УДК 004.056

А.В. Вергейчик, В.П. Кушнир

Моделирование систем физической защиты

Рассматривается разработанная модель системы физической защиты, модель нарушителя.
Кратко описан алгоритм анализа системы физической защиты по предложенным моделям.

Система физической защиты (СФЗ) может быть определена как совокупность элементов или компонентов, предназначенных для достижения безопасного функционирования объекта в соответствии с планом. Основными функциями СФЗ являются: обнаружение, задержка, реагирование. Функция обнаружения характеризуется вероятностью обнаружения, задержка характеризуется временем преодоления СФЗ, реагирование – временем реакции охраны [1].

В принятой модели СФЗ критерием эффективности СФЗ принимается критерий своевременности обнаружения несанкционированного доступа (НСД). Под своевременным обнаружением понимается принятие решения об обнаружении НСД в такой момент времени, когда остается еще достаточно времени для развёртывания сил охраны и перехвата нарушителя. Время реагирования сил охраны $T_{\text{Р}}$ определяет критическую точку обнаружения (КТО). КТО – это точка на маршруте движения нарушителя, после которой обнаружение НСД не позволяет силам охраны своевременно прибыть к месту перехвата и оказать эффективное противодействие нарушителям [2]. В этой точке время реагирования сил охраны еще не превосходит минимальное время совершения НСД: $T_{\text{НСД}} \geq T_{\text{Р}}$.

Модель системы физической защиты состоит из нескольких компонентов: модель нарушителя, модель объекта. Модель нарушителя представляет собой совокупность стратегии действий нарушителя и матриц навыков: матрицу вероятностей P (1) и матрицу времен T (2).

$$P = \begin{pmatrix} p_{1,1} & p_{1,2} & \cdots & p_{1,\text{n}} \\ p_{2,1} & p_{2,2} & \cdots & p_{2,\text{n}} \\ \cdots & \cdots & \cdots & \cdots \\ p_{\text{m},1} & p_{\text{m},2} & \cdots & p_{\text{m,n}} \end{pmatrix} \quad (1)$$

Элементом матрицы вероятностей $p_{i,j}$ является вероятность обнаружения НСД при преодолении элемента СФЗ i-го типа, используя j-й навык из набора навыков нарушителя.

$$T = \begin{pmatrix} t_{1,1} & t_{1,2} & \cdots & t_{1,\text{n}} \\ t_{2,1} & t_{2,2} & \cdots & t_{2,\text{n}} \\ \cdots & \cdots & \cdots & \cdots \\ t_{\text{m},1} & t_{\text{m},2} & \cdots & t_{\text{m,n}} \end{pmatrix} \quad (2)$$

Элементом матрицы вероятностей $t_{i,j}$ является время преодоления элемента СФЗ i-го типа, используя j-й навык из набора навыков нарушителя.

В предлагаемой модели рассматриваются три основных стратегии нарушителя при преодолении барьеров СФЗ: минимизация времени преодоления, минимизация вероятности обнаружения и оптимальная стратегия. При оптимальной стратегии до КТО нарушитель действует согласно стратегии минимизации вероятности обнаружения (скрытое проникновение), а после КТО – согласно стратегии минимизации времени преодоления (силовой прорыв). Данная комбинированная стратегия показана на рис. 1. Применение данной стратегии в модели нарушителя соответствует принципу гарантированного результата и снимает неопределенность в стратегии поведения нарушителя.

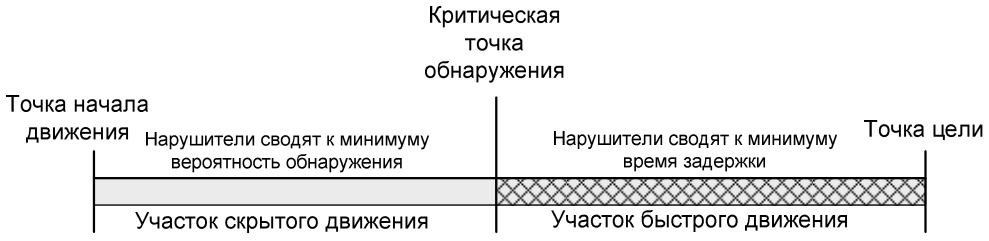

Рис. 1. Модель комбинированной стратегии действий нарушителя

Модель объекта представляет собой граф, представленный в виде матрицы смежности **M**[a, b]. Вершинами данного графа являются области однородности (ОО) – области на объекте, где совпадают три основные характеристики системы физической защиты: время реакции охраны, время преодоления данной области нарушителем и вероятность обнаружения нарушителя устройствами обнаружения, действующими в данной области. Характеристиками ОО служат: набор устройств и инженерных

