МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

УНИВЕРСИТЕТ ИТМО

В. В. ВОЛХОНСКИЙ

СИСТЕМЫ ФИЗИЧЕСКОЙ ЗАЩИТЫ.

Основы теории

Учебное пособие

УНИВЕРСИТЕТ ИТМО

Санкт-Петербург
2017

Рецензент:
кандидат технических наук Т.М. Рахматуллина

Волхонский В. В Системы физической защиты. Основы теории: Учебное пособие. – СПб: Университет ИТМО, 2017. – 102 с.

Рассматриваются основные вопросы теории систем безопасности и, как частного случая, систем физической защиты. Анализируется терминология, угрозы объекту, потери, риски, особенности воздействия угрозы на объект, модели нарушителя, процедуры проектирования и оценки эффективности. Рассматриваются концептуальные вопросы построения систем физической защиты.

Учебное пособие предназначено для обучения магистров по направлению 16.04.01 «Техническая физика» в рамках магистерских программ «Оптоэлектронные системы безопасности» и «Физика и техника оптоэлектронных информационных систем» и бакалавров по направлению 12.03.05 «Лазерная техника и лазерные технологии».

Рекомендовано к печати Ученым советом факультета световой и лазерной инженерии, протокол № 5 от 03.05.2017.

УНИВЕРСИТЕТ ИТМО

Университет ИТМО – ведущий вуз России в области информационных и фотонных технологий, один из немногих российских вузов, получивших в 2009 году статус национального исследовательского университета. С 2013 года Университет ИТМО – участник программы повышения конкурентоспособности российских университетов среди ведущих мировых научно-образовательных центров, известной как проект «5 в 100». Цель Университета ИТМО – становление исследовательского университета мирового уровня, предпринимательского по типу, ориентированного на интернационализацию всех направлений деятельности.

Содержание

Предисловие

Рост разнообразия различных по характеру и степени опасности угроз практически во всех областях жизнедеятельности человека требует разработки и применения средств и методов эффективной защиты от этих угроз. В решении таких задач важнейшее место занимает система физической защиты (СФЗ), как один из основных элементов системы обеспечения комплексной безопасности любого объекта. СФЗ использует широко известные средства обеспечения безопасности, такие как средства охранной и пожарной сигнализации, ТВ-наблюдения, контроля и управления доступом, инженерной укрепленности и многие другие. Они позволяют эффективно решать проблемы обеспечения безопасности в самых разных практических задачах, в том числе в областях ядерной безопасности (ЯБ), защиты объектов информатизации (ОИ), критической инфраструктуры, культурного наследия и т.д.

Разнообразие угроз различным жизненным приоритетам требует и комплексного подхода к обеспечению как безопасности в целом, так и к решению задачи физической защиты объектов, как одной из основных составляющих общей задачи обеспечения безопасности. К примеру, можно ли решить задачу информационной безопасности серверной (как помещения со средствами хранения и обработки информации) без охранной сигнализации, без контроля окружающей температуры (повышение которой может вызвать выход из строя оборудования) или без учета риска затопления от системы отопления?

Поэтому учет всех видов угроз в комплексе и выбор и применение соответствующих адекватных угрозам средств и методов должны лежать в основе подхода к созданию СФЗ.

Построение эффективной системы безопасности невозможно без комплексного подхода, охватывающего выявление всех основных угроз, оценку возможного ущерба

при реализации этих угроз и создание комплекса технических средств (ТС) защиты объекта (естественно, при определенных ограничениях, например, на стоимость системы).

Рассматриваемым вопросам физической защиты различных объектов прямо или косвенно посвящено много работ, например, [1–10]. Однако большинство из них в значительной степени касается определенных прикладных задач. Но упомянутое разнообразие угроз требует рассмотрения вопросов физической защиты объектов с более общей позиции, с одной стороны, и, с другой стороны, учета специфики таких объектов при сохранении общности в подходе к решаемым задачам в других предметно ориентированных областях.

В пособии рассматриваются общие вопросы теории физической защиты объектов и разработки систем физической защиты. При этом многие вопросы справедливы не только для задач физической защиты, но и для самых разных систем обеспечения безопасности.

Автор будет признателен за отзывы и замечания, которые можно направлять по адресу volkhonski@mail.ru.

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

На современном этапе развития систем безопасности (СБ) и, как их частных случаев, систем физической защиты (СФЗ) в условиях увеличения количества угроз и способов их реализации, роста разнообразия и важности объектов обеспечения безопасности (ООБ), различных методов и средств обеспечения безопасности возникает необходимость обобщения, уточнения и четкого определения существующих понятий для того, чтобы специалисты в разных предметно ориентированных областях говорили «на одном языке», вкладывая в смысловое значение одних и тех же терминов одинаковый смысл. Это является причиной того, что публикуются работы, посвященные именно терминологии в той или иной области [10-12], а также терминологические словари, к примеру, [13, 14]. И, конечно, многие термины определены в государственных стандартах России.

Вопросы терминологии, на первый взгляд второстепенные, по сути, являются весьма важными в любых предметно ориентированных областях обеспечения безопасности, в том числе в области ФЗ.

Причина этого заключается в следующем. Терминология в различных сферах применения ресурсов, средств и методов (РСМ) обеспечения безопасности, например информационной (ИБ), ядерной, противокриминальной и других, разрабатывалась, как правило, в соответствии с историческими потребностями и востребованностью тех или иных РСМ обеспечения безопасности для определенных задач. На начальном этапе различные термины и понятия формулировались с учетом особенностей и специфики практических задач каждой конкретной области, а это неизбежно ограничивало общность понятий. Хотя такая задача, как формулировка общих определений, при этом обычно и не ставилась. Конечно, предметно ориентированные определения также нужны, однако они,

как минимум, должны быть согласованы с общими определениями, применимыми для разных прикладных задач.

Вопрос терминологии важен и с точки зрения международного общения специалистов, требующего перевода рассматриваемых понятий с русского на английский и наоборот.

Рассмотрим основные вопросы терминологии применительно к тематике данной работы.

1.1. Безопасность

Понятие безопасности является достаточно широким и разносторонним. Поэтому прежде всего определимся с общим термином *безопасность*, поскольку задача ФЗ любых объектов является частным случаем общей задачи обеспечения безопасности какого-либо объекта.

В понятие *объекта обеспечения безопасности* будем включать не только собственно *объект,* но и *субъект*, понимая под этими терминами следующее:

субъект – человек, личность как носитель каких-либо свойств;

объект – любые объекты флоры и фауны; составляющие окружающей среды; имущество (включая здания, сооружения, предметы,…); ресурсы, информацию, имеющие материальную, культурную, историческую или иную ценность для субъекта обеспечения безопасности.

Воспользуемся определением рассматриваемого термина *безопасность* из Закона Российской Федерации «О безопасности» [15]:

«Безопасность – состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз». «*Жизненно важные интересы* – совокупность потребностей, удовлетворение которых надежно обеспечивает существование и возможности прогрессивного развития личности, общества и государства».

Понятие *жизненно важные интересы* можно также определить как *жизненные приоритеты* [15].

Приведенное выше определение безопасности включает и другие составляющие, такие, к примеру, как государственная безопасность или права и свободы личности и т. п., которые в данной работе не рассматриваются.

Определение безопасности можно сделать более общим, убрав излишнюю детализацию и определив *безопасность* как *состояние защищенности объекта обеспечения безопасности от различных угроз.*

Исходя из приведенных определений, можно говорить и о том, что термины *безопасность* и *защищенность от угроз* идентичны, поскольку первый из них означает *состояние защищенности …от…угроз*.

С общей точки зрения, можно говорить о трех аспектах понимания термина *безопасность*.

Во-первых, как состояние защищенности ООБ от чего-либо, от каких-либо угроз. Например, противокриминальная, антитеррористическая, противопожарная и т. п. безопасность.

Во-вторых, как безопасность определенного ООБ, т. е. состояние защищенности чего-либо. К примеру, безопасность информации, государства и т. п.

В-третьих, как неспособность чего-либо нанести ущерб ООБ. Примерами могут служить безопасность продуктов питания, т. е. отсутствие угроз для здоровья со стороны продуктов при их потреблении, или электробезопасность оборудования, означающая отсутствие угрозы поражения пользователей электрическим током со стороны электроприборов.

1.2. Система безопасности

Задача обеспечения безопасности любого объекта решается системой безопасности этого объекта. Поэтому в первую очередь отметим, что систему обеспечения безопасности следует рассматривать в комплексе, во всех ее аспектах, т. е.

как систему, решающую задачи или выполняющую все следующие основные функции, необходимые для обеспечения безопасности [6, 11]:

- предотвращение угроз или поддержание безопасного состояния объекта (как идеальный вариант функционирования СБ);
- обнаружение угроз (желательно на более раннем этапе, пока ситуация не развилась до опасной стадии, когда ООБ может быть нанесен ущерб);
- противодействие возникшим угрозам (для уменьшения последствий реализации угрозы);
- ликвидация угроз, по возможности до нанесения ООБ ущерба;
- анализ произошедшего в целях совершенствования используемых средств обеспечения безопасности и методов их использования.

При этом необходимо помнить, что основная функция СБ – *недопущение ущерба объекту обеспечения безопасности*. Таким образом, если проанализировать вышеприведенные задачи, то становится ясно, что основная функция СБ выполняется только в тех случаях, когда угроза либо предотвращена, либо своевременно ликвидирована. Здесь надо отметить типичную ошибку, допускаемую при оценке результатов создания той или иной системы. Например, создается система охранной сигнализации (СОС) или система телевизионного наблюдения (ТВ-наблюдения) некоторого объекта и заявляется, что «обеспечена безопасность» объекта. Но при этом из упомянутых выше функций выполняется практически только задача обнаружения угрозы, в данном примере несанкционированного проникновения, но не ее ликвидация. На деле все должно быть направлено не только на обнаружение, но и на ликвидацию угрозы до нанесения объекту ущерба. Только тогда можно говорить о решении задачи обеспечения безопасности объекта. Для этого в вышеприведенном приме-

ре необходимо обязательно обеспечить реагирование на обнаруженную угрозу, например, выслать группу задержания, чтобы предотвратить кражу.

Для того чтобы сформулировать понятие *системы безопасности*, необходимо определить в общем виде три составляющие данного понятия:

- объект обеспечения безопасности;
- угрозы этому объекту;
- средства (технические и программные), методы (правовые нормы, организационные мероприятия и т. п.) и ресурсы обеспечения безопасности.

С точки зрения общности формулировки, применимой к любой предметно ориентированной задаче, можно дать следующее общее определение системы безопасности.

Система безопасности – это совокупность ресурсов, средств и методов, обеспечивающих предотвращение, обнаружение и ликвидацию угроз жизни, здоровью, среде обитания, имуществу, ресурсам и информации.

Здесь определено, во-первых, что такое система безопасности (совокупность ресурсов, методов и средств…), во-вторых, какие функции она решает (…обеспечивает предотвращение, обнаружение и ликвидацию угроз…), и, наконец, объект обеспечения безопасности (…жизнь, здоровье, среда обитания, имущество, ресурсы и информация).

Проанализируем детальнее составляющие этого определения.

«…совокупность ресурсов, средств и методов и …» – означающая, что (какие ресурсы и средства) и как (какие методы) используется для решения задачи обеспечения безопасности. При этом подразумевается [11] полный перечень технических средств (аппаратных, программных, инженерной защиты,...), ресурсов (финансовых, материальных, трудовых,…), а также методов их использования (включая законодательно-нормативную базу). Фактически это перечень того,

что необходимо в данном случае для решения задачи обеспечения требуемого уровня безопасности конкретного объекта.

«...обеспечивающих поддержание безопасного состояния объекта, предотвращение, обнаружение и ликвидацию угроз...» – необходимость всего этого определяется основными функциями СБ. В частности, ликвидация достигается при использовании в системе соответствующих методов и средств противодействия и ликвидации или ограничения угрозы (средства автоматизированного пожаротушения, блокировки замков при проникновении, включение средств противодействия утечке информации, систем управления жизнеобеспечением зданий, соответствующие методы действия службы охраны и т. д.).

«...жизни, здоровью, среде обитания, имуществу, ресурсам и информации» – это список жизненных приоритетов, охватывающий все сферы жизнедеятельности людей, а также живых организмов, материальные, информационные и другие ресурсы. Поэтому в эти понятия вписываются практически все возможные объекты защиты.

Если говорить об упоминавшихся выше трех аспектах трактовки термина *безопасность*, то применительно к понятию СБ его надо понимать не только в первых двух смысловых значениях, а и в третьем варианте, поскольку один из принципов построения системы безопасности состоит в том, что сама СБ не должна создавать угроз объекту, безопасность которого она обеспечивает.

В зависимости от того, какие задачи ставятся при создании СБ, можно говорить об обеспечении:

- противокриминального;
- противопожарного;
- антитеррористического;
- антивандального;
- технологического;

- информационного;
- экономического;
- экологического;
- радиационно-химического;
- бактериологического

и других направлений обеспечения безопасности конкретного субъекта или объекта, необходимых в каждой определенной задаче.

Это деление достаточно условно. В ряде случаев средства и методы решения задач упомянутых составляющих обеспечения безопасности могут перекрываться, например, противокриминальная защита решает также часть вопросов антитеррористической, антивандальной и информационной безопасности. Но это еще раз подчеркивает необходимость разработки общего комплексного решения, учитывающего все особенности объекта.

1.3. Технические средства обеспечения безопасности

Для дальнейшего анализа терминов имеет смысл определиться с составом основных технических средств (ТС) обеспечения безопасности применительно к рассматриваемым задачам обеспечения ФЗ. В составе этих средств обычно присутствуют различные комплексы или подсистемы, выполняющие разные функции по обеспечению безопасности объектов. При этом надо учесть, что в современных условиях в значительном числе случаев трудно и обычно нецелесообразно разделять разные подсистемы безопасности или функции, выполняемые этими подсистемами. Так, для одного и того же ООБ одни и те же средства, к примеру, охранной сигнализации, контроля доступа, ТВ-наблюдения и другие, могут решать задачи антитеррористической, противокриминальной, информационной и других видов безопасности. И наоборот, материальные ресурсы могут быть ООБ при решении задач

обеспечения упомянутых выше видов безопасности, к примеру информационной.

Сказанное иллюстрирует рис. 1, на котором представлен состав основных ТС обеспечения безопасности – охранной и пожарной сигнализации, ТВ-наблюдения, контроля доступа, инженерно-технической защиты и др. А также показана возможность использования перечисленных средств для решения различных прикладных задач обеспечения безопасности – противокриминальной, антитеррористической, информационной и т. д.

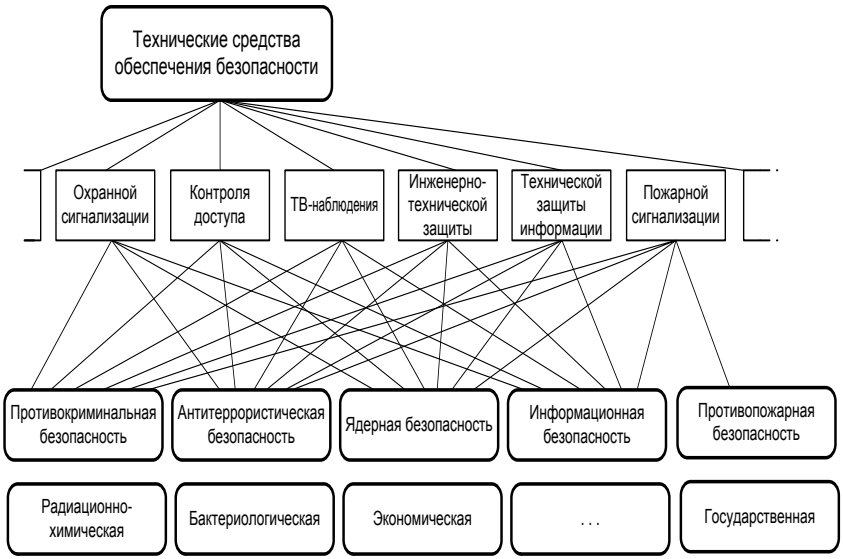


Рис. 1. Технические средства обеспечения безопасности

Очевидно, что одни и те же ТС могут использоваться в различных практических задачах.

Понятие безопасности является достаточно широким и разносторонним, и невозможно охватить одновременно все проблемы. Поэтому в данной работе, как отмечалось выше, не рассматриваются такие вопросы, как государственная

безопасность, бактериологическая и радиационно-химическая безопасность и др., а основное внимание будет уделено средствам обеспечения физической защиты, а также методам и способам их использования.

