КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (1), 2018
ISSN 2663 - 4023

УДК 004.056

Щебланін Юрій Миколайович
Кандидат технічних наук, старший науковий співробітник
Державний університет телекомунікацій, Київ, Україна
OrcID: 0000-0002-3231-6750
sheblanin@ukr.net
Рабчун Дмитро Ігорович
аспірант, асистент кафедри управління інформаційною та кібернетичною безпекою
Державний університет телекомунікацій, Київ, Україна
OrcID: 0000-0002-5555-0910
rabchundima92@gmail.com

МАТЕМАТИЧНА МОДЕЛЬ ПОРУШНИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Анотація. Для забезпечення інформаційної безпеки в автоматизованих системах управління, побудови ефективної системи захисту інформації, мало виявити канали витоку інформації, проаналізувати можливі загрози, наслідки їх реалізації та оцінити втрати. Потрібно ще добре уявляти вигляд порушника. Однією з найважливіших складових ймовірного сценарію здійснення протиправних дій щодо доступу до інформації є модель порушника. Наявність такої моделі порушника безпеки, котра постійно коригується на основі отримання нових знань про можливості порушника та зміни в системі захисту, на основі аналізу причин порушень які відбулися, дозволить вплинути на самі ці причини, а також точніше визначити вимоги до системи забезпечення інформаційної безпеки від даного виду порушень. Правильно побудована модель порушника інформаційної безпеки, (адекватна реальності), у котрій відбиваються його практичні та теоретичні можливості, апріорні знання, час і місце дії і т.п. характеристики — важлива складова успішного проведення аналізу ризику та визначення вимог до складу та характеристиками системи захисту. У роботі розглянуті труднощі математичного моделювання при дослідженні інформаційного протистояння, які обумовлені, з одного боку, невизначеністю дій суперника, з другого – складністю створення умовного образу, який в найбільшій степені відповідає розгалуженій захисній структурі. При створенні математичної моделі однією з основних задач є визначення параметрів і характеристик, які формують цільову функцію. Розгляду цієї задачі і присвячена дана робота. Розглянуто модель, в якій цільова функція визначає частку втраченої при нападі інформації і виражається через динамічну вразливість системи, котра залежить від співвідношення ресурсів нападу і захисту, а також від імовірності реалізації такого співвідношення. Розглянуто форму цих залежностей. Вразливість виражається дробово-степеневою функцією, в якій показник степеня визначається природою інформаційної системи та її структурою. Щільність імовірності виділення нападом ресурсів x при заданій кількості ресурсів захисту задається двопараметричним законом розподілу. Підбираючи показники в обох залежностях, можна досягти їх максимального наближення до статистичних кривих і зрештою сформувати в явній формі цільову функцію.

Ключові слова: інформаційна безпека, математичне моделювання, модель порушника, розподіл ресурсів.

1. ВСТУП

Із переходом в інформаційну епоху найважливішим ресурсом сучасності стала інформація. Саме з цим пов’язаний перехід людства від глобальних військових конфліктів (боротьба за ресурси, території) до інформаційних протистоянь. Попри це витрати від такого протистояння не тільки залишаються незмінними, а навпаки — зростаюсь. Для ведення ефективної боротьби та для ефективного захисту інформації фахівцями було розроблено та запропоновано різні види моделей, зокрема, математичних, для початкового прогнозування ризиків і втрат пов’язаних із веденням інформаційного протиборства. Такі моделі дозволяють нам із заданою точністю

відобразити сам процес і, що є найголовнішим, його наслідки. Визначившись із ресурсами котрими володітиме сторона нападу, наступним кроком буде перехід до моделювання ситуації динамічного протистояння, коли одна із сторін буде реагувати на дії іншої, таким чином зменшуючи втрати від інформаційного протистояння.

Метою наукової роботи є дослідження та моделювання дій порушника інформаційної безпеки. В рамках представленої роботи проведений аналіз поведінки порушника інформаційної безпеки з точки зору виділення ним ресурсів на напад, запропоновано метод для визначення ймовірності виділення певної кількості ресурсів, описані існуючі моделі порушників ІБ, приведено статистику нападів на корпоративні інформаційні мережі та системи.

2. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Статистика є одним із основних інструментів при побудові математичної моделі. На сьогоднішній день найбільша кількість статистичної інформації про інциденти інформаційної безпеки надходить з США, ФРН, Великої Британії. Це зумовлено, насамперед, розвиненістю інформаційних технологій в цих країнах, а також наявністю транснаціональних корпорацій, котрі останнім часом серйозно відносяться до питання безпеки.

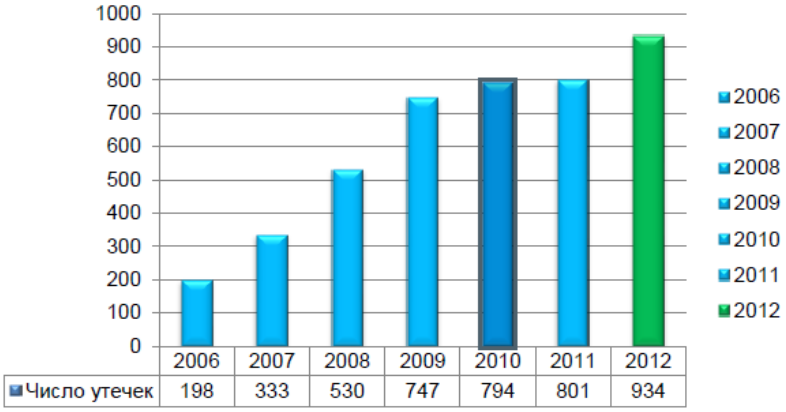

Рис.1. Кількість зареєстрованих інцидентів

Перш за все, варто відмітити позитивну динаміку в зростанні кількості нападів. По відношенню до 2008 року кількість нападів збільшилась на 40%, з одного боку це пов'язане, безпосередньо, із збільшенням кількості атак, а з іншого — ускладнення та інтеграція СЗІ і відповідного збільшення випадків реєстрації інцидентів [3].

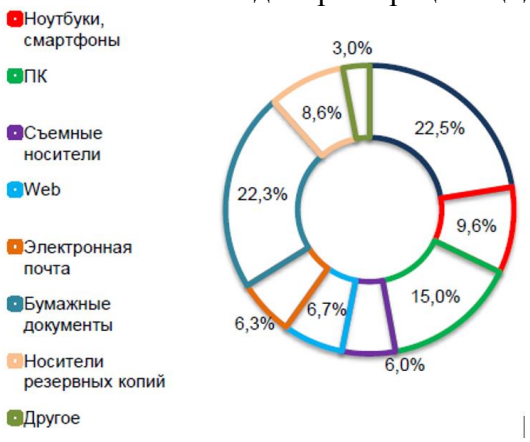

Рис.2. Розподіл інцидентів по каналам

ISSN 2663 - 4023

Щодо каналів витоку, то згідно звіту компанії InfoWatch вони поділяються на: мобільні пристрої, ПК, зовнішні носії, WEB, електронна пошта, паперові носії, носії резервних копій, інше. Досі найбільшим каналом витоку є паперові носії інформації. Для переходу до моделювання слід також привести статистику у відповідності до виду атаки (навмисна, ненавмисна).

