разователя. Как показали исследования, погрешности от шумов и альязинга имеют аддитивный характер, суммарное влияние которых не превышает 0,2 % в конце диапазона измерения и 2 % – в начале.

***Ключевые слова:*** сопротивление, измерение импеданса, частотные анализаторы импеданса, активные измерительные преобразователи, альязинг, передаточная характеристика, погрешности измерения импеданса.

***Ivakh R.V., Khoma V.V., Khoma Yu.V., Pytel I.D.*** **The Research of the Errors of the Model of a Direct Measure Impedance Analyser**

Our study describes and analyzes the main sources of the error of direct action impedance analyzers based on active measurement converters. As a results of the investigations performed, is that such phenomena as noise and aliasing have been found to be the most important. These factors make the biggest impact on the accuracy of the in-phase and quadrature components of the output voltage of the active converter. Studies have shown that errors caused by noise and aliasing have an additive nature, and their overall impact does not exceed 0.2 % at the end of the measurement range and 2 % – in the beginning.

***Keywords:*** impedance measurement, impedance analyzers, active measurement convertors, alyazinh, transfers characteristic impedance measurement error.





# 4. ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ГАЛУЗІ

*УДК 004.[056+3.75]:061.[68+69]*

## АНАЛІЗ НАЯВНИХ ПІДХОДІВ ДО ПРОТИДІЇ НЕСАНКЦІОНОВАНОМУ ДОСТУПУ В ІНФОРМАЦІЙНИХ МЕРЕЖАХ ДЕРЖАВИ НА ОСНОВІ ТЕОРІЇ ІГОР

***В.Б. Дудикевич[1], І.Р. Опірський[2], В.А. Сусукайло[3]***

Для вирішення проблеми кількісного оцінювання захищеності автоматизованих систем розроблено моделі процесів нападу та захисту інформації на основі математичного апарату теорії матричних ігор. Представлено математичний апарат та метод використання теорії ігор у процесі нападу на інформацію в інформаційних мережах держави. Представлено матричну гру, рішення якої дає змогу визначити найбільш небезпечний засіб реалізації несанкціонованого доступу (НСД), найефективніший засіб захисту інформації і розмір мінімального збитку, заподіяного використанням відповідної системи захисту інформації (СЗІ). Проведено аналіз застосування матричних ігор для моделювання процесів нападу на інформацію в інформаційних мережах держави.

***Ключові слова:*** несанкціонований доступ, теорія ігор, комплексні системи захисту інформації, захист інформації, загрози, інформаційні мережі держави.

**Вступ**. На сьогодні створення системи протидії загрозам (СПЗ) неможливе без дослідження й узагальнення світового досвіду побудови інформаційно-телекомунікаційних систем (ІТС) та їх складових підсистем, ключовим елементом яких є зокрема СПЗ від НСД. Математичними забезпеченнями таких систем є моделі процесів нападу на інформацію та її захисту. Базисом таких моделей є математичний аналіз, який не в змозі забезпечити адекватність процесів, що моделюються реальними процесами, які відбуваються в ІТС. Основними причинами недосконалості математичного аналізу, що використовується нині, полягає в труднощах формалізації завдань показу та несанкціонованого (НСД) щодо інформації та її захисту, які пов'язані з процесами, що складно формалізуються і змінюють свої параметри протягом функціонування інформаційної мережі держави (ІМД), як складової ІТС. Внаслідок цього не виконується вимога до компенсаційного аналізу функціонування СПЗ, що призводить до зниження їх ефективності та ускладнення розроблення перспективних систем на їх базі.

Отже, питання про створення та подальшого розвитку підходу до моделювання процесів НСД щодо інформації у ІМД на базі сучасного математичного інструментарію є відкритим і актуальним та потребує детального наукового дослідження. Очевидно, розроблення принципово нових математичних моделей процесів НСД на інформацію природно повинна здійснюватися, виходячи із

[1] проф. В.Б. Дудикевич, д-р техн. наук – НУ "Львівська політехніка";
[2] ст. викл. І.Р. Опірський, канд. тех. наук – НУ "Львівська політехніка";
[3] студ. В.А. Сусукайло – НУ "Львівська політехніка"

аналізу відомих підходів та моделей, а також тих принципів, на основі яких вони розроблені і які покладені в їх основу, що зроблено у попередніх дослідженнях [1-3].

