Та или иная форма уязвимости конфиденциальной информации может реализовываться в результате преднамеренного или случайного дестабилизирующего воздействия различными способами на носитель информации или на саму информацию со стороны источников воздействия. Такими источниками могут быть люди (сотрудники предприятия, конкуренты, злоумышленники), технические средства обработки и передачи информации, средства связи, стихийные бедствия и др. Способами дестабилизирующего воздействия на информацию являются: ее копирование (фотографирование), записывание, передача, заражение программ обработки информации вирусами, нарушение технологии обработки и хранения информации, выход (или вывод) из строя и нарушение режима работы технических средств обработки и передачи информации, физическое воздействие на информацию и др. Реализация указанных форм проявления уязвимости конфиденциальной информации приводит или может привести к двум видам уязвимости информации – ее утрате или утечке. Таким образом, анализируя существующие угрозы безопасности информационных ресурсов предприятия, представляется возможным сделать ряд выводов:

Во-первых, основными источниками конфиденциальной информации на предприятии являются как физические лица (персонал, контрагенты, клиенты и деловые партнеры), так и различного рода объекты: документы, публикации, технические носители информации и объекты информатизации (основные и вспомогательные технические средства и системы, защищаемые помещения). Поэтому при решении задач защиты важных сведений нужно учитывать каждый из перечисленных носителей и источников информации в отдельности и его информативность в конкретных условиях.

Во-вторых, анализ основных угроз безопасности и возможных форм проявления уязвимости конфиденциальной информации предприятия показывает, что защите подлежит информация как речевая, так и обрабатываемая техническими средствами, а также представленная в виде информативных электрических сигналов, физических полей, носителей на бумажной, магнитной, оптической и иной основе, в виде информационных массивов и баз данных в автономных персональных ЭВМ.

В-третьих, добытая конкурентами как дозволенными, так и не дозволенными методами сбора конфиденциальная информация о предприятии может быть использована ими для нанесения ущерба деятельности предприятия.

В-четвертых, сбор интересующей информации о предприятии может проводиться различными методами, способами и средствами с использованием разнообразных каналов несанкционированного доступа к конфиденциальной информации и ее носителям.

С. В. Белов
Россия, г. Астрахань, АГТУ

ОЦЕНКА СТЕПЕНИ НАБЛЮДАЕМОСТИ ТЕРРИТОРИИ БЕЗ ИСПОЛЬЗОВАНИЯ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ

Задача повышения эффективности использования технических средств обеспечения защиты (ТСОЗ) объекта информации является актуальной ввиду большой стоимости ТСОЗ и их важности в процессе защиты. Данная работа посвящена формализации и разработке методов решения ряда задач, возникающих в процессе обеспечения защиты объекта информации с использованием ТСОЗ.

Для решения задачи повышения эффективности использования ТСОЗ, прежде всего, необходимо сформировать список показателей, характеризующих эффективность использования ТСОЗ. Для формирования списка показателей будем исходить из следующей этапности действий потенциального злоумышленника при проникновении к защищаемой информации.

1. Выявление объекта, содержащего информацию, которая представляет интерес для злоумышленника.

2. Наблюдение объекта информации.

3. Разработка вариантов проникновения к защищаемой информации.

4. Реализация основного варианта проникновения на объект.

5. В случае возникновения непредвиденных проблем, реализация одного из альтернативных вариантов.

6. Уход из объекта защиты с возможной полной или частичной ликвидацией следов проникновения.

Использование ТСОЗ представляет наибольшей интерес для противодействия на втором, четвертом, пятом и шестом этапах действия злоумышленника. Именно на втором этапе задача ТСОЗ – максимально затруднить злоумышленнику наблюдение объекта – характеризуется показателем W_0 наблюдаемости объекта защиты.

На четвертом этапе задача ТСОЗ – обеспечить максимальную прозрачность и наблюдаемость объекта для систем защиты, которая характеризуется, прежде всего, показателями Z1 наблюдаемости объекта без использования ТСОЗ в статических условиях контроля, Z2 – эффективности использования ТСОЗ в процессе обеспечения защиты. Критерии Z3, Z4 определяют эффективность использования охранных групп в процессе динамического (например, обход и контроль объекта), и адаптивного (например, оперативность прибытия в зону нарушения защиты) контроля объекта. На пятом этапе задача определяется показателем Z5, описывающим полноту и быстроту перекрытия (блокировки) всех возможных путей перемещения злоумышленника в случае выявления потенциальной возможности нарушения защиты. Наконец, на шестом этапе – показателем Z6 эффективности действия защиты по нейтрализации злоумышленника и последствий его проникновения на объект защиты информации.

Целесообразно перечисленные выше показатели привязать к конкретным территориальным и временным координатам. Однако мы ограничимся рассмотрением совокупности перечисленных показателей, привязанных к (и изменяющихся) каждой элементарной зоне объекта защиты информации (рис. 1.):

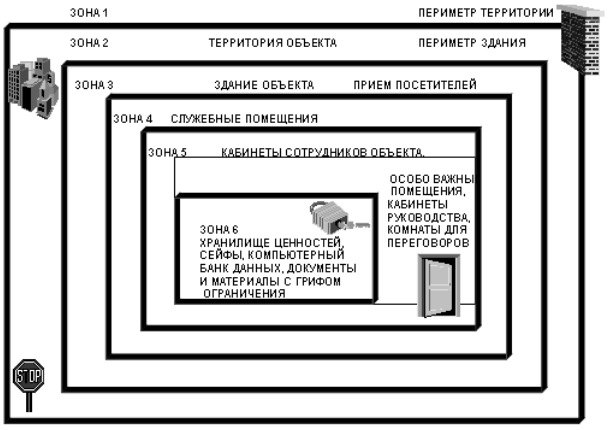

Рис. 1. Типы зон охраняемого объекта

внешнее окружение, территория до забора организации; территория объекта, территория от забора до зданий; здания; - комнаты; хранилища информации.

