

УДК 621.39

К ВОПРОСУ ЕДИНСТВА ТЕРМИНОЛОГИИ В ЗАДАЧАХ ФИЗИЧЕСКОЙ ЗАЩИТЫ ОБЪЕКТОВ

В. В. Волхонский,

канд. техн. наук, доцент

С. Л. Малышкин,

аспирант

Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

Анализируются термины и определения физической защиты, используемые в различных предметно-ориентированных областях информационной, ядерной, антикриминальной и антитеррористической безопасности, в государственных стандартах и литературных источниках. Показаны существенные отличия в используемых определениях. Предлагаются единые обоснованные определения физической защиты и системы физической защиты, согласующиеся с нормативными документами и стандартами и позволяющие устранить разночтения в терминологии в области методов и средств обеспечения физической безопасности объектов.

Ключевые слова — физическая защита, физическая безопасность, терминология, определения.

Введение

В настоящее время сложилась ситуация, когда специалисты в области обеспечения безопасности иногда говорят на «разных языках», используя различные формулировки для обозначения одного и того же понятия и одинаковые термины для обозначения разных задач и систем. Вызвано это тем, что ряд существующих терминов являются в значительной степени проблемно-ориентированными. Это относится, в частности, к таким понятиям как «физическая защита» (ФЗ) и «система физической защиты» (СФЗ). Такое отсутствие единства терминологии в некоторых случаях приводит к проблемам как в области практики создания СФЗ, так и при решении вопросов теории синтеза и анализа средств и систем обеспечения безопасности.

С этой точки зрения нужно говорить о целесообразности и актуальности формулировки общих терминов, справедливых для любых объектов обеспечения безопасности. Поэтому в данной работе авторы ставят следующие основные задачи:

— анализ известных терминов «физическая защита» и «система физической защиты», используемых в областях информационной и ядерной безопасности и в других предметно-ориентированных областях;

— на основе этого анализа — формулировка единых терминов, с одной стороны, инвариантных к конкретным проблемно-ориентированным областям и, с другой стороны, применимых для других предметно-ориентированных задач обеспечения безопасности, терминов, согласующихся с уже имеющимися определениями государственных стандартов.

Анализ ситуации в области терминологии

Вопросы терминологии в различных областях методов и средств обеспечения безопасности (МСОБ), например, информационной или ядерной, разрабатывались, как правило, в соответствии с историческими потребностями и востребованностью тех или иных МСОБ. На начальном этапе упомянутые понятия ФЗ и СФЗ формулировались в разных предметно-ориентированных областях с учетом специфики каждой конкретной области, что неизбежно ограничивало общность понятия. Конечно, предметно-ориентированные определения также нужны, однако они, как минимум, должны быть согласованы с общими определениями.

Более того, само понятие «физическая защита» трактуется в разных документах и особенно разными авторами принципиально различным образом. Существует, например, мнение, что ин-

формационная безопасность не включает ФЗ, при том, что в государственных стандартах определено понятие ФЗ информации [1—3].

Этот вопрос важен и с точки зрения международного общения специалистов, требующего перевода рассматриваемых понятий с русского на английский и наоборот. Примером попытки решить такую задачу может служить работа [4].

На современном этапе развития систем безопасности и, как их частных случаев, СФЗ в условиях увеличения количества угроз и способов их реализации, роста разнообразия объектов обеспечения безопасности (ООБ), различных МСОБ возникает необходимость обобщения и уточнения существующих понятий.

