Ministry of Education and Science of Ukraine

# ODESSA NATIONAL ACADEMY OF FOOD TECHNOLOGIES

International Competition of
Student Scientific Works

# BLACK SEA SCIENCE 2018

## PROCEEDINGS


April, 4, 2018

ODESSA, ONAFT 2018

Ministry of Education and Science of Ukraine

Odessa National Academy of Food Technologies

International Competition of Student Scientific Works

# BLACK SEA SCIENCE 2018

**Proceedings**

**April 4, 2018**



Odessa, ONAFT 2018

Міністерство освіти і науки України

Одеська національна академія харчових технологій

Міжнародний конкурс студентських наукових робіт

# BLACK SEA SCIENCE 2018

**Матеріали**

**4 квітня 2018 року**



Одеса, ОНАХТ 2018

**UDC 001(262.5):378.4.091.27(08)**
**BBC 421D221**
**B64**



**Black Sea Science 2018**: Proceedings of the International Competition of Student Scientific Works, April 4, 2018, Odessa / Odessa National Academy of Food Technologies; B. Yegorov, M. Mardar (editors-in-chief.) [*et al.*]. – Odessa: ONAFT, 2018. – 827 p.

Proceedings of International Competition of Student Scientific Works «Black Sea Science 2018» contain the works of winners of the competition.

The author of the work is responsible for the accuracy of the information.

**ISBN 978-966-289-181-2** Odessa National Academy of Food Technologies

**УДК 001(262.5):378.4.091.27(08)**
**ББК 421D221**
**В64**



**Black Sea Science 2018**: Матеріали Міжнародного конкурсу студентських наукових робіт, 4 квітня 2018 р., Одеса / Одеська національна академія харчових технологій; Б. В. Єгоров, М. Р. Мардар (відп. ред.) [та ін.]. – Одеса: ОНАХТ, 2018. – 827 с.

Збірник включає матеріали робіт переможців Міжнародного конкурсу студентських наукових робіт «Black Sea Science 2018**».**

За достовірність інформації відповідає автор публікації.

**ISBN 978-966-289-181-2** Одеська національна академія харчових технологій

## Organizing committee:

**Prof. Bogdan Yegorov,** D.Sc., Rector of Odessa National Academy of Food Technologies, Head of the Committee

**Prof. Maryna Mardar,** D.Sc., Vice-Rector for Scientific and Pedagogical Work and International Relations of Odessa National Academy of Food Technologies, Deputy Head of the Committee

**Prof. Stefan Dragoev,** D.Sc., Vice-Rector on Research and Business Partnerships of University of Food Technologies (Bulgaria)

**Prof. Baurzhan Nurakhmetov,** D.Sc., First Vice-Rector of Almaty Technological University (Kazakhstan)

**Prof. Andrzei Kowalski,** Dr. habil., Director of Institute of Agricultural and Food Economics (Poland)

**Dr. Olivera Djuragic,** Ph.D., Director of Scientific Institute of Food Technology of University of Novi Sad (Serbia)

**Prof. Mircea Bernic,** Dr. habil., Vice-Rector on Research and Doctorate of Technical University of Moldova (Moldova)

**Prof. Jacek Wrobel,** Dr. habil., Rector of West Pomeranian University of Technology (Poland)

**Prof. Michael Zinigrad,** D.Sc., Rector of Ariel University (Israel)

**Dr. Mei Lehe,** PhD, Vice-President of Ningbo Institute of Technology, Zhejiang University (China)

**Prof. Plamen Kangalov,** Ph.D., Vice-Rector on Education of "Angel Kanchev" University of Ruse (Bulgaria)

**Dr. Alexander Sychev,** Ph.D., Assoc. Professor of Sukhoi State Technical University of Gomel (Belarus)

**Dr. Hanna Lilishentseva**, Ph.D., Assoc. Professor, Head of the Department of Merchandise of Foodstuff of Belarus State Economic University (Belarus)

**Prof. Heinz Leuenberger,** Ph.D., University of Applied Sciences and Arts Northwestern Switzerland (Switzerland)

## Організаційний комітет:

**Єгоров Богдан Вікторович** – д.т.н., професор, ректор – Одеська національна академія харчових технологій – голова оргкомітету

**Мардар Марина Ромиківна** – д.т.н., професор, проректор з науково–педагогічної роботи та міжнародних зв'язків – Одеська національна академія харчових технологій – заступник голови оргкомітету

**Драгоєв Стефан Георгієв**– д.т.н., професор, проректор з наукової роботи і бізнес партнерства – Університет харчових технологій (Болгарія)

**Нурахметов Бауржан Кумаргалієвич** – д.т.н., професор, перший проректор – Алматинський технологічний університет (Казахстан)

**Ковальські Анджей** – доктор-хабілітат, професор, директор інституту економіки сільськогосподарської та харчової промисловості – Інститут сільськогосподарської та продовольчої економіки (Польща)

**Дюрагіц Олівера** – доктор, директор інституту харчових технологій – Університет в м. Нові Сад (Сербія)

**Бернік Мірча** – доктор-хабілітат, професор, проректор з наукової роботи та докторантури – Технічний університет Молдови (Молдова)

**Вробель Яцек**– доктор-хабілітат, професор, ректор – Західнопоморський технологічний університет (Польща)

**Зініград Михаїл** – доктор наук, професор, ректор – Аріельський університет (Ізраїль)

**Лехе Мей** – доктор, віце-президент – Технологічний інститут Нінбо Чжэцзянського університету (Китай)

**Кангалов Пламен** – професор, доктор, проректор з навчальної роботи – Русенський університет «Ангел Канчев» (Болгарія)

**Сичев Олександр Васильович** – к.т.н, доцент, проректор з навчальної роботи – Гомельський державний технічний університет ім. П. Й. Сухого (Білорусь)

**Лілішенцева Анна Миколаївна** – к.т.н, доцент, зав. кафедрою товарознавства продовольчих товарів – Білоруський державний економічний університет (Білорусь)

**Леунбергер Хайнц** – доктор, професор – Університет прикладних наук і мистецтв Північно-західної Швейцарії (Швейцарія)

# DYNAMIC PROPERTIES OF PROVIDING CYBERSECURITY PROCESSES AT THE EXAMPLE OF CYBERSECURITY'S AUDIT

Author – Kozlova O.
Supervisor – Kononovych V.
*Odessa National Polytechnic University*

*The paper considers the process of development from information security to cybernetic security of infrastructure objects, and in particular, processes of cyber security audit. It has been established that the aspects of the dynamics of information and cyber security processes have not been adequately studied, and they do not disclose a complete formal and systemic approach to solving cybersecurity problems. In this regard, developed a logical-linguistic model of a risk-oriented approach to planning cyber security activities and the mathematical model of two-stage cyclical management of audit processes. The use of the mathematical model will contribute to a more accurate understanding of the dynamic properties and the development of the necessary system and extra-systemic measures to ensure cybersecurity. The process of conducting an audit based on the cybernetic cycle is being investigated. The model of the audit process is constructed using the logistic function and discrete reflections. The conditions of bifurcations, the nature of possible irregular oscillations in a dynamical system are determined. The working conditions that violate the normal functioning of the system are determined, hinders the audit of cybersecurity, and for the first time allowed to reasonably explain under what conditions the audit process will be disrupted.*

# ДИНАМІЧНІ ВЛАСТИВОСТІ ПРОЦЕСІВ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ НА ПРИКЛАДІ АУДИТУ КІБЕРБЕЗПЕКИ

Автор – Козлова О.Ю.
Керівник – Кононович В.Г.
*Одеський національний політехнічний університет*

## Вступ

Інформаційний та кібернетичний простори відіграють важливу роль в економічному та соціальному розвитку кожної країни світу. В Україні існує ціла низка проблем вразливості інформаційної сфери відносно стороннього кібернетичного впливу. Протистояти фізичному руйнуванню технічних засобів, порушенню функціонування об'єктів нападу та протиправній діяльності соціальних інженерів з дня на день стає все важче через недостатнє кадрове забезпечення відповідними фахівцями у сфері інформаційної та кібербезпеки. Необхідним є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави [1].