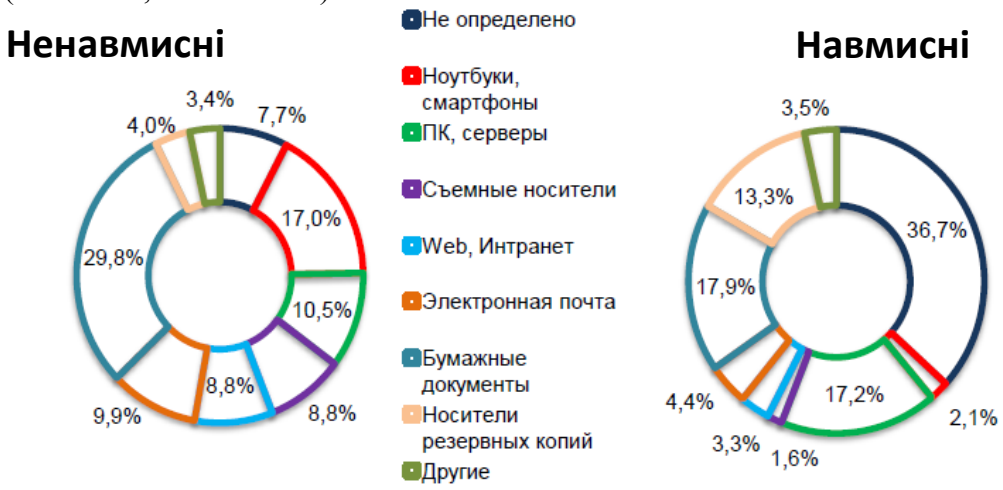

Рис.3. Розподіл навмисних і ненавмисних інцидентів по каналам

Використовуючи отримані дані, а також оцінивши методом експертних оцінок потенційні втрати від реалізації загроз по відповідним каналам отримуємо таблицю з ризиками.

Таблиця 1

Визначення ризиків ІБ КІС на основі статистичних і експертних даних

		Кол-во атак, %			Риск	
№	Канал утечки	Случайные	Намеренные	Ущерб	Случайные	Намеренные
1	не определено	7,7%	36,7%	2	0,154	0,057
2	мобильные устр.	17,0%	2,1%	2	0,340	0,007
3	ПК, серверы	10,5%	17,2%	5	0,525	0,090
4	съемные носители	8,8%	1,6%	3	0,264	0,004
5	WEB	8,8%	3,3%	3	0,264	0,009
6	электронная почта	9,9%	4,4%	4	0,396	0,017
7	бумажные носители	29,8%	17,9%	4	1,192	0,213
8	носители резервных к.	4,0%	13,3%	5	0,200	0,027
9	др	3,4%	3,5%	2	0,068	0,002

Таким чином, в 2012 році Аналітичним центром компанії InfoWatch було зареєстровано 934 опублікованих ЗМІ інциденти ІБ. Найбільша частина з котрих припадає на персональні дані — 89,4%. Найпопулярнішим каналом витоку є паперові носії. На мою думку, представлену вибірку можна вважати репрезентативною, так як вона включає більшість країн світу, всі сфер народного господарства і комерційної діяльності.

Розглянемо у якості прикладу систему з двох об’єктів та використаємо математичну модель [4], в якій цільова функція визначає частку втраченої інформації в системі має вигляд:

$$i(x,y)=\sum_{k=1}^{l} i_k(x,y)=\sum_{k=1}^{l} g_k \cdot p_k \cdot q_k(x)\cdot f_k(x,y) \quad (1)$$

де x та y — ресурси нападу і, відповідно, захисту, $\sum_{k=1}^{l} x_k = X$; $\sum_{k=1}^{l} y_k = Y$;

k — номер об'єкта;

g_k — відносна вартість інформації на k-му об'єкті (через g_k також позначається сам об'єкт);

p_k — імовірність нападу на k-й об'єкт;

$q_k(x)$ — щільність імовірності виділення нападом ресурсів x на k-ий об'єкт;

$f_k(x,y)$ — імовірність вилучення інформації з k-го об'єкту, яку розглядаємо як динамічну вразливість об'єкта.

У цьому розділі всю увагу приділено функції $q_k(x)$, як показника котрий характеризує дії нападника.

