БЕЗПЕКА ІНФОРМАЦІЇ

2020, vol. 26, issue 2

http://infosecurity.nau.edu.ua; http://jrnl.nau.edu.ua/index.php/Infosecurity

Alternative serial title: ***Ukrainian Scientific Journal of Information Security***

ISSN 2225-5036 (Print), ISSN 2411-071X (Online)

Key title: ***Bezpeka ìnformacìì***

Abbreviated key title: ***Bezpeka ìnf.***

Науковий журнал «Безпека інформації» засновано у 1995 році. Засновником та видавцем є Національний авіаційний університет (м. Київ, Україна). Основною метою журналу є висвітлення результатів наукових досліджень та поширення інформації з усіх аспектів інформаційної безпеки. Журнал виходить три рази на рік українською, англійською та російською (змішаними) мовами. Категорії читачів: студенти, аспіранти, докторанти, викладачі, науковці та фахівці у галузі інформаційної безпеки. У журналі можуть публікуватися виключно оригінальні, раніше не опубліковані статті у галузі інформаційної безпеки. Усі статті, опубліковані у журналі, рецензуються членами редакційної колегії або уповноваженими експертами. Редакція може не поділяти думок авторів. Відповідальність за науковий зміст поданих матеріалів несуть виключно автори.

Ukrainian Scientific Journal of Information Security was established in 1995. National Aviation University (Kyiv, Ukraine) is the founder and publisher of the journal. The main aim of the journal is to highlight the results of scientific researches and the dissemination of information on all information security aspects. Journal is published three times (issues) a year in Ukrainian, English & Russian (mixed languages). Categories of readers: students, postgraduate students, doctoral candidates, researchers & experts in information security. Journal publishes only original unpublished articles in information security. All papers published in journal are reviewed by members of Editorial Board or by appointed experts. Editorial Board may disagree with the authors. Authors are responsible for the scientific content of submitted materials.

Научный журнал «Безопасность информации» основан в 1995 году. Учредителем и издателем является Национальный авиационный университет (г. Киев, Украина). Основной целью журнала является освещение результатов научных исследований и распространение информации по всем аспектам информационной безопасности. Журнал выходит три раза в год на украинском, английском и русском (смешанных) языках. Категории читателей: студенты, аспиранты, докторанты, преподаватели, ученые и специалисты в области информационной безопасности. В журнале могут публиковаться исключительно оригинальные, ранее не опубликованные статьи в области информационной безопасности. Все статьи, опубликованные в журнале, рецензируются членами редакционной коллегии или уполномоченными экспертами. Редакция может не разделять мнений авторов. Ответственность за научное содержание представленных материалов несут исключительно авторы.

Зареєстровано Державною реєстраційною службою України (Свідоцтво КВ № 18940-7730 ПР від 25 травня 2012 р.)

Рекомендовано до друку Вченою радою Національного авіаційного університету (протокол № 5 від 1 липня 2020 р.)

Включено до **категорії «Б»** переліку наукових фахових видань України, в яких можуть публікуватися результати дисертаційних робіт на здобуття наукових ступенів доктора (кандидата) технічних наук (Наказ МОН України № 975 від 11.07.2019).

ABSTRACTED / INDEXED IN: EBSCO*host*, INDEX COPERNICUS, CrossRef, Google Scholar, Ukrainian Journal of Abstracts «Dzherelo», Russian Science Citation Index (eLIBRARY.RU), Simple Search Metadata (SSM), Bielefeld Academic Search Engine (BASE), WorldCat (OAIster), ISSN & Ulrich's Periodicals Directory.

Редакційна колегія

Адреса редакційної колегії

03680, УКРАЇНА, м. Київ
проспект Космонавта Комарова, 1
Національний авіаційний університет
Кафедра безпеки інформаційних технологій
корпус 11, кімната 422, телефон: +38 (044) 406-70-22
Головний редактор проф. Корченко Олександр Григорович
Ел. пошта: ***infosecurity@nau.edu.ua***

Editorial board

Editorial Address

03680, Kyiv, UKRAINE
Kosmonavta Komarova ave. 1
National Aviation University
Academic Department of IT-Security
Building 11, Room 422, Phone: +38 (044) 406-70-22
Editor-in-Chief Prof. Oleksandr G. Korchenko
E-mail: ***infosecurity@nau.edu.ua***

Зміст

Contents

© Saliieva O., Yaremchuk Yu. Cognitive model for studying the level of protection of a critical infrastructure object // Ukrainian Scientific Journal of Information Security, 2020, vol. 26, issue 2, pp. 64-73.

КІБЕРБЕЗПЕКА ТА ЗАХИСТ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ / CYBERSECURITY & CRITICAL INFORMATION INFRASTRUCTURE PROTECTION

DOI: 10.18372/2225-5036.26.14915

КОГНІТИВНА МОДЕЛЬ ДЛЯ ДОСЛІДЖЕННЯ РІВНЯ ЗАХИЩЕНОСТІ ОБ'ЄКТА КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Ольга Салієва, Юрій Яремчук

Вінницький національний технічний університет

САЛІЄВА Ольга Володимирівна

Рік та місце народження: 1982 рік, м. Вінниця, Україна.
Освіта: Вінницький державний педагогічний інститут ім. М. Коцюбинського, 2004 рік; Вінницький національний технічний університет, 2018 рік.
Посада: аспірантка кафедри менеджменту та безпеки інформаційних систем з 2016 року.
Наукові інтереси: нечітка математика, безпека інформаційних систем.
Публікації: більше 20 наукових публікацій, серед яких наукові статті, матеріали і тези доповідей на наукових конференціях, свідоцтва про реєстрацію авторського права на твір.
E-mail: salieva8257@gmail.com.
Orcid ID: 0000-0003-2388-7321.

ЯРЕМЧУК Юрій Євгенович, д.т.н., професор

Рік та місце народження: 1974 рік, м. Вінниця, Україна.
Освіта: Вінницький національний технічний університет, 1996 рік.
Посада: директор Центру інформаційних технологій та захисту інформації, професор кафедри менеджменту та безпеки інформаційних систем, з 2010 року.
Наукові інтереси: криптографічний та стеганографічний захист інформації, технічний захист інформації, безпека інформаційних систем.
Публікації: понад 270 публікацій, у тому числі 2 монографії, 140 статей у наукових фахових виданнях, 20 підручників та навчальних посібників, автор 20-ти патентів на корисну модель та 20-х свідоцтв про реєстрацію авторського права на твір.
E-mail: yurevyar@vntu.edu.ua.
Orcid ID: 0000-0002-6303-7703.

Анотація. *Для вирішення питань щодо забезпечення захищеності об'єктів критичної інфраструктури необхідно проаналізувати потенційні загрози, дослідити взаємозв'язки між ними та визначити вплив даних загроз на досліджувану систему. При цьому з'являються деякі труднощі пов'язані із високим ступенем невизначеності, складністю строгої формалізації та суб'єктивним характером даних задач. У зв'язку з цим у роботі пропонується використання когнітивного підходу, який не потребує великого обсягу експериментальних даних, надає можливість опрацьовувати доступну експерту інформацію та враховувати як якісні так і кількісні фактори. На основі даного підходу було створено когнітивну модель, яка базуються на нечіткій когнітивній карті та дозволяє дослідити вплив потенційних загроз на рівень захищеності об'єкта критичної інфраструктури. Здійснено оцінювання структурно-топологічних властивостей нечіткої когнітивної карти, визначено її щільність, індекс ієрархії та центральність концептів. Із сформованої експертним шляхом множини концептів виділено найбільш вагомі. Проведено сценарне моделювання впливу даних концептів на захищеність об'єкта критичної інфраструктури. Дані отримані у результаті запуску відповідних сценаріїв дозволяють дослідити відносну зміну досліджуваної системи та сприяють ефективному вирішенню питань щодо підвищення рівня захищеності об'єктів критичної інфраструктури.*

Ключові слова: *інформаційна безпека, критична інфраструктура, загрози безпеці, когнітивне моделювання, нечітка когнітивна карта.*

Вступ

Стратегічно важливим для функціонування економіки і безпеки держави, суспільства та населення є захист об'єктів критичної інфраструктури (КІ) – підприємств та установ (незалежно від форми власності) таких галузей, як енергетика, хімічна промисловість, транспорт, банки та фінанси, інформаційні технології та телекомунікації (електронні комунікації), продовольство, охорона здоров'я, комунальне господарство, виведення з ладу або руйнування яких може мати вплив на національну безпеку і оборону, природне середовище, призвести до значних матеріальних та фінансових збитків, людських жертв [1]. У свою чергу, інформатизація об'єктів КІ викликає безліч ризиків, пов'язаних із порушенням функціонування інформаційних систем КІ, що може призвести до розвитку надзвичайних ситуацій, пов'язаних з великомасштабним порушенням життєдіяльності як окремих міст, так і усієї держави в цілому. Тому варто звернути особливу увагу на забезпечення інформаційної безпеки об'єктів КІ, враховуючи вплив потенційних загроз.

Вивчення даного питання відображається у роботах як українських, так і зарубіжних вчених. Зокрема, у роботі [2] розглянуто особливості забезпечення кібербезпеки об'єктів КІ. Автори роботи [3] здійснили аналіз факторів впливу на стан кібербезпеки інформаційної системи об'єкта КІ.

У роботі [4] запропоновано графічний та аналітичний методи оцінювання сумарного ризику кібербезпеки об'єктів КІ у результаті дії множини кіберзагроз.

Автором роботи [5] проаналізовано потенційні негативні наслідки, до яких може призвести кібератака на інформаційно-телекомунікаційну систему об'єкта КІ та запропоновано єдиний класифікатор таких наслідків.

У роботі [6] науковці розглянули принципи оцінювання ефективності дій зловмисника на об'єктах КІ та представили «операційний комплекс» моделювання процесів порушення інформаційної безпеки КІ.

Автори праці [7] запропонували нову технологію аналізу кіберзагроз та оцінювання ризиків порушення кібербезпеки КІ, що базується на використанні авторської інтелектуальної системи. Дана технологія включає етапи виявлення кіберзагроз; моделювання сценаріїв екстремальних ситуацій, викликаних реалізацією кіберзагроз; оцінювання ризиків і ранжування активів інформаційно-комунікаційної системи об'єкта КІ за ступенем їх критичності, і дозволяє виконати оцінювання кількості критично вразливих активів, обгрунтувати склад та ймовірність реалізації кіберзагроз.

Таким чином, значна увага приділяється дослідженням пов'язаним із забезпеченням безпеки об'єктів КІ при впливі на них ймовірних загроз. Причому дана задача характеризується високим ступенем невизначеності, складністю строгої формалізації та має суб'єктивний характер. Тому для її вирішення доцільно скористатися когнітивним підходом, який базується на побудові нечіткої когнітивної карти (НКК), тобто орієнтованого графа, вершини (концепти) якого представляють системні змінні, а зважені дуги відображають силу впливу одного концепта на інший [8]. У роботах [9] та [10] запропоновано когнітивні моделі, які дозволяють аналізувати вплив загроз на рівень захищеності комп'ютерної мережі та системи захисту інформації відповідно. Однак дані моделі є доволі вузькими, тому не можуть повною мірою відобразити предметну область КІ. Отже, актуальним є дослідження можливості побудови когнітивної моделі для оцінювання та прогнозування впливу потенційних загроз на рівень захищеності об'єкта КІ.

Мета роботи

Побудувати когнітивну модель для дослідження рівня захищеності об'єкта КІ.

Постановка задачі

Для досягнення поставленої мети необхідно:

– визначити структуру НКК предметної області (тобто склад її концептів та причинно-наслідкові зв'язки між ними);

– визначити силу впливу між кожною парою концептів;

– побудувати модель на основі НКК для дослідження рівня захищеності об'єкта КІ;

– визначити структурно-топологічні властивості розробленої НКК;

– визначити найвпливовіші концепти досліджуваної системи;

– провести сценарне моделювання для аналізу впливу найвагоміших загроз на рівень захищеності об'єкта КІ.

Побудова когнітивної моделі на основі НКК для дослідження рівня захищеності об'єкта КІ.

Дослідимо об'єкт КІ, який відноситься до класу об'єктів, що передбачає доступ до мережі Інтернет та відображає максимальне представлення структурних складових. Сформуємо множину загроз даному об'єкту, відмітивши, що основні напрями вектора атак направлені на ІТ-інфраструктуру та операційні технології [11]. Причому, велика кількість загроз спрямована на систему контролю та збору даних (SCADA) та на розподілені системи управління (DCS), які надають життєво важливі послуги КІ [12].

Доцільно виділити такі категорії загроз, на які має бути налаштовано захист КІ [13]:

– аварії й технічні збої, зокрема авіаційні катастрофи, ядерні аварії, пожежі, аварії у системах енергозабезпечення, викиди небезпечних речовин, відмови систем, аварії та надзвичайні події, зумовлені недбалістю, організаційними помилками тощо;

– небезпечні природні явища, зокрема надзвичайні погодні умови, лісові, степові й торф'яні пожежі, сейсмічні явища, епідемії та пандемії, космічні явища, урагани, торнадо, землетруси, цунамі, повені тощо;

– зловмисні дії, зокрема зловмисні дії груп або окремих осіб, таких як терористи, злочинці й диверсанти, а також бойові дії в умовах війни.

Особливо небезпечними є комбіновані загрози й загрози, реалізація яких може призвести до катастрофічних і різноманітних каскадних ефектів унаслідок взаємозалежності елементів КІ.

Загрози КІ можна розглядати не лише з огляду на характер їх походження, а й на елементи КІ, на які ці загрози спрямовані [13]:

– фізичні елементи, зокрема обладнання й ресурси об'єктів КІ;

– системи управління та комунікації, зокрема автоматизованих систем управління та систем зв'язку;

– персонал об'єктів, зокрема диспетчерський, оперативний, який безпосередньо забезпечує функціонування КІ у реальному часі.

У результаті проведення експертами аналізу можливих загроз безпеці КІ було сформовано множину найвагоміших, з точки зору вивчення даної проблеми, концептів:

– K_1 – природні явища;

– K_2 – техногенний вплив;

– K_3 – соціально-політичний вплив;

– K_4 – економічний вплив;

– K_5 – правовий вплив;

– K_6 – військове вторгнення;

– K_7 – терористичний вплив;

– K_8 – промислове шпигунство;

– K_9 – хакерський вплив;

– K_{10} – вплив управлінських рішень та організаційних заходів;

– K_{11} – інсайдерський вплив;

– K_{12} – безпека каналів зв'язку КІ;

– K_{13} – надійність, відмовостійкість складових КІ;

– K_{14} – захищеність КІ;

– K_{15} – захищеність системи безпеки;

– K_{16} – захищеність комп'ютерної мережі;

– K_{17} – безпека центру управління;

– K_{18} – безпека обслуговуючих систем та обладнання;

– K_{19} – безпека обслуговуючого персоналу;

– K_{20} – захищеність сховищ даних;

– K_{21} – захищеність хмарних серверів;

– K_{22} – безпека інформаційної інфраструктури;

– K_{23} – безпека Інтернет-додатків;

– K_{24} – безпека Інтернет;

– K_{25} – мережеві атаки;

– K_{26} – шкідливі програми;

– K_{27} – DoS-атаки.

Вплив загроз на K_{15} – захищеність системи безпеки та K_{16} – захищеність комп'ютерної мережі можна здійснювати на основі моделей, представлених у роботах [9, 10].

Наступним кроком є визначення сили впливу $w_{ij} \in [-1;1]$, що відображає зміни одного концепта K_i на зміну іншого K_j. Вирішення даної задачі здійснюється експертним шляхом за допомогою лінгвістичних термів та відповідних їм числових діапазонів.

Задамо нечітку лінгвістичну шкалу:

СИЛА ЗВ'ЯЗКУ = {Не впливає; Дуже слабка; Слабка; Середня; Сильна; Дуже сильна}.

Кожному з цих термів поставимо у відповідність деякий числовий діапазон:

$$w_{ij} = \begin{Bmatrix} (0{,}85;1], \ позитивна\ дуже\ сильна; \\ (0{,}6;0{,}85], \ позитивна\ сильна; \\ (0{,}35;0{,}6], \ позитивна\ середня; \\ (0{,}15;0{,}35], \ позитивна\ слабка; \\ (0;0{,}15], \ позитивна\ дуже\ слабка; \\ 0, \ не\ впливає; \\ (0;-0{,}15], \ негативна\ дуже\ слабка; \\ (-0{,}15;-0{,}35], \ негативна\ слабка; \\ (-0{,}35;-0{,}6], \ негативна\ середня; \\ (-0{,}6;-0{,}85], \ негативна\ сильна; \\ (-0{,}85;-1], \ негативна\ дуже\ сильна \end{Bmatrix}.$$

При позитивній силі зв'язку зростання концепта-причини призводить до збільшення концепта-наслідка, а при негативній – до зменшення.

Визначивши склад концептів та силу впливу причинно-наслідкових зв'язків між ними, побудуємо НКК для дослідження рівня захищеності об'єкта КІ (рис. 1).

Моделювання виконано з використанням засобів програмного забезпечення Mental Modeler [14].

Розглянемо матрицю $W = \left\lfloor w(K_i, K_j) \right\rfloor_{n \times n}$ взаємовпливів концептів даної НКК (табл. 1-2).

Визначимо структурно-топологічні властивості розробленої НКК, проаналізувавши такі показники структурної складності НКК як щільність, індекс ієрархії та центральність концептів:

а) щільність (коефіцієнт кластеризації) – показує ступінь зв'язності графа, який відображає дану НКК:

$$d = \frac{m}{n \cdot (n-1)}, \quad (1)$$

де m – загальна кількість зв'язків НКК, а n – загальна кількість концептів НКК.

У нашому випадку $n = 27$, $m = 128$, підставивши відповідні значення у формулу (1), отримаємо, що $d = 0{,}18$. Дане значення вказує на достатню складність розробленої моделі. Чим вище значення щільності, тим більше потенційних політик управління.