1.4. Системы физической защиты

Термины *физическая защита* или *системы физической защиты* используются в различных документах и литературе в четырех смысловых значениях:

1) защита от физических лиц;
2) защита физическими лицами (сотрудниками служб охраны);
3) использование физических препятствий для достижения цели нарушителем (угрозой);
4) обеспечение физической целостности объектов.

В последнем случае понятие физической целостности учитывает сохранение размеров, формы, состояния объекта защиты. В это понятие включено также и сохранение взаимного пространственного расположения различных элементов ООБ без нарушения целостности каждого из элементов (например, в случае кражи это перемещение чего-либо с объекта). Сохранение физического состояния подразумевает и невозможность появления чего или кого-либо на ООБ (к примеру, нарушителя в помещении ООБ), приводящего к изменению состояния какой-либо среды (воздушной, водной и т. д.) внутри или вокруг объекта.

Проанализируем эти смысловые значения. Можно говорить о том, что в той или иной мере правильны все четыре значения, но применительно только к конкретным практическим задачам. Кроме того, каждое их этих смысловых значений учитывает не все возможные угрозы.

В первом случае угрозой считаются только физические лица, хотя очевидно, что угрозы могут исходить не только от физических и не только от неуполномоченных лиц. Имеется

ряд других угроз, аналогичных по наносимому ущербу, а зачастую и превосходящих его. Примерами могут служить ситуации на АЭС Фокусима (реализовавшаяся угроза – природное явление) и Чернобыльской АЭС (реализовавшаяся угроза – неправильные действия уполномоченных лиц – персонала). Таким образом, подобное ограничение перечня угроз снижает общность определений, поскольку одни и те же последствия могут быть при реализации разных угроз.

Второй вариант (защита физическими лицами) представляется также частным случаем, поскольку сотрудники службы охраны составляют лишь часть системы обеспечения физической безопасности и практически всегда используются в сочетании с техническим средствами обеспечения безопасности.

Третий случай (использование физических препятствий) также является частным, так как препятствия, создающие задержку в развитии угрозы, могут быть не только физическими, а, например, программными, организационными и другими. И только одними препятствиями задача ФЗ не решается.

Последнее смысловое значение (обеспечение физической целостности) определяет защищенность объекта от произвольных в общем случае угроз и учитывает возможность некоторых специфических способов реализации угроз и конкретных объектов. Например, проникновение на ОИ без нарушения физической целостности его элементов для съема информации по визуальному или акустическому каналу. В таком случае, как отмечалось выше, появляется некий объект (человек или беспилотный летательный аппарат) и происходит изменение параметров воздушной среды на ООБ. Это изменение может обнаруживаться средствами СФЗ.

Таким образом, можно говорить, что все четыре трактовки могут быть использованы, в том числе, и в различных сочетаниях. Например, обеспечение физической целостности объекта от физических лиц путем создания физических пре-

пятствий и с привлечением физических лиц (сотрудников охраны).

Поэтому, обобщая сказанное, можно дать нижеследующие определения терминов ФЗ и СФЗ.

Физическая защита – это защита объекта путем применения совокупности ресурсов, средств и методов по обеспечению предотвращения, обнаружения и ликвидации угроз физической целостности объекта защиты.

Система физической защиты – это совокупность ресурсов, средств и методов, обеспечивающих предотвращение, обнаружение и ликвидацию угроз физической целостности объекта защиты.

Вышесказанное легко распространить для определенных прикладных задач, например для задач защиты ОИ, конкретизируя объект защиты.

Физическая защита объекта информатизации – это защита объекта путем применения совокупности ресурсов, средств и методов по обеспечению предотвращения, обнаружения и ликвидации угроз физической целостности объекта информатизации и средств обработки, передачи и хранения информации.

Система физической защиты объекта информатизации – это совокупность ресурсов, средств и методов, обеспечивающих предотвращение, обнаружение и ликвидацию угроз физической целостности объекту информатизации и средствам обработки, передачи и хранения информации.

Эти определения практически полностью согласуются с приведенными выше определениями стандартов, в первую очередь [20, 21] с учетом обобщения на произвольный комплекс угрозы, а не только такого частного случая угрозы, как нарушитель.

Сформулируем перечень основных технических средств ФЗ объекта. С учетом состава ТС обеспечения безопасности, рассмотренного выше (см. рис. 1), специфики обеспечения

физической защиты к ним могут быть отнесены следующие средства (рис. 2):

- охранной сигнализации;
- пожарной сигнализации;
- ТВ-наблюдения;
- контроля доступа;
- инженерно-технической защиты;
- обеспечения (связи, энергопитания, транспорта и т. п.);
- реагирования.

Рис. 2. Состав технических средств физической защиты

1.5. Средства реагирования

Остановимся еще на одном понятии, не относящемся непосредственно к ТС ФЗ, но напрямую связанном с такой важной составляющей обеспечения безопасности, как ресурсы, средства и методы реагирования на угрозы. Обычно это персонал служб безопасности (иногда также называемых силы службы безопасности, силы ответного действия, персонал охраны) с соответствующим материальным (оружие, средства связи, транспорт и др.) и организационно-методическим обеспечением. Эти службы немедленно предпринимают ответные

действия, направленные на отражение обнаруженной угрозы, которым можно дать следующее определение.

Средства реагирования – ресурсы системы физической защиты (технические, инженерные и иные средства и методы их использования) для реагирования на возможную или возникшую угрозу ООБ.

Силы реагирования – персонал службы безопасности и ресурсы, необходимые для реагирования на возможную или возникшую угрозу объекту обеспечения безопасности.

Также можно говорить и о методах реагирования, т. е. использовании соответствующих ресурсов и средств.

В эти определения осознанно включены не только персонал охраны, но и технические и инженерные средства, поскольку сейчас все большее распространение получают автоматизированные и автоматические средства реагирования на угрозы. Например, средства автоматизированного пожаротушения и дымоудаления или средства нелетального воздействия на нарушителя.

Контрольные вопросы к главе 1

1. Дайте мотивированное определение безопасности.
2. Перечислите основные аспекты понимания термина безопасность.
3. Объясните, чем отличаются термины безопасность и защищенность.
4. Объясните, каковы основные функции СБ.
5. Объясните, какова основная функция СБ и почему.
6. Дайте мотивированное определение системы безопасности.
7. Перечислите основные направления (прикладные задачи) обеспечения безопасности.
8. Перечислите основные технические средства обеспечения безопасности.

9. Поясните возможности использования основных технических средств обеспечения безопасности в различных прикладных задачах.
10. Каковы могут быть трактовки термина *физическая защита*.
11. Дайте мотивированные определения физической защиты и системы физической защиты.
12. Перечислите основные технические средства физической защиты объектов.
13. Расскажите, что такое ресурсы и средства реагирования.

2. ЗАДАЧИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

2.1. Основные задачи системы обеспечения безопасности

Рассмотрим, какие наиболее важные задачи должны решать системы безопасности по обеспечению безопасности объекта (рис. 3).

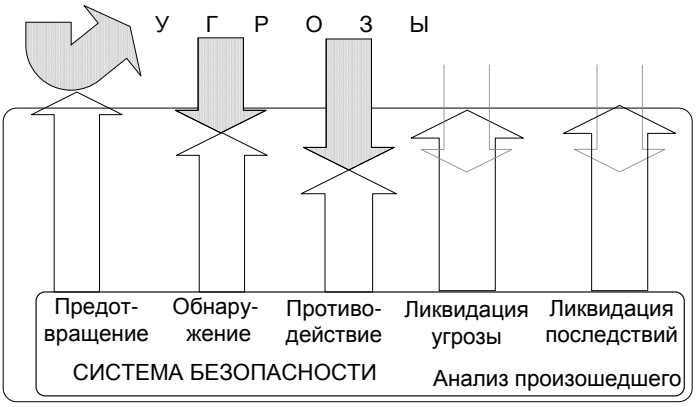


Рис. 3. Задачи системы безопасности

1. *Предотвращение угроз,* т. е. поддержание безопасного состояния или жизнедеятельности объекта обеспечения безопасности как идеальный вариант, к которому нужно стремиться, при котором отсутствуют потери или ущерб для ООБ. Это может достигаться различными методами и способами:
   - ликвидацией потенциальных источников угроз;
   - созданием условий, делающих невозможным реализацию угрозы, например использованием средств инженерной укрепленности объекта;
   - обнаружением угроз и их ликвидацией до непосредственного воздействия на объект и др.

2. *Обнаружение угроз* ООБ. Это важнейшая задача, без решения которой невозможно обеспечить безопасность объекта. Более того, обнаружение угроз должно быть реализовано по возможности раньше, чтобы можно было успеть принять действенные меры по ликвидации угроз и последствий от их реализации. Поэтому желательно решить задачу обнаружения либо на этапе подготовительных действий до начала реализации угрозы, либо до ее прямого воздействия на объект. Это даст возможность максимально эффективно начать противодействие им и свести к минимуму возможные последствия (потери).
3. *Противодействие угрозам*, позволяющее замедлить процесс их реализации и уменьшить уровень воздействия угрозы на объект, тем самым минимизировав последствия и потери, а также более эффективно предпринять действия по ликвидации угроз.

   Важно отметить, что противодействие реализующейся угрозе принципиально возможно не только после, но и до ее обнаружения. Так, использование негорючих материалов при строительстве замедляет процесс распространения пожара. И такие возможности надо использовать. Однако приоритетным является замедление развития угрозы именно после обнаружения. Тогда имеется больше времени на ее ликвидацию до нанесения существенного ущерба объекту.
4. *Ликвидация угроз* и прекращение процесса образования потерь, позволяющие свести к разумному минимуму последствия реализации угрозы и, следовательно, минимизировать возможные потери.
5. *Ликвидация последствий* реализации угрозы. Сюда можно отнести восстановление ООБ и восполнение различного вида потерь.

6. *Анализ произошедшего* в целях недопущения подобных ситуаций в будущем и более эффективной организации системы безопасности, включая:
   - ликвидацию или блокирование источников потенциальных угроз;
   - модернизацию системы (добавление новых средств обнаружения и т. п.);
   - модификацию методов использования системы, например реагирования на угрозы;
   - привлечение дополнительных ресурсов (к примеру, увеличение количества групп задержания).

Очевидно, что перечисленные задачи взаимосвязаны и требуют единого решения, учитывающего все особенности ООБ, возможных угроз и способов их реализации. Ясно также, что для решения этих задач необходимы разнообразные РСМ их применения. С этой точки зрения СБ в общем случае должна представлять собой совокупность технических, программных, организационных и всех других необходимых РСМ их использования.

Система безопасности может создаваться для уже существующего объекта. Но в идеальном случае она должна разрабатываться уже с началом создания самого ООБ – думать об обеспечении безопасности объекта надо уже с момента его проектирования, поскольку существует ряд угроз, которые нельзя или трудно будет учесть после завершения строительства. Например: возможность землетрясения, угрозы использования некачественных материалов или нарушения технологии строительства, угроза подготовки теракта на этапе строительства.

2.2. Этапы разработки системы безопасности

Для того чтобы решить задачу построения СБ, в общем случае необходимо, во-первых, сформулировать жизненно важные интересы или приоритеты; во-вторых, выявить воз-

можные угрозы, которые могут нанести ущерб этим жизненным приоритетам; в-третьих, выбрать, как и чем можно решить задачу обеспечения безопасности, и, наконец, оценить эффективность предложенного решения.

Таким образом, основные этапы разработки СБ в общем виде будут состоять в определении того:

- что защищать (четкая формулировка объекта обеспечения безопасности, т. е. жизненных приоритетов);
- от чего защищать (создание перечня угроз объекту обеспечения безопасности);
- чем и как защищать (выбор ресурсов, средств и методов обеспечения безопасности);
- а также в оценке эффективности выбранного решения (совокупности ресурсов, средств и методов их использования).

Эти этапы и последовательность их выполнения иллюстрируются на рис. 4.

После выполнения первых трех этапов производится оценка эффективности созданной системы безопасности по каким-либо критериям, например результативным или вероятностным, и при определенных ограничениях, к примеру, на стоимость.

На основании результатов оценки эффективности по выбранным критериям разработанное решение для СБ либо принимается, либо отвергается. В последнем случае в зависимости от причин такого решения происходит уточнение и корректировка данных, используемых на разных этапах разработки системы. Например, сокращаются или расширяются списки угроз, учитываемых при разработке, или выбираются другие технические решения.

Затем следует повторение всей процедуры или ее отдельных этапов.

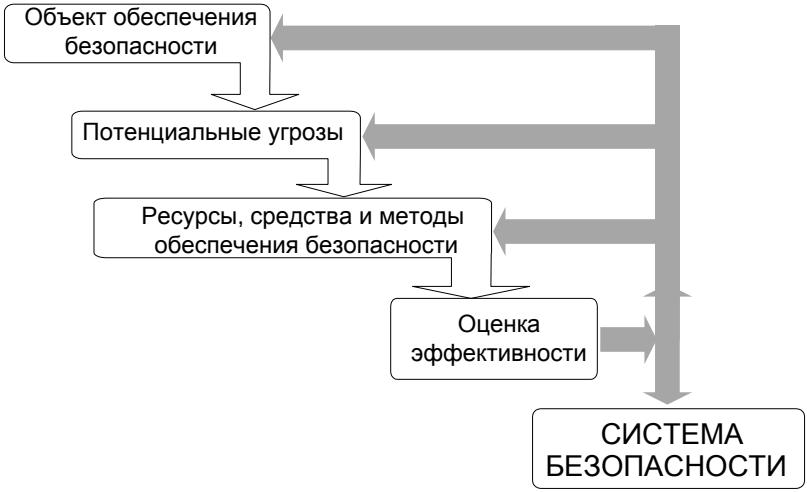


Рис. 4. Этапы разработки системы безопасности

К примеру, если принято решение не учитывать какую-либо угрозу, ранее включенную в список, то процедура должна повторяться, начиная с третьего этапа. А если сокращен перечень жизненных приоритетов, т. е. произошла корректировка ООБ (перечня жизненных приоритетов), то со второго.

2.3. Жизненные приоритеты

Выделенный первый этап последовательности решения задачи построения СБ состоит в необходимости определить, что защищать (формулировка объекта обеспечения безопасности). Очевидно, без знания того, что защищать, невозможно определить, от чего защищать и, тем более чем и как защищать. Поэтому первым шагом процесса создания СБ является анализ объекта защиты, т. е. отбор жизненно важных приоритетов.

Сформулируем, что может представлять собой ООБ. В самом общем виде угрозы могут быть:

- жизни и здоровью (конечно, в первую очередь человека, но не только его);
- среде обитания (ее состояние непосредственно влияет на безопасность жизни и здоровья, а зачастую и материальных ценностей);
- имуществу (движимому и недвижимому);
- информации (на любых носителях, включая каналы передачи информации и процессы);
- ресурсам (финансовым, природным, производственным, транспортным и др.).

В эти понятия вписываются практически все основные элементы ООБ. Очевидно, что на практике как сам список, так и содержание перечисленных выше приоритетов в каждом случае может быть различным и будет зависеть от конкретных задач и особенностей ООБ.

Общий список жизненных приоритетов должен в дальнейшем уточняться: определяется, что из этого общего списка предполагается включить в итоговый перечень приоритетов, т. е. что конкретно планируется защищать. К примеру, только материальное имущество. Далее список должен детализироваться. То есть уточняется, что в перечень этого имущества входят, например, только компьютеры и оргтехника.

В результате на начальном этапе должен быть составлен общий подробный список, который может включать в себя следующие перечисления.

Во-первых, непосредственно субъекты и объекты обеспечения безопасности:

- субъекты обеспечения безопасности (жители, сотрудники предприятия, обслуживающий персонал, посетители и т. п. категории людей);
- наиболее важные части или элементы объекта (например, серверная, склад готовой продукции и т. п.);

- дорогостоящее имущество и ресурсы, находящиеся на объекте (компьютеры и оргтехника, денежные средства, горючее и т. д.);
- информация, средства и каналы ее передачи (Интернет, проводная и беспроводная телефонная связь и т. д.), носители информации, средства обработки и т. п.;
- окружающая среда, включая представителей флоры и фауны;
- …

Во-вторых, все то, что прямо или косвенно может влиять на безопасность ООБ:

- пути и средства передвижения субъектов (маршруты и сооружения на этих маршрутах, автотранспорт, железнодорожный транспорт и т. д.);
- пути и средства перемещения (доставки или отправки) имущества и ресурсов (виды транспорта, способы упаковки, погрузки и т. п.);
- условия работы и другие факторы, влияющие на безопасность людей;
- состояние окружающей среды, ее параметры, влияющие на безопасность людей и объектов;
- средства жизнеобеспечения объекта (энергопитания, теплоснабжения, питания сотрудников и т. д.), влияющие на безопасность субъектов и безопасное функционирование объекта, а также способы и средства их транспортировки (кабельные сети, трубопроводы, автотранспорт и т. д.);
- социально-этнические и общественно-политические особенности региона, которые, например, могут привести к волнениям, демонстрациям, погромам;
- …

В-третьих, к этому списку следует отнести и саму систему безопасности в плане возможных угроз непосредственно СБ, а также угроз объекту, создаваемых системой

безопасности как при ее штатном функционировании, так и с точки зрения возможного использования против ООБ.

