

4. Кремень В. Освіта і наука в Україні – інноваційні аспекти. Стратегія. Реалізація. Результати / В. Кремень. – К.: Грамота, 2005. – 448 с.

5. Особистісно орієнтовані технології навчання і виховання у вищих навчальних закладах: кол. монографія / [Андрущенко В.П., Дивинська Н.О., Корольов Б.І., Левшин М.М., Луговий В.І., Муковіз О.П.] / заг.ред В.П. Андрущенко, В.І. Луговий.-К.: Педагогічна думка, 2008. – 254с.

6. Пархоменко В.В. Дослідження стану сформованості економічної культури студентів економічних спеціальностей / В.В.Пархоменко // Zbiór raportów naukowych. «Pedagogika Współczesna nauka. Nowy wygląd» (30.01.2015 – 31.01.2015). – Warszawa: Wydawca: Sp. z o.o. «Diamond trading tour», 2015. – str. 50–58.

7. Черушева Г.Б Принципи педагогічної підготовки майбутніх магістрів економіки / Г.Б Черушева, В.В Пархоменко // Бізнес-аналітика в управлінні зовнішньоекономічною діяльністю: матеріали III Міжнарод. наук.-практ. конференції 11 листопада 2015 р. – К.: ДП “Інформ.-аналіт. агенство”. – С. 175-178.

Л. П. Перхун,

кандидат педагогічних наук,

доцент кафедри економічної кібернетики,

Національна академія статистики, обліку та аудиту, м. Київ;

О. М. Ізосімов,

викладач циклової комісії програмування

Коледжу бізнесу та аналітики

Національної академії статистики, обліку та аудиту

МОДЕЛЬ ВЗАЄМОДІЇ ХАКЕРСЬКИХ АТАК ТА ІНСТРУМЕНТІВ ЗАХИСТУ ПРОТИ НИХ

На сьогодні найбільш відомою і дослідженою моделлю взаємодії сутностей двох видів – «хижаків» і «жертв» – вважається модель Лотки-Вольтера та її різновиди [1]. У досліджуваній нами предметній області роль «жертв» будуть виконувати хакерські атаки, а «хижаків» - інструменти захисту проти них.

З аналізу предметної області побудована така модифікована модель:

$$\begin{aligned}x' &= ax - kx^2 - bxy \\y' &= -cy + \left(\frac{1}{b} - y\right) \cdot\end{aligned}\quad (1)$$

У моделі (1) перше рівняння описує динаміку хакерських атак, друге – динаміку розвитку інструментів захисту проти них.

Схарактеризуємо змінні та параметри моделі:

x – кількість хакерських атак;

y – кількість інструментів захисту проти хакерських атак;

a – коефіцієнт природного приросту кількості хакерських атак;

k – коефіцієнт внутривидової конкуренції для атакуючих ($k = \frac{1}{K}$, K у

класичній моделі з врахуванням внутривидової конкуренції- ємність ніші популяції, у нашому випадку – максимально можлива кількість атак);

b – коефіцієнт результативності одного інструменту захисту проти хакерських атак («пожирання» з біологічної точки зору);

c – коефіцієнт природнього зменшення кількості інструментів захисту проти хакерських атак за одиницю часу (їх “вимирання” при нульовій результативності протидії) [2].

Перший доданок ax першого рівняння моделі (1) показує природний приріст хакерських атак в одиницю часу. Очевидно, що кожна результативна атака має бути поштовхом до, як мінімум, ще однієї аналогічної атаки. Тому доданок ax не може бути меншим за кількість результативних атак у випадку наявності тільки одного інструменту протидії. Результативність одного інструментів захисту проти хакерських атак характеризується параметром b . Відповідно, у такому випадку позитивними будуть $(1-b)x$ хакерських атак. Отже, параметр a може змінюватись у межах $[1-b; \infty]$.

Другий доданок першого рівняння моделі (1) $-kx^2$ описує внутривидову конкуренцію за наявні ресурси, $k = \frac{1}{K}$, K – максимально можлива кількість атак. З точки зору теорії K дорівнює реальній кількості потенційних об’єктів для хакерських атак. У розрахунках слід вважати K досить великим числом. Відповідно k – досить мале число (чим більше K , тим ближче k до нуля).

Третій доданок першого рівняння моделі (1) $-bxy$ описує величину зменшення кількості позитивних хакерських атак. Параметр b дорівнює частці перерваних хакерських атак у розрахунку на один інструмент захисту, відповідно $0 < b \leq 1$.

Випадок $b = 0$ не розглядається ($b = 0$ означатиме, що жоден інструмент захисту не спрацьовує). Усереднена частка таких інструментів описана параметром c другого рівняння. Відповідно $0 < c \leq 1$, а перший доданок другого рівняння моделі (1) показує величину зменшення кількості інструментів захисту проти хакерських атак завдяки зниженню їх результативності.

Випадок $b = 1$ з практичної точки зору означає, що один інструмент протидії затримує 100% хакерських атак, що, якщо й можливо, але протягом невеликого терміну часу.

Другий доданок другого рівняння моделі (1) $(\frac{1}{b} - y)$ задає приріст інструментів протидії хакерським атакам, $\frac{1}{b}$ – необхідна кількість таких інструментів для випадку переривання всіх наявних атак, y – кількість наявних схем.

На практиці цікавою для аналізу є динаміка взаємодії хакерських атак та інструментів захисту проти них, яку можна дослідити методами якісного дослідження диференціальних рівнянь та їх систем.

Список використаних джерел

1. Моделирование экономической динамики: учеб. пособие / Т.С. Клебанова, Н.А. Дубровина, О.Ю. Полякова [и др.]. – Х.: ИД «ИНЖЭК», 2005. – 244 с.
2. Перхун Л.П. Модель динаміки взаємодії шахрайських атак та інструментів боротьби з ними / Л. П. Перхун, І.І. Поникла, В.С. Чудик // Ефективна економіка. – 2014. – № 1. – С. 28-34.

Н. Г. Петухова,

кандидат економічних наук,

доцент кафедри комерції та логістики,

*УО «Белорусский торгово-экономический университет
потребительской кооперации», г. Гомель, Республика Беларусь*

Т. В. Бондарева,

старший преподаватель

кафедры комерції та логістики,

*УО «Белорусский торгово-экономический университет
потребительской кооперации», г. Гомель, Республика Беларусь*

СОВРЕМЕННЫЕ ТЕНДЕНЦИИ РАЗВИТИЯ ВНЕШНЕЭКОНОМИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ ПОТРЕБИТЕЛЬСКОЙ КООПЕРАЦИИ РЕСПУБЛИКИ БЕЛАРУСЬ

С 1 апреля 2014 года торговое унитарное предприятие (ТУП) «Белкоопвнешторг Белкоопсоюза» является крупнейшим центром экспортно-импортных операций Республики Беларусь. Деятельность компании направлена на экспорт-импорт товаров белорусских и зарубежных производителей, оптовую и розничную торговлю, грузоперевозки, общественное питание, а также производство и реализацию изделий из