УДК 654.924

В. В. ВОЛХОНСКИЙ

КРИТЕРИИ ВЫБОРА КОНТРОЛИРУЕМЫХ СРЕДСТВАМИ ОБНАРУЖЕНИЯ ПАРАМЕТРОВ В СИСТЕМЕ БЕЗОПАСНОСТИ

Представлен анализ модели системы безопасности на основе теории множеств с учетом специфики системы безопасности, особенностей проявления угроз и условий окружающей среды. Сформулированы критерии выбора параметров объекта, контролируемых средствами обнаружения.

Ключевые слова: *система безопасности, параметры средств обнаружения, критерии выбора.*

Введение. Важнейшим элементом любой системы физической и информационной безопасности являются средства обнаружения угроз. При этом очевидно, что основные характеристики системы существенно зависят как от параметров самих средств обнаружения, так и от выбора физических параметров объекта, которые должны контролироваться этими средствами и которые изменяются под воздействием угроз. С этой точки зрения весьма важным представляется необходимость формулировки общих рекомендаций и критериев по выбору упомянутых параметров. В известных источниках (см., например, [1—3]) рассматриваются лишь частные практические рекомендации, требующие теоретического обобщения, аналитического обоснования и развития применительно к различным ситуациям. Поэтому задача такого обобщения, обоснования и развития представляется актуальной и рассматривается в настоящей статье.

Модель системы безопасности. Рассмотрим интегрированную систему безопасности, состоящую из нескольких подсистем. Из общей структуры технических средств системы безопасности [2] можно выделить средства обнаружения угроз и датчики контроля состояния окружающей среды, средства сбора и обработки информации и средства противодействия угрозам. Причина выбора именно этих средств очевидна — согласно общему определению систем безопасности [2], они являются обязательными элементами любой такой системы как совокупности методов и средств предупреждения, обнаружения и ликвидации угроз жизни, здоровью, окружающей среде, имуществу, информации и ресурсам.

В общем случае имеется совокупность входных воздействий, контролируемых соответствующими датчиками. Можно выделить две основные составляющие этих воздействий: 1) множество $\mathbf{E} = [E_1, E_2, ..., E_N]$ параметров, характеризующих воздействия окружающей среды и влияющих на функционирование объекта и системы безопасности в целом; 2) множество $\mathbf{O}$ параметров объекта, изменяющихся под воздействием угроз охраняемому объекту.

Множество $\mathbf{O}$ состоит из подмножеств $\mathbf{O}_j$, определяющих физический характер проявления каждой j-й из J возможных угроз при их реализации: $\mathbf{O} = \left[\mathbf{O}_1, \mathbf{O}_2, ...\mathbf{O}_j, ...\mathbf{O}_J\right]$. Для этих подмножеств справедливо соотношение $\mathbf{O} = \bigcup_{j=1}^{J} \mathbf{O}_J$. Также можно утверждать, что в общем случае подмножества, соответствующие j-й и i-й угрозам, пересекающиеся, т.е. $\mathbf{O}_j \bigcap_{j,i \in J} \mathbf{O}_i \neq \varnothing$. Иными словами, часть рассматриваемых параметров, характеризующих раз-

ные угрозы, могут совпадать. Например, повышение температуры в помещениях контролируемого объекта может быть вызвано либо такой угрозой, как пожар, либо неисправностью системы кондиционирования воздуха. Кроме того, при отсутствии проявлений *j*-й угрозы соответствующее подмножество $\mathbf{O}_j \neq \varnothing$.

Множество $\mathbf{E}$ параметров окружающей среды, как правило, представляет собой воздействия, сходные по характеру с проявлением угроз. К примеру, для доплеровских датчиков это может быть движение некоторых объектов (лопастей вентиляторов, жидкостей в трубах и т.п.), приводящее к такому же эффекту, как и обнаружение нарушителей. Следовательно, воздействия окружающей среды могут совпадать с проявлениями угроз, т.е. $\mathbf{E} \bigcap \mathbf{O} \neq \varnothing$. Таким образом, для обнаружения *j*-й угрозы необходимо рассматривать совокупность $\mathbf{S}_j = (\mathbf{O}_j \cup \mathbf{E})$ воздействий среды и проявлений угрозы.