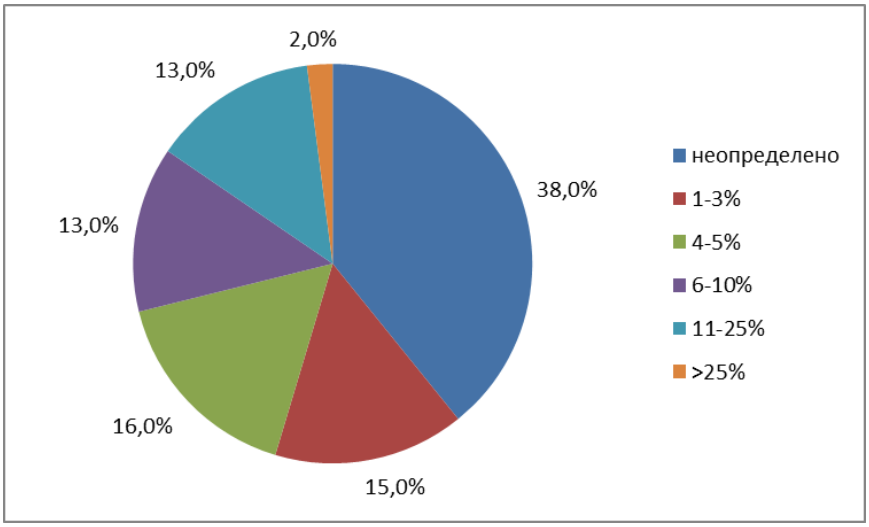

Рис.4. Бюджет IT на інформаційну безпеку

Використовуючи інформацію із вищезгаданого звіту, а також інших звітів щодо інцидентів інформаційної безпеки побудовано статистичну криву, котра відображає ймовірність виділення порушником ресурсів для нападу на КІС. Слід звернути увагу на те, що точної інформації про кількість ресурсів котрі виділяються для нападу на інформаційні системи не існує, проте за основу можна взяти функцію $q(y)$ — щільність ймовірностей виділення ресурсів y на захист, так як обидві залежності ($q(x)$ та $q(y)$) визначаються вартістю інформації на об'єкті [4].

Скористаючись звітом SANS Institute InfoSec "Risk, Loss and Security Spending in the Financial Sector: A SANS Survey" опублікованому в березні 2014 року визначимо вигляд залежності $q(y)$. Після проведення елементарних операцій і вирівнювання інтервалів отримано 5 статистичних точок [3]. Наступним кроком здійснено підбір виду закону розподілу і його параметрів, який буде проходити найближче до статистичних точок. Було розглянуто ряд найпоширеніших двопараметричних законів, найбільш

близьким до статистичних точок виявилась щільність ймовірностей логнормального закону розподілу.

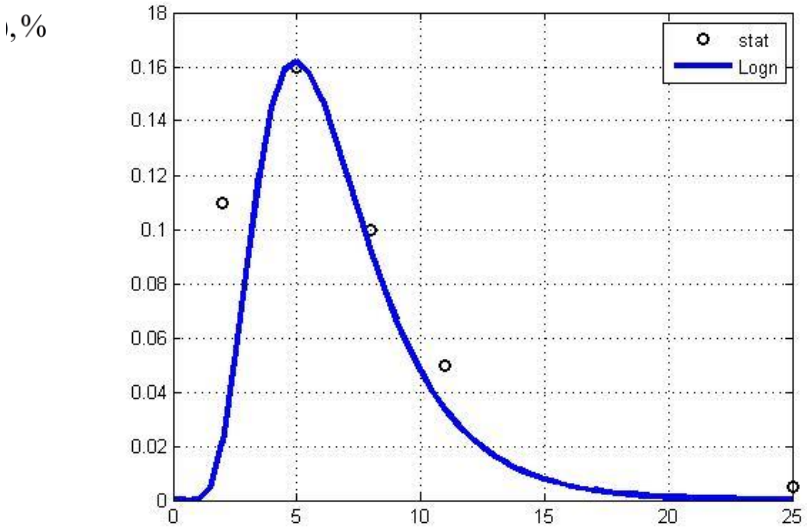

Рис.5. Значення $q(x)$ побудовані на основі статистичних даних і найбільш близькі до цієї залежності розподіли

На рис.5 точками відмічені значення, котрі відповідають статистиці в [3] і щільність ймовірностей логнормального закону розподілу при значеннях $\mu = 1.8$, $\sigma = 0.45$. Значення параметрів σ, μ було підібрано таким чином, щоб координати максимумів $q(x)$ співпали з точкою $q_{\max} = 16$, $x_{\max} = 5$.

Для реалізації описаного методу було використано математичний комплекс MatLAB, який дозволяє аналізувати та ілюструвати статистичні дані, а також проводити вибір найбільш близького закону розподілу і його параметри. Набір параметрів розподілу визначається експертними оцінками на підставі даних про конкретну систему захисту, зовнішнє і внутрішнє середовище підприємства.

Таким чином запропонований метод можна використовувати для оцінки ймовірності виділення нападником на КІС певної кількості ресурсів, що дозволяє нам виробити оптимальну по втратам стратегію захисту [6].

