УДК 65.012.8
https://doi.org/10.32686/1812-5220-2019-16-4-82-93

ISSN 1812-5220

Компоненты риска физической безопасности

Филиппов Д. Л.,
МГТУ им. Н. Э. Баумана,
105005, Россия, г. Москва,
2-я Бауманская ул., д. 5, стр. 1

Аннотация
В статье рассматриваются существующие методики анализа риска при проектировании систем физической защиты. Отмечено, что в экспертном методе анализа уязвимость оценивается интегрально, что не гарантирует соблюдения принципа равнопрочности, уязвимости элементов физической защиты рассматриваются без связи с уязвимостями самого объекта и параметрами модели нарушителя, не учитываются такие показатели, как катализаторы и ингибиторы угрозы. Отмечено, что для повышения адекватности физической защиты требуется формирование банка данных угроз безопасности и актуальных уязвимостей.

Ключевые слова: физическая безопасность, ущерб, анализ угроз, субъект угрозы, уязвимость объекта.

Для цитирования: Филиппов Д. Л. Компоненты риска физической безопасности // Проблемы анализа риска. Т. 16. 2019. № 4. С. 82—93, https://doi.org/10.32686/1812-5220-2019-16-4-82-93

Components of physical security risk

Filippov Dmitry L.,
Bauman State Technical University,
105005, Russia, Moscow,
2nd Baumanskaya St., 5, bldg 1

Annotation
The article considers the existing methods of risk analysis in the design of physical protection systems. It is noted that in the expert method vulnerability assessed integrally, that does not guarantee the principle of equal strength, vulnerability elements of physical protection are considered without regard to the vulnerability of the object itself, and parameters of the model of the intruder, not taking into account such factors as catalysts and inhibitors of the threat. Noted that to improve the adequacy of physical protection required the formation of a databank of security threats and vulnerabilities.

Keywords: physical security, damage, analysis of threats, the subject of the threat, the vulnerability of the object.

For citation: Filippov Dmitry L. Components of physical security risk // Issues of Risk Analysis. Vol. 16. 2019. No. 4. P. 82—93, https://doi.org/10.32686/1812-5220-2019-16-4-82-93

Содержание

Введение

Все организации сталкиваются с определенной степенью физической угрозы, т. е. угрозы, исходящей от физического воздействия: террористической, криминальной, а также вызванной действиями человека техногенной или природной угрозы (при стихийных бедствиях).

Физическая безопасность объекта есть непременное условие его успешного функционирования и развития и поэтому важна для любых объектов и актуальна всегда.

Определение понятия «физическая безопасность» основывается на определении более общего понятия «безопасность». Однако ныне действующий Федеральный закон № 390-ФЗ «О безопасности» от 28.12.2010, отменяя определение ФЗ № 2446-1 от 05.03.1992 как состояние защищенности, своего определения на дает. Обратившись к другим нормативным документам, можно найти следующие формулировки.

1. Безопасность — состояние, при котором отсутствует недопустимый риск, связанный с причинением вреда жизни или здоровью граждан, имуществу физических или юридических лиц, государственному или муниципальному имуществу, окружающей среде… (Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании» (в ред. ФЗ от 09.05.2005 № 45-ФЗ, от 01.05.2007 № 65-ФЗ).

2. Безопасность — отсутствие неприемлемого риска (ГОСТ Р 51898-2002 Аспекты безопасности. Правила включения в стандарты).

3. Безопасность — отсутствие недопустимого риска, связанного с возможностью причинения вреда и (или) нанесения ущерба (Соглашение правительств государств — членов ЕАЭС от 25.01.2008 (в ред. от 10.10 2011)).

4. Безопасность — отсутствие недопустимого риска, связанного с возможностью нанесения ущерба (Российская энциклопедия по охране труда).

Приняв такое определение безопасности, приходим к выводу, что под физической безопасностью следует понимать отсутствие недопустимого риска физического воздействия на объект, связанного с недопустимым ущербом.

Однако подобное определение физической безопасности ни в отечественной ни в зарубежной литературе не встречается, зато широко распространено следующее.

Физическая безопасность — это мероприятия, входящие в состав обеспечения комплексной безопасности и направленные на создание системы защиты организации, активов и персонала от внешних угроз и противоправных действий физических лиц. Это технические средства охраны организации, сотрудники, обеспечивающие безопасность организации, действующая режимная (пропускная) система охраны организации, органично вписывающаяся в бизнес-процессы организации [21].

Физическая безопасность — это термин, используемый для определения интеграции людей, процедур и оборудования для защиты активов от угроз и рисков (от кражи, вандализма, саботажа и несанкционированного доступа) [22].

То есть понятие «физическая безопасность» ***подменяется*** понятием «физическая защита». Использование такого определения не позволяет анализировать факторы угрозы и получить обоснованные данные для противодействия.

