УДК 654.924

КРИТЕРИИ ВЫБОРА И ОЦЕНКИ СТРУКТУРЫ СРЕДСТВ ОБНАРУЖЕНИЯ

Волхонский В.В.

Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
197101, г. Санкт-Петербург, Кронверкский проспект, дом 49, e-mail: volkhonski@bkl.ru

В статье рассматриваются основные характеристики системы безопасности, которые существенно зависят как от параметров средств обнаружения угроз объекту обеспечения безопасности, так и от структуры этих средств обнаружения на объекте. Автор статьи говорит о двух основных группах методов повышения эффективности функционирования общей структуры средств обнаружения угроз объекту обеспечения безопасности. Для модели системы безопасности на основе теории множеств с учетом специфики системы безопасности и особенностей проявления угроз и окружающих условий формулируются критерии выбора и оценки структуры и параметров средств обнаружения. В статье сформулированы основные критерии выбора контролируемых средствами обнаружения параметров, которые можно использовать при структурном синтезе системы или разработке устройств обнаружения: инвариантности к воздействию окружающей среды. Для повышения эффективности средств обнаружения угроз необходимо выполнение таких основных критериев, как инвариантность датчиков контроля состояния объекта, минимизация влияния окружающей среды на параметры, являющиеся проявлением угрозы, и других.

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

CHOICE AND ESTIMATION CRITERIONS OF DETCTION DEVICES STRUCTURE

Volkhonskiy V.V.

Saint-Petersburg National Research University of Information Technology, Mechanics and Optics
197101, St. Petersburg, Kronverksky Avenue, Building 49, e-mail: volkhonski@bkl.ru

In article the basic characteristics of system of safety which essentially depend as on parameters of sensors of threats to object of safety, and from structure of these sensors on object are considered. The author of article speaks about two basic groups of methods of increase of efficiency of functioning of the general structure of sensors of threats to object of safety. For security system model based on set theory with taking in account specific of security system features, treats manifestations and environmental conditions criterions of choice and estimation of detection devices parameters and structure are formulated. In article the basic criteria of a choice of parameters supervised by sensors which can be used at structural synthesis of system or working out of devices of detection are formulated: invariancy to environment influence. For increase of efficiency of sensors of threats performance of such basic criteria, as invariancy of gages of control of a condition of object, minimization of influence of environment on the parameters which are display of threat and others is necessary.
Keywords: Security system, detection devices parameters, choice and estimation criterions.

Основные характеристики системы безопасности (СБ) существенно зависят как от параметров средств обнаружения (СО) угроз объекту обеспечения безопасности, так и от структуры этих средств обнаружения на объекте. В свою очередь параметры СО будут в значительной мере определяться выбором физических параметров объекта, которые должны контролироваться СО и которые изменяются под воздействием угроз. Поэтому важно сформулировать критерии выбора контролируемых параметров, структуры СО и оценки их эффективности.

Модель системы безопасности

Из общей структуры технических средств системы безопасности [1] можно выделить, в первую очередь, средства обнаружения угроз, датчики контроля окружающей среды, средства сбора и обработки информации и средства противодействия, поскольку это обязательные элементы любой подобной системы. На состояние объекта (т.е. на его безопасность) могут влиять как внешние, так и внутренние угрозы, которые СБ должна обнаружить и ликвидировать до момента нанесения существенного ущерба. На рис. 1 изображена диаграмма, учитывающая упомянутые элементы СБ, контролируемые параметры и угрозы объекту.

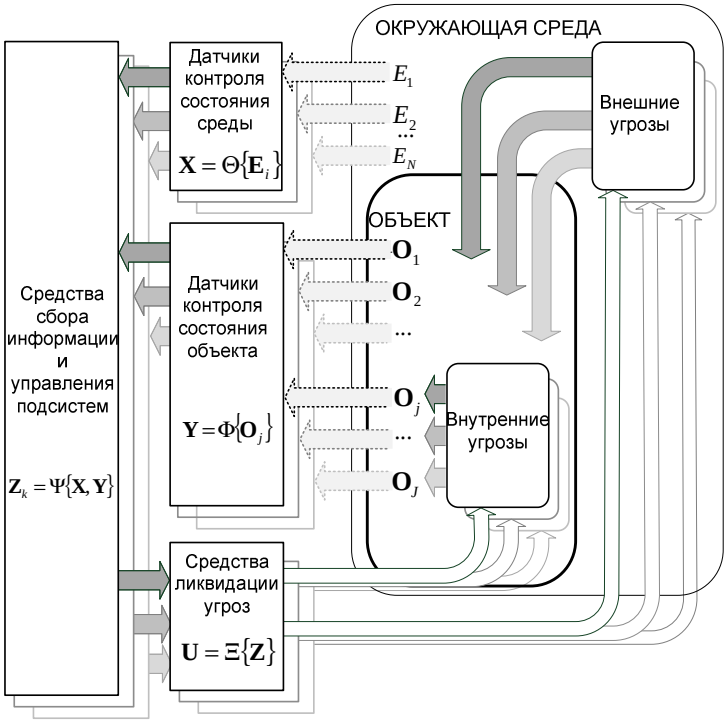

Рис. 1. Обобщенная модель системы безопасности.

