Министерство образования и науки Украины

Донецкий национальный университет экономики и торговли имени Михаила Туган-Барановского

Кафедра экономики предприятия

**Реферат** на тему:

«КОНЦЕПЦИЯ БЕЗОПАСНОСТИ И ПРИНЦИПЫ СОЗДАНИЯ СИСТЕМ ФИЗИЧЕСКОЙ ЗАЩИТЫ ВАЖНЫХ ПРОМЫШЛЕННЫХ ОБЪЕКТОВ»

**Выполнила:**

студентка группы ЭП-06-Д

Травкина Мария

**Преподаватель:**

Корнилова Е. В.

Донецк 2010

**Введение**

В современных условиях сложной криминогенной обстановки в мире и Украине 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.

**1. Принципы создания СФЗ**

**1.1 Термины и определения**

В настоящем документе применяются следующие ключевые термины и определения.

**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.

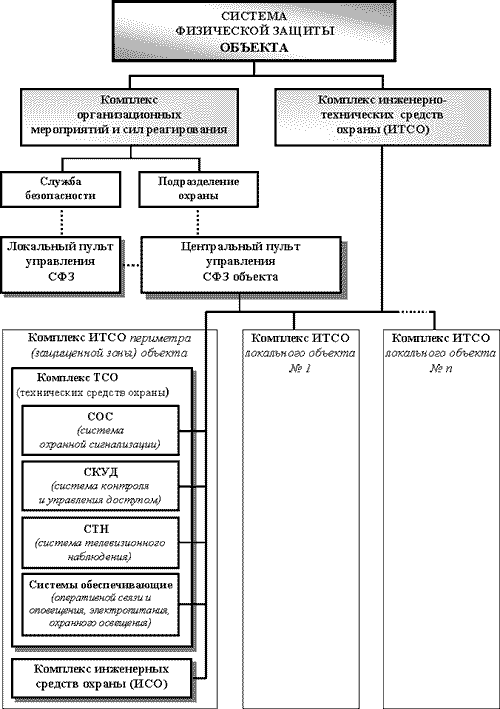
**Уязвимость (объекта)** - степень несоответствия принятых мер защиты (объекта) прогнозируемым угрозам или заданным требованиям безопасности.

**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).

**1.2 Структура СФЗ**

"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 рис. 1.



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 [1].

**1.3 Принципы и порядок создания СФЗ**

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 [2]: 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.

**1.4 Концепция физической безопасности объекта**

автоматизированная персонал защита несанкционированное

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?".

**2. Анализ уязвимости объекта**

**2.1 Цели и задачи анализа**

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 по п.п. а-в проводятся методом экспертных оценок комиссией, в состав которой входят специалисты НИКИРЭТ и специалисты соответствующих служб заказчика: безопасности, главного технолога, главного инженера, пожарной охраны. Работы по п.п. г-д 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).

**2.2 Предметы защиты**

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.

**2.3 Угрозы безопасности**

Основными угрозами безопасности, которые могут привести к утрате корпоративных ресурсов предприятия, являются [3]:

* 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?

**2.4 Оценка уязвимости существующей СФЗ объекта**

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.

**2.5 Оценка возможного ущерба от реализации прогнозируемых угроз**

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.

**2.6 Количественная оценка уязвимости объекта и эффективности существующей СФЗ**

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.

**2.7 Разработка общих рекомендаций по обеспечению безопасности объекта**

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

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

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 [3]. 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.

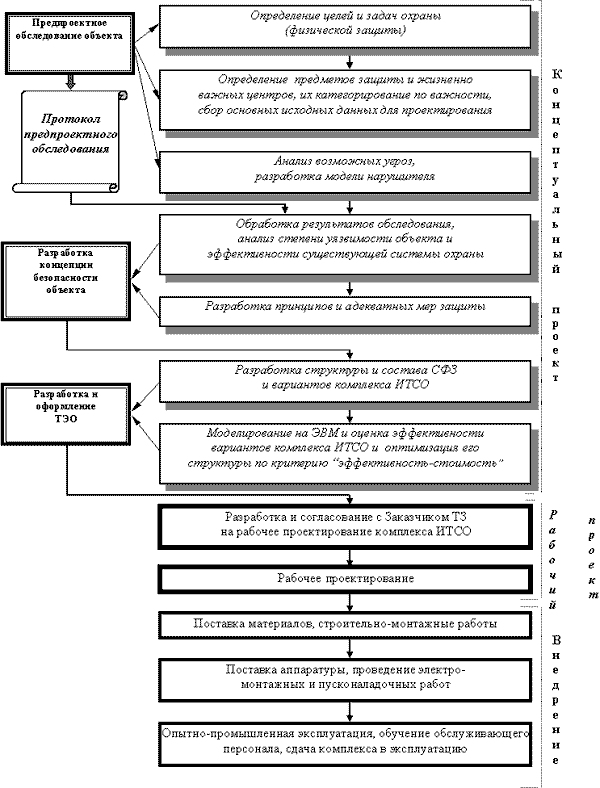
Такой подход позволяет избежать серьезных ошибок в рабочем проекте, а следовательно, и излишних затрат на возможную доработку системы при ее эксплуатации.

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 рис. 2.



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) [4]. 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.

**Заключение**

1. Создание эффективных систем безопасности важных объектов не может базироваться на довольно часто применяемом на практике принципе "разумной достаточности", а требует комплексного научного подхода.

2. Проектирование интегрированных систем физической безопасности важных объектов целесообразно проводить в две стадии:

* концептуальное (системное) проектирование;
* рабочее проектирование.

3. Проведение анализа уязвимости и количественной оценки эффективности СФЗ объекта позволяет на ранней стадии проектирования выбрать оптимальный вариант комплекса ИТСО по критерию "эффективность-стоимость".

**Литература**

1. Мишин Е.Т., Оленин Ю.А.,Капитонов А.А."Системы безопасности предприятия - новые акценты // Конверсия в машиностроении, 1998, № 4.
2. 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.
3. Оленин Ю.А., Алаухов С.Ф. К вопросу категорирования объектов с позиции охранной безопасности // Системы безопасности, связи и телекоммуникаций, 1999, № 30, С. 26.
4. Алаухов С.Ф, Коцеруба В.Я. Вопросы создания систем физической защиты для крупных промышленных объектов // Системы безопасности, 2001, № 41, С. 93.