б) індекс ієрархії (h): $h = \frac{12 \cdot \sigma_{od}^2}{n^2 - 1}$, де

$$\sigma_{od}^2 = \frac{\sum_{i=1}^{n} (od_i - \mu_{od})^2}{n}, \ \mu_{od} = \frac{\sum_{i=1}^{n} od_i}{n}.$$

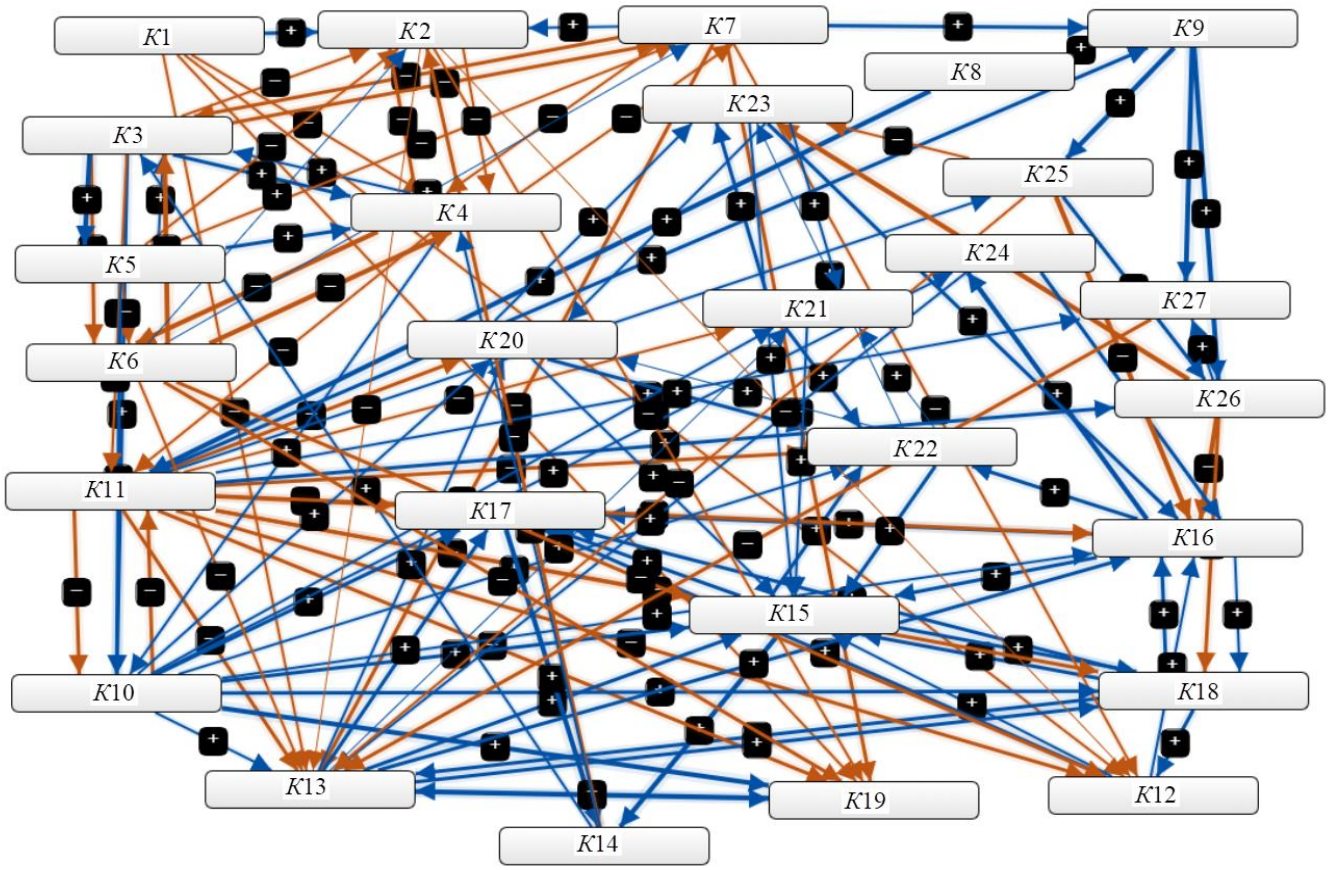


Рис. 1. НКК для дослідження рівня захищеності об'єкта КІ

Таблиця 1

Матриця взаємовпливів концептів НКК предметної області на концепти $K_1 - K_{15}$

	K_1	K_2	K_3	K_4	K_5	K_6	K_7	K_8	K_9	K_{10}	K_{11}	K_{12}	K_{13}	K_{14}	K_{15}
K_1	0	0,55	0	-0,4	0	0	0	0	0	0	0	-0,2	-0,3	0	0
K_2	0	0	0	-0,4	0	0	0	0	0	0	0	-0,1	-0,15	0	0
K_3	0	-0,35	0	0,7	0,85	-0,7	-0,5	0	0	0,75	-0,2	0	0	0	0
K_4	0	-0,5	0,3	0	0	-0,87	-0,4	0	0	0,35	-0,35	0	0	0	0
K_5	0	-0,4	0,4	0,55	0	-0,4	-0,4	0	0	0,8	-0,1	0	0	0	0
K_6	0	0,1	-0,85	-0,85	0	0	0,1	0	0	0	0	-0,5	-0,4	0	0
K_7	0	0,2	-0,5	-0,2	0	0	0	0	0,8	0	0	-0,3	-0,55	0	0
K_8	0	0	0	0	0	0	0	0	0,7	0	0,9	0	0	0	0
K_9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
K_{10}	0	0	0	0	0	0	0	0	0	0	-0,7	0	0,2	0	0,7
K_{11}	0	0	0	0	0	0	0	0	0,8	-0,6	0	-0,6	-0,75	0	-0,8
K_{12}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,4
K_{13}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,55
K_{14}	0	-0,6	0,35	0,4	0	0	0	0	0	0	0	0	0	0	0
K_{15}	0	0	0	0	0	0	0	0	0	0	0	0	0	0,95	0
K_{16}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,5
K_{17}	0	0	0	0	0	0	0	0	0	0	0	0	0	0,95	0
K_{18}	0	0	0	0	0	0	0	0	0	0	0	0,7	0,5	0	0,8

K_{19}	0	0	0	0	0	0	0	0	0	0	0	0	0,7	0	0
K_{20}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,35
K_{21}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,35
K_{22}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,6
K_{23}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,4
K_{24}	0	0	0	0	0	0	0	0	0	0	0	0	0,35	0	0
K_{25}	0	0	0	0	0	0	0	0	0	0	0	0	-0,2	0	0
K_{26}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
K_{27}	0	0	0	0	0	0	0	0	0	0	0	0	-0,6	0	0

Таблиця 2

Матриця взаємовпливів концептів НКК предметної області на концепти $K_{16} - K_{27}$

	K_{16}	K_{17}	K_{18}	K_{19}	K_{20}	K_{21}	K_{22}	K_{23}	K_{24}	K_{25}	K_{26}	K_{27}
K_1	0	0	0	-0,2	0	0	0	0	0	0	0	0
K_2	0	0	0	-0,4	0	0	0	0	0	0	0	0
K_3	0	0	0	0	0	0	0	0	0	0	0	0
K_4	0	0	0	0	0	0	0	0	0	0	0	0
K_5	0	0	0	0	0	0	0	0	0	0	0	0
K_6	0	0	0	-0,75	0	0	0	0	0	0	0	0
K_7	0	0	0	-0,55	0	0	0	0	0	0	0	0
K_8	0	0	0	0	0	0	0	0	0	0	0	0
K_9	0	0	0	0	0	0	0	0	0	0,9	0,9	0,9
K_{10}	0,4	0,7	0,6	0,9	0,4	0,2	0,25	0	0,4	0	0	0
K_{11}	-0,8	-0,8	-0,8	-0,6	-0,6	-0,4	-0,8	0	0	0,3	0,5	0,2
K_{12}	0,3	0,65	0	0	0	0	0	0	0	0	0	0
K_{13}	0,55	0,55	0,8	0,55	0,2	0,1	0	0	0	0	0	0
K_{14}	0	0	0	0	0	0	0	0	0	0	0	0
K_{15}	0	0,8	0,6	0	0	0	0,6	0	0	0	0	0
K_{16}	0	0,6	0,4	0	0	0	0,7	0	0,85	0	0	0
K_{17}	0	0	0	0	0	0	0	0	0	0	0	0
K_{18}	0,8	0,8	0	0	0	0	0	0	0	0	0	0
K_{19}	0	0	0	0	0	0	0	0	0	0	0	0
K_{20}	0	0	0	0	0	0	0,8	0,4	0	0	0	0
K_{21}	0	0	0	0	0	0	0,55	0,8	0	0	0	0
K_{22}	0	0	0	0	0,15	0,1	0	0,1	0	0	0	0
K_{23}	0,75	0	0	0	0,3	0,2	0	0	0	0	0	0
K_{24}	0,75	0	0	0	0	0	0	0	0	0	0	0
K_{25}	-0,9	0	0	0	0	0	0	-0,25	0	0	0,7	0
K_{26}	-0,9	0	-0,65	0	0	0	0	-0,85	0	0	0	0,2
K_{27}	0	0	0	0	0	0	0	0	0	0	0	0

При $h=1$ система є повністю ієрархічною, при $h=0$ – повністю демократичною. Демократичні системи більш адаптивні до змін зовнішнього середовища завдяки високому рівню їх інтеграції та зв'язності. У нашому випадку $\mu_{od}=2{,}51,\quad \sigma^2_{od}=3{,}13$, тоді $h=0{,}16$, що свідчить про високу демократичність досліджуваної системи.

в) центральність концепта – характеризує ступінь взаємодії і-го концепта НКК з його сусідами:

– вихідна центральність – показує сукупну силу зв'язків (w_{ij}), що виходять з аналізованого концепта K_i:

$$od_i=\sum_{j=1}^{n} w_{ij};$$

– вхідна центральність – показує сукупну силу зв'язків (w_{ij}), що входять до аналізованого концепта K_i:

$$id_i=\sum_{j=1}^{n} w_{ij};$$

– загальна центральність концепта: $td_i=od_i+id_i.$

Розрахунок показників центральності показав, що найбільш високу структурну значимість має концепт K_{11} $(td_i=11{,}6)$, а також концепти $K_{16}, K_{15}, K_{13}, K_{10}$ (показники $td_{16,}\ td_{15}, td_{13}, td_{10}$ рівні відповідно 9,2; 8,39; 8,0; 7,95). Дані концепти акумулюють найбільшу кількість зв'язків від інших концептів, тобто відіграють роль своєрідних центрів впливу у НКК для дослідження рівня захищеності об'єкта КІ. Зазначимо, що найменшу структурну значимість відіграє концепт K_8 $(td_i=1{,}6)$.

Сценарне моделювання для оцінювання впливу найвагоміших загроз на рівень захищеності об'єкта КІ.

Сценарний аналіз дозволяє отримати прогноз розвитку досліджуваної ситуації, визначити, оцінити і знизити рівень невизначеності впливу найвагоміших концептів, що впливають на захищеність об'єкта КІ. Це, у свою чергу, сприятиме формуванню стратегічних управлінських рішень щодо підсилення захисту об'єкта КІ. Метод побудови сценаріїв найбільш повно дозволяє проаналізувати вплив найвагоміших загроз на рівень захищеності об'єкта КІ в умовах невизначеності та мінливості оточуючого середовища.

Сценарій 1. Змоделюємо ситуацію, при якій спостерігатиметься максимальне збільшення інсайдерського впливу (K_{11}) на захищеність об'єкта КІ.

Зауважимо, що численні дослідження, проведені у останні роки, показують, що більше 80% усіх інцидентів, пов'язаних з порушенням інформаційної безпеки, викликані внутрішніми загрозами. Джерелами таких загроз, що спричиняють порушення конфіденційності інформації, є, як правило, інсайдери, тобто особи, що мають через свій службовий стан доступ до інформації обмеженого доступу або ж співробітники, які намагаються його отримати [15].

При максимальному інсайдерському впливі спостерігатиметься така реакція досліджуваної системи (рис. 2).

Аналізуючи отриману стовпчасту діаграму можна зробити висновок, що найбільше зменшиться значення концептів K_{16} – захищеність комп'ютерної мережі (на 0,24) та K_{18} – безпека обслуговуючих систем та обладнання (на 0,21). Крім того, значно погіршиться K_{13} – надійність, відмовостійкість складових КІ (на 0,17), K_{22} – безпека інформаційної інфраструктури (на 0,16), K_{17} – безпека центру управління (на 0,14), K_{19} – безпека обслуговуючого персоналу (на 0,13), K_{12} – безпека каналів зв'язку КІ (на 0,12), K_{15} – захищеність системи безпеки (на 0,12) та K_{20} – захищеність сховищ даних (на 0,12). Проте K_{14} – захищеність КІ послабиться лише на 0,03.

Для попередження негативних наслідків необхідно особливу увагу приділяти основним компонентам комплексної системи організованих заходів й технічних засобів захисту від інсайдерів, а саме [16]:

– нормативно-правовій базі;

– системі контролю та управління персоналізованим доступом до корпоративних ресурсів КІ;

– моніторингу дій користувачів інформації;

– використанню технічних засобів, що здійснюють контроль й очистку комп'ютерних систем;

– кадровому забезпеченню (обов'язкова наявність штатного спеціаліста, що забезпечує захист від внутрішніх загроз);

– забезпеченню відповідного рівня корпоративної культури, що впливає на підвищення рівня корпоративної безпеки КІ;

– ретельній підбір кадрів, що матимуть доступ до інсайдерської інформації;

– формування ефективного мотиваційного механізму для працівників.

Реалізація зазначених заходів допоможе зменшити інсайдерський вплив та підвищити рівень захищеності КІ.

Сценарій 2. Розглянемо як зміниться стан досліджуваної системи при максимальному послабленні концепта K_{16} – захищеність комп'ютерної мережі.

Відмітимо, що комп'ютерна мережа є базисом для функціонування інформаційних систем у різних сегментах діяльності об'єкта КІ. Адже вона забезпечує передавання даних і комунікацію між автоматизованими вузлами даного об'єкта, управління правами доступу до інформаційних ресурсів і безпосередньо впливає на ефективне впровадження та застосування інформаційних технологій. Тому цікаво змоделювати даний сценарій для аналізу відносної зміни рівня системи (рис. 3).

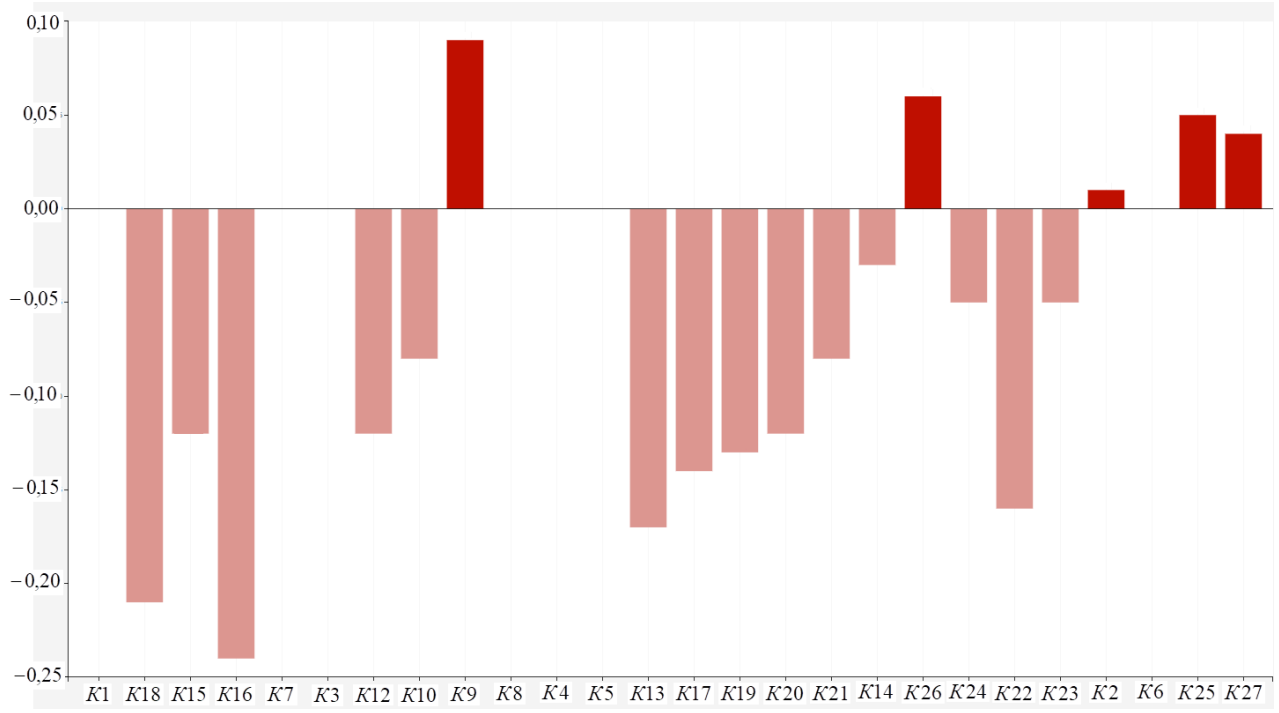


Рис. 2. Реакція досліджуваної системи на максимальний інсайдерський вплив

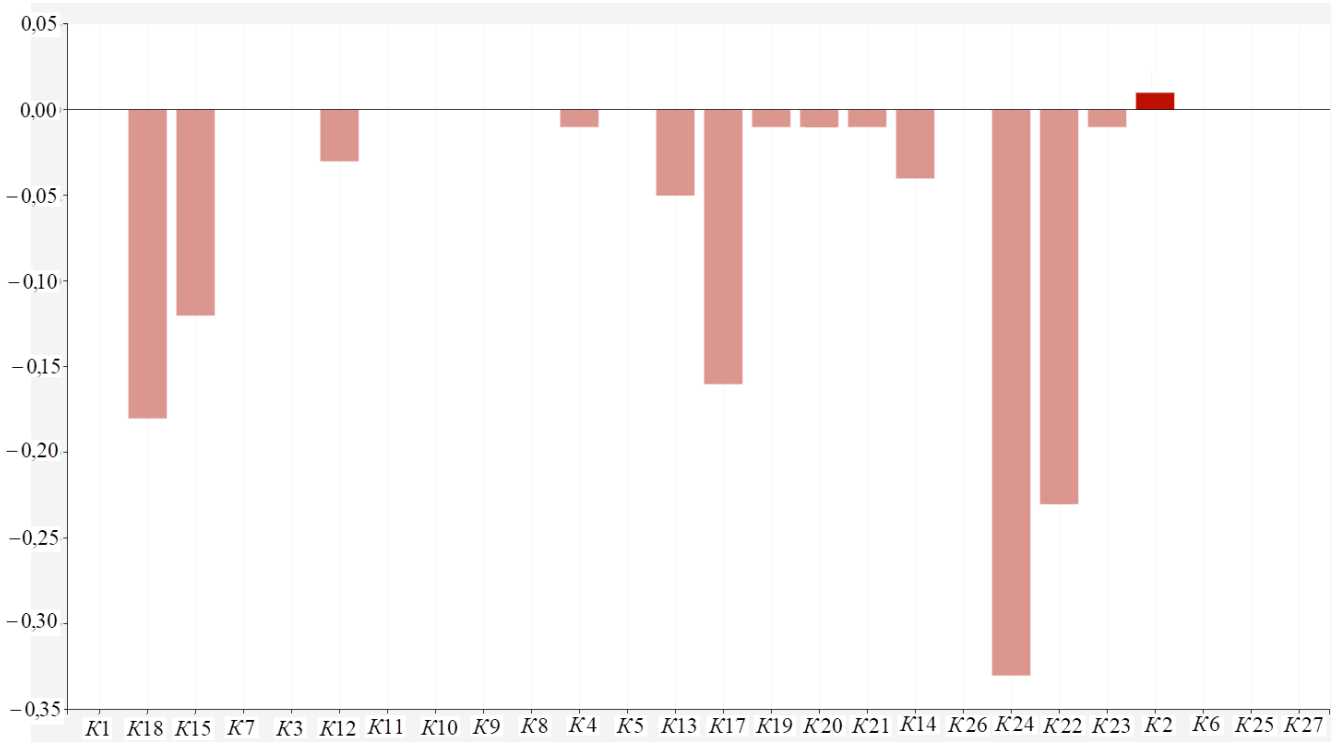


Рис. 3. Реакція досліджуваної системи при максимальному послабленні захисту комп'ютерної мережі

Дослідивши отриману гістограму, можна зробити висновок, що при максимальному послабленні захисту комп'ютерної мережі найбільше зменшаться значення концептів: K_{24} – безпека Інтернет (на 0,33), K_{18} – безпека обслуговуючих систем та обладнання (на 0,28), K_{22} – безпека інформаційної інфраструктури (на 0,25), K_{17} – безпека центру управління (на 0,24) та K_{15} – захищеність системи безпеки (на 0,18). Значення інших концептів системи зміняться не суттєво. При цьому K_{14} – захищеність КІ послабиться на 0,06.