Очевидно, что каждый объект имеет свои специфические особенности, и на практике этот список может быть сокращен или дополнен и детализирован в дальнейшем. Кроме того, на формирование этого списка могут повлиять различные ограничения – финансовые, юридические, организационные и др. Поэтому затем из упомянутого общего списка выделяются те жизненные приоритеты, которые будут учитываться при разработке системы. Например, ставится задача обеспечения только безопасности людей (жизни и здоровья), а также материальных и информационных ресурсов. Тогда из списка могут быть исключены пути и средства передвижения и транспортировки и средства жизнеобеспечения, которые не входят в компетенцию разработчиков системы и на которые они не могут повлиять.

2.4. Потери

Как отмечалось выше, ущерб или потери для объекта, возникающие при реализации той или иной угрозы, могут существенно отличаться. Поэтому необходимы критерии отбора тех угроз, которые надо обнаружить и ликвидировать.

2.5. Уровень потерь

Для оценки уровня возможных потерь для ООБ при реализации какой-либо угрозы можно использовать следующие понятия.

Несущественные потери – это потери, не приводящие к сколько-нибудь существенному вреду жизненным интересам ООБ, т. е. те, которыми можно пренебречь; подобные потери можно называть также *приемлемыми*.

Существенные потери – это потери, приводящие к существенному вреду жизненным интересам ООБ.

Неприемлемые потери – это потери, приводящие к неприемлемому вреду жизненным интересам ООБ.

Уровень «существенности» и «неприемлемости» может быть различным в разных ситуациях. Так, потери в несколько десятков тысяч рублей будут существенными для большинства граждан. В то же время для крупной компании они будут несущественными. Угон единственной автомашины у гражданина будет существенным (или даже неприемлемым) для него, а для автопарка, в котором несколько сотен автомашин, такой ущерб может быть приемлемым. Поэтому рассматриваемая оценка существенности или неприемлемости должна выполняться с учетом конкретных задачи и ООБ.

Понятия существенности и несущественности зависят также и от вида ООБ. Так, если речь идет о жизни и здоровье человека, то и оценка степени существенности потерь должна быть совсем другой по сравнению со случаем материальных потерь. И в большинстве случаев такие потери считаются существенными и неприемлемыми.

2.6. Условные потери

Будем использовать нижеследующие понятия и обозначения возможных потерь:

$П_о$ – общие возможные потери для ООБ;

$П_j$ – потери, которые нанесены или могут быть нанесены *j*-й угрозой.

Также введем понятие *условных потерь* (или относительного ущерба) $У_j$, которое будем определять как отношение

$$У_j = П_j / П_о .$$

Тогда условные потери будут представлять собой нормированную величину с диапазоном значений от 0 (потерь нет) до 1 (потеряно все). Значение условных потерь $У_j$

применимо для оценки уровня существенности угрозы. В этом случае можно говорить о том, что если $У_j << 1$ или $У_j \to 0$, то ущерб несущественный. А при значении $У_j \to 1$ ущерб неприемлемый.

Знания одного значения условных потерь обычно не достаточно для принятия решения о необходимости учета угрозы. Так, в упоминавшемся примере с землетрясением возможный ущерб близок к единице. Но эту угрозу имеет смысл учитывать только в районах высокой сейсмоактивности, там, где вероятность реализации этой угрозы высока. Следовательно, необходим учет также и значения вероятности $P_у$ реализации угрозы.

Для оценки реальных условных потерь может быть использовано произведение $K = P_у \cdot У_j$ вероятности $P_у$ реализации угрозы за некоторый период времени на значение возможного условного ущерба $У_j$, наносимого такой угрозой. Конкретные промежуточные соотношения или граница между «несущественностью» и «неприемлемостью», как упоминалось выше, определяется с учетом условий каждой конкретной задачи.

2.7. Первичные и вторичные потери

Одним из основных критериев отбора существенных угроз является наносимый ими ущерб. С точки зрения полноты учета возможных потерь необходимо принимать во внимание не только возможные прямые потери, обусловленные непосредственно реализацией угрозы, но и вторичные, вызванные последствиями реализации этой угрозы или борьбы с ней при ее ликвидации. Так, пожар, кроме непосредственных потерь от сгоревшего имущества, может привести и к потерям в непрерывности производственного процесса с соответствующими дополнительными экономическими потерями и потерями от заливки объекта водой при тушении пожара. И такие вто-

ричные потери в ряде случаев могут существенно превышать первичные (прямые). Поэтому при анализе возможных потерь от последствий реализации угрозы необходимо обязательно учитывать как первичные, так и вторичные потери.

2.8. Риски

В зависимости от реальных условий любая потенциальная угроза может как реализовываться, так и не реализовываться. Поэтому можно говорить о необходимости учета вероятности реализации той или иной угрозы, иными словами, о риске реализации угрозы.

Кроме того, нужно говорить и о том, что в результате реализации угрозы возникает риск тех или иных потерь для субъекта или объекта обеспечения безопасности. Отсюда вытекает следующее определение понятия риска.

Риск – это возможность реализации угрозы, приводящей к тому или иному уровню потерь для объекта обеспечения безопасности.

При реализации угрозы потери могут и не возникнуть или оказаться приемлемыми. Например, если при своевременном обнаружении возгорания система автоматизированного пожаротушения ликвидировала очаг возгорания на начальной стадии, то потери могут быть минимальными (приемлемыми). Поэтому можно говорить о следующих основных видах рисков:

- реализации угроз;
- возникновения потерь при реализации угрозы.

Риск может быть оценен значением вероятности P_y реализации угрозы и уровнем $П_j$ возможных потерь от ее реализации или, что обычно удобнее, уровнем условных потерь $У_j$.

Заметим, что влиять на уровень риска реализации угрозы сложно или не всегда возможно. А уменьшить риск возникновения потерь, как правило, вполне реально. Например, по-

влиять на риск реализации такой угрозы, как попадание молнии в здание или сооружение, практически невозможно, при этом риск возникновения потерь весьма велик. Однако уменьшить уровень возможных потерь достаточно просто установкой молниеотводов.

Риск возникновения потерь при реализации угрозы можно разделить на два вида:

- до создания системы безопасности;
- после создания системы безопасности.

Такое деление может характеризовать риск возникновения потерь для объекта, соответственно, не оборудованного и оборудованного системой обеспечения безопасности. Первый важен, прежде всего, при проектировании СБ, т. е. при отборе существенных угроз и выборе необходимых методов и средств их обнаружения и ликвидации. Второй вид риска может служить мерой, во-первых, степени опасности реализации соответствующей угрозы и, во-вторых, мерой оценки эффективности созданной СБ. Для этого надо сравнить или риски до и после создания СБ, или возможные потери до и после реализации системы.

Кроме того, применительно к ряду угроз криминального, террористического характера или вандализма можно говорить и о *риске безнаказанности выполнения несанкционированных действий*.

При выполнении этапов разработки СБ, реализации системы и в процессе ее функционирования могут возникать и другие риски, приводящие к тем или иным ошибкам или возникновению ситуаций, в которых СБ не выполнит своих функций. Поэтому также надо иметь в виду следующие риски, связанные непосредственно с процессом разработки и реализации самой СБ и процесса ее функционирования.

- Технический – возможность отказа СБ как совокупности технических, программных и других средств и, как следст-

вие, необнаружение угрозы и (или) невозможность ликвидировать угрозу.

- Непредсказуемый, т. е. риск непредсказуемого развития ситуации при реализации какой-либо угрозы. Так, при проникновении преступников на объект в целях хищения может оказаться, что на нем находятся люди. Поэтому реализация угрозы материальных потерь может привести к угрозе жизни и здоровью людей как свидетелей преступления. Другой пример – риск падения самолета на здание. Можно учесть такой риск расчетом прочности, чтобы не произошло разрушение всего объекта. Но непредсказуемым могут оказаться последствия возникшего пожара и горение большого количества топлива, находившегося в баках самолета.
- Осознанный, при сознательном отказе на этапе анализа от:
  - обеспечения безопасности того или иного жизненно важного интереса;
  - учета какой-либо угрозы.
- Заданный – взятый за основу возможный риск реализации угрозы и уровень последствий (потерь) при этом. К примеру, принятие приемлемым риска потери при пожаре только имущества, находящегося на складе, и отказ от системы автоматизированного пожаротушения может привести к существенно бóльшим потерям за счет разрушения строительных конструкций склада при горении с высокой температурой и, следовательно, потери самого здания.
- Системный, связанный с угрозами, создаваемыми самой СБ при ее функционировании и внештатных ситуациях. Например, неправильный учет пропускной способности точек контроля доступа на стадион может привести к давке и гибели людей, а на предприятии – к потерям рабочего времени сотрудников. А незнание сотрудников, как вести себя при срабатывании системы оповещения при запуске

системы газового или порошкового пожаротушения, создает угрозу их жизни.

- Субъективный, так называемый «человеческий фактор», включающий разные составляющие:
  - неправильный выбор состава и типа оборудования;
  - ошибки монтажа и программирования параметров системы и т. п. вследствие небрежности или недостаточной квалификации;
  - неправильное или нецелевое использование оборудования СФЗ;
  - умышленные или случайные неправильные действия.

Перечисленные риски дополнительно свидетельствуют о важности полноты учета рисков возникновения всех реальных и потенциально возможных угроз при разработке СБ любого объекта.

Контрольные вопросы к главе 2

1. Перечислите основные задачи системы обеспечения безопасности и проиллюстрируйте на примерах.
2. Перечислите и объясните основные этапы разработки системы безопасности.
3. Расскажите, что такое жизненные приоритеты.
4. Расскажите, что такое потери.
5. Расскажите, что такое уровень потерь.
6. Расскажите, что такое условные потери.
7. Объясните, что такое первичные и вторичные потери.
8. Объясните, что такое риски и какие они бывают.
9. Объясните, что такое технический риск.
10. Объясните, что такое непредсказуемый риск.
11. Объясните, что такое осознанный риск.
12. Объясните, что такое заданный риск.
13. Объясните, что такое системный риск.
14. Объясните, что такое субъективный риск.

3. УГРОЗЫ

Сформулируем понятие угрозы для субъекта или объекта обеспечения безопасности и выберем критерии их оценки и отбора в список угроз, которые надо учитывать при разработке СФЗ.

В литературе используются различные определения угроз. В самом общем виде можно говорить, что *угроза* – это события, действия, процессы и т. п. факторы, приводящие к возможности возникновения ситуации, при которой происходит нарушение состояния защищенности объекта обеспечения безопасности и, следовательно, к возможности нанесения ему ущерба (т. е. того или иного уровня потерь).

Поэтому можно говорить о том, что *угроза* – это нечто или некто, угрожающее ООБ и способное нанести ему ущерб. «Нечто или некто» может быть самым разным: природным явлением, пожаром, человеком, социальным или этническим конфликтом, технологическим процессом, экономической или политической ситуацией и т. д.

Учитывая это, можно дать следующее определение угрозы.

Угроза – это потенциальная возможность нанесения потерь объекту обеспечения безопасности.

3.1. Степень опасности угроз

Различные угрозы представляют разную степень опасности для ООБ с точки зрения возможного ущерба, который может иметь место при реализации каждой угрозы. Поэтому наличие той или иной угрозы для ООБ само по себе еще не достаточно для принятия решения о том, нужно ли ее учитывать при разработке СБ или нет. Среди общего списка многочисленных угроз можно выделить угрозы с меньшей или большей вероятностью их реализации. Например, вероят-

ность кражи выше на первых этажах зданий в магазинах с большими застекленными окнами, там, где, разбив стекло, можно быстро совершить кражу и скрыться с места преступления. А вероятность такой угрозы как землетрясение весьма высока в районах высокой сейсмической активности и мала в регионах с низкой сейсмоактивностью.

С этой точки зрения первым критерием для отбора (учета) угрозы может служить вероятность ее реализации. Поэтому имеет смысл ввести такой термин, как реальная угроза.

Реальная угроза – это угроза, вероятность реализации которой высока.

Знания только вероятности реализации угрозы недостаточно для принятия решения об ее учете при разработке СБ. Необходимо учитывать также уровень возможных потерь при ее реализации. Очевидно, что в первую очередь имеет смысл учитывать угрозы, приводящие к существенным потерям для ООБ. Например, на складе автопокрышек угроза возникновение протечки не приведет к сколько-нибудь существенным потерям. В то же время в библиотеке или на складе канцелярских товаров протечка приведет к значительным материальным потерям. Следовательно, в первом случае такую угрозу можно и не учитывать, а во втором целесообразно учесть необходимость ее обнаружения (например, установкой датчиков влажности).

Поэтому вторым критерием отбора угрозы может служить уровень возможного ущерба или потерь, наносимых этой угрозой тому или иному объекту. С этой точки зрения полезным будет термин существенная угроза.

Существенная угроза – это угроза, при реализации которой потери для объекта обеспечения безопасности могут быть существенными.

Ясно, что эти критерии (вероятность реализации и уровень возможных потерь) могут и должны анализироваться и учитываться как вместе, так и по отдельности. Например,

кража может быть совершена с достаточно высокой вероятностью, и потери могут быть заметными. Такая угроза обычно учитывается. Вероятность пожара достаточно низка, но потери от него могут быть очень большими, можно потерять все: и имущество, и здание, и, что наиболее важно, жизнь и здоровье людей. Поэтому такая угроза практически всегда должна учитываться. А в ряде случаев необходимость ее учета закреплена законодательно и не подлежит обсуждению.

3.2. Особенности реализации угроз

Очевидно, что значение наносимых угрозой потерь может быть различным не только при реализации разных угроз, но и при разных способах реализации одной и той же угрозы. Поэтому учет способа реализации угрозы важен, прежде всего, с точки зрения правильности выбора конкретных средств обнаружения этой угрозы. Обнаружение одной и той же угрозы при разных способах ее реализации может потребовать несколько различных устройств обнаружения, следовательно, и разного состава и структуры СБ.

Последствия для ООБ (потери) при разных способах реализации одной и той же угрозы могут быть как одними и теми же, так и различными. Поэтому с точки зрения решения задачи синтеза СБ очень важен не только перечень реальных и существенных угроз, но и анализ способов реализации каждой из составленного списка этих угроз. От этого в существенной степени будут зависеть требуемые параметры и характеристики проектируемой СБ.

3.3. Типы угроз

Угрозы можно классифицировать по различным признакам, например, по расположению источника угроз, по способу воздействия на ООБ и по многим другим.

Внешние и внутренние угрозы

Внешние – это угрозы объекту обеспечения безопасности, источник которых находится вне объекта обеспечения безопасности.

Внутренние – это угрозы, источники которых находятся внутри самого объекта.

Первичные и вторичные угрозы

Первичные – это угрозы, непосредственно воздействующие на объект обеспечения безопасности и приводящие к потерям.

Вторичные – это угрозы, создаваемые последствиями реализации другой первичной угрозы. Поскольку к понятиям первичной и вторичной угроз применимо деление на внешние и внутренние, то возможны различные сочетания первичных внутренних и внешних и вторичных внутренних и внешних.

Прямые и опосредованные угрозы

Прямые – это угрозы, воздействующие непосредственно на объект обеспечения безопасности или его составные части.

Опосредованные – это те угрозы, которые воздействуют на цель не непосредственно, напрямую, а через другие элементы объекта или окружающей среды, т. е. через некоторый вторичный, специально используемый, источник угроз.

Вторичные и опосредованные угрозы являются схожими, и в обоих случаях возникает новая угроза, являющаяся последствием реализации другой угрозы. Отличие состоит в том, что опосредованная угроза создается специально для реализации вторичной угрозы определенного характера, направленной против объекта, т. е. это угрозы, продуманные заранее.

Отвлекающие угрозы

Отвлекающие – угрозы, в задачу которых входит отвлечь внимание средств реагирования от основной, реальной угрозы для обеспечения достижения цели. Иными словами, создаваемые для определенного воздействия либо на объект обеспечения безопасности, либо на систему безопасности с целью обеспечить возможность эффективной реализации основной угрозы.