2.1. ВИЗНАЧЕННЯ РОЗПОДІЛУ РЕСУРСІВ ПО ОБ'ЄКТАМ ЗАХИСТУ

Наступна складова математичної моделі $f(x, y)$, яка характеризує динамічну вразливість об'єкта захисту, також може бути використана для моделювання дій порушника. Використання такого підходу дозволяє нам перейти від статичного протистояння, коли ресурси нападу фіксувались і були сталими величинами, до динамічного — оптимізація ресурсів захисту виконується з врахуванням інформації про дії суперника, відповідно то термінології теорії ігор це послідовна гра з повною інформацією.

Для опису динамічної вразливості використовується дробово-степенева функція, так як вона відповідає вимогам: $f(x, y)$ приймає значення у діапазоні від 0 до 1, при

ISSN 2663 - 4023

$\frac{x}{y} \to 0 \quad f_k(x,y) \to 0$, при $\frac{x}{y} \to \infty \quad f_k(x,y) \to 1$: $\qquad f(x,y) = \frac{\left(\frac{x}{y}\right)^n}{\left(\frac{x}{y}\right)^n + c}$

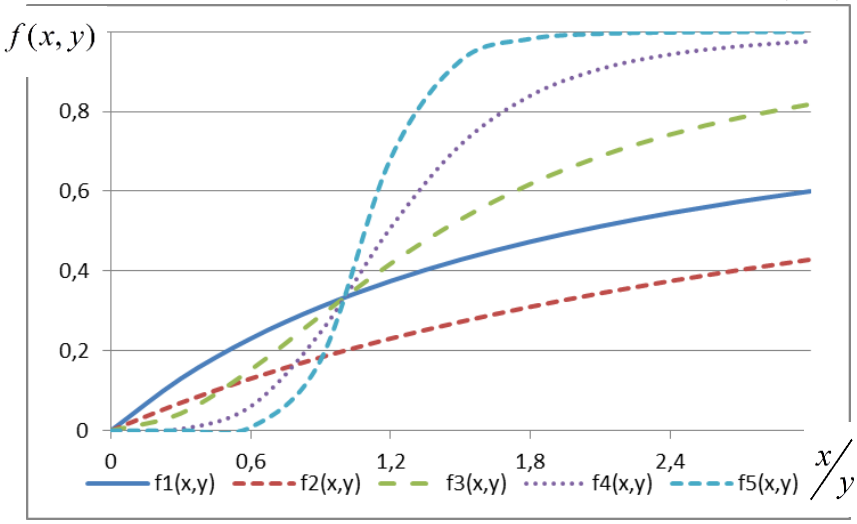

Рис.6. Вигляд функції вразливості при різних значеннях c, n:

f1 - $c=2$, $n=1$; *f2* - $c=4$, $n=1$; *f3* - $c=2$, $n=2$
f4 - $c=2$, $n=4$ *f5* - $c=2$, $n=8$

На рис.6 зображено залежність вразливості перешкоди f від співвідношення ресурсів $\frac{x}{y}$, виділених нападом і захистом.

Параметри n, c визначаються особливостями систем захисту і природою об'єктів на яких зберігається інформація. Варто відмітити, що дробово-лінійним функціям вразливості ($n=1$) можуть відповідати фізичні системи захисту інформації: внесення інвестицій навіть на початкових етапах ($\frac{x}{y}<1$) дає певні результати. Прикладами таких систем можуть бути: охорона периметру, захист від витоку каналами ПЕМВН, тощо. Дробово-нелінійні функції ($n>1$) можуть описувати вразливість, наприклад, криптографічних систем: внесення інвестицій не приносить результату до моменту коли з'ясований ключ або виявлена уразливість криптоалгоритму, після цього моменту вразливість криптосистеми різко збільшується, що видно на лініях f4 та f5.

Коефіцієнт c може інтерпретуватись як природна захищеність, наприклад: рекомендується облаштовувати серверні приміщення невеликих мереж в окремих кімнатах, які не мають суміжних дверей з іншими приміщеннями і знаходяться якомога далі від сходів і виходів.