Небезпека кіберзлочинності була усвідомлена ще в часи приєднання України до міжнародної «Конвенції про кіберзлочинність». А термін «кібербезпека кіберпростору» з'явився у лексиконі українських спеціалістів зовсім недавно. Щодо поняття «кібербезпека» розгорнулась дискусія. Визначення понять «інформаційна безпека» та «кібербезпека» дуже схожі у багатьох авторів [1-3] і формально відрізняються додаванням понять «кіберпростір», як об'єкту захисту, «кіберзагроз» тощо. Кібербезпека розглядається як безпека специфічного виду інформації – управлінської інформації [2]. Приставка «кібер-» виділяє «клас кіберсистем, які використовуються для вирішення задач управлінського характеру». «В кіберсистемах на перше місце виділяється вимоги неперервності й стійкості управління. А ці вимоги можуть бути виконані лише при умові забезпечення доступності, цілісності та конфіденційності вхідної інформації [3]». Для уточнення термінів ще потрібні додаткові дослідження.

Міжнародна спільнота накопичила немалу кількість стандартів та передових практик захисту критично важливих об'єктів інфраструктури [4]. Важливе місце в системі інформаційної безпеки та кібербезпеки займає аудит [5-6]. Основним призначенням аудиту кібербезпеки об'єкта інформаційної діяльності є формування, як правило, незалежної оцінки кібербезпеки.

За метою проведення аудит поділяється на аудит для підтвердження відповідності вимогам національної системи нормативно-правових документів інформаційної безпеки та на аудит підтвердження відповідності міжнародним стандартам ISO\IEC 15408 [7]».

В процесі експлуатації систем кібербезпеки низка процесів, таких як аудит, моніторинг, автоматизовані дії збору, реєстрації даних та

обробки інцидентів інформаційної безпеки тощо, мають працювати безперервно і циклічно.

Для поступового поліпшення різних видів діяльності, зокрема, аудиту кібербезпеки застосовують процесно-орієнтовані підходи до управління. Такі циклічні процеси реалізуються послідовністю етапів: планування, дії, перевірки, впливання. При автоматизації певних етапів застосовують алгоритми штучного інтелекту, та системи прийняття рішень людиною-оператором. Такі змішані системи, як правило, являються нелінійними.

У той же час, теорія нелінійної динаміки та синергетики дають приклади складної поведінки систем, складених з простих нелінійних елементів, здатних генерувати динамічний хаос. Виникає проблема вивчення умов впливу нелінійних явищ на поведінку системи.

Як і в багатьох сферах при системному підході системи кібербезпеки розглядаються як динамічні системи, які складаються із множини механізмів і функцій, які теоретики пов'язують із феноменом самоорганізації. Ряд спеціалістів застосовують методи нелінійної динаміки для вивчення властивостей процесів захисту інформації [8-9]. Процеси аудиту, зокрема внутрішнього, є принципово циклічним і нелінійними. Ці питання потребують своєї розробки.

Проблемам прийняття рішень, аудиту присвячено гігантський обсяг літератури. Вкажемо деякі з них, що використані у даній роботі. Моделі та теорія систем прийняття рішень представлені в [10-11]. Приклади автоматизації управління безпекою та застосування циклічних процедур управління наведені в [12-13]. Хорошим посібником по є [14].

Конкретні дослідження нелінійних властивостей періодичних процесів управління, зокрема процесів аудиту кібербезпеки, авторам невідомі. Тому динамічні властивості процесів аудиту та можлива його складна поведінка системи аудиту досліджені ще недостатньо і дана тема є актуальною.

*Метою роботи* є удосконалення термінології у частині понять «кібербезпеки», пристосування найпростішої дискретної математичної моделі динаміки циклічного процесу до проведення процедур аудиту та виявлення впливу нелінійних властивостей на протікання процесу аудиту.

Для досягнення вказаної мети потрібно вирішити наступні задачі:

1. Аналізу та уточнення семантичної моделі поняття «система кібербезпеки»;

2. Пристосування математичної моделі періодичного процесу проведення аудиту для системи управління, яка дозволяє визначити умови і границі виникаючих нелінійних ефектів та можливого детермінованого хаосу.

3. Дослідити поведінку системи проведення аудиту кібербезпеки за допомогою дискретної математичної моделі динамічної системи, яка включає в себе найпростіші нелінійні елементи та описує динамічну систему за допомогою двох дискретних відображень і визначити інтервали параметрів нормального функціонування динамічної системи.

Дискретна математична модель процесу аудиту розв'язується методами чисельного моделювання. Визначаються умови біфуркацій, характер можливих нерегулярних коливань процесу аудиту. Отримані результати дозволяють підвищити ефективність роботи циклічних систем управління системи проведення аудиту та формалізувати напрямки подальших досліджень щодо розробки ефективних систем управління процесом аудиту з використанням методів нелінійної динаміки.

Об'єктом дослідження є поняття кібербезпеки та періодичні й неперіодичні процеси поведінки системи управління аудитом кібербезпеки.

Предметом дослідження є уточнення терміну «кібербезпека» та вплив нелінійних явищ на поведінку системи управління аудитом кібербезпеки.

Методи розробки базуються на теорії кібербезпеки, теорії прийняття рішень, теорії нелінійної динаміки.

У першому розділі наведено порівняльний огляд понять «кібербезпеки» та інформаційної безпеки у світлі еволюції систем захисту інформації.

Другий розділ присвячено особливостям кібербезпеки у промисловій сфері.

У третьому розділі розглянуто застосування циклічних процедур в управлінні та процесно-орієнтований підхід до управління аудитом кібербезпеки, що застосовується в технологіях забезпечення кібербезпеки.

У четвертому розділі подано математичне описання моделі динамічної системи, яка характеризує процес проведення аудиту кібербезпеки та результати вивчення поведінки динамічної системи, яка відображає процес проведення аудиту кібербезпеки. Аналізується

двомірне логістичне відображення (система із двох дискретних рівнянь). Будуються рівняння руху та біфуркаційні діаграми для динамічної системи. Отримується висновок щодо недостатньої надійності системи аудиту при збільшенні інтенсивності проведення процесів.

Результати даної роботи можуть бути використані при визначенні раціонального режиму проведення процесів аудиту кібербезпеки.

Результати виконання в даній роботі дослідження опубліковані у двох наукових статтях у журналі «Інформатика і математичні методи моделювання»:

– том 6, № 4 [15];

– том 7, № 3 [16].

