УДК 654.924

ОСОБЕННОСТИ РАЗРАБОТКИ СТРУКТУРЫ СРЕДСТВ ОБНАРУЖЕНИЯ УГРОЗ ОХРАНЯЕМОМУ ОБЪЕКТУ

В.В. Волхонский, А.Г. Крупнов

Выполнен анализ возможных воздействий на средства обнаружения угроз. Предложен подход для учета этих воздействий, позволяющий решать задачи разработки структуры средств обнаружения и делать аргументированный выбор их параметров и характеристик. Показаны ограничения в использовании метода многорубежной охраны. Даны рекомендации по построению структуры средств обнаружения.

Ключевые слова: угрозы, средства обнаружения, система безопасности, охраняемый объект.

Введение

Как известно, одна из важнейших задач системы безопасности (СБ) – это своевременное и надежное обнаружение комплекса угроз объекту обеспечения безопасности [1]. Очевидно, что возможность решения этой задачи зависит как от конкретных видов угроз, так и от правильности выбора средств обнаружения (СО) и их расположения на объекте обеспечения безопасности, т.е. от структуры СО угроз. В настоящее время имеется достаточно много публикаций по вопросам выбора принципа действия, параметров и расположения на объекте одиночных устройств обнаружения [2]. О днако для совокупности СО задачи выбора структуры комплекса СО решаются лишь на уровне эмпирических рекомендаций. В частности, это относится к методу многорубежной охраны в системах охранной сигнализации [3, 4] с использованием нескольких СО несанкционированного проникновения (НСП). Однако эти рекомендации ограничиваются необходимостью использовать СО разного физического принципа действия. При этом не говориться о выборе конкретного физического принципа действия, взаимного расположения самих СО и их зон обнаружения (ЗО), что, несомненно, должно оказывать влияние на вероятность обнаружения угрозы.

Таким образом, возникает задача аргументированного выбора упомянутых параметров с учетом вероятностных характеристик, что позволило бы повысить эффективность СБ.

Поскольку задачи обнаружения различных видов угроз имеют специфику, в дальнейшем ограничимся наиболее распространенным случаем НСП. При необходимости результаты, приведенные ниже, могут быть обобщены и на другие виды угроз.

Модели нарушителя

Возможности по обнаружению проникновения в значительной мере будут зависеть от степени подготовленности нарушителя, которая может характеризоваться моделью потенциального нарушителя. Общие вопросы разработки модели нарушителя рассмотрены в [5]. Для предварительного анализа возможно использование упрощенной модели, для которой можно условно выделить следующие три основных категории.

- *Неподготовленный,* действующий без априорной информации об объекте и СБ. Вероятнее всего, он будет проникать через наиболее уязвимые места объекта. Неподготовленный нарушитель обычно не имеет конкретной цели и действует спонтанно.
- *Подготовленный*, обладающий простейшими подручными средствами (инструменты, лестница и др.) и априорной информацией об объекте и СБ, в том числе базовыми знаниями о принципах функционирования СБ, в частности, СО. Зная о возможном наличии средств охраны, он будет искать также и менее защищенные СО места. Подготовленный нарушитель имеет, как правило, конкретную цель и тактику действий.
- *Высококвалифицированный*, владеющий существенной априорной информацией как об объекте, так и о СБ, включая знание ее основных параметров и деталей функционирования ее элементов, а также имеющий специальные средства (инструменты, детали и приборы, и др.). В дополнение к этому он может применять различные методы и способы противодействия системе безопасности и воздействия на нее, основываясь на предварительной информации не только об объекте, но и о самой СБ, собранной ранее. Проникновение возможно с любого направления, с применением различных методов «обхода» средств обнаружения и с возможным воздействием на различные элементы СБ как в процессе проникновения, так и выполненным предварительно.