3.4. Источники угроз

Для составления общего перечня угроз объекту целесообразно выполнить анализ не только очевидных угроз, но и возможных источников потенциальных угроз. В общем случае источники угрозы можно объединить в следующие основные группы (рис. 5): криминогенные, террористические, техногенные, природные, экономические, информационные, субъективные, социально-этнические, общественно-политические и многие другие. Этот перечень, к сожалению, постоянно пополняется и расширяется.

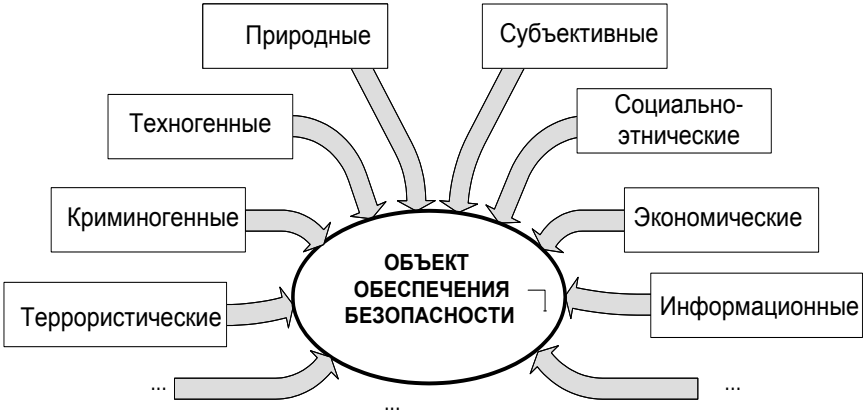


Рис. 5. Источники угроз

При этом надо понимать следующее.

Во-первых, одна и та же угроза может возникать из различных источников. Например (рис. 6), возгорание и пожар могут возникнуть как результат поджога (источник криминальный или террористический), неисправности электропроводки или оборудования (технические неисправности), небрежности человека (субъективный фактор) или удара молнии (природное явление).

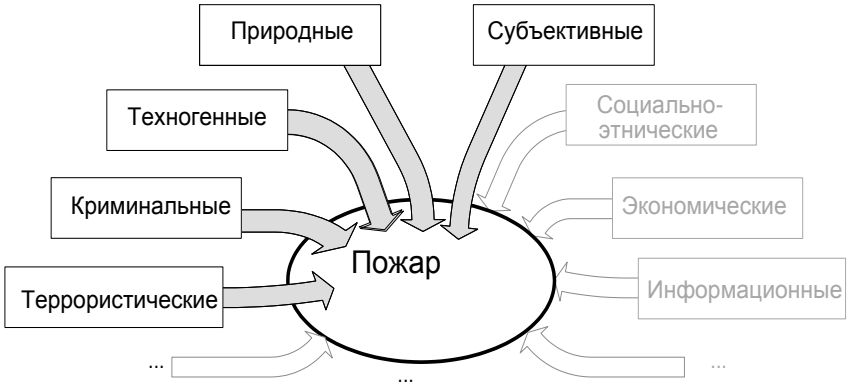


Рис. 6. Источники возникновения пожара

Другой пример – утечка газа может быть следствием реализации угроз из различных источников: криминального (несанкционированная врезка в газопровод); террористического (умышленное повреждение с конечной целью достижения не только политического эффекта и экономических потерь, но и взрыва и пожара, приводящих к людским потерям); технического (некачественный шов или неисправная арматура); природного (повреждение трубопровода в результате землетрясения); субъективного (халатность при проведении земляных работ, приводящая к повреждению трубы).

При этом последствия (потери) во всех случаях могут быть как одними и теми же, так и существенно различными.

Во-вторых, один источник может создавать несколько угроз. Например, угрозами криминального характера могут быть кража, ограбление, мошенничество и др.

И, в-третьих, новым источником ряда угроз могут служить результат реализации другой угрозы. Так, в предыдущем примере утечка газа ведет к новым угрозам – взрыва и пожара или отравления людей.

3.5. Виды угроз

К наиболее типичным и опасным можно отнести следующие основные виды угроз из упомянутых выше.

Криминогенные

Это достаточно распространенные угрозы, такие как:

- кража (тайное хищение чужого имущества);
- грабеж (хищение чужого имущества, совершенное открыто, в присутствии владельца, без насилия над личностью или с насилием, которое не опасно для жизни и здоровья);
- разбой (нападение в целях хищения чужого имущества, сопряженного с применением опасного для жизни или здоровья насилия либо угрозой его применения);
- мошенничество;
- подкуп сотрудников предприятия, персонала охраны, служб доставки и др.;
- запугивание, шантаж сотрудников;
- сговор с работающими на предприятии или охраной и т. п. угрозы.

Экономические

Сюда можно отнести угрозы:

- преступлений, связанных, к примеру, с некорректной конкуренцией и имеющих целью нанесение прямого материального ущерба;.

- происшествий, приводящих к нарушению непрерывности бизнеса, что косвенно ведет к материальным потерям;
- происшествий, приводящих к потере репутации компании, влияющей на экономические показатели;
- информационной безопасности, нарушение которой часто влечет как вторичную угрозу, так и материальные потери;
- другие подобные угрозы. Например, при выводе из строя сетевого сервера или сборочного конвейера будут иметь место не только прямой материальный ущерб (непосредственно стоимость поврежденного оборудования), но и вторичные косвенные – потери времени и ресурсов на восстановление, упущенная выгода от остановки производства, потеря репутации компании от срыва поставок и т. п.

Вандализм

Представляет собой умышленное и бессмысленное повреждение и уничтожение культурных, материальных ценностей и информационных ресурсов.

Террористические

Это предумышленное, политически мотивированное насилие, совершаемое против мирного населения или объектов обычно с целью повлиять на настроение общества, на принятие решений органами государственной власти, связанное с устрашением населения, которое может реализовываться в виде террористических актов с применением различной тактики и средств. Например:

- с использованием смертников;
- без использования смертников (закладка и подрыв дистанционно управляемого фугаса, распыление отравляющих веществ, …);
- с применением собственных транспортных средств (машина начиненная взрывчаткой);

- с силовым захватом транспортных средств (например, самолета);
- с использованием в качестве инструмента реализации теракта взрывчатых или отравляющих веществ, транспортных средств, оружия;
- и другими, приводящими, как правило, к неприемлемым, трагическим потерям.

Информационные

Это угрозы, связанные с возможными утечками информации, ее несанкционированным использованием, модификацией и уничтожением:

- съем информации по различным каналам утечки с последующим ее использованием для несанкционированных действий;
- модификация информации с той или иной целью;
- уничтожение информации;
- несанкционированное использование информации для нанесения потерь объекту защиты и т. д.

Природные

Подобные угрозы вызваны различными природными явлениями, такими как:

- наводнение;
- землетрясение;
- извержение вулкана, приводящее к возникновению ряда угроз (выброс лавы, пиропластические потоки, выброс пепла в атмосферу, который может привести к выходу из строя авиационных двигателей и др.);
- цунами;
- удар молнии, повлекший механические повреждения конструктивных элементов и, как вторичную угрозу, – пожар;
- туман – серьезная причина возникновения угрозы безопасности полетов в аэропорту;

- магнитные бури, приводящие к выводу из строя некоторых систем связи;
- другие явления, которые могут в той или иной мере нанести непосредственный ущерб объекту или повлиять на режим его функционирования.

Вероятность реализации той или иной угрозы, упомянутой выше, будет существенным образом зависеть от региона и места нахождения конкретного объекта.

Техногенные

К ним относятся угрозы техногенного характера:

- неисправность (поломка) оборудования;
- ошибки при проектировании или производстве оборудования;
- сбои программных средств;
- потеря оборудованием своих технических свойств в результате старения или внешнего воздействия на него (например, коррозии), которые могут приводить к возникновению потерь практически любого уровня.

Системные

Имеется несколько видов таких угроз.

Угрозы системе безопасности. Представляют собой обычно один из способов предварительной подготовки преступления. Но могут быть вызваны и неправильными проектированием, установкой, программированием или эксплуатацией, например:

- случайное или умышленное механическое или электрическое повреждение элементов системы;
- несанкционированное изменение, перепрограммирование параметров и характеристик элементов системы;
- блокирование и маскирование устройств обнаружения, делающее невозможным выполнение ими своих функций по обнаружению;

• обесточивание системы безопасности

и т. п. угрозы, при которых СФЗ или ее отдельные элементы, например устройства обнаружения, полностью или частично не выполняют своих функций.

Угрозы, создаваемые системой безопасности. Как и любая технически сложная система, сама СБ может служить источником ряда угроз для ООБ. К ним можно отнести угрозы, создаваемые:

- средствами противодействия (к примеру, подсистемой автоматизированного газового пожаротушения, ...);
- непредвиденными нарушениями режима функционирования СБ за счет неправильного выбора параметров системы;
- нарушением режима функционирования СБ за счет сбоев в работе системы;
- угрозами умышленного использования СБ для нанесения ущерба ООБ.

Очевидно, что рассмотренные примеры не исчерпывают всех реальных ситуаций. Список возможных угроз, к сожалению, постоянно расширяется и может быть продолжен или сокращен в каждой конкретной задаче.

3.6. ЗАДАЧА И ЦЕЛЬ УГРОЗЫ

Введем понятия цели и задачи угрозы.

Цель угрозы

В общем случае под термином *цель* будем понимать ту составляющую, элемент или часть объекта обеспечения безопасности, на которую может воздействовать угроза и непосредственно которой может быть нанесен ущерб.

Если говорить о таких угрозах, как криминальные или террористические, то под понятием цели будем понимать прямое толкование этого слова – людские, материальные или информационные ресурсы. К примеру, целью кражи может

быть персональный компьютер и другая дорогостоящая оргтехника.

Для некоторых других видов угроз (например, природных) под целью будем понимать ту часть объекта или субъекта обеспечения безопасности, которым может быть нанесен вред этой угрозой. Для такой угрозы, как пожар, цель – это практически все здание и имущество, а также люди. Цель такой угрозы, как землетрясение, – это здание (как первичная цель), а затем и материальные ресурсы и люди (как вторичная, обусловленная разрушением здания).

Задача угрозы

Понятие цели применимо ко всем угрозам, но понятие *задачи* можно использовать только для угроз, реализуемых преступником. Если говорить об источниках угроз, связанных с участием преступников, то их задачи могут существенно отличаться, даже если цель одна и та же. Например, цель кражи (получение материальной выгоды) реализуется, если преступник не только достиг объекта, но и вышел за пределы досягаемости сил реагирования, когда он остался безнаказанным.

Поэтому в общем случае достижение цели угрозой еще не достаточно для нанесения существенного ущерба объекту. Так, в случае кражи существенных потерь можно избежать, задержав преступника практически на любом этапе противоправных действий, в том числе при отходе с места преступления или даже после выхода из здания, вернув имущество, которое преступник пытался похитить. И потери могут быть минимальными, приемлемыми – материальное имущество возвращается. Хотя могут быть потери от повреждения дверей, окон и других элементов конструкции здания, через которые имело место несанкционированное проникновение при совершении кражи. Эти примеры показывают, что наносимый

ущерб может быть различным при нейтрализации угрозы на разных этапах ее развития.

При других видах криминальных преступлений – в случае грабежа или разбойного нападения – ущерб будет определяться не только потерей материальных ценностей, но и возможным нанесенным вредом здоровью потерпевшего. Поэтому, несмотря на то, что при своевременном задержании преступника после совершения преступления задача последнего не решена, существенные или неприемлемые потери для объекта все равно могут иметь место.

Аналогичная ситуация будет и с рядом преступлений экономического характера, но здесь преступник, как и при краже, обычно ставит задачу выхода из зоны досягаемости в прямом либо в переносном смысле (старается остаться необнаруженным).

В случае вандализма или терроризма уже само достижение преступником цели обычно позволяет ему решить поставленную задачу. Цель несанкционированных действий будет достигнута уже до отхода преступников, и потери могут быть существенными и даже неприемлемыми. Например, вандал разобьет скульптуру или террорист-смертник подорвет себя в толпе людей. Задержание преступника, если оно будет возможно, уже не меняет ситуацию – объект понесет существенные или неприемлемые потери. Система безопасности в этом случае может лишь помочь свершить правосудие, а это тоже немаловажно.

Заметим, что ряд преступлений может решаться и без непосредственного проникновения на объект. Прекращением поставок электроэнергии на объект, задержкой поставки комплектующих или съемом конфиденциальной информации по тем или иным каналам утечки (например, каналам беспроводной телефонии) с последующим ее использованием можно нанести существенный ущерб.

Еще один случай, отличающийся от предыдущих, может иметь место, когда у преступника есть официальный доступ на объект, т. е. источник угрозы находится на самом объекте, например, подкупленный или запуганный сотрудник предприятия. В этом случае несанкционированного проникновения может не потребоваться, если упоминавшийся сотрудник имеет официальный доступ к цели преступления. Речь может идти только об обнаружении несанкционированных действий в процессе их выполнения и задержании при отходе или впоследствии – после обнаружения факта несанкционированных действий. Более того, если несанкционированные действия не обнаружены в момент их выполнения, то позже можно либо совсем их не заметить, либо выявить через какое-то определенное время. Пример – копирование конфиденциальной документации с последующим выносом ее или передачей по каналам связи.

Таким образом, в разных случаях цель и задача преступника, методы его действий и используемые им средства или проявления каких-либо других угроз могут существенно отличаться, что требует различных МСОБ, в частности выбора специфических средств обнаружения несанкционированных действий и организации адекватного реагирования. Поэтому при построении СБ необходим не просто тщательный и всесторонний анализ угроз, но и учет особенностей реализации этих угроз, поскольку от этого в существенной степени будут зависеть требуемые параметры и характеристики проектируемой СБ.

Контрольные вопросы к главе 3

1. Расскажите, что такое угрозы.
2. Объясните и проиллюстрируйте на примерах степень опасности угроз.
3. Объясните важность учета особенностей реализации угроз и проиллюстрируйте на примерах.

4. Перечислите основные типы угроз. Приведите примеры.
5. Перечислите основные источники угроз. Приведите примеры.
6. Перечислите основные виды угроз из разных источников. Приведите примеры.
7. Приведите примеры криминогенных угроз.
8. Приведите примеры экономических угроз.
9. Приведите примеры террористических угроз.
10. Приведите примеры техногенных угроз.
11. Приведите примеры природных угроз.
12. Объясните, что такое угрозы, создаваемые системе и системой безопасности.
13. Расскажите, что такое задача и цель угрозы. Приведите примеры.

4. ВОЗДЕЙСТВИЕ УГРОЗЫ НА ОБЪЕКТ

Как уже отмечалось, угрозы могут классифицироваться по различным признакам, таким как место нахождения источника угрозы относительно ООБ, взаимосвязь угрозы с другими угрозами, особенности возникновения и реализации и многим другим. Рассмотрим этот вопрос подробнее.

4.1. ВНЕШНИЕ И ВНУТРЕННИЕ УГРОЗЫ

Угрозы могут подразделяться по месту нахождения их источника.

Внешние – это угрозы объекту обеспечения безопасности, источник которых находится вне объекта обеспечения безопасности (рис. 7). Это могут быть криминогенные (кража, нападение), террористические, угрозы природного характера (наводнение, удар молнии) и др.

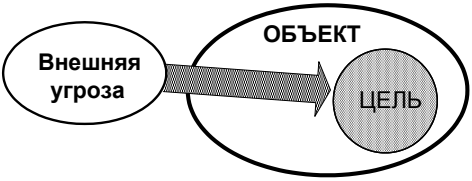


Рис. 7. Внешняя угроза

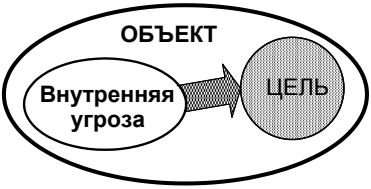


Рис. 8. Внутренняя угроза

Внутренние угрозы – это угрозы, источники которых находятся внутри самого объекта (рис. 8). Например, угрозы,

вызванные техническими неисправностями технологического оборудования или систем автоматизации здания, которые могут привести к материальным потерям и к нанесению вреда здоровью работающих; или угрозы, обусловленные так называемым человеческим фактором – ошибочными действиями персонала.

Одна и та же угроза (как внутренняя, так и внешняя) может воздействовать на несколько целей (рис. 9). Например, одна такая угроза как пожар создает угрозы практически всем элементам ООБ. И такая угроза может быть как внутренней (к примеру, пожар, вызванный неисправностью электропроводки в квартире), так и внешней (причина возгорания – пожар в соседнем помещении).