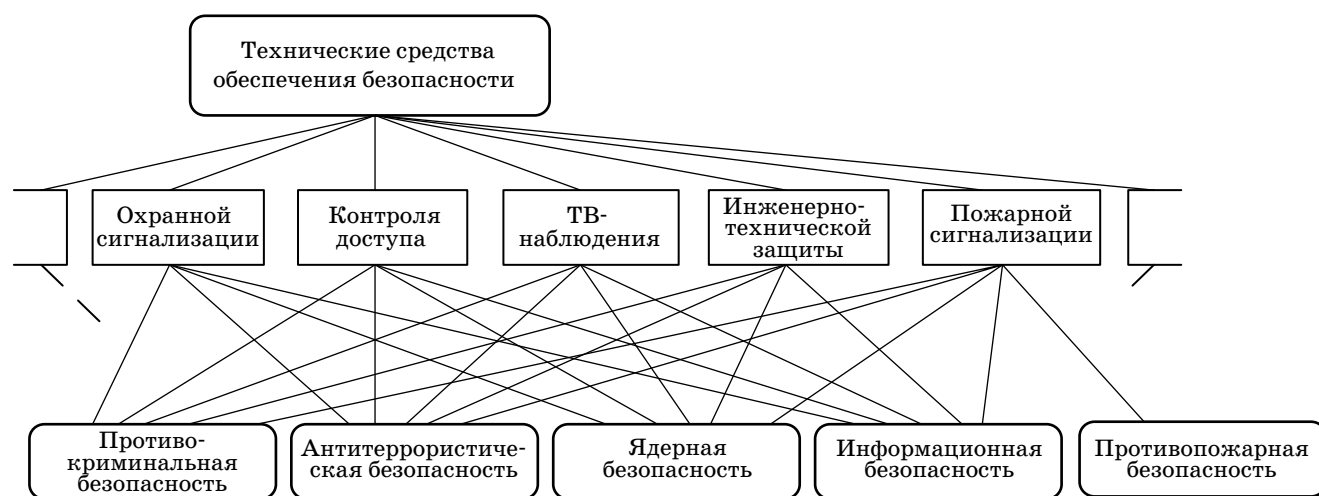
Наиболее полно и логично с научно-методической точки зрения термины, связанные с обеспечением ФЗ, сформулированы применительно к задачам ФЗ информации как одного из видов защиты информации (ЗИ). Это же можно сказать и о вопросах защиты ядерных объектов в силу их чрезвычайной важности (возможности нанесения не просто существенных, а катастрофических потерь). Однако о других проблемно-ориентированных областях этого сказать нельзя — термины, определяющие ФЗ и СФЗ, либо практически не используются, либо имеют другой, зачастую принципиально отличный смысл.

В соответствующих документах [1—3] даны определения рассматриваемых терминов для задач ЗИ. И это в определенной степени понятно, поскольку задачи ЗИ требуют использования практически всех МСОБ, так как обеспечение ЗИ невозможно без обеспечения безопасности собственно объекта информатизации и средств обработки и хранения информации, находящихся на

нем, в отличие от частных задач, к примеру, обеспечения безопасности только материальных ресурсов.

Нужно отметить и тот факт, что на настоящем уровне развития системы безопасности объекты информатизации становятся наиболее общими и сложными (с точки зрения обеспечения безопасности), требующими применения наибольшего перечня МСОБ. Ведь современные объекты в большинстве случаев являются в той или иной степени объектами информатизации. Так, любой, даже небольшой офис или квартира сейчас немыслимы без компьютерных средств обработки, хранения и передачи информации. Можно ли решить задачу информационной безопасности серверной как объекта информатизации, например, без контроля окружающей температуры (повышение которой может вызвать выход из строя оборудования) или учета риска затопления?

Еще одна сторона рассматриваемого вопроса состоит в том, что в современных условиях в значительном числе случаев трудно и обычно нецелесообразно разделять подсистемы безопасности или выполняемые ими функции. Так, для одного и того же объекта обеспечения безопасности одни и те же средства, к примеру, охранной сигнализации, контроля доступа, ТВ-наблюдения и др., могут решать задачи антитеррористической, противокриминальной, информационной и других видов безопасности. И, наоборот, материальные ресурсы могут быть объектом обеспечения безопасности, например информационной. Однако в некоторых задачах, в частности, в области средств противокриминальной безопасности (систем охранной сигнализации и др.) термин «физическая защита» практически не используется или ис-



■ Технические средства обеспечения безопасности

пользуется в другом смысле, отличном от задач информационной и ядерной безопасности.

Сказанное иллюстрирует рисунок, где представлен основной состав технических средств обеспечения физической безопасности — охранной и пожарной сигнализации, ТВ-наблюдения, контроля доступа, инженерно-технической защиты и т. д. А также показана необходимость использования перечисленных средств для решения различных прикладных задач обеспечения безопасности — противокриминальной, антитеррористической, информационной и др.

Очевидно, что одни и те же средства используются практически во всех задачах. А это также подтверждает целесообразность решения поставленной задачи — формулировки единых терминов.

