# ТЕОРЕТИКО-ИГРОВОЕ МОДЕЛИРОВАНИЯ ПОВЕДЕНИЯ АЗАРТНОГО НАРУШИТЕЛЯ ПРИ ЗАЩИТЕ ИНФОРМАЦИОННЫХ РЕСУРСОВ

*Т. В. Вахний, А. К. Гуц*
vahniytv@mail.ru, aguts@mail.ru
*Омский государственный университет им. Ф. М. Достоевского*

*Описывается теоретико-игровой способ моделирования поведения азартного злоумышленника, представляющую особую угрозу при атаках на информационные компьютерные ресурсы.*

Известно, что при реализации новых подходов к защите информационных ресурсов с целью выработки решений и отработки средств защиты информации всё больше используется игровой подход, включающий, в том числе, и математические методы теории матричных игр [1,2]. Для достижения этой цели необходимо решить следующие задачи: произвести выбор стратегии; спланировать игру, осуществить математическое моделирование вариантов игры, провести игру, оценить эффективности стратегий игры и ролевых действий игроков (нарушитель-защитник) [3].

Одной из наиболее значимых фигур среди нарушителей является *азартный злоумышленник*. Учет его психологии и моделирование его поведения позволяет построить либо ловушки для его идентификации, либо для направления его активности в ложном направлении.

Игровой поход при математическом моделировании пары игроков «нарушитель-защитник» представляет собой матричную игру $G$ с матрицей $(g_{ij})$. Обозначим через $val(G)$ значение игры. Азартный злоумышленник в силу своей психологии и увлечённый желанием нанести как можно больший ущерб атакуемой компьютеризированной системы и преуменьшающий свои неудачи в предыдущих попытках атак на систему воспринимает игру $G$ как матричную игру $f(G)$ с матрицей $(f(g_{ij}))$, где $f$ так называемая функция полезности.

В случае азартного нарушителя эта функция задается непрерывной выпуклой (вниз) вещественной функцией $f : R \to R$.

Как доказано в [4], в случае азартной функции полезности имеют место утверждения: 1) из $val(G) = 0$ следует $val(f(G)) \geq 0,$ т.е. нарушитель может видеть победу там, где её нет; 2) из $val(G) > 0$ следует $val(f(G)) \geq val(G),$ т.е. азартный нарушитель преувеличивает размер успеха; 3) при любом опыте $x$ предыдущих вторжений существует такая игра $G_0$, что $val(G_0) < 0$ (реальный проигрыш, неудачная атака) и $val(G_0 + xE) > f(x)$, где $E$ матрица, состоящая из

единиц, т.е. азартный нарушитель всегда будет повторять некоторые проигрышные атаки (игру $G_0$).

Следовательно, организация матричной игры $G_0$ и её подробное исследование – это, по сути дела, изучение психологии азартного нарушителя. Его поимка задача более сложная: для этого необходимо реализовать матричную игру $G_0$ как информационный ресурс, способный привлечь (или отвлечь) внимание злоумышленника подобно тому, как это делалось в известном проекте медовой сети (honey net) [5].

**Библиографический список**


1. Воробьев А.А. Методы оценивания и обеспечения гарантированного уровня защиты информации от несанкционированного доступа в вычислительной сети автоматизированной системы управления: Автореф. дис. … к-та техн. наук /А.А.Воробьёв. – СПб., 1997. - 15 с.
2. Нестеров С.А. Разработка методов и средств проектирования инфраструктуры обеспечения информационной безопасности автоматизированных систем: Автореф. дис. … к-та техн. наук /С.А.Нестеров. – СПб., 2002. - 18 с.
3. Климов С.М. Проблемы создания компьютерных стратегических игр для оценки защищенности критически важных информационных сегментов [Электронный ресурс] - Режим доступа: http://www.contrterror.tsure.ru/site/magazine12/02-06-Klimov.htm. – Загл. с экрана.
4. Кемень Дж., Томпсон Дж. Влияние психологического отношения на исходы игры / Сборник переводов под ред. Н.Н.Воробьева. М.:ФМ, 1961. С.222-253.
5. The Honeynet Project [Электронный ресурс] - Режим доступа: http://www.honeynet.org. – Загл. с экрана.