## 1. Визначення понять кібербезпеки та інформаційної безпеки

Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року визначає: «Кібербезпека – це захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечується сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенціальних загроз національній безпеці України у кіберпросторі», де «кіберпростір – середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікації з використанням мережі Інтернет та або інших глобальних мереж передачі даних». «Кіберзахист – це сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем [17]». В Законі України «Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» від 9 січня 2007 року визначається: «Інформаційна безпека – стан захищеності життєво важливих інтересів людини, суспільства і держави, за якого запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанк-

ціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації [18]».

Взаємовідношення понять у сферах безпеки в кіберпросторі у контексті ISO 27032 представлені на рис. 1. Кібербезпека забезпечується у наступних сферах: безпека застосувань і операційних систем, безпека інформаційно-комунікаційних мереж, безпека роботи в Інтернет, захист інформації у ключових системах інформаційної інфраструктури і, зокрема, в об'єктах критичної інфраструктури, а також у сферах боротьби з кіберзлочинністю та забезпечення безпеки роботи у кіберпросторі. Даний рисунок справляє те уявлення, що кібербезпека є складовою частиною інформаційної безпеки. Формально це так. Кібернетичні системи, як системи управління, у своєму сучасному вигляді, являються підмножиною інформаційних систем.

Але, судячи з визначень, які наведено вище, поняття «кібербезпека» більш ширше у відношенні об'єктів, яких воно стосується. На рис. 2 показані об'єкти/суб'єкти які охоплюються, відповідно, інформаційною (ІБ) та кібернетичною безпекою (КБ).

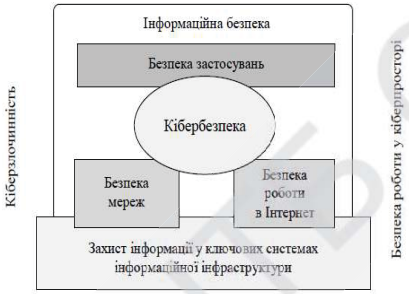



**Рис. 1. Місце кібербезпеки серед інших сфер безпеки**

*Джерело: ISO 27032:2012*


**Рис. 2. Охоплення об'єктів інформаційної та кібербезпеки**

Ретроспективно системи захисту інформації розвивалось переходячи до наступних етапів:

– захист інформації системами технічного та криптографічного захисту, за допомогою криптографічних, технічних, організаційних, а тепер і програмних засобів;

– забезпечення інформаційної безпеки інформаційних ресурсів в автоматизованих системах. До інформаційних ресурсів відноситься

інформація, засоби обробки інформації та (звернемо увагу) обслуговуючий персонал (НД ТЗІ 1.1-003-99);

– забезпечення інформаційної безпеки інформаційних технологій, зокрема в інформаційно-комунікаційних системах. На цьому етапі об'єктом захисту стає також відкрита інформація, важлива для особи, суспільства та держави;

– забезпечення кібернетичної безпеки кіберпростору. Кіберпростір охоплює інформацію, інформаційні технології, персонал, користувачів і все те, що виникає при комунікаціях суб'єктів і об'єктів та взаємодії їх між собою.

Сформулюємо головні відмінності інформаційної та кібербезпеки, користуючись переліком «Базові заходи кібербезпеки», які наведені в роботі [19]:

- Об'єктом забезпечення кібербезпеки стає кіберпростір. Його важлива складова – інформаційно-комунікаційна та телекомунікаційна системи.

- Ще більше приділяється уваги готовності мереж, що важливо з точки зору відбиття DDOS-атак.

- Суб'єктом забезпечення кібербезпеки стають, крім персоналу, конечні користувачі. Для безпеки конечних користувачів передбачаються низка заходів, включаючи застосування персональних між мережевих екранів та систем виявлення вторгнень.

- Методи соціальної інженерії є не лише засобом нападу, а й захистом від атак.

- Актуалізуються як обов'язкові процеси менеджменту, моніторингу і аудиту, динаміка яких є предметом даного дослідження.

## 2. Особливості кібербезпеки у промисловій сфері

У промисловій сфері інформаційні технології повинні відповідати підвищенням вимогам до експлуатаційних характеристик та параметрів безпеки. Наприклад, переважна більшість особливих міркувань наведені у публікації МАГАТЕ STI/PUB/1527 [20], які показують основні особливості системи кібербезпеки у сфері промислового виробництва. У табл. 1 представлені на основі матеріалів Національного інституту стандартів і технологій США (НІСТ) дані щодо основних відмінностях промислових систем управління (ПСУ) та класичними системами на базі ІТ.

**Таблиця 1 – Відмінності між системами на базі IT і ПСУ**

| **Категорія** | **Система на базі інформаційних технологій** | **Промислова система управління** |
|---|---|---|
| 1 | 2 | 3 |
| Вимоги до робочих характеристик | Не являється системою реального часу. Спрацювання має бути стабільним.<br>Вимагається висока продуктивність.<br>Можуть бути прийнятними великі затримки та флуктуації | Являється системою реального часу Критичним являється час спрацювання.<br>Прийнятна помірна продуктивність.<br>Великі затримки та/або флуктуації являються серйозною проблемою |
| Вимоги до експлуатаційної готовності | Такі види реакції як перенавантаження прийнятні.<br>Недоліки у плані експлуатаційної готовності часто можуть бути допустимі, у залежності від експлуатаційних вимог системи | Такі види реакції як перенавантаження можуть виявитись не прийнятними з погляду вимог процесу до експлуатаційної готовності.<br>Відключення повинні плануватись завчасно, за декілька днів/тижнів.<br>Висока експлуатаційна готовність вимагає широких випробувань перед введенням в експлуатацію |
| Вимоги у відношенні управління ризиком | Конфіденційність і цілісність являються головними вимогами.<br>Відмово стійкість менш важлива – короткочасне відключення не створює значного ризику.<br>Головним наслідком у плані ризику являється затримка виконання бізнес операцій | Головною вимогою являється безпека персоналу, а потім захист технологічного процесу.<br>Відмово стійкість вельми важлива, навіть короткочасне відключення не прийнятне.<br>Головними наслідками у плані ризику являється не дотримання регулюючих положень, втрата життя людей, обладнання або продукції |

| 1 | 2 | 3 |
|---|---|---|
| Питання фізичної безпеки, яким надається основна увага в архітектурі | Першочергова увага приділяється захисту активів ІТ та інформації, яка зберігається у цих активах або передається між нами.<br>Для центрального сервера може бути потрібною висока степінь захисту | Головною метою являється захист периферійних клієнтів (наприклад, таких периферійних пристроїв, як контролери технологічного процесу<br>захист центрального сервера також являється важливим |
| Не навмисні наслідки | Рішення по забезпеченню фізичної безпеки проектуються на основі технічної системи ІТ | Інструментальні засоби забезпечення фізичної безпеки повинні проходити тестування, з тим щоб гарантувати, що вони не створюють загрози нормальній роботі ПСУ |
| Взаємодія з критичними часовими параметрами | Менш критична взаємодія в аварійних ситуаціях.<br>Може бути здійснена з необхідній степені контролем доступу із жорсткими обмеженнями | Критично важливою є реакція на взаємодію людей та інші види взаємодії в аварійних ситуаціях.<br>Доступ до ПСУ слід строго контролювати, але при цьому не повинні створюватись перепони взаємодії «людина-машина» |
| Експлуатація системи | Системи проектуються для використання зі стандартними операційними системами.<br>Оновлення не являється складним при наявності автоматизованих засобів розгортання | Різні та розроблені по замовленню операційні системи, часто без можливостей забезпечення фізичної безпеки.<br>Зміни програмного забезпечення повинні проводитись обережно, за звичай постачальником програмного забезпечення, з погляду наявності спеціалізованих алгоритмів управління та можливості наявності змінених апаратних засобів та програмного забезпечення |