Описавши необхідні складові цільової функції (1) і визначившись із обмеженнями можна визначити оптимальний розподіл ресурсів нападу, який буде забезпечувати максимальне значення вилученої інформації $i(x,y)$. Дані результати відображатимуть найгірший для сторони захисту результат: нападник володіє необхідною інформацією про систему захисту (кількість об'єктів на яких зберігається і оброблюється інформація, параметри системи захисту), знає (точно чи наближено) ресурси, котрі виділяються на захист кожного з об'єктів.

ISSN 2663 - 4023

Для прикладу розглянемо систему захисту, котра складається з двох об'єктів g_1 та g_2, і двох перешкод f_1, f_2. Параметри системи: $g_1 = 0.4$, $g_2 = 0.6$, $c_1 = 4$, $c_2 = 8$, $n_1 = n_2 = 1$. Ресурси захисту незмінні і становлять $y_1 = y_2 = 0.05$. Відповідно до попереднього розділу ресурси нападу змінюються в інтервалі $X = [0.04..0.18]$, як найбільш ймовірні. Цільова функція приймає вигляд:

$i(x, y) = 0.4 \frac{x_1 / 0.05}{x_1 / 0.05 + 4} + 0.6 \frac{x_2 / 0.05}{x_2 / 0.05 + 8}$. Критерій оптимальності для сторони нападу — максимум $i(x, y)$.

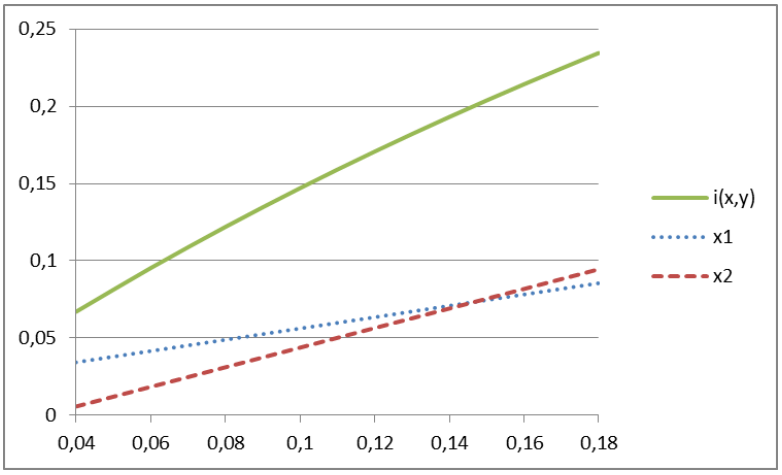

Рис.7. Залежність кількості вилученої інформації від розміру ресурсів нападу, їх розподіл по об'єктам

На рис. 7 зображено результат дій сторони нападу. Звісно, такий показник, як максимум вилученої інформації не може використовуватись в якості основного, адже при збільшенні ресурсів на напад більш ніж в 4 рази нападник вилучив тільки в 3,5 рази більше інформації. Для подальшого аналізу інвестицій у напад (для кращого розуміння дій порушника) потрібно звернутись до економічних показників, таких як: прибуток від інвестицій, рентабельність та інші.

3. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

В рамках наукової роботи мною було проаналізовано існуючі моделі порушника інформаційної безпеки, виділені основні параметри і характеристики за якими можливо класифікувати нападника. Зібрана статистична інформація з вітчизняних та іноземних джерел в сфері інформаційної безпеки і, що становить особливу вагу, запропоновано метод для моделювання поведінки порушника, а саме визначення ймовірності виділення ресурсів x на напад.

Математичні моделі інформаційного протистояння при всій різноманітності їх форм є близькими за своєю сутністю. Цільова функція виражає одну з споріднених величин: частку втраченої інформації, імовірність порушення системи захисту, ризик втрат, який визначається як добуток імовірності реалізації загрози на завданий збиток, тощо. Основна характеристика системи захисту, яка впливає на значення цільової функції – це вразливість, котра в тій чи іншій формі виражається через співвідношення

