

ПРИМЕНЕНИЕ МОДЕЛИ «ХИЩНИК-ЖЕРТВА» В РЕШЕНИИ ЗАДАЧИ ОТРАЖЕНИЯ КИБЕРАТАК

М.С. Кондратов¹, И.А. Долотов¹, Г.К. Хисаметдинова¹, Э.Р. Гиззатова¹

¹Уфимский университет науки и технологий, г. Уфа
e-mail: egorlag8553@gmail.com

Аннотация

В работе представлено численное решение задачи отражения кибератак на основе модели Лотки-Вольтерры. Приведены графики функций количества отраженных кибератак и функции количества уровней защиты. Результаты моделирования позволяют прогнозировать поведение функций при изменении отдельных параметров модели.

Ключевые слова: математическое моделирование, модель Лотки-Вольтерры, численное решение системы дифференциальных уравнений.

Введение

Модель Лотки- Вольтерры нашла свое применение не только в биологических задачах, для описания которых она используется чаще всего, но и в других областях, где подход «хищник-жертва» удобен в воспроизведении экспериментальных данных. Заложенная в модели система дифференциальных уравнений дает возможность описывать динамику поведения функции - «хищник» и функции – «жертва» во времени, что позволяет использовать ее в тех задачах, где важен учет влияния параметров модели на длину временных интервалов пиковых значений входящих в нее функций.

1. Математическая модель описания задачи динамики популяций «хищник-жертва»

При переходе к задаче определения временных интервалов отражения кибератак, необходимо привести математическое описание биологической модели «хищник-жертва», представляющей собой систему обыкновенных дифференциальных уравнений первого порядка:

$$\begin{aligned}\frac{dx}{dt} &= (\alpha - \beta y)x, \\ \frac{dy}{dt} &= (-\gamma + \delta x)y,\end{aligned}\tag{1}$$

где в соответствии с: x – численность популяции жертв; y – численность популяции хищников; t – время; α – коэффициент рождаемости жертв; β – коэффициент, описывающий снижение численности жертв за счёт встреч с хищниками; γ – коэффициент смертности хищников в отсутствие пищи; δ – коэффициент прироста хищников, связанный с потреблением жертв. Каждое уравнение системы (1) характеризует поведение своей функции, при этом в отсутствие «хищников» ($y=0$) популяция «жертв» резко возрастает (экспоненциальный рост численности), а при

отсутствии «жертв» ($x=0$) популяция «хищников» постепенно вымирает (медленный спад численности).

Вообще говоря, система (1) допустима в описании не только указанной задачи отражения кибератак, но и в экономике для анализа рыночной динамики, которая включает взаимообратное соответствие конкурирующих фирм, взаимодополняющих сервисов и экономику общего потребления. Также в экологии для моделирования популяционной динамики и прогнозирования влияния изменений климата/пищи на численность видов.

2. Вычислительный эксперимент моделирования задачи отражения кибератак на основе системы «хищник-жертва»

Одной из современных и актуальных задач информационной безопасности является математическое моделирование процессов реализации и отражения кибератак, в ней должна учитываться динамика взаимодействия между атакующей стороной (нарушителем) и защищающей стороной (аппаратные межсетевые экраны, шифрование данных, электронные подписи).

На основе работы [1] вводятся параметры, ассоциируемые с параметрами модели – $\alpha, \beta, \gamma, \delta$ и функциями – x, y . Так, параметр α – скорость распространения атак; β – эффективность защиты против атак; γ – скорость деградации защиты; δ – влияние атак на защиту; функция x – число успешных атак, y – уровень защищенности.

В настоящей работе были приняты следующие значения параметров и исходных значений функций: $\alpha=0,25, \beta=0,018, \gamma=0,12, \delta=0,009$.

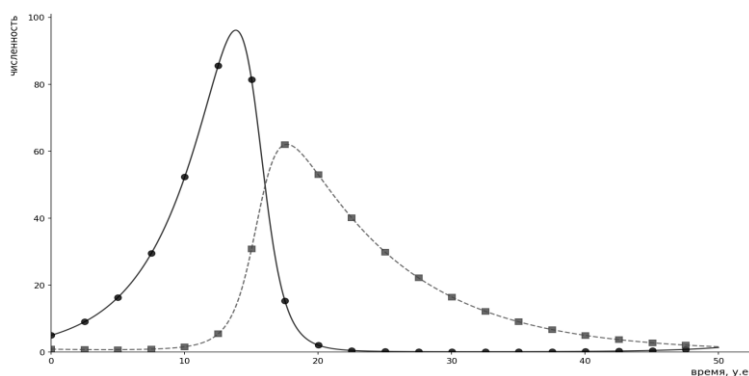


Рисунок 1 – Соотношение функций количества кибератак и отражений во времени с данными: $\alpha=0,25, \beta=0,018, \gamma=0,12, \delta=0,009$

На рисунке 1 приведены функции, соотносимые как число успешных атак и уровень защищенности (число межсетевых экранов на предприятии). Видно, что при резком увеличении уровня защищенности в точках t от 6-ой минуты до 7-ой минуты (практически моментально), также резко падает число кибератак с 95 до 40 процентов. Такое поведение соответствует существующим реалиям на производстве, в силу временного запаса от обнаружения атаки до включения аппаратных устройств в пределах 10 минут, что на рисунке 1 отмечено «индукционным» поведением функции x от 0 до 5 минут.