| 1 | 2 | 3 |
|---|---|---|
| Ресурсні обмеження | Системи задаються з достатніми ресурсами для підтримки додавання сторонніх прикладних програм, таких як рішення по забезпеченню фізичної безпеки | Системи проектуються з метою підтримки запланованого виробничого процесу з мінімальною пам'яттю та обчислювальними ресурсами в підтримку додавання технології фізичної безпеки |
| Системи зв'язку | Стандартні комунікаційні протоколи.<br>Головним чином проводові мережі з певними локалізованими можливостями безпроводового зв'язку.<br>Типова практика роботи з мережами IT | Численні спеціалізовані та стандартні комунікаційні протоколи<br>Використовується декілька типів засобів комунікацій, включаючи спеціалізовані проводові мережі без проводові (радіо та супутникові) комунікації.<br>Мережі являються складними та іноді вимагають експертних знань інженерів з систем управління |
| Управління змінами | Змінення програмного забезпечення здійснюється своєчасно за наявності хорошої політики та процедур фізичної безпеки. Процедури часто автоматизовані | Змінення програмного забезпечення повинно повністю піддаватись тестуванню і проводитись у системі поступово з метою збереження цілісності системи управління. Відключення ПСУ часто повинні плануватись та розподілятись за графіком завчасно, за декілька днів/тижнів |
| Комплексна підтримка | Допускаються різноманітні стилі підтримки | Сервісна підтримка здійснюється за звичай здійснюється єдиним постачальником |
| Термін служби компонентів | Термін служби складає прядка 3 – 5 років | Термін служби складає прядка 15 – 20 років |
| Доступ до компонентів | Компоненти за звичай локалізовані й легкодоступні | Компоненти можуть бути ізольованими, віддаленими і вимагати значних фізичних зусиль для отримання доступу до них |

### 3. Управління процесами аудиту кібербезпеки

Цикли важливі при вирішенні практичних задач кібербезпеки. Циклічність і прогнозування за допомогою минулих циклів майбутніх станів складають суть сучасного підходу до процесно-орієнтованого управління.

У стандарті ISO 9001:2008 сформульовані вимоги до системи менеджменту якості, щодо постійного поліпшення її результативності на основі процесно-орієнтованого підходу [21]. Всім процесам виробництва продукції чи послуг в організації притаманні певні відхилення від заданих значень внаслідок багатьох причин. Для зниження відхилень виробництва застосовують в управлінні, наприклад, концепцію PDCA (плануй (Plan), роби (Do), перевіряй (Check), дій (Act)). Результативність процесів забезпечується управляючим зворотним зв'язком по критерію, який необхідно поліпшити із заданою точністю.

Основними елементами циклу PDCA є (рис. 3):

P – визначення цілей та прийняття рішення щодо необхідних змін (розробляння плану);

D – здійснення змін (втілення плану);

C – вимірювання та аналіз результатів (контроль виконання плану);

A – проведення необхідних дій, якщо результати не відповідають запланованим, або стандартизація дій у випадку успіху (виправляння плану).


**Рис. 3. Цикл постійного поліпшення системи менеджменту якості згідно стандарта ISO 9001:2008**

У міжнародному стандарті ISO 9000 дано таке визначення: «Процес – це сукупність взаємозв'язаних або взаємодіючих видів діяльності, які перетворюють входи у заплановані виходи». Процес управління – це певна сукупність управлінських дій, які направлені на досягнення цілей шляхом перетворення ресурсів на «вході» (фінансові, матеріально-технічні та кадрові) у потрібний результат забезпечення життєдіяльності на «виході» системи. В середині процесу відбувається застосування та переробка матеріальних або фінансових потоків, інформації в інші потоки або послуги. Аналіз та поліпшення виконують по відношенню до процесу в цілому для досягнення цілі в умовах, що склалися.

Усе, що отримано на виході процесу, має бути перевірено. Для прийняття рішення власник процесу повинен отримати інформацію про хід процесу, про результати процесу та інформацію від споживача, щодо степені його задоволеності продуктом. Власник процесу контролює із встановленою періодичністю хід процесу та приймає рішення у випадках відхилення ходу процесу від нормального. Власник процесу в ході управління планує (Plan) розподіл ресурсів для досягнення цілей процесу з максимальною ефективністю. В ході виконання (Do) процесу власник перевіряє (Check) хід процесу на основі інформації, яка поступає в результаті вимірювання параметрів процесу. Власник процесу веде оперативне управління процесом, коригуючи (Act), змінюючи хід процесу. Діяльність власника процесу носить циклічний характер при нормальному ході процесу або аперіодичний – у випадках виникнення проблемних ситуацій, які вимагають термінового втручання. Процес – це модель реальної діяльності. Для того, щоб процедура виконувалася правильно й ефективно, всі ці етапи повинні безупинно, послідовно й циклічно повторюватися. Останнім часом такі цикли називають кібернетичними. Кібернетичні цикли управління знаходять застосування у процесах проведення аудиту кібербезпеки.

При управлінні інформаційною безпекою використовують процеси оцінки ризиків інформаційної безпеки, організації і експлуатації захисних заходів, навчання персоналу інформаційній безпеці та інші. Серед них визначальними є процеси контролю та перевірки інформаційної безпеки. Аудит займає особливе місце в системі забезпечення інформаційної безпеки об'єкта інформаційної діяльності, який формує незалежну оцінку інформаційної безпеки. Своєчасність, точність і повнота оцінок інформаційної безпеки, отриманих у результаті ауди-

ту, дають змогу виявити вразливості системи, скоригувати їх, щоб удосконалити процеси забезпечення інформаційної безпеки.

Результативність, надійність та об'єктивність висновків за результатами аудиту забезпечуються чітким дотриманням принципів проведення аудиту, таких як: відповідальність, обачність, неупередженість, непідкупність та уміння зберігати таємницю та інших.

Використання ризико-орієнтованого підходу до планування заходів аудиту є одним з можливих варіантів збільшення ефективності аудиту (рис. 4).

Аудит може бути зовнішнім та внутрішнім за методами проведення.

Зовнішній аудит – разовий захід та проводиться за ініціативою керівництва сторонньою організацією відповідної кваліфікації. Висновки за результатами цього аудиту використовуються для покращення якості процесів організації. Проводити його слід регулярно.

Для самооцінки стану інформаційної безпеки силами самої організації проводиться внутрішній аудит, тобто проводиться пошук слабких місць, покращення якості процесів організації, оцінка ступеня відповідності системи забезпечення безпеки вимогам діючих нормативно-правових документів. Ця діяльність є безперервною і затверджується керівництвом організації.

Аудит починається з процедури ініціації. На цьому етапі повинні бути визначені межі проведення обстеження, до яких відносяться переліки: фізичних осіб, ресурсів, приміщення, основні види загроз, організаційні, фізичні та програмно-технічні аспекти забезпечення інформаційної безпеки.