Вывод формул для выше перечисленных показателей осуществляется на основе стандартных методов математики (аналитической геометрии и интегрального исчисления).

Приведем аналитические соотношения для одного из наиболее важных показателей из перечисленных выше – показателя Z1 наблюдаемости зоны.

Любую поверхность можно задать функцией $z = f(x, y)$. Кроме этого любой объект на плоскости можно задать следующей функцией: $z = f(x, y, x_0, y_0)$, (1)

где x_0, y_0 - центр данного объекта.

Для каждого типа объекта (куст, дерево, яма, столб, любой другой искусственный предмет) можно задать шаблон, при котором достигается оптимальная наблюдаемость плоскости

$$z = f_{sh}(x, y, x_i, y_i) \tag{2}$$

с центром в точке (x_i, y_i)

Тогда для любой точки (x, y) относительно наблюдателя в точке (0, 0) можно записать следующие соотношения:

$$L = \max_{(x,y)\in G} g(x, y)$$

$$g(x, y) = \left(\sum_i \left[\frac{f_i^{(k)}(x, y, x_i, y_i)}{f_{sh}^{(k)}(x - x_i, y - y_i)} - 1 \right]^{\alpha} \right)^{1/\alpha} \cdot \chi(\varphi(x, y) \in \Phi(x_i, y_i), \sqrt{x^2 + y^2} > \sqrt{x_i^2 + y_i^2}) \tag{3}$$

где G – часть территории наблюдения, которую оцениваем;

α - константа, подбираемая путем эксперимента;

k – тип объекта;

χ - функция описывающая положение точки (x,y) в тени объекта;

$\Phi(x_i, y_i)$ - характеристика шаблона, описывающая вертикальный контур шаблона (как площадь, так и степень прозрачности шаблона). Может задаваться аналитически, алгоритмически и случайным датчиком.

Чем больше g(x,y) тем меньше точка наблюдаема. Тогда L показывает на менее наблюдаемую точку на плоскости.

Для удобства перейдем в полярную систему координат

$$\begin{aligned} x &= x_0 + \rho \cos \varphi, \\ y &= y_0 + \rho \sin \varphi. \end{aligned} \tag{4}$$

Для наблюдаемости зоны можно записать следующее соотношение:

$$z_1 = \left(\iint_{\rho,\varphi} L^{\alpha} r dr dx \right)^{1/\alpha}. \tag{5}$$

На основе приведенных соотношений может быть оценена степень наблюдаемости как всей территории, так и ее фрагментов, выявлены наиболее уязвимые участки территории, а также найдены наиболее слабо контролируемые маршруты пути передвижения по контролируемой территории.

В частности задача выбора маршрута заключается в следующем. Пусть траектория передвижения по маршруту L (рис. 2.) от границы зоны (X_1,Y_1) до объекта защиты информации (X_0,Y_0) задается следующими параметрическими уравнениями:

$$\begin{cases} x = \varphi(t) \\ y = \psi(t) \end{cases} \qquad 0 \le t \le T\,, \tag{6}$$

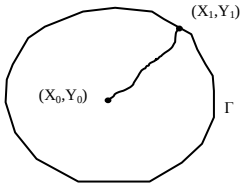

Рис. 1

где T – время движения по маршруту.

Тогда
$$x_1 = \varphi(0);\ x_0 = \varphi(T);$$
$$y_1 = \psi(0);\ y_0 = \psi(T). \tag{7}$$

Тогда выбор маршрута определяется соотношением $\inf\limits_{(x_1,y_1)\in\Gamma}\left(\max\limits_{t} g(\varphi(t),\psi(t))\right)$, (8)

где $\max\limits_{t} g(\varphi(t),\psi(t))$ описывает возможность обнаружения злоумышленника хотя бы на одной из точек траектории.

Д.Б. Халяпин, Д.С. Чередниченко
Россия, г.Москва, РГГУ

ОПТИМИЗАЦИЯ ВИБРОЗАШУМЛЕНИЯ НЕСУЩИХ КОНСТРУКЦИЙ ВЫДЕЛЕННОГО ПОМЕЩЕНИЯ ЗА СЧЕТ ИСПОЛЬЗОВАНИЯ АКУСТИЧЕСКИХ ВОЛНОВОДОВ

В настоящее время на российском рынке представлено значительное количество различных систем виброакустической защиты помещений с разными характеристиками. Однако в использовании всех этих систем существует одна трудность - все датчики имеют круговые диаграммы области зашумления, а зашумлять необходимо прямоугольные поверхности (рис. 1). В результате у пользователя есть две возможности - использовать датчики по соприкосновению зон зашумления (при минимальном количестве датчиков) или для устранения зон недостаточной зашумленности (темные области на рис.1) значительно увеличивать в ряде случаев количество вибраторов. Последнее потребует увеличения мощности систем, увеличение объема монтажных работ и т.п. На факультете защиты информации РГГУ на этапе проведения дипломной работы был разработан зашумляющий датчик с конфигурацией зоны зашумления близкой к прямоугольной. Это удалось достичь путем использования акустических волноводов, обеспечивающих перенос части энергии датчика в незакрытые участки защищаемой поверхности (рис. 2 и 3).

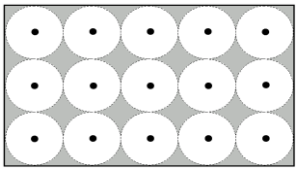

Рис. 1. Вариант расположения датчиков на защищаемой поверхности стены