# ФОРМИРОВАНИЕ РОБАСТНОГО ПОДХОДА К УПРАВЛЕНИЮ ПРИОРИТЕТАМИ ПРИ ОБНАРУЖЕНИИ И ПРОТИВОДЕЙСТВИИ КОМПЬЮТЕРНЫХ АТАК

Д.А. КОМЛИКОВ

Сформулируем постановку задачи "инвариантного" управления приоритетами в условиях изменения характеристик задающего воздействия (формировании стратегии организации прерывания воздействий компьютерных атак (далее — КА) на объекты информационных технологий (далее — ИТ) информационных систем (далее — ИС)) с точки зрения робастного подхода.

Рассмотрим возможность получения экстраполированных оценок (оценок при рассмотрении которых система принятия решений (далее — СПР) не имеет возможности активной коррекции и вмешательства извне) законов изменения воздействия КА и внедрения враждебного кода (далее — ВК) на объекты ИТ ИС с приоритетной дисциплиной разделения временного ресурса дискриминатора. Рассмотрим структуру объектов ИТ ИС в виде парциального канала.

Основной задачей является разработка методики синтеза робастных управлений, корректирующих средние времена обслуживания и экстраполяции в зависимости от характеристик организации КА и внедрения ВК (в частном случае, величин характеризующих динамику процесса — скоростей и ускорений). Рассмотрим задачу управления защитой для не полностью определенных объектов ИТ ИС, подверженных воздействию возмущений в СПР с приоритетами и экстраполяцией как наиболее важную.

Не полностью определенный объект ИТ или объект ИТ в условиях ограниченной неопределенности можно рассматривать как семейство объектов ИТ ИС, которое определяется множествами принадлежности параметров или характеристик этого объекта ИТ, а также множествами принадлежности внешних возмущений. Таким образом, возникает задача управления не единственным объектом ИТ, а семейством или множеством объектов ИТ ИС, что необходимо при управлении средствами обнаружения и противодействия КА систем защиты информации (далее — СЗИ) ИС. Решение этой задачи при отсутствии внешних возмущений приводит к определению фиксированного управляющего средства, обеспечивающего устойчивость СПР для всего семейства объектов ИТ. Такие СПР называются робастно устойчивыми.

Актуальность придания СПР робастизирующих свойств продемонстрируем на примере неоднородности законов изменения скоростей и ускорений при моделировании воздействий КА на объекты ИТ в зависимости от их нахождения в зоне опасности, отслеживаемой фильтрами СПР для организации противодействия КА и противодействия внедрению ВК.

Исходные формулы для расчета: $\left|\dot{\varepsilon}\right| = \frac{V}{4}\sin^2\varepsilon$, $\left|\ddot{\varepsilon}\right| = \left|\dot{\varepsilon}\right|\frac{V}{4}\left|\sin 2\varepsilon\right|$.

При прогнозировании последствий КА и организации противодействия КА опишем модель для оценки влияния робастного управления на точность принятия решения для дискретного аналога СПР принятия решений с ПИ-управлением.

Пусть передаточная функция $K_{uu}(p)=K_{uu}/p$, а $\upsilon(t)$ — белый шум со спектральной плотностью $N$. в первом состоянии, когда ключ замкнут, уравнение СПР относительно ошибки управления

$$e^{(1)}(t) = -Ke^{(1)}(t) + \dot{x} - K_{uu}\mathrm{v}(t) \quad K = K_g K_{uu},$$

а во втором состоянии

$e^{(2)}(t) = \dot{x}, \quad \dot{x} = \text{const}.$

Составим уравнения для математических ожиданий в различных положениях ключа, для чего воспользуемся общей формой записи уравнений моментов. Так уравнения для математических ожиданий принимают вид:

$$\dot{m}^{(1)}(t) = -Km^{(1)}(t) + \dot{x}\,p^{(1)}(t) - v^{(1)}m^{(1)}(t) + v^{(2)}m^{(2)}(t),$$

$$\dot{m}^{(2)}(t) = \dot{x}\,p^{(2)}(t) - v^{(2)}m^{(2)}(t) + v^{(1)}m^{(1)}(t).$$

После математических преобразований уравнений с учетом того, что ошибкой в режиме обслуживания не пренебрегать, и она выступает как начальное значение для режима экстраполяции, то, устремив степень устойчивости к $\infty$, уравнения для математических ожиданий примут следующий вид:

$$m^{(1)}(z) = 0,5z^{-1}m^{(1)}(z) + 0,5p^{(1)}\left(v^{(1)}, v^{(2)}\right)V_0 - v^{(1)}z^{-1}m^{(1)}(z) + v^{(2)}z^{-1}m^{(2)}(z),$$

$$m^{(2)}(z) = z^{-1}m^{(2)}(z) + p^{(2)}\left(v^{(1)}, v^{(2)}\right)V_0 - v^{(2)}z^{-1}m^{(2)}(z) + v^{(1)}z^{-1}m^{(1)}(z).$$

В результате перегруппировки и преобразований с учетом степени робастного управления α и степени задержки Z, получим конечное выражение для математического ожидания $m^{(2)}(i)$ с учетом робастного управления:

$$m^{(2)}(i) = \frac{1}{1-v^{(2)}\left(1-v^{(2)}\right)}\left(\frac{V_0}{v^{(1)}+v^{(2)}}\left(v^{(1)}\left(1-3v^{(2)}\right)+\left(A-v^{(2)}\right)\left(1+3v^{(1)}+A\right)\right)-\right.$$

$$-m^{(2)}(i-1)\left(A+v^{(1)}-0,5-v^{(2)}\left(3-2v^{(2)}+v^{(1)}\right)\right)-m^{(2)}(i-2)\left(A\left(1+v^{(1)}+A\left(1-2v^{(2)}\right)-\right.\right.$$

$$\left.\left.-2v^{(2)}\left(1+v^{(1)}-0,5v^{(2)}-0,25\right)\right)\right)-m^{(2)}(i-3)\left(v^{(2)}\left(0,5-v^{(2)}\right)+A\left(v^{(1)}-v^{(2)}-0,5\right)\right)\Bigg),$$

где $A = \dfrac{\left(v^{(1)}+v^{(2)}\right)-v^{(1)}\left(1-v^{(2)}\right)-v^{(2)}\left(1+v^{(2)}\right)}{v^{(1)}+v^{(2)}}$.

Для доказательства эффективности робастного управления проведем сравнительную оценку выражений для $m^{(2)}(i)$ с робастным управлением и без него.

Зафиксировав значения $v_0^{(1)}$; $v_0^{(2)}$ и изменяя $V_0$, проведем моделирование и проанализируем устойчивость СПР к внешним возмущениям. Результаты моделирования подтверждают, что так же как и в СПР, где начальной ошибкой, обусловленной режимом обслуживания, пренебрегали, качество работы робастной СПР при обнаружении и противодействии КА на порядок выше чем "штатной", а робастизирующие свойства улучшают качество работы СПР при обнаружении и противодействии КА практически на два порядка.

## К ВОПРОСУ АНАЛИТИЧЕСКОГО МОДЕЛИРОВАНИЯ DOS АТАК

Л.В. НОВИКОВА

Среди различного вида атак на информационные системы (ИС) особое место занимают DoS атаки. DoS атаки (Denial of Service, отказ в обслуживании) являются наиболее известной формой хакерских атак, против которых труднее всего создать стопроцентную защиту. Для организации DoS требуется минимум знаний и умений. Атака DoS делает ИС недоступной для обычного использования за счет превышения допустимых возможностей функционирования ИС.