Эти локальные поверхности перекрываются на границах, т. е.

$$\Pi_{UT}^{k} \bigcap \Pi_{UT}^{k+1} = \Pi_{UT}^{k,k+1} \neq 0 .$$

Такое перекрытие границ снимает неопределенность при принятии решения о принадлежности сигналов каналов давления (U_{Pj}) и температуры (U_{Tj}) к той или другой области, если значения этих сигналов формально принадлежат границе этих областей $U_{Pj}, U_{Tj} \in \Pi_{UT}^{k,k+1}$.

Построенная таким образом система локальных пространственных элементов является аппроксимацией экспериментальной пространственной градуировочной характеристики интеллектуального датчика.

В качестве моделей элементарных аппроксимирующих элементов можно использовать модель элементарной аппроксимирующей плоскости или модель элементарной аппроксимирующей поверхности в виде полинома [2, 3, 4].

Коэффициенты аппроксимации элементарных аппроксимирующих элементов ММГХ определяются стандартным способом с помощью метода наименьших квадратов.

Как показало моделирование [3, 4], основанное на результатах испытаний первичных преобразователей давления, при высоких точностных характеристиках ПП, использование мультисегментной модели пространственных градуировочных характеристик в интеллектуальном датчике давления может обеспечить прецизионную точность измерения значений давления в широком диапазоне изменения давлений и температур.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Клевцов С.И., Пьявченко О.Н., Удод Е.В.* Метод мультисегментной аппроксимации градуировочной характеристики для прецизионных вычислений давления в интеллектуальных датчиках //Проблемы разработки перспективных микро- и наноэлектронных систем –2008. Сборник научных трудов /Под общ. ред. А.Л. Стемпковского. – М.: ИППМ РАН, 2008. – С.384-390.
2. *Клевцов С.И.* Пространственно-полиномиальные модели аппроксимации градуировочной характеристики интеллектуального датчика // Труды Международных научно-технических конференций "Интеллектуальные системы" и "Интеллектуальные САПР". Научные издания в 3-х томах. –М.: Изд-во физико-математической литературы, 2004. Т.2. –468с. –С.309-314.
3. *Клевцов С.И., Клевцова А.Б.* Мультисегментная пространственная модель градуировочной характеристики интеллектуального датчика //Материалы международной научной конференции "Цифровые методы и технологии". Ч.4. –Таганрог: Изд-во "Антон", ТРТУ, 2005. – С.21-26.
4. *Клевцов С.И., Удод Е.В.* Пространственная плоскостная модель градуировочной характеристики интеллектуального датчика давления // Известия ТРТУ. 2005. –№1. – С.99-107.

УДК 681.3.01

Д.Ю. Гужва

МОДЕЛЬ УГРОЗ ИНФОТЕЛЕКОММУНИКАЦИОННОЙ СИСТЕМЕ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Обеспечение безопасности информационных ресурсов является одной из основных составляющих проектных решений при разработке современных инфотелекоммуникационных систем специального назначения (ИТКС ВН) и их систем защиты. Адекватная настройка систем защиты информации зависит от уровня подготовки администраторов безопасности ИТКС ВН, которые должны хорошо

знать архитектуру современного общего и прикладного программного обеспечения, технологии построения локальных и глобальных вычислительных сетей, возможности по защите информации телекоммуникационных систем и СУБД, современные технологии и средства защиты информации в вычислительных сетях.

Современным компьютерным атакам может успешно противостоять только система с возможностями, в несколько раз превосходящими возможности нападающего. Это определяется так называемым законом зависимости эффективности защиты информации в ИТКС ВН от объема и важности обрабатываемой информации, а также от возможностей злоумышленника.

Так как принятие решения на адекватное применение средств защиты затрудняется, с одной стороны, высокой динамичностью противостоящих сторон, а с другой – появлением все большего числа новых способов компьютерных атак, возникает необходимость определения перечня угроз информационной безопасности и разработки их модели.