Щоб запобігти вищезазначеним негативним наслідкам необхідно впроваджувати та застосовувати ефективні механізми і засоби для забезпечення мережевої безпеки на об'єктах КІ, які захищатимуть мережу від несанкціонованого доступу, випадкового або навмисного втручання у її роботу або спроб руйнування її компонентів.

Сценарій 3. Змоделюємо ситуацію, яка відображатиме зміни концептів системи при максимально можливому послабленні захищеності системи безпеки.

Основною метою створення системи безпеки на об'єктах КІ є попередження та нейтралізація загроз, реалізація яких може призвести до порушення функціонування складових КІ, що, у свою чергу, може негативно вплинути на загальнодержавну, екологічну та суспільну безпеку. Дана система проводить комплексні адміністративно-правові, інформаційно-аналітичні, організаційно-управлінські, та інші заходи, спрямовані на забезпечення стійкого функціонування об'єктів КІ.

Розглянемо реакцію досліджуваної системи на максимально негативну зміну концепта K_{15} – захищеність системи безпеки (рис. 4).

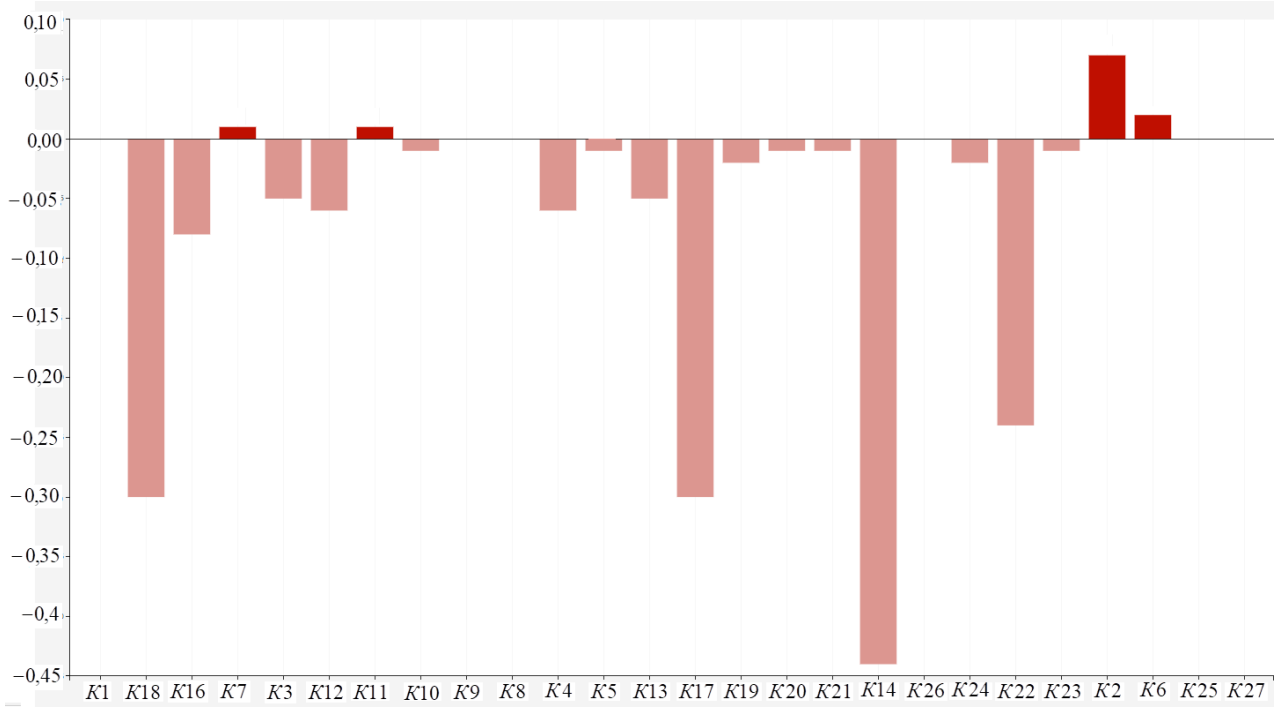


Рис. 4. Реакція досліджуваної системи при максимальному послабленні захищеності системи безпеки

Проаналізувавши отриману стовпчасту діаграму, можна зробити висновок, що при максимальному послабленні захищеності системи безпеки спостерігатиметься найбільша вразливість захищеності критичної інфраструктури, адже значення даного концепта знизиться на 0,44. При цьому безпека інформаційної інфраструктури (K_{22}) послабиться на 0,24, а безпека обслуговуючих систем та обладнання (K_{18}) і безпека центру управління (K_{17}) – кожна на 0,3. Для попередження даної ситуації необхідно особливу увагу приділити захищеності системи безпеки, послаблення якої може призвести до вкрай негативних наслідків функціонування об'єктів КІ, що у результаті спровокує небезпечний вплив на навколишнє середовище та людство в цілому.

Таким чином, розроблена когнітивна модель для дослідження рівня захищеності об'єкта КІ дозволяє прослідкувати відносну зміну досліджуваної системи на зміни тих чи інших концептів, визначивши найвагоміші з них. На основі результатів сценарного моделювання можна розробити чіткий план управління спрямований на підвищення захищеності об'єктів КІ, які є стратегічно важливими для розвитку держави.

Висновки

Побудовано когнітивну модель дослідження рівня захищеності об'єкта КІ. На основі проведеного аналізу показників структурної складності НКК, визначено структурно-топологічні властивості розробленої моделі. Встановлено значення коефіцієнта кластеризації НКК ($d = 0{,}18$), яке свідчить про достатню складність розробленої моделі. Визначено індекс ієрархії ($h = 0{,}16$), що відображає високу демократичність досліджуваної системи. Розраховано показники центральності, за допомогою яких встановлено, що найбільш високу структурну значимість має концепт K_{11} ($td_i = 11{,}6$), а також концепти K_{16}, K_{15}, K_{13}, K_{10} (показники центральності яких відповідно рівні 9,2; 8,39; 8,0; 7,95).

Проведено сценарне моделювання для визначення відносної зміни досліджуваної системи при максимально негативному впливі найвагоміших концептів. Проаналізувавши отримані результати, можна зробити висновок, що захищеність КІ максимально знизиться (на 0,44) якщо найбільшою мірою послабиться захищеність системи безпеки. При зростанні інсайдерського впливу спостерігатиметься, у першу чергу, погіршення захищеності комп'ютерної мережі (на 0,24) та безпеки обслуговуючих систем та обладнання (на 0,21). У свою чергу, при максимальному послабленні захисту комп'ютерної мережі найбільше знизиться безпека Інтернет (на 0,33), безпека обслуговуючих систем та обладнання (на 0,28), безпека інформаційної інфраструктури (на 0,25) та безпека центру управління (на 0,24).

На основі аналізу отриманих даних можна запобігти порушенню режимів функціонування ключових елементів об'єктів КІ, що, у свою чергу, може призвести до розвитку надзвичайних ситуацій, здатних паралізувати життєдіяльність як окремих міст, так і усієї держави в цілому.

Література

[1]. Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави: Постанова КМУ від 23.08.2016 р. № 563 . *Офіційний вісник України*. 2016. №69.

[2]. С. Гончар, "Особливості забезпечення кібербезпеки об'єктів критичної інфраструктури", *Моделювання та інформаційні технології*, Вип. 80, С. 27-32, 2017.

[3]. С. Гончар, Г. Леоненко, "Аналіз факторів впливу на стан кібербезпеки інформаційної системи об'єкту критичної інфраструктури", *Information technology and security*, Vol. 4, issue 2 (7), С. 262-268, 2016.

[4]. В. Мохор, С. Гончар, О. Дибач, "Методи оцінки сумарного ризику кібербезпеки об'єктів критичної інфраструктури", *Ядерна та радіаційна безпека*, Вип. 2, С. 4-8, 2019.

[5]. Ю. Дрейс, "Аналіз базової термінології і негативних наслідків кібератак на інформаційно-телекомунікаційні системи об'єктів критичної інфраструктури держави", *Захист інформації*, Т. 19, № 3, С. 214-222, 2017.

[6]. И. Горбачев, А. Глухов, "Моделирование процессов нарушения информационной безопасности критической инфраструктуры", *Тр. СПИИ РАН*, Вып. 1 (38), С. 112–135, 2015.

[7]. Д. Гаськова, А. Массель, "Технология анализа киберугроз и оценка рисков нарушения кибербезопасности критической инфраструктуры", *Вопросы кибербезопасности*, №2(30), С. 42-49, 2019.

[8]. B. Kosko, "Fuzzy Cognitive Maps", *International Journal of Man-Machine Studies*, Vol. 24, No. 1, pp. 65-75, 1986.

[9]. О. Салієва, Ю. Яремчук, "Розробка когнітивної моделі для аналізу впливу загроз на рівень захищеності комп'ютерної мережі", *Реєстрація, зберігання і обробка даних*, №4, С. 28–39, 2019.

[10]. О. Салієва, Ю. Яремчук, "Визначення рівня захищеності системи захисту інформації на основі когнітивного моделювання", *Безпека інформації*, №1, С. 42-49, 2020.

[11]. А. Массель, Д. Гаськова, "Онтологический инжиниринг для разработки интеллектуальной системы анализа угроз и оценки рисков кибербезопасности энергетических объектов", *Онтология проектирования*, Т. 9, №2(32), С. 225-238, 2019.

[12]. A. Leandros, K. Ki-Hyung, J. Helge, "Cruz Cyber security of critical infrastructures", *ICT Express*, №4, pp. 42-45, 2018.

[13]. Д. Бірюков, С. Кондратов, О. Суходоля, *Зелена книга з питань захисту критичної інфраструктури в Україні*, К., 2016, 176 с.

[14]. S. Gray, J. De Kok, A.E.R. Helfgott, B. O'Dwyer, R. Jordan, A. Nyaki, "Using fuzzy cognitive mapping as a participatory approach to analyze change, preferred states, and perceived resilience of social-ecological sys-tems", *Ecology and Society*, 20(2):11, 2015. [Electronic resource]. Online access: http://www. ecologyandsociety. org/vol20/iss2/art11.

[15]. В. Козюра, В. Хорошко, "Заходи протидії прихованої передачі інформації в локальних мережах. Актуальні проблеми управління інформаційною безпекою держави", *зб. тез наук. доп. наук.-практ. конф., Київ : Нац. акад. СБУ*, С. 91-93, 2018.

[16]. В. Малащенко, "Теоретичні підходи до проблем та сучасних способів захисту від «інсайдерів»", *Ефективність державного управління*, Вип. 29, 2011. [Електронний ресурс]. Режим доступу: http://archive.nbuv.gov.ua/portal/soc_gum/Edu/2011_29/fail/malashchenko.pdf.

УДК 004.056.53

Салиева О.В., Яремчук Ю.Е. Когнитивная модель для исследования уровня защищенности объекта критической инфраструктуры

Аннотация. *Для решения вопросов по обеспечению защищенности объектов критической инфраструктуры необходимо проанализировать потенциальные угрозы, исследовать взаимосвязи между ними и определить влияние данных угроз на исследуемую систему. При этом появляются некоторые трудности связаны с высокой степенью неопределенности, сложности строгой формализации и субъективным характером данных задач. В связи с этим в работе предлагается использование когнитивного подхода, который не требует большого объема экспериментальных данных, дает возможность обрабатывать доступную экспертную информацию и учитывать, как качественные, так и количественные факторы. На основе данного подхода была создана когнитивная модель, которая основанная на нечеткой когнитивной карте и позволяет проанализировать влияние потенциальных угроз на уровень защищенности объектов критической инфраструктуры. Осуществлено оценивания структурно-топологических свойств нечеткой когнитивной карты, определены ее плотность, индекс иерархии и центральность концептов. С множества концептов выделены наиболее весомые. Проведено сценарное моделирование влияния данных концептов на защищенность объектов критической инфраструктуры. Данные получены в результате запуска соответствующих сценариев позволяют исследовать относительное изменение исследуемой системы и способствуют эффективному решению вопросов по повышению уровня защищенности объектов критической инфраструктуры.*

Ключевые слова: *информационная безопасность, критическая инфраструктура, угрозы безопасности, когнитивное моделирование, нечеткая когнитивная карта.*

Saliieva O., Yaremchuk Yu. Cognitive model for studying the level of protection of a critical infrastructure object
Abstract*. The protection of critical infrastructure is strategically important for the functioning of the economy and security of the state, society and the population. To address the protection of critical infrastructure, it is necessary to analyze potential threats, explore the relationships between them and determine the impact of these threats on the system under study. However, there are some difficulties associated with a high degree of uncertainty, the complexity of strict formalization and the subjective nature of these tasks. In this regard, the paper proposes the use of a cognitive approach, which does not require a large amount of experimental data, provides an opportunity to process the information available to the expert and take into account both qualitative and quantitative factors. Based on this approach, a cognitive model was created, which is based on a fuzzy cognitive map and allows to study the impact of potential threats on the level of protection of critical infrastructure. To build a fuzzy cognitive map, many of the most important critical infrastructure threats from the point of view of this problem have been formed and causal links have been established between them. The evaluation of structural and topological properties of fuzzy cognitive map is carried out, its density, hierarchy index and centrality of concepts are determined. From the set of expertly formed set of concepts, the most important ones are selected. To determine the relative change in the level of protection of the critical infrastructure, a scenario modeling of the impact of the most important concepts on the studied system was performed. Based on the analysis of the data obtained as a result of the launch of appropriate scenarios, it is possible to prevent disruption of key elements of critical infrastructure, which, in turn, can lead to emergencies that can paralyze the lives of individual cities and the state as a whole.*
Keywords: *information security, critical infrastructure, security threats, cognitive modeling, fuzzy cognitive map.*

Салієва Ольга Володимирівна, аспірантка кафедри менеджменту та безпеки інформаційних систем Вінницького національного технічного університету.
Салиева Ольга Владимировна, аспирантка кафедры менеджмента и безопасности информационных систем Винницкого национального технического университета.
Saliieva Olha, graduate student of the Department of Management and Security of Information Systems, Vinnytsia National Technical University.

Яремчук Юрій Євгенович, директор Центру інформаційних технологій та захисту інформації, професор кафедри менеджменту та безпеки інформаційних систем Вінницького національного технічного університету.
Яремчук Юрий Евгеньевич, директор Центра информационных технологий и защиты информации, профессор кафедры менеджмента и безопасности информационных систем Винницкого национального технического университета.
Yaremchuk Yurii, Director of the Center for Information Technologies and Information Protection, Professor of the Department of Management and Security of Information Systems, Vinnytsia National Technical University.

Отримано *15 липня 2020 року*, затверджено редколегією *10 серпня 2020 року*

© Tkach Yu. Trends in the development of modern cyber space and its security in conditions of information conflict // Ukrainian Scientific Journal of Information Security, 2020, vol. 26, issue 2, pp. 74-79.

DOI: 10.18372/2225-5036.26.14916

ТЕНДЕНЦІЇ РОЗВИТКУ СУЧАСНОГО КІБЕРПРОСТОРУ ТА ЙОГО ЗАХИЩЕНОСТІ В УМОВАХ ІНФОРМАЦІЙНОГО ПРОТИБОРСТВА

Юлія Ткач

Національний університет «Чернігівська політехніка»

ТКАЧ Юлія Миколаївна, д.пед.н., доцент

Рік та місце народження: 1979 рік, м. Чернігів, Україна.
Освіта: Чернігівський національний технологічний університет, 2012 рік; Чернігівський державний педагогічний університет ім. Т.Г. Шевченка, 2001.
Посада: завідувач кафедри кібербезпеки та математичного моделювання з 2010 р.
Наукові інтереси: інформаційна та кібербезпека.
Публікації: більше 80 наукових публікацій, серед яких, підручники, навчальні посібники, монографії, наукові статті та тези.
E-mail: tkachym79@gmail.com.
Orcid ID: 0000-0002-8565-0525.

Анотація. *У статті розглянуто актуальне питання формування кіберпростору та особливості його захисту. Визначено тенденції його розвитку в умовах інформаційного протиборства, а саме: інформаційна безпека напряму залежить від кібербезпеки, тобто політики безпеки, що реалізується у кіберпросторі; кіберпростір поступово перетворюється у п'ятий театр військових дій; для забезпечення переваги у кіберпросторі провідні країни світу починають формувати військово-мережевий комплекс; проблеми інформаційної безпеки у кіберпросторі та формування військово-мережевого комплексу приводять до перерозподілу повноважень існуючих гравців в сфері захисту інформації; надання послуг із захисту інформації у кіберпросторі стає новим видом бізнесу. Зроблено висновок, що в умовах, що сьогодні склались, тобто інформаційного протиборства, принципове значення має підтримка розробки і виробництва в Україні конкурентних інформаційно-комунікаційних засобів (у тому числі, з використанням вітчизняної мікроелектроніки, яку потрібно відновити та розвивати) та програмного забезпечення в інтересах українських користувачів, а також застосування таких засобів в Україні, і передусім, в оборонному комплексі і на об'єктах критичної цивільної інфраструктури, з метою протидії інформаційним впливам.*

Ключові слова: *інформаційне протиборство, інформаційний простір, кіберпростір, кібербезпека, інформаційна безпека.*

Актуальність

Стрімкий розвиток інформаційних технологій, надзвичайно висока активність засобів масових інформації в житті суспільства обумовили масштабні інформаційні впливи як на окрему людину, так і на цілі країни. Це в свою чергу спричинило появу нових технічних й психологічних засобів, які здатні впливати на психіку та свідомість окремої особистості й цілих націй. Таким чином, розпочалась ера інформаційного протиборства.

Аналіз останніх досліджень

У сучасній літературі проблема інформаційного протиборства розглядалась багатьма науковцями, зокрема Т. Батура, Горбулін В., Грищук Р., Р. Гумінський, Додонов О., Князєва Є., Д. Ланде, Молодецька К., Новиков Д., Почепцов Г., Пую А. , Розторгуєв С., Б. Хоган, Хорошко В., Чхартишвили А. та ін. Незважаючи на це, актуальними та малодослідженими залишись питання формування кіберпростору та визначення тенденцій його розвитку в сучасних умовах та врахування при цьому стану інформаційного протиборства.