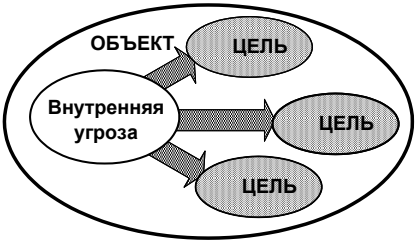


Рис. 9. Одна внутренняя угроза нескольким целям

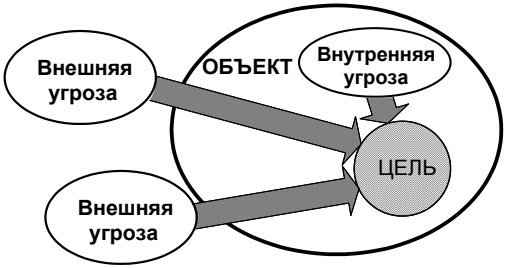


Рис. 10. Несколько угроз одной цели

Возможны варианты нескольких различных угроз одной и той же цели (рис. 10). Так, одно и то же имущество можно

потерять по различным причинам: вследствие реализации кражи, пожара, протечки и ряда других, как внешних, так и внутренних, угроз. Угроза выхода из строя технологического оборудования может быть следствием его старения или преждевременного износа по причине выполненного либо не вовремя, либо не в полном объеме, либо некачественного технического обслуживания этого оборудования (первичный источник угрозы – субъективный, а именно человеческий фактор). Это может привести к ускоренному старению и выходу из строя оборудования с последующим возникновением вторичных угроз.

4.2. Первичные и вторичные угрозы

С точки зрения последовательности их воздействия на ООБ угрозы могут подразделяться на первичные и вторичные.

Первичные – это угрозы, непосредственно воздействующие на цель и приводящие к потерям (см. рис. 7–10). Например, пожар непосредственно может приводить к потерям людских, материальных и информационных ресурсов.

Вторичные – это угрозы, вызванные последствиями реализации другой угрозы (рис. 11). Так, при ликвидации такой угрозы, как пожар, сам процесс тушения пожара или срабатывание системы автоматизированного пожаротушения может привести к реализации вторичных угроз, например, к существенным протечкам в другие помещения, не затронутые пожаром, которым по этой причине будет нанесен ущерб. Другая вторичная угроза в этом примере: выделение ядовитых продуктов горения при пожаре может быть причиной значительно больших неприемлемых потерь – человеческих жертв.

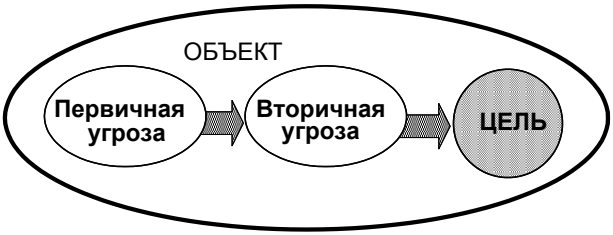


Рис. 1.11. Вторичные угрозы

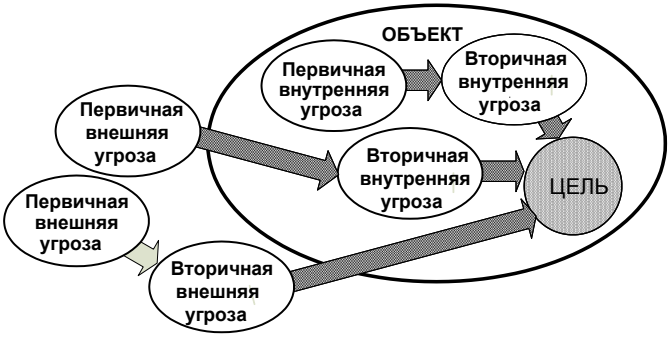
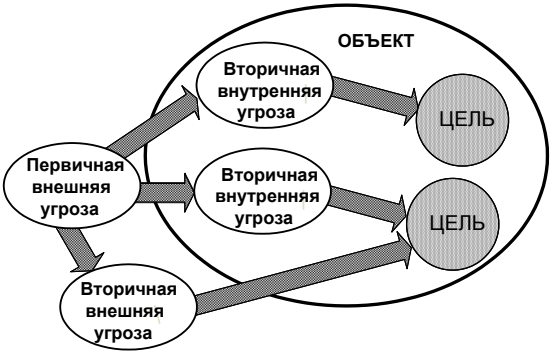


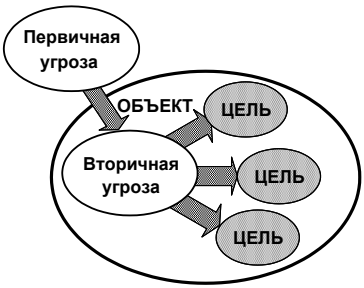
Рис. 12. Внешние и внутренние вторичные угрозы

К понятиям первичной и вторичной угроз применимо деление их на внешние и внутренние, поэтому возможны различные сочетания первичных внутренних и внешних и вторичных внутренних и внешних угроз (рис. 12).

Одна первичная угроза может приводить к возникновению нескольких других угроз (рис. 13, *а*, *б*), воздействующих как на одну, так и на несколько целей. Так, утечка газа из газопровода может привести к появлению нескольких видов угроз: отравления газом, возникновения пожара и взрыву – и, как следствие, к угрозам жизни и здоровью людей, а также к материальным и экологическим потерям.



а)



б)

Рис. 13. Первичные и вторичные угрозы: *а* – возникновение вторичных угроз одной цели; *б* – воздействие одной угрозы на несколько целей

Вышеприведенные примеры сочетаний различных угроз свидетельствуют о возможности возникновения на практике и других ситуаций. А это еще раз подчеркивает важность тщательного анализа всех источников, видов и особенностей реализации угроз, позволяющего предусмотреть возможность их обнаружения и противодействия им.

4.3. Прямые и опосредованные угрозы

Прямые и опосредованные угрозы в определенной степени похожи на первичные и вторичные – они различаются порядком воздействия на цель.

Прямые – это угрозы, воздействующие непосредственно на цель (см. рис. 7–10).

Опосредованные угрозы – это те, которые воздействуют на цель не непосредственно, напрямую, а через другие элементы объекта или окружающей среды (рис. 14), через некоторый вторичный, специально используемый или созданный источник угроз. Например, чтобы нанести материальный ущерб, не обязательно проникать на объект. Вывод из строя каналов подачи электроэнергии на объект может привести к прекращению работы холодильных камер и порче продуктов.

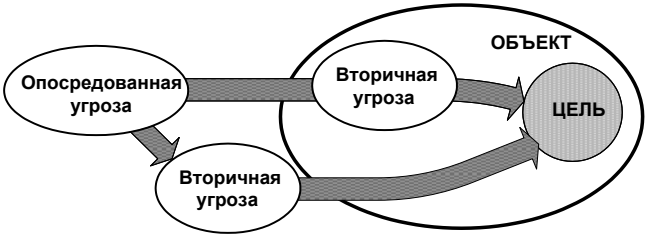


Рис. 14. Опосредованная угроза

Вторичные и опосредованные угрозы являются схожими. В одном и в другом случае в результате реализации специально организованной первичной угрозы возникает новая конкретная вторичная угроза. Таким образом, опосредованная угроза также является вторичной. Разница между опосредованными и вторичными угрозами состоит в том, что опосредованные – это продуманные заранее угрозы, реализация которых вызывает вполне определенные потери для ООБ. В отличие от опосредованной, вторичная угроза непосредственно (по замыслу) не связана с первичной (хотя и может быть спрогнозирована).

Опосредованная вторичная угроза может быть многоступенчатой, когда создается последовательность из нескольких угроз. Так, упомянутое отключение электроэнергии может привести к прекращению работы системы охлаждения серверной и в свою очередь к выходу из строя самих серверов с соответствующими последствиями в прерывании бизнеса и угрозе информационных потерь.

Другим примером может служить следующая ситуация. По причине поджога (внешняя прямая угроза) возникло возгорание. Срабатывание системы пожарной сигнализации привело отключению (разблокированию) системы контроля доступа и, следовательно, к возможности несанкционированного проникновения на объект. В этом случае пожар, как первичная угроза, послужил причиной возникновения вторичной опосредованной угрозы несанкционированного проникновения.

4.4. Отвлекающие угрозы

Организация прямой или опосредованной угрозы объекту не обязательно ставит целью нанесение ему прямого ущерба. Это может быть ложная, отвлекающая угроза, используемая для нарушения режима функционирования объекта, которое в свою очередь позволит упростить достижение реальной цели.

Отвлекающие угрозы создаются обычно специально, чтобы отвлечь от основной угрозы силы реагирования СБ. Например, чтобы увеличить задержку прибытия группы задержания на объект путем организации ложного вызова (ложной тревоги на другом объекте). Отвлекающие угрозы могут быть и случайными, не организованными специально. Например, пожарная тревога с последующей эвакуацией сотрудников и покупателей может подтолкнуть кого-либо на кражу имущества.

Таким образом, отвлекающая угроза может непосредственно и не приводить к какому-либо ущербу для ООБ, а только имеет целью отвлечь силы реагирования.

4.5. Модели нарушителя

Одним из основных источников угроз ООБ является тот или иной вид несанкционированных действий нарушителей. Поэтому учет такой угрозы является обязательным практически в любой СБ. Нужно понимать, что конкретный способ реализации такой угрозы и, следовательно, характер ее проявления при несанкционированных действиях будет существенно зависеть от квалификации и оснащенности нарушителя(ей) и тактики его(их) действий. Для учета этих особенностей необходимо сформулировать модель нарушителя(ей), учитывающую наиболее полно и точно его(их) возможное поведение при выполнении им(ими) несанкционированных действий. Общие вопросы разработки модели нарушителей рассмотрены в ряде работ, например в [33–35].

Одна из типичных моделей использует деление нарушителей на три основные категории:

- неподготовленный (неквалифицированный);
- подготовленный (квалифицированный);
- высококвалифицированный.

Неподготовленный нарушитель действует без априорной информации об объекте и системе безопасности. Такой нарушитель вероятнее всего будет проникать через наиболее уязвимые места объекта, например, через двери, открывая или взламывая их, либо через окна, разбивая стекла. Обычно он не имеет конкретной цели и действует спонтанно. Например наркоман, которому для покупки дозы наркотиков необходимы либо деньги, либо какое-нибудь имущество, которое можно быстро и просто продать.

Подготовленный нарушитель обладает некоторыми подручными средствами (инструментами, лестницей,…) и некоторой априорной информацией об объекте (к примеру, о наличии привлекательных материальных или финансовых средств), а также о СБ (например, такой, как базовые знания о принципах функционирования СБ и, в частности, средств обнаружения (СО)). Зная о возможном наличии СБ, он будет искать также и менее защищенные средствами обнаружения и технической укрепленности места. Например, двери и окна обычно в первую очередь блокируются магнитоконтактными датчиками. Поэтому преступник с большей вероятностью будет вынимать или вырезать стекло или проем в двери, чтобы не нарушить состояние магнитоконтактного датчика, или проламывать пол, потолок или стены (если, конечно, позволят условия). Подготовленный нарушитель имеет, как правило, конкретные цель и задачу, а также предварительно выбранную тактику действий.

Высококвалифицированный нарушитель владеет существенной априорной информацией как об объекте, так и о системе безопасности, включая знание ее основных параметров и особенностей функционирования ее элементов. А также имеет специальные средства (инструменты, детали и приборы,…). В дополнение к этому, он может применять различные методы и способы противодействия СБ и воздействия на нее, основываясь на предварительной информации, собранной ранее не только об объекте, но и о самой системе. Проникновение возможно с любого направления, с применением различных методов «обхода» СО и с возможным воздействием на различные элементы СБ как в процессе проникновения, так и выполненным предварительно.

Другими параметрами и характеристиками нарушителей могут служить их количество (одиночные или групповые), наличие оружия, способ проникновения на объект на начальном

этапе несанкционированного проникновения (открыто с использованием силы или тайно) и др.

4.6. Реакция системы безопасности

Очевидно, что любая угроза должна быть, прежде всего, обнаружена. Лишь в этом случае можно говорить о реакции системы, т. е. о возможности противодействия угрозе и ее ликвидации. Но последнее выполнимо только при своевременном обнаружении угрозы, когда есть достаточно времени для ее ликвидации. В свою очередь угроза должна быть ликвидирована до нанесения ООБ существенных потерь. Если это выполняется, то СБ решает свою основную задачу.

В общем случае *реакция системы безопасности* – это действия сил и средств реагирования на потенциально возможную или на обнаруженную угрозу для противодействия и ликвидации как самой угрозы, так и ее последствий.

Эти действия или возможности базируются на соответствующей совокупности ресурсов, средств, методов. В зависимости от вида угрозы конкретное содержание упомянутых методов и средств реагирования системы по противодействию и ликвидации угрозы и ее последствий может существенно меняться. Отличия будут зависеть от разных факторов.

Во-первых, от того, есть или нет возможности ликвидировать угрозу. Например, землетрясение ликвидировать невозможно, а криминальные угрозы ликвидировать можно. Поэтому для угроз, которые ликвидировать невозможно, понятие реакции СБ соответствует использованию совокупности РСМ реагирования по минимизации возможного ущерба и ликвидации вторичных угроз. Так, рассматривая в качестве примера землетрясение, речь следует вести о совокупности таких методов и средств, как соответствующее сейсмостойкое проектирование и строительство зданий, использование эффективных процедур оповещения и эвакуации людей и т. п.

Во-вторых, от момента времени, когда угроза обнаружена. Чем раньше произошло обнаружение, тем больше времени есть для реагирования на угрозу, поскольку момент обнаружения определяет начало отсчета возможной реакции СБ на обнаруженную угрозу. Для этого используются понятия *своевременного обнаружения* и *критической точки обнаружения* (КТО) [1].

В-третьих, от момента времени, когда объекту может быть нанесен существенный ущерб. Ясно, что угроза должна быть ликвидирована до этого момента времени.

Для определения этого момента необходимо учитывать вид угрозы и возможности системы по пресечению несанкционированных действий. При разных видах угроз несанкционированные действия можно ликвидировать в разные моменты времени, но в любом случае это надо сделать до нанесения существенных потерь ООБ. Задача нарушителя может состоять не только в непосредственном достижении цели. Например, как уже говорилось, задача преступника при совершении кражи (материальная выгода) решается, если он вышел за пределы досягаемости сил реагирования, иначе говоря, если он остался безнаказанным. Если нарушитель был задержан непосредственно после совершения кражи до выхода за пределы досягаемости сил реагирования, то потери, как правило, минимальны и приемлемы, поскольку похищенное возвращается.

Однако террористу-смертнику выходить за пределы досягаемости сил реагирования не требуется, поскольку достижение им цели уже позволяет решить поставленную задачу – реализовать теракт, и потери могут быть катастрофические.

В соответствии с принципом своевременного обнаружения, эффективность СФЗ определяет вероятность обнаружения нарушителя в тот момент, когда у сил реагирования достаточно времени для нейтрализации нарушителя на пути его к цели.

4.7. Уязвимые места

Уязвимость – это параметр, характеризующий возможность нанесения описываемой системе повреждений любой природы теми или иными внешними или внутренними средствами или факторами.

С точки зрения объекта, к которому применяются термины *уязвимость* или *уязвимые места*, можно говорить о двух основных приложениях: во-первых, к объекту обеспечения безопасности и, во-вторых, к самой системе безопасности.

Создание СБ уменьшает возможности нанесения ущерба ООБ, поскольку устраняет ряд уязвимостей или уменьшает возможности их использования для нанесения потерь объекту. Поэтому можно выделить два вида уязвимости: до создания системы безопасности на объекте и после ее создания, другими словами, для объекта, не оборудованного и оборудованного системой безопасности.

В первом случае анализ уязвимостей важен прежде всего на этапе проектирования СБ при оценке существенности угроз, возможных способов их реализации и выборе необходимых методов и средств их предотвращения, обнаружения и ликвидации. И результат этого анализа, то есть выявленные уязвимости, могут служить мерой степени опасности реализации соответствующей угрозы до создания СБ. А после создания системы – мерой оценки эффективности созданной СБ.

Если говорить об уязвимости самой СБ, то этот вариант можно рассматривать как частный случай уязвимости объекта, поскольку система, установленная на объекте, становится частью самого объекта. Следовательно, нанесение ущерба СБ неизбежно приведет либо к возможности нанесения ущерба ООБ, либо к появлению дополнительных уязвимостей объекта. Поэтому применительно к СБ понятие уязвимости имеет смысл использовать на этапе ее разработки для оценки за-

щищенности того или иного варианта системы от какого-либо вида угроз.