В интегрированных системах безопасности имеется обычно *N* подсистем с различным функциональным назначением, например: охранная и пожарная сигнализация, контроль доступа, ТВ-наблюдение и др. В общем случае *n*-я подсистема, $n = 1, ..., N$, контролирует набор параметров $\mathbf{S}_j^{\text{п}n}$, зависящих от физических проявлений соответствующей *j*-й угрозы. При этом очевидно, что должно выполняться условие $\mathbf{S}_j^{\text{п}n} \subseteq \mathbf{S}_j$. Следовательно, на основе множеств $\mathbf{E}$ и $\mathbf{O}$ можно сформировать подмножества $\mathbf{S}_j^{\text{п}n}$, контролируемые соответствующими *n*-ми подсистемами. Эти подмножества $\mathbf{S}_j^{\text{п}n} \subseteq (\mathbf{O}_j \cup \mathbf{E})$ могут включать в себя часть или все элементы множеств $\mathbf{E}$ и $\mathbf{O}$.

Критерии выбора параметров. Рассмотрим особенности выбора набора параметров, контролируемых устройствами обнаружения. Для начала ограничимся случаем, когда каждая *n*-я подсистема контролирует только *j*-ю угрозу, соответствующую основному функциональному назначению этой подсистемы. Тогда $n = j$, а соответствующее подмножество будет $\mathbf{S}_j^{\text{п}j}$. К примеру, подсистема пожарной сигнализации контролирует возникновение такой угрозы, как возгорание.

Сформулируем основные критерии выбора этих параметров.

1. Как отмечалось, в общем случае подмножества $\mathbf{S}_j^{\text{п}j}$ включают в себя все элементы множеств $\mathbf{E}$ и $\mathbf{O}_j$, в том числе:

— подмножество, соответствующее пересечению $\mathbf{O}_j \cap \mathbf{E}$ и определяющее те характеризующие проявление угрозы параметры, на которые может оказывать влияние окружающая среда;

— подмножество $\mathbf{E} \setminus \mathbf{O}_j$, определяющее параметры, характеризующие воздействия окружающей среды, на которые не влияет наличие угроз.

Отсюда следует первый критерий выбора контролируемых параметров: $\mathbf{S}_j^{\text{п}j} \cap (\mathbf{E} \setminus \mathbf{O}_j) \to \varnothing$, т.е. датчики контроля состояния объекта должны быть *инвариантны к воздействиям окружающей среды*, которые не совпадают с проявлением угроз. Например, для пассивных инфракрасных (ПИК) датчиков — это минимизация воздействия на них засветки, которая не представляет собой проявление угрозы.

2. Второй критерий можно сформулировать как $\mathbf{E} \bigcap \mathbf{O}_j \to \varnothing$. Физически это означает необходимость *минимизации воздействия окружающей среды на параметры, характеризующие проявление угрозы*. Очевидно, что на характер проявления угрозы и, как следствие, на

множество $\mathbf{O}_j$ невозможно оказать сколько-нибудь заметное влияние. То же самое можно сказать и о множестве $\mathbf{E}$ параметров окружающей среды. Уровень влияния $\mathbf{E}$ обычно можно только свести к минимуму, например, устранив источники воздушных потоков и перепадов температур в помещении, где используются ПИК-датчики движения. Как частный случай, второй критерий можно записать в виде соотношения $\mathbf{S}_j^{\text{пj}} \subseteq (\mathbf{O}_j \setminus \mathbf{E})$, что соответствует исключению из анализа части параметров объекта, совпадающих с параметрами окружающей среды. Однако в этой ситуации могут возникнуть противоречия с критерием информативности, который рассматривается ниже (см. п. 7).

3. Поскольку на практике условия, соответствующие второму критерию, не всегда выполнимы, то можно говорить о необходимости обеспечить *минимум возможного влияния окружающей среды:* $\mathbf{E} \bigcap \mathbf{S}_j^{\text{пj}} \to \varnothing$. Это достигается выбором помехоустойчивых устройств, инвариантных к тому или другому виду воздействия, и правильностью установки таких устройств. Для предыдущего примера это означает выбор расположения ПИК-датчика, при котором засветка прямым солнечным светом исключена.