Для выполнения своих функций система безопасности должна контролировать соответствующими датчиками следующие совокупности входных воздействий.

1. Совокупность N возможных факторов воздействия $\mathbf{E}^j = [E_1^j, E_2^j, ..., E_N^j]$, определяющих окружающие условия (ОУ) и влияющие на работоспособность и характеристики j-о СО. Обозначим n-е воздействие на это СО как E_n^j. Совокупность $\mathbf{E}$ параметров окружающей среды, как правило, представляет собой воздействия, по характеру сходные с проявлением угроз. К примеру, движение некоторых объектов (жидкостей в трубах, лопастей вентиляторов и т.п.) для доплеровских датчиков обнаружения движения нарушителей. Или такой параметр, как температура окружающей среды, влияет на работоспособность пассивных инфракрасных (ПИК) устройств обнаружения проникновения

и является проявлением такой угрозы, как пожар. Следовательно, они могут совпадать с проявлениями угроз, т.е. $\mathbf{E} \cap \mathbf{O} \neq \varnothing$. Т.о. для обнаружения j-й угрозы необходимо рассматривать совокупность $\mathbf{S}_j = (\mathbf{O}_j \cup \mathbf{E})$ воздействий среды и проявлений угрозы.

2. Совокупность $\mathbf{O}$ параметров объекта, меняющихся под воздействием угроз на объект, т.е. определяющих физический характер проявления угрозы при ее реализации. Множество $\mathbf{O}$ состоит из J подмножеств $\mathbf{O}_j$, определяющих физический характер проявление каждой j-й из J возможных угроз $\mathbf{O} = \lfloor \mathbf{O}_1, \mathbf{O}_2, ... \mathbf{O}_j, ... \mathbf{O}_J \rfloor$. Для этих подмножеств справедливо соотношение $\mathbf{O} = \bigcup_{j=1}^{J} \mathbf{O}_J$. Также можно утверждать, что в общем случае эти подмножества пересекающиеся, т.е. $\mathbf{O}_j \bigcap_{j,i \in J} \mathbf{O}_i \neq \varnothing$.

Кроме того, надо учесть, что в общем случае возможно противодействие средствами обнаружения. Например, применяемые при реализации такой угрозы, как несанкционированное проникновение нарушителя. Это может быть плотная одежда, позволяющая уменьшить эффективность ПИК датчиков или закраска их оптической системы. Поэтому надо учитывать также еще два множества [2].

3. Множество $\mathbf{B}^i = [B_1^i, B_2^i, ..., B_M^i]$ из M возможных пассивных способов воздействия нарушителя B_m^j на i-е СО (ПВ) средство обнаружения.

4. Совокупность L активных способов воздействия $\mathbf{A}^i = [A_1^i, A_2^i, ..., A_L^i,]$ на i-е СО (АВ). Обозначим l-е активное воздействие на i-е средство обнаружения как A_l^i .

Будем рассматривать наиболее опасный для СБ случай, когда множества А и В полностью определяют характер изменения контролируемых параметров $\mathbf{O} \subseteq (\mathbf{A} \cup \mathbf{B})$. Также будем учитывать те параметры $\mathbf{E}^j$ окружающей среды, которые совпадают с проявлением j-й угрозы и непосредственно влияют на функционирование средств обнаружения угроз. Т.е. будем рассматривать общий случай, включающий возможности любых воздействий (активных и/или пассивных) на СО, а также разных факторов окружающих условий. Тогда i-е средство обнаружения j-й угрозы будут воспринимать воздействие $\mathbf{S}_j^i \subseteq (\mathbf{A}^i \cap \mathbf{B}^i \cap \mathbf{E}^i)$. Очевидно, что эти воздействия снижают вероятность обнаружения, следовательно, и эффективность системы безопасности в целом. Кроме того, говоря о воздействиях, стоит учитывать такие воздействия, которые оказывают существенное влияние на характеристики и параметры средств обнаружения. Будем называть их эффективными воздействиями $\mathbf{S}_j^{i\,эфф}$ на i-е средство обнаружение j-й угрозы.

Методы повышения эффективности СО

Можно говорить о двух основных группах методов повышения эффективности функционирования общей структуры средств обнаружения угроз объекту обеспечения безопасности.