Введем еще одно понятие, необходимое для анализа.

Уязвимое место – часть объекта или системы безопасности, позволяющая либо непосредственно достичь цели, либо получить такую возможность без обнаружения или за промежуток времени, в течение которого система безопасности не сможет адекватно среагировать на угрозу, благодаря чему преступник выполнит поставленную задачу.

Примерами типичных уязвимых мест могут служить технически слабо защищенные места объекта, привлекающие преступника простотой их вскрытия, – непрочная дверь с простым замком, которую легко взломать при использовании даже примитивных средств. В случае ненадежного канала поставки средств обеспечения производственного процесса, к примеру сырья или топлива, его нарушения приведут (при отсутствии запаса) к остановке технологического процесса и, следовательно, к материальным потерям. Легкая доступность охранного извещателя без контроля вскрытия корпуса позволит вывести его из строя без обнаружения этого действия. И, тем самым, предварительно создать уязвимость – возможность проникновения без обнаружения. К уязвимостям объекта можно отнести и наличие маршрутов проникновения, не оборудованных СО.

Таким образом, уязвимое место объекта (с точки зрения технической укрепленности) может использоваться непосредственно для проникновения в целях достижения поставленной преступником задачи, например, для выбора маршрута проникновения или легко достижимой цели, а уязвимое место системы безопасности – для вывода ее полностью или частично из строя для создания необнаруживаемого маршрута проникновения.

Для СБ можно говорить об уязвимости так же, как о зависимости работоспособности системы от состояния источника питания, например, при отсутствии его резервирования или малом времени работы от резервного источника питания. Или о зависимости вероятности обнаружения ПИК-датчиков от температуры окружающей среды: при температурах, близких к температуре тела, надежность обнаружения может существенно уменьшаться при отсутствии надлежащей термокомпенсации.

4.8. Ограничения

Создание любого устройства, тем более системы, должно производиться при определенных ограничениях. Список таких ограничений и их состав будет определяться в каждом конкретном случае с учетом всех особенностей объекта, решаемой задачи обеспечения безопасности и имеющихся возможностей. Рассмотрим наиболее типичные ограничения, которые могут иметь место при разработке СФЗ.

1. *Экономические*. Такие ограничения в той или иной мере присутствуют всегда. Они могут существенно повлиять на функциональный, количественный и качественный состав системы и, как показывает практика, обычно в худшую сторону. К основным составляющим экономических ограничений можно отнести стоимости следующих составляющих общих затрат на создание и использование системы на этапах:
    - проектирования;
    - закупки оборудования;
    - монтажа и пусконаладки;
    - эксплуатации;
    - модернизации и др.

Но всегда надо помнить, что, с одной стороны, реальная безопасность не может стоить дешево, а с другой стороны, нет необходимости в чрезмерных затратах.

2. *Технические*. Несмотря на высокий современный уровень развития, ТС обеспечения безопасности имеют определенные ограничения. Эти ограничения могут касаться функциональных возможностей оборудования, его надежности, возможности использования на конкретном объекте в конкретных условиях эксплуатации и др. И, как следствие, это накладывает ограничения и на создаваемую СФЗ. К таким ограничениям относятся:
    - современный уровень развития технических средств;
    - функциональные возможности конкретного оборудования;
    - надежность оборудования;
    - удобство монтажа и некоторые другие.
3. *Организационные* ограничения, связанные с определенными правилами и процедурами функционирования конкретного объекта обеспечения безопасности. Они могут включать:
    - удобство использования;
    - возможности по технической поддержке;
    - возможности по адаптации системы к режиму функционирования объекта;
    - возможности по организации реагирования на обнаруженные угрозы и т. п.
4. *Юридические* ограничения, связанные с особенностями законодательства страны. Так, использование ресурсов современного оборудования может ограничиваться существующими законами и другими нормативными актами. Например, запретом использовать скрытое наблюдение или создавать базу данных биометрических признаков

пользователей. Другой пример – допустимость использования средств нелетального воздействия на преступника как средств противодействия.

5. *Ведомственные* ограничения, имеющиеся в ряде организаций в силу специфики решаемых задач и некоторых других требований на использование того или иного оборудования или тактики его применения, которые регламентируются внутренними документами организации. Примером могут служить перечни оборудования, разрешенного к использованию на объектах этой организации.

Контрольные вопросы к главе 4

1. Объясните и проиллюстрируйте на примерах, как воздействуют на защищаемый объект внешние и внутренние угрозы.
2. Объясните и проиллюстрируйте на примерах, как воздействуют на защищаемый объект первичные и вторичные угрозы.
3. Объясните и проиллюстрируйте на примерах, как воздействуют на защищаемый объект прямые и опосредованные угрозы.
4. Объясните и проиллюстрируйте на примерах, как воздействуют на защищаемый объект отвлекающие угрозы.
5. Расскажите, что такое модели нарушителя. Приведите примеры таких моделей и объясните, чем они могут характеризоваться.
6. Расскажите, что такое реакция системы безопасности.
7. Расскажите и проиллюстрируйте на примерах, что такое уязвимые места объекта.
8. Перечислите возможные ограничения при проектировании СФЗ.
9. Конкретизируйте перечень возможных экономических ограничений при проектировании СФЗ.

10. Конкретизируйте перечень возможных технических ограничений при проектировании СФЗ.
11. Конкретизируйте перечень возможных организационных ограничений при проектировании СФЗ.
12. Конкретизируйте перечень возможных юридических и ведомственных ограничений при проектировании СФЗ.

5. ПРОЦЕДУРА РАЗРАБОТКИ СИСТЕМЫ

Совокупность и последовательность действий, которые необходимо выполнить при разработке СБ, представляют собой процедуру разработки системы (рис. 15). Будем учитывать риски при процедуре разработки СФЗ и возможные ограничения на проведение тех или иных действий, которые могут привести к тому, что система не выполнит (полностью или частично) свои функции.

5.1. Объект обеспечения безопасности

Первоочередная задача при выполнении процедуры разработки СБ – формализация объекта обеспечения безопасности. Без знания того, что необходимо защищать, невозможно построить систему защиты. Поэтому прежде всего следует четко сформулировать, что из себя представляет объект защиты. Для этого необходимо выполнить следующее.

- ☑ Составить общий список жизненных приоритетов, подлежащих защите.
- ☑ Из общего списка жизненных приоритетов отобрать наиболее существенные для решаемой задачи. При этом нужно учитывать несколько видов риска. Осознанный риск – та составляющая жизненных приоритетов, которая не включена в список, не будет защищаться. Например, из общего списка приоритетов: жизнь, здоровье, окружающая среда, имущество, ресурсы и информация – выбрано только имущество. Значит, безопасность остальных групп жизненных приоритетов полностью или частично обеспечиваться не будет.
- ☑ Конкретизировать список составленных жизненных приоритетов. Например, детализировать перечень имущества с учетом ценности (как материальной, так и информационной или культурно-исторической), особенно-

стей его расположения на объекте и возможностей доступа к нему.

В результате должен быть определен итоговый список жизненных приоритетов и, таким образом, сформулирован ООБ. В нашем случае это перечень наиболее ценного имущества, утрата которого приведет к существенным потерям.

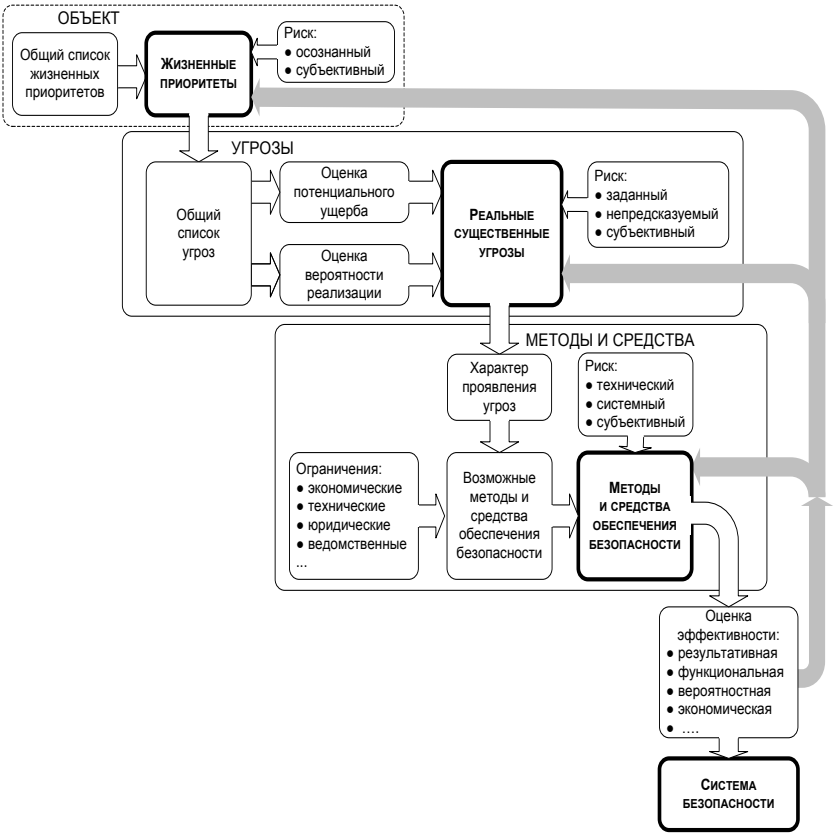


Рис. 15. Процедура разработки системы безопасности

5.2. Угрозы объекту обеспечения безопасности

На втором этапе определения угроз ООБ необходимо выполнить следующее.

- ☑ На основании сформированного итогового списка жизненных приоритетов, т. е. объекта обеспечения безопасности, формируется общий перечень угроз этому объекту, реализация которых может привести к потерям. Этот перечень должен включать все существующие и потенциально возможные угрозы с учетом всех имеющихся и потенциальных источников и видов угроз, таких как внешние и внутренние, прямые и опосредованные, первичные и вторичные. Так, если из общего списка приоритетов (жизнь, здоровье, окружающая среда, имущество, ресурсы и информация) выбрано только имущество, то угрозами ему могут быть пожар, кража, разбой или грабеж, протечка воды, утечка газа и некоторые другие.
- ☑ Проводится отбор угроз, приводящих к существенным потерям, т. е. составляется список существенных угроз. В рассматриваемом примере это могут быть пожар, кража, протечка воды, утечка газа.
- ☑ Проводится отбор наиболее вероятных угроз. Предположим, что наиболее вероятными являются пожар, кража и протечка воды. Эти угрозы являются реальными.
- ☑ На основании сравнения результатов выполнения двух предыдущих пунктов составляется список реальных существенных угроз, которые будут служить исходными данными для выбора методов и средств обеспечения безопасности. В рассматриваемом примере малая вероятность реализации утечки газа позволяет сократить список, оставив в нем только пожар, кражу и протечку. Риск на этом этапе может быть заданным (правильно ли были оценены вероятности реализации угроз и возмож-

ный уровень потерь при их реализации) и непредсказуемым (например, вор, чтобы скрыть следы преступления, открыл газовый вентиль).

5.3. Методы и средства обеспечения безопасности объекта

Третий этап определения МСОБ объекта состоит в решении следующих задач.

- ☑ Максимально точно оценивается характер физического проявления реальных существенных угроз по каждой позиции. Это необходимо будет для выбора принципа действия соответствующих средств обнаружения. Например, кража из офиса может быть совершена днем (в рабочее время) или ночью скрытно (в нерабочее время). Днем она может быть реализована сотрудником, посторонним под видом посетителя, через подкупленного или запуганного сотрудника, обслуживающим персоналом, представителем курьерской службы и т. д. Ночью преступник может проникнуть через дверь (подобрать ключи или использовать отмычки, взломать замок или дверь, проломить стену, потолок или пол и т. д.) либо через окно (разбить или вырезать стекло или открыть раму).
- ☑ Характер физического проявления угроз позволяет выбрать возможные средства предупреждения и обнаружения этих угроз и методы использования этих средств.
- ☑ Из всех возможных средств отбираются наиболее полно удовлетворяющие условиям поставленной задачи и ограничениям:
  - экономическим (стоимость создания и эксплуатации системы);
  - техническим (функциональные возможности и надежность существующего оборудования);

- ведомственным (ведомственные ограничения на использование того или иного вида оборудования)

и другим с учетом рисков:

- технического (техническая реализуемость и надежность);
- субъективного (ошибки проектировщиков, установщиков, обслуживающего персонала);
- системного (возможные угрозы, создаваемые разрабатываемой СБ).

На основании выбранных средств обеспечения безопасности и методов их использования формируется предварительная аппаратная, программная и организационная конфигурации системы безопасности.

Контрольные вопросы к главе 5

1. Объясните, что такое процедура разработки СФЗ.
2. Расскажите о таком этапе общей процедуры разработки системы безопасности, как определение объекта обеспечения безопасности.
3. Объясните, каковы риски и ограничения на этапе определения объекта обеспечения безопасности.
4. Расскажите о таком этапе общей процедуры разработки системы безопасности, как определение угроз объекту обеспечения безопасности.
5. Объясните, каковы риски и ограничения на этапе определения угроз объекту обеспечения безопасности.
6. Расскажите о таком этапе общей процедуры разработки системы безопасности, как определение ресурсов, методов и средств обеспечения безопасности объекта.
7. Объясните, каковы риски и ограничения на этапе определения ресурсов, методов и средств обеспечения безопасности объекта.

6. ОЦЕНКА ЭФФЕКТИВНОСТИ

Итогом выполнения рассмотренных трех этапов процедуры проектирования будет СБ, обладающая определенными характеристиками и возможностями. Однако для завершения общей процедуры нужно выполнить оценку эффективности полученного решения по выбранному критерию(ям) эффективности при заданных ограничения. С общей точки зрения ТС считается эффективной, если она в заданных условиях эксплуатации полностью и в установленные сроки выполняет свои целевые функции; в нашем случае – это когда не допускается существенный ущерб для ООБ и затраты на создание и эксплуатацию системы не превышают положительного эффекта от использования системы.

Очевидно, что оценка эффективности проводится теми или иными методами по заданным критериям и ограничениям. Если соответствующий критерий не удовлетворяется, то производится корректировка на одном из предыдущих этапов. Например, если система не соответствует экономическим ограничениям, то можно выбрать более дешевое оборудование (с увеличением уровня технического риска), отказаться от обеспечения безопасности какого-либо приоритета (например, сократить список имущества), отказаться от учета каких-нибудь угроз, к примеру, от контроля протечки воды (с соответствующим увеличением уровня заданного риска) и т. д.

Поэтому процедура разработки в общем случае является повторяющейся, многоступенчатой до достижения выполнения всех критериев и ограничений. Возможны также и корректировки технического задания как при невозможности его выполнения по тем или иным причинам, так, впрочем, и при возможности улучшения характеристик с приемлемыми затратами.

Различают два основных смысловых значения понятия *эффективность*:

- эффективность – соотношение между достигнутыми результатами и ресурсами, которые были затрачены;
- результативность – степень достижения результатов, которые запланированы.

Соответственно этому используются две различные трактовки этого понятия: экономическая и результативная эффективность.

При всей важности экономической эффективности правильнее понимать под эффективностью СФЗ именно результативную эффективность, а эффективность в смысле экономичности выделять в группу комплексных показателей вида «эффективность – стоимость». При этом очевидно, что СБ обычно не дает прямого экономического эффекта. Поэтому кратко рассмотрим особенности оценки экономического эффекта от создания СБ.

6.1. Оценка экономической эффективности

Экономические методы оценки эффективности ТС опираются на следующие характеристики:

- положительный экономический эффект в результате использования системы – E;
- общие затраты З, включающие стоимость:
  - создания системы (оборудование и монтаж) – C_c;
  - обслуживания системы в процессе эксплуатации – C_o.

Критерий, отвечающий указанным требованиям, может быть представлен в следующем виде:

$$Э = E - З,$$

где Э – эффективность системы; $З = C_c + C_o$ – затраты на создание и эксплуатацию системы.

Поскольку обычно СБ непосредственно не дает положительного экономического эффекта (экономии), то применительно к таким системам вопрос с оценкой экономии может решаться следующим образом.

