УДК 681.3.07

Н.С. КОВАЛЕНКО

Бердянский государственный педагогический университет, Украина

ВЫБОР ВАРИАНТОВ АНАЛИЗА И ОЦЕНКИ ЖИВУЧЕСТИ И НАДЕЖНОСТИ ИНТЕГРИРОВАНЫХ СИСТЕМ БЕЗОПАСНОСТИ ОБЪЕКТОВ СО СЛОЖНОЙ ИНФРАСТРУКТУРОЙ

Рассмотрены показатели эффективности систем безопасности объектов. Приводятся варианты анализа и оценки интегрированных систем объектовой безопасности (ИСОБ). Количественный и качественный анализ защиты критических и бизнес-критических объектов.

вероятность обнаружения событий, частота ложных тревог, условный риск, зона контроля

Введение

Постановка задачи анализа и оценки эффективности систем безопасности объектов. В настоящее время достаточно актуальными становятся проблемы обеспечения безопасности объектов государственной а также других форм собственности. К данной категории объектов можно отнести электростанции, авиационные, морские и речные порты, автомобильные, железнодорожные терминалы, площадки для хранения, переработки, транспортировки продукции и грузов и др.

Перечисленные выше объекты, требующие комплексных мер безопасности, характеризуются, как правило, неоднородным рельефом со сложным геометрическим периметром, разветвленными инфраструктурами. Для современного подхода к решению этой проблемы необходимо эффективное использование технических средств в системах безопасности. Такие системы объединяют современные средства видеонаблюдения, автоматической регистрации, контроля и реакции на события с учетом индивидуальных особенностей объектов [1 – 4].

Принцип проектирования вышеуказанных систем на основе зонально-модульной архитектуры позволяет проанализировать роботу и дать оценку каждому из звеньев интегрированных систем объектовой безопасности (ИСОБ) в отдельности [1, 3].

Под интегрированными системами объектовой безопасности понимается совокупность взаимосвязанных и обладающих технической, программной, информационной и эксплуатационной совместимостью подсистем [3]: датчики видеомониторинга, охранно-пожарной сигнализации и др; контроль и управление доступом; обработка информации об охраняемом объекте; управление зонами контроля;

При постановке и реализации задач по обеспечению эффективной работы систем безопасности объектов следует учитывать множество факторов и показателей, влияющих на их живучесть и гарантоспособность: оптимальное использование аппаратных и программных ресурсов, возможность расширения системы, ее модернизации, монтажа, пусконаладочных работ в условиях уже действующей системы, техобслуживание, ремонт и др; работа в жестких климатических условиях при многолетней бесперебойной эксплуатации с минимальными отказами; исключение несанкционированного доступа к системным ресурсам и физических воздействий, приводящих к потере информации и отказу технических средств; реакция всей системы, скорость передачи, обработки и оперативного контроля в режиме реального времени а также возможность быстрого анализа архивной информации; оптимальное сочетание стоимости оборудования, технических и организационных работ с достаточностью вышеперечисленных показателей.

Цель данной работы – выбор показателей для анализа и оценки интегрированных систем объектовой безопасности.

Выбор показателей эффективности систем безопасности объектов

Для проведения анализа и оценки живучести и надежности вышеуказанных систем предлагается учитывать следующие показатели, существенно влияющие на эффективность работы отдельных составляющих так и на весь комплекс в целом [1, 2].

Вероятность обнаружения событий (ВОС*)* – Рс для идеальной ИСОБ равна единице Рс=1,0, но реально таких систем не существует, поэтому следует применять доверительный уровень ВОС – Сс, который для реальной ВОС всегда меньше единицы Сс<1,0. При проектировании выбирается величина Сс=0,9-0,99 [2]. ВОС зависит от следующих факторов: объекта, события, которые необходимо обнаружить (статический, динамический характер события и др.); настройки датчиков по факторам инфраструктуры охраняемого объекта; климатических, погодных условий; технического состояния ИСОБ. Эти факторы варьируются, поэтому величина ВОС – условная, основанная на задании режимов работы конкретной зоны контроля ИСОБ.

Частота ложных тревог (ЧЛТ) – число ложных срабатываний, не вызванное событиями, вторжением и др., в течение заданного промежутка времени, для идеальных систем равна нулю. На практике все системы, взаимодействуют с окружающей средой и не “могут” отличить вторжение или события от других явлений в зонах контроля. Поэтому для установления причины сигнала из зоны контроля и необходимости реакции нужна оценка событий от всей ИСОБ. Существенное значение имеет применение видеоконтроля, который визуально позволяет воспроизвести события как в режиме реального времени, так и с последующим востребованием.

Уязвимость по отношению к преодолению (УП). Определяется формированием зон контроля, а также прогнозируемым переходом по объекту из зоны в зону, которые имеют различную уязвимость. Существует два основных способа преодоления систем охраны: обход системы датчиковых средств, имеющих ограниченную зону контроля, обнаружения; обман (субъективный фактор, пересечение зоны контроля, не вызывая сигнала тревоги).

Ценовой показатель (ЦП). С – стоимость проектирования, эксплуатации и другие затраты на ИСОБ [4]. Исходя из этого, могут быть сформулированы два оптимизационных варианта анализа интегрированной системы объектовой безопасности: обеспечение требуемой эффективности ИСОБ при минимизации стоимостных затрат; достижение максимальной эффективности ИСОБ при заданной стоимости.