Методы воздействия на СБ

Для достижения своей цели нарушитель может использовать различные приемы и средства, а также маршруты проникновения, позволяющие свести к минимуму вероятность обнаружения НСП. Выбор преступником этих методов и средств определяется априорной информацией о типе СО, их физическом принципе действия, расположении на объекте и т.п. Вероятность обнаружения также зависит от квалификации преступника, точнее, от его возможностей по использованию средств и методов, уменьшающих

вероятность его обнаружения. В связи с этим известные модели нарушителей, упомянутые выше, целесообразно связать с методами и способами воздействия на СО того или иного типа нарушителя.

Можно говорить о двух основных методах несанкционированного воздействия на средства обнаружения для снижения вероятности обнаружения.

1. *Пассивный метод***,** предполагающий использование приемов и средств, уменьшающих вероятность обнаружения без прямого или косвенного воздействия на само устройство обнаружения или другие элементы СБ. Такой метод можно условно назвать обходом средств обнаружения. Примерами могут служить следующие действия:
   - Перемещение на границах зон обнаружения, где чувствительность, а, следовательно, и вероятность обнаружения ниже;
   - Перемещение со скоростями вне рабочего диапазона обнаружения (выше или ниже соответственно максимальной и минимальной скоростей обнаружения);
   - Использование средств снижения видимости объекта обнаружения в рабочем спектральном диапазоне.
2. *Активный метод,* использующий непосредственные воздействия на СО, иначе говоря, воздействия (механические, электрические, программные и т.п.), нарушающие нормальное функционирование элементов СБ и либо снижающие вероятность обнаружения угрозы, либо исключающие саму возможность обнаружения. Такой метод можно условно назвать противодействием СО. Подобное противодействие СО может быть прямым (к примеру, закрашивание оптической системы) или косвенным (например, загораживание зоны обнаружения).

Сравнивая методы воздействия на СБ и модели нарушителей, можно говорить о том, что неподготовленный преступник не использует никакие из упомянутых методов, подготовленный – пассивные методы, а высококвалифицированный – все методы, как пассивные, так и активные.

Многорубежная охрана

Проанализируем применяемый в настоящее время способ использования многорубежной охраны [3, 4] с учетом модели нарушителя и различных вариантов структуры и состава СО. Предполагая, что используется модель неподготовленного нарушителя, а средства обнаружения имеют разные физические принципы действия, можно говорить, как показано в [4], о независимости функционирования СО разных рубежей. Обозначая вероятности P_i обнаружения каждым *i*-ым рубежом (т.е *i*-ым СО), вероятность P^I обнаружения хотя бы одним из рубежей будет для двух рубежей равна $P^2 = P_1 + P_2 - P_1P_2$, а для трех – $P^3 = P_1 + P_2 + P_3 - P_1P_2 - P_1P_3 - P_2P_3 + P_1P_2P_3$. Таким образом, многорубежная охрана позволяет повысить вероятность обнаружения СБ в целом. На практике обычно используется до трех рубежей в одной подсистеме, например, охранной сигнализации. Однако, учитывая возможности по обнаружению одной и той же угрозы разными подсистемами безопасности [4], для интегрированной системы безопасности можно использовать общее выражение $P^I = 1 - \prod_{i=1}^{I}(1 - P_i)$ для произвольного количества рубежей.

В случае подготовленного нарушителя, использующего активные и пассивные методы воздействия на СО, предположение о независимости функционирования средств обнаружения становится неправомочным. Также это предположение не будет соответствовать действительности в случае перекрытия зон обнаружения. Другими словами, используемые рекомендации по организации многорубежной охраны соответствуют действительности, но только для неподготовленного нарушителя. В связи с этим требуется оценка вероятности обнаружения с учетом влияния на условия окружающей среды и различных методов активного и пассивного воздействия.

Анализ вероятности обнаружения

В общем случае вероятность обнаружения будет зависеть от ряда факторов, к основным из которых можно отнести следующие.