Найскладніший та найтриваліший етап це збирання інформації аудиту, тому що саме на цьому етапі проводиться вивчення документації та тісна взаємодія аудитора з посадовими особами організації.

Далі аудитори повинні виконати аналіз даних, при цьому можна використовувати один із трьох методів.

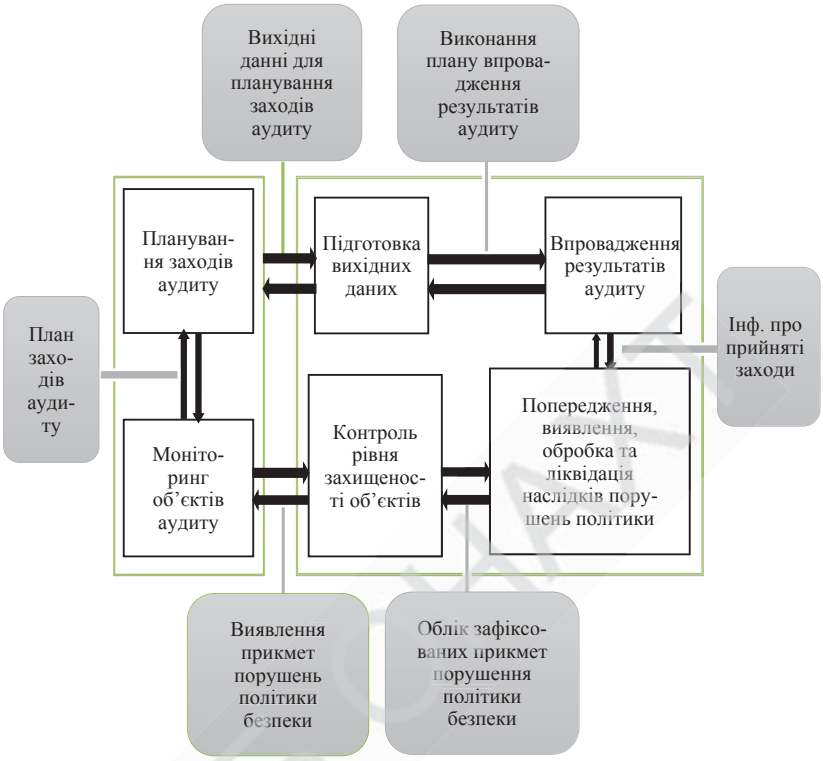



**Рис. 4. Схема реалізації ризико-орієнтованого підходу до планування заходів аудиту**

Перший підхід, який базується на аналізі ризиків – найскладніший, трудомісткий та вимагає найвищої кваліфікації аудитора, тому що необхідно визначити індивідуальний набір вимог інформаційної безпеки, що враховує особливості середовища її функціонування та існуючі загрози інформаційної безпеки.

Другий підхід – практичний та опирається на використання стандартів інформаційної безпеки, які визначають базовий набір вимог інформаційної безпеки. Стандарти можуть визначити різні набори вимог залежно від рівня захищеності, приналежності та призначення.

Третій підхід припускає комбінування перших двох. Він є найефективніший. Базовий набір вимог інформаційної безпеки визнача-

ється стандартом, додаткові вимоги формуються а основі аналізу ризиків.

Четвертий підхід складний і найбільш відповідальний. Аналіз ризиків – це те, з чого повинна починатися побудова будь-якої системи інформаційної безпеки. Він полягає у виявленні існуючих ризиків та їх оцінки якісної або кількісної.

Далі проводиться оцінка відповідності вимогам стандартів. Виявляться вимоги інформаційної безпеки, які не реалізовані в системі. Виходячи з цього, робляться висновки про відповідність.

Вироблення рекомендацій за наслідками аналізу, які повинні бути конкретними, економічно обґрунтованими, аргументованими (підкріпленими результатами аналізи) і відсортованими за ступенем важливості.

Підготовка звітних документів, які повинні містити опис цілей проведення аудиту, характеристику обстеження, вказівку границь проведення аудиту та методів. Звіт є основним результатом проведення аудиту, якість якого характеризує якісь роботи аудитора.

Завдяки циклічній схемі управління процесом аудит функціонує в контурі із зворотним зв'язком. Тоді, мається певне запізнювання, можуть проявлятись різні нелінійні явища. Ці явища можуть негативно впливати на надійність системи аудиту і всієї системи управління кібербезпекою.

Сучасна теорія нелінійних динамічних систем надає просунуті методи їх дослідження. Перейдемо до розгляду характеру можливого впливу нелінійності на роботу систем управління аудитом кібербезпеки.

## 4 Пристосування математичної моделі циклічного управління до процесів управління аудитом

### *4.1 Виведення експериментальних модельних формул*

Подібна задача вирішувалась стосовно циклічного управління кібербезпекою в [див. 8] і стосовно управління колективною та індивідуальною свідомістю громадян у [див. 9]. «Ефективність людської дії здебільшого залежить від правильного управлінського рішення, що, у свою чергу, залежить від інформаційного моделювання ситуації, від пошуку потрібної інформації та її переробки. Лавиноподібне зростання інформаційних потоків, у яких змішувались потрібна і непотрібна інформація («інформаційні шуми»), у значній мірі утруднив поведінку людини та висунув на передній план вибірковий пошук потрібної

інформації з наступною її редукцією для прийняття тих чи інших рішень [22, с. 142]».

В процесі аудиту збирається, обробляється і генерується інформація щодо загроз, механізмів захисту, дій персоналу тощо. Інформація поступає у вигляді документів, повідомлень, які утворюють дискретний потік. Тому модель має формуватись не за допомогою аналогових диференційних рівнянь, а за допомогою, так званих, дискретних відображень. Нас цікавлять такі найпростіші моделі, які можна розв'язувати цифровими методами [23].

Процеси навколишнього світу бувають лінійні і нелінійні. Фізичні процеси часто описують лінійними функціями. Але нелінійних залежностей у природі значно більше. Зокрема, соціальні, економічні, психологічні процеси, як правило, нелінійні. Тому математична модель процесів управління аудитом інформаційної безпеки має бути нелінійною.

Найпростішими нелінійними функціями є квадратичні або гіперболічні функції. Оберемо найпростіші нелінійні дискретні відображення, які описані Малінецьким [24] і вперше були досліджені Фейгенбаумом.

Будемо розглядати деякий аналітичний процес управління від моменту часу, коли на початку циклу управління в момент $t_0$ на вхід управляючого елемента системи подавався вектор вхідних сигналів $\mathbf{X}_0 = \{x_{01}, x_{02}, ...\}$, обчислено результат $\mathbf{S}_0$, на виході управляючого елемента системи маємо вектор вихідних сигналів $\mathbf{Y}_0(S_0)$. Припустимо, що сума $\mathbf{S}$ та вихідний сигнал $\mathbf{Y}_0(S_0)$ запам'ятовується у системі. Саме така вимога необхідна, щоб інтелектуальна динамічна система не «забувала» свою, принаймні найближчу, історію [25].