**Об'єкт дослідження** – методи теорії ігор у задачах захисту інформації.

**Предмет дослідження** – математичні моделі та матричний апарат прогнозування НСД в ІМД.

**Мета роботи** – проведення дослідження та аналізу можливості застосування моделей на базі матричного апарату теорії ігор у задачах захисту інформації, з метою використання їх для прогнозування НСД в ІМД.

**Виклад основного матеріалу**. Передумовою застосування теорії ігор у задачах захисту інформації є антагоністична природа цілей суб'єктів інформаційного конфлікту – гравців, кожен з яких намагається досягнути одночасно несумісних положень. Інформаційний конфлікт в ІТС, як системне явище, характеризується структурними, динамічними та теоретико-ігровими властивостями. З огляду на це, постає актуальна проблема врахування цих властивостей під час моделювання процесів нападу на інформацію.

Проаналізувавши літературні джерела, з'ясовано, що на сьогодні відомо низку наукових досліджень [4-6], де теорію ігор використовують у галузі захисту інформації як математичний інструмент. Але треба зауважити, що незважаючи на це, відомі підходи не дають змоги вирішити проблему захисту інформації в повному обсязі. Вперше дані про застосування теорії ігор для розв'язання часткових задач захисту інформації з'явилися у публікації А.А. Воробйова [7].

Вперше теоретико-ігровий підхід до моделювання процесів нападу на інформацію та її захисту застосовано для оцінювання захищеності автоматизованих систем, що становлять інформаційну і телекомунікаційну інфраструктуру держави [7]. Основою для розроблення цього підходу стала методологія кількісного оцінювання захищеності автоматизованих систем, яку вперше подано у [7]. Для рішення проблеми кількісного оцінювання захищеності автоматизованих систем автори розробили моделі процесів нападу та захисту інформації на основі математичного апарату теорії матричних ігор. Суть моделювання процесів нападу на інформацію матричною грою полягає в такому.

Модель процесу нападу на інформацію класифіковано як скінчену гру двох гравців з нульовою сумою. Гра $\Gamma$ для одного об'єкта АС $S_k$, $k = 1,2,...,l$, де об'єкти АС задаються трійкою

$$\Gamma = \{X, Y, \Phi\} \quad (1)$$

де: $\Phi = \Phi(x_i, y_i)$ – плата, що є функцією двох змінних $x_i \in X$ і $y_i \in Y$ ($X = \{x_i\}$ – повний перелік можливих загроз НСД у вигляді скінченої множини, $i = 1,2,...,n$; $Y = \{y_i\}$ – скінченна множина засобів захисту інформації на об'єкті $S_k$ АС, ($j = 1,2,...,m$). Значення плати $\Phi$, в міру скінченності множини $X$ та $Y$, має матричне подання

$$\Phi = \| \phi_{ij} \|, \ \phi_{ij} = \Phi(x_i, y_i). \quad (2)$$

Процес нападу на інформацію полягає в тому, що перший гравець незалежно від другого обирає стратегії $x_i \in X$, де $i$ означає вибір рядка матриці, ін-





ший – засіб захисту інформації $y_i \in Y$ – стратегії, де $j$ означає вибір стовпця. При цьому перетин обраного рядка і стовпця є відповідною платою $\phi_{ij}$ першого гравця і виграшем другого.

Рішення матричної гри (1), (2) дає змогу визначити найбільш небезпечний засіб реалізації НСД $x^*_i \in X$, найефективніший засіб захисту інформації $y^*_i \in Y$ і розмір мінімального збитку $\phi_{ij}$, заподіяного використанням відповідної СЗІ $y^*_i \in Y$. Але розрахунок таких показників здійснюється тільки в статичній постановці. Статика моделі проявляється на етапі формування платіжної матриці (2). Значне різноманіття можливих способів реалізації НСД і стрімка динаміка їх перебіг ставить під сумнів адекватність цієї моделі реальним процесам нападу на інформацію.

