УДК 655.3

МЕТОДИКА КОМПЛЕКСНОЙ ОЦЕНКИ НАДЕЖНОСТИ СИСТЕМЫ ОГРАНИЧЕНИЯ ДОСТУПА

О.В. МЕЛЕХ, В.В. ТКАЧЕНКО

Объединенный институт проблем информатики НАН Беларуси
Сурганова, 6, Минск, 220012, Беларусь

Поступила в редакцию 11 ноября 2008

Предложена методика комплексной оценки надежности системы ограничения доступа на основе обобщенного критерия, связывающего частные эксплуатационные и качественные показатели системы, которая позволяет упростить процесс сравнительного анализа вариантов системы ограничения доступа и выбора из них рационального для практической реализации с учетом условий применения системы и оперативной обстановки в конкретных ситуациях. Приведен расчет комплексного показателя надежности на определенном рубеже охраны активным ИК-датчиком "Световой барьер ограничения доступа".

Ключевые слова: методика комплексной оценки надежности, комплексный показатель надежности, система ограничения доступа, вероятность пропуска, вероятность ложных тревог, активный ИК-датчик.

Введение

Вопрос надежности аппаратуры настолько же важен, насколько сложен и неоднозначен. Особое значение этот вопрос приобретает в отношении систем ограничения доступа.

Актуальность вопроса обусловлена, с одной стороны, увеличением угроз различным объектам, с другой — расширением рынка систем контроля доступа и ростом конкуренции. В таких условиях потребителю иногда бывает сложно сделать вывод относительно того, какой проект системы ограничения доступа предпочтительнее.

Для расчета надежности любой системы ограничения доступа необходимо учитывать надежность совместной работы всех устройств, используемых в составе системы. В таком случае разработчики и пользователи могут правильно оценить риски, связанные с использованием той или иной системы контроля доступа и сделать выбор с учетом конкретных условий использования.

Теоретический анализ

На практике при оценке рисков принято различать следующие показатели технических систем: качественные, эксплуатационные и физические [1]. Показатели качества определяются в количественных единицах. Эксплуатационные показатели определяют первоначальную стоимость оборудования и стоимость его эксплуатации, удобство работы с этим оборудованием, ремонтоспособность и пр. Физические показатели характеризуют средства, которыми достигнут необходимый результат. Большинство этих показателей взаимосвязано и изменяется в зависимости от изменения одного из них. Надежность, как правило, относят к показателям качественным, однако она тесно взаимосвязана и с эксплуатационными показателями.

Предлагаемая методика комплексной оценки надежности системы ограничения доступа построена на расчете комплексного показателя надежности [2], который одновременно дает представление о двух и более свойствах, определяющих качество технической системы. В большинстве случаев комплексный показатель (обозначим его K) определяется математическим выражением на основе единичных показателей, например:

$$K = \sum_{i=1}^{m} a_i k_i \qquad (1)$$

где m — число единичных показателей, принятых во внимание; a_i — коэффициент, показывающий вес (важность, значимость) i-го единичного показателя для данного вида радиоэлектронного устройства; k_i — значение единичного показателя качества.

Для того, чтобы воспользоваться (1), значения k_i должны быть представлены в нормированном безразмерном исчислении. На практике распространена нормировка, при которой диапазон реальных значений k_i определяется на отрезке (0…1). Причем ноль соответствует лучшему случаю, а единица — худшему с точки зрения функционирования и потребительских свойств радиоэлектронного устройства.

Методика

В случае охраны периметра предлагается считать важнейшими единичными показателями надежности вероятность пропуска нарушителя на охраняемый объект и вероятность ложных срабатываний датчика обнаружения. Причем в каждом отдельном случае в зависимости от условий применения отдельной системы контроля доступа важность (значимость) этих показателей предлагается определять потребителю.

Методика комплексной оценки надежности системы ограничения доступа позволяет упростить процесс сравнительного анализа вариантов системы ограничения доступа и выбора из них рационального для практической реализации с учетом условий применения системы и оперативной обстановки в конкретных ситуациях, когда экономические затраты, являющиеся следствиями пропуска объекта и ложного срабатывания, относятся как $a_{\text{пр}}/P_{\text{лс}}$:

$$K = a_{\text{пр}} P_{\text{пр}} + a_{\text{лс}} P_{\text{лс}}. \qquad (2)$$

Применяемые для систем охраны периметра датчики должны иметь вероятность пропуска ($P_{\text{пр}}$) на охраняемый объект равную 0, однако на практике таких датчиков не существует. Вероятность пропуска — понятие комплексное, и в каждом отдельном случае зависит от ряда факторов. Это могут быть условия установки датчика, характеристики объекта обнаружения, принцип работы датчика, техническое состояние аппаратуры, погодные условия и многое другое. Эти факторы могут варьироваться, поэтому значение $P_{\text{пр}}$ для конкретного датчика не является постоянной величиной и зависит от условий его работы. Кроме того, необходимо знать методику оценки $P_{\text{пр}}$. Модель обнаружения можно описать двумя параметрами: вероятностью обнаружения и уровнем подготовки нарушителя. Выражение для расчета вероятности пропуска нарушителя датчиком обнаружения имеет вид:

