Радоуцкий В. Ю. канд. техн. наук, проф.,
Шаптала В. Г., д-р техн. наук, проф.,
Ветрова Ю. В., канд. техн. наук, доц.
Белгородский государственный технологический университет им. В.Г. Шухова

МАТЕМАТИЧЕСКИЕ МЕТОДЫ АНАЛИЗА ЭФФЕКТИВНОСТИ ФУНКЦИОНИРОВАНИЯ СИСТЕМ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ*

vs1606@mail.ru

Анализ состояния проблемы эффективности функционирования систем комплексной безопасности высших учебных заведений (ВУЗ) показал практически полное отсутствие методических разработок в данной области. Однако то, что ВУЗы относится к объектам социальной значимости и являются специфичными по многим признакам объектами, определяет необходимость разработки методического обеспечения оценки эффективности функционирования технических средств безопасности.

Ключевые слова: *анализ, безопасность, технические средства, комплексная безопасность, эффективность, метод, имитационное моделирование.*

Введение. Одной из целей функционирования системы организационно-технического управления является планирование структуры и состава технических средств безопасности (ТСБ), оптимальных для рассматриваемого объекта с точки зрения установленных критериев [1]. Поэтому выбор критерия эффективности функционирования технических средств безопасности.

Проектирование ТСБ всегда является затратным механизмом, поэтому анализ его воздействия на дестабилизирующие факторы, максимизация интенсивности данного воздействия - важные задачи для проектировщика. В соответствии с [2], «эффективность защиты информации — это степень соответствия результатов защиты информации поставленной цели». По аналогии с данным определением, под *эффективностью* системы безопасности будем понимать степень соответствия ТСБ своему целевому предназначению. Целью функционирования ТСБ при этом является обеспечение защищенности людских, информационных и материальных ресурсов от действия внутренних и внешних угроз, т.е. противодействие любым попыткам нанести ущерб защищаемым объектам [3].

Методология. При работе использовались методы системного анализа, теории вероятности, теории принятия решений, методы оптимизации, методы математического и имитационного моделирования.

Основная часть. Задавшись целью анализа систем безопасности, целесообразно в общих чертах представить себе, какими особенностями обладает ТСБ как составная часть системы комплексной безопасности (СКБ). Отметим следующие ее особенности [4]:

1. *Конфликтность интересов.* Принципиальное отличие КСБ от других человеко-машинных систем заключается в наличии конфликта интересов в системе «охрана-нарушитель».

2. *Априорная неопределенность исходных данных для проектирования системы. В первую очередь это касается перечня угроз, модели нарушителя, а также сценариев развития конфликтной ситуации. СКБ — слабоформализованная система.*

3. *Случайный характер временных параметров,* в том числе случайность времени движения охраны и нарушителя, времени преодоления физических барьеров, момента срабатываний средств обнаружения и пр.

4. *Трудоемкость организации эксперимента.* Лучшим способом анализа эффективности СКБ является организация учений, однако этот способ связан с привлечением значительных материальных и людских ресурсов и в силу этого не получил широкого распространения. «Поведение» СКБ целесообразно изучать с помощью математического моделирования. Для построения модели необходимо выявить структуру системы, цели функционирования СКБ, критерии эффективности, а также разработать инструмент их оценки. Модель - инструмент исследования СКБ [5].

Эффективность систем оценивается с помощью показателей эффективности. При этом в отношении сложных человеко-машинных систем предпочтительнее использование термина «показатель эффективности функционирования», который характеризует степень соответствия оцениваемой системы своему назначению [6].

Показатели эффективности функционирования могут носить количественный или качественный характер. Во многих случаях оценок бинарного типа (соответствует / не соответствует требованиям) вполне достаточно, чтобы ответить на вопрос, насколько защищен объект.

Однако, количественные методы более приемлемы. Могут применяться вероятностные показатели эффективности, такие как безопасность информации [7], вероятность выполнения задачи системой, вероятность преодоления защитных барьеров за время t и т.д. [8]. Показатели эффективности могут носить стоимостной характер: стоимость создания, внедрения, поддержки СКБ; затраты на восстановление нормальной работы после реализации угрозы и т.д.

Система безопасности представляет собой сбалансированную совокупность элементов обнаружения нарушителя, задержки продвижения нарушителя по пути следования, а также элементов реагирования сил охраны на действия нарушителя.

Оценив приведенные характеристики тем или иным способом, можно вынести суждение об эффективности СКБ в целом.

Рассмотрим следующие методы анализа:

- детерминистический подход;
- логико-вероятностное моделирование;
- имитационное моделирование [9].

Детерминистический подход

Указанный подход связан с заданием и последующей проверкой требований, содержащихся в нормативно-технической документации, техническом задании на проектирование, в рабочем проекте оборудования объекта средствами безопасности. Проводится категорирование объектов охраны в зависимости от их важности/потенциальной опасности, возможного

и/или допустимого социально-экономического ущерба. Для объектов каждой категории устанавливаются дифференцированные требования по организации охраны и инженерно-технической укрепленности конструктивных элементов объекта. При этом уровень защищенности должен соответствовать значимости объекта, выражаемой через его категорию, в этом состоит основной принцип проектирования эффективной ТСБ. Состояние ТСБ оценивается экспертным путем. Экспертная оценка - средство переработки слабоструктурированных данных, при котором используются суждения экспертов для подготовки обоснованных решений.