4. Расширим ограничения на рассматриваемую задачу и проанализируем возможность *обнаружения одной угрозы разными подсистемами.* С этим неотъемлемо связана возможность обнаружения разных угроз одной подсистемой.

Пусть каждой *j*-й подсистеме соответствует свое подмножество контролируемых параметров $\mathbf{S}_j^{\text{пj}}$. Тогда если подмножество $\mathbf{O}_i$ проявления *i*-й угрозы и подмножество $\mathbf{S}_j^{\text{пj}}$ параметров, контролируемых *j*-й подсистемой, непересекающиеся, т.е. $\mathbf{S}_j^{\text{пj}} \bigcap \mathbf{O}_i = \varnothing$, то такая подсистема может обнаруживать только „свои“ угрозы (для обнаружения которых эта подсистема функционально предназначена, т.е. $\mathbf{S}_i \bigcap \mathbf{O}_j \neq \varnothing$). В противном случае, если $\mathbf{S}_j^{\text{пj}} \bigcap \mathbf{O}_i \neq \varnothing$, у такой подсистемы появляется возможность обнаруживать не только „свою“ *j*-ю угрозу, но и *i*-ю угрозу „другой“ подсистемы. Для этого необходимо выполнение условий $\mathbf{S}_j^{\text{пj}} \bigcap \mathbf{O}_i \neq \varnothing$, $\mathbf{S}_i^{\text{пi}} \bigcap \mathbf{O}_j \neq \varnothing$, $i, j \in 1, ..., J$. По сути эти два условия идентичны: первое соответствует возможности одной подсистемы обнаруживать разные угрозы, а второе — возможности обнаружения одной угрозы разными подсистемами. Иными словами, кроме основного функционального назначения такая подсистема сможет реализовать функции и других подсистем по обнаружению угроз. К примеру, обнаружение несанкционированного проникновения нарушителя осуществляется, прежде всего, предназначенной для этого подсистемой охранной сигнализации. Однако в рассматриваемом случае оно может быть обнаружено также подсистемами контроля доступа и ТВ-наблюдения. Так, например, признаки пожара — это повышение температуры, изменения состава воздуха за счет появления частиц дыма, видимые изменения (задымление, пламя). Типичные датчики системы пожарной сигнализации реагируют на первые два проявления, а система ТВ-наблюдения — на третье. Значит, система ТВ-наблюдения может решать и задачи обнаружения возгорания.

На этом имеет смысл остановиться подробнее. Учет данного критерия позволит достичь выигрыша в вероятности обнаружения угрозы. В частности, в работе [2] приведено выражение для условного предотвращенного ущерба:

$$У_{\text{п}} = V \prod_{j=1}^{J} \left[1 - У_j^{\text{н}} \prod_{n=1}^{N} \left(1 - p_{nj}^{\text{п}} \right) \right],$$

где V — важность, значимость объекта защиты, в относительных единицах; J — количество угроз; $У_j^{н}$ — максимальный относительный ущерб, наносимый *j*-й угрозой; $p_{nj}^{п}$ — вероятность предотвращения *n*-й подсистемой безопасности *j*-й угрозы.

Также в этой работе выполнены расчеты, которые показывают, что использование для обнаружения одной угрозы нескольких подсистем позволяет повысить эффективность системы безопасности, т.е. существенно увеличить значение условного предотвращенного ущерба $У_{п}$.

5. Чтобы обеспечить *различимость проявлений разных угроз* необходимо выполнение условий $\left(\mathbf{S}_j^{пj} \cap \mathbf{O}_i\right) \cap \left(\mathbf{S}_j^{пj} \cap \mathbf{O}_j\right) = \varnothing$, $\left(\mathbf{S}_j^{пj} \cap \mathbf{O}_j\right) \cap \left(\mathbf{S}_i^{пi} \cap \mathbf{O}_j\right) = \varnothing$, $i, j \in 1, ..., J$. Применительно к физической реализации это означает использование различных (несовпадающих) контролируемых параметров для разных угроз.