Галузь застосування цієї матрично-ігрової моделі є досить обмеженою, оскільки гра в такій постановці не завжди має рішення в чистих стратегіях. Відсутність сідловок точки породжує проблему рішення гри у вигляді комбінованих стратегій, які змінюються за випадковим законом з випадковою частотою. Внаслідок зміщення стратегія не гарантована, тобто рівень захищеності АС оцінюється апостеріорно. Окрім цього, практична реалізація рішення у змішаних стратегіях, як правило, неможлива.

Вперше у вітчизняній науково-технічній літературі запропоновано застосувати теорію ігор для управління інформаційною безпекою [8]. Автори зазначили, що застосування теорії ігор дасть змогу розвинути кількісний підхід в управлінні інформаційною безпекою. При цьому створювані управлінські моделі дають змогу ухвалювати оптимальні рішення в умовах невизначеності або неповної інформації в конфліктній ситуації. Спираючись на цю тезу, подальші наукові дослідження вітчизняних науковців, наприклад у [9], ґрунтуються на теоретичних основах, викладених у [8].

Наукова публікація [9] з проблематики застосування теорії ігор у задачах захисту інформації з'явилась відносно недавно. Модель процесу нападу на інформацію в [9] подано в ігровій інтерпретації. У моделі [9] передбачено, що обсяг інформації, яку може отримати неавторизований користувач (гравець) у процесі нападу на інформацію, визначається деякою функцією $I(x, y)$, де: $x$ – ресурс гравця, що нападає; $y$ – ресурс гравця, який захищається. Якщо $f(n)$ для гравця, що нападає, є цінністю $n$ одиниць інформації, а $g(n)$ є сумарними витратами на створення і заощадження інформації, то чистий прибуток гравця, що атакує, визначається як

$$V(x, y) = f[I(x, y)] - x, \quad (3)$$

а втрати

$$U(x, y) = g[I(x, y)] + y. \quad (4)$$

Оптимальна стратегія нападу існує у тому разі, коли виконується таке співвідношення:

$$f'[I(x, y)] = \frac{dI(x, y)}{dx} = 1. \quad (5)$$

Антагоністична природа цієї гри визначає оптимальну стратегію другого гравця як

$$g'[I(x,y)] = \frac{dI(x,y)}{dy} = 1. \quad (6)$$

Аналіз цієї моделі (3)-(6) показує, що процес нападу на інформацію подано в суворій постановці. На практиці ця модель застосування не знайшла. У моделі не передбачено процедуру оцінювання цінності інформації, а також не розроблено методик отримання аналітичного вигляду функцій $I$, $f$ та $g$ для загального випадку, що досі залишається невирішеною проблемою. Проблеми застосування матричних ігор для моделювання процесів нападу на інформацію порушено у роботі [7]. У мірі абсолютної схожості цих робіт подано їх узагальнений аналіз.

Процес нападу на інформацію та її захисту подано як антагоністичну гру з нульовою сумою, але жодна із запропонованих моделей не має суворого ігрового рішення. Ігрові моделі розглядають з позицій оптимального розподілу ресурсів гравців сторін, що конфліктують. Оптимальні стратегії розподілу ресурсів нападу $X$ та захисту $Y$ за сукупністю об'єктів $S$ знаходяться з матриці виразів $F$. Елементи $f_{ij}(x_i, y_i)$ матриці випадків $F$ запропоновано знаходити з використанням моделі Гроса

$$f_{ij}(x_i, y_i) = g_{ij}(x_i - y_i),\ j = \overline{1,n}, i = \overline{1,m} \quad (7)$$

де $g_{ij}$ – коефіцієнт інформаційної важливості. Практичне застосування відомих моделей на базі матричного апарату теорії ігор для рішення задач захисту інформації потребує додаткової розробки алгоритмів розрахунку вхідних даних (елементів матриці виграшів). На сьогодні запропоновані алгоритми розрахунку вхідних даних на базі моделі Гроса є складними, трудомісткими, а проблема їх формування потребує додаткових досліджень

**Висновки**. Розроблення принципово нових математичних моделей процесів захисту від НСД в ІМД природно повинно здійснюватися, виходячи із аналізу відомих підходів та моделей, а також тих принципів, на основі яких вони розроблені і які покладені в їх основу.