Перечень и классификация наиболее вероятных угроз определены в Доктрине информационной безопасности РФ и руководящих документах ФСТЭК [1]. Основными классами угроз являются: угрозы информационной безопасности телекоммуникационных средств и систем; угрозы систем передачи данных; угрозы национальной безопасности РФ в информационной сфере; угрозы информационной безопасности в сфере обороны.

Угрозы информационной безопасности реализуются на основе единого алгоритма атаки, который в общем случае разделяется на пять этапов [2, 3, 4]. На первом этапе злоумышленник проводит разведку вычислительной сети, ее исследование. При этом осуществляются попытки непосредственного проникновения на объект, просмотр доступных *Web*-страниц, баз данных *WhoIs*. В результате противнику будет известны номера телефонов, *IP*-адреса и другая общедоступная информация.

Следующим этапом будет попытка обнаружения модема, подключенного в обход периметровой системы защиты. Если такой модем будет обнаружен, последует попытка проникновения через него в сеть. При невозможности такого, достаточно легкого, способа проникновения в сеть будет применен другой способ – сетевое сканирование. Целью сканирования является поиск активных хостов, трассировка маршрутов и отдельных узлов, активных портов. После данного этапа злоумышленнику становится известной структура всей исследуемой сети, и он приступает к реализации третьего этапа – созданию сценария атаки. Какой будет атака, зависит от классификации злоумышленника и его конечной цели.

Непосредственное проведение атаки является четвертым этапом. Последним этапом действий злоумышленника будет являться уничтожение следов своей деятельности.

Модель угроз ИТКС ВН целесообразно строить по блочному принципу. Каждый блок модели должен соответствовать *i*-му состоянию угрозы. Данная модель представлена на рисунке 1, на котором приведены следующие состояния: $S0$ – исследование сети; $S1$ – проведение внутренней атаки; $S2$ – проведение внешней атаки через модем; $S3$ –проникновение в демилитаризованную зону сети через межсетевой экран (внешняя атака); $S4$ – проникновение во внутреннюю сеть; $S5$ – обман *IDS*; $S6$ – получение доступа злоумышленника к приложениям ОС; $S7$ – взлом системы защиты; $S8$ – получение доступа к информации; $S9$ – поддержка доступа; $S10$ – скрытие атаки.

Все состояния разделяются на три подмножества: $V1$ – подготовка атаки; $V2$ – реализация атаки; $V3$ – завершение атаки.

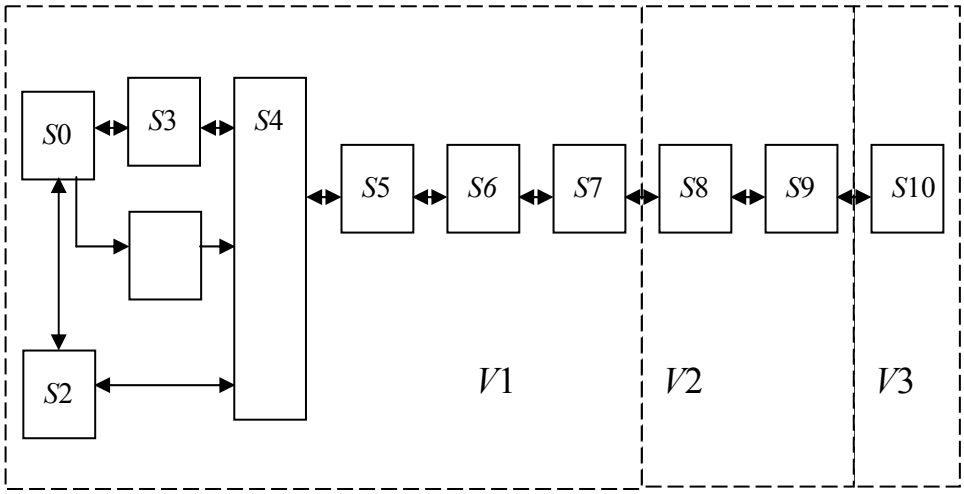

Рис.1. Модель угроз ИТКС ВНугр

Начальным состоянием является $S0$. Конечным состоянием всегда будет $S10$, так как нарушитель всегда постарается оставить для себя способ повторного вхождения в сеть. Следует отметить, что угроза вида «отказ в обслуживании» в модели рассматривается как крайняя мера, причем ей предшествуют этапы, в модели полностью описываемые.