6. Поскольку при несанкционированном проникновении нарушитель может применять методы противодействия средствам обнаружения (активные и пассивные) и различные средства снижения вероятности обнаружения, целесообразно рассмотреть возможность *минимизировать последствия таких действий*. Применительно к частной задаче выбора структуры средств обнаружения данная возможность рассмотрена в работе [3]. В этой работе показана необходимость выполнения условия $\bigcup\limits_{m \in M} B_m^j \cap \bigcup\limits_{l \in L} B_l^k = \varnothing$, $j, k \in J$, означающего, что события любой пары *m*-го и *l*-го пассивных воздействий B_m^j и B_l^k на средства обнаружения *j*-й и *k*-й угроз, применяемых квалифицированным нарушителем, должны быть несовместными в целях обеспечения невозможности одновременного выполнения этих воздействий. Этот подход можно развить и для общего случая как пассивных воздействий, так и совместных активных A_m^j и пассивных B_l^j воздействий, т.е. $\bigcup\limits_{m \in M} A_m^j \cap \bigcup\limits_{l \in L} A_l^k = \varnothing$, $\bigcup\limits_{m \in M} A_m^j \cap \bigcup\limits_{l \in L} B_l^k = \varnothing$, $j, k \in J$, что также соответствует требованию несовместности рассматриваемых воздействий.

Применительно к рассматриваемой задаче этот критерий соответствует условию выбора параметров $\mathbf{S}_j \cap \mathbf{S}_i \to \varnothing$, которое заключается в следующем. При использовании разными подсистемами одних и тех же параметров, характеризующих проявление угрозы (элементов множества $\mathbf{S}_j$) и требующих одних и тех же физических принципов обнаружения, возникают новые угрозы, которые могут привести к ухудшению параметров системы, а именно:

— изменение какого-либо из элементов множества $\mathbf{S}_j$ в худшую сторону при любых воздействиях (например, окружающей среды) будет оказывать одинаковое негативное влияние на обе подсистемы;

— дополнительные искусственные воздействия, снижающие интенсивность проявления угрозы (например, действия квалифицированного нарушителя [1, 3]), будут одинаково снижать характеристики обеих подсистем.

В этой связи для обнаружения различных физических проявлений угроз имеет смысл использовать разные подсистемы. Применительно к синтезу структуры средств обнаружения в целом целесообразно также следовать рекомендациям, приведенным в работе [1].

7. Для определения степени полноты использования информации о проявлениях угрозы необходимо ввести критерий $\mathbf{S}_j \to \mathbf{O}_i$ *максимальной информативности средств обнаружения*. Этот критерий показывает целесообразность использования всех характеризующих проявление угрозы параметров, а также соответствующих многопараметрических средств обнаружения.

Порядок и приоритетность выполнения условий, заданных сформулированными критериями, могут быть различными для разных конкретных задач. Выполнение этих условий, тем

не менее, позволяет повысить как вероятность обнаружения угроз, так и защищенность системы от воздействий нарушителя и окружающей среды.

Заключение. Предложенная модель системы безопасности на основе теории множеств учитывает как специфику системы, так и особенности проявления угроз объекту обеспечения безопасности и воздействия окружающей среды.

На основе предложенной модели сформулированы критерии выбора параметров, контролируемых средствами обнаружения системы, которые заключаются в анализе соотношений между множествами параметров объекта и параметров, характеризующих проявления угроз и воздействия окружающей среды. Сформулированные критерии можно использовать при структурном синтезе системы безопасности или разработке устройств обнаружения.

Проанализированы возможности обнаружения угроз разными подсистемами и сформулированы критерии выбора контролируемых параметров, позволяющие повысить вероятность обнаружения, в том числе, в условиях пассивного и активного противодействия нарушителя средствам обнаружения.

СПИСОК ЛИТЕРАТУРЫ

1. *Гарсиа М.* Проектирование и оценка систем физической защиты. М.: Мир, 2003. 388 с.

2. *Волхонский В. В.* Системы охранной сигнализации. СПб: Экополис и культура, 2005. 204 с.

3. *Волхонский В. В., Крупнов А. Г.* Особенности разработки структуры средств обнаружения угроз охраняемому объекту // Науч.-техн. вестн. СПбГУ ИТМО. 2011. № 4(74). С. 131—136.

Сведения об авторе

Владимир Владимирович Волхонский — канд. техн. наук, доцент; Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, кафедра твердотельной оптоэлектроники; E-mail: volkhonski@mail.ru

Рекомендована кафедрой твердотельной оптоэлектроники

Поступила в редакцию 21.11.11 г.