УДК 65.012.8

ISSN 1812-5220

Об отечественной нормативно-методической базе физической безопасности

Д. Л. Филиппов,
МГТУ им. Н. Э. Баумана,
г. Москва

Аннотация

В данной статье рассмотрено положение с нормативно-методической базой физической безопасности. Отмечено, что методики категорирования, анализа угроз и уязвимостей отличаются нечеткостью понятийного аппарата, отсутствует единый терминологический подход. Указано, что в анализе угроз зачастую не рассматривается связь уязвимостей и модели нарушителя. Не составлен банк данных угроз безопасности и актуальных уязвимостей.

Ключевые слова: нормативная база, категорирование, анализ угроз, модель нарушителя, уязвимость.

Содержание

Введение

Создание высокоэффективной системы физической защиты (СФЗ) основывается на концептуальном проекте, главные цели которого — определение путей и методов решения основных задач по обеспечению физической защиты объекта, разработка принципиальных технических и организационных решений, основных алгоритмов работы систем и их взаимодействия. Концептуальное проектирование СФЗ использует согласованные с заказчиком и **утвержденные** результаты категорирования и **утвержденные** результаты анализа угроз (а именно проектную модель угроз и проектную модель нарушителя) для последующего формирования на основании полученных данных стратегии противодействия угрозам, разработки организационных мероприятий, тактики действий сил охраны и создания инженерно-технической инфраструктуры, позволяющей силам охраны наиболее эффективно реализовать свои возможности.

В свою очередь категорирование и анализ угроз не могут быть проведены иначе, как на основании жесткой нормативной и методической базы. К сожалению, следует признать, что на сегодняшний день такая база отечественных нормативных документов в значительной мере отсутствует и даже не находится в процессе формирования и развития.

Ситуация может быть обусловлена рядом проблем. Как отмечает ряд специалистов, «первой проблемой является отсутствие до настоящего времени научно обоснованного понятийного аппарата, обеспечивающего четкое и однозначное понимание некоторых применяемых в теории безопасности терминов. Наиболее остро эта проблема проявляется при использовании расплывчатых понятий

и терминов, которые тем не менее имеют вполне легальное место в законах и различного рода нормативных правовых актах и обладают обязательной силой» [1, 2].

Использование противоречивых, ведомственно ориентированных понятий влечет за собой нарушение принципа адекватности при построении систем физической защиты и, соответственно, снижение их эффективности, чревато непредвиденными последствиями или необоснованным завышением стоимости разработки, реализации систем и стоимости владения комплексом инженерно-технических средств охраны.

Достаточно привести такой пример: в национальном стандарте РФ ГОСТ Р 52551-2006 «Системы охраны и безопасности. Термины и определения», в федеральных законах «О транспортной безопасности» от 09.02.2007 № 16-ФЗ (последняя редакция), «О безопасности объектов топливно-энергетического комплекса» от 21.07.2011 № 256-ФЗ и целом ряде других актов приводится определение понятия «безопасность», калькированное из прежнего Федерального закона от 05.03.1992 № 2446-1 (ред. от 26.06.2008) «О безопасности», а именно — «безопасность есть состояние защищенности…». В то время как ныне действующий закон «О безопасности» ФЗ № 390 от 28.12.2010 отменяет действие прежнего, в том числе и это определение, и не дает нового [3]. А это значит, что заимствованные определения теряют свою юридическую основу.

1. Методики категорирования объектов

Методические рекомендации по категорированию объектов тоже весьма разнородны и не образуют целостной системы. Не существует общей Государственной системы категорирования опасных объектов, а существует целый ряд ведомственных методик: методика МЧС [4], характеризующая объект с точки зрения возможности возникновения на нем ЧС и его масштаба, методика МВД, опирающаяся на количественные показатели материального ущерба, но не рассматривающая виртуальные потери [5], методики Минатома России [6], Минтранса [7] и др. При этом в перечень оснований для отнесения объекта к той или иной категории иногда входят, а иногда и не входят данные об актуальных угрозах и уязвимостях. С другой стороны, в эти методики в большинстве случаев прямо включены вполне конкретные требования к числу и виду физических барьеров, оборудованию контрольно-пропускных пунктов, средствам локализации взрывных устройств, к средствам индивидуальной защиты. Тем самым обходятся такие важнейшие этапы создания СФЗ, как анализ угроз и концептуальное проектирование. Кроме того, выполнение этих рекомендаций подразумевает только один метод противодействия — защиту расстоянием, исключая и защиту временем, и сдерживание. При этом упор делается именно на физическую укрепленность и упускается из виду принципиальное положение, что СФЗ имеет не одну, а три составляющих — кроме комплекса инженерно-технических средств охраны еще и организационно-режимные мероприятия, и персонал СФЗ.