Виділення невирішених раніше частин загальної проблеми

Незважаючи на численні дослідження у напрямку захисту інформації, досі залишаються не визначеними тенденції розвитку захищеного кіберпростору, особливо важливо це зробити в сучасних умовах інформаційного протиборства

Метою статті є визначення тенденції розвитку сучасного кіберпростору та особливостей його захищеності в умовах інформаційного протиборства.

Виклад основного матеріалу

В умовах інформаційного протиборства розвиток бездротових технологій та цифрової інфраструктури радикально змінило відношення людини зі своїм середовищем проживання та друг з другом. Інтернет-технології глибоко проникли у різні сфери життєдіяльності, повсякденними стали елементи електронного світу (електронний уряд, електронні пос-

луги, електронні документи, електронні гроші, електронний підпис), звичайним стало дистанційне навчання, наради, робота тощо. Тобто сформувалась нова сутність ***кіберпростір*** (cyberspace). Кіберпростір став середовищем для маніпулювання суспільною думкою і тим самим став джерелом інформаційно-психологічних впливів. При цьому, засоби, що використовуються є досить різноманітними, від технічних до психологічних.

Розглянемо як на даний час співвідносяться між собою поняття інформаційний простір, кіберпростір та кібербезпека.

Інформаційний простір (рис. 1) – це область ведення інформаційної війни, дії в якому можуть розгортатися як в психологічній сфері, так і в технічній сфері [11].

Психологічна сфера - це область інформаційного простору, яка об'єднує мислення особового складу ЗС та мирного населення. Це область, в якій формуються наміри командирів, доктрини, тактика, методи протиборства, мораль, поняття згуртованості підрозділів, рівень підготовки, досвід, розуміння ситуації та суспільна думка населення [12].

Технічна сфера - це область інформаційного простору, в якій створюється, обробляється та накопичується інформація. Крім того, це область, в якій функціонують системи управління, зв'язку та розвідки [12]. В подальшому в ряді керівних документів розвиток та уточнення поняття технічної сфери інформаційного простору призвело до створення понятійного апарату кіберпростору.

Вперше загальне визначення кіберпростору було надано дослідницькою службою конгресу США для того, щоб через термінологічний базис "кіберпонять" визначати сутності, які відносяться до протиборства в технічній сфері інформаційного простору (іншими словами, області ведення інформаційної війни) [1-2]. Основи цієї термінології надані в керівних документах ЗС США [3-7] та міжнародних стандартах ITU-T та ISO [8-10].

Рис. 1. Декомпозиція інформаційного простору [12]

Кіберпростір - всеохоплююча множина зв'язків між людьми, яка створена на основі комп'ютерів та телекомунікацій незалежно від фізичного чи географічного положення [5].

У Єдиному статуті комітету начальників штабів Збройних сил США кіберпростір визначено наступним чином [5]: «*Кіберпростір* - це сфера (область), в якій застосовуються різні РЕЗ (зв'язку, радіолокації, розвідки, навігації, автоматизації, управління та наведення) для прийому, передачі, обробки, зберігання, трансформації інформації та пов'язана з ними інформаційна інфраструктура ЗС».

У міжнародному стандарті ISO/IEC 27032:2012 [8] кіберпростір визначено з урахуванням тенденцій розвитку глобальної мережі Інтернету: *Кіберпростір* - це середовище, яке не існує у будь-якій фізичній формі, та являє собою наслідок результату взаємодії людей, програмного забезпечення та послуг в Інтернеті за допомоги технологій, засобів та мереж. У цьому ж стандарті через поняття кіберпростір визначено також термін "кібербезпека": *Кібербезпека* - це безпека в кіберпросторі [8].

У рекомендації X.1205 МСЭ-Т [9] кібербезпека визначена через поняття кіберпростору та систему управління ризиками: *Кібербезпека* — це набір засобів, стратегій, принципів забезпечення безпеки, мір з забезпечення безпеки, керівних принципів, підходів к керівництву ризиками, дій, професійної підготовки, практичному досвіду, страхуванню та технологій, які можуть бути використані для захисту кіберпростору, ресурсів організації та користувача.

Стандарт ISO/IEC 27032:2012 [8] визначає зв'язок термінів кібербезпека, мережева безпека, прикладна безпека, Інтернет безпека та безпека критичних інформаційних інфраструктур. В стандарті надана візуалізація зв'язку цих термінів (рис. 2). З точки зору міжнародних експертів усі ці терміни об'єднує поняття інформаційна безпека.

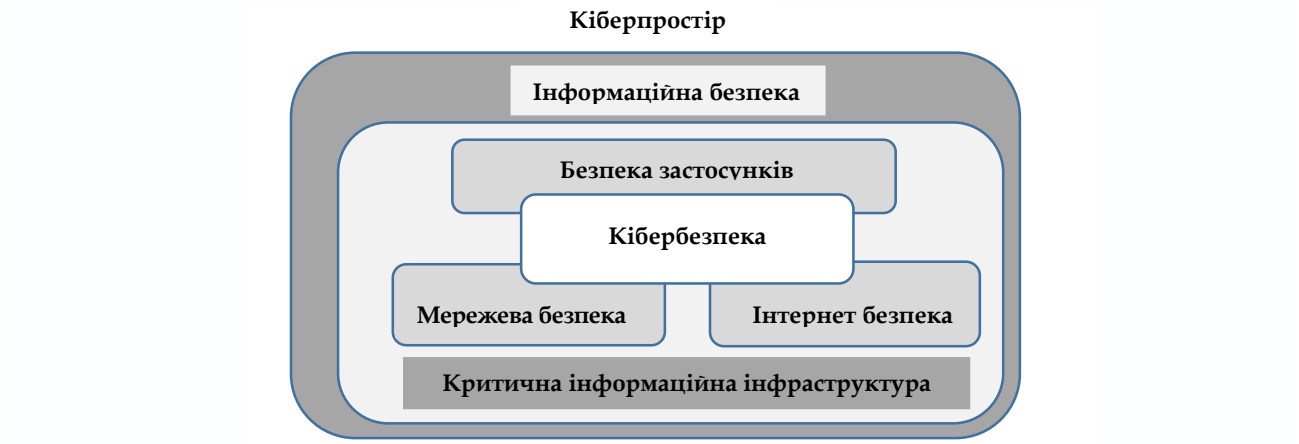


Рис. 2. Зв'язок терміну «кібербезпека» с термінологічним базисом стандарту ISO/IEC 27032:2012 [8]

Таким чином, основу кіберпростору складають сукупність розподілених у просторі взаємопов'язаних електронних засобів (комп'ютерів, серверів, мережевих маршрутизаторів, сховищ даних, шифраторів тощо) з відповідним програмним забезпеченням, за допомогою яких створюється та циркулює інформація (обробляється, передається, запам'ятовується та зберігається).

С інфраструктурної точки зору глобальний кіберпростір можна розглядати як адресний простір, що складається з національних та регіональних сегментів Інтернету.

Суб'єктами кіберпростору є людина, суспільство, держава, а також жива істота, яка спроможна сприйняти, запам'ятати та переробити інформацію, а також обмінятися нею [19].

Аналізуючи процес розвитку кіберпростору можна виділити декілька цікавих тенденцій, які в найближчому майбутньому суттєво вплинуть на його функціювання.

Тенденція перша: *Інформаційна безпека напряму залежить від кібербезпеки, тобто політики безпеки, що реалізується у кіберпросторі.*

Фактор наявності кіберпростору починає істотно впливати на інформаційну сферу будь-якої держави. З точки зору інтересів країни, кіберпростір треба розглядати як частину національної інфраструктури, яка має окреслені межі та потребує певної системи безпеки, як й інші елементи державної інфраструктури. Основна проблема кіберпростору - це забезпечення безпеки інформації, яка там циркулює, та стійкість його національного сегменту к кібератакам.

Інформаційна зброя стирає відмінність між військовими цілями і цивільними об'єктами, що обумовлено тісним взаємозв'язком та взаємозалежністю військових і цивільних інформаційних інфраструктур. Можна припустити, що в майбутньому високотехнологічні цивільні інформаційні системи, у тому числі що підтримують роботу критичних інфраструктур, будуть головними цілями нападу зі сторони можливого противника.

Перемога у інформаційному протиборстві в кіберпросторі може вирішити остаточний результат військового протиборства в цілому і вона може бути досягнута без здійснення традиційних бойових операцій, а тільки за рахунок застосування інформаційно-комунікаційні технології.

Тенденція друга: *кіберпростір поступово перетворюється у п'ятий театр військових дій.*

Кіберпростір поряд з традиційними наземним, морським, повітряним та космічним стає новим театром військових дій, де разом з військами планується участь спецслужб країни, хакерів та усіх тих, хто може створювати та використовувати інформаційні технології для нанесення ударів по ворогу.

Ряд країн (в першу чергу, США, Росія, Китай) вже проводять державну політику, яка розглядає кіберпростір як поле боя, внаслідок чого направляє свої зусилля на встановлення повного контролю в цій сфері, створюючи засоби та можливості на здійснення такого контролю. Такі прецеденти численні - інформаційна зброя використовувалася в усіх військових конфліктах на протязі останніх двадцяти років, вона стала важливою частиною озброєння збройних Китаю, Росії, США та їх союзників. Є дані, що роботи щодо розвитку потенціалу інформаційного протиборства проводять більш ніж 120 країн світу (для прикладу, розробки в області ядерної зброї ведуть не більше 20 країн).

Війни майбутнього будуть вестися в режимі онлайн, коли противник, окрім застосування сил на полі бою, буде використовувати вразливості комп'ютерних систем озброєння, інформаційних систем керування державних структур та об'єктів критичної інфраструктури для їх руйнування та знищення, а також соціальні мережі для створення паніки серед населення в масштабі цілої країни для зниження його здатності к супротиву агресії.

Кібервійни з фантастичних романів перекочовують у реальність. Вже відбувається трансформація усієї військової інформаційної архітектури, спостерігається "інформатизація" традиційних збройних сил і "інтелектуалізація" озброєнь. Активно розвивається концепція ексцентричного ведення бойових дій, мається на увазі досягнення переваги над ворогом шляхом ефективної організації збору, обробки і використання інформації.

Сьогодні можна вже говорити про те, що інформаційна зброя в деяких розвинених країнах перей-

шла в розряд тактичної. Повідомляється про розробки високочастотної електромагнітної імпульсної зброї, здатної виводити з ладу електроніку в радіусі сотень кілометрів. Експерти відмічають, що низка країн такі можливості має в розпорядженні вже нині. Ведуться розробки мікрохвильової зброї великої потужності, здатної змінювати траєкторію ракет у польоті, викликати перевантаження або виведення із ладу мереж зв'язку, телеметричного устаткування та електроніки систем озброєння. Вона також здатна вражати екрановані приміщення, захищені від радіоактивного випромінювання, та завдавати збитку здоров'ю й життю осіб, що знаходяться в радіусі її дії.

Тенденція третя: *для забезпечення переваги у кіберпросторі провідні країни світу починають формувати військово-мережевий комплекс.*

В часи "холодної війни", коли за відсутності активних воєнних дій розгорнулася безпрецедентна "гонка озброєнь", в США та СРСР уперше виникли так звані військово-промислові комплекси (ВПК). Основною задачею ВПК на першому плані виступив такий чинник могутності, як спроможність розробляти й виготовляти озброєння та військову техніку (ОВТ) на сучасному рівні і в належній кількості.

Під військово-промисловим комплексом розуміють сукупність підприємств і організацій тієї чи іншої країни, що виготовляють ОВТ для потреб збройних сил своєї держави та на експорт (рис.3). В офіційних документах України (а також Росії) зараз замість ВПК, як правило, вживається термін оборонно-промисловий комплекс [13].

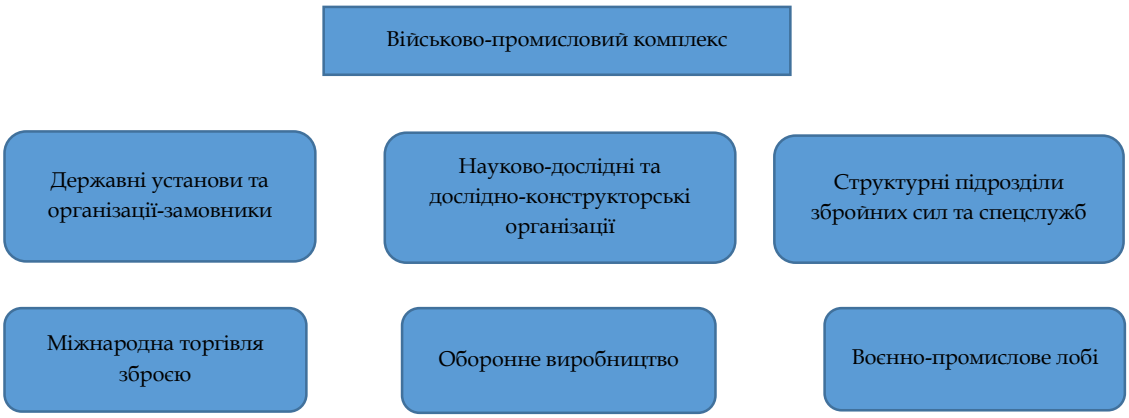


Рис. 3. Структура військово-промислового комплексу

Військово-промисловий комплекс – це суспільний феномен, у підґрунті якого лежить збіг інтересів керівництва воєнних корпорацій, вищого командного складу ЗС і високих посадових осіб держави, а одним з головних проявів є лобіювання бізнес-інтересів воєнної промисловості на вищому державному рівні та посилення її впливу на суспільні процеси. До нього звичайно зараховують ракетно-космічну, авіабудівну, суднобудівну, бронетанкову, радіоелектронну та артилерійсько-стрілецьку галузі.

Процеси, які зараз проходять в сфері інформаційного протиборства та кіберпростору, подібні процесам часів створення ВПК. Ми є свідками формування *військово-мережевого комплексу*, коли інтереси та можливості спецслужб і воєнного сектору країни переплітаються з інтересами та можливостями приватних структур, що в найближчий час разюче змінює як сам кіберпростір, так і характер воєнних дій в ньому.

Для вирішення цієї задачі відбувається колаборація державних структур з техноіндустрією Інтернету - крупними виробниками мікроелектроніки, обчислювальної та телекомунікаційної техніки щодо збору інформації о користувачах. В засобах масової інформації неодноразово з'являлися дані щодо співпраці зі спецслужбами таких відомих потужних виробники засобів телекомунікації (Cisco, Huaway), шифраторів (Crypto AG, Omnisec, Mils Electronic), програмного забезпечення (Microsoft), соціальних мереж (Facebook, Вконтакте, Одноклассники), антивірусних систем (Касперский, McAfee), постачальників послуг електронної пошти, мережевих та Інтернет-гігантів (Google, Yahoo, AT&T, CenturyLink, Verizon). Така співпраця включає навіть вбудовування необхідних бекдорів та передачі спецслужбам таємні вразливості в апаратному та програмному забезпеченні, у тому числі діючі ключі шифрування [15].

Тенденція четверта: *проблеми інформаційної безпеки у кіберпросторі та формування військово-мережевого комплексу приводять до перерозподілу повноважень існуючих гравців в сфері захисту інформації.*

Існуючі проблеми інформаційної безпеки кіберпростору показують, що державні органи не будуть основними гравцями в цій сфері, усякому разі її постійними лідерами. Вони будуть виробляти стратегію, встановлювати закони і контролювати стандарти безпеки кіберпростору, а ключові об'єкти інфраструктури повинні будуть їх виконувати. Але повсякденна робота по захисту ключових промислових об'єктів стане турботою корпорацій, які впораються з цією задачею не гірше держави. Вони будуть створювати новий вид послуг зі сканування, аналізу трафіка та застосування власних методів виявлення шкідливих програм та хакерської активності - методів, які будуть основані на тих даних, які компанії будуть збирати в режимі реального часу в своїх інформаційних мережах, а також в мережах своїх клієнтів. Це виходить свого роду краудсорсінг, коли залучають до вирішення тих чи інших проблем інноваційної діяльності широке коло осіб для використання їх творчих здібностей, знань та досвіду для субпідрядної роботи із застосування інформаційних технологій.

Ці ж організації будуть створювати кіберармії та навчати їх воювати в мережі, що зрештою приведе до їх інтеграції з арсеналом збройних сил країни.

Тенденція п'ята: *Надання послуг із захисту інформації у кіберпросторі стає новим видом бізнесу.*

Більш того, ці ж самі організації будуть не просто розслідувати вже здійсненні вторгнення, а й пропонувати свої послуги по захисту мереж клієнтів від потенційних загроз, подібно тому, як охоронні фірми пропонують убезпечити наші дома і офіси від грабіжників.

Для того, щоб захиститись від повсякденних кіберзагроз будуть створюватися безпечні зони Інтернету, тобто повноцінні кібернетичні інфраструктури, у яких безпека буде поставлена на чільне місце, а трафік аналізуватися більш активно та ретельно, ніж у загальнодоступному Інтернеті. Це буде свого роду "екозона безпеки", онлайн аналог особливо охоронюваної території.

Підвищена кібербезпека стане привабливою споживчою якістю, той особливістю, яка буде залучати клієнтів. Кампанії, що візьмуться за створення та обслугу таких захищених кіберзон (інтернет-провайдери, банки та інші, що мають діло з персональними даними), будуть залучати найбільш досвідчених і кваліфікованих співробітників, оскільки рівень зарплат у них буде значно більший ніж у державному чи воєнному секторі.

Як і в любій приватній організації, власники такої інфраструктури зможуть обмежувати її користування, встановлювати правила й вимоги їх виконання, а також пропонувати особливі переваги, насамперед безпеку. В межах таких мереж буде ретельно проводитись аналіз трафіку щодо шкідливих програм, надсилатися попередження о потенційній загрозі особовим даним, проводиться контроль тих, хто намагається війти в мережу, та не допускати в неї будь-яких підозрілих користувачів.

Слід відзначити ще той факт, що у державному та військовому секторах багатьох країн використовуються комерційні програмні продукти, які майже завжди мають вади в захисті, робить обороноздатність країни потенційно уразливою для нападів кібернетичних сил противника (його військових формувань, спецслужб, хакерів та терористів).

Проблему інформаційної безпеки в Україні загострює фундаментальна залежність українських інформаційних інфраструктур від зарубіжних комп'ютерних засобів. Майже 90% об'ємів продажів телекомунікаційного устаткування на внутрішньому ринку (його місткість нараховується мільярдами доларів) припадає на зарубіжні устаткування, запасні частини або комплектуючі, що використовуються при ремонті та обслуговуванні. Така залежність небезпечна не лише з точки зору економічної безпеки країни, але й безпеки в ширшому контексті, особливо враховуючи, що зарубіжне програмне забезпечення широко використовується на стратегічних об'єктах українського оборонного комплексу. Відомі непоодинокі реальні прецеденти щодо закладок недокументованих програмних модулів для здійснення втручання в роботу програмного забезпечення.