Известные определения для предметно-ориентированных приложений

Проанализируем основные определения, касающиеся СФЗ, представленные в стандартах и специальной литературе. Как уже отмечалось, в основном приводятся определения, учитывающие специфику различных предметно-ориентированных отраслей.

Защита информации

Для задач ЗИ основными документами можно считать стандарты [1—3]. В них сформулированы следующие понятия и определения.

В соответствии со стандартом [1], термин «защита информации» включает четыре понятия: правовую, криптографическую, техническую и физическую защиту информации.

Физическая защита информации определена как защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты. При этом:

1) организационные мероприятия по обеспечению ФЗ информации предусматривают установление режимных, временных, территориальных, пространственных ограничений на условия использования и распорядок работы объекта защиты;

2) к объектам ЗИ могут быть отнесены охраняемая территория, здание (сооружение), выделенное помещение, информация и (или) информационные ресурсы объекта информатизации.

В свою очередь термин «объект информатизации» раскрывается в ГОСТах [1, 3].

Объект информатизации [3] — совокупность информационных ресурсов, средств и систем об-

работки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров.

Объект информатизации защищаемый [1] — объект информатизации, предназначенный для обработки защищаемой информации с требуемым уровнем ее защищенности.

Техника ЗИ, среди прочих, включает ряд средств ФЗ информации на объекте, а именно [2]:

- охранную и охранно-пожарную сигнализацию;
- охранное телевидение и наблюдение;
- инженерно-техническую защиту объектов, а также управления, например, доступом к информации.

Отметим, что приведенные выше определение термина «объект информатизации» и состав техники ЗИ можно рассматривать как пример удачной формулировки ООБ и МСОБ. Формулировки общей и в то же время достаточно детализированной, учитывающей практически все аспекты конкретной прикладной задачи обеспечения информационной безопасности.

Однако с точки зрения общности имеет смысл учитывать вопросы защиты не только от проникновения или доступа неуполномоченных физических лиц, но и от других угроз (в общем случае произвольных), приводящих к существенным потерям.

Ядерная безопасность

Для ядерных объектов соответствующие термины приводятся в документах [5—9].

В соответствии с законом [5], *физическая защита* ядерных установок, радиационных источников, пунктов хранения ядерных материалов и радиоактивных веществ предусматривает единую систему планирования, координации, контроля и реализации комплекса технических и организационных мер, направленных на:

- предотвращение несанкционированного проникновения на территорию ядерных установок, радиационных источников и пунктов хранения, предотвращение несанкционированного доступа к ядерным материалам и радиоактивным веществам, предотвращение их хищения или порчи;
- своевременное обнаружение и пресечение любых посягательств на целостность и сохранность ядерных материалов и радиоактивных веществ, своевременное обнаружение и пресечение диверсионных и террористических актов, угро-

жающих безопасности ядерных установок, радиационных источников и пунктов хранения;

— обнаружение и возвращение пропавших или похищенных ядерных материалов и радиоактивных веществ.

В документе [6] представлены следующие определения.

Физическая защита — совокупность организационных мероприятий, инженерно-технических средств и действий подразделений охраны в целях предотвращения диверсий или хищений ядерных материалов.

Система физической защиты ядерно-опасных объектов и радиационно-опасных объектов — совокупность организационных мероприятий, инженерно-технических средств и действий подразделений охраны, предназначенных для обеспечения физической защиты ядерных материалов, ядерных установок, радиоактивных веществ, радиационных источников.

В постановлении [7] приведены другие определения.

Физическая защита — деятельность в области использования атомной энергии, осуществляемая в целях предотвращения диверсий и хищений в отношении ядерных материалов, ядерных установок и пунктов хранения.

Система физической защиты представляет собой единую систему планирования, координации, контроля и реализации комплекса технических и организационных мер для осуществления физической защиты.

Также к отрасли ядерной безопасности относятся следующие определения [10].

Физическая защита — совокупность организационных мероприятий, инженерно-технических средств и действий подразделений охраны в целях предотвращения диверсий или хищений.

Система физической защиты — система организационных, административных и правовых мер и инженерно-технических средств, предназначенных для обеспечения физической защиты ядерных материалов и ядерных установок на конкретном ядерном объекте.