2. Нормативная база анализа угроз

Нормативная документация по анализу угроз в не меньшей степени отличается нечеткостью понятий. В некоторых случаях документ называется «анализ угроз», в других подобный по сути документ называется «анализ уязвимости» или «анализ уязвимостей», и даже «угрозы уязвимостей». Попробуем разобраться. Что является общим понятием, а что частным — анализ угроз или анализ уязвимостей?

Как показано в [8], угроза имеет конкретно-адресный характер и включает в себя два компонента — намерение и возможность нанесения ущерба объекту безопасности. Намерение генерируется источником угрозы и реализуется субъектом угрозы, чаще всего называемым нарушителем, а возможность реализации угрозы определяется уязвимостями, неотъемлемым свойством объекта. Причем уязвимость и субъект угрозы связаны функционально: каждая уязвимость актуальна только для определенного нарушителя, обладающего возможностью ее использования. То есть для одного нарушителя данная конкретная уязвимость существует и может быть использована, для другого типа нарушителя — нет, причем такая зависимость может быть оценена и вероятностно, и количественно. Этот аспект полностью игнорируется в методиках оценки уязвимостей, любая уязвимость рассматривается в расчете на максимально опасного нарушителя, что приводит к многократному увеличению преграждающей

способности физических барьеров и повышению стоимости СФЗ в целом.

Актуализация модели нарушителя приведена в статье [9], где рассматриваются три возможных модели нарушителя:

«Технологическая модель нарушителя (ТМН) — разрабатываемая как набор характеристик потенциальных нарушителей, при которых они способны реализовать соответствующие угрозы объекту. Это минимально необходимое количество нарушителей определенного типа и оснащенности, которое понадобится для реализации конкретной угрозы по определенному сценарию, исходя из особенностей функционирования объекта.

Оперативная модель нарушителя (ОМН), разрабатываемая как 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), разрабатываемая как набор характеристик потенциальных нарушителей, которым должна успешно противостоять СФЗ объекта. ПМН — это то максимальное количество нарушителей определенного качества, реализующих конкретную угрозу по определенному сценарию, действия которых, по мнению государства, должны быть успешно пресечены СФЗ объекта».

Таким образом, уязвимости должны рассматриваться во взаимосвязи с моделями нарушителя и актуализироваться по данным перечня угроз и оперативным данным. Что же касается перечня угроз и уязвимостей, то можно указать лишь один документ, в котором угрозы указываются явно: «Перечень потенциальных угроз совершения актов незаконного вмешательства в деятельность объектов транспортной инфраструктуры и транспортных средств, утвержденный Приказом Минтранса России, ФСБ России и МВД России от 5 марта 2010 г. № 52/112/134» [10], где указывается только 9 типовых угроз.

А перечень уязвимостей приведен в РБ 009-99 — «Методология оценки уязвимости физической защиты ядерных материалов и ядерных установок» [11], где названы актуальные факторы уязвимостей общим числом лишь 58. Необходимо отметить, что этот документ наиболее гармоничен и полон, в частности в нем рассматриваются уязвимости, относящиеся и к организационным решениям, и к инженерно-технической укрепленности, и к силовым подразделениям.

Во всех же остальных случаях специалистам, проводящим анализ угроз, предлагается пользоваться методом экспертных оценок. Этот метод вносит субъективные ошибки, а кроме того, он основывается на исторических данных, т.е. на опыте известных экспертам инцидентов, произошедших ранее, иногда значительно ранее, в то время как сценарии реализации угроз, возможности субъектов угроз и соответствующие этим сценариям уязвимости стремительно изменяются со временем.

Отсутствие необходимых нормативных стандартов не позволяет провести базовый анализ угроз. Экспертный же метод идентификации актуальных угроз и соответствующих уязвимостей отличается повышенной детализацией, следовательно, на его проведение требуются значительные ресурсы и время. За это время изменяются и сами угрозы, и способы их реализации.