Первая группа основана на построении правильной структуры СО на объекте (количества, типа, взаимного расположения СО и т.п.). Вопросы, связанные с первым методом, рассмотрены в [2]. Основной принцип заключается в выполнении критерия $\bigcup S_j^{i\,\text{ýôô}} \cap \bigcup S_j^{k\,\text{ýôô}} = \varnothing, \quad \forall\, j,i,k \in J; i \neq k$ несовместности воздействий, применяемых нарушителем к любой паре из J СО. Основные способы реализации этой группы методов базируются на следующих приемах.

1. Сочетание в различных комбинациях отдельных одноканальных устройств обнаружения, расположенных в различных местах объекта обеспечения безопасности.

2. Комбинирование, т.е. совмещение в одном устройстве нескольких обнаружителей с разным принципом действия и различными физическими контролируемыми параметрами с принятием общего решения по единому алгоритму на основе информации от всех обнаружителей. Т.е. использование многоканальных СО угроз.

3. Совмещение в одном корпусе или расположение рядом одноканальных устройств обнаружения, принимающих решения индивидуально.

В любом из перечисленных способов при использовании нескольких СО это соответствует так называемой многорубежной охране.

При правильно сформированной структуре вероятность обнаружения будет определяться количеством K устройств обнаружения (или рубежей) по выражению $P_{\text{îáí}} = 1 - \prod_{k=1}^{K}(1 - P_k)$. Графики на рис. 2 иллюстрируют зависимость вероятности обнаружения на каждом из следующих рубежей при различных значениях вероятности обнаружения одним рубежом и позволяют сделать оценку требуемого количества рубежей и исходной вероятности обнаружения каждым их них.

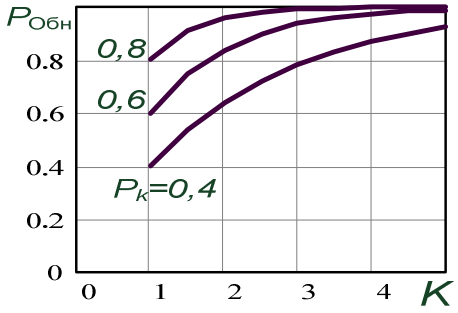

Рис. 2. Зависимость вероятности обнаружения от количества рубежей.

Ясно, что невыполнение (полное или частичное) критерия несовместности воздействий приведет к снижению значения P_k и, как следствие, к уменьшению $P_{\text{îáí}}$ в целом.

Упомянутый выше критерий может использоваться как при синтезе структуры СО, так и для анализа существующих структур.

Вторая группа методов основана на повышения эффективности функционирования самих СО, реализуемых прежде всего правильным выбором контролируемых параметров и применяемыми алгоритмами обработки. Из рис. 2 видна существенная зависимость вероятности $P_{\text{îáí}}$ обнаружения угрозы от значений вероятности P_k обнаружения отдельных СО. Поэтому целесообразно сформулировать основные критерии выбора совокупности параметров $\mathbf{S}_j^i$, контролируемых средствами обнаружения, позволяющие максимизировать этот параметр.

Критерии выбора параметров

Критерии выбора множества $\mathbf{S}_j^{\text{ïîä}\,i}$ физических параметров проявления j-й угрозы, контролируемых средствами обнаружения i-й подсистемы безопасности (ПС), могут быть сформулированы на основе анализа соотношений между множествами различных воздействий, упомянутых выше. Для повышения эффективности СО угроз необходимо выполнение следующих основных критериев.

1. Инвариантность датчиков контроля состояния объекта к воздействию окружающей среды $\mathbf{E}\setminus\mathbf{O}_j$, которые не совпадают с проявлением угроз, т.е. $\mathbf{S}_j^{\text{ïîä}\,j}\cap(\mathbf{E}\setminus\mathbf{O}_j)\to\varnothing$.

2. Минимизация влияния окружающей среды на параметры, являющиеся проявлением угрозы $\mathbf{E}\bigcap\mathbf{O}_j\to\varnothing$. В частном случае $\mathbf{S}_j^{\text{ïîä}\,j}\subseteq(\mathbf{O}_j\setminus\mathbf{E})$. Т.е. исключение из анализа параметров объекта, перекрывающихся с воздействиями среды.

3. Минимум возможного воздействия $\mathbf{E}\bigcap\mathbf{S}_j^{\text{ïîä}\,j}\to\varnothing$, достигаемого выбором СО, инвариантных к различного вида воздействиям.