$$P_{\text{пр}} = P_{\text{п}}(1-m) + P_{\text{к}}(m), \qquad (3)$$

где m — доля квалифицированных нарушителей, посягающих на охраняемый объект; $(1–m)$ — доля подготовленных нарушителей, посягающих на охраняемый объект; $P_{\text{к}}$ — вероятность обхода датчика квалифицированным нарушителем; $P_{\text{п}}$ — вероятность пропуска подготовленного нарушителя датчиком обнаружения с учетом возможности выхода датчика из строя из-за внезапного отказа:

$$P_{\text{п}} = 1 - P_{\text{об}} P_{\text{б}}, \qquad (4)$$

где $P_{\text{об}}$ — вероятность обнаружения работоспособного датчика, указанная в его технических условиях; $P_{\text{б}}$ — вероятность безотказной работы датчика.

Для идеального датчика вероятность обнаружения $P_{об}$ равна 1 — на сто пересечений линии периметра должно быть сто сигналов тревоги. Однако на практике таких датчиков не существует, поэтому $P_{об}$ всегда меньше 1.

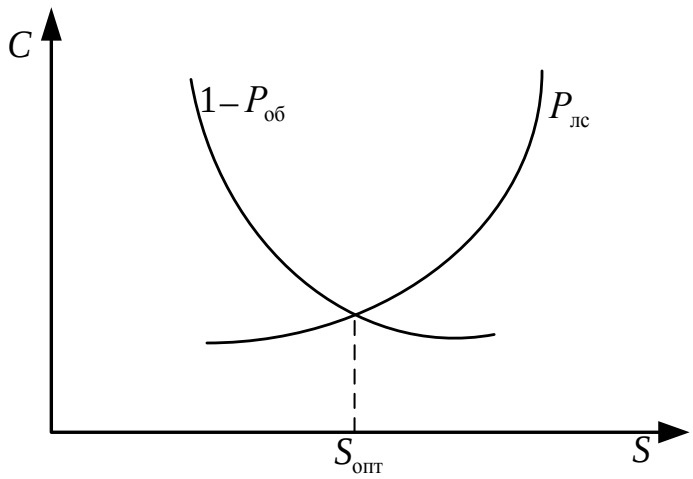
Вероятность безотказной работы датчика определяется по формуле:

$$P_{б} = \exp(-T_{к} / T_{о}), \quad (5)$$

где $T_{к}$ — период контроля работоспособности датчика обнаружения, указанный в его технических условиях; $T_{о}$ — среднее время наработки на отказ датчика обнаружения, указанное в его технических условиях.

Идеальный датчик невозможно преодолеть незамеченным, чего нельзя сказать о реальных приборах. Различные модели датчиков имеют разную уязвимость. Существует два основных способа преодолеть систему — обход и обман. Поскольку все датчики имеют ограниченную зону обнаружения, любой датчик можно преодолеть, обойдя эту зону. Данная проблема решается совершенствованием различных инженерных заграждений. Кроме того, зная физические принципы работы датчика, можно разработать методы пересечения его зоны обнаружения, например, снижение видимого контраста нарушителя или снижение скорости его движения.

Вероятность обнаружения повышается с уменьшением порога срабатывания датчика (повышением его чувствительности), однако при этом возрастает вероятность ложного срабатывания ($P_{лс}$). Эта ситуация показана на рисунке.



Взаимосвязь вероятности обнаружения ($P_{об}$) и вероятности ложных срабатываний $P_{лс}$

Вероятность ложных срабатываний также можно определить как число ложных срабатываний датчика, отнесенное к числу его опросов (если оно достаточно велико).

Сложность расчета среднего времени наработки на ложное срабатывание состоит в том, что испытания датчиков обнаружения на помехоустойчивость в полигонных условиях проводятся изготовителем в условиях помеховой обстановки, которая характерна для данного полигона. В то время как в процессе эксплуатации датчика на реальном объекте интенсивность помеховой обстановки может быть существенно выше.

Согласно [3] при использовании пуассоновской модели потока ложных срабатываний вероятность хотя бы одного ложного срабатывания за время наблюдения T определяется по формуле:

$$P_{лс} = 1 - \exp(-TK_{лс} / T_{лс}), \quad (6)$$

где $T_{лс}$ — среднее время наработки на ложные срабатывания датчика, указанного в его технических условиях; $K_{лс}$ — коэффициент интенсивности помеховой обстановки на охраняемом объекте, определяемый соотношением

$$K_{лс} = N_о / N_п), \quad (7)$$

где $N_о$ — количество ложных срабатываний датчика в год на охраняемом объекте; $N_п$ — количество ложных срабатываний датчика в год на полигоне.

Коэффициент интенсивности помеховой обстановки на охраняемом объекте показывает, во сколько раз количество ложных срабатываний датчика на объекте будет больше, чем количество ложных срабатываний этого датчика на полигоне.