Висновки. Таким чином, інформаційне протиборство в кіберпросторі буде являти собою комплекс заходів, які спрямовані на захист системи світоглядних орієнтирів, установок, стереотипів, на основі яких базується можливість особи або цілого народу дати відсіч агресору.

Виходячи з вищевикладеного, принципове значення має підтримка розробки і виробництва в Україні конкурентних інформаційно-комунікаційних засобів (у тому числі, з використанням вітчизняної мікроелектроніки, яку потрібно відновити та розвивати) та програмного забезпечення в інтересах українських користувачів, а також застосування таких засобів в Україні, і передусім, в оборонному комплексі і на об'єктах критичної цивільної інфраструктури, з метою протидії інформаційним впливам.

Література

[1]. *Cyber Space Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, Washington D.C.: The White House, 2009.

[2]. *Informational Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World,* Washington D.C.: The White House, 2011.

[3]. *Department of Defense Strategy for Operating in Cyberspace*, Washington D.C.: U.S. Department of Defense, 2011.

[4]. *AFDD 3-12. Cyberspace Operations*, USAF, 2010, 60 p.

[5]. *AFDD 3-13. Information Operations*, USAF, 2011, 65 p.

[6]. *AFPD 10-7. Information Operations*, USAF, 2006, 29 p.

[7]. *DoDD 3600.1. Information Operations*, US DoD, 2013, 12 p.

[8]. *Стандарт ISO/IEC 27032:2012*. Інформаційні технології. Методи забезпечення безпеки. Керівні вказівки по забезпеченню кібербезпеки, 2012.

[9]. *Стандарт ITU-T X.1205:2008. Огляд кібербезпеки*, Женева: МСЭ-Т, 2008, 162 с. [Електронний ресурс]. Режим доступу: www.itu.int/ITU-T.

[10]. *Безпека в електрозв'язку та інформаційних технологіях. Огляд змісту та застосування діючих Рекомендацій МСЭ-Т для забезпечення захищеного електрозв'язку*, Женева: МСЭ-Т, 2009, 162 с. . [Електронний ресурс]. Режим доступу: www.itu.int/ITU-T.

[11]. *JP 3-13. Information Operations*, US Joint Chiefs of Staff, 2012, 69 p.

[12]. *JP 3-13.1. Electronic Warfare*, US Joint Chiefs of Staff, 2007, 115 p.

[13]. *Воєнно-промисловий комплекс* [Електронний ресурс]. Режим доступу: https://uk. wikipedia.org/wiki/ Воєнно-промисловий комплекс.

[14]. Я. Левин, *Интернет как оружие. Что скрывает Google, Tor и ЦРУ*, М.: Индивидуум, 2019, 360 с.

[15]. Ш. Харис, *Кибервойн@: Пятый театр военных действий,* М.: Альпина нон-фикшин, 2020, 390 с.

[16]. Л. Пирцхалава, В. Хорошко, Ю. Хохлачова, М. Шелест, *Информационное противоборство в современных условиях: [монография]*, Под ред. профессора В. Хорошко, К.: ЦП "Компринт", 2019, 226 с.

[17]. М. Карпінський, Ю. Ткач, Я. Усов, "Захищене інформаційне середовище", *ITSec: Безпека інформаційних технологій: IX міжнародна науково-технічна конференція, 22-27 березня 2019 р.*, К.: НАУ, С. 45-46, 2019.

[18]. Ю. Ткач, М. Шелест, М. Карпинський, "О развитии киберпространства и его защищенности", *I міжнародна науково-практична конференція «Безпека ресурсів інформаційних систем» (Information Systems of Security Resources), Чернігів, 16-17 квітня 2020 р.*,Чернігів, С. 103-105, 2020.

[19]. В. Фурашев, "Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності", *Інформація і право*, №2(5), С. 162-169, 2012.

УДК 004.056.5

Ткач Ю.Н. Тенденции развития современного киберпространстве и его защищенности в условиях информационного противоборства

Аннотация. *В статье рассмотрены актуальные вопросы формирования киберпространства. Определены тенденции его развития в условиях информационного противоборства, а именно: информационная безопасность напрямую зависит от кибербезопасности, есть политики безопасности, которая реализуется в киберпространстве; киберпространство постепенно превращается в пятый театр военных действий; для обеспечения преимущества в киберпространстве ведущие страны мира начинают формировать военно-сетевой комплекс; проблемы информационной безопасности в киберпространстве и формирования военно-сетевого комплекса приводят к перераспределению полномочий существующих игроков в сфере защиты информации; предоставление услуг по защите информации в киберпространстве становится новым видом бизнеса. Сделан вывод, что в условиях, сегодня сложились, то есть информационного противоборства, принципиальное значение имеет поддержка разработки и производства в Украине конкурентных информационно-коммуникационных средств (в том числе, с использованием отечественной микроэлектроники, которую нужно восстановить и развивать) и программного обеспечения в интересах украинских пользователей, а также применение таких средств в Украине, и прежде всего, в оборонном комплексе и на объектах критической гражданской инфраструктуры, с целью противодействия информационным воздействиям.*

Ключевые слова: *информационное противоборство, информационное пространство, киберпространство, кибербезопасность, информационная безопасность.*

Tkach Yu. Trends in the development of modern cyber space and its security in conditions of information conflict

Abstract. *The article considers the topical issue of cyberspace formation and features of its protection. It is proposed to distinguish between the concepts of information space, cyberspace and cybersecurity. Namely, the information space is an area of information warfare, actions in which can unfold both in the psychological sphere and in the technical sphere; cyberspace - a comprehensive set of connections between people, which is created on the basis of computers and telecommunications, regardless of physical or geographical location; Cybersecurity is a set of tools, strategies, security principles, security measures, guidelines, risk management approaches, actions, training, hands-on experience, insurance and technologies that can be used to protect cyberspace, organizational and user resources. The decomposition of the information space is determined and constructed. The tendencies of its development in the conditions of information confrontation are determined, namely: information security directly depends on cybersecurity, ie security policy implemented in cyberspace; cyberspace is gradually becoming the fifth theater of operations; to ensure the advantage in cyberspace, the world's leading countries are beginning to form a military-network complex; problems of information security in cyberspace and the formation of a military-network complex lead to a redistribution of powers of existing players in the field of information protection; the provision of information security services in cyberspace is becoming a new type of business. It is concluded that in the current conditions, ie information confrontation, it is essential to support the development and production in Ukraine of competitive information and communication tools (including the use of domestic microelectronics, which needs to be restored and developed) and software in the interests of Ukrainian users, as well as the use of such tools in Ukraine, and especially in the defense sector and at critical civilian infrastructure, in order to counter information influences.*

Keywords: *information confrontation, information space, cyberspace, cybersecurity, information security.*

Ткач Юлія Миколаївна, д.пед.н., доцент завідувач кафедри кібербезпеки та математичного моделювання Національного університету «Чернігівська політехніка».

Ткач Юлия Николаевна, д.пед.н., доцент, заведующий кафедрой кибербезопасности и математического моделирования Национального университета «Черниговская политехника».

Tkach Yuliia, Doctor of Pedagogical Sciences, Associate Professor, Head of the Department of Cybersecurity and Mathematical Simulation of the National University "Chernihiv Polytechnic".

Отримано *02 липня 2020 року*, затверджено редколегією *29 липня 2020 року*

© Popereshnyak S. Software for testing small-length bit sequences for randomness // Ukrainian Scientific Journal of Information Security, 2020, vol. 26, issue 2, pp. 80-86.

КРИПТОЛОГІЯ / CRYPTOLOGY

DOI: 10.18372/2225-5036.26.14867

ПРОГРАМНИЙ ЗАСІБ ДЛЯ ТЕСТУВАННЯ БІТОВОЇ ПОСЛІДОВНОСТІ МАЛОЇ ДОВЖИНИ НА ВИПАДКОВІСТЬ

Світлана Поперешняк

Київський національний університет імені Тараса Шевченка, Україна

ПОПЕРЕШНЯК Світлана Володимирівна, к.ф.-м.н., доцент

Рік та місце народження: 1980 рік, м. Кіровоград, Україна.
Освіта: Кіровоградський державний педагогічний університет імені Володимира Винниченка, 2002 рік.
Посада: доцент кафедри програмних систем і технологій факультету інформаційних технологій Київського національного університету імені Тараса Шевченка.
Наукові інтереси: програмна інженерія, автоматизація процесів виробництва, інформаційні технології, захист інформації, використання багатовимірних статистик для тестування бітової послідовності на випадковість.
Публікації: більше 100 наукових публікацій, серед яких навчальні посібники, наукові статті, матеріали та тези доповідей на конференціях.
E-mail: spopereshnyak@gmail.com.
Orcid ID: 0000-0002-0531-9809.

Анотація. *Данна стаття вивчає випадковість і найбільш відомі наборі тестів для її виявлення. Особлива увага приділяється статистичному дослідженню бітових послідовностей. Наявні набори тестів показують низьку гнучкість та універсальність у засобах знаходження прихованих шаблонів у даних невеликої довжини (до 100 біт). Для вирішення цієї проблеми запропоновано використовувати алгоритми на основі багатовимірних статистик. Дані алгоритми поєднують усі переваги статистичних методів та є єдиною альтернативою для аналізу послідовностей короткої та середньої довжини. У даній роботі розглянуто статичне тестування послідовностей з використанням багатовимірної статистики. У роботі наведені формули для тестування випадкових бітових послідовностей на випадковості, з використанням двовимірної або тривимірної статистика, яка може бути застосована для тестування коротких і середніх послідовностей. Для реалізації запропонованої методики було розроблено програмний засіб для тестування бітової послідовності на випадковість. Даний засіб включає в себе тести NIST, а також тести з використанням багатовимірної статистики, які добре себе зарекомендували при тестуванні бітової послідовності малої довжини. В результаті застосування розробленого засобу можливо проаналізувати бітову послідовність та вибирати якісну псевдовипадкову послідовність для використання в тій чи іншій предметної області.*

Ключові слова: *програмний засіб, бітова послідовність, тестування, багатовимірні статистики, випадкові послідовності, псевдовипадкова послідовність, статистичне тестування.*

Вступ

Більшість об'єктів і явищ, що нас оточують, мають випадкову природу. Для адекватного опису, вивчення і моделювання часто виявляється недостатньо детермінованих підходів, тому закономірно залучення стохастичних (тобто таких, що мають випадковий характер) методів вирішення різноманітних завдань. У зв'язку з цим випадкові числа, послідовності таких чисел і генератори, які їх виробляють знаходять все більше широке застосування в науці, техніці, зв'язку, різних інформаційних технологіях, а також у багатьох аспектах повсякденного життя [1-3].

Історично випадкові числа почали використовуватися для проведення вибіркових спостережень замість неперервних. Випадкові числа застосовуються при вирішенні складних обчислювальних задач і реалізації обчислювальних методів. Розвиток ЕОМ, з одного боку, розширило коло завдань, що використовують випадкові числа, а з іншого - пред'явило високі вимоги до якості їх генерації. Таким чином, випадкові числа відіграють важливу роль в інформатиці, розподілених обчисленнях, криптографії та інших областях.

Аналіз існуючих досліджень

Розглянемо найвідоміші набори тестів для перевірки бітових послідовностей. Варто зауважити, що деякі з методів випробувань в наборах збігаються, адже вони всі засновані на одному математичному підґрунті.

NIST Statistical Test Suite

NIST STS – специфікація та відповідна бібліотека на мові С, що були випущені Інститутом Стандартів та

Технологій США. Пакет складається з 15 тестів для аналізу бітових послідовностей, що були згенеровані ГПЧ або АГВЧ. Повний опис тестів доступний в [4].

Тести Diehard

Батарея статистичних тестів призначена для виміру якості ГПЧ та АГВЧ, що була створена Джорджом Марсалі у 1995 році. В основі більшості тестів лежить використання генератора для побудови послідовності відповідно да наданої специфікації і порівняння її характеристик з очікуваними від випадкової. Деякі з наведених випробувань можна виділити в групи за подібністю, а інші являють собою один тест. Більше інформації про тести можна знайти в [5, 6].

TestU01

Об'ємна бібліотека тестів на мові С, що включає реалізацію ГПЧ, тести та батареї тестів. Всі випробування що надаються, поділені в групи відповідно до модулів програми [7].

Аналіз тестів із зазначених статистичних пакетів дає можливість зробити висновок, що область перевірки випадковості далеко не є завершеною і потребує додаткового дослідження та покращення існуючих підходів. До проблем більшості тестів можна віднести:

– Випробування потребують послідовності великої довжини.

Наприклад, мінімальна рекомендована довжина послідовностей для NIST варіюється від 100 до 10^6, а деякі з тестів Diehard потребують по 100-200 тисяч біт. Звісно, якість результату покращується при збільшенні вибірки в будь-якому статистичному дослідженні, але не існує альтернативи для перевірки коротких послідовностей.

– Деякі з параметрів тестів неможливо змінити.

Це здебільшого стосується тестів Diehard, які потребують генерації послідовності фіксованої довжини відповідно до специфікації. Зміна параметрів має ключове значення для проведення якісного дослідження.

– Рішення про проходження тесту приймає тільки два значення (так/ні).

Результатами тесту повинні також бути точні та значущі числові значення. Це дозволить порівнювати результати різних тестів або одного тесту для різних послідовностей.

– Відсутність програмних пакетів для тестування.

Розробка пакетів для дослідження випадкових чисел без програмного забезпечення є доволі сумнівною роботою, адже область застосування повністю складається з інформаційних технологій.

Отже, в методах перевірки бітових послідовностей є достатньо проблем для вирішення та підходів для покращення. Особливий інтерес для дослідження складає відсутність тестів, що можуть дати адекватні результати на коротких послідовностях [8].

Метою даної роботи є покращення існуючих та впровадження нових методів тестування бітової послідовності на випадковість. Це включає розробку формального опису статистичних тестів та реалізацію відповідних програмних продуктів. Мета роботи – формальна та програмна реалізація існуючих тестів (на прикладі тестів NIST) та методів тестування заснованих на використанні багатовимірних статистик.

Основна частина дослідження

Специфіка тестів описаних пакетів є такою, що на основі вхідної послідовності бітів визначається статистика яка або є результатом, або використовується для його пошуку. Цей підхід враховує тільки одну характеристику послідовності при одному випробуванні. Багатовимірні статистики орієнтовані на декілька властивостей, що дозволяє більш точніше оцінити коротку послідовність, але має свої недоліки в тестуванні довгої через надмірно велику кількість варіантів комбінацій статистик.

Проблеми малих і великих вибірок відносяться до основних проблем, що виникають при практичному застосуванні методів аналізу даних. Будемо використовувати класифікацію вибірок за чисельністю наведену в [8], виходячи з вимог представлених в програмі критеріїв:

– дуже малі вибірки - від 5 до 12;
– малі вибірки - від 13 до 40;
– вибірки середньої чисельності - від 41 до 100;
– великі вибірки - від 101 і вище.

Відповідно до [1], генератори випадкових чисел мають тенденцію до створення великої кількості повторюваних шаблонів. Тести багатовимірних статистик, також, надають більш ефективні результати в перевірці шаблонів за рахунок оцінки декількох статистик одночасно.

Математично-статистичний аналіз послідовностей, як правило, відбувається в два етапи. Наведемо опис основних етапів:

1. Перший етап можна назвати підготовчим, він найбільш трудомісткий, тут виконується основна маса обчислень.

1.1. При допомозі дослідного генератора формуються випадкові послідовності (або вводяться задані послідовності).

1.2. Для кожної послідовності обчислюється статистика тесту. Якщо працює батарея тестів (проводиться відразу декілька тестів), то статистика за результатами виписується для кожного тесту.

1.3. Для кожної послідовності, що обчислюється ймовірність значущості.

1.4. Отриманні статистики та ймовірності значущості зберігаються.

2. На другому етапі проводиться обробка, отриманих результати.

2.1. Перевірка статистичної гіпотези

2.1.1. Формулювання нульової та альтернативної гіпотези.

2.1.2. При допомозі критеріїв погодження перевіряють гіпотези на відповідність розподілених статистичних даних і ймовірностей значущих гіпотетичних розподілів.

2.1.3. Визначається кількість послідовностей, які пройшли тест. Будується довірчий інтервал для останньої величини.

2.1.4. Порівняння долі послідовностей які попали в довірчий інтервал з рівнем значущості та прийняття рішення про проходження тестів.

2.2. Приймається рішення про те, чи можна вважати тест таким, що пройшов.

2.3. Якщо результати задовільні приймається рішення про завершення тесту, в противному разі переходимо до кроку 1.2.

2.4. Остаточні висновки.

Методи що представлені в роботі засновані на дослідженні кількості входжень двох- та трьох-бітових шаблонів в послідовність бітів. Тести на основі багатовимірних статистик в результаті виконання надають спільну вірогідність відповідної кількості шаблонів в послідовності заданої довжини. Той самий результат можна отримати за допомогою емпіричного підрахунку. Припустимо, що виконується розрахунок спільної вірогідності для всіх можливих значень $k_1 = \eta(11)$, $k_2 = \eta(000)$ та послідовності довжиною 3. Кількості входжень k_1 та k_2 до послідовності наведено в табл. 1.

Таблиця 1

Поява шаблонів в послідовності довжиною 3

Послідовність	**k_1**	**k_2**
000	0	1
001	0	0
010	0	0
011	1	0
100	0	0
101	0	0
110	1	0
111	2	0

Підрахувавши кількість появи для всіх можливих комбінацій k_1 та k_2, можна знайти відповідні вірогідності (табл. 2).

Таблиця 2

Входження шаблонів в послідовність довжиною 3

k_1	**k_2**	**Кількість**	**Вірогідність**
2	0	1	0,125
1	0	2	0,25
0	0	4	0,5
0	1	1	0,125

Емпіричним методом знайдено спільну вірогідність для заданої довжини і всіх можливих значень k. Цей підхід є доволі простим і наглядно показує для чого використовуються методи багатовимірних статистик, але не є ефективним (кількість послідовностей які необхідно перевірити при довжині 32 – 2^{32}). Випробування побудовані на формулах спільної вірогідності є більш доцільними як в математичному сенсі, так і в програмному.

Тести багатовимірних статистик відрізняються тільки шаблонами, на які перевіряється послідовність. Кожен метод отримує на вхід випадкову величину:

$\gamma 1, \gamma 2 \ldots, \gamma n$, де $\gamma i \in \{0, 1\}$, $i = 1,2\ldots,n$, $n > 0$.

Для даної величини визначається кількість специфічних шаблонів k1, k2 та k3 (якщо це визначено методом) і виконується обчислення за допомогою формули специфічної для методу.