Действительно, наиболее полно физическая безопасность обеспечивается интегрированной системой физической защиты (СФЗ) [12], однако такая система не есть стандартное решение, которое подходит для всех случаев. Система физической защиты для ее эффективности должна быть адекватна фактическому риску. Определение факторов риска, влияющих на конкретный объект, гарантирует, что конкретная организация видит наибольшую отдачу от инвестиций, затраченных на усилия по противодействию угрозам. Построение СФЗ без методической, аналитической оценки риска может привести к нерациональному использованию ресурсов на чрезмерную защиту, существенному ограничению функционирования объекта или, что еще хуже, не сможет обеспечить адекватную защиту критических элементов объекта.

1. Параметры риска — основа проектирования СФЗ

Как в России, так и за рубежом существует целый ряд методических разработок проектирования СФЗ, цель которых обеспечить эффективную защиту от всех возможных угроз и всех способов их реализации и в то же время поддерживать равновесие

с другими факторами, такими как стоимость системы, свободное функционирование и структурная целостность объекта [8, 9, 12, 13, 16]. Входные данные для проектирования чаще всего получают в результате исследования объекта безопасности и анализа угроз, являющихся элементами анализа риска.

«Риск» — одно из наиболее сложных, многогранных и противоречивых понятий в теории безопасности [1]. Стандартизованное определение риска нанесения ущерба: «Комплексный показатель, характеризующий вероятность возникновения ущерба за нормированный период времени и его величину» [3]. «Риск — это функция угрозы активам, последствий и уязвимости» [19].

Обеспечение физической безопасности часто понимается как снижение до приемлемого уровня рисков злонамеренных действий. При этом неприемлемый (недопустимый) риск определяют как возможность наступления такого события, в результате которого нанесенный ущерб больше наперед заданного фиксированного значения (базового критерия). Например, недопустимый ущерб для коммерческой организации может быть определен как ущерб, который не может быть возмещен полностью за счет средств, имеющихся для возмещения (страховых средств), и расчетной прибыли за время восстановления ее до начальной доходности. Такой ущерб приводит к прекращению деятельности коммерческой организации, то есть к банкротству.

На основе приведенных определений можно принять ожидаемый риск равным произведению вероятности события на величину ожидаемого ущерба.

$$R = P_a \cdot C, \tag{1}$$

где R — риск, P_a — вероятность реализации угрозы, C — величина ожидаемого ущерба.

Поскольку рассчитать вероятность наступления событий, влекущих за собой ущерб (likelihood of damage), заранее с приемлемой точностью практически невозможно из-за их недетерминированного характера, т. е. недостатка знаний о характере угрозы, сопутствующих обстоятельствах и др., применяют методы экспертной оценки, основанные на анализе ранее произошедших событий. Такие методы называют анализом угроз и анализом уязвимостей [8]. Приняв, что вероятность ущерба есть произведение вероятности существования угрозы и вероятности использования угрозой уязвимости

$$P_a = T \cdot V, \tag{2}$$

и сделав подстановку в (1), получим

$$R = T \cdot V \cdot C, \tag{3}$$

где R — риск, T — вероятность существования угрозы, V — вероятность использования угрозой уязвимости, C — величина ожидаемого ущерба.

По рекомендациям Сандийских лабораторий [20] разработка эффективной системы физической защиты включает в себя определение характеристик активов и определение контекста исследования, определение возможного ущерба, идентификацию и ранжирование угроз, оценку уязвимости, определение целей системы физической защиты, разработку концепции системы физической защиты, оценку эффективности проекта, вероятно, коррекцию и/или доработку.

Первый шаг разработки СФЗ требует подробного описания самого объекта — местоположение, границы участка, местоположение здания, планы этажей и точки доступа, т. е. контекста для анализа. Кроме того, необходимо идентифицировать применяемые технологии, характеристику рабочих состояний объекта безопасности и условий его функционирования, рабочие и аварийные режимы, выделить критические элементы, а также идентифицировать любые существующие функции физической защиты. Эта информация может быть получена из нескольких источников, включая чертежи проекта установки, описания процессов, отчеты по анализу безопасности, отчеты о воздействии на окружающую среду и обзоры объектов.

В отечественной практике при выработке требований к защите объектов такая процедура сходна с категорированием объекта. Категорирование учитывает, во-первых, государственную, общественно-социальную, коммерческую или личностную значимость объекта, т. е. ценность актива, во-вторых, вероятность возникновения чрезвычайной ситуации (ЧС) на объекте и его масштабы, возможно,

выходящие за пределы объекта, в-третьих, собственно материальные потери с учетом весового коэффициента, учитывающего возможность и время их восстановления.

2. Определение ущерба

Наряду с понятием «ущерб» (damage) часто используются и другие близкие или эквивалентные ему термины: вред (detriment), потери (loss), убытки (damages), урон (harm), последствия (consequences), гибель (downfall), затраты (costs) и т. д.

Ущерб (consequences) — 1) убытки, непредвиденные расходы, утрата имущества и денег или репутации, недополученная выгода; 2) вред, наносимый деятельностью одного субъекта другим субъектам.