4. Возможность обнаружения одной угрозы разными ПС безопасности требует выполнения условий $\mathbf{S}_j^{\text{ïîä}\,j}\bigcap\mathbf{O}_i\neq\varnothing$, $\mathbf{S}_i^{\text{ïîä}\,i}\bigcap\mathbf{O}_j\neq\varnothing$, $i,j\in 1,\ldots J$. При выполнении этого критерия такая ПС, кроме основного функционального назначения, сможет решать функции и других подсистем по обнаружению угроз.

5. Различимость проявлений разных угроз требует выполнения условий $\left(\mathbf{S}_j^{\text{ÏÑ}\,j} \cap \mathbf{O}_i\right) \cap \left(\mathbf{S}_j^{\text{ÏÑ}\,j} \cap \mathbf{O}_j\right) = \varnothing$, $\left(\mathbf{S}_j^{\text{ÏÑ}\,j} \cap \mathbf{O}_j\right) \cap \left(\mathbf{S}_i^{\text{ÏÑ}\,i} \cap \mathbf{O}_j\right) = \varnothing$, $i, j \in 1,...J$ использования несовпадающих контролируемых параметров для разных угроз.

6. Критерий $\mathbf{S}_j \to \mathbf{O}_i$ максимальной информативности СО, свидетельствующий о степени полноты использования информации о проявлениях угрозы.

Заключение

1. Для предложенной модели СБ на основе теории множеств в работе проанализированы воздействия, которые определяют выбор состава и структуры СО угроз.

2. Проанализированы основные методы повышения эффективности функционирования общей структуры средств обнаружения угроз объекту обеспечения безопасности.

3. Сформулированы основные критерии выбора контролируемых средствами обнаружения параметров, которые можно использовать при структурном синтезе системы или разработке устройств обнаружения: инвариантности к воздействию окружающей среды; минимизации влияния окружающей среды на параметры, являющиеся проявлением угрозы; минимума возможного воздействия; обнаружения одной угрозы разными подсистемами; различимости проявлений разных угроз и максимальной информативности.

Полученные результаты позволяют сделать обоснованный выбор параметров средств обнаружения и использовать их для оценки эффективности как самих СО, так и общей структуры этих средств на объекте обеспечения безопасности.

Список литературы

1. Волхонский В.В. Системы охранной сигнализации. – 2-е изд., доп. и перераб. – СПб. : Экополис и культура, 2005. – 204 с.

2. Волхонский В.В., Крупнов А.Г. Особенности разработки структуры средств обнаружения угроз охраняемому объекту // Науч.-техн. вестник Санкт-Петерб. гос. ун-та информац. технологий, механики и оптики. – 2011. – № 4 (74). – С. 131–136.

3. Волик Б.Г., Кибзун А.И. Моделирование и анализ безопасности и риска в сложных системах // Автоматика и телемеханика. – 2003. – № 7. – С. 3–4.

4. Карабанов Ю.Ф., Печеркин А.С., Сидоров В.И., Ткаченко В.А. Разработка основных требований к системам управления промышленной безопасностью в организациях, эксплуатирующих опасные производственные объекты // Безопасность труда в промышленности. – 2002. – № 9. – С. 36–37.

5. Мистров Л.Е. Методика синтеза систем информационной безопасности организационно-технических систем // Приборы и системы. Управление, контроль, диагностика. – 2010. – № 10. – С. 4–11.

6. Мистров Л.Е. Модель синтеза систем информационной безопасности организационно-технических систем // Информационная безопасность регионов. – 2011. – № 1. – С. 21–33.

7. Рагимов Э.Р.О. Механизм верификации безопасности программных средств, функционирующих в системе защиты информации корпоративных сетей // Вопросы защиты информации. – 2010. – № 4. – С. 37–40.

8. Шивдяков Л.А., Ступников А.В., Язов Ю.К. Система показателей для оценки состояния обеспечения безопасности информации // Информация и безопасность. – 2010. – Т. 13. – № 2. – С. 251–254.

9. Шивдяков Л.А., Соловьев С.В., Язов Ю.К. Некоторые онтологические аспекты проблемы обеспечения безопасности информации в критически важных системах информационной инфраструктуры // Информация и безопасность. – 2010. – Т. 13. – № 3. – С. 411–414.

10. Шипилов А.В., Смуров С.В., Мёдов И.Н. Подходы к анализу угроз безопасности информации, циркулирующей в автоматизированных системах // Информационно-измерительные и управляющие системы. – 2009. – Т. 7. – № 2. – С. 77–81.

Рецензенты:

Зарубин В.С., д.т.н., доцент, начальник кафедры технических систем безопасности Воронежского института МВД России, г. Воронеж.

Веселов А.В., д.т.н., ведущий специалист, представительство ЗАО «Ханивелл Секьюрити Нидерланд Б.В.», г. Санкт-Петербург.