Внешними воздействующими факторами являются: наличие у злоумышленников достаточно хороших сканеров сетей, его профессиональная подготовленность, осведомленность о структуре сети и системы защиты информации.

Основными рассчитываемыми параметрами модели угроз являются вероятности воздействия системы угроз на систему защиты информации вычислительных сетей военного назначения и вероятность вскрытия системы защиты информации.

В качестве аппарата для построения математической модели угроз, к которой осуществим переход от описательной блочной модели, выберем аппарат марковских цепей.

Основной задачей марковской цепи является нахождение безусловной вероятности пребывания системы угроз в состоянии S_i [5]. Возможные состояния системы угроз известны, они принадлежат конечному множеству. Переход системы из состояния в состояние считается мгновенным. Следовательно, модель угроз разрабатывается как марковский процесс с дискретным состоянием. Положим, что система угроз последовательно переходит от события к событию, причем для любого момента времени t_0 вероятность каждого из событий в будущем зависит только от ее состояния в настоящем и не зависит от того, когда и как она пришла в это состояние. Обозначим вероятность нахождения системы в состоянии s_i в момент времени t через $P_i(t)$:

$$P_i(t) = P\{S(t) = s_i\} \quad , \tag{1}$$

где $S(t)$ – случайное состояние системы S в момент t.

Очевидно, что для системы угроз с дискретным состоянием в любой момент сумма вероятностей равна единице:

$$\sum P_i(t) = 1 \cdot \quad (2)$$

Определим переходную вероятность следующим образом:

$$P_{ij} = P\{S(k) = s_j \mid S(k-1) = s_i\} \qquad (i, j = 1, 2, \ldots, n). \quad (3)$$

Найдем начальное состояние системы $p_i(0)$, причем вероятности составляющих начальное состояние системы угрозы в сумме будут составлять единицу:

$$\sum_{i=1}^{n} p_i(0) = 1 \ . \quad (4)$$

При нахождении вероятностей угроз на *k*-м шаге воспользуемся размеченным графом, представленным на рис. 2.

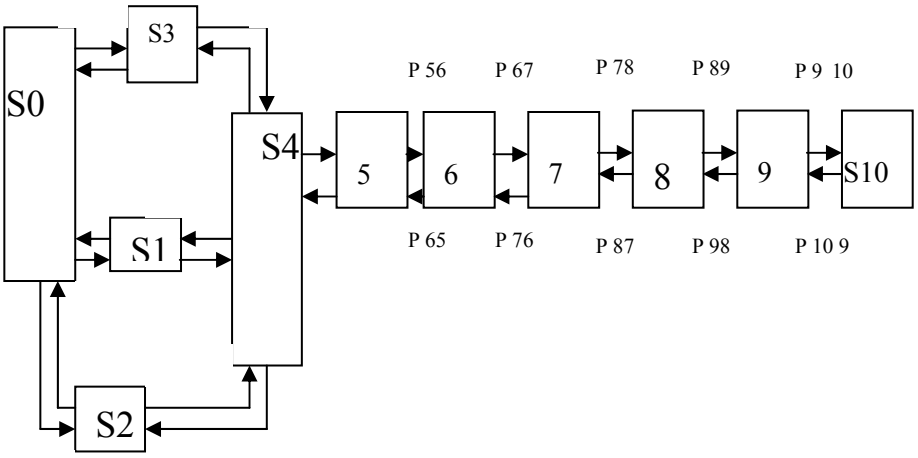

Рис.2. Марковская модель угроз ИТКС ВН

По формуле полной вероятности получим

$$P_i(1) = \sum_{i=1}^{n} P\{S(1) = s_i \mid S(0) = s_i\} P\{S(0) = s_i\} = \sum_{i=1}^{n} p_{ij} p_i(0)$$