Задачи ФЗ на ядерном объекте [7]:

— предупреждение несанкционированных действий;

— своевременное обнаружение несанкционированных действий;

— задержка (замедление) проникновения (продвижения) нарушителя;

— реагирование на несанкционированные действия и нейтрализация нарушителей для пресечения несанкционированных действий.

В постановлении [7] также приведен состав средств СФЗ. Так, *инженерными средствами* СФЗ являются физические барьеры, посты охраны и

инженерное оборудование охраняемых зон и постов охраны. *Техническими средствами* СФЗ являются элементы и устройства, входящие в состав следующих основных функциональных систем:

— охранной сигнализации;

— тревожно-вызывной сигнализации;

— контроля и управления доступом;

— оптико-электронного наблюдения и оценки ситуации;

— оперативной связи и оповещения (в том числе средств проводной связи и радиосвязи);

— защиты информации;

— обеспечения электропитания, освещения.

В документе [8] рассмотрены требования к СФЗ и ее составным частям. В частности, согласно данному документу, *система физической защиты* является частью общей системы организационно-технических мер, осуществляемых на ядерных объектах в целях обеспечения безопасности деятельности в области использования атомной энергии.

Общие технические требования к техническим средствам ФЗ ядерных объектов и к составным частям СФЗ устанавливает стандарт [9], в том числе требования надежности, эргономики, технологичности, комплектности.

Отметим имеющийся, на наш взгляд, недостаток с точки зрения общности определений в области ядерной безопасности, заключающийся в том, что практически во всех определениях угрозой ООБ считаются неуполномоченные физические лица (нарушители). Однако очевидно, что есть и ряд других угроз, например, исходящих от сотрудников, т. е. формально уполномоченных для доступа лиц, или природного характера.

Противокриминальная защита

В области противокриминальной защиты или, как ее еще называют, охраны термин «физическая защита» в смысле, определенном стандартами в области информационной безопасности, практически не используется. Хотя применяются те же самые технические средства. Ряд схожих по звучанию терминов и понятий предлагается в различных публикациях.

Так, в учебном пособии [12], посвященном системам охранной сигнализации, система обеспечения безопасности объекта определяется как совокупность *физической защиты, инженерной защиты, технической защиты и специальной защиты*. Автор использует следующие определения перечисленных терминов.

Физическая защита обеспечивается службой охраны, основной задачей которой является предупреждение несанкционированного физического проникновения на территорию, в здания и

помещения объекта злоумышленников и их сдерживание в течение расчетного времени (до прибытия полиции или сил поддержки).

Инженерная защита предусматривает использование усиленных дверей и дверных коробок, металлических решеток, усиленных ограждающих конструкций, усиленных запоров, сейфов повышенной стойкости.

Техническая защита включает систему охранной сигнализации, систему телевизионного наблюдения, систему тревожного оповещения, автоматизированную систему контроля доступа, переговорные устройства, средства связи, пожарной сигнализации, средства проверки почтовой корреспонденции, охранного освещения, резервного (аварийного) электропитания, систему дежурного и тревожного освещения.

Специальная защита обеспечивает защиту от утечки информации, представляющей особую ценность, а также проверку надежности (лояльности) персонала службы охраны, материально ответственных лиц и некоторых других категорий служащих.

Заметим, что термины «физическая защита» и «техническая защита», используемые в работе [12], принципиально расходятся с рассмотренными выше формулировками стандартов для задач ЗИ и ядерной безопасности.

Общие определения

Рассмотрим еще несколько определений, которые обладают определенной степенью общности и могут быть отнесены к разным предметно-ориентированным областям, например, противокриминальной, антитеррористической и другим видам защиты.

В работе [11] даются следующие определения.

Система физической защиты представляет собой совокупность правовых норм, организационных мер и технических решений, направленных на защиту жизненно важных интересов и ресурсов охраняемого объекта от угроз, источниками которых являются несанкционированные воздействия физических лиц.

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

С точки зрения общности формулировок может быть полезным определение системы безопасности [13], применимое к любым предметно-ориентированным областям: *система безопасности* — это совокупность всех методов и средств, обеспечивающих поддержание безопасного состояния объекта, предотвращение, обнаружение

и ликвидацию угроз жизни, здоровью, среде обитания, имуществу и информации.

