть установлены следующие виды профессиональной подготовки персонала физической защиты: начальная подготовка, повышение квалификации, переподготовка.

Начальная подготовка должна проводиться с кандидатами, подобранными для назначения на вакантные должности и отвечающими соответствующим квалификационным требованиям к конкретным категориям персонала физической защиты, которые определены в документе, устанавливающем требования к персоналу физической защиты ядерных материалов.

Переподготовка и повышение квалификации персонала физической защиты должны представлять собой систему мероприятий по углубленной подготовке руководящего состава и специалистов в области физической защиты с целью повышения их профессиональных знаний, умений и навыков.

Требования к комплексу ИТСФ3.

В состав комплекса ИТСФЗ должны входить ТСФЗ и инженерные средства.

Комплекс ИТСФЗ должен решать следующие задачи:

- обеспечение оперативного, устойчивого и непрерывного управления системой физической защиты;

- обеспечение установленного режима доступа персонала к ядерным материалам, на ядерную установку, в пункт хранения;

- выдача сигналов на пункты управления системы физической защиты о проникновении в охраняемые зоны, здания, сооружения, помещения или в грузовые отсеки транспортных средств, перевозящих ядерные материалы и ядерные установки, лиц, не имеющих на это права, или с нарушением установленного порядка (далее - несанкционированное проникновение);

- определение на периметрах (границах) охраняемых зон времени и места несанкционированных проникновений, а на периметре (границе) защищенной зоны - направления движения нарушителей;

- задержка (замедление) проникновения (продвижения) нарушителей;

- создание подразделениям охраны благоприятных условий для выполнения служебных задач и обеспечение возможности действий по задержанию нарушителей;

- обзорное наблюдение за охраняемыми зонами, охраняемыми зданиями, сооружениями, помещениями с целью оценки ситуации;

- регистрация (документирование) сигналов от ИТСФЗ, распоряжений и команд, отдаваемых органами управления системы физической зашиты, и докладов операторов пунктов управления системы физической зашиты.

В проекте создания (совершенствования) комплекса ИТСФЗ должны быть учтены условия эксплуатации ИТСФ3.

Условия эксплуатации ИТСФЗ для конкретных ядерных установок и пунктов хранения должны устанавливаться заказчиком в технических заданиях на создание (совершенствование) комплекса ИТСФ3.

На ИТСФЗ должна быть разработана эксплуатационная документация.

Комплекс ТСФЗ должен осуществлять:

- сбор, обработку, анализ и контроль всей получаемой информации;

- обеспечение возможности оценки тревожной ситуации в реальном масштабе времени;

- формирование и передачу сообщений (установленных сигналов) силам охраны, реагирования и органам управления системы физической защиты;

- обеспечение информационного взаимодействия между ЦПУ и ЛПУ;

- выработку управляющих воздействий на управляемые физические барьеры и средства обеспечения функционирования системы физической защиты;

- контроль состояния и работоспособности ИТСФЗ;

- контроль действий и местоположения персонала при его работе с ядерными материалами, на ядерных установках и в пунктах хранения;

- хранение и выдачу информации о функционировании системы физической защиты, попытках ее преодоления и несанкционированных действиях по отношению к защищаемым объектам и к самим ИТСФ3.

Необходимость и порядок информационного взаимодействия комплекса ИТСФЗ с системами ядерной, радиационной, экологической, технической, пожарной безопасности ядерного объекта должна устанавливаться в техническом задании на создание (совершенствование) системы физической защиты.

ИТСФЗ должны обеспечивать:

- надежную и непрерывную работу во всех заданных режимах работы;

- контроль наличия неисправностей (пропадание видеосигнала, вскрытие оборудования, попытки доступа к линиям связи и т.п.), информирование об этом оператора и архивирование данной информации;

- дистанционный контроль состояния работоспособности ИТСФ3.

ИТСФЗ должны:

- сохранять работоспособность в случае отключения основного электропитания, что должно обеспечиваться наличием резервных источников электропитания и осуществляться путем автоматического переключения основного электропитания на резервное;

- отображать информацию на соответствующий ЛПУ и ЦПУ с обязательной регистрацией перехода ИТСФЗ или их элементов на резервное питание.

Техническими средствами физической защиты являются элементы и устройства, входящие в состав следующих основных функциональных систем:

- охранной сигнализации;

- ТВС;

- СКУД;

- оптико-электронного наблюдения и оценки ситуации;

- COCO (в том числе средства проводной связи и радиосвязи);

- СТК;

- защиты информации;

- обеспечения электропитанием, освещением.