Ущерб может быть **материальным**, если он заключается в полной или частичной утрате следующих активов:

- здания, сооружения, а также технологическое оборудование;
- финансовые ценности;
- ценность какого-либо предмета или вещества в материальном выражении, причем ценность вариативна и различна для ее обладателя и похитителя. Для вандала же она практически равна нулю;
- ресурсы. Производственные, топливные и энергоресурсы, трафик общедоступных вычислительных сетей;
- опасный предмет (материал), хищение которого может повлечь за собой многократно превосходящие его стоимость потери;
- художественная или культовая ценность, включая культовые здания и архитектурные памятники, которая также вариативна и часто невосполнима;
- условия жизнеобеспечения. С неуклонным ухудшением экологической обстановки на планете Земля и истощением ресурсов их материальная ценность будет только возрастать. Например, ценность питьевой воды, нефальсифицированных продуктов питания, чистого воздуха, рекреативных зон. Лишение человека этих условий является несомненным ущербом;
- основополагающие ценности человеческого общества. Жизнь человека. Здоровье. Свобода. Право выбора. Возможность развития. Способность к самосохранению, самовоспроизводству и самосовершенствованию.

Виртуальный ущерб предполагает потерю неосязаемых активов:

- информация;
- ноу-хау;
- бизнес-планы;
- имидж, репутация;
- потери доверия населения;
- свобода слова, свобода самовыражения.

Необходимо заметить, что виртуальные потери обязательно влекут за собой ряд материальных потерь. Тем не менее при проектировании СФЗ учету должен подлежать только прямой материальный ущерб, для которого разработаны относительно единообразные методы оценки и такой виртуальный ущерб, влияние которого на материальный очевидно. В противном случае неопределенность оценки возрастет многократно и сделает ее бессмысленной.

Очевидно, что приведенный список активов, полная или частичная утрата которых будет расценена как ущерб, не является ни окончательным, ни исчерпывающим. Что также относится и к спискам угроз и уязвимостей.

Различают прямой и косвенный ущерб**. К прямому** ущербу от какого-либо воздействия относятся выраженные в стоимостной форме затраты, потери и убытки, обусловленные именно этим воздействием в данное время и в данном конкретном месте. Составляющие прямого экономического ущерба, как правило, поддаются документальному подтверждению на уровне «первичного звена» (организации, предприятия, муниципального образования), основанному на данных бухгалтерского учета, актов списания имущества, иных документов, имеющих достаточно высокую степень достоверности и поддающихся проверке. Для физических лиц основу должны составлять экспертные оценки физического и экономического ущерба.

К **косвенному** ущербу от какого-то действия относятся вынужденные затраты, потери, убытки, обусловленные вторичными эффектами (действиями или бездействиями, порожденными первичным действием) природного, техногенного или террористического характера, которые являются основой для развития каскада косвенных потерь [7]. Главной составляющей косвенного ущерба для самого юридического и физического лица является упущенная

непосредственно им выгода в связи с прекращением или приостановкой деятельности вследствие чрезвычайной ситуации техногенного, природного характера или криминальной, или террористической деятельности.

3. Определение угроз

Выявление угроз — это сложный процесс, который слишком часто формализуется, потому что для оценки угрозы на первый взгляд недостаточно информации и он часто рассматривается как технически недостижимый.

По мнению специалистов Сандийских лабораторий, угрозой является все, что может сорвать миссию системы [16]. **Угроза (threat)** — наиболее конкретная и непосредственная форма опасности, создаваемая целенаправленной деятельностью откровенно враждебных сил. Опасность и угроза представляют собой разные уровни состояния, подрывающего безопасность социума. Угроза — это стадия крайнего обострения противоречий, непосредственно предконфликтное состояние, когда налицо готовность одного из субъектов применить силу в отношении конкретного объекта для достижения своих целей. В чем разница между опасностью и угрозой?

Во-первых, угрозу отличает от опасности степень готовности к причинению ущерба.

Во-вторых, угроза, как показано в [5], включает в себя как минимум два компонента: намерение (intention) и возможность (opportunity) нанесения ущерба объекту безопасности. Причем намерение генерируется источником угрозы в соответствии с его идеологией и реализуется субъектом угрозы, чаще всего называемым нарушителем, а возможность реализации угрозы определяется, с одной стороны, ресурсами угрозы, а с другой — способностью субъекта угрозы использовать уязвимости, неотъемлемые свойства объекта безопасности.

В-третьих, угроза всегда носит конкретно-адресный характер (targeting — нацеливание), что предполагает наличие явных субъекта угрозы и объекта, на который направлено ее действие, непосредственная возможность нанесения ущерба, от начала осуществления которой ее отделяет лишь временной интервал, необходимый для принятия решения о реализации угрозы, стечений обстоятельств, благоприятный случай или параметры развития аварийной ситуации.

Очевидно, что при снижении степени угрозы сама угроза как таковая полностью не исчезает, а трансформируется в свою потенциальную форму, содержание которой соответствует состоянию опасности. Таким образом, переход угроз в состояние опасностей приумножает количество последних, что подтверждается анализом объективных событий, произошедших в последние годы в мире. Отсюда следует, что отдельно взятый объект защитить, например, от криминальных угроз нельзя!

В табл. 1 приведены типовые угрозы различного характера.

Среди угроз, вызванных деятельностью человека, исходя из мотивации действий можно выделить:

- непреднамеренные угрозы, вызванные ошибками в проектировании объекта и его элементов, ошибками в действиях персонала и т. п.;
- преднамеренные угрозы, связанные с корыстными устремлениями людей.