ресурсів нападу і захисту. В цільову функцію входить також імовірність виділення на напад певної кількості ресурсів при заданій кількості ресурсів захисту. Наведена методика дозволяє, користуючись статистичними даними, визначити згадані величини і сформувати цільову функцію. Подальші дослідження повинні бути направлені на збір статистичної інформації і встановлення відповідності між характеристиками реальних інформаційних систем та їх вразливістю.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Д. І. Рабчун, «Оцінка ефективності інформаційної безпеки з урахуванням економічних показників», *Сучасний захист інформації*, №4, сс. 91–96, 2015.
[2] A. Platzer, *Logical Analysis of Hybrid Dynamical Systems: Proving Theorems for Complex Dynamics*, USA, Springer, 2010. DOI: 10.1007/978-3-642-14509-4.
[3] R. Shanmugavadivu, "Network Intrusion Detection System Using Fuzzy Logic," *Indian Journal of Computer Science and Engineering (IJCSE)*, vol. 2, pp. 101–111, 2011.
[4] М. Г. Медведєв і І. О. Пащенко, *Теорія ймовірностей та математична статистика*, Київ, Ліра-К, 2008.
[5] Є. Г. Левченко і А. О. Рабчун, «Оптимізаційні задачі менеджменту інформаційної безпеки», *Сучасний захист інформації*, №1 (1), сс. 16–24, 2010.
[6] М. В. Демчишин, Є. Г. Левченко і Д. І. Рабчун, «Графоаналітичний метод пошуку сідлової точки в ігрових задачах інформаційної безпеки», *Системні дослідження та інформаційні технології*, №3, сс.48–61, 2014.
[7] L. A. Gordon and M. P. Loeb, "The Economics of Information Security Investment," *ACM Transactions on Information and System Security*, vol. 5, no. 4, pp.438–457, 2002.
[8] В. В. Глушак і О. М. Новіков, «Синтез структури системи захисту інформації з використанням позиційної гри захисника та зловмисника», *Системні дослідження та інформаційні технології*, №2, сс. 89–100, 2013.
[9] H. I. Ansoff, *Strategic Management, UK : Palgrave Macmillan*, 2007. DOI: 10.1057/9780230590601.
[10] T. Moore, D. Pym and C. Ioannidis, *Economics of Information Security and Privacy*, US, Springer, 2010. DOI: 10.1007/978-1-4419-6967-5.
[11] S. Goel and V. Chen, "Information Security Risk Analyses – a Matrix-Based Approach," in *Information Resource Management Association International Conference*, San Diego, USA, 2005.
[12] L. A. Zadeh, "Stochastic Finite-State Systems in Control Theory," *Information Sciences*, no. 251, pp. 1–9, 2013.
[13] В. В. Глушак і О. М. Новіков, «Метод проектування систем захисту інформації з використанням детермінованої гри „захисник-зловмисник"», *Наукові вісті НТУУ «КПІ»*, №2, сс. 46–53, 2011.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№1 (1), 2018
ISSN 2663 - 4023

UDC 004.056

Yury Shcheblanin
Candidate of Sciences, Senior Research
State University of Telecommunications, Kyiv, Ukraine
OrcID: 0000-0002-3231-6750
sheblanin@ukr.net

Dmytro Rabchun
Postgraduate, Assistant of the Department
State University of Telecommunications, Kyiv, Ukraine
OrcID: 0000-0002-5555-0910
rabchundima92@gmail.com

MATHEMATICAL MODEL OF INFORMATION SECURITY'S THEAT AGENT

Abstract. To provide information security in automated control systems, the construction of an effective system of information security, it was not enough to identify channels of information leakage, to analyze the possible threats, the consequences of their implementation and estimate the losses. It is necessary to imagine an offender even better. An offender model is one of the most important components of a possible scenario for unlawful actions on access to information. The existence of such a model of a security breach, which is constantly corrected on the basis of obtaining new knowledge about the possibilities of the offender and changes in the security system, based on an analysis of the causes of violations, will allow themselves to affect these reasons, as well as more precisely define the requirements for the information security system from this type of violations. Correctly constructed model of the violator of information security, (adequate to reality), which reflects his practical and theoretical capabilities, a priori knowledge, time and place of action, etc. characteristics are an important part of a successful risk analysis and the definition of requirements for the composition and characteristics of the protection system. The difficulties of mathematical modeling in the study of information confrontation, which are conditioned, on the one hand, by the uncertainty of the opponent's actions, and on the other, the complexity of creating a conditional image, which in the largest degree corresponds to the branched protective structure, is considered in the paper. When creating a mathematical model one of the main tasks is to determine the parameters and characteristics that form the target function. The consideration of this task is devoted to this work. A model is considered in which the target function determines the proportion of information lost during an attack and is expressed through the dynamic vulnerability of the system, which depends on the ratio of attacks and protection resources, as well as on the likelihood of the implementation of such a relationship. The form of these dependencies is considered. The vulnerability is expressed by the fractional-power function in which the degree of power is determined by the nature of the information system and its structure. The density of probability of allocating an attack of resources with a given number of defense resources is given by a two-parameter distribution law. By selecting the indicators in both dependencies, it is possible to reach their maximum approximation to the statistical curves and eventually to form an explicit form of the target function.