Функціонал перетворень в управляючому циклі нам невідомий. Щоб вивчити вклад управляючого елемента в процес управління, будемо вважати, що, у найпростішому випадку, всі інші перетворення в управляючому однозначні і мають адитивний характер. Тоді, в кінці циклу управління в момент часу $t_1$, після закінчення перехідних процесів, маємо вектор вхідних сигналів $\mathbf{X}_1 = \{x_{11}, x_{12}, ...\}$, встановлюється сума $S_1$, на виході управляючого елемента системи маємо вихідний сигнал $Y_1(S_1)$. При цьому, $S_1 = S_0 + s_{in}$, де $s_{in}$ – зміна суми $S$ під впливом потоку управління. Потік управління може бути постійним, періодичним; хаотичним або шумовим тощо.

Задамо найпростіше нелінійне правило переходу від $Y_0(S_0)$ до $Y_1(S_1)$ таким чином, щоб зміна суми $S$ за один крок в одному управляючому елементі циклу записувалася так:

$$S_1 = \frac{dy}{dS} = \alpha S_0 (1 - S_0) + s_{in}. \quad (1)$$

Провівши ітераційні перетворення, у загальному вигляді отримуємо формулу

$$S_{n+1} = \alpha S_n (1 - S_n) + s_{in}, \quad (2)$$

де $n$ – номер ітерації, яке можна вважати модельним часом;

α – параметр, який називають коефіцієнтом росту.

Таким чином, отримано одномірне дискретне відображення із вхідним потоком. Якщо $s_{in} = 0$, то маємо одномірне дискретне відображення, яке наливають *логістичним відображенням* і яке ретельно проаналізоване у численних публікаціях [див. 24]. Зокрема відомо, що при невеликих значеннях α ($0 < \alpha < 1$) $S_n \to 0$ при $n \to \infty$, незалежно від вибору початкового значення $S_0$. Існують нерухомі точки, для яких справедлива рівність

$$S^* = \alpha S^* (1 - S^*). \quad (3)$$

При $\alpha < 1$ квадратне рівняння (3) має один невід'ємний корінь $S^* = 0$. Нерухома точка стійка. При $\alpha > 1$ невід'ємних коренів два: $S^* = 0$ і $S^* = (\alpha - 1) / \alpha$. При $\alpha = 1$ нерухома точка $S^* = 0$ втрачає стійкість, а нова нерухома точка стає стійкою. При цьому, із збільшенням α виникають коливання. Управляючий елемент буде видавати по черзі два рішення: числа. При подальшому збільшенні α виникають наступні біфуркації подвоєння періоду за сценарієм Фейгенбаума та детермінований хаос.

Тепер розглянемо найпростішу модель циклового інформаційного процесу управління, який складається з двох етапів:

- аналізу інформаційного потоку даних аудиту (відбір потрібної інформації, редукція, консолідація, переробка) – $x_{in}$. Інтенсивність дискретного інформаційного потоку управляючого елемента цього етапу позначимо за $x$;

- прийняття рішень та обробки вихідного інформаційного потоку для корекції заходів захисту (формування та видача управлінського

рішення) – $x_{out}$. Інтенсивність дискретного інформаційного потоку управляючого елемента цього етапу позначимо за y.

Врахуємо прямі та зворотні зв'язки між управляючими елементами циклу за допомогою коефіцієнтів двох типів.

Коефіцієнти *p, q* характеризують синтаксичну обробку інформації (формати, списки, таблиці тощо).

Коефіцієнти $k_{ij}$ характеризують семантичну обробку інформації, коли робляться висновки, нові рішення, виникає нова інформація. Після простих перетворень нашу математичну модель динамічної системи Ф(*x*, *y*) приводять до такого вигляду:

$$\Phi(x, y)=\begin{cases} x_{n+1} = x_n - k_{xy} p x_n^2 + k_{yx} q y_n^2 + x_{in} \\ y_{n+1} = y_n + k_{xy} p x_n^2 - (k_{yx} + k_{out}) q y_n^2 \end{cases}, \quad (4)$$

де *x, y* – динамічні змінні, які визначають інтенсивність інформаційних елементів потоку на етапах обробки інформації; $k_{ij}$ – перехідні коефіцієнти, що характеризують динамічну взаємодію етапів обробки інформації; *p, q* – розподільчі коефіцієнти, $x_{in}$ – інтенсивність інформаційних елементів потоку, що поступають на перший етап обробки; причому, $\{k_{ij}\}$ и $\{p, q\} \in (0,1)$, $\{x, y\} \in R$, $x_{in} = const \in R^+$.

Наявність у системі двох груп коефіцієнтів ($k_{ij}$ та *p, q*) має конкретну фізичну інтерпретацію: коефіцієнти $k_{ij}$ описують відносну величину редукції і консолідації інформації за синтаксичними ознаками, наприклад, форматами відомостей і повідомлень, та задають долю інформаційного потоку, який переходить з одного етапу на сусідній.

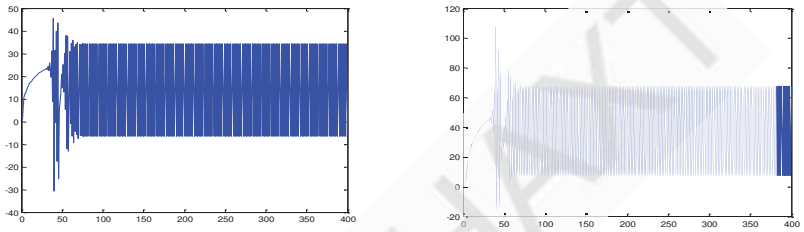
Частина інформаційного потоку переходить на попередній етап обробки для виправлення неточностей, врахування зауважень тощо. Коефіцієнти *p, q* описують розподіл елементів інформаційного потоку за їх видами по семантичним ознакам, наприклад, по змісту. Перехід між етапами обробки у нелінійній системі визначається добутком коефіцієнтів обох груп.

Методи дослідження дискретних відображень проаналізовані у численних публікаціях [див. 24]. Авторами було проведено вирішення системи дискретних відображень чисельними методами. Розглянемо результати експериментів.

***4.2 Результати математичних експериментів.***

Процедури аналізу динамічних систем включають перевірку всіх траєкторій на стійкість та виявлення початкових умов, за яких траєк-

торії потрапляють в околи кожної з нерухомих точок. У даному випадку доцільно встановлювати початкові умови виходячи із практичних міркувань – на початку моделювання на всіх етапах обробки інформації руху немає і здійснюється включення вхідного потоку заданої інтенсивності. Тому, для відображення рівнянь руху чисельно вирішуємо систему рівнянь (4) при початкових умовах: $x_0 = 0$; $y_0 = 0$. Графіки рівнянь руху у вигляді проекцій на площини 0*xt*, 0*yt* при тих же значеннях коефіцієнтів системи рівнянь (4), інтенсивності вхідного потоку $x_{in} = 4{,}94$ показані на рис. 5.



**а** **б**

**Рис. 5. Графіки рівнянь руху в проекціях на площини: а – 0*xt*; б – 0*yt***

Рішення мають три характерні ділянки: початкова, турбулентна і усталена (при заданих значеннях параметрів – квазіперіодична). Початкова ділянка (модельний час *t* у проміжку від 0 до 30 одиниць) відрізняється плавним зростанням величини інтенсивності потоку. Початкова ділянка тим довша, чим менша інтенсивність вхідного потоку.