Рассмотренные характеристики связаны между собой таким параметром, как чувствительность датчика. Чувствительность — величина, обратная порогу. Порог — некое значение, ниже которого сигналы интерпретируются как шумы. Порог регулируется во время настройки датчика. Чем больше чувствительность, тем меньше вероятность пропуска.

Экспериментальная часть

Для примера рассчитаем вероятность пропуска нарушителя на определенном рубеже охраны активным ИК-датчиком "Световой барьер" (СБ), который представляет собой однолучевой аварийный датчик безопасности, предназначенный для контроля доступа на объекты. Принцип действия СБ основан на импульсной частотной модуляции инфракрасного излучения (ИК-излучения). СБ состоит из передатчика ИК-излучения, приемника ИК-излучения и электронного блока управления с исполнительным реле, контакты которого могут быть настроены на замыкание или на размыкание [4].

В нашем случае система должна иметь $P_{об}$=0,95 для человека массой 70 кг, пересекающего зону обнаружения пешком, ползком, прыжками, бегом или перекатывающегося при скорости 0,1–5 м/с при частоте ложных тревог не более двух в сутки. Из указаний в технических условиях период контроля работоспособности датчика принимается равным $T_к$=24 ч, а среднее время наработки на отказ датчика обнаружения, указанное в его технических условиях, составляет $T_о$=60000 ч [5].

Таким образом, для расчета вероятности безотказной работы ИК-датчика используем (5) и получаем:

$P_б$=exp(–24/60000)=0,9996.

Тогда вероятность пропуска подготовленного нарушителя активным ИК-датчиком обнаружения определенного рубежа охраны с учетом возможности выхода датчика из строя из-за внезапного отказа (4):

$P_п$=1–0,95·0,9996=0,05.

Для важного объекта доля квалифицированных нарушителей, посягающих на охраняемый объект, составляет m=0,1, вероятность обхода датчика квалифицированным нарушителем принимаем равной $P_к$=0,5 [3].

Тогда выражение для вероятности пропуска нарушителя активным ИК-датчиком обнаружения, установленным на определенном рубеже охраны объекта, примет вид (2):

$P_{пр}$=0,05 (1–0,1)+0,5 (0,1)=0,095.

Следовательно, при применении активного ИК-датчика на определенном рубеже охраны вероятность пропуска этим датчиком нарушителя равняется 0,095. Для повышения надежности обнаружения нарушителя обычно наращивают количество рубежей защиты с несколькими датчиками, установленными на одном участке периметра территории объекта.

В нашем случае при использовании активного ИК-датчика вероятность ложных срабатываний $P_{лс}$=0,85, что объясняется высокой чувствительностью датчика обнаружения.

Вероятность пропуска является основной характеристикой, позволяющей судить о достоверности, следовательно, при расчете комплексного показателя надежности коэффициенты значимости (важности) расставляются следующим образом.

Для вероятности пропуска $P_{пр}$ коэффициент, показывающий вес (важность, значимость) равен 1, $\alpha_{пр}$=1, а коэффициент, показывающий вес (важность, значимость) вероятности ложных

срабатываний $P_{лс}$ равен 0, $\alpha_{лс}$=0. Следовательно, в нашем случае комплексный показатель надежности равен вероятности пропуска:

K=0,095.

С точки зрения функционирования и потребительских свойств охранного ИК-датчика нуль соответствует лучшему случаю, а единица — худшему. Поэтому в нашем случае комплексный показатель надежности K стремится к нулю.

Заключение

Описанный в статье подход к определению надежности систем контроля доступа имеет свои преимущества. В результате его применения устанавливается функциональная связь качественных и эксплуатационных показателей с физическими показателями, такими как внутренние шумы и внешние помехи. Поэтому эта проблема продолжает оставаться актуальной и ведущим направлением в ее решении становится совершенствование методик определения показателей качества охранных систем с учетом всех возможных внешних факторов.

TECHNIQUE OF A COMPLEX ESTIMATION OF RELIABILITY OF ACCESS RESTRICTION SYSTEM

O.V. MELEKH, V.V. TKACHENKO

Abstract

The technique of a complex estimation of reliability of system of restriction of access on the basis of the generalized criterion connecting private operational and quality indicators of system which allows to simplify process of the comparative analysis of variants of system of restriction of access and a choice of them rational for practical realization taking into account conditions of application of system and operative conditions in concrete situations is offered. The calculation of a complex indicator of reliability on a certain boundary of protection by the active IR-gauge "Light barrier of restriction of access" is given.

Литература

1. *Арутюнов М.Г., Маркович В.Д.* Скоростной ввод-вывод информации. М., 1970.
2. *Боровиков С.М.* Метод. пособ. по учеб. дисциплинам "Теоретические основы конструирования, технологии и надежности" и "Инженерное обеспечение надежности РЭС". Минск, 2003.
3. *Шепитько Г.Е.* Проблемы охранной безопасности объектов / Под ред. проф. В.А. Минаева. М., 1995.
4. *Мелех О.В.* // Материалы 5-й Белоруско-российской науч.-техн. конф. "Технические средства защиты информации". 30 мая 2007 г. Минск, 2007.
5. IEC 60839-2-3:1987 Active infrared detectors. General technical requirements and test methods.