Положительный эффект E от использования СБ может характеризоваться потенциально возможными потерями $П_п$ для объекта. То есть предотвращенными потерями, которые могли бы иметь место при отсутствии СБ, но будут предотвращены за счет ликвидации угроз защищаемому объекту создаваемой системой безопасности. Тогда экономическая эффективность будет определяться выражением

$$Э = П_п – З.$$

На практике в ряде случаев СБ или ее отдельные подсистемы все-таки могут давать и прямой положительный экономический эффект. Также можно говорить и о возможном косвенном экономическом эффекте, напрямую не связанном с задачами обеспечения безопасности. Например, путем сокращения персонала за счет применения автоматических систем контроля и управления доступом или благодаря автоматизированному учету рабочего времени при этом.

Поэтому не исключается возможность одновременного использования обоих параметров – суммы непосредственно положительного экономического эффекта *E* и предотвращенных потерь $П_п$.

В некоторых задачах удобнее использовать в качестве численного параметра относительную экономическую эффективность. Тогда критерий эффективности произвольной ТС [34] применительно к СФЗ может быть записан как

$$Э_о = \frac{П_п – З}{П_о},$$

где $Э_о$ – относительная эффективность; $П_п$ – предотвращенные потери в результате использования системы; З – затраты на создание и эксплуатацию системы; $П_о$ – общие возможные потери.

Или с учетом прямого $E_п$ и косвенного $E_к$ положительного эффекта

$$Э_о = \frac{(П_п + E_п + E_к) - З}{П_о}.$$

В свою очередь, как было показано выше, предотвращенные потери $П_п$ определяются произведением $П_п = П_о У_п$ общих возможных потерь $П_о$ на относительный предотвращенный ущерб $У_п$ в результате использования СБ. Значения $У_п$ могут меняться от 0 (потери не предотвратили) до 1 (полностью предотвратили потери, хотя можно было потерять все). Тогда можно переписать выражение для общего критерия эффективности как

$$Э_о = \frac{П_о У_п - З}{П_о} = У_п - \frac{З}{П_о}.$$

Учтем, что $У_п = 0…1$, а диапазон разумных значений затрат на создание системы З не должен превышать общих возможных потерь $П_о$, поэтому можно записать $0 < \frac{З}{П_о} < 1.$ Тогда становится очевидным, что для достижения положительного значения эффективности $Э_о > 0$ необходимо, чтобы условный предотвращенный ущерб превосходил относительные затраты на создание и эксплуатацию системы. Поэтому критерием оценки разумности планируемых затрат на создание системы может служить соотношение $У_п > \frac{З}{П_о}$.

Приведенные рассуждения и выражения позволяют сделать оценки экономической эффективности создаваемой или разработанной системы безопасности.

6.2. Методы оценки эффективности СФЗ

Известные методы оценки эффективности СФЗ, как правило, основаны на формализованном представлении процесса функционирования системы и воздействий на ООБ извне (внешняя угроза) и изнутри (внутренняя угроза). Для этого разрабатываются соответствующие модели:

- объекта и режима его функционирования;
- нарушителя;
- планируемого режима функционирования (или наоборот – опасного состояния) СФЗ в штатных ситуациях;
- реального режима функционирования СФЗ в нештатных ситуациях;
- боестолкновения и т. д.

Далее, анализируя эти данные, получают значения того или иного показателя эффективности в рамках выбранной модели.

Известны многие методы оценки эффективности, такие как детерминистический подход, логико-вероятностные методы, методы анализа иерархий, нечетких множеств, вероятностно-временного анализа и др.

Ясно, что возможно сочетание этих методов для разных этапов реализации угроз и различных частей объекта. Сложность реальных объектов обеспечения безопасности требует, как правило, для реализации упомянутых методов использования компьютерного моделирования и расчетов. На сегодняшний момент существует ряд подобных программ, а также ведутся разработки по их совершенствованию и созданию новых.

Существующие методы решения рассматриваемой задачи могут существенно отличаться по принципиальному подходу, и отличия основываются, прежде всего, на априорной информации об объекте и угрозах и используемом критерии эффективности. В частности это могут быть следующие.

1. *Результативные*. Критерием при таком методе является достижение некоторых результатов работы СФЗ. Например, достижение того или иного уровня обеспечения безопасности (защищенности) объекта.

2. *Функциональные*. В таком случае критерий – соответствие функциональных возможностей созданной системы условиям технического задания.

3. *Экономические*. Как следует из названия, критерием в данном случае является достижение определенного экономического эффекта. Обычно это соотношение затрат на создание системы и уровня предотвращенных потерь, которые могут служить основной мерой достигаемого экономического эффекта.

4. *Вероятностные*. В этом случае в качестве критериев используются вероятности тех или иных событий, к примеру, возможность достижения требуемых вероятностей обнаружения угроз, пресечения несанкционированных действий, ложных тревог и т. п.

Упомянутые методы и используемые в них критерии оценки результатов могут быть применены как к СФЗ в целом, так и к отдельным ее частям или подсистемам, поскольку, анализируя СБ как сложную иерархическую систему, обычно можно применять принцип декомпозиции. Однако, естественно, окончательный и более полный вывод можно сделать только на основе анализа эффективности функционирования всех подсистем не по отдельности, а во взаимодействии.

6.3. Точность оценки эффективности

Возможности и точность используемого метода в значительной степени зависят от исходных данных о:

- системе;
- объекте обеспечения безопасности;
- модели нарушителей (угроз).

Эти данные могут быть получены на основе экспертных оценок, экспериментальных исследований, вероятностных параметров и, конечно, комбинированных, использующих несколько способов получения исходных данных.

Рассмотрим кратко основные особенности получения исходных данных, которые могут подразделяться по разным признакам.

1. По способу отображения реальных процессов используемыми моделями [35]:
   - эвристические, представляющие словесное описание, основанное на опыте и умозаключениях экспертов. Такая модель может быть разработана различными путями, например методом «мозгового штурма» или ответами экспертов на контрольные вопросы;
   - математические, основанные на последовательности математических или (и) логических выражений, описывающих реальные процессы. Такие модели более универсальны и точны и часто являются основой для компьютерных программ расчета;
   - графические – это разнообразные схемы, графы, деревья и т. п. При их построении используется субъективное представление эксперта о функционировании объекта, однако элементы схемы связаны между собой строгими логическими связями. Поэтому такие модели занимают промежуточное положение между двумя предыдущими типами.
2. По характеру точности определения входных данных:
   - детерминированные;
   - вероятностные.

Если в первом случае входные данные, т. е. характеристики процесса развития угрозы, к примеру проникновения, имеют предопределенные значения, то во втором случае упомянутые данные представляют собой случайные величи-

ны с некоторыми статистическими характеристиками, например законом распределения и его моментами.

3. По способу определения различных характеристик и принятия тех или иных решений:

- экспертные, в которых на различных шагах решения принимает эксперт, полагаясь на свой опыт в данной области;
- аналитические, в которых решения принимаются по определенному алгоритму (например, математической формуле);
- экспериментальные, в которых решения принимаются на основании учений или экспериментов на реальном объекте или в приближенных к реальным условиях;
- комбинированные, сочетающие два или более других методов.

4. По степени полноты учета различных параметров ООБ. В данном случае можно говорить о сложности объекта и используемого метода. Признаками сложности могут являться большое количество входных параметров, множество связей между отдельными элементами системы, вероятностный характер протекания процессов и т. д. Четкого правила разделения в таком случае нет, но можно сказать, что сложность метода определяется уровнем затраченных ресурсов и времени и во многом определяет точность оценки.

5. По степени полноты учета модели потенциального нарушителя (ресурсов, возможностей и характера нарушителей). Например, не все методы могут учитывать действия внутреннего нарушителя, сознательные и неумышленные, вызванные нарушениями правил или непрофессионализмом персонала (защита от «дурака» и от «профессора») и т. д.

6. По способам реализации метода:

- программные, в основе которых лежит использование компьютерных программ и программных комплексов, позволяющих сэкономить время на выполнение однотипных вычислений и снизить вероятность ошибки, сюда также можно отнести программные игровые модели;
- аналитические, основанные на строгом алгоритме анализа исходных данных, производимых экспертом (экспертами);
- моделирование, т. е. проведение учений на реальном объекте или в приближенных к реальным условиях;
- экспертные, в которых эксперт (эксперты) дает оценку эффективности СФЗ, основываясь на своем опыте.

Перечисленные выше особенности демонстрируют разнообразие существующих методов анализа эффективности, которые могут быть использованы в той или иной задаче оценки эффективности СБ. И, как следствие, сложность и ответственность выбора того или иного метода.

Контрольные вопросы к главе 6

1. Расскажите, что такое экономическая эффективность СФЗ.
2. Объясните, что такое результативная эффективность СФЗ.
3. Объясните, что такое экономический эффект от создания СФЗ.
4. Расскажите, что такое относительная экономическая эффективность СФЗ.
5. Объясните, что такое предотвращенные потери.
6. Расскажите, как осуществляется оценка экономической эффективности.
7. Какие характеристики и параметры объекта, угрозы СФЗ и их модели нужны для оценки эффективности.

8. Перечислите основные методы оценки эффективности СФЗ.
9. Расскажите, от чего зависит точность оценки эффективности СФЗ.
10. Основные особенности получения исходных данных, которые могут подразделяться по разным признакам.
11. Перечислите основные особенности получения исходных данных по способу отображения реальных процессов используемыми моделями.
12. Перечислите основные особенности получения исходных данных по способу определения различных характеристик и принятия решений.
13. Перечислите основные особенности получения исходных данных по степени полноты учета различных параметров ООБ.
14. Перечислите основные особенности получения исходных данных по степени полноты учета модели потенциального нарушителя.
15. Перечислите основные особенности получения исходных данных по способам реализации метода.

7. КОНЦЕПТУАЛЬНЫЕ ВОПРОСЫ ПОСТРОЕНИЯ СФЗ

7.1. Основные положения

При создания СФЗ и выборе состава и общей структуры сложных интегрированных комплексных СФЗ необходим учет следующих основополагающих положений.

Решение задачи обеспечения безопасности в широком смысле с учетом всех составляющих, необходимых для эффективного обеспечения противокриминального, антитеррористического, антивандального, технологического, информационного, экономического, экологического и других направлений обеспечения безопасности субъекта или объекта, необходимых в каждой конкретной ситуации, включая вопросы автоматизации и управления для зданий и сооружений.

Реализация интегрированного решения упомянутых выше задач в комплексе на всех нижеперечисленных этапах построения и функционирования СБ в оптимальном смысле, соответствующем задаче, требованиям заказчика и ограничениям:

- анализа объекта и всех его особенностей (определение ООБ);
- анализа угроз и рисков;
- проектирования системы (выбора ресурсов, методов и средств обеспечения физической безопасности объекта);
- монтажа оборудования;
- пусконаладочных работ;
- обучения персонала СБ на начальном этапе;
- поддержания уровня квалификации в процессе эксплуатации;
- обучения персонала объекта поведению в штатных и нештатных ситуациях;

- технического обслуживания системы в процессе эксплуатации;
- расширения системы для обеспечения безопасности новых элементов объекта и защиты от новых угроз;
- модернизации системы (модернизации программного обеспечения и оборудования для увеличения эффективности СБ).

Единое решение по созданию системы, обеспечивающее следующие условия.

- Предметно ориентированные решения для конкретных отраслей и задач (транспорта, энергетики, зданий и сооружений, объектов для спортивно-массовых мероприятий,…) с учетом специфики ООБ и особенностей проявления угроз.
- Полный спектр предлагаемых технических и программных средств для реализации решения.
- Разработку комплекса организационных мероприятий по реагированию на нештатные ситуации персонала СБ и самого ООБ.
- Возможность сопровождения системы на всех этапах проектирования и реализации предлагаемого решения.
- Учет, по возможности, всех угроз, приводящих к существенным потерям для субъекта или объекта обеспечения безопасности; вероятностей и способов реализации этих угроз.
- Оценку рисков и возможных потерь от реализации угроз до и после создания системы. Вероятности реализации угроз и уровни допустимых потерь определяются на основе анализа совместно с заказчиком.
- Оценку рисков и возможных потерь от реализации самой СФЗ.
- Обеспечение защищенности СФЗ.
- Оценку эффективности СФЗ.

Для возможности выполнить это необходим достаточно полный набор априорных данных об объекте обеспечения ФЗ.

7.2. Основные исходные данные

Очевидно, что для решения задачи создания СФЗ необходим определенный набор исходных данных, касающихся ООБ. Ясно, что в каждом конкретном случае эти исходные данные будут различаться и зависеть от особенностей как объекта, так и режима его функционирования. При этом надо учесть все, что так или иначе, прямо или косвенно может повлиять на безопасность объекта, на возможность решения всех задач, упомянутых выше. Перечислим основные исходные данные.

Общая структура объекта

Информация об общей структуре объекта может включать в себя следующие сведения.

- ✓ Перечень групп объектов или комплексов, территориально разнесенных между собой.
- ✓ Состав и функциональное назначение объектов в каждой группе.
- ✓ Структурный и функциональный состав каждого объекта.
- ✓ Конструктивное исполнение каждого объекта (конструкция и материалы стен, окон и т. д.).
- ✓ Распределение ресурсов (материальных, денежных, информационных и др.) по объекту.
- ✓ Территориальное расположение объектов в стране, регионе, на местности с учетом особенностей рельефа, растительности, других близлежащих объектов и коммуникаций.
- ✓ Окружающий объекты рельеф (с точки зрения возможности визуального наблюдения, осуществления терактов со стороны и т. п.).

- ✓ Наличие и характеристики водных объектов (моря, каналов, водоводов, рек и т. п.), находящихся в непосредственном контакте с объектом ФЗ, например пересекающих объект или граничащих с этим объектом).
- ✓ Социальные, этнические и религиозные особенности региона. Зависимость населения региона от объекта, социальный состав населения, уровень безработицы, наличие и взаимоотношения различных социальных групп.
- ✓ Количественный и структурный состав персонала – сотрудников объекта (руководства, рядовых, охраны, обслуживающего персонала, уборщиц, ремонтников и т. д.); посетителей объекта, в том числе имеющих необходимость какого-либо взаимодействия с объектом, обеспечивающих обслуживание объекта и поставки на объект.
- ✓ Количество постоянно находящихся людей на объекте. Ориентировочное каждодневное количество посетителей этих объектов (максимальное, пиковые нагрузки, изменение количества во времени и в календарные периоды и т. д.).

Транспортная инфраструктура объекта

Информация о транспортной ифраструктуре объекта может включать в себя следующие основные элементы.

- ✓ Каждодневные способы доставки персонала, участников и посетителей на объекты (какой транспорт – железнодорожный, автомобильный и т. д., с разделением по посетителям, участникам и обслуживающему персоналу) из мест их нахождения на период различных мероприятий.
- ✓ Каждодневные способы перемещения персонала и посетителей внутри объектов.

- ✓ Разовые (на период различных мероприятий – перед ним, в течение и после него) способы транспортировки персонала, участников, посетителей и обслуживающего персонала (морским, железнодорожным или автомобильным транспортом) через аэропорты, морские порты и т. д.

Основные средства жизнеобеспечения этих объектов (кабельные или воздушные линии электропередач, каналы поставки продуктов, воды, теплоснабжение – централизованное, местное и т. п.).

Каналы связи, которые используются непосредственно для целей обеспечения режима функционирования объектов, их защищенность, возможности их использования для СБ, возможность прокладки специальных каналов связи для СБ и т. п.

Материалы, имеющиеся в распоряжении заказчика. Исходные технические требования заказчика к системе или ее элементам. Организационные требования к режиму функционирования системы. Специфические (ведомственные и иные) требования к интегрированной СБ. Анализ угроз, рисков и уязвимостей, сделанный заказчиком.

Ограничения на зоны ответственности различных служб к примеру, необходимость распределения ответственности за решение таких задач, как обеспечение безопасности от подготовки терактов на этапе строительства; защита информации, в частности, каналов связи; защита средств жизнеобеспечения этих объектов, расположенных вне самих объектов; контроль поставок продуктов питания, напитков и т. п.; обеспечение безопасности морских акваторий (над- и подводных); обеспечение безопасности воздушного пространства; обеспечение режима безопасности на окружающих, господствующих высотах и т. д.

В каждом конкретном случае вышеприведенный перечень может расширяться и дополняться или сокращаться в зависимости от поставленных требований и ограничений. Очевидно, что нельзя учесть все особенности без знания условий конкретной решаемой задачи.

7.3. Принципы построения системы

Интегрированная СФЗ должна строиться на основе и с учетом различных положений и критериев, изложенных выше. Это обеспечивает возможность достижения следующих базовых принципов построения интегрированной системы физической защиты.