Отдельные элементы (устройства), используемые в составе комплекса ТСФЗ, могут обеспечивать реализацию требований, предъявляемых к одной или нескольким функциональным системам (интегрированные системы и устройства).

Отказ или вывод из строя какого-либо элемента комплекса ИТСФЗ не должен нарушать функционирование системы физической защиты. С этой целью должны быть предусмотрены компенсирующие мероприятия.

Управление ИТСФЗ должно осуществляться службой безопасности с ЦПУ. Управлять ИТСФЗ с ЛПУ может как служба безопасности, так и подразделение охраны ядерного объекта. Должен обеспечиваться доступ оператора ЦПУ к информации, поступающей на ЛПУ.

Операторы, осуществляющие дежурство на ЦПУ и соответствующих ЛПУ, должны быть проинформированы об особенностях технологического процесса в необходимом для выполнения своих обязанностей объеме.

В целях организации управления в системе физической защиты должны применяться:

- система двусторонней связи между центральным и локальными пунктами управления, а также между пунктами управления и подразделениями охраны;

- средства радиосвязи в подразделениях охраны и службы безопасности.

Центральный и локальные пункты управления должны быть размещены в охраняемой зоне.

На каждом ядерном объекте на стадии проектирования комплекса ИТСФЗ должны быть определены состав оборудования пунктов управления системы физической защиты, их место размещения и оснащение, а также количество ЛПУ (с учетом их возможностей частичного управления ИТСФЗ).

К инженерным средствам физической защиты относятся:

- физические барьеры;

- инженерное оборудование охраняемых зон и контрольно-пропускных пунктов (постов) охраны.

Инженерные средства должны:

- затруднять действия нарушителей при попытках несанкционированного проникновения;

- вырабатывать сигналы воздействия на управляемые физические барьеры;

- обозначать границы охраняемых зон;

- защищать персонал при несении дежурства в пунктах управления системы физической защиты, дежурных по контрольно-пропускным пунктам (постам), часовых на постах караулов и личного состава подразделений охраны при выполнении задач по пресечению несанкционированных действий и задержанию нарушителей.

Физические барьеры предназначены для воспрепятствования проходу людей и проезду транспортных средств в охраняемые зоны (выходу людей и выезду транспортных средств из охраняемых зон), задержки (замедления) проникновения (продвижения) нарушителей.

Физическими барьерами являются:

- строительные конструкции ядерного объекта (стены, перекрытия, ворота, двери);

- специально разработанные конструкции (заграждения, противотаранные устройства, решетки, усиленные двери, контейнеры);

- другие физические (в том числе естественные) препятствия.

В случае примыкания ядерного объекта к акватории должны быть приняты меры по защите от проникновения нарушителей со стороны акватории - установка сетей и других специальных средств, патрулирование катерами (если по береговой черте не представляется возможным оборудовать запретную зону, поскольку этому мешает причал и др.) и т.п.

Требования к составным частям комплекса технических средств физической защиты.

Требования к системе охранной сигнализации.

Система охранной сигнализации предназначена для обнаружения попыток и фактов совершения несанкционированных действий и должна информировать об этих событиях персонал физической защиты, другие функциональные системы, входящие в систему физической защиты, для выполнения соответствующих адекватных действий, а также автоматически подавать необходимые команды управления на исполнительные устройства и управляемые физические барьеры.

Система охранной сигнализации должна обеспечивать:

- обнаружение несанкционированного доступа;

- выдачу сигнала о срабатывании средств обнаружения на ЦПУ (ЛПУ) и протоколирование этого события;

- ведение архива всех событий, происходящих в системе физической защиты, с фиксацией всех необходимых сведений для их последующей однозначной идентификации (тип и номер устройства, тип и причина события, дата и время его наступления и т.п.);

- исключение возможности бесконтрольного снятия с охраны и постановки под охрану;

- осуществление функции приема (снятия) средств обнаружения (группы средств обнаружения) под контроль (с контроля).

Требования к ТВС.

ТВС предназначена для экстренного вызова сил реагирования, информирования о совершении несанкционированных действий, выдачи сигнала о принуждении со стороны нарушителя, а также для контроля жизнедеятельности часового и для контроля прохода патруля по заранее заданному маршруту.