В рассматриваемом определении можно отметить один, возможно спорный, момент: весь этот перечень ООБ формально можно сократить до понятия «ресурсы», которые могут быть людскими, информационными, материальными, природными, финансовыми, транспортными и др. Однако перечень в определении не учитывает некоторые виды ресурсов, например транспортные или финансовые. Поэтому имеет смысл дополнить перечень словом «ресурсами». Но в силу важности и специфики обеспечения безопасности каждой из первых четырех составляющих их целесообразно включать в определение, не обобщая.

Основываясь на этом общем определении системы безопасности, можно выделить следующие составляющие этого определения применительно к СФЗ как частному случаю системы безопасности:

- объект физической защиты;
- угрозы этому объекту;
- средства (технические и программные) и методы (правовые нормы, организационные мероприятия и т. п.) ФЗ объекта.

Антитеррористическая защита

Наиболее близкими к рассматриваемым терминам в области антитеррористической безопасности можно считать следующие.

Обеспечение антитеррористической защищенности — реализация совокупности проектных решений, организационно-технических и специальных мероприятий, направленных на обеспечение безопасности здания (сооружения) в целях предотвращения совершения террористического акта и (или) минимизации его последствий [14].

Система обеспечения антитеррористической защищенности — организационно-техническая система, включающая в себя совокупность технических систем антитеррористической защищенности, технических средств или их комплексов, программное обеспечение, а также документированные процедуры штатных действий персонала, эксплуатационную документацию, материалы, инструменты, приборы, необходимые для использования в антитеррористической защищенности объекта [15].

Антитеррористическая защищенность объекта — состояние здания, строения, сооружения или иного объекта, при котором обеспечивается безопасность его функционирования посредством применения инженерно-технических и режимных мер, направленных на предотвращение совершения террористического акта [15].

Эти определения по сути совпадают с определениями из области ядерной и информационной

безопасности, хотя по формулировкам имеют достаточно заметные различия.

Терминология в иностранной литературе

В зарубежной литературе используются нижеперечисленные основные термины.

Физическая защита (Physical Protection) — это характеристика ядерных энергетических систем, которая определяет степень противодействия краже материалов, пригодных для ядерных взрывных устройств или устройств рассеивания радиации, а также саботажу объектов и транспортировке межнациональными организациями и другими внешними нарушителями [16].

Система физической защиты (Physical Protection System) — совокупность людей, процедур и оборудования для физической защиты имущества или сооружений [17].

Физическая охрана (безопасность) (Physical Security) характеризует меры, разработанные для ограничения несанкционированного доступа персонала (в том числе атакующих или даже случайных злоумышленников) в здание, на объект, к ресурсам или хранимой информации, а также определяет правила по разработке структуры противодействия потенциально враждебным действиям [18].

Физическая защита (Physical Security) — это защита персонала, оборудования, программ, сетей и данных от физических явлений и событий, которые могут привести к существенным потерям или нанести урон предприятию, учреждению или организации. Она включает защиту от пожара, стихийных бедствий, хищения, кражи со взломом, вандализма и терроризма [19].

Перевод этих терминов свидетельствует об их близости к терминам, рассмотренным выше для обеспечения ЗИ и ядерной безопасности.

Заметим, что определение *системы физической защиты*, данное в стандарте [15], является наиболее общим, относящимся к любым объектам.

Анализируя все вышесказанное, можно сделать выводы о следующих особенностях существующих определений:

- наличие ограничений в существующей терминологии, в частности, учитывающих не все угрозы;

- наличие явного разночтения в трактовке одинаковых терминов в разных областях, в различных документах и разными авторами;

- отсутствие единых терминов, применимых с необходимыми уточнениями, к разным предметно-ориентированным областям;

- наличие наиболее корректной терминологии в области ЗИ, что позволяет взять эти определения за основу.

Все это в целом подтверждает целесообразность поставленной авторами в работе задачи.

Предлагаемые термины

Обоснуем и сформулируем максимально общие определения ФЗ и СФЗ, которые, при необходимости, могли бы служить для формулировки частных и более детальных определений для предметно-ориентированных областей. Анализируя определения, приведенные выше, можно сделать вывод, что термины «физическая защита» или «система физической защиты» используются в четырех смысловых значениях:

- 1) защита от физических лиц;
- 2) защита физическими лицами (сотрудниками служб охраны);
- 3) использование физических препятствий (и как следствие — задержки для их преодоления) для достижения цели нарушителем (угрозой);
- 4) обеспечение физической целостности объектов.