Условный риск (УР) – готовность объекта принять определенную величину риска в заданный период времени или понести затраты на уменьшение этого риска. При наличии ограниченных ресурсов, предназначенных для проектирования и построения ИСОБ применение этих ресурсов должно быть тщательно обосновано для каждой зоны контроля чтобы сбалансировать показатели вероятности обнаружения событий, частоту ложных тревог и другие параметры эффективности системы.

Подход к анализу и оценке надежности и живучести систем безопасности объектов

При постановке задач для ИСОБ и усовершенствовании ее в процессе эксплуатации возникает необходимость анализа эффективности, с которой ИСОБ решает эти задачи. Имеется ряд причин для оценки существующей или проектируемой системы защиты [1, 2]: износ или моральное старение элементов системы; появление на объекте новых процессов, функций, ценностей и др.; увеличение условного риска. Такой анализ может быть качественным и количественным.

Количественный анализ необходимо проводить на объектах, потеря работоспособности или имущества которого недопустима при минимальном условном риске. Это характерно для критических систем. В каждом из этих случаев потеря работоспособности или повреждение даже части объекта по причине ИСОБ повлекла бы тяжелые последствия.

При организации ИСОБ таких объектов необходимо использовать вариант:

$$ВОС \to \max;$$

$$ЧЛТ \le ЧЛТ_{треб.}; УП \le УП_{треб.}; C \le C_{доп.}$$

Количественному анализу подвергаются системы с высоким уровнем защиты и для его проведения требуются показатели эффективности отдельных зон контроля и элементов системы.

Качественный анализ удобнее применять для систем с низким уровнем защиты. Такие системы охраняют объекты меньшей значимости (стоимости) чем критические и бизнес-критические, потеря или повреждение которых может иметь минимальный риск. В случае ограниченных ресурсов ИСОБ должна обеспечить максимальную защиту намеченных (бизнес-критических) объектов, а оставшиеся ресурсы системы направить на обеспечение безопасности менее значимого объекта т.е. с минимальным риском и использовать вариант:

$$C \to \min;$$

$$ВОС \geq ВОС_{треб.}; ЧЛТ \leq ЧЛТ_{треб.}; УП \leq УП_{треб.}$$

Независимо от выбранного метода анализа – качественного или количественного, правильное использование выбранных показателей оценки системы обеспечит ее наиболее полный и достоверный результат.

В большинстве случаев несанкционированные события на охраняемом объекте спровоцированы человеческим фактором (нарушителем). Поэтому в качестве инструментального средства оценки эффективности систем охраны объектов предлагается использовать **диаграммы последовательности действий нарушителя (ДПД).** ДПД представляет собой метод графического представления стратегий, которые нарушитель может выбрать для осуществления своей цели, или моделирование последовательности действий нарушителя для оценки вероятности достижения нарушителем его цели с учетом возможных стратегий (или набора стратегий).

Для оценки насколько эффективно ИСОБ защищает охраняемый объект, необходимо определить риск, который остается после ее реализации для этого применимо уравнение риска [1]:

$$R = Pt\,(1 - Pi)\,C, \qquad (1)$$

где R – риск для объекта при условии несанкционированных действий (вторжения), диапазон возможных значений от 0 до 1.0, причем R = 0 – полное отсутствие риска, а R = 1,0 – максимальный риск. Риск оценивается вероятностью несанкционированных действий за определенный период времени t – P_t. Эта величина определяется при помощи экспертных оценок на основе обработки данных от ДПД и равна 0 при отсутствии вторжений, а 1 – если вторжение не подлежит сомнению.

В целом процесс оценки риска может служить в качестве метода определения компоненты риска – Pi, который в зависимости от допустимого условного риска позволит принять решение по улучшению параметров проекта или модернизации существующей системы с целью уменьшения ее уязвимости, повышению надежности и гарантоспособности.

Заключение

Для создания и эксплуатации интегрированных систем безопасности объектов, построенных на сочетании перспективных промышленных устройств и современных информационных технологий, требуется сбалансированный подход к выбору показателей анализа и оценки эффективности всей системы и отдельных ее элементов, который позволит повысить безопасность охраняемых объектов.

Литература

1. Гарсиа М. Проектирование и оценка систем физической защиты. – М.: Мир, 2003. – 386 с.

2. Коваленко Н.С. Анализ нижних звеньев интегрированных систем объектовой безопасности // Збірник наукових праць ХУ ПС. – Х.: ХУ ПС, 2006. – Вип.1 (13). – С. 60-62.

3. Бохан К.А., Коваленко Н.С., Киященко Ю.В. Анализ и разработка архитектуры интегрированных систем безопасности объектов со сложной инфраструктурой // Радіоелектронні і комп'ютерні системи. – 2006. – № 7. – С. 115-120.

4. Комари И.Э., Горбенко А.В. Анализ задач разработки и реинжиниринга компьютерных сетей для критических приложений // Радіоелектронні і комп'ютерні системи. – 2006. – № 7. – С. 32-35.

Поступила в редакцию 12.03.2007

Рецензент: д-р техн. наук, проф. В.С. Харченко, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Харьков.