$$(j = 1, 2, \ldots, n) \quad (5)$$

Таким образом, получено распределение вероятностей системы угроз на первом шаге. На втором шаге система угроз будет в состоянии s_j , для которого справедливо:

$$p_j = P\{S(2) = s_j \mid S(1) = s_i\} \quad . \quad (6)$$

По формуле полной вероятности находим

$$p_j(2) = \sum_{i=1}^{n} p_i(1) p_{ij} \qquad (j = 1, 2, \ldots, n). \quad (7)$$

Переходя таким же способом от $k = 2$ к $k = 3$ и т.д., получим рекуррентную формулу

$$p_j(k) = \sum_{i=1}^{n} p_i(k-1) p_{ij} \qquad (k = 1, 2, \ldots; j = 1, 2\ldots, n). \quad (8)$$

Полученные с помощью (5–8) безусловные вероятности нахождения системы угроз на любом (*k*-м) шаге состояния способствуют построению в ИТКС ВН достаточно адекватной и высокоэффективной системы защиты информации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Документы ФСТЭК РФ. «Информационная безопасность и защита информации». Сборник терминов и определений.
2. *Лукацкий А.В.* Обнаружение атак. – СПб.: БХВ-Петербург, 2001.
3. *Норткатт С., Новак Д.* Обнаружение вторжений в сеть. –М.: Изд-во «ЛОРИ», 2001.
4. *Скудис Э.* Противостояние хакерам. Полное руководство по компьютерным атакам и эффективной защите: Пер. с англ. – М.: ДМК Пресс, 2003. – 502 с.
5. *Венцель Е.С., Овчаров Л.А.* Теория случайных процессов и ее инженерные приложения. – М.: Наука. 1991.

УДК 621.33

А.Б. Клевцова, Г.С. Клевцов

МОДЕЛИ ПАРАМЕТРИЧЕСКОЙ ЭКСПРЕСС-ОЦЕНКИ СОСТОЯНИЯ ТЕХНИЧЕСКОГО ОБЪЕКТА

Оценка состояния сложного технического объекта является одной из важных задач мониторинга. Эта задача базируется на изучении поведения технического объекта, математические модели которого в общем случае описываются интегро-дифференциальными уравнениями [1]. Для предварительной оценки состояния предпочтительнее использование упрощенных моделей технического объекта, построенных на основе приближенных функциональных зависимостей между переменными объекта. Часто экспресс-оценка является достаточной для прогнозирования и предотвращения нештатных и аварийных ситуаций. Дополнительным преимуществом такого подхода служит возможность осуществления оценки на нижних уровнях распределенной микрокомпьютерной системы мониторинга, где выполнение сложных вычислений в реальном масштабе времени затруднительно или нереализуемо.

В настоящей статье рассматриваются особенности различных моделей параметрической экспресс-оценки состояния технического объекта.

Модель рейтинговой оценки строится на основе структурной декомпозиции объекта на составляющие компоненты [2]. Набор компонентов определяется в результате декомпозиции объекта на значимые функционально законченные единицы. Для каждого компонента назначается ряд критериев, позволяющих полностью охарактеризовать данный компонент. Общая совокупность критериев всех компонентов используется для построения единого критерия для рейтинговой оценки объекта управления.

Для нахождения рейтинговой оценки объекта можно воспользоваться следующей формулой:

$$R = \sum_{i=1}^{N} (Vp_i * \sum_{j=1}^{P} (K_j * Vk_j)),$$

где R – рейтинг; $i=1,2,...,N$ – вектор компонентов; Vp_i – весовой коэффициент i-го компонента; $j=1,2,...,P$ – вектор критериев в компоненте; K_j – числовое значение j-го критерия; Vk_j – весовой коэффициент j-го критерия.

Необходимость ввода весовых коэффициентов компонента и весовых коэффициентов критериев вызвана тем, что как критерии в одном компоненте, так и