ТВС должна обеспечивать:

- информирование персонала физической защиты о срабатывании ее устройств;

- определение места вызова;

- скрытость ее установки и удобство пользования вызывным устройством;

- невозможность снятия с контроля устройств ТВС;

- отличие сигналов о срабатывании устройств ТВС от сигналов о срабатывании устройств системы охранной сигнализации;

- контроль жизнедеятельности операторов пунктов управления, часовых и контролеров, находящихся на посту.

Информация, поступающая в ЦПУ и ЛПУ от устройств ТВС, должна иметь приоритет представления ее оператору по сравнению с другими сигналами.

При выборе устройств ТВС и мест их установки должны быть учтены:

- доступность для персонала физической защиты и рассредоточенность в местах несения службы;

- воздействия на персонал физической защиты, возникающие в результате угроз.

Требования к составным частям инженерных средств физической защиты.

Требования к ограждениям ядерных установок и пунктов хранения.

Ограждения ядерных установок и пунктов хранения предназначены для воспрепятствования проходу людей и проезду транспортных средств в охраняемые зоны (из охраняемых зон), минуя контрольно-пропускные пункты (посты). Ограждения строятся по периметрам охраняемых зон.

Основное ограждение проходит по периметру защищенной зоны. По периметру защищенной зоны должна быть расположена запретная зона. Внутренние и внешние ограждения запретной зоны проходят по ее границам.

Ограждения должны отвечать следующим требованиям:

- отсутствие в конструкции элементов, облегчающих преодоление ограждений;

- минимальное количество изломов.

Требования к инженерным заграждениям.

Инженерные заграждения - это средства и конструкции, установленные или устроенные в охраняемой зоне, на подступах к зданиям, сооружениям охраняемых ядерных установок, пунктов хранения с целью затруднить движение нарушителей и создать благоприятные условия для его своевременного задержания подразделениями охраны в пределах запретной зоны или на подступах к зданиям, сооружениям.

Инженерные заграждения могут быть постоянными и переносными, а по назначению - для задержки (замедления) проникновения (продвижения) людей либо транспортных средств.

Конструкция инженерных заграждений должна удовлетворять следующим требованиям:

- затруднять продвижение нарушителей вглубь ядерного объекта на время, достаточное для своевременного его задержания подразделениями охраны;

- не препятствовать нормальной работе средств обнаружения;

- обеспечивать условия для безопасного несения службы личным составом подразделений охраны.

Достаточность инженерных заграждений на периметрах охраняемых зон должна подтверждаться расчетами при оценке эффективности системы физической защиты и результатами учений.

Для передвижения подразделений охраны на транспортных средствах должна использоваться дорожная сеть внутри территории ядерного объекта, ядерных установок, пунктов хранения, а также специальные дороги (дороги охраны), которые могут строиться в запретной зоне или вне ее в зависимости от ширины запретной зоны. Дороги охраны должны пролегать вне зоны действия средств обнаружения и иметь минимальное количество пересечений с существующими на ядерных установках, в пунктах хранения автомобильными и железными дорогами. Они должны быть оборудованы знаками, предусмотренными Правилами дорожного движения. Для разворота и разъезда со встречными транспортными средствами на дороге должны быть устроены расширения. Их ширина и частота установки должны определяться местными условиями.

Для предупреждения о запрещении прохода в запретную зону по линии ее ограждений должны быть установлены предупредительные знаки с надписью: "Запретная зона. Проход (проезд) запрещен (закрыт)". В отдельных случаях должен быть предупредительный знак с надписью: "Посторонним лицам проход запрещен". Надпись должна быть на русском языке, а в отдельных случаях - на русском и соответствующем национальном языке.

Предупредительные знаки должны устанавливаться по внутреннему и внешнему ограждениям запретной зоны с использованием опор ограждений или отдельных столбов. Предупредительные знаки должны обязательно устанавливаться на изгибах (углах) запретной зоны, калитках и воротах в запретные зоны.

Общие требования к охраняемым зонам

Система физической защиты должна быть построена по зональному принципу.

В зависимости от категории предметов физической защиты, помещений, зданий, сооружений и промышленных площадок, в которых размещаются предметы физической защиты, на ядерном объекте должны быть выделены и документально оформлены охраняемые зоны и зоны ограниченного доступа со схемой расположения периметров охраняемых зон и ядерного объекта.