Перший тест виконується, щоб знайти спільну вірогідність появи подій $k1 = \eta(tt^*)$ та $k_2 = \eta(t1t^*) + \eta(t0t^*)$, при $t \in \{0, 1\}$, $t^*=1 - t$:

$$P\left\{\eta\left(tt^*\right) = k_1, \eta\left(t1t^*\right) + \eta\left(t0t^*\right) = k_2\right\} = \sum_{m_1=k_1}^{n-k_1} p^{m_1} q^{m_0} \sum \prod_{i=0}^{1} C_{k_1}^{\delta_i} C_{m_i-k_1}^{k_1-\delta_i},$$

де n – довжина бітової послідовності, p – вірогідність появи t, q – вірогідність появи t* (q = 1 - p), $m_0 = n - m_1$, $\sum$ - сума по всім комбінаціям δ_0 та δ_1, таким, що: $\delta_0 + \delta_1 = 2k_1 + k_2$.

Другий метод тестування знаходить спільну вірогідність появи подій $k_1 = \eta(tt^*)$ та $k_2 = \eta(ttt^*)$:

$$P\left\{\eta\left(tt^*\right) = k_1, \eta\left(ttt^*\right) = k_2\right\} = \sum_{m_1=k_1}^{n-k_1} p^{m_1} q^{m_0} C_{k_1}^{k_2} C_{m_1-k_1}^{k_2} C_{m_0}^{k_1}.$$

Третій метод оцінює вірогідність появи шаблонів $k_1 = \eta(tt^*)$, $k_2 = \eta(t1t^*)$ та $k_3 = \eta(t0t^*)$:

$$P\left\{\eta\left(tt^*\right) = k_1, \eta\left(t1t^*\right) = k_2, \eta\left(t0t^*\right) = k_3\right\} = \sum_{m_1=k_1}^{n-k_1} p^{m_1} q^{m_0} C_{k_1}^{k_2} C_{k_1}^{k_3} C_{m_1-k_1}^{k_2} C_{m_0-k_1}^{k_3}.$$

За допомогою четвертого методу можна визначити вірогідність подій k1 = η(tt*) та k2 = η(ttt):

$$P\left\{\eta\left(tt^*\right) = k_1, \eta\left(ttt\right) = k_2\right\} = \sum_{m_1=k_1}^{n-k_1} p^{m_1} q^{m_0} C_{m_0}^{k_1} \times \sum_{i \in \{k_1, k_1+1\}} C_i^{m_1-k_2-i} Z\left(m_1 - i, m_1 - i - k_2\right),$$

де $Z(a,b) = \begin{cases} C_{a-1}^{b-1}, \text{ якщо } a \geq b \geq 0; \\ 1, \text{ якщо } a = b = 0; \\ 0, \text{ в іншому випадку} \end{cases}$.

Враховуючи, що обробка вхідних запитів є найважливішою задачею серверу, розглянемо типовий сценарій за допомогою діаграми діяльності (рис. 1). Як можна бачити, процес є доволі складним, і містить багато етапів на яких можуть виникнути критичні та помилкові ситуації.

Згідно з специфікацією NIST [1], та описаних методів багатовимірних статистик [9-11] створено бібліотеку що надає користувачам два інтерфейси для виконання відповідних статистичних тестів в мові програмування Java. Ціллю програмного засобу є забезпечення користувачів можливістю тестування бітових послідовностей на випадковість за допомогою графічного інтерфейсу. Він повинен забезпечити високий рівень зручності використання: надавати свободу дій, врахувати можливість помилок, повідомляти інформацію про стан системи та містити довідкові матеріали.

Відповідно до основного функціоналу який повинен забезпечувати додаток, між задачами, що виконує веб-додаток та задачами серверу є чіткий розподіл. Перший працює незалежно більшу частину часу, і викликає другого тільки коли не може виконати поставлену задачу самостійно.

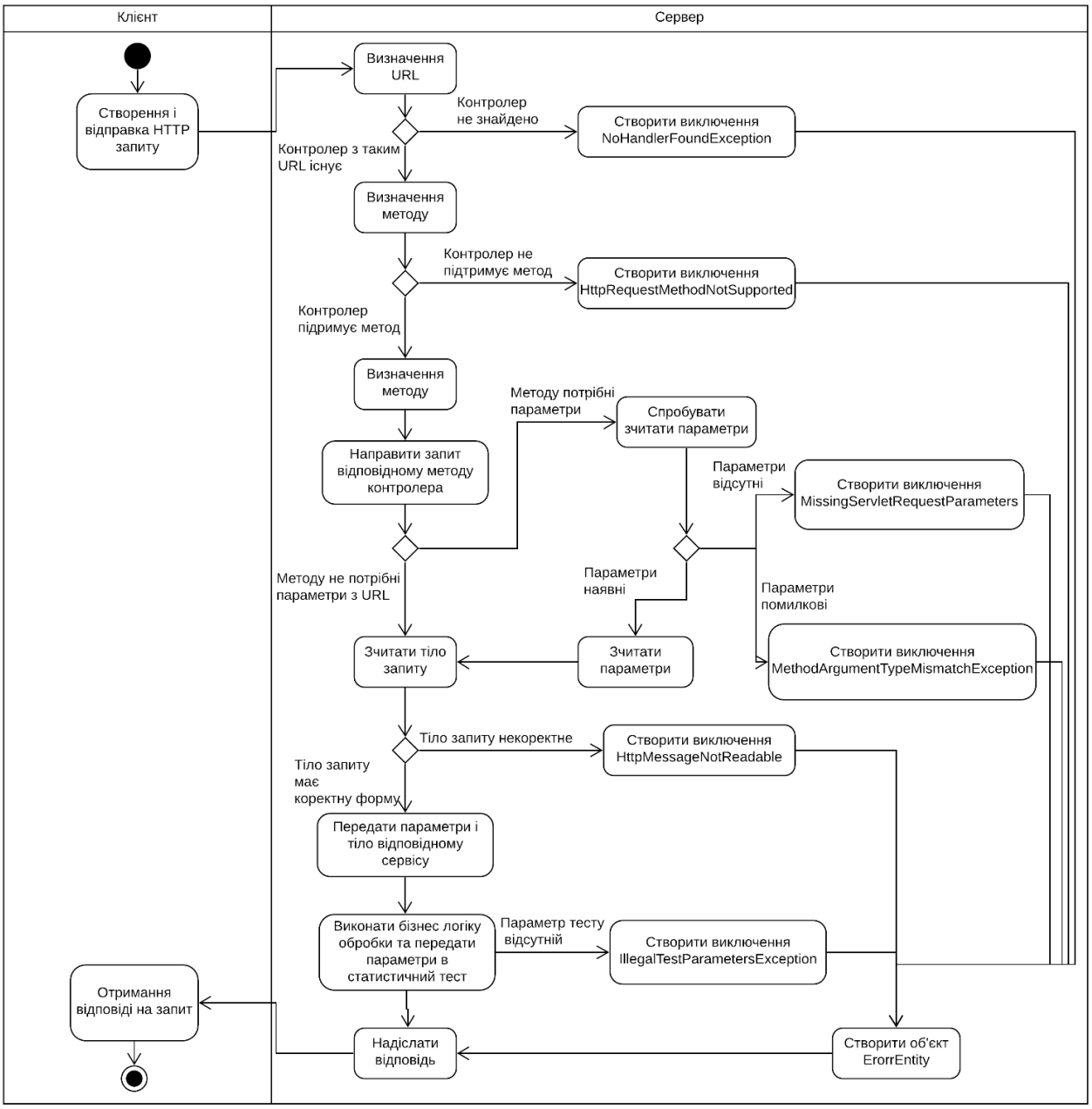


Рис. 1. Діаграма діяльності

Застосунок складається з однієї «сторінки», відповідно до принципів створення front end за допомогою React. Так, верхній та нижній та нижній колонтитули залишаються незмінними незалежно від URL, а зміст який знаходиться посередині завжди змінюється в залежності поточної адреси. Верхня навігаційна панель надає можливість перейти на 3 сторінки, зміст яких описано в табл. 3.

Таблиця 3

Зміст сторінок навігаційної панелі

Назва сторінки	Опис сторінки
Головна сторінка	Загальна інформація про тести та бітові послідовності і про призначення програмного продукту
Сторінка тестів NIST	Містить 16 сторінок що відповідають окремим тестам NIST та сторінку з комплексним тестом
Сторінка тестів багатовимірних статистик	Містить 9 сторінок що відповідають окремим тестам багатовимірних статистик та сторінку з комплексним тестом

Всі сторінки з тестами містять додаткове меню в якому можна обрати один окремий, або комплексний тест. На сторінці останнього, користувачу надається можливість ввести вхідні параметри, та вибрати один або декілька методів одночасно. Сторінки окремих тестів містять форми введення даних і теоретичну інформацію.

Загальний принцип спільної роботи пакету програм представлений на діаграмі діяльності (рис. 2). Як

можна бачити, виконання навіть одного тесту не є тривіальною задачею, що включає багато етапів з використанням всіх модулів. За рахунок чітко визначених протоколів та інтерфейсів комунікації між модулями системи, та «лінивого виконання» всіх етапів, досягається високий рівень ефективності та надійності системи.

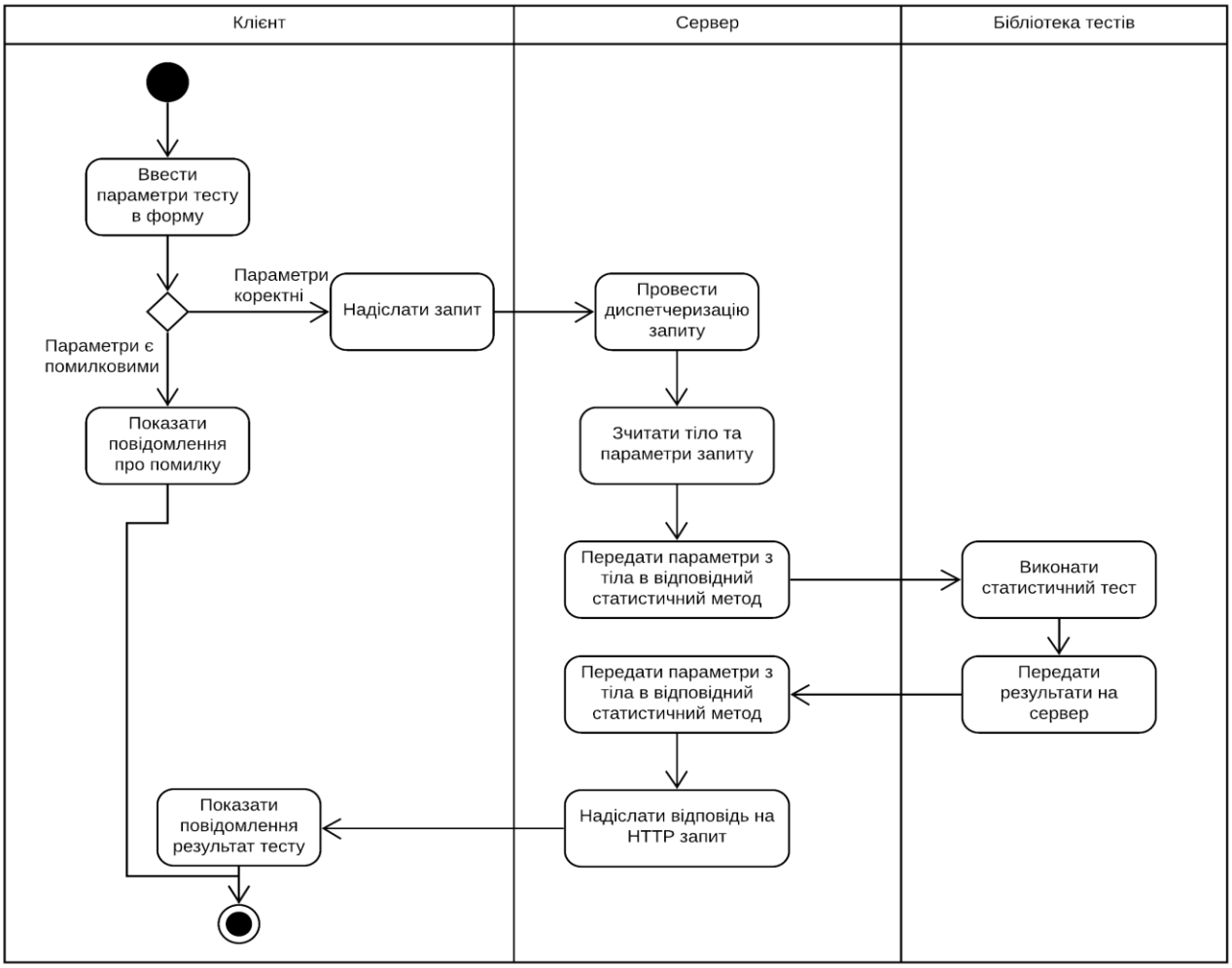


Рис. 2. Діаграма діяльності для повного циклу запит-відповідь

Доступ до прикладного інтерфейсу можна отримати за рахунок виконання запитів. Створення HTTP запитів пропонується проводити з використанням мов програмування, однак для тестування API можна використати HTTP клієнт на зразок

Веб-додаток

При переході на сайт з пошукової системи, користувача буде направлено на головну сторінку. Якщо було введено адресу іншої сторінки веб-додатку, або перейдено за посиланням з іншого ресурсу, відкриється сторінка за що знаходиться за конкретною адресою.

Головна сторінка надає довідкову інформацію про зміст веб-додатку та корисні посилання. Використавши верхню навігаційну панель, можна перейти на сторінки що відповідають тестам NIST (рис. 3) та багатовимірних статистик.

За замовчуванням відкриваються комплексні тести, тобто для одночасного виконання декількох методів. Кожна форма містить елементи управління «Checkbox» для вибору окремих тестів та вибору/зняття всіх одночасно. В текстові поля вводиться послідовність бітів.

Бокові панелі на обох сторінках містять меню в якому можна обрати окремо один з тестів. На сторінці з методом можна отримати довідкову інформацію і виконати обчислення.

Форми містять текстові поля для введення кожного з параметрів тесту, в самих полях є підказки про дані які необхідно вводити. Кнопка «Тест» слугує для виконання методу, а результат буде показано справа. Використання даної кнопки при некоректних даних в полях форми, призводить до появи повідомлення про помилку, текст якого завжди відповідає змісту помилки.

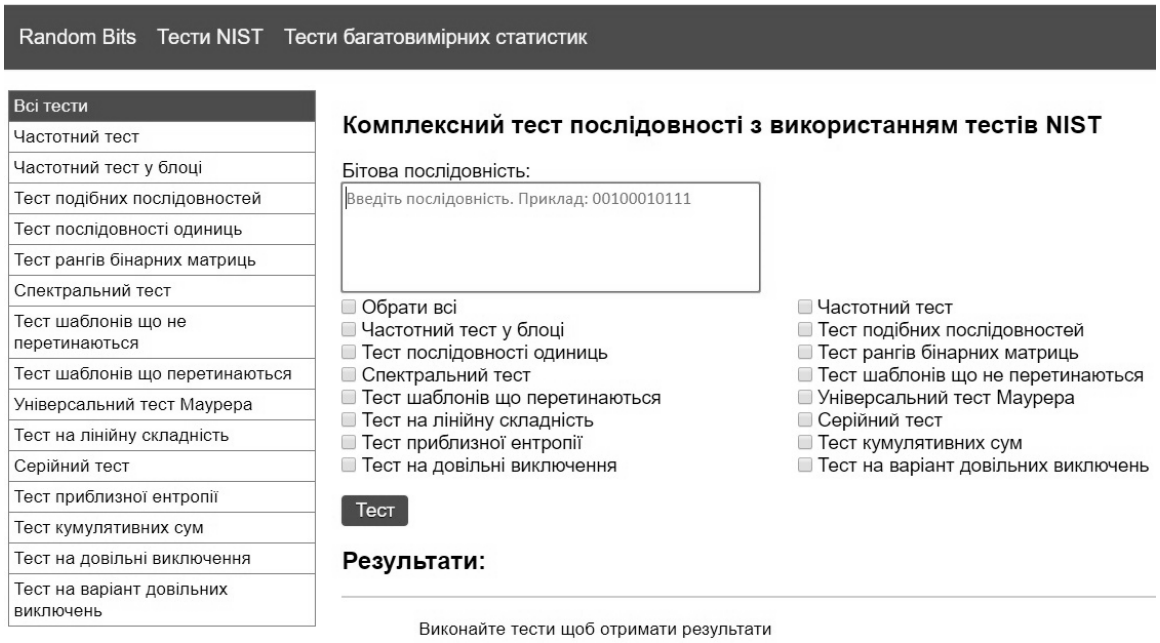


Рис. 3. Сторінка NIST

Висновки

Тестування бітової послідовності на випадковість не є новою проблемою. Наразі існує велика кількість пакетів тестів, що вирішують дану задачу. Однак, специфіка предметних галузей, системи тестування та проблеми існуючих методів, вказують на актуальність даного питання та необхідність покращення існуючих методів тестування.

Тести багатовимірних статистик дозволяють краще дослідити послідовність за рахунок використання одночасно декількох характеристик послідовності. Вони засновані на дослідженні шаблонів довжин два та/або три, і допомагають виявляти приховані залежності між даними. Головною перевагою тестів є їх ефективність на послідовностях короткої довжини.

Запропонований в роботі підхід і програмний засіб надає декілька можливих рівнів використання, в залежності від вимог користувача, і складається з:

– Бібліотека на мові Java, що включає 15 тестів NIST та 9 тестів багатовимірних статистик.

– Прикладний програмний інтерфейс що надає можливість використовувати тести за допомогою HTTP запитів.

– Веб-додаток, який може бути використано для тестування послідовностей через браузер.

Даний програмний засіб рекомендовано використовувати при дослідженні послідовностей на випадковість. Вони можуть бути застосовані в одні з наступних областей:

– Наукові дослідження – встановлення залежності між будь-якими експериментальними даними, розробка генераторів псевдовипадкових чисел, створення нових методів перевірки послідовності на випадковість.

– Криптографія – перевірка послідовностей згенерованих генераторами псевдовипадкових чисел, дослідження алгоритмів шифрування.

– Розробка та супровід програмних продуктів – тестування ефективності алгоритмів та систем заснованих на випадковості, перевірка криптографічних засобів системи.

Література

[1]. Д. Кнут, *Искусство программирования. Том 2. Получисленные алгоритмы*, М.: Вильямс, 2007, 832 с.

[2]. М. Иванов, Д. Михайлов, И. Чугунков, *Стохастические методы и средства защиты информации в компьютерных системах и сетях*, М.: Кудиц-Пресс, 2009, 512 с.

[3]. М. Иванов, И. Чугунков, *Криптографические методы защиты информации в компьютерных системах и сетях*, М.: НИЯУ МИФИ, 2012, 400 с.

[4]. A. Rukhin, *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*, National Institute of Standards and Technology, 2010. [Electronic resource]. Online: https:// nvlpubs. nist. gov / nistpubs / Legacy / SP / nistspecial publication800-22r1a.pdf.

[5]. *DIEHARD Statistical Tests*. [Electronic resource]. Online: https://stat.fsu.edu/pub/diehard/.

[6]. *Diehard Tests*. [Electronic resource]. Online: https://en.wikipedia.org/wiki/Diehard_tests.