Логико-вероятностные методы

Эти методы позволяют получить количественную оценку **риска** как меры опасности. Они давно применяются в отечественной практике для анализа надежности и безопасности сложных технических систем. В основе их лежат два понятия: *степень риска* и *уровень защищенности.* Степень риска $К_{риск}(у)$ - вероятность невыполнения СКБ своей целевой функции. Обратная величина характеризует уровень защищенности:

$$К_{защ}(у)=1-К_{риск(у)} \quad (1)$$

Оценка защищенности - процедура оценки показателей $К_{риск}$, $К_{защ}$ для людей и имущества на охраняемом объекте. Составляется сценарий развития опасности (граф вида «дерево»), представляющий собой логико- вероятностную модель функционирования СКБ. Далее с помощью логико- вероятностных преобразований находится значение вероятностной функции Р, при которой значение функции опасности равно 1 (это означает наступление опасного события), и определяется степень риска, присутствующего в системе: $К_{риск}(у)$. Трудность здесь заключается в обеспечении достоверности исходных данных. Различают объективные и субъективные вероятности. Объективными являются характеристики технических средств охраны, полученные по результатам натурных испытаний. Качественно иную (субъективную) природу имеют результаты анализа уязвимости, отражающие интуитивные представления о возможности и характере реализации угрозы.

Имитационное моделирование

Вероятностный подход к анализу базируется на предположениях о случайности и независимости временных параметров в системе «охрана- нарушитель». Эффективность здесь понимается как вероятность пресечения несанкционированных действий нарушителя:

$$P_{прес} = P_{обн} \cdot P_{нейтр} \quad (2)$$

где: $Р_{обн}$ - вероятность обнаружения нарушителя;

$Р_{нейтр}$ - вероятность нейтрализации нарушителя.

Как оценить эти вероятности? Один из методов — имитационное моделирование. Каждая конфликтная ситуация в СКБ просчитывается много раз, по результатам набирается статистика захватов нарушителя. Эффективность СКБ оценивается статистически как отношение числа захватов к общему числу испытаний. Количество опытов определяется исходя из того, что при заданной доверительной вероятности необходимо обеспечить требуемую точность оценки.

Достоинства и недостатки методов

Достоинством детерминистического подхода является то, что в руки проектировщика даются четкие и ясные критерии того, как оборудован объект техническими средствами охраны. Основная проблема — способ получения интегрального показателя. Наиболее распространена «линейная свертка» вида:

$$z_c = \sum_j k_j \cdot y_j \quad (3)$$

Необходимо помнить, что операция осреднения имеет смысл, если частные показатели однотипны, то есть имеют одинаковую «физическую природу». Если это не так, такой интегральный показатель не имеет физического смысла.

Достоинством имитационного моделирования является физически обоснованный критерий эффективности (вероятность). Недостаток - трудность его интерпретации и нормирования. Пусть в результате анализа получено значение $P_{прес} = 0,9$. Неясно, много это или мало, достаточен уровень защиты объекта или нет?

В результате использования логико-вероятностных методов для анализа эффективности СКБ тоже получается число $К_{риск}(у)$. Но смысл здесь не в цифре, а в том, что логико-вероятностное моделирование позволяет построить модель безопасного функционирования СКБ, определить «уязвимые места» системы и оценить «вклад» каждого из них, ранжируя их по степени опасности. В качестве недостатков здесь можно отметить трудоемкость логических преобразований при анализе сложных сценариев (переход от функции опасного состояния к вероятностной функции), а также разнородность исходных данных (объективных, которые можно достоверно оценить; субъективных, отражающих «ожидания угрозы»).

Вывод. Следует отметить, что с целью избавления от упомянутых недостатков каждого из приведенных методов, необходимо разработать метод оценки эффективности, который по возможности должен комбинировать приведенные.

** Работа выполнена в рамках программы стратегического развития БГТУ им. В.Г. Шухова на 2012 – 2016 годы.*

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Шаптала В.Г., Радоуцкий В.Ю., Шаптала В.В. Системы информационной поддержки принятия управленческих решений при ликвидации последствий чрезвычайных ситуаций органами управления ВУЗа // Вестник Белгородского государственного технологического университета им. В.Г. Шухова. 2011. №3. С. 91-93.

2. ГОСТ Р 50922-96. Защита информации. Основные термины и определения. М.: Госстандарт России, 1996. 12 с.

3. Концепция безопасности коммерческого банка. http ://spk.ru/ security/

4. Шаптала В.Г., Радоуцкий В.Ю., Шульженко В.Н. Концепция обеспечения безопасности высших учебных заведений // Вестник Белгородского государственного технологического университета им. В.Г. Шухова. 2009. №3м. С. 127-129.

5. Радоуцкий В.Ю., Шаптала В.Г., Методологические основы моделирования систем обеспечения комплексной безопасности ВУЗов // Вестник Белгородского государственного технологического университета им. В.Г. Шухова. 2008. №3м. С. 64-66.

6. Завгородний В. И. Комплексная защита информации в компьютерных системах: уч. пос. М.: Логос. 2001. 264 с.

7. Руководящий документ Гостехкомиссии России (утв. Решением Гостехкомиссии России от 30.03.1992 г.). Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. М.: Военное издательство, 1992. 12с.

8. Lokhmatov M.V. Evaluation of intelligent building security system effectiveness // Proceedings of the Workshop on Computer Science and Information Technologies (CSIT'2005), Vol. 3, Ufa: Ufa State Aviation Technical University, 2005. 228-232 pp.

9. Панин О. А. Анализ эффективности интегрированных систем безопасности: принципы, критерии, методы // Системы безопасности.2006. №2. С.60 - 62.