Сооружения, комплексы, установки, устройства, оборудование, технические средства и коммуникации, не предусмотренные в проектах ядерного объекта, ядерной установки, пункта хранения, не должны размещаться в охраняемых зонах.

В местах наиболее вероятного проникновения нарушителей в охраняемую зону с использованием транспортных средств должны приниматься меры, исключающие или существенно затрудняющие проникновение (установка противотаранных устройств и др.).

Прилегающая к границе охраняемой зоны местность должна быть очищена от кустарника, деревья прорежены таким образом, чтобы исключалась возможность их использования для ее преодоления.

Для организации прохода людей и проезда транспортных средств по периметру охраняемой зоны должны оборудоваться контрольно-пропускные пункты (посты). Контрольно-пропускные пункты (посты) должны располагаться с учетом организации движения транспорта и прохода людей и обеспечивать требуемую пропускную способность.

На контрольно-пропускных пунктах (постах) должен осуществляться контроль правомочности прохода (проезда) и идентификация проходящих людей (проезжающих транспортных средств), обеспечиваться санкционированный доступ людей и транспортных средств и задержание нарушителей, должны приниматься меры по предотвращению несанкционированного проноса и провоза ядерных материалов, ядерных установок, радиоактивных веществ, взрывчатых веществ, холодного и огнестрельного оружия, других запрещенных предметов.

Контрольно-пропускные пункты (посты) должны быть оборудованы и (или) оснащены средствами защиты от поражения стрелковым оружием персонала, выполняющего контрольные и пропускные функции.

Транспортные контрольно-пропускные пункты должны оборудоваться противотаранными устройствами.

Часовой (постовой) контрольно-пропускного пункта (поста) должен быть обеспечен информацией:

- о включенных, выключенных и неисправных пропускных устройствах;

- о причинах блокирования людей и направлении прохода (в охраняемую зону или из нее).

Доступ в особо важную зону и выполнение работ в ней должны осуществляться с применением правила двух лиц.

Должна быть определена необходимость выполнения правила двух лиц и порядок его осуществления, в том числе в части, касающейся организации охраны ядерного объекта, при проведении работ в категорированных помещениях, не отнесенных к особо важной зоне, а также при проверках транспортных средств, вывозимых контейнеров и емкостей на контрольно-пропускных пунктах (постах).

Общие требования к оснащению охраняемых зон

Периметры охраняемых зон должны быть оснащены ИТСФЗ, обеспечивающими обнаружение несанкционированных действий, экстренный вызов сил реагирования и представление информации для оценки ситуации, а также задерживающими продвижение нарушителей к предметам физической защиты.

Не должно быть участков границ охраняемых зон, недоступных для наблюдения. Средства обнаружения должны быть размещены таким образом, чтобы отсутствовали неконтролируемые участки ("мертвые зоны").

Пропускное устройство, установленное на контрольно-пропускном пункте (посту), помимо работы в автоматическом режиме, должно обеспечивать возможность пропуска лиц по разовым пропускам и спискам для контроля и оперативного управления на контрольно-пропускном пункте (посту).

Подъезды (дороги, участки местности) к периметрам охраняемых зон (на путях наиболее вероятного прорыва нарушителей с использованием транспортных средств) и транспортным контрольно-пропускным пунктам (постам) должны быть оснащены противотаранными устройствами, сооружениями, рвами, противотаранными стенками, бетонными блоками, а дорожное полотно должно иметь надолбы, крутые повороты и т.п. для исключения возможности развития необходимых для прорыва скоростей, либо должны приниматься другие меры, исключающие или существенно затрудняющие такой прорыв.

Транспортные контрольно-пропускные пункты (посты) должны быть оборудованы въездными и выездными воротами, досмотровыми ямами, эстакадами, смотровыми зеркалами или другими техническими средствами, обеспечивающими возможность досмотра транспортного средства со всех сторон, противотаранными устройствами, средствами обнаружения провоза ядерных материалов и радиоактивных веществ.

Все входы в категорированные здания, сооружения, помещения и выходы из них должны оборудоваться средствами обнаружения, контроля и управления доступом и при необходимости - наблюдения и оценки ситуации.

Аварийные выходы должны обеспечивать беспрепятственный выход людей в чрезвычайных ситуациях.

На ядерном объекте должен быть разработан порядок учета, хранения и контроля замков и ключей, использующихся в системе физической защиты.