Можно говорить о том, что в той или иной мере правильны все смысловые значения, но применительно только к конкретным предметно-ориентированным задачам. Кроме того, они учитывают не все угрозы. Проанализируем эти смысловые понятия.

В первом пункте 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. И угроз не только прямых, но и опосредованных. Примерами могут служить ситуации на Чернобыльской АЭС (реализовавшаяся угроза — уполномоченные лица — персонал) и АЭС «Фокусима» (реализовавшаяся угроза — природное явление). Таким образом, подобное ограничение перечня угроз снижает общность определений, поскольку одни и те же последствия могут быть при реализации разных угроз.

Второй пункт представляется также частным случаем, поскольку сотрудники службы охраны составляют лишь часть системы обеспечения физической безопасности и практически всегда используются в сочетании с техническими средствами.

Третий также является частным случаем, так как препятствия, создающие задержку в развитии угрозы, могут быть не только физические, а, например, программные, организационные и др. Кроме того, только одними препятствиями задача физической защиты не решается.

Поэтому последнее смысловое значение — *обеспечение физической целостности ООБ* — представляется наиболее правильным и общим, так

как определяет объект защиты от произвольных в общем случае угроз.

К такому же выводу можно прийти и путем других рассуждений. Выделим главное, суть, которая должна определять понятия. Нет сомнения, что главное — это *объект защиты* (объект обеспечения безопасности), поскольку все делается ради этого объекта. Поэтому, по нашему мнению, надо говорить, прежде всего, о *сохранении физической целостности объекта защиты* или связанных с ним и влияющих на его физическую целостность составляющих (например, окружающей среды). Так, применительно к задачам ЗИ — это объект информатизации, включая носители и средства обработки информации.

Более того, в рассмотренных выше терминах ЗИ и ядерной безопасности явно прослеживается задача сохранения физической целостности ООБ.

Таким образом, можно дать следующие определения ФЗ и СФЗ.

Физическая защита — это совокупность действий по обеспечению физической целостности ООБ.

Система физической защиты — это совокупность методов и средств обеспечения физической целостности ООБ.

При этом под различными составляющими определения будем понимать следующее:

- совокупность методов — правовые, организационные, юридические, морально-этические и другие методы, необходимые для решения задачи;

- совокупность средств — средства, необходимые для решения задачи, такие как аппаратные, программные и инженерно-технические. Применительно к конкретным средствам, используемым в настоящее время, они наиболее полно определены в стандарте [2];

- физическая целостность — учитывает кроме собственно физической целостности также изменение взаимного пространственного расположения различных элементов ООБ без нарушения целостности каждого из элементов (например, в случае кражи — это перемещение объекта);

- объект обеспечения безопасности — жизнь, здоровье, среда обитания, имущество, информация [13] и ресурсы.

Вышесказанное практически полностью согласуется с определениями стандартов (в первую очередь, [1, 2]) с учетом конкретизации объекта обеспечения физической безопасности и частного случая угроз (нарушителя).

Сформулируем перечень основных средств ФЗ ООБ с учетом приведенных в документах [2, 7]:

- охранная сигнализация;
- пожарная сигнализация;
- ТВ-наблюдение;

- контроль доступа;
- инженерно-техническая защита;
- обеспечение (связи, энергопитания, транспорта и т. п.).

Остановимся еще на одном понятии, не относящемся к техническим средствам ФЗ, но напрямую связанном с такой важной составляющей обеспечения безопасности, как реагирование на угрозы, — персонал служб безопасности. Тем более, что это трактуется некоторыми авторами как собственно ФЗ [12].

В документе [4] дается два схожих смысловых значения определений. *Силы службы безопасности* — силы охраны на ядерном объекте, в чьи обязанности входит первыми нанести ответный удар в случае атаки. *Силы ответного действия* — персонал охраны, немедленно принимающий ответные действия, направленные на отражение угрозы, исходящей от нарушителя.

Обобщая эти определения на произвольные ООБ и угрозы, можно дать соответствующее определение.

Средства реагирования — ресурсы системы безопасности (персонал, технические, программные, инженерные и организационные средства) для реагирования на возможную или возникшую угрозу ООБ.

Авторы осознанно включили в определение не только персонал охраны, но и технические, программные, инженерные и организационные 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.