- Совокупность факторов, определяющих окружающие условия (ОУ) и влияющие на *j*-ое СО. Обозначим их $\mathbf{E}^j$.
- Пассивные способы воздействия (ПВ) на *j*-ое средство обнаружения или обход СО. Обозначим *n*-ое пассивное воздействие на *j*-ое СО как B_n^j, а множество N возможных воздействий на средства обнаружения как $\mathbf{B}^j$**.**
- Активные способы воздействия (АВ). Пусть множество $\mathbf{A}^j$ определяет совокупность K возможных воздействий A_k^j на *j*-ое СО.

Тогда вероятность обнаружения i-ой угрозы T_i j-ым СО можно записать как функцию упомянутых выше факторов $P_i^j = P(D_i^j / \mathbf{E, B, A})$. При условии воздействия всех факторов множество $\mathbf{S}$ возможных воздействий будет определяться пересечением подмножеств АВ, ПВ и ОУ, т.е. $\mathbf{S} \subseteq (\mathbf{A} \cap \mathbf{B} \cap \mathbf{E})$. Обычно имеет место только часть $\mathbf{S}_i$ воздействий, формируемых i-ой угрозой и определяемых соответствующими подмножествами $\mathbf{E}_i \subset \mathbf{E}$, $\mathbf{B}_i \subset \mathbf{B}$, $\mathbf{A}_i \subset \mathbf{A}$, для которых справедливы соотношения $\mathbf{S}_i \subseteq (\mathbf{A}_i \cap \mathbf{B}_i \cap \mathbf{E}_i)$, $\mathbf{S}_i \subset \mathbf{S}$. Заметим, что в общем случае $\mathbf{A} \bigcap \mathbf{E} \neq \varnothing$, $\mathbf{A} \bigcap \mathbf{B} \neq \varnothing$ и $\mathbf{E} \bigcap \mathbf{B} \neq \varnothing$, т.е. факторы АВ, ПВ и ОУ могут частично совпадать.

Ясно, что рассматриваемые воздействия, как правило, приводят к уменьшению вероятности обнаружения и эффективности СБ в целом. Рассматривать крайне редкие случаи повышения вероятности обнаружения при том или ином виде воздействия вряд ли имеет смысл. В связи с этим с точки зрения увеличения надежности обнаружения необходимо обеспечить независимость функционирования СО от окружающих условий, пассивных и активных воздействий, насколько это возможно.

Проанализируем, какие требования к структуре средств обнаружения должны предъявляться при использовании модели подготовленного нарушителя, т.е. только пассивных способов воздействий на СО.

Очевидно, что N возможных пассивных воздействий $\mathbf{B}^j = [B_1^j, B_2^j, ..., B_N^j,]$ на j-ое СО зависят, в первую очередь, от принципа действия СО и его положения на объекте, а, следовательно, и расположения зоны обнаружения. Аналогично для k-го СО L воздействий $\mathbf{B}^k = [B_1^k, B_2^k, ..., B_L^k,]$ могут совпадать или отличаться от j-го в зависимости от принципа их действия и взаимного расположения.

Для повышения вероятности обнаружения необходимо исключить возможность одновременного разного пассивного воздействия на оба СО. Для этого события любой пары B_n^j и B_l^k должны быть несовместными, $B_n^j \bigcap B_l^k = \varnothing$, для обеспечения невозможности одновременно выполнения этого воздействия, т.е.

$$\bigcup_{n \in N} B_n^j \bigcap \bigcup_{l \in L} B_l^k = \varnothing \ , \ j \in J, k \in K \ . \qquad (1)$$

Невыполнение последнего равенства соответствует случаю, когда есть общий(ие) фактор(ы) ПВ, одновременно применимый(ые) к обоим СО.

Простым способом проверки правильности приведенных выше рассуждений может служить выбор принципов действия каналов обнаружения комбинированных датчиков движения. В настоящее время используется практически только одно сочетание – пассивный инфракрасный и радиоволновой. Действительно, преобразуя выражение (1) для случая воздействий ОУ на СО, можно записать выражение, определяющее необходимость $\bigcup_{n \in N} E_n^j \bigcap \bigcup_{l \in L} E_l^k = \varnothing$, $j \in J, k \in K$. Это выполняется практически в полной мере для упомянутого сочетания, подобранного опытным путем, но не для других. Таким образом, полученные результаты могут служить математическим обоснованием такого выбора.