Адекватность

При построении СФЗ необходима адекватность:

- структуры и состава системы возможным угрозам и рискам;
- стоимости создания системы предотвращенным возможным потерям;
- обоснованности всех используемых элементов системы;
- соответствия требованиям государственных стандартов и ведомственных документов;
- согласованности с различными структурами, участвующими в процессе обеспечения безопасности.

Функциональность

Функциональность – это прежде всего возможность своевременно и максимально эффективно реагировать на угрозу. Иными словами, возможности СФЗ по выполнению всех основных функций за требуемый промежуток времени, необходимый для реакции на нештатную ситуацию в определенных условиях по выполнению поставленных задач:

- предотвращения угроз;
- обнаружения угроз;

- задержки в развитии угрозы;
- минимизации последствий реализации угроз (восстановление системы и объекта);
- ликвидации угроз;
- ликвидации последствий;
- анализа произошедшего;
- корректировки параметров методов и средств в целях недопущения повторения подобной ситуации в дальнейшем и снижения потерь при ее повторении.

Управляемость, включающая:

- подверженность подсистем централизованному и децентрализованному управлению;
- возможность надлежащей обработки поступающей информации;
- высокую степень автоматизации процессов обработки информации и принятия решения в целях минимизации «человеческого фактора»;
- контроль доступа персонала к управлению и другим действиям с системой.

Защищенность

Защищенность системы, позволяет контролировать, тестировать и охранять саму себя от возможных некорректных и несанкционированных действий, таких как:

- физический и программный доступ к элементам системы и каналам связи;
- съем информации о системе и ее элементах;
- модификация и уничтожение информации в системе;
- ошибочные действия (защита от «дурака» и от «профессора»);
- прямое физическое воздействие на средства обнаружения, передачи и обработки информации, например, вскрытие элементов системы, повреждение каналов связи и т. п.;

- НСД, изменяющие режим функционирования системы, к примеру, действия, отвлекающие службы реагирования от выполнения своих прямых функций;
- непрямое воздействие на средства обнаружения, передачи и обработки информации, изменяющее параметры системы, такие как маскирование и блокирование средств обнаружения угроз, постановка помех в каналах связи, съем информации о системе, попытки несанкционированного изменения ее параметров и т. п. действий;
- НСД по управлению системой (осуществляемые обычно путем контроля уровня доступа персонала к СБ).

Безопасность, состоящая в том, что СБ:

- не должна создавать дополнительные угрозы субъектам и объектам обеспечения безопасности;
- не должна создавать угрозы самой себе;
- не должна приводить к сколько-нибудь существенному изменению режима функционирования объекта;
- должна обеспечивать минимизацию возможных последствий ошибочных действий самой системы и персонала, управляющего ею.

Энергонезависимость

Одно из обязательных требований к СФЗ – энергонезависимость от внешних источников питания, характеризующаяся наличием резервных источников питания элементов системы; продолжительностью работы от резервных источников питания; продолжительностью восстановления резервных источников питания; продолжительностью перехода на резервное питание.

Структурность

Структурность СФЗ предъявляет следующие требования, прежде всего к программной и аппаратной масштабируемости системы:

- аппаратная и программная гибкость (аппаратная и программная модульность);
- пространственно-распределенная архитектура, которая должна представлять собой набор подсистем, объединенных каналами связи с общими средствами сбора и обработки информации и управления;
- многоуровневая архитектура обнаружения угроз и принятия решения.

Взаимозаменяемость, т. е. многофункциональность подсистем, обеспечивающая возможность разных подсистем выполнять не только свои основные функции, но и части функций других подсистем для возможности обнаружения одних и тех же угроз разными подсистемами.

Восстанавливаемость после нештатной ситуации, определяемая временем функционального восстановления системы (полного или частичного), позволяющая продолжить выполнение ею тех или иных функций (возвращение группы задержания на исходную позицию, переустановка датчиков и т. п.); продолжительность технического (аппаратного и (или) программного) восстановления системы (полного или частичного) для ремонта оборудования, переустановки программного обеспечения после сбоев и т. д.

Анализируемость произошедших ситуаций на объекте и в системе без создания каких-либо ограничений на продолжение выполнения СБ своих функций; протоколирование и архивирование информации о всех событиях в системе.

Профессиональность СФЗ заключается в следующем:

- использовании специализированного оборудования и программного обеспечения;
- решении основных функций обеспечения безопасности предназначенной именно для этого специализированной подсистемой;

- использовании специализированных каналов связи, предназначенных только для СБ, т. е. использование замкнутых, а не квазизамкнутых систем связи;
- использовании специализированного системного программного обеспечения для интеграции, а не адаптированного программного обеспечения подсистемы;
- профессиональном уровне проектировщиков, поставщиков, монтажников и пользователей СБ.

Инвариантность системы к следующему:

- изменениям параметров окружающей среды;
- изменениям состояния и условий взаимодействия с другими элементами объекта;
- изменениям состояния элементов защищаемого объекта;
- выходу из строя одной или нескольких подсистем (не приводящему к выводу из строя системы обеспечения безопасности в целом);
- состоянию систем жизнеобеспечения объекта и СФЗ (электропитания, кондиционирования, в частности, система не должна выходить из строя при отключении электроэнергии на объекте);
- инвариантность к типу используемых каналов связи, возможность их дублирования.

Информативность устройств обнаружения угроз и эффективное обнаружение угроз с учетом максимально раннего обнаружения, по возможности, на этапе подготовительных или начальных действий и максимально надежного обнаружения; соответствия принципов их обнаружения характеру проявления угроз; обнаружения одних и тех же угроз на основе различных физических принципов; обнаружения одних и тех же угроз разными подсистемами для повышения вероятности обнаружения; интегрального принятия решения на основе использования комплекса информации от СО всех подсистем.

Надежность оборудования: самодиагностика и самоконтроль элементов системы с автоматическим выявлением не только самих неисправностей, но и потенциальных возможностей их возникновения; резервирование («горячее» или «холодное») всех основных жизненно важных элементов системы (каналов передачи информации, накопителей на жестких дисках, основных устройств обработки информации, …); резервирование выполняемых функций (переключение выполняемых функций неисправного устройства на исправное,…); и возможность каждой из подсистем функционировать самостоятельно, независимо от состояния каналов связи и работоспособности других подсистем; возможность использовать каналы передачи информации с различными физическими принципами действия.

Адаптивность – возможность высокой степени адаптации (аппаратной, программной, организационной, функциональной) к особенностям объекта и режиму функционирования для минимизации возможного влияния на них.

Совместимость для возможности информационного взаимодействия (интеграции) с другими функциональными системами объекта и оборудования нижнего уровня (датчиков контроля состояния объекта) различных производителей.

Соответствие СФЗ вышеперечисленным принципам не всегда возможно, однако оно может позволить повысить ее эффективность, а следовательно, обеспечить более высокую степень защищенности объекта обеспечения безопасности от различных угроз.

Контрольные вопросы к главе 7

1. Перечислите и объясните основные положения, учитываемые при построении СФЗ.
2. Перечислите основные исходные данные для построения СФЗ.

3. Расскажите, какие сведения об общей структуре объекта необходимы для построения СФЗ.
4. Расскажите, какие сведения о транспортной инфраструктуре объекта необходимы для построения СФЗ.
5. Расскажите, какие сведения о средствах жизнеобеспечения объекта и каналах связи необходимы для построения СФЗ.
6. Перечислите основные принципы построения СФЗ.
7. Объясните принцип адекватности СФЗ.
8. Объясните принцип функциональности СФЗ.
9. Объясните принцип защищенности СФЗ.
10. Объясните принцип энергонезависимости СФЗ.
11. Объясните принцип профессиональности СФЗ.
12. Объясните принцип инвариантности СФЗ.
13. Объясните принцип информативности СФЗ.

Литература

1. Гарсиа М. Проектирование и оценка систем физической защиты. – М.: Мир. – 2003. – 388 с.
2. Петраков А. В., Дорошенко П. С., Савлуков Н. В. Охрана и защита современного предприятия. – М.: Энергоатомиздат, 1999. – 568 с.
3. Петраков А. В., Лагутин В. С. Телеохрана. – 4-е изд., доп. – М.: Academia, 2012. – 502 с.
4. Петраков А. В. Защита и охрана личности, собственности, информации: справ. пособие. – М.: Радио и связь, 1997. – 318 с.
5. Петраков А. В., Лагутин В. С. ТелеинфраультраВизуализация как защищённое ТелеВидение. – М.: Academia, 2012. – 642 с.
6. Волхонский В. В. Системы охранной сигнализации. – 2-е изд., доп. и перераб. – СПб.: Экополис и культура, 2005. – 204 с.
7. Измайлов А. В. Методы проектирования и анализ эффективности систем физической защиты ядерных материалов и установок: учеб. пособие. – М.: МИФИ, 2002. – 52 с.
8. Физическая защита ядерных объектов: учебн. пособие для вузов/ П. В. Бондарев, А. В. Измайлов, А. И. Толстой; под ред. Н. С. Погожина. – М.: МИФИ, 2008. – 584 с.
9. Степанов Б. П., Годовых А. В. Основы проектирования систем защиты ядерных объектов: учеб. пособие. – Томск: Изд-во Томского политех. ун-та, 2009. – 118 с.
10. Зайцев А. В. Где находится последний рубеж комплексной системы безопасности // Алгоритм безопасности. – 2013. – № 1. – С. 9–16.
11. Волхонский В. В., Малышкин С. Л. К вопросу единства терминологии в задачах физической защиты объектов // Информационно-управляющие системы. – 2013. – № 5. – С. 61–68.

12. Волхонский В. В., Малышкин С. Л. Определение, состав и функции систем физической защиты // Алгоритм безопасности. – 2013. – № 3. – С. 18–21.
13. English/Russian and Russian/English Glossary of Physical Protection Terms / Soo Hoo, M. S. – Sandia National Labs., Albuquerque, NM (United States), 1995. – 103 p.
14. Новикова Е. Г., Петраков А. В., Рабовский С. В. Бизнес – Безопасность – Телекоммуникации: Терминологический словарь. – М.: Радио и связь, 2001. – 304 с.
15. Закон Российской Федерации N 2446-1 "О безопасности" от 05.03.1992 (ред. от 26.06.2008).
16. ГОСТ Р 52551-2006. Системы охраны и безопасности. Национальный стандарт Российской Федерации. Термины и определения. – М.: Стандартинформ, 2006. – 19 с.
17. СП 132.13330.2011 Обеспечение антитеррористической защищенности зданий и сооружений. Общие требования проектирования: свод правил: введ. 20.09.2011. – 6 с.
18. СТО – П-119-01-05.2012 Обеспечение антитеррористической защищенности зданий и сооружений. Общие требования: утвержден 04.05.2012. – 43 с.
19. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения: введ. 1.02.2008. – М.: Стандартинформ, 2008. – 8 с.
20. ГОСТ Р 52069.0-2003. Защита информации. Система стандартов. Основные положения: введ. 01.01.2004. – М.: Изд-во стандартов, 2003. – 12 с.
21. ГОСТ Р 51275. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения: введ. 26.12.2006. – М.: Стандартинформ, 2007. – 11 с.
22. Федеральный закон от 21.11.1995 N 170-ФЗ "Об использовании атомной энергии" // Собрание законодательства Российской Федерации. – 1995. – № 48. – С. 45–52.

23. РД-07-01-2004 Методические указания по проведению оценки состояния физической защиты ядерно- и радиационно-опасных объектов по результатам проведенной инспекции: введ. 01.01.2005. www.russgost.ru (дата обращения: 12.11.2012).
24. Постановление Правительства РФ от 19.07.2007 N 456 «Об утверждении Правил физической защиты ядерных материалов, ядерных установок и пунктов хранения ядерных материалов». www.referent. ru (дата обращения: 12.11.2012).
25. НП-083-07 Требования к системам физической защиты ядерных материалов, ядерных установок и пунктов хранения ядерных материалов: введ. 01.06.2008// Ядерная и радиационная безопасность. – 2008. – № 2. – С. 15–30.
26. ГОСТ Р 52860-2007. Технические средства физической защиты. Общие технические требования: введ. 27.12.2007. – М.: Стандартинформ, 2008. – 27 с.
27. Bari R., et al. Proliferation Resistance and Physical Protection Evaluation Methodology Development and Applications. – Brookhaven National Laboratory, 2009. – P. 61–69.
28. Fedrick Charlie, Matthew Brayon. Physical Protection Principles / – Nuclear Installation Dept. AELB. – Retrieved: http://www.aelb.gov.my (дата обращения: 11.11.2012).
29. Edward J. Conrath, et al. Structural Design for Physical Security: State of the Practice / Task Committee, Structural Engineering Institute, ASCE Reston, 1999. – 264 p.
30. missinglinksecurity.com: Missing Link Security. http://www.missinglinksecurity.com/ (дата обращения: 15.11.2012).
31. Бояринцев А. В., Ничиков А. В., Редькин В. Б. Общий подход к разработке моделей нарушителей // Системы безопасности. – 2007. – № 4. – С. 50–53.
32. Бояринцев А. В., Ничиков А. В. Использование перечней угроз и моделей нарушителя при формировании облика сис-

тем физической защиты объектов // Мир и безопасность. – 2008. – № 4.

33. Радаев Н. Н. Моделируя повадки нарушителя. Формализация нарушителя в задаче оценки эффективности системы физической защиты объекта // Безопасность, достоверность, информация. – 2008. – № 1. – С. 16–22.

34. Цветков А. Г. Принципы количественной оценки эффективности радиоэлектронных средств. – М.: Сов. радио, 1971. – 200 с.

35. Волхонский В. В., Малышкин С. Л. Сравнительный анализ методов оценки эффективности систем физической защиты объекту // Охрана, безопасность, связь – 2012: материалы XVI Всерос. науч.-практ. конф., Воронеж. – 2012. – С. 206-207.

УНИВЕРСИТЕТ ИТМО

Миссия университета – генерация передовых знаний, внедрение инновационных разработок и подготовка элитных кадров, способных действовать в условиях быстро меняющегося мира и обеспечивать опережающее развитие науки, технологий и других областей для содействия решению актуальных задач.

КАФЕДРА СВЕТОВЫХ ТЕХОЛОГИЙ И ОПТОЭЛЕКТРОНИКИ

Кафедра световых технологий и оптоэлектроники (СТО) организована в 2015 году и является преемницей кафедры твердотельной оптоэлектроники (ТТОЭ) и базовой магистерской кафедры светодиодных технологий (СТ). Заведующий кафедрой – Бугров В.Е. доктор физ.-мат. наук, лауреат премии Правительства РФ в области науки и техники 2012 года, директор мегафакультета фотоники.

Кафедра ТТОЭ организована в 1988 году в период активного развития оптоэлетроники как компонентной базы высокоскоростных систем передачи и обработки информации и ее выделения в самостоятельную область науки, техники и производства. Заведующий кафедрой с 1988 по 2015 гг. – доктор техн. наук, профессор Прокопенко В.Т. В 2002 году по результатам научных исследований и подготовку научных кадров высшей квалификации ему присвоено почетное звание «Заслуженный деятель науки РФ».

Кафедра СТ основана в октябре 2011 года, осуществляла свою деятельность в рамках программы стратегического партнерства Санкт-Петербургского национального университета информационных технологий, механики и оптики (Университе-

та ИТМО) и компании ЗАО «Оптоган», а затем ЗАО «Светлана-Оптоэлектроника». Заведующий кафедрой – доктор физ.-мат. наук Бугров В.Е.

Кафедра СТО реализует программы подготовки бакалавров 12.03.05 «Лазеры для информационно-коммуникационных систем»и магистров 12.04.02 «Светодиодные технологии» и 16.04.01 «Физика и техника оптоэлектронных информационных систем»

Специалисты кафедры обладают большим опытом научной, преподавательской и производственной деятельности. Кафедра имеет оснащенные учебные и научные лаборатории. Основные направления научной деятельности сотрудников кафедры СТО сосредоточены в области спектроскопии твердого тела, разработки и создания светодиодных модулей различного применения и исследования их свойств, разработки и исследования свойств различных (рефрактометрических, волоконно-оптических и др.) датчиков измерения физических величин.

Волхонский Владимир Владимирович

СИСТЕМЫ ФИЗИЧЕСКОЙ ЗАЩИТЫ
Основы теории

Учебное пособие

Корректор *А. Г. Ларионова*

В авторской редакции
Редакционно-издательский отдел Университета ИТМО
Зав. РИО Н.Ф. Гусарова
Подписано к печати
Заказ №
Тираж 100 экз.
Отпечатано на ризографе

Редакционно-издательский отдел
Университета ИТМО
197101, Санкт-Петербург, Кронверкский пр., 49