Источники угроз по отношению к объекту безопасности могут быть внешними или внутренними.

В основе угрозы лежит идеология. Это может быть агрессивная политика, военная доктрина, фанатизм, пренебрежение к законам, безнравственность и коррупция, низкий уровень технической грамотности проектировщиков и безответственность и преступная халатность персонала. Источник угрозы располагает ресурсами для их исполнения, такими как информационные ресурсы, людские ресурсы, материальные и технические ресурсы, технологии, финансовые средства, руководства по террористической деятельности, методы обучения, методы влияния на исполнителей, специальное ПО.

Привлекательность объекта для источника угроз зависит от его целей — материальных, конкурентных, политических. Также она зависит от информированности о легкости или трудности достижения, об имеющихся уязвимостях или возможности их активизации или создания, о простоте или сложности осуществления угрозы и о материальной или целевой выгоде от реализации угрозы.

Катализаторы угроз — ситуации и события на объекте и в обществе в целом, технологические изменения, личные обстоятельства, давление

Таблица 1. Типовые угрозы различного характера
Table 1. Standard threats of various character

Виды угроз	Цель	Способ	Объект
Террористические	Влияние на внутреннюю и внешнюю политику государства	Террористические акты, захват заложников	Люди, сооружения, высокотехнологичные объекты
Криминальные	Незаконное обогащение	Хищения, шантаж, мошенничество, вандализм	Люди, материальные и культурные ценности, информация, репутация
Недобросовестная конкуренция (реализуется через криминальные)	Получение незаконных односторонних преимуществ	Хищение ноу-хау, образцов, подлог, вандализм, вербовка агентов влияния	Информация, продукция, производство, люди, репутация
Техногенные	Ложная экономия ресурсов и времени в проекте и создании объектов, наем персонала низкой квалификации	Аварии, катастрофы	Персонал, население окружающих районов, оборудование, структура объектов
Природные	Мнимый выигрыш в географическом положении, экономия в строительстве и эксплуатации	Ошибки расположения объекта и проекта, не учитывающие природные факторы	Люди, здания, сооружения, техническая инфраструктура

со стороны социальной среды, общественное восприятие. Возрастание выгоды от хищения, конкурентная выгода, вандализм (не приобретает, но тешит самолюбие), политические цели (террор). Стремление преступной группы получить финансовое вознаграждение, чтобы поддержать свой стиль жизни.

Ингибиторы угрозы делают объект непривлекательной целью. К ним относится трудность подготовки и осуществления противоправного действия, трудность преодоления системы физической защиты, нехватка времени на подготовку, отсутствие пособников, высокая стоимость участия, сомнительная выгода, чувствительность к восприятию общественности, восприятие социальной средой, боязнь захвата и физического воздействия, страх неудачи, правовые последствия в виде сурового и неотвратимого наказания.

Катализаторы и ингибиторы угроз в значительной мере устанавливаются при обследовании объекта.

Субъект угрозы — нарушитель — лицо или группа лиц, совершившее или пытающееся реализовать угрозу, а также лицо, оказывающее ему в этом содействие [15]. Под нарушителем в общем виде можно рассматривать лицо или группу лиц, которые в результате предумышленных или непредумышленных действий обеспечивают реализацию угроз безопасности объекта. Следует заметить, что на выбор термина «субъект угроз — нарушитель» повлияло широкое распространение метода «защита расстоянием» и определения безопасности как состояния защищенности. При структурном анализе феномена безопасности в качестве субъекта угроз далеко не всегда этот термин уместен.

Модель нарушителя — совокупность сведений о численности, оснащенности, подготовленности, осведомленности и тактике действий нарушителей, их мотивации и преследуемых ими целях, которые используются при выработке требований к системе физической защиты и оценке ее эффективности, т. е. представляет собой совокупность его качественных и количественных характеристик. Актуализация модели нарушителя приведена в статье [6], где рассматриваются три возможные модели нарушителя. Технологическая модель нарушителя (ТМН) — набор характеристик потенциальных нарушителей, при которых они способны реализовать соответствующие угрозы объекту. Оперативная модель нарушителя (ОМН) — предполагаемый набор характеристик потенциальных нарушителей на текущий момент времени. ОМН в значительной части должна быть результатом деятельности соответствующих компетентных органов (ФСБ,

МВД и пр.). Проектная модель нарушителя (ПМН) — суперпозиция технологической и оперативной моделей — набор характеристик потенциальных нарушителей, которым и должна успешно противостоять СФЗ объекта.

Способов или сценариев осуществления угроз физической безопасности существует множество. Их изучение, систематизация информации о попытках реализации различного рода угроз, имевших место в прошлом, представляют несомненную ценность, и именно на ней строятся экспертные заключения об уровне риска. Тем более что принятые в конкретной группе злоумышленников способы осуществления криминальных и даже террористических действий редко меняются. Однако появление новых способов и приемов всегда резко повышает вероятность реализации угрозы и приводит к более тяжелым последствиям. Некоторые сценарии осуществления угроз могут предполагать создание на охраняемом объекте нарушителем чрезвычайной ситуации (поджог, отключение электропитания, затопление, блокирование проходов, незапланированная потеря каналов связи и др.), поэтому решения по обеспечению безопасности при штатных, чрезвычайных и катастрофических ситуациях должны быть заранее проработаны по рациональному критерию.