Используя формулу полной вероятности применительно к рассматриваемой задаче, можно записать выражение для вероятности обнаружения при условии воздействий на СО комплекса угроз

$$P^j(D^j / \mathbf{E, B, A}) = \sum_{i=1}^{I} P(\mathbf{S}_i^j) \cdot P(D^j / \mathbf{S}_i^j), \text{ где } \mathbf{S}_i^j \subseteq \mathbf{S}. \qquad (2)$$

Из этого выражения и предыдущих рассуждений можно сделать общие выводы, что для обеспечения максимума вероятности обнаружения угрозы необходимы:

- инженерное обеспечение объекта и структура СО, позволяющие свести к минимуму вероятность $P(\mathbf{S}_i^j)$ реализации различных видов воздействий;
- структура СО, обеспечивающая минимум влияния окружающих условий и, следовательно, максимум вероятности $P(D^j / \mathbf{S}_i^j)$;
- выбор СО, обладающих минимальной чувствительностью к неинформативным физическим параметрам объекта, т.е. параметрам, на которые не воздействует угроза при ее реализации.

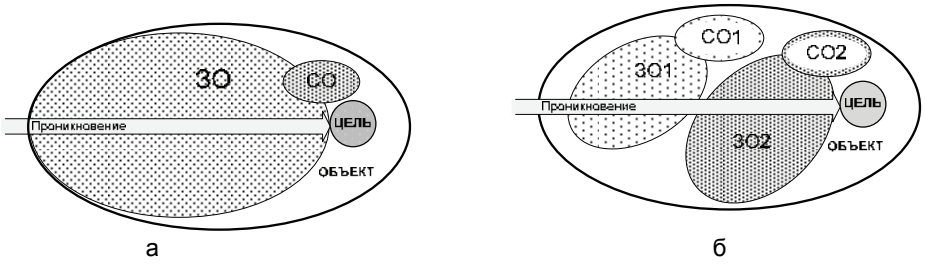
Из первого пункта следует также необходимость обнаружения не только угрозы объекту, но и воздействия на элементы системы безопасности. Это, впрочем, можно рассматривать как дополнительную угрозу, но не объекту, а самой системе безопасности.

Более детальные выводы можно сделать на основе анализа конкретной ситуации с использованием того или иного метода анализа или оптимизации выражения (2).

Выбор положения и формы зон обнаружения

Проанализируем требования к взаимному расположению средств обнаружения и соответствующих им зон обнаружения.

Одиночная зона – простейший случай (рис. 1, а), при котором возможность использования различных воздействий не представляет трудностей.



а б

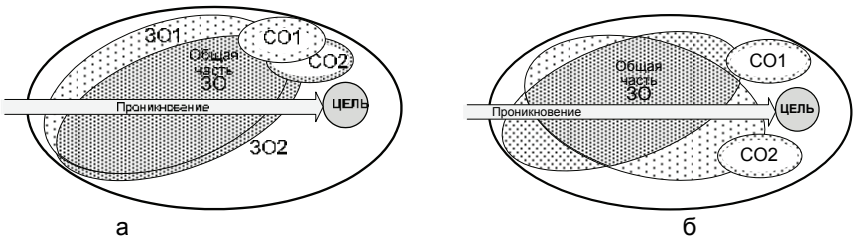
Рис. 1. Одиночная (а) и последовательные (б) зоны обнаружения

Два требования по расположению зон обнаружения на объекте в этом случае очевидны и относятся к любой модели нарушителя [1].