Порядок учета, хранения и контроля замков и ключей должен предусматривать:

- регистрацию всех лиц, получивших доступ к ключам;

- регистрацию выдачи и сдачи ключей;

- проверку наличия ключей и меры по предотвращению их несанкционированного использования;

- замену в кратчайшие сроки замков и ключей при обнаружении факта или при появлении подозрения относительно несанкционированного использования замков и ключей.

Каждому замку и ключу должен быть присвоен инвентарный номер согласно журналу учета замков и ключей. На каждом ключе должен быть отштампован его инвентарный номер. Ключи должны оставаться в пределах соответствующей охраняемой зоны.

Требования к эксплуатации инженерно-технических средств физической защиты.

Эксплуатация ИТСФЗ должна включать техническую эксплуатацию и применение ИТСФЗ по назначению.

Техническая эксплуатация ИТСФЗ представляет собой комплекс организационных и технических мероприятий, обеспечивающих сбережение, поддержание в исправном состоянии и постоянной готовности ИТСФЗ к применению, восстановление их работоспособности и ресурса.

Техническая эксплуатация ИТСФЗ должна включать:

- профессиональный отбор и допуск персонала физической защиты к эксплуатации ИТСФЗ;

- планирование технической эксплуатации;

- проверку функционирования, техническое обслуживание и ремонт;

- материально-техническое и метрологическое обеспечение;

- ведение эксплуатационной и учетной документации;

- учет, хранение, транспортирование и консервацию;

- сбор, учет и анализ эксплуатационных данных о надежности и устойчивости работы ИТСФЗ;

- контроль и оценку технического состояния и организации эксплуатации;

- организацию работ по обеспечению и соблюдению правил и мер безопасности при эксплуатации.

Планирование технической эксплуатации ИТСФ3.

Должна быть спланирована техническая эксплуатация ИТСФЗ на ядерных установках, в пунктах хранения.

В планах должны отражаться мероприятия:

- по техническому обслуживанию;

- по организации ремонта и хранению;

- по материально-техническому обеспечению эксплуатации;

- по организации сбора, учета и анализа данных о помехоустойчивости и эксплуатационной надежности ТСФЗ;

- по технике безопасности;

- по контролю за техническим состоянием и организацией эксплуатации ИТСФ3.

физическая безопасность защита

# Заключение

В заключение можно сделать следующие выводы.

Предметы физической безопасности предприятия – это ресурсы Компании, которые должны быть максимально защищены.

**Основные задачи обеспечения физической безопасности организации:**

1) Исключение чрезвычайных ситуаций, которые могут привести к утрате корпоративных ресурсов (пожар в офисе и на объектах организации, авария в энерго, тепло и водоснабжении, приведшая к срыву работы персонала, др.);

2) Снижение вероятности возникновения угрозы для жизни и здоровья персонала. (Охрана VIP персон, служба оперативного дежурного, дежурство контролеров в аптеках и в офисе организации, недопущение хищений или порчи товаро-материальных ценностей);

3) Комплексное использование сил службы безопасности и охраны и инженерно-технических средств на объекте в целях защиты собственности;

4) Воспрепятствование незаконному проникновению на объекты организации посторонних лиц, имеющих целью получение доступа к имуществу, финансам, служебным документам, информации на электронных носителях;

5) Ограничение и разграничение доступа различных категорий посетителей на территорию, в здания и помещения организации;

6) Выявление и пресечение незаконных действий лиц и преступных групп, взаимодействие с правоохранительными органами по правовым вопросам и вопросам оперативной работы.

Физическая безопасность предприятия включает в себя следующие основные элементы:

- силы и средства службы безопасности;

- силы и средства службы охраны (в т.ч. сторонних организаций, привлекаемых для охраны на договорной основе);

- личная охрана VIP-персон;

- служба оперативного дежурного;

- контролеры в аптеках, контролеры КПП;

- оперативные группы;

- операторы;

- технический отдел;

- сотрудники вневедомственной охраны.