[7]. *TestU01: A software library in ANSI C for empirical testing of random number generators*. Department d'Informatique et de Recherche Operationnelle, University of Montreal. 2013. [Electronic resource]. Online: http://simul.iro.umontreal. ca/testu01/ guide-shorttestu01.pdf.

[8]. И. Гайдышев, *Программное обеспечение анализа данных AtteStat. Руководство пользователя. Версия 13*, 2012, 505 с.

[9]. S. Popereshnyak, G. Dimitrov, "The Testing of Pseudorandom Sequences using Multidimensional Statistics", *Proceedings of the 1st International Workshop on Digital Content & Smart Multimedia (DCSMart 2019) Lviv, Ukraine, December 23-25*, pp. 151-161, 2019.

[10]. V. Masol, S. Popereshnyak, "Statistical analysis of local sections of bits sequences", *Journal of Automation and Information Sciences,* Vol. 51, pp. 31-45, 2019. DOI: 10.1615/JAutomatInf Scien.v51.i10.30.

[11]. V. Masol, S. Popereshnyak, "Checking the Randomness of Bits Disposition in Local Segments of the (0, 1)-Sequence", *Cybernetics and Systems Analysis,* no. 56(3), pp. 1-8, 2020. DOI: 10.1007/s10559-020-00267-0.

УДК 519.212.2 : 681.51

Поперешняк С.В. Программное средство для тестирования битовых последовательностей малой длины на случайность

Аннотация. *Данная статья изучает случайность и наиболее известные наборе тестов для ее обнаружения. Особое внимание уделяется статистическому исследованию битовых последовательностей. Имеющиеся наборы тестов показывают низкую гибкость и универсальность в средствах нахождения скрытых шаблонов в данных небольшой длины (до 100 бит). Для решения этой проблемы предложено использовать алгоритмы на основе многомерных статистик. Данные алгоритмы сочетают все преимущества статистических методов и является единственной альтернативой для анализа последовательностей короткой и средней длины. В данной работе рассмотрены статическое тестирование последовательностей с использованием многомерной статистики. В работе приведены формулы для тестирования битовых последовательностей на случайность, с использованием двумерных или трехмерных статистик, которые могут быть применены для тестирования коротких и средних последовательностей. Для реализации предложенной методики было разработано программное средство для тестирования битовой последовательности на случайность. Данное средство включает в себя тесты NIST, а также тесты с использованием многомерной статистики, которые хорошо себя зарекомендовали при тестировании битовой последовательности малой длины. В результате применения разработанного средства возможно проанализировать битную последовательность и выбрать наиболее качественную псевдослучайную последовательность для использования в той или иной предметной области.*

Ключевые слова: *программное средство, битная последовательность, тестирование, многомерные статистики; случайные последовательности; псевдослучайная последовательность; статистическое тестирование.*

Popereshnyak S. Software for testing small-length bit sequences for randomness

Abstract. *This article dedicated to systematization of scientific positions about the static testing of sequences, widely used in cryptographic systems of information protection for the production of key and additional information (random numbers, vectors of initialization etc.) In this paper, randomness and the best-known test suite for detecting it is examined. Testing a bit sequence for randomness is not a new problem. Now there are a large number of test packages that solve this problem. Particular attention is paid to the statistical study of bit sequences. However, the specificity of subject areas, testing systems and problems of existing methods indicate the relevance of this issue and the need to improve existing testing methods. The available test suites show low flexibility and versatility in finding hidden patterns in small data lengths (up to 100 bits). To solve this problem, it is proposed to use algorithms based on multivariate statistics. Tests for multivariate statistics allow you to better explore a sequence by using multiple sequence characteristics simultaneously. They are based on examining patterns of length two and/or three and help to uncover hidden dependencies between data. These algorithms combine all the advantages of statistical methods and are the only alternative for analyzing short and medium length sequences. In this paper, static testing of sequences using multivariate statistics is considered. The paper provides formulas for testing bit sequences for randomness, using two-dimensional or three-dimensional statistics, which can be used to test short and medium sequences. To implement the proposed technique, a software tool was developed to test the bit sequence for randomness. This tool includes NIST tests as well as tests using multivariate statistics, which have worked well for testing short bit sequences. As a result of using the developed tool, it is possible to analyze a bit sequence and select the highest quality pseudo-random sequence for use in a particular subject area.*

Keywords: *software, bit sequence, testing, multidimensional statistics; random sequences; pseudo-random sequence; statistical testing.*

Поперешняк Світлана Володимирівна, кандидат фізико-математичних наук, доцент, доцент кафедри програмних систем і технологій факультету інформаційних технологій Київського національного університету імені Тараса Шевченка.

Поперешняк Светлана Владимировна, кандидат физико-математических наук, доцент, доцент кафедры программных систем и технологий факультета информационных технологий Киевского национального университета имени Тараса Шевченко.

Popereshnyak Svitlana, PhD (Theory of Probability and Mathematical Statistics), Associate Professor of Department of Software Systems and Technologies, Taras Shevchenko National University of Kyiv.

Отримано *28 липня 2020 року*, затверджено редколегією *12 серпня 2020 року*

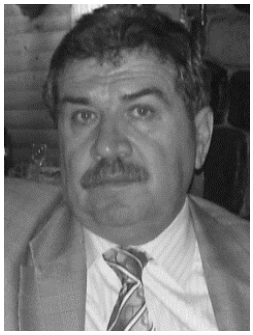
ISSN 2225-5036 (Print), ISSN 2411-071X (Online)
http://infosecurity.nau.edu.ua; http://jrnl.nau.edu.ua/index.php/Infosecurity

DOI: 10.18372/2225-5036.26.14876

АНАЛІЗ ОПЕРАЦІЙ МОДУЛЬНОГО ТА ПОКОМПОНЕНТНОГО ДОДАВАННЯ У БЛОКОВИХ ШИФРАХ

Геннадій Гулак

Інститут проблем математичних машин і систем Національної академії наук України



ГУЛАК Геннадій Миколайович, к.т.н., доцент

Рік та місце народження: 1955, РК.
Освіта: Вища школа КДБ СРСР.
Посада: завідувач лабораторії досліджень кібербезпеки Інституту проблем математичних машин і систем Національної академії наук України.
Наукові інтереси: криптографія, кібербезпека та інформаційна безпека, гарантоздатні системи.
Публікації: 25 наукових публікацій, 5 навчальних посібників.
E-mail: h.hulak@ukr.net.
Orcid ID: 0000-0001-9131-9233.

Анотація У роботі досліджуються властивості операцій модульного та покомпонентного додавання, що використовуються у вузлах блокових шифрів, які забезпечують додавання ключової інформації (ключові суматори), та їх вплив на практичну криптографічну стійкість. Для цього отримані допоміжні результати щодо функцій розподілу імовірностей звичайних та модульних сум незалежних рівномірно розподілених випадкових величин. В основній частині доведено що послідовність бітів переносу в наступний розряд при модульному додаванні чисел $a, b \in Z_{p^n}$, утворюють однорідний ланцюг Маркова з визначеним початковим станом та відповідною матрицею переходів, а також обчислена імовірність того, що при модульному та покомпонентному додаванні в результаті утвориться $k < n$-1 переходів між блоками, в яких всі компоненти співпадають, та блоками, в яких всі компоненти не співпадають. З урахуванням допоміжних результатів у статті отриманні та порівняні імовірнісні характеристики операцій покомпонентного та модульного додавання (віднімання), обчислені імовірності співпадіння результатів зазначених операцій, зроблені висновки щодо коректності (некоректності) використання відповідних модифікацій блокових шифрів для побудови оцінок стійкості, наведені практично застосовні зразки блоків заміни до блокових шифрів, які відповідають визначеним умовам, визначена можливість вразливості шифру до певних типів різницевих атак за умови наявності додаткової інформації щодо того, що при оцінці стійкості даного шифру використовувалась його модифікація, отримана шляхом заміни операції у ключовому суматорі на деяку іншу. У статті обґрунтовані висновки, що заміна операції у ключовому суматорі або блоку підстановки шифру недопустима без попередніх досліджень, що полягають в обчисленні і порівнянні відповідних параметрів.

Ключові слова: блоковий шифр, блок заміни, ключовий суматор, операція модульного додавання, операція покомпонентного додавання, криптографічна стійкість

Вступ

У якості механізму забезпечення конфіденційності інформації, контролю її цілісності, а також реалізації процедур автентифікації, генерації ключами та управління ними в гарантоздатних інформаційних системах різного призначення широко використовуються симетричні криптосистеми. Серед означених криптосистем особливе місце займають блокові шифри (далі – БШ), які, зазвичай, спеціально проектуються для застосування у системах захисту інформації в комп'ютерних мережах, автоматизованих системах управління тощо [1] - [3].

Головною характеристикою застосовності БШ для виконання перелічених вище функцій є їх практична криптографічна стійкість, яка визначається у ході проектування та досліджень цих шифрів для всіх відомих на поточний час видів криптоаналітичних атак [2] – [4].

Практична стійкість криптографічних алгоритмів є базовою умовою безпеки засобів захисту, в яких вони вбудовані, але особливості програмної або апаратної реалізації можуть утворювати небезпечні стани у роботі цих засобів, внаслідок чого можуть бути викривлені вхідні дані або структурні елементи цих алгоритмів, що може призвести до суттєвого зниження рівня безпеки криптографічних перетворень [5] – [7]. В свою чергу, зниження рівня інформаційної безпеки або кібербезпеки засобів криптографічного захисту інформації може мати наслідком зниження рівня функціональної безпеки інформаційної системи, отже – її гарантоз-

датності. Окремо слід зазначити, що під час виробництва засобів захисту або їх експлуатації некоректна зміна параметрів та елементів криптографічної схеми також може мати негативні наслідки для гарантоздатності інформаційної системи [5], [8].

Таким чином, у ході проектування та досліджень засобів криптографічного захисту інформації вкрай необхідно враховувати припустимі межі зміни параметрів або елементів криптогріфчних алгоритмів у разі випадкових факторів (помилка проектанта, збій/ відмова засобу) або навмисних впливів (втручання інсайдерів/ зловмисників). У визначених умовах у випадку БШ об'єктами особливої уваги постають раундові операції з ключовими даними та блоки заміни [3], [4]

Слід зазначити, що проектування сучасних БШ ґрунтується на визначених у роботі К. Шеннона [9] принципах розсіювання *(diffusion)* та перемішування *(confusion)*. Такі принципи передбачають, що під час проектування шифру забезпечується вплив кожного знаку ключа або відкритого тексту на багато знаків шифрованого тексту, а також побудову криптографічного перетворення таким чином, щоб максимально ускладнити відновлення алгебраїчних та статистичних зв'язків між від відкритим текстом, ключем та шифрованим текстом. Тому найбільш поширеним методом побудови сучасних БШ для комп'ютерних систем є метод, заснований на застосуванні ітераційних схем [3], в яких криптографічне перетворення реалізується шляхом суперпозиції багато разів повторюваних простих з точки зору обчислювальної складності перетворень, кожне з яких вносить певний внесок в сумарне розсіювання і перемішування. В зв'язку з цим виникає питання про знаходження такого набору операцій на множині бітових векторів (відкритих текстів), які, з одного боку, зручно реалізуються програмним або апаратним способом, а з іншого – мають «хороші» перемішуючі та розсіювачі властивості [10]-[15].

З іншого боку, при оцінюванні стійкості БШ до різних методів криптоаналізу (зокрема, до лінійного та різницевого) дослідники іноді намагаються замість вихідного шифру використовувати його спрощену модель. При цьому, автори зменшують кількість раундів БШ, змінюють ключовий розклад, а особливо часто замінюють (явно або неявно) модульне додавання у ключовому суматорі на покомпонентне (побітове). Таке спрощення найчастіше використовується для алгоритмів ГОСТ 28147-89, "Мухомор", "Калина" [16] - [18]. Там операція додавання за модулем 2^{32} замінюється операцією побітового додавання, що суттєво спрощує криптоаналіз. Якихось обґрунтованих аргументів стосовно математичної коректності такої заміни у роботах не наводиться; лише деякі міркування відносно того, що при заміні нелінійної (відносно $\oplus$) операції на лінійну стійкість алгоритму не зростає. Оскільки такі міркування зустрічаються досить часто, то постає питання: "Чи можна при оцінці криптографічної стійкості алгоритму замінювати одну операцію на іншу, отримуючи при цьому еквівалентний у сенсі криптостійкості алгоритм?". Саме відповіді на це питання, а також на деякі суміжні з ним, присвячена дана робота.

Тому актуальність даної роботи визначається необхідністю обґрунтування можливості використання модифікацій БШ з заміною операції у ключовому суматорі або, навпаки, обґрунтуванням некоректності такої заміни.

Метою даної роботи є отримання та порівняння імовірнісних характеристик операцій покомпонентного та модульного додавання, отримання імовірностей співпадіння результатів цих операцій, формування висновків щодо коректності використання відповідних моделей БШ для оцінки стійкості вихідного алгоритму, а також виявлення можливої вразливості шифру до певних типів різницевих атак за умови наявності додаткової інформації щодо того, що при оцінці стійкості даного шифру використовувалась його модифікація, отримана шляхом заміни операції у ключовому суматорі на деяку іншу.

Схожі питання для побітових операцій розглянуті в [18], проте у цій роботі отримано узагальнення її результатів на випадок довільного простого модуля p, але лише в частковому випадку двох доданків.

1. Допоміжні позначення та результати

При доведенні основних результатів будуть використовуватись наступні позначення та твердження. Тут і надалі під $\left(V_n(p), \oplus_p\right)$ будемо розуміти множину векторів довжини n з операцією покомпонентного додавання за модулем простого числа p, а під $\left(Z_{p^n}, +\right)$ – адитивну групу кільця лишків з операцією додавання за модулем p^n. Кожному цілому числу $z \in Z_{p^n}$ поставимо у відповідність вектор довжини n, що є p-арним поданням цього числа. Таким чином, ми ототожнюємо множини Z_{p^n} та $V_n(p)$. Ціле число та відповідний йому p-арний вектор ми будемо позначати однаково; з контексту буде зрозуміло, яке саме подання мається на увазі.

Для будь-якого $t \geq 0$ введемо наступні позначення:

$$s_t = \left(\frac{1}{2} + \frac{1}{2p^t}\right); \quad q_t = 1 - s_t.$$

Лема 1: нехай випадкові величини x та y рівноімовірно розподілені на множині $\{0, \ldots, a-1\}$, $a \in N$. Тоді

$$P(x + y < a) = P(x + y \geq a - 1) = \frac{1}{2} + \frac{1}{2a};$$

$$P(x + y < a - 1) = P(x + y \geq a) = \frac{1}{2} - \frac{1}{2a}.$$

Доведення. За формулою повної імовірності,

$$P(x+y<a)=\sum_{i=0}^{a-1}P(x+y<a/y=i)\cdot P(y=i)=\sum_{i=0}^{a-1}P(x<a-i)\cdot P(y=i)=$$

$$=\frac{1}{a}\sum_{i=0}^{a-1}P(x<a-i)=\frac{1}{a}\sum_{j=1}^{a}P(x<j)=\frac{1}{a}\sum_{j=1}^{a}\frac{j}{a}=\frac{1}{a^2}\cdot\frac{(a+1)\cdot a}{2}=\frac{a+1}{2a}=\frac{1}{2}+\frac{1}{2a}.$$

Аналогічно доведемо друге твердження леми:

$$P(x+y<a-1)=$$

$$\sum_{i=0}^{a-1}P(x+y<a-1/y=i)\cdot P(y=i)=\sum_{i=0}^{a-1}P(x<a-i-1)\cdot P(y=i)=$$

$$=\frac{1}{a}\sum_{i=0}^{a-1}P(x<a-i-1)=\frac{1}{a}\sum_{j=0}^{a-1}P(x<j)=\frac{1}{a}\sum_{j=1}^{a-1}P(x<j)=\frac{1}{a}\sum_{j=1}^{a-1}\frac{j}{a}=$$

$$=\frac{1}{a^2}\cdot\frac{(a-1)\cdot a}{2}=\frac{a-1}{2a}=\frac{1}{2}-\frac{1}{2a}.$$

Оскільки

$$P(x+y<a)=1-P(x+y\ge a)=\frac{1}{2}+\frac{1}{2a}$$

та

$$P(x+y<a-1)=1-P(x+y\ge a-1)=\frac{1}{2}-\frac{1}{2a},$$

то

$$P(x+y\ge a)=P(x+y<a-1)=\frac{1}{2}-\frac{1}{2a}$$

і

$$P(x+y\ge a-1)=P(x+y<a)=\frac{1}{2}+\frac{1}{2a}.$$

Лему доведено.

Лема 2: нехай випадкові величини *x* та *y* рівноімовірно розподілені на групі $\left(Z_{p^n},+\right)$. Тоді

$$P(x\le y)=\frac{1}{2}+\frac{1}{2p^n}=s_n;\ P(x>y)=\frac{1}{2}-\frac{1}{2p^n}=q_n.$$

Доведення: позначимо $s=P(x>y)$. Зазначимо, що $P(x=y)=\frac{p^n}{p^{2n}}=\frac{1}{p^n}$. Знайдемо *s*. Використовуємо те, що $P(x\le y)=1-P(x>y)$; тоді

$$P(x<y)+P(x=y)=1-P(x>y).$$

Оскільки $P(x>y)=P(x<y)=s$, отримаємо рівність $s+\frac{1}{p^n}=1-s$, звідки $s=\frac{1}{2}-\frac{1}{2p^n}$.

Тоді

$$P(x>y)=s=\frac{1}{2}-\frac{1}{2p^n}\ ,\text{ а}$$

$$P(x\le y)=1-P(x>y)=1-s=1-\left(\frac{1}{2}-\frac{1}{2p^n}\right)=\frac{1}{2}+\frac{1}{2p^n}.$$

В наших позначеннях,

$$P(x>y)=\frac{1}{2}-\frac{1}{2p^n}=q_n\ \text{ та }\ P(x\le y)=\frac{1}{2}+\frac{1}{2p^n}=s_n.$$

Лему доведено.

2. Порівняння операцій модульного та покомпонентного додавання

Введемо наступні позначення. Нехай $m,n,p\in N$; зазвичай через *p* ми будемо позначати просте число.

Нехай $a,b\in Z_{p^n}$, $a=(a_{n-1},...,a_0), b=(b_{n-1},...,b_0)$.

Позначимо $z=(z_{n-1},...,z_0)$, де $z=(a+b)\bmod p^n$, та $y=(y_{n-1},...,y_0)$, де $y_i=(a_i+b_i)\bmod p$.

Також позначимо:

$$\nu_0=0,$$

$$\nu_i=\begin{cases}0, \text{ якщо } a_{i-1}+b_{i-1}+\nu_{i-1}<p,\\ 1, \text{ інакше,}\end{cases}$$

де $i=1,...,n-1$.

Зрозуміло, що ν_i є бітом переносу в наступний розряд при модульному додаванні чисел *a* та *b*.

Також ми будемо використовувати позначення розділу I.

В наших позначеннях справедлива наступна лема.