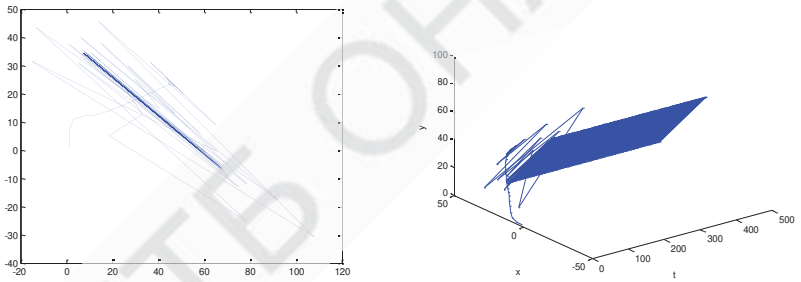
Турбулентна ділянка на графіках рис. 5 триває у проміжку від 30 до 70 модельних одиниць, характеризується хаотичними коливаннями, викиди досягають великих значень і при збільшенні інтенсивності вхідного потоку прямують до нескінченності.

Турбулентності у цій моделі, за даних параметрів виникають при $x_{in} > 4{,}94$. Поступово хаотичні коливання затухають і замінюються стаціонарними квазіперіодичними коливаннями. В усталеній ділянці, в залежності від величин параметрів системи, відбуваються біфуркації подвоєння періоду Фейгенбаума. Періодичні коливання змінюються на квазіперіодичні а потім – динамічним хаосом [26, с. 184].

Причиною виникнення коливань і турбулентності являються зворотні зв'язки у кожному з етапів обробки інформації та перехідні процеси при включенні потоку. Потік не може вирости миттєво і наростає плавно, а потім виникає турбулентність.

***4.3 Турбулентні перехідні процеси***

Коливальний характер процесів системи (4) тісно пов'язаний з турбулентними явищами перехідного періоду. Ці явища мають у своїй основі причину – наявність у системі позитивних зворотних зв'язків. Для більш детального аналізу турбулентної ділянки процесу обробки інформаційного потоку в системі (4) розглянемо фазовий портрет системи у перехідному і стаціонарному режимах. Значення коефіцієнтів системи та початкові умови залишаються тими ж. На рис. 6 а представлена проекція багатовимірного фазового портрета на площину 0*xy*, тобто атрактор, а на рис. 6 б – його проекція на трьохвимірний простір 0*xyt*. Останнє дозволяє прослідкувати еволюцію траєкторії до атрактору.

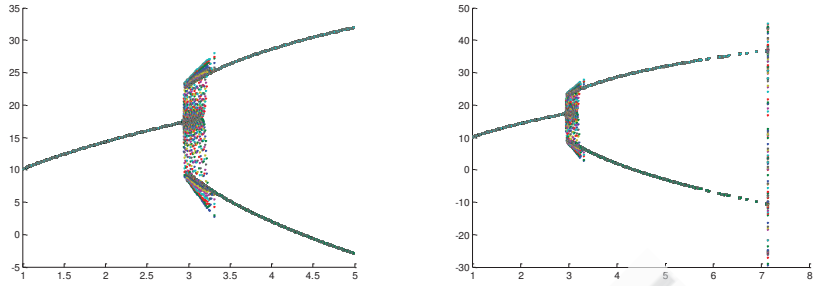



**а** **б**

**Рис. 6. Перехідний процес:**
**а – атрактор системи; б – його еволюція**

У турбулентному режимі спостерігаються хаотичні траєкторії. У стаціонарному режимі маємо атрактор.

Розглянемо структурну стійкість системи. Для дослідження структурної стійкості системи вивчені біфуркаційні діаграми, приклад яких показано на рис. 7. Перша біфуркація співпадає з виникненням турбулентності. Навколо стійкої і нестійкої гілок біфуркації виникають хаотичні коливання (так званий «чубчик»).




**а** **б**

**Рис. 7. Біфуркаційна діаграма: а – при $x_{in}$ в інтервалі [1, 5]; б – при $x_{in}$ в інтервалі [1, 8]**

Деякі траєкторії мають спрямовуються до нескінченності. У моделі вони досягають –NaN або +NaN (мінус і плюс машинної нескінченності). Такі траєкторії в моделі «гинуть». Траєкторії, що вижили, можуть існувати і при другій біфуркації подвоєння періоду. Але при збільшенні інтенсивності вхідного потоку траєкторій, які вижили, стає все менше. Тому дослідження другої біфуркації у цій моделі, з наявними комп'ютерними ресурсами, практично неможливо. Можна припустити, що друга біфуркація також супроводжується турбулентністю. На рис. 7 б видно залишки «чубчика» на другій біфуркації.

Таким чином, турбулентність динамічних систем типу системи (1), для яких характерна наявність позитивних зворотних зв'язків, визначаються природними властивостями цих систем. Турбулентність виникає як при включенні вхідного інформаційного потоку, так і при його виключенні. Управління вхідним потоком не змінює якісний характер турбулентності, який визначається властивостями системи (1), але дозволяє зменшити величину викидів.

Отримані в даній роботі результати, застосовні у багатьох областях. Наприклад, силова установка автомобіля на холостих обертах може викликати сильні коливання корпусу автомобіля, навіть якщо він стоїть на місці. Під час руху збільшуються потужність і оберти двигуна, а трясіння корпуса зникає і далі залежить лише від нерівностей дороги. Процеси виводу на повну потужність крупних енергетичних агрегатів, атомних реакторів тощо та їх зупинка також проявляють ознаки нестійкості.

Таким чином, можна визначити інтервал значень параметрів нормального функціонування нелінійного процесу у складі циклічної системи управління аудитом. При виході за межі цих інтервалів виникають біфуркації, що виражаються у появі періодичних, а потім нерегулярних коливань, а далі у появі детермінованого хаосу.

**Висновки**

Проведено уточнення поняття «кібербезпека», яке здійснено відносно розширення об'єктів забезпечення кібербезпеки у порівнянні з поняттям «інформаційної безпеки».

Найпростіша дискретна математична модель динаміки циклічного процесу пристосована до обробки даних аудиту, яка описує два етапи: етап аналізу інформаційного потоку даних аудиту (відбір потрібної інформації, редукція, консолідація, переробка); та етап прийняття рішень й обробки вихідного інформаційного потоку для корекції заходів захисту (формування та видача управлінського рішення).

У системі аудиту кібербезпеки для своєї безперервної роботи, яка управляється за принципами кібернетичних циклів управління, можливі порушення нормальної їх роботи із-за впливу нелінійності при високій інтенсивності процесів. Тоді, ці явища можуть негативно впливати на надійність функціонування системи аудиту кібербезпеки.

Можна визначити інтервал значень параметрів нормального функціонування процесу аудиту кібербезпеки складі циклічної системи управління. При виході за межі цих інтервалів виникають біфуркації, що виражаються у появі періодичних, а потім нерегулярних коливань а далі детермінованого хаосу.

Проведене дослідження моделі динамічних систем з двохрівневим потоком показало, що в них можуть виникати стаціонарні квазіперіодичні коливання, біфуркації, а в перехідний період можливі турбулентність і сингулярність.

Отримані результати дозволяють підвищити ефективність роботи циклічних систем управління обробкою інцидентів інформаційної безпеки.

Напрямом подальшої роботи буде детальний аналіз моделі динаміки процесів аудиту кібербезпеки.

**Список використаної літератури**

1. Бурячок, В.Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / В. Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. – К.: ДУТ, 2015. – 288 с.