Еще одна особенность существующего положения в том, что в одном и том же документе смешивается анализ угроз (или, как иногда указано, анализ уязвимости) с оценкой эффективности СФЗ. Это объясняется тем, что под уязвимостью в таком случае понимают не отдельное конкретное свойство объекта безопасности (включая его систему физической защиты), которое может быть использовано конкретным нарушителем для реализации конкретной угрозы в конкретных условиях, а некую неощутимую интегральную характеристику, предполагаемую степень несоответствия принятых мер защиты (объекта) прогнозируемым угрозам или заданным требованиям безопасности, т.е. неполную эффективность. В то время как:

- в этих исследованиях рассматриваются различные предметы — либо сам защищаемый объект, либо его СФЗ;
- при анализе угроз объект может еще и не иметь СФЗ;
- задачей анализа угроз является выявление и формализация ряда параметров, а на этапе оценки эффективности они уже формализованы и утверждены;

• основная цель анализа угроз — получить обоснованные данные для проектирования СФЗ;

• основная цель оценки эффективности — проверка соответствия СФЗ выполнению своих функций на должном уровне и выявление ошибок в проектировании.

Заключение

Сравнивая нормативную базу в области физической безопасности с нормативной базой в области информационной безопасности, и в частности в области менеджмента риска, можно убедиться в большей полноте последней. В стандартах, отражающих международную практику, например ГОСТ Р ИСО/МЭК ТО 13335-3-2007, раскрываются понятия угрозы и уязвимости, указывается порядок их анализа. В распоряжении специалистов по анализу риска имеется банк данных угроз безопасности [12], он насчитывает на сегодняшний день 194 угрозы и более 15 400 уязвимостей.

Значимость нормативно-методической базы в области безопасности нельзя переоценить: применение расплывчатых терминов имеет своим следствием не только ошибки в концептуальном проектировании систем физической защиты, а следовательно, неправильное построение системы и завышение ее стоимости, но и ошибки первого рода — недооценка или игнорирование вновь возникающих угроз.

Литература

1. Белов В.П., Голяков А.Д., Талалаев Д.В. О нормировании безопасности информационно-управляющих систем. Автоматика, связь, информатика, 2006.
2. Белов В.П., Голяков А.Д. Терминологическая база теории безопасности. Стандарты и качество, № 9, 2004, стр. 48—51.
3. ФЗ РФ № 390 от 28 декабря 2010 года «О безопасности».
4. Приказ МЧС России от 28.02.2003 № 105 «Классы опасности потенциально опасного объекта, устанавливаемые по результатам прогнозирования возможных чрезвычайных ситуаций».
5. Р 78.36.028-2012 Технические средства обнаружения проникновения и угроз различных видов.
6. Федеральные нормы и правила в области использования атомной энергии «Правила физической защиты радиоактивных веществ, радиационных источников и пунктов хранения» (НП-034-15).
7. Приказ Министерства транспорта Российской Федерации (Минтранс России) от 21 февраля 2011 г. № 62 «О Порядке установления количества категорий и критериев категорирования объектов транспортной инфраструктуры и транспортных средств компетентными органами в области обеспечения транспортной безопасности».
8. Гацко М. О соотношении понятий «угроза» и «опасность» // Обозреватель. 1997. № 7. URL: http://www.rau.su/observer/N07_97/ 7_06. HTM
9. Бояринцев А.В., Ничиков А.В., Редькин В.Б. Общий подход к разработке моделей нарушителей. «Системы безопасности». № 4, 2007.
10. Перечень потенциальных угроз совершения актов незаконного вмешательства в деятельность объектов транспортной инфраструктуры и транспортных средств, утвержденный приказом Министерства транспорта Российской Федерации, Федеральной службы безопасности Российской Федерации, Министерства внутренних дел Российской Федерации от 5 марта 2010 г. № 52/112/134.
11. РБ 009-99 — «Методология оценки уязвимости физической защиты ядерных материалов и ядерных установок».
12. Банк данных угроз безопасности информации. http://bdu.fstec.ru/threat

Сведения об авторе

Филиппов Дмитрий Леонидович: доцент кафедры ИУ-10 МГТУ им. Н.Э. Баумана

Количество публикаций: 12

Область научных интересов: системы физической защиты, теория систем безопасности, анализ рисков

Контактная информация:

Адрес: 105005, г. Москва, 2-я Бауманская ул., д. 5

Тел.: +7 (499) 236-68-37

E-mail: filippov@frtk.ru