Угрозы физической безопасности отличаются весьма широким разнообразием, возможно, поэтому они не имеют исчерпывающих перечней и описаний, таких как угрозы информационной безопасности в автоматизированных информационных системах, которые имеют такие стандартные описания. Например, банк данных угроз информационной безопасности ФСТЭК насчитывает уже 194 описанные угрозы и более 15 000 уязвимостей [11].

В табл. 2 приводится пример описания отдельной угрозы из этого банка данных.

Необходимо заметить, что в данном документе «источником угроз» называется нарушитель, с чем нельзя согласиться, по мнению автора, источник угроз — вся угрожающая структура.

Составление и постоянное пополнение аналогичного банка типовых угроз физической безопасности, несомненно, способствовало бы повышению адекватности анализа угроз при проектировании СФЗ.

Наиболее опасен технологический терроризм, заключающийся в применении или угрозе применения ядерного, химического и бактериологического оружия, радиоактивных и высокотоксичных химических, биологических веществ, а также угрозе захвата ядерных и иных промышленных объектов, представляющих повышенную опасность для жизни и здоровья людей. Криминальный терроризм заключается в использовании уголовными преступниками методов насилия и устрашения, заимствованных из практики террористических организаций. В пособии «Оценка и управление угрозой терроризма» департамента юстиции США [17]

Таблица 2. Описание угрозы из банка данных ФСТЭК
Table 2. Descriptions of threat from a databank of FSTEC

УБИ.160:	**Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации**
Описание угрозы	Угроза заключается в возможности осуществления внешним нарушителем кражи компьютера (и подключенных к нему устройств), USB-накопителей, оптических дисков или других средств хранения, обработки, ввода/вывода/передачи информации. Данная угроза обусловлена слабостями мер контроля физического доступа к средствам хранения, обработки и (или) ввода/вывода/передачи информации. Реализация данной угрозы возможна при условии наличия у нарушителя физического доступа к носителям информации (внешним, съемным и внутренним накопителям), средствам обработки информации (процессору, контроллерам устройств и т. п.) и средствам ввода/вывода информации (клавиатура и т. п.)
Источники угрозы	Внешний нарушитель с низким потенциалом
Объект воздействия	Сервер, рабочая станция, носитель информации, аппаратное обеспечение
Последствия реализации угрозы	Нарушение конфиденциальности. Нарушение доступности

показано, как уровень террористической угрозы определяется в зависимости от степени и комбинации следующих факторов:

- **наличие**: террористическая группа присутствует или может получить доступ к данному объекту, может располагаться в ближайшем населенном пункте. Существует информация об ее активности в течение последнего времени;
- **возможность**: возможность террористической группы для совершения теракта по оперативным данным была доказана, оценена численность и разработана оперативная модель нарушителя;
- **намерение**: имеются доказательства деятельности террористической группы, в том числе указано и оценено намерение и заинтересованность осуществлять террористическую деятельность на данном объекте или в данном населенном пункте;
- **история**: продемонстрирована террористическая деятельность террористической группы в прошлом;
- **таргетинг** (нацеливание): существует актуальная заслуживающая доверия информация или деятельность, которая свидетельствует о подготовке к конкретным террористическим операциям, как, например, сбор разведывательных данных группой подозреваемых, подготовка деструктивных устройств и другие действия. Угроза готовится для конкретной атаки;
- **среда безопасности**: указывает, влияет ли положение в области безопасности угрожаемой структуры на способность террористических элементов выполнять свои намерения. Рассматриваются вопросы о том, как относится юрисдикция к терроризму и принимались ли сильные проактивные контрмеры для борьбы с такой угрозой.

В соответствии с ГОСТ Р 52551-2006 Системы охраны и безопасности. Термины и определения «угроза террористическая — это совокупность условий и факторов, создающих опасность преднамеренного противоправного уничтожения или нанесения ущерба объекту, гибели людей, причинения им значительного имущественного ущерба с применением холодного, огнестрельного оружия, взрывчатых веществ либо наступления иных общественно опасных последствий...».

Угроза террористическая — инструмент, технология геополитики. Она несет в себе все признаки **проекта** — планирование, привлечение ресурсов, финансирование, набор и подготовку кадров, информационное и технологическое обеспечение и даже научные разработки. Формы ее проявления разнообразны, даже намеренно вызванная природная или техногенная угроза — это тоже терроризм.

Криминальная угроза — это тоже **проект** со всеми его атрибутами. Причем криминальная среда, и даже один отдельно взятый криминальный элемент, постоянно генерирует и поддерживает одновременно много проектов в соответствии со своей криминальной специализацией (окраской). В основе возникновения и развития криминальных угроз лежат противоречия, серьезно нарушающие нормальное функционирование социума в различных сферах жизнедеятельности — экономической, политической, социально-нравственной, межэтнической, конфессиональной и иных.