Заключение

В настоящей работе получены следующие основные результаты.

1. Проанализированы основные термины стандартов, руководящих документов и работ различных авторов в областях обеспечения информационной, ядерной и других видов безопасности.

2. Показано разночтение одних и тех же терминов, использующихся в разных предметных областях и сформулированных разными авторами, а также недостаточная общность определений.

3. Показана целесообразность разработки общих терминов, применимых не только для задач обеспечения информационной и ядерной безопасности, но и для любых других задач.

4. Предложены обоснованные определения ФЗ и СФЗ, с одной стороны, согласующиеся с руководящими документами и стандартами в пред-

метно-ориентированных областях и, с другой стороны, являющиеся общими и позволяющие устранить разночтения в терминологии в области методов и средств обеспечения физической безопасности.

5. Сформулирован состав технических средств СФЗ и его взаимосвязь с техническими средствами объединенной системы безопасности.

Литература

1. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения: введ. 01.02.2008. – М.: Стандартинформ, 2008. – 8 с.
2. ГОСТ Р 52069.0-2003. Защита информации. Система стандартов. Основные положения: введ. 01.01.2004. – М.: Изд-во стандартов, 2003. – 12 с.
3. ГОСТ Р 51275. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения: введ. 01.02.2008. <http://protect.gost.ru/document.aspx?control=7&id=129071> (дата обращения: 12.11.2012).
4. **Soo Hoo**. English/Russian and Russian/English Glossary of Physical Protection Terms. – Sandia National Labs., Albuquerque, NM (United States), 1995. – 103 p.
5. **Федеральный закон** от 21.11.1995 № 170-ФЗ «Об использовании атомной энергии» // Собрание законодательства Российской Федерации. 1995. № 48. С. 45–52.
6. **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).
7. **Постановление** Правительства РФ от 19.07.2007 № 456 «Об утверждении Правил физической защиты ядерных материалов, ядерных установок и пунктов хранения ядерных материалов». www.referent.ru (дата обращения: 12.11.2012).
8. **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.
9. ГОСТ Р 52860-2007. Технические средства физической защиты. Общие технические требования:

В заключение отметим, что хотя авторы и старались максимально аргументировать свое мнение, они не считают предложенные термины окончательной версией. Работа в определенной степени носит дискуссионный характер, авторы готовы к обсуждению этого вопроса и с удовольствием выслушают замечания заинтересованных специалистов.

введ. 27.12.2007. – М.: Стандартинформ, 2008. – 27 с.

10. **Бондарев П. В.** и др. Физическая защита ядерных объектов / МИФИ. – М., 2004. – 489 с.
11. **Алаухов С. Ф., Коцербуба В. Я.** Концепция безопасности и принципы создания систем физической защиты важных промышленных объектов / ФГУП «НИКИРЭТ», 2005. www.sec.ru (дата обращения: 11.11.2012).
12. **Магауренов Р. Г.** Системы охранной сигнализации: основы теории и принципы построения: учеб. пособие. – М.: Горячая линия–Телеком, 2004. – 367 с.
13. **Волхонский В. В.** Системы охранной сигнализации. 2-е изд., доп. и перераб. – СПб.: Экополис и культура, 2005. – 204 с.
14. **СП 132.13330.2011**. Обеспечение антитеррористической защищенности зданий и сооружений. Общие требования проектирования: свод правил: введ. 20.09.2011. – 6 с.
15. **СТО – П-119-01-05.2012**. Обеспечение антитеррористической защищенности зданий и сооружений. Общие требования: утвержден 04.05.2012. – 43 с.
16. **Bari R.** et al. Proliferation Resistance and Physical Protection Evaluation Methodology Development and Applications / Brookhaven National Laboratory, 2009. – P. 61–69.
17. **Fedrick Charlie, Matthew Brayon**. Physical Protection Principles / Nuclear Installation Dept. AELB. – Retrieved: <http://www.aelb.gov.my> (дата обращения: 11.11.2012).
18. **Edward J. Conrath** et al. Structural Design for Physical Security: State of the Practice / Task Committee, Structural Engineering Institute, ASCE Reston, 1999. – 264 p.
19. **missinglinksecurity.com**: Missing Link Security. <http://www.missinglinksecurity.com/> (дата обращения: 15.11.2012).