Отже, як показує практика експлуатації СЗІ, оцінки захищеності інформації в АС повинні враховувати не тільки антагоністичну природу суб'єктів інформаційного конфлікту, а й динаміку змін власне процесів нападу на інформацію та їх захисту. Тому в статичній постановці цей напрям наукових досліджень подальшого розвитку не отримав, а стає основою для розроблення нових підходів на його основі.

## Література

1. Опірський І.Р. Особливості процедури прогнозування несанкціонованого доступу / І.Р. Опірський // Захист інформації : зб. наук. праць. – К. : Вид-во НАУ. – 2014. – Спец. вип. – С. 74-80.

2. Опірський І.Р. Проблематика основного постулату прогнозування НСД / І.Р. Опірський // Сучасна спеціальна техніка : зб. наук. праць. – К. : Вид-во ДНДІ МВС України. – 2015. – № 2(41). – С. 3-9.





3. Опірський І.Р. Класифікація моделей захисту інформації в інформаційних мережах держави / І.Р. Опірський // Науковий вісник НЛТУ України : зб. наук.-техн. праць. – Львів : РВВ НЛТУ України. – 2015. – Вип. 25.10. – С. 329-335.

4. Грищук Р.В. Теоретичні основи моделювання процесів нападу на інформацію методами теорій диференціальних ігор та диференціальних перетворень / Р.В. Грищук. – Житомир : Вид-во "Рута". – 280 с.

5. Мулен Э. Теория игр / Э. Мулен. – М. : Изд-во "Миф", 1985. – 199 с.

6. Крапивин В.Ф. Теоретико-игровые методы синтеза сложных систем в конфликтных ситуациях / В.Ф. Крапивин. – М. : Изд-во "Сов. радио", 1972-192 с.

7. Воробьев А.А. Оценивание защищённости автоматизированных систем на основе методов теории игр / А.А. Воробьев, Г.В. Куликов, А.В. Непомнящих // Информационные технологии : сб. науч. тр. – М. : Изд-во "Новые технологии", 2007. – 24 с.

8. Андреєв В.І. Стратегія управління інформаційною безпекою / В.І. Андреєв, В.Д. Козюра, Л.М. Скачек, В.О. Хорошко. – К. : Вид-во ДУІКТ, 2007. – 272 с.

9. Хорошко В.А. Информационная безопасность Украины. Основные проблемы и перспективы / В.А. Хорошко // Захист інформації : зб. наук. праць. – К. : Вид-во НАУ. – 2008. – Спец. вип. – С. 6.9.

Надійшла до редакції 28.03.2016 р.

***Дудикевич В.Б., Опирский И.Р., Сусукайло В.А.*** **Анализ существующих подходов к противодействию несанкционированным доступам в информационных сетях государства на основе теории игр**

Для решения проблемы количественной оценки защищенности автоматизированных систем разработаны модели процессов нападения и защиты информации на основе математического аппарата теории матричных игр. Представлены математический аппарат и метод использования теории игр при процессе нападения на информацию в информационных сетях государства. Представлена матричная игра, решение которой позволяет определить наиболее опасное средство реализации несанкционированного доступа (НСД), эффективное средство защиты информации и размер минимального ущерба, причиненного использованием соответствующей системы защиты информации (СЗИ). Проведен анализ применения матричных игр для моделирования процессов нападения на информацию в информационных сетях государства.

***Ключевые слова:*** несанкционированный доступ, теория игр, комплексные системы защиты информации, защита информации, угрозы, информационные сети государства.

***Dudykevych V.B., Opirskyy I.R., Susukaylo V.A.*** **The Analysis of Existing Approaches to Deal with Unauthorized Access to the Information Networks of the State on the Basis of Game Theory**

To solve the problem of quantifying the security of automated systems, the models for the processes of attacks and data protection are designed on the basis of the mathematical apparatus of the theory of matrix games. A mathematical apparatus and method of using game theory for the process of the attack on the information in the information networks of the state are presented. The matrix game solution may allow identifying the most dangerous means of implementation of the UA, the effective means of information protection and the minimum size of the damage caused by the use of appropriate INS. The analysis of the use of matrix games for the simulation of the attack on the information in the information networks of the state is conducted.

***Keywords:*** unauthorized access, game theory, complex systems of information protection, information security, threats, information networks of state.