Наиболее опасными криминальными угрозами являются угрозы со стороны организованных преступных формирований, в первую очередь имеющих коррупционные связи с представителями органов власти и управления правоохранительных органов с целью вовлечь их в преступную деятельность.

Выходными данными для дальнейшего проектирования СФЗ является ранжированный перечень так называемых проектных угроз — the design basis threat (DBT), оцениваемых по вероятности их существования.

3. Определение уязвимости

Совершенно равноправно существуют два различных толкования понятия «уязвимость», и, похоже, никого это не смущает. Первое определение дано в [8]: «Уязвимость — свойство ФЗ, характеризуемое наличием в ФЗ уязвимых мест». Такой подход подтверждается и в определении Сандийских лабораторий [16] традиционным, «классическим» уравнением риска:

$$R = P_A \cdot (1 - P_E) \cdot C, \quad (4)$$

где P_A — вероятность нападения противника, P_E — вероятность эффективного противодействия системы безопасности, C — ущерб от атаки.

Под уязвимостью в таком случае понимают интегральную характеристику, предполагаемую

степень несоответствия $(1 - P_E)$ принятых мер защиты объекта прогнозируемым угрозам или заданным требованиям безопасности, т. е. неполную эффективность СФЗ. Уязвимость здесь рассматривается как внутреннее свойство объекта, в целом создающее восприимчивость к воздействию источника угрозы, которое может привести к ущербу.

Уязвимость, определяемая через эффективность СФЗ как интегральный показатель, имеет многочисленные методики ее определения и анализа, обязательные к применению. При этом весьма затруднительно интерпретировать конкретное значение уязвимости в «классическом» уравнении. Что означает уязвимость, например, 0,05? Что ущерб в результате атак уменьшится в 20 раз? Или что только 5 из 100 возможных маршрутов нарушителя приведут его к цели раньше охранников? Или вероятность того, что актив привлечет внимание угрожающей структуры, равна 0,05? Все эти интерпретации имеют совершенно разный смысл и приводят к разным результатам.

Поэтому больше информации даст рассмотрение уязвимости как дифференциального показателя, который в некоторых документах называется фактором уязвимости (ФУ) [8]. Каждый объект безопасности содержит в себе некоторые критические элементы, на которые в конечном счете и направлены угрозы. Например, места хранения ценностей, особенности оборудования на опасном производстве, уязвимые места строительных конструкций, элементы транспортной системы, технологические агрегаты и т. п. Пример: теракт на Баксанской ГЭС в 2010 г., где взрывные устройства были заложены именно в уязвимые места электрооборудования с целью нанесения максимального урона.

Определения уязвимости как дифференциального показателя учитывают критические элементы объекта как отдельно, так и вкупе с элементами системы физической защиты, которые предназначены для противодействия конкретным угрозам против этих критических элементов: «Уязвимость элемента инфраструктуры является функцией его внутренней конструкции и системы охраны (физической или другой) и изменяется с течением времени. Внутренняя конструкция элемента инфраструктуры определяет сильные и слабые стороны, связанные с конкретной атакой, и эти сильные и слабые стороны могут быть оценены на основе анализа элемента и параметров его конструкции» [13].

DHS (**Department** of **Homeland Security**) [17] определяет оценку уязвимости от террористической угрозы следующим образом: «Выявление слабых мест в физических структурах, системах защиты персонала, процессах или других областях, которые могут использоваться террористами. Оценка уязвимости также может предлагать варианты устранения или смягчения этих слабых мест». Уязвимостью являются характеристики системы, которые вызывают ухудшение состояния или отказ, подвергаясь угрозе или нападению. Уязвимость элемента инфраструктуры является функцией его внутренней конструкции и системы физической защиты.

Действия субъектов угрозы могут использовать, раскрыть или даже создать неожиданные уязвимости в инфраструктуре и системах охраны, которые глубоко зарыты и становятся видны только в экстремальных условиях или при необычных совпадениях. Примерами могут служить намеренное ослабление физических барьеров, выведение из строя функциональных систем физической защиты, внедрение агентов влияния или подкуп сотрудников, как охранников, так и операторов, установка в информационное обеспечение объекта вредительских программ, которые в определенный момент могут блокировать жизненные функции управления. Все эти действия источник угрозы совершает за счет своих ресурсов.

Уязвимость изменяется с течением времени. При попытке реализации угрозы нарушителем может быть создано окно времени, в котором активирована уязвимость. Физическое устаревание или деградация критических элементов объекта и элементов СФЗ также может повлиять со временем на уязвимость инфраструктуры. Таким образом, понятие «уязвимость» объединяет в себе и критические элементы актива, и несовершенства составляющих СФЗ объекта, а рассматривать и оценивать ее следует на всех этапах жизненного цикла объекта.

В методологии РБ-009-99 Минатома [8] приведены списки факторов уязвимости, причем, что особенно ценно, они разделены на три группы по принадлежности к составляющим частям физической защиты.

К первой группе относятся ФУ организационных мероприятий, как, например, несоответствие объему и характеру предъявляемых требований таких организационно-распорядительных документов, как положение о службе безопасности, положение о пропускном режиме и разрешительной системе допуска и доступа к активам, план взаимодействия администрации, службы безопасности и подразделений охраны объекта с органами ФСБ России и МВД России в штатных и чрезвычайных ситуациях и т. п.