**Меры обеспечения эффективного функционирования физической безопасности предприятия:**

- строгий учет и четкий порядок хранения подлежащих защите товарно-материальных ценностей, финансовых ресурсов, бухгалтерской отчетности, машинных носителей информации;

- высокая подготовка персонала в соответствии со штатным расписанием, четким знанием и строгим выполнением персоналом своих функциональных обязанностей;

- персональная ответственность за свои действия каждого сотрудника, соприкасающегося в рамках своих должностных обязанностей с материальными, финансовыми и информационными ресурсами;

- строгое выполнение всеми сотрудниками требований установленного режима на объекте;

- эффективный контроль за соблюдением установленного режима на объекте;

- принятие мер профилактического воздействия к потенциальным нарушителям;

- эффективная работа сотрудников службы безопасности и охраны по своевременному выявлению и пресечению противоправных действий нарушителей (попытки хищения товарно-материальных ценностей и финансовых ресурсов, несанкционированное проникновение на территорию режимного объекта и к информации, представляющей коммерческую тайну, провокационные действия экстремистов, угроза жизни и здоровью персонала со стороны террористов, попытка поджога или закладки взрывчатых веществ, др.);

- результативная работа сил службы безопасности, эффективное взаимодействие с правоохранительными органами, своевременное информированием руководства организации о преднамеренных или непреднамеренных противоправных действиях недобросовестных сотрудников, партнеров по бизнесу, других лиц;

- высокий профессиональный навык и опыт работы работников службы безопасности и охраны. Реализация системы инженерно-технических средств безопасности, предусматривающей многорубежность построения охраны территории, зданий и помещений с комплексным применением современных средств обнаружения, видеонаблюдения, сбора и обработки информации, обеспечивающих достоверное отображение и объективное документирование событий;

- устойчивая работа системы пожарной сигнализации и автоматического пожаротушения на объектах организации, ее своевременная проверка и обслуживание.

# Список литературы

1. Алаухов С.Ф, Коцеруба В.Я. Вопросы создания систем физической защиты для крупных промышленных объектов // Системы безопасности, 2001, № 41, С. 93.
2. Барсуков, В.С. Безопасность: технологии, средства, услуги / В.С. Барсуков. - М., 2001 - 496 с.
3. Барсуков, В.С. Современные технологии безопасности / В.С. Барсуков, В.В. Водолазский. - М.: Нолидж, 2000. - 496 с., ил.
4. Галатенко В.А. Стандарты информационной безопасности / Под редакцией академика РАН В.Б. Бетелина // М.: ИНТУИТ.РУ «Интернет-университет информационных технологий», 2004
5. Денисов В.Ф. Методы и средства проектирования функциональных профилей систем управления в организационно-технических системах // Перспективные информационные технологии в научных исследованиях, проектировании и обучении – Самара: СГАУ, 2006
6. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты – К.: ДиаСофт, 2005
7. Измайлов А.В. Методы системного проектирования комплексов технических средств физической защиты российских ядерных объектов // Российско-американский семинар по физической защите ядерных материалов и установок, ГП СНПО "Элерон", М., Россия. 1995.
8. Инженерно-техническая укрепленность. Технические средства охраны. Требования и нормы проектирования по защите объектов от преступных посягательств. МВД РФ. М., 2002
9. Колчин А.Ф., Овсянников М.В., Стрекалов А.Ф., Сумароков С.В. Управление жизненным циклом продукции. – М.: Ахарсис, 2002
10. Мишин Е.Т., Оленин Ю.А.,Капитонов А.А."Системы безопасности предприятия - новые акценты // Конверсия в машиностроении, 1998, № 4.
11. Одинцов А.А. Экономическая и и информационная безопасность предпринимательства: учеб.пособие для вузов. - М.: Академия, 2008
12. Оленин Ю.А., Алаухов С.Ф. К вопросу категорирования объектов с позиции охранной безопасности // Системы безопасности, связи и телекоммуникаций, 1999, № 30, С. 26.
13. Садердинов А.А., Трайнев В.А., Федулов А.А. Информационная безопасность предприятия: Учебное пособие. – М.: Издательско-торговая корпорация «Дашков и Ко», 2004
14. Системы охранные телевизионные. Общие технические требования и методы испытаний. М., 2000
15. Станкевич В.И. Замысел построения комплексной системы обеспечения безопасности территории, М: НИИ автоматической аппаратуры им. академика В.С. Семенихина.
16. Трубачев А.П. Разработка требований к безопасности продуктов и систем информационных технологий на основе ГОСТ Р ИСО/МЭК 15408-2002 – М.: ООО "Центр безопасности информации
17. Ярочкин, В.И. Информационная безопасность. Учебник для студентов вузов / 3-е изд. - М.: Академический проект: Трикста, 2005. - 544 с.