– Начало зоны обнаружения должно быть максимально приближено к периметру объекта, чтобы обеспечить возможность максимально раннего обнаружения.
– Предполагаемый маршрут НСП должен, по возможности, больше проходить по зоне обнаружения, поскольку при этом возрастает продолжительность воздействия на физический параметр зоны, контролируемый средством обнаружения. Для этого нужно выбирать параметры зоны обнаружения (положение и размеры) таким образом, чтобы преступник перемещался по зоне, в идеальном случае, на всем маршруте несанкционированного проникновения (рис. 1, а).

Неперекрывающиеся зоны обнаружения. Упоминавшаяся многорубежная охрана состоит в использовании нескольких ЗО на маршруте НСП. С точки зрения расположения этих зон они могут быть последовательными, не перекрывающимися (рис. 1, б) или с перекрытием (рис. 2). Но в первом случае при проникновении подготовленного нарушителя не будет выполняться требование несовместности $B_n^j \bigcap B_l^k = \varnothing$ пассивных воздействий, поскольку в каждой из следующих последовательных (без перекрытия) ЗО может применяться новый набор ПВ, соответствующий физическому принципу действия конкретного типа СО. Например, для структуры СО на рис. 1, б, можно применить сначала воздействие B_i^1, а затем B_k^2, делая это независимо. С точки зрения снижения возможности ПВ на СО действительно целесообразно использовать СО различного физического принципа действия [3]. Это усложняет задачу НСП, но не является оптимальным решением, т.е. лишь отчасти усложняет задачу нарушителя и повышает надежность обнаружения.

Перекрывающиеся зоны обнаружения. При перекрывающихся зонах (рис. 2) возникает необходимость использования одновременно нескольких воздействий. В связи с этим совмещение ЗО позволяет затруднить или полностью исключить ПВ на все СО одновременно. Если зоны обнаружения перекрываются, возможно несколько вариантов.



а б

Рис. 2. Перекрывающиеся ЗО средств обнаружения, расположенных в одном (а) и разных местах (б)

1. Перекрывающиеся зоны обнаружения СО одного физического принципа действия, расположенных в одной области объекта (рис. 2, а). При этом для обхода обоих СО потребуются одни и те же действия. Следовательно, такой вариант не приведет практически к сколько-нибудь существенному увеличению вероятности обнаружения.
2. Перекрывающиеся зоны обнаружения СО одного физического принципа действия, установленных в разных областях объекта, например, как на рис. 2, б. В этом случае часть действий, необходимых для

обхода разных СО, будут отличаться (т.е. может выполняться сформулированное выше требование несовместности действий), и обычно выполнить их одновременно не удается.

3. Перекрывающиеся зоны СО с разными физическими принципами действия, расположенные в одном месте. В такой ситуации методы и средства обхода, как правило, будут отличаться в значительной мере, зачастую полностью, что исключает использование их одновременно. Следовательно, и вероятность обнаружения будет выше.

Очевидно, что при решении практических задач на основе приведенных выше рассуждений требуется учет конкретного физического принципа действия СО.

Основные правила выбора структуры средств обнаружения

Учитывая изложенное выше, в дополнение к общим требованиям к системе безопасности [1] можно сформулировать основные правила или принципы построения структуры средств обнаружения угроз на объекте обеспечения безопасности, состоящие в необходимости обеспечить следующее:

1. Использование перекрытия ЗО в пространстве, т.е. решение задачи обнаружения угрозы одновременно во времени несколькими средствами обнаружения;
2. Выбор места установки каждого СО и их взаимного расположения так, чтобы эффективные пассивные воздействия на средства обнаружения были несовместными для разных СО, контролирующих одну и туже зону, т.е. создание условий, требующих выполнения невыполнимого;
3. Возможность выявления эффективных активных воздействий на средства обнаружения либо самим СО, либо специализированными средствами обнаружений воздействия в любом состоянии (в любом режиме работы) СБ;
4. Использование многопараметрических СО, т.е. средств, анализирующих одновременно несколько физических параметров объекта обеспечения безопасности при реализации угрозы;
5. Равную защищенность объекта или цели(ей), предполагающую возможность своевременного реагирования после обнаружения угрозы для любого маршрута НСП;
6. Формирование зон(ы) обнаружения, перекрывающей любой и весь маршрут НСП или, по крайней мере, наиболее уязвимые места возможного маршрута;
7. Использование инженерных средств технической укрепленности, вынуждающих нарушителя двигаться по маршруту с максимально надежным обнаружением НСП.