2. Соколов М.С. Кибернетическая безопасность – понятие, значение и эволюция от военных основ к самостоятельному виду безопасности // Военное право. – 2012. – № 1. – 24 с. – Режим доступу: http://db.inforeg.ru/eni/artList.asp?j=4&id=0220913464&idfull=0421200099

3. Архипов, А. Приставка кибер-: все ли очевидно? / Александр Архипов // Захист інформації. Том 18, №3. – 2016. – С. 203-209.

4. Руководство по передовой практике защиты важнейших объектов неядерной энергетической инфраструктуры от террористических актов в связи с угрозами, исходящими от киберпространства / Антитеррористическое подразделение Департамента по противодействию транснациональным угрозам Секретариата ОБСЕ. – ОБСЕ: Vienna, Austria, 2013. – 96 с.

5. Курило А.П. Аудит информационной безопасности / Курило А.П., Зефиров С.Л., Голованов В.Б. / М.: Издательская группа «БДЦ-пресс». – 2006. – 304 с.

6. Аудит та управління інцидентами інформаційної безпеки : навч. посіб. /[Корченко О.Г., Гнатюк С.О., Казмірчук С.В. та ін.]. – К.: Центр навч.-наук. та наук.-пр. видань НА СБ України, 2014. 190 с.

7. Тардаскіна Т.М., Кононович В.Г. Менеджмент інформаційної безпеки в галузі зв'язку: навч. посібник. Затверджено Міністерством освіти та науки України як навчальний посібник для студентів вищих навчальних закладів [Лист № 1/11-7791 від 13 серпня 2010 року] / – Одеса: ОНАЗ, – 2010. – 268 с.

8. Кононович В.Г. Нелінійні моделі циклічного управління кібербезпекою / В.Г. Кононович, І.В. Кононович, А.І. Міхова // «Інформаційні управляючі системи та технології» (ІУСТ – ОДЕСА – 2015). Матеріали Міжнародної науково-практичної конференції, 22-24 вересня 2015 р., Одеса / відп. ред. В.В. Вичужанін. – 2015. – 336 с. – С. 171-173.

9. Кононович В.Г. Модель системы информационной безопасности консолидированной информации при информационном противоборстве (Раздел 16) / В.Г. Кононович, И.В. Кононович // Информационные технологии и защита информации в информационно-коммуникационных системах : монография / под редакцией

В.С. Пономаренко – Х. : Вид-во ТОВ «Щедра садиба плюс», 2015. – 486 с. – С. 220-233.

10. В.Ф. Ситник Системи підтримки прийняття рішень: Навч. посіб. – К.: КНЕУ, 2009. – 614 с.

11. Орлов А.И. Теория принятия решений. Учебное пособие / А.И.Орлов. – М.: Издательство Экзамен, 2005. – 656 с. – Режим доступа: http://www.aup.ru/books/m157/1_1.htm

12. Прохоров С.А., Федосеев А.А., Иващенко А.В. Автоматизация комплексного управления безопасностью предприятия / Самара: СНЦ РАН, 2008 – 55 с.

13. Кононович В.Г. Технічна експлуатація систем захисту інформації телекомунікаційних мереж загального користування. Частина 4 – Інформаційна безпека комунікаційних мереж та послуг. Реагування на атаки: навч. посібник / В.Г. Кононович, С.В. Гладиш; За ред. чл.-кор. МАЗ В.Г. Кононовича. – Одеса: ОНАЗ ім. О.С. Попова, 2009. – 208 с.

14. Круг П. Г. Нейронные сети и нейрокомпьютеры: Учебное пособие по курсу «Микропроцессоры». – М.: Издательство МЭИ, 2002. – 176 с.

15. Кононович, В.Г. Вплив нелінійності нейрона на циклічну систему управління / В.Г. Кононович, О.Ю. Козлова, О.Ю. Кунянський // Інформатика та математичні методи моделювання. – Одеса. – 2016. Том 6. № 3. – С. 290-296.

16. Козлова О.Ю., В.Г. Динамічні властивості процесів забезпечення кібербезпеки на прикладі аудиту кібербезпеки / О.Ю. Козлова, В.Г. Кононович, І. В. Кононович, М.Г. Романюков, Л.М. Тимошенко // Інформатика та математичні методи моделювання. – Одеса. – 2017. Том 7. № 3. – С. 205-212.

17. Про Основні засади забезпечення кібербезпеки України. Наказ від 05.10.2017 р. за № 2163-19 [Електронний ресурс] // Законодавство України – Режим доступу http://zakon3.rada.gov.ua/laws/show/2163-19

18. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки. Наказ від 09.01.2007 р за № 537-16 [Електронний ресурс] // Законодавство України – Режим доступу http://zakon0.rada.gov.ua/laws/show/537-16

19. Марков А.С. Руководящие указания по кибербезопасности в контексте ISO 27032 / А.С. Марков, В.Л. Цирлов // Вопросы Кибербезопасности, № 1(2), 2014. – С. 28-25.

20. МАГАТЕ STI/PUB/1527 «Компьютерная безопасность на ядерных установках. Справочное руководство // Технические руково-

дящие материалы». – МАГАТЭ, Вена, 2012 (Серия изданий МАГАТЭ по физической ядерной безопасности № 17). – 90 с.

21. 21 ДСТУ ISO 9001:2009 Системи менеджменту якості. Вимоги [Аналог ISO 9001:2008]. – 32 с.

22. Информационная безопасность системы организационного управления. Теоретические основы : в 2 т. / Н.А. Кузнецов, В.В. Кульба, Е.А. Микрин и др.; [отв. ред. Н.А. Кузнецов, В.В. Кульба] ; Ин-т проблем передачи информ. РАН. – М.: Наука, 2006. Т.1 – 495 с.

23. Шампайн Л.Ф. Решение обыкновенных дифференциальных уравнений с использованием МАТЛАБ: Учебное пособие / Л.Ф. Шампайн, И. Гладвел, С. Томпсон. Пер. с англ. – СПб.: Издательство «Лань», 2009. – 304 с. (Учебники для вузов. Специальная литература).

24. Малинецкий Г.Г. Математические основы синергетики. Хаос, структуры, вычислительный эксперимент. / Г.Г. Малинецкий. – М.: КомКнига, 2005. – 312 с.

25. Лачинов В.М. Информодинамика или Путь к Миру открытых систем / [Електронний ресурс] В.М. Лачинов, А.О. Поляков. – СПб: Издат. СПбГТУ, 1999. – С. 364. (Санкт-Петербургский институт информатики и автоматизации). – Режим доступу: http://www.polyakov.com/informodynamics/index.html. – Назва з екрану.

26. Табор М. Хаос и интегрируемость в нелинейных системах / Табор Михал. Пер. с англ. – М.: Эдиториал УРСС, 2001. – 320 с.

*Наукове видання*

**Міжнародний конкурс студентських наукових робіт**

# BLACK SEA SCIENCE 2018

Матеріали



Верстка – Н.М. Ковальчук

Формат 60х84/16. Гарнітура Times New Roman.
Умовно-друк. арк. 48,07. Тираж 300. Замовлення № 0518-105.

Видавництво і друкарня – Видавничий дім «Гельветика»
73034, м. Херсон, вул. Паровозна, 46-а, офіс 105
Телефон +38 (0552) 39 95 80
E-mail: mailbox@helvetica.com.ua
Свідоцтво суб'єкта видавничої справи
ДК № 4392 від 20.08.2012 р.