Ко второй группе относятся ФУ инженерно-технических средств, например, остаточный ресурс элементов ТСФЗ, обеспечение непрерывности рубежа обнаружения по периметру охраняемой зоны, состояние контрольно-пропускных пунктов (КПП) зданий, сооружений, помещений, расположенных во внутренней и особо важной зонах, оснащенность рубежей средствами охранного телевидения и управления доступом, транспортных КПП противотаранными барьерами.

К третьей группе — ФУ действий подразделений охраны, такие как соответствие ведомственным нормативным документам обеспеченности вооружением, транспортом и средствами связи, практических действий подразделений охраны при получении сигнала тревоги, время реагирования подразделений охраны, обеспечивающее перехват нарушителя на возможных маршрутах продвижения нарушителя.

Основополагающим условием анализа уязвимостей является то, что уязвимости должны рассматриваться во взаимосвязи с моделями нарушителя и актуализироваться по данным перечня угроз, ориентированных на конкретный ущерб, и по оперативным данным. Уязвимость и субъект угрозы (нарушитель) связаны функционально: каждая уязвимость актуальна только для определенного нарушителя, обладающего возможностью ее поиска, активации и/или создания и последующего использования. То есть для одной модели нарушителя данная уязвимость может быть использована, для другой модели — нет и как бы не существует.

Взаимодействие нарушителя с активом через уязвимость определяет способы реализации угроз, которые могут быть тайными, явными, силовыми и т. п. Очевидно, что для реализации угрозы должен произойти целый ряд событий и должна быть пройдена целая цепочка уязвимостей. Источник угроз (ИУ) получает информацию об имеющихся на объекте безопасности привлекательных активах, об уязвимостях, оценивает катализаторы и ингибиторы угрозы. ИУ располагает соответствующими ресурсами и может выделить субъекта для реализации угрозы. Субъект угрозы вместе с пособниками активизирует или создает уязвимости и, преодолевая сопротивление СФЗ (физических барьеров, зоны охранной сигнализации и контроля доступа, системы охранного телевидения, силового противодействия охраны и др.), получает доступ к активу.

Выходными данными для дальнейшего проектирования СФЗ является перечень уязвимостей, оцениваемых по вероятности их использования проектными угрозами.

Таким образом, для идентификации риска требуется установить актуальность угрозы данному активу (оценить целенаправленность и характеристики субъекта угрозы). Сравнивая характеристики ОМН и ТМН, можно сделать вывод об осуществимости угрозы при данной уязвимости и конкретных внешних условиях и спрогнозировать способ реализации угрозы. Цепочек взаимодействия нарушителя и уязвимостей может быть много, тем не менее при анализе угроз объекта безопасности должны быть исследованы все возможные варианты, в том числе и одновременные атаки с разных направлений, для того, чтобы соблюсти принцип равнопрочности СФЗ, которая обязана противостоять любому выбранному способу реализации угрозы с равной эффективностью, обеспечивая приемлемый уровень риска для объекта в целом.

Заключение

Практическая деятельность по определению стратегий и методов противодействия угрозам физической безопасности основывается на анализе угроз, входными данными для которого являются результаты предпроектного обследования объекта, идентификация активов и возможного ущерба, установление актуальных угроз и их субъектов, оценка уязвимостей как элементов объекта, так и имеющейся на объекте системы физической безопасности. Составление и постоянное пополнение банка типовых угроз физической безопасности и банка

типовых уязвимостей, способствующие повышению адекватности анализа угроз при проектировании СФЗ, можно считать одной из важнейших задач. Но не менее важно получить наиболее свежие данные от силовых ведомств об актуализации угроз, ОМН, о новых способах реализации угроз. Рассмотрение функциональной связи уязвимости и субъекта угрозы (нарушителя) позволит избежать упрощенных решений, а исследование катализаторов и ингибиторов угроз поможет расширить арсенал стратегий противодействия, не ограничиваясь только методом защиты расстоянием или временем, что в конечном итоге повысит эффективность проектируемых СФЗ и снизит материальные затраты.

Литература [References]