Строго говоря, такая характеристика как вероятность обнаружения, используемая в работе, может оказаться в ряде случаев недостаточной для анализа уязвимостей объекта критической инфраструктуры, поскольку в такой ситуации не учитываются протяженность зон обнаружения и распределение вероятности обнаружения по зоне. В таких случаях представляется целесообразным использование плотности распределения вероятности обнаружения на маршруте прохождения нарушителя и способа анализа, предложенного в [6]. Очевидно, что при этом форма плотности распределения вероятности будет зависеть от окружающих условий и применяемых пассивных и активных способов противодействия. Из этих же рассуждений следует также необходимость тщательного учета протяженности зоны обнаружения и возможной формы кривой плотности распределения вероятности обнаружения.

Заключение

На основе анализа известных методов и приемов построения структуры средств обнаружения на объектах обеспечения безопасности и возможных воздействий на СО в работе получены следующие результаты.

- Предложен подход к анализу структуры СО на основе описания вероятности обнаружения как функции множества воздействий на средства обнаружения, позволяющий получить математическое выражение для вероятности обнаружения и учитывающий окружающие условия, пассивные и активные воздействия на СО угроз. Проанализированы соотношения между подмножествами пассивных и активных воздействий и окружающих условий на СО.
- Показано, что для повышения вероятности обнаружения угроз необходимо обеспечить выполнение требования несовместности воздействий на СО.
- Обоснована целесообразность установки средств обнаружения одного физического принципа действия в разных частях объекта, а разного – в одной, с перекрытием их зон обнаружения.
- Показано, что при использовании известного метода многорубежной охраны имеются ограничения. Так, для увеличения вероятности обнаружения целесообразно перекрытие зон обнаружения, а выбор взаимного расположения СО будет зависеть от их физического принципа действия.
- Обобщены и математически подтверждены известные требования к построению структуры СО, в частности, по используемому сочетанию типов обнаружителей в комбинированных датчиках движения (пассивный инфракрасный и радиоволновой).

В целом, полученные результаты позволяют осуществить аргументированный выбор принципа действия и взаимного расположения на объекте СО для минимизации возможности действий нарушителя по снижению вероятности обнаружения НСП.

Литература

1. Волхонский В.В. Основные положения концепции обеспечения безопасности объектов // Научно-технический вестник СПбГУ ИТМО. – 2011. – № 3(73). – С. 116–121.
2. Волхонский В.В. Извещатели охранной сигнализации. Изд. 4-е доп. и перераб. – СПб: Экополис и культура. – 2004. – 272 с.
3. Коновалов В.А., Севрюков Д.В., Хасянов Р.С. Многорубежная защита. Особенности охраны периметра в обеспечении комплексной безопасности особо важных объектов // Системы безопасности. – 2007. – № 3. – С. 114–117.
4. Волхонский В.В. Системы охранной сигнализации. 2-е изд., доп. и перераб. – СПб: Экополис и культура. – 2005. – 204 с.
5. Бояринцев А.В., Ничиков А.В., Редькин В.Б. Общий подход к разработке моделей нарушителей // Системы безопасности. – 2007. – № 4. – С. 50–53.
6. Волхонский В.В. Подход к оценке вероятности пресечения несанкционированных действий в объединенной системе безопасности // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – Київ, 2000. – С. 77–81.

Волхонский Владимир Владимирович – ЗАО Хоневелл, кандидат технических наук, доцент, руководитель направления систем безопасности, volkhonski@mail.ru

Крупнов Алексей Геннадьевич – Санкт-Петербургский государственный университет информационных технологий, механики и оптики, студент, krupnov@list.ru