Следующий рисунок 2 характеризует фазовую траекторию функций $x(t)$ и $y(t)$. Четко прослеживаются петли поведения функций во времени.

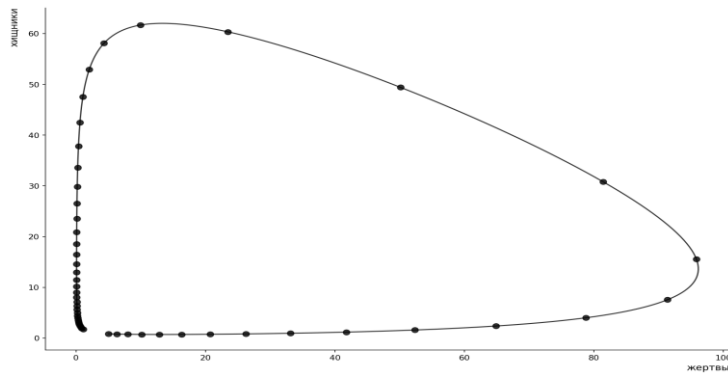


Рисунок 2 – Фазовая траектория функций количества кибератак и отражений во времени с данными: $\alpha=0,25$, $\beta=0,018$, $\gamma=0,12$, $\delta=0,009$

На рисунке 3 приведена фазовая траектория с увеличенным на 20% значением параметра α . В сравнении фазовых траекторий на рисунке 2 и рисунке 3, можно отметить, что увеличение скорости распространения кибератак влечет рост амплитуды колебаний числа успешных атак, и запаздывание системы защиты.

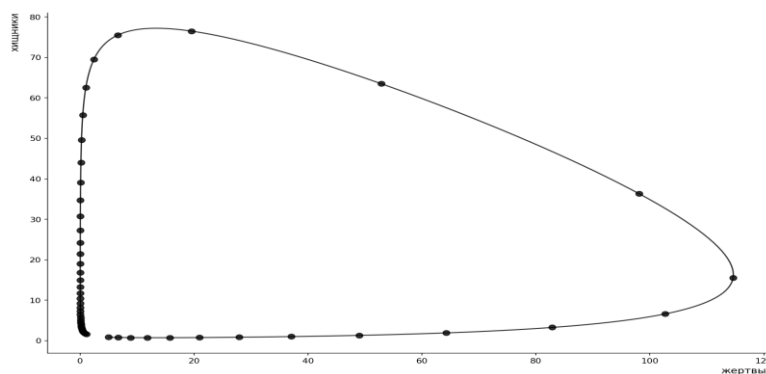


Рисунок 3 – Фазовая траектория функций количества кибератак и отражений во времени с данными: $\alpha=0,3$, $\beta=0,018$, $\gamma=0,12$, $\delta=0,009$

Таким образом, увеличение лишь одного параметра модели влечет изменение динамики движения функций и самого вида фазовой траектории.

Заключение

На основании полученных результатов, приведенных на рисунках 1-3, можно спрогнозировать дальнейшее поведение функций:

1) в связи с ростом амплитуды колебаний численности успешных атак, появляется больше возможностей для реализации угроз, что тоже самое, значительные пики активности атак;

2) смещение фазовых соотношений между числом атак и уровнем защищённости, ведет к отставанию системы реагирования, поскольку ресурсы защиты не успевают компенсировать возросшую интенсивность угроз;

3) дальнейшее увеличение средней численности успешных атак за период колебаний, однозначно прогнозирует рост общего ущерба от реализации угроз информационной безопасности.

Следовательно, при переходе системы защиты в режим более глубоких и продолжительных колебаний потребуется либо увеличения ресурсов защиты, либо внедрения превентивных механизмов, снижающих начальную интенсивность распространения атак.

Список использованных источников

1. Trapeznikov, E.V. Modeling, Optimization and Information Technology. – 2024. – V. 12, № 2.

APPLICATION OF THE PREDATOR-PREY MODEL IN SOLVING THE PROBLEM OF CYBERATTACK RESPONSE

¹M.S. Kondratov, ¹I.A. Dolotov, ¹G.K. Khisametdinova, ¹E.R. Gizzatova

*¹Ufa University of Science and Technology, Ufa
e-mail: egorlag8553@gmail.com*

Abstract

The paper presents a numerical solution to the problem of cyberattack response based on the Lotka–Volterra model. Graphs of the function of the number of repelled cyberattacks and the function of the number of protection levels are provided. The simulation results make it possible to predict the behavior of the functions when individual parameters of the model are changed.

Keywords: mathematical modeling, Lotka–Volterra model, numerical solution of a system of differential equations.