1. Белов В. П., Голяков А. Д. Терминологическая база теории безопасности. Стандарты и качество. 2004. № 9. С. 48—51. [Belov V. P., Golyakov A. D. Terminology database of the theory of safety // Standards and Quality. 2004. No. 9. P. 48—51 (Russia).]
2. Руководство по безопасности при использовании атомной энергии «Рекомендации по проведению анализа уязвимости радиационного объекта» (РБ-120-16) (утв. приказом ФСЭТАН № 535 от 14.12.2016). [The guide to safety when using atomic energy "Recommendations about carrying out analisa of vulnerability of a radiation object" (RB-120-16). It is approved by the order FSETAN No. 535 of 14.12.2016. (Russia).]
3. ГОСТ Р 52551-2006 Системы охраны и безопасности. Термины и определения. [GOST P 52551-2006 of the Systems of protection and safety. Terms and definitions. (Russia).]
4. ГОСТ Р 22.10.01-2001 Безопасность в чрезвычайных ситуациях. Оценка ущерба. Термины и определения. [GOST P 22.10.01-2001 Safety in emergency situations. Damage assessment. Terms and definitions. (Russia).]
5. Гацко М. О соотношении понятий «угроза» и «опасность» // Обозреватель. 1997. № 7. [Gatsko M. About a ratio of the concepts "threat" and "danger" // The Observer. 1997. No. 7.]
6. Бояринцев А. В., Ничиков А. В., Редькин В. Б. Общий подход к разработке моделей нарушителей // Системы безопасности. 2007. № 4. С. 50—53. [Boyarintsev A. V., Nichikov A. V., Redkin V. B. General approach to development of models of violators // Security systems. 2007. No. 4. P. 50—53 (Russia).]
7. Единая межведомственная методика оценки ущерба от чрезвычайных ситуаций техногенного, природного и террористического характера, а также классификации и учета чрезвычайных ситуаций. М.: ФГУ ВНИИ ГОЧС (ФЦ), 2004 г. [Uniform interdepartmental technique of assessment of damage from emergency situations of technogenic, natural and terrorist character and also classification and accounting of emergency situations. M.: All-Russian Research Institute GOChS (FTs) Federal State Institution, 2004.]
8. РБ 009-99 Методология оценки уязвимости физической защиты ядерных материалов и ядерных установок. [RB 009-99 Methodology of assessment of vulnerability of physical protection of nuclear materials and nuclear facilities (Russia).]
9. Руководство по безопасности при использовании атомной энергии «Рекомендации по проведению анализа уязвимости радиационного объекта» (РБ-120-16) (утв. приказом Федеральной службы по экологическому, технологическому и атомному надзору от 14 декабря 2016 г. № 535). [Guide to safety when using atomic energy of "The recommendation about carrying out the analysis of vulnerability of a radiation object" (RB-120-16) (утв. order of Federal Service for Environmental, Technological and Nuclear Supervision of December 14, 2016. No. 535).]
10. Дудко Д. Какой будет динамика роста внутренних угроз в ближайшее время? [Dudko D. What will be dynamics of growth of internal threats in the nearest future?] http://www.securitylab.ru/blog/personal/ddudko/303607.php
11. Банк данных угроз безопасности информации. [Databank of threats to security of information] http://bdu.fstec.ru/threat
12. Гарсиа М. Проектирование и оценка систем физической защиты / пер. с англ. В. И. Воропаев [и др.]; Ред.: Р. Г. Магауенов. М.: Мир: АСТ, 2003. 386 с.: ил. (Технология безопасности). Пер. изд.: The Design and Evaluation of Physical Protection Systems / Garcia M. L. (Boston). ISBN 5-03-003522-2.
13. Garcia M. L. Vulnerability Assessment of Physical Protection Systems, Boston, Butterworth-Heinemann, 2006.
14. Darril Gibson. CompTIA Security+: Get Certified Get Ahead: SY0-401 Study Guide, 2014.
15. ГОСТ Р 52860-2007 Технические средства физической защиты. Общие технические требования.

[GOST P 52860-2007 Technical means of physical protection. General technical requirements.]
16. Betty Biringer. A Risk Assessment Methodology for Physical Security. Systems Analysis and Development Department, 5845. Sandia National Laboratories, MS 0759.
17. Alberto R. Gonzales, Regina B. Schofield, Domingo S. Herraiz. Assessing and Managing the Terrorism Threat U. S. Department of Justice. Office of Justice Programs. Bureau of Justice Assistance, 2005.
18. Arnold B. Baker, Robert J. Eagan, and other. A Scalable Systems Approach for Critical Infrastructure Security, SAND REPORT, SAND2002-0877, 2002.
19. Nancy A. Renfroe, Joseph L. Smith. Threat / Vulnerability Assessments and Risk Analysis. Whole Building' Design Techniques and Technologies. https://www.wbdg.org/resources/threat-vulnerability-assessments-and-risk-analysis.
20. Whitehead D. W., Potter C. S., O'Connor S. L. Nuclear Power Plant Security. Assessment Technical Manual, SANDIA REPORT, SAND2007-5591, 2007.
21. http://www.s-director.ru/project/physical_security.html
22. Science Direct/Journals & Books. https://www.sciencedirect.com/topics/computer-science/physical-security.

Сведения об авторе

Филиппов Дмитрий Леонидович: доцент кафедры ИУ-10 МГТУ им. Н. Э. Баумана
Количество публикаций: 14
Область научных интересов: системы физической защиты, менеджмент рисков, безопасность бизнеса
Контактная информация:
Адрес: 105005, г. Москва, 2-я Бауманская ул., д. 5, стр. 1
Телефон: +7 (903) 538-50-01
E-mail: filippov@frtk.ru

Автор заявляет об отсутствии конфликта интересов.
Дата поступления: 20.05.2019
Дата принятия к публикации: 01.07.2019
Дата публикации: 30.08.2019

The author declare no conflict of interest.
Came to edition: 20.05.2019
Date of acceptance to the publication: 01.07.2019
Date of publication: 30.08.2019