средств охраны, установленных или действующих в данной зоне, а также время реакции сил охраны. ОО служат для построения пространственной модели объекта. Пример областей однородностей и графа однородности показан на рис. 2.

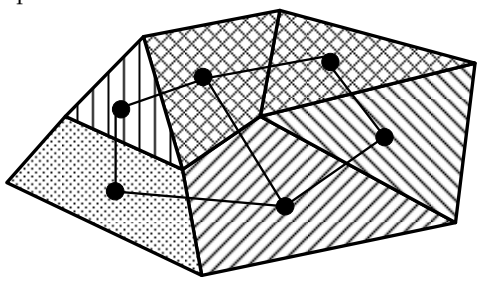

Рис. 2. Области однородности с графом (пространственной моделью) объекта

Задача анализа СФЗ состоит в том, чтобы определить наличие критических путей (таких путей, где вероятность своевременного обнаружения $P_{\text{ОБ}}$ будет больше минимально заданной вероятности обнаружения $P_{\min}$). Поиск критических путей производится по следующему алгоритму:

ЭТАП 1: По модифицированному алгоритму Дейкстры находятся все пути из множества точек начала движения $N = (n_1, n_2, \ldots, n_i, \ldots, n_k)$ (областей однородности, расположенных на периметре объекта) к множеству целевых точек $C = (c_1, c_2, \ldots, c_j, \ldots, c_m)$ (областей однородности, в которых находятся критические элементы объекта). Подробное описание этого алгоритма выходит за рамки данной статьи. Получаем набор векторов вида (3):

$$v = (n_i \ldots m_a \ldots c_j). \tag{3}$$

ЭТАП 2: Расчет производим согласно оптимальной стратегии действий нарушителя. На каждом векторе v (3) находим КТО – точку, в которой $\sum_{i=\kappa}^{ц} T_j < T_{\text{охр.КТО}}$, где $T_{\text{охр.КТО}}$ – время реакции охраны в критической точке обнаружения; T_j – время преодоления j-й зоны однородности СФЗ, расположенной между КТО и целевой зоной. Время преодоления берется из матрицы навыков нарушителя T (2), оно должно быть минимально из всего набора времен при преодолении элементов системы физической защиты в j-й зоне однородности. Итоговая оценка найденного пути v (3) (вероятность своевременного обнаружения) $P_{\text{ОБ}}$ будет являться вероятностью обнаружения нарушителя до КТО и находится по формуле (4):

$$P_{\text{ОБ}} = 1 - \prod_{j=1}^{\kappa} (1 - P_j). \tag{4}$$

Вероятность обнаружения P_j берется из матрицы вероятностей навыков нарушителя P (1). Выбранная вероятность должна быть минимальна из всего набора вероятностей обнаружения НСД при преодолении элементов СФЗ в j-й зоне однородности.

При $P_{\text{ОБ}} \le P_{\min}$ найденный путь v будет являться критическим. По наличию или отсутствию критических путей делается вывод о достаточности или недостаточности мероприятий по физической защите объекта.

Литература

1. Оленин Ю.А. Основы систем безопасности объектов: Учеб. пособие. – Пенза: Информ.-издат. центр ПГУ, 2002. – 122 с.

2. Гарсиа М. Проектирование и оценка систем физической защиты. – М.: Мир, 2003. – 386 с.

Вергейчик А.В.

Кушнир Виктор Петрович
ФГОУ ВПО «Сибирский федеральный университет»
профессор кафедры «Информационная безопасность»
Эл. почта: kushnir@kraskript.ru.

A.V.Vergeychik, V.P. Kushnir

Physical protection systems modeling

In article show new physical protection systems model, breaker model. Shortly describe analyze algorithms physical protection systems by offer model.