Keywords: information security, mathematical modeling, threat agent model, resource management.

REFERENCES

[1] D. I. Rabchun, "Otsinka efektyvnosti informatsiynoyi bezpeky z urakhuvannyam ekonomichnykh pokaznykiv [Estimation of efficiency of information security taking into account economic indicators]," *Suchasnyy zakhyst informatsiyi*, no. 4, pp. 91–96, 2015. (In Ukrainian).

[2] A. Platzer, *Logical Analysis of Hybrid Dynamical Systems: Proving Theorems for Complex Dynamics*, USA, Springer, 2010. DOI: 10.1007/978-3-642-14509-4.

[3] R. Shanmugavadivu, "Network Intrusion Detection System Using Fuzzy Logic," *Indian Journal of Computer Science and Engineering (IJCSE)*, vol. 2, pp. 101–111, 2011.
[4] M. H. Medvedyev and I. O. Pashchenko, *Teoriya ymovirnostey ta matematychna statystyka* [*Probability theory and mathematical statistics*], Kyiv, Lira-K, 2008. (In Ukrainian).
[5] Ye. H. Levchenko and A. O. Rabchun, "Optymizatsiyni zadachi menedzhmentu informatsiynoyi bezpeky [Optimization tasks of information security management]," *Suchasnyy zakhyst informatsiyi*, no. 1 (1), pp. 16–24, 2010. (In Ukrainian).
[6] M. V. Demchyshyn, Ye. H. Levchenko and D. I. Rabchun, "Hrafoanalitychnyy metod poshuku sidlovoyi tochky v ihrovykh zadachakh informatsiynoyi bezpeky [Graph-analytic method of finding a saddle point in game information security tasks]," *Systemni doslidzhennya ta informatsiyni tekhnolohiyi*, no. 3, pp.48–61, 2014. (In Ukrainian).
[7] L. A. Gordon and M. P. Loeb, "The Economics of Information Security Investment," *ACM Transactions on Information and System Security*, vol. 5, no. 4, pp.438–457, 2002.
[8] V. V. Hlushak and O. M. Novikov, "Syntez struktury systemy zakhystu informatsiyi z vykorystannyam pozytsiynoyi hry zakhysnyka ta zlovmysnyka [Synthesis of the structure of the information security system with the use of a defensive and intruder positional game]," *Systemni doslidzhennya ta informatsiyni tekhnolohiyi*, no. 2, pp. 89–100, 2013. (In Ukrainian).
[9] H. I. Ansoff, *Strategic Management, UK : Palgrave Macmillan*, 2007. DOI: 10.1057/9780230590601.
[10] T. Moore, D. Pym and C. Ioannidis, *Economics of Information Security and Privacy*, US, Springer, 2010. DOI: 10.1007/978-1-4419-6967-5.
[11] S. Goel and V. Chen, "Information Security Risk Analyses – a Matrix-Based Approach," in *Information Resource Management Association International Conference*, San Diego, USA, 2005.
[12] L. A. Zadeh, "Stochastic Finite-State Systems in Control Theory," *Information Sciences*, no. 251, pp. 1–9, 2013.
[13] V. V. Hlushak and O. M. Novikov, "Metod proektuvannya system zakhystu informatsiyi z vykorystannyam determinovanoyi hry zakhysnyk-zlovmysnyk [Method of designing information security systems using deterministic game 'defender-intruder']," *Naukovi visti NTUU "KPI,"* no. 2, pp. 46–53, 2011. (In Ukrainian).