Лема 3: нехай випадкові величини *a* та *b* рівноімовірно розподілені Z_{p^n}. Тоді:

$$P(\nu_i=0)=s_i,\ P(\nu_i=1)=q_i,\ i=\overline{1,n}.$$

Доведення: з означення ν_i випливає, що

$$P(\nu_i=0)=P(\overline{a_{i-1}a_{i-2}...a_0}+\overline{b_{i-1}b_{i-2}...b_0}<p^i).$$

Тоді, за лемою 1, $P(\nu_i=0)=s_i, i=\overline{1,n}$.

Аналогічно, $P(\nu_i=1)=1-s_i=q_i, i=\overline{1,n}$.

Лему доведено.

З використанням леми 3 можна довести наступну теорему.

Теорема 4: послідовність $\nu_i, i\ge 1$, утворює однорідний ланцюг Маркова з початковим станом $\nu_0=0$ та з матрицею переходів

$$P=(p_{ij})_{i,j=1}^{2},$$

де $p_{00}=p_{11}=s_1;\ p_{01}=p_{10}=q_1$.

Доведення: за означенням,

$$P(\nu_i=0)=P(a_{i-1}+b_{i-1}+\nu_{i-1}<p),$$

$$P(\nu_i=1)=1-P(\nu_i=0).$$

Тому $P(\nu_i=a/\nu_{i-1,...,\nu_1})=P(\nu_i=a/\nu_{i-1})$,

що відповідає означенню ланцюга Маркова.

Імовірності переходів обчислимо безпосередньо:

$$P_{11}=P(\nu_i=1/\nu_{i-1}=1)=P(a_{i-1}+b_{i-1}+1\ge p)=P(a_{i-1}+b_{i-1}\ge p-1)=\frac{1}{2}+\frac{1}{2p}=s_1;$$

$$P_{01}=P(\nu_i=1/\nu_{i-1}=0)=P(a_{i-1}+b_{i-1}\ge p)=\frac{1}{2}-\frac{1}{2p}=q_1;$$

$$P_{10}=P(\nu_i=0/\nu_{i-1}=1)=P(a_{i-1}+b_{i-1}+1<p)=P(a_{i-1}+b_{i-1}<p-1)=\frac{1}{2}-\frac{1}{2p}=q_1;$$

$$P_{00}=P(\nu_i=0/\nu_{i-1}=0)=P(a_{i-1}+b_{i-1}<p)=\frac{1}{2}+\frac{1}{2p}=s_1.$$

Теорему доведено.

Сформулюємо наслідки з теореми 4.

Наслідок 5: позначимо $p_i = P(y_i = z_i)$. Тоді $p_i = \frac{1}{2} + \frac{1}{2p^i}$, тобто $p_i \to \frac{1}{2}, i \to \infty$.

Доведення: за лемою 1, $P(y_i = z_i) = P(\nu_i = 0) = \frac{1}{2} + \frac{1}{2p^i}$. Наслідок доведено.

Наслідок 6: у наших позначеннях

$$P(y = z) = \left(\frac{1}{2} + \frac{1}{2p}\right)^{n-1}.$$

Доведення: так як послідовність ν_i, $i \geq 1$, утворює однорідний ланцюг Маркова з початковим станом $\nu_0 = 0$, маємо:

$$P(y = z) = P(\bigcap_{i=0}^{n-1}\{y_i = z_i\}) = P(y_{n-1} = z_{n-1} \Big/ y_0 = z_0, ..., y_{n-2} = z_{n-2}) \times$$
$$P(y_{n-2} = z_{n-2} \Big/ y_0 = z_0, ..., y_{n-3} = z_{n-3}) \cdot ... \cdot P(y_1 = z_1 \Big/ y_0 = z_0) =$$
$$P(\nu_{n-1} = 0 \Big/ \nu_0 = 0, ..., \nu_{n-2} = 0) \times$$
$$P(\nu_{n-2} = 0 \Big/ \nu_0 = 0, ..., \nu_{n-3} = 0) \cdot ... \cdot P(\nu_1 = 0 \Big/ \nu_0 = 0) \cdot P(\nu_0 = 0) =$$
$$P(\nu_{n-1} = 0 \Big/ \nu_{n-2} = 0) \times$$
$$P(\nu_{n-2} = 0 \Big/ \nu_{n-3} = 0) \times ... \times P(\nu_1 = 0 \Big/ \nu_0 = 0) \cdot 1 = s_1^{n-1} = \left(\frac{1}{2} + \frac{1}{2p}\right)^{n-1}.$$

Наслідок доведено.

Наслідок 7: у наших позначеннях справедлива рівність:

$$P(y_0 = z_0,\ y_1 = z_1, ...,\ y_{k-1} = z_{k-1},\ y_k \neq$$
$$z_k,\ y_{k+1} \neq z_{k+1},\ ...,\ y_{n-1} \neq z_{n-1}) = \left(\frac{1}{2} + \frac{1}{2p}\right)^{n-2} \cdot \left(\frac{1}{2} - \frac{1}{2p}\right),$$

де $k = 1,...,n-1$.

Доведення: за формулою множення імовірностей,

$$P(y_0 = z_0, y_1 = z_1, ..., y_{k-1} = z_{k-1}, y_k \neq$$
$$z_k, y_{k+1} \neq z_{k+1}, ..., y_{n-1} \neq z_{n-1},) =$$
$$P(\nu_0 = 0) \cdot P(\nu_1 = 0 \Big/ \nu_0 = 0) \times$$
$$\times P(\nu_2 = 0 \Big/ \nu_1 = 0) \cdot ... \cdot P(\nu_{k-1} = 0 \Big/ \nu_{k-2} = 0) \cdot$$
$$P(\nu_k = 1 \Big/ \nu_{k-1} = 0) \cdot P(\nu_{k+1} = 1 \Big/ \nu_k = 1) \cdot$$
$$P(\nu_{k+2} = 1 \Big/ \nu_{k+1} = 1) \cdot ... \times$$
$$\times P(\nu_{n-1} = 1 \Big/ \nu_{n-2} = 1) =$$
$$1 \cdot \left(\frac{1}{2} + \frac{1}{2p}\right)^{k-1} \cdot \left(\frac{1}{2} - \frac{1}{2p}\right) \cdot \left(\frac{1}{2} + \frac{1}{2p}\right)^{n-k-1} =$$
$$\left(\frac{1}{2} + \frac{1}{2p}\right)^{n-2} \cdot \left(\frac{1}{2} - \frac{1}{2p}\right).$$

Наслідок 8: імовірність того, що при модульному та покомпонентному додаванні в результаті утвориться $k < n-1$ переходів між блоками, в яких всі компоненти співпадають, та блоками, в яких всі компоненти не співпадають, визначається наступною формулою:

$$\left(\frac{1}{2} + \frac{1}{2p}\right)^{n-k-1} \cdot \left(\frac{1}{2} - \frac{1}{2p}\right)^{k}.$$

Доведення здійснюється аналогічно доведенню наслідку 7.

3. Порівняння результатів операцій модульного та покомпонентного віднімання

Позначимо $w = (w_{n-1}, ..., w_0)$, де $w = (a-b) \bmod p^n$ та $u = (u_{n-1}, ..., u_0)$, де $u_i = (a_i - b_i) \bmod p$.

Також позначимо:

$$\mu_i = 0;$$
$$\mu_i = \begin{cases} 0, \text{ якщо } a_{i-1} - \mu_{i-1} \geq b_{i-1} \\ 1, \text{ інакше.} \end{cases}, i = 1..n-1.$$

Зрозуміло, що μ_i є бітом запозичення в наступному розряді при модульному відніманні чисел *a* та *b*.

Також ми будемо використовувати позначення пункту 1.

В наших позначеннях справедлива наступна лема:

Лема 9: нехай випадкові величини *a, b* рівноімовірно розподілені на Z_{p^n}. Тоді:

$$P(\mu_i = 0) = s_i,\ P(\mu_i = 1) = q_i,\ i = \overline{1,n}.$$

Доведення: з означення μ_i, випливає, що

$$P(\mu_i = 0) = P(\overline{a_{i-1}a_{i-2}...a_0} \geq \overline{b_{i-1}b_{i-2}...b_0}).$$

Тоді, за лемою 2,

$$P(\mu_i = 0) = s_i, i = \overline{1,n}.$$

Аналогічно,

$$P(\mu_i = 1) = 1 - s_i = q_i, i = \overline{1,n}.$$

З використанням леми 9 можна довести наступну теорему.

Теорема 10: послідовність μ_i, $i \geq 1$, утворює однорідний ланцюг Маркова з початковим станом $\mu_0 = 0$ та з матрицею переходів

$$P = (p_{ij})_{i,j=1}^{2},$$

де $p_{00} = p_{11} = s_1;\ p_{01} = p_{10} = q_1$.

Доведення: за означенням,

$$P(\mu_i = 0) = P(a_{i-1} - \mu_{i-1} \geq b_{i-1}),$$
$$P(\mu_i = 1) = 1 - P(\mu_i = 0).$$

Тому

$$P(\mu_i = a / \mu_{i-1},...,\mu_0) = P(\mu_i = a / \mu_{i-1}),$$

що відповідає означенню ланцюга Маркова.

Імовірності переходів обчислимо безпосередньо:

$$P_{11} = P(\mu_i = 1 / \mu_{i-1} = 1) =$$

$$P(a_{i-1} - 1 < b_{i-1}) = P(a_{i-1} < b_{i-1} + 1) =$$

$$= \sum_{k=0}^{p-1} P\left(a_{i-1} < b_{i-1} + 1 / a_{i-1} = \kappa\right) \cdot P(a_{i-1} = \kappa) =$$

$$\sum_{k=0}^{p-1} P\left(k < b_{i-1} + 1\right) \cdot P(a_{i-1} = k) =$$

$$= \frac{1}{p} \cdot (p + p - 1 + p - 2 + ... + 1) \cdot \frac{1}{p} =$$

$$\frac{1}{p} \cdot \frac{1+p}{2} \cdot p \cdot \frac{1}{p} = \frac{1}{2p} + \frac{1}{2} = s_1;$$

$$P_{01} = P(\mu_i = 1 / \mu_{i-1} = 0) = P(a_{i-1} < b_{i-1}) = \frac{1}{2} - \frac{1}{2p} = q_1;$$

$$P_{10} = P(\mu_i = 0 / \mu_{i-1} = 1) =$$

$$P(a_{i-1} - 1 \geq b_{i-1}) =$$

$$1 - P(a_{i-1} - 1 < b_{i-1}) =$$

$$1 - (\frac{1}{2} + \frac{1}{2p}) = \frac{1}{2} - \frac{1}{2p} = q_1;$$

$$P_{00} = P(\mu_i = 0 / \mu_{i-1} = 0) = P(a_{i-1} \geq b_{i-1}) = \frac{1}{2} + \frac{1}{2p} = s_1.$$

Теорему доведено.

Сформуємо наслідки з теореми 10.

Наслідок 11: позначимо $p_i = P(w_i = u_i)$.

Тоді $p_i = \frac{1}{2} + \frac{1}{2p^i}$, тобто $p_i \to \frac{1}{2}, i \to \infty.$

Доведення:

За лемою 2, $P(w_i = u_i) = P(\mu_i = 0) = \frac{1}{2} + \frac{1}{2p^i}$.

Наслідок доведено.

Наслідок 12: у наших позначеннях

$$P(w = u) = \left(\frac{1}{2} + \frac{1}{2p}\right)^{n-1}.$$

Доведення: так як послідовність μ_i, $i \geq 1$, утворює однорідний ланцюг Маркова з початковим станом $\mu_0 = 0$, маємо:

$$P(w = u) = P(\bigcap_{i=0}^{n-1} \{w_i = u_i\}) =$$

$$= P(w_{n-1} = u_{n-1} / w_0 = u_0, ..., w_{n-2} = u_{n-2}) \cdot$$

$$P(w_{n-2} = u_{n-2} / w_0 = u_0, ..., w_{n-3} = u_{n-3}) \cdot ... \cdot$$

$$P(w_1 = u_1 / w_0 = u_0) =$$

$$= P(\mu_{n-1} = 0 / \mu_0 = 0, ..., \mu_{n-2} = 0) \cdot$$

$$P(\mu_{n-2} = 0 / \mu_0 = 0, ..., \mu_{n-3} = 0) \cdot ... \cdot$$

$$P(\mu_1 = 0 / \mu_0 = 0) \cdot P(\mu_0 = 0) =$$

$$= P(\mu_{n-1} = 0 / \mu_{n-2} = 0) \cdot P(\mu_{n-2} = 0 / \mu_{n-3} = 0) \cdot ... \cdot$$

$$P(\mu_1 = 0 / \mu_0 = 0) \cdot 1 = s_1^{n-1} = \left(\frac{1}{2} + \frac{1}{2p}\right)^{n-1}.$$

Наслідок доведено.

Наслідок 13: у наших позначеннях виконується рівність

$$P(w_0 = u_0, w_1 = u_1, ..., w_{k-1} = u_{k-1}, w_k \neq u_k, w_{k+1} \neq u_{k+1}, ..., w_{n-1} \neq u_{n-1},) =$$

$$= \left(\frac{1}{2} + \frac{1}{2p}\right)^{n-2} \cdot \left(\frac{1}{2} - \frac{1}{2p}\right),$$

Доведення наслідку здійснюється аналогічно доведенню наслідку 6.

Наслідок 14: імовірність того, що при модульному та покомпонентному відніманні в результаті утвориться $k < n$-1 переходів між блоками, в яких всі компоненти співпадають, та блоками, в яких всі компоненти не співпадають, визначається наступною формулою:

$$\left(\frac{1}{2} + \frac{1}{2p}\right)^{n-k-1} \cdot \left(\frac{1}{2} - \frac{1}{2p}\right)^{k}.$$

Доведення здійснюється аналогічно доведенню наслідку 13.

4 Загрози зменшення криптографічної стійкості шифру у разі некоректної заміни його окремих компонент

Як видно з попередніх розділів, результати операцій побітового та модульного додавання суттєво відрізняються. Це призводить до висновку, що різницеві характеристики перетворень, які є складовими шифру, теж можуть суттєво відрізнятись при різних вхідних/вихідних операціях. Зокрема цей факт ще раз підтверджує, що стійкість шифру до класичного (побітового) різницевого криптоаналізу не гарантує його стійкість до цілочисельного, і навпаки. Але, крім цього, цю особливість взаємної поведінки операцій можна також використати для внесення певних змін в структуру шифру, що призведуть до навмисного погіршення його різницевих характеристик. Важливо, що при цьому користувач шифру буде вважати, що зміни внесено для покращення різницевих властивостей шифру. Далі розглянемо декілька ситуацій з внесенням таких змін.

Введемо наступні позначення. Для довільного $n \in N$ позначимо через $V_n = \{0,1\}^n$ множину n-вимірних бітових векторів. Тут і надалі векторам з V_n будуть природнім чином ставитись у відповідність цілі числа від 0 до $2^n - 1$, $n \in N$.

Якщо $n = pu, \quad p \geq 2,$ то будь-який $x \in V_n$ може бути поданий у вигляді $x = (x^{(p)}, ..., x^{(1)})$, $x^{(i)} \in V_u, \quad i = \overline{1, p}$.

На множині V_n введемо наступні операції та відображення. Для довільних $a,b \in V_n$ через $a \oplus b$ будемо позначати результат побітового додавання векторів *a* та *b*, а через $a+b$ та $a-b$ відповідно результати додавання та віднімання цілих чисел за модулем 2^n.

Бієктивне відображення $S: V_n \to V_n$ задамо наступним чином:

$\forall x \in V_n: \ S(x) = (S^{(p)}(x^{(p)}), ..., S^{(1)}(x^{(1)})), \quad x^{(i)} \in V_u, i = \overline{1, p}$,

де $S^{(i)}: V_u \to V_u, \quad i = \overline{1, p}$ – бієктивні відображення. Це відображення часто називають блоком підстановки, а відображення $S^{(i)}$ – *s*-блоками.

Нехай $L: V_n \to V_n$ – лінійний оператор.

Для довільної функції $F: V_n \times V_n \to V_n$ позначимо $F_k(x) := F(k, x), \ k, x \in V_n$. Ми будемо розглядати шифри, у яких раундові функції мають вигляд

$$F_k(x) = L\big(S(x \oplus k)\big) \text{ або } F_k(x) = L\big(S(x + k)\big). \quad (1)$$

Для довільного s-блока покладемо

$$d^s_{\oplus,+}(\alpha, \beta) = 2^{-u} \sum_{k \in V_u} \delta(s(k \oplus \alpha) - s(k), \beta), \quad (2)$$

$$d^s_{\oplus,\oplus}(\alpha, \beta) = 2^{-u} \sum_{k \in V_u} \delta(s(k \oplus \alpha) \oplus s(k), \beta), \quad (3)$$

$$d^s_{+,+}(\alpha, \beta) = 2^{-u} \sum_{k \in V_u} \delta(s(k + \alpha) - s(k), \beta), \quad (4)$$

$$d^s_{+,\oplus}(\alpha, \beta) = 2^{-u} \sum_{k \in V_u} \delta(s(k + \alpha) \oplus s(k), \beta). \quad (5)$$

Також покладемо

$$\Delta^s_{\oplus,+} = \max_{\alpha, \beta \in V_u \setminus \{0\}} d^s_{\oplus,+}(\alpha, \beta), \quad (6)$$

і аналогічно визначимо

$$\Delta^s_{\oplus,\oplus}, \quad \Delta^s_{+,+} \text{ та } \Delta^s_{+,\oplus}. \quad (7)$$

Зауважимо, що імовірність диференціалу шифру та імовірність його диференціальної характеристики прямо пропорційна Δ^u, де Δ – один з параметрів (6) та (7), в залежності від операції у ключовому суматорі та від операції, відносно якої беруться вхідна та вихідна різниці. Показник степені залежить від відповідного індексу галуження та деяких інших параметрів шифру. Тому, збільшуючи імовірність раундового диференціалу, ми тим самим збільшуємо імовірність диференціалу та диференціальної характеристики всього шифру, тобто зменшуємо його стійкість до різницевого криптоаналізу. Загрози зменшення стійкості шифру можна спостерігати у наступних варіантах внесення змін.

Загроза 1. Некоректна заміна ключового суматора.

Варіант 1а. Відбувається заміна ключового суматора з операції побітового додавання на операцію модульного додавання.

Аргументом для такої заміни може бути помилкове обґрунтування: підвищення нелінійності шифру призведе до збільшення стійкості до різницевого криптоаналізу.

Потенційна загрозою у цьому варіанті є зменшення стійкості до цілочисельного або класичного різницевого криптоаналізу.

Умовою реалізації загрози є наявність у раундовій функції таких s-блоків, для яких

$$\Delta^s_{+,\oplus} > \Delta^s_{\oplus,\oplus} \quad (8)$$

або

$$\Delta^s_{+,+} > \Delta^s_{\oplus,+}. \quad (9)$$

Дійсно, згідно [19], після такої заміни ключового суматора максимальна імовірність раундового побітового диференціалу буде визначатись параметром $\Delta^s_{+,\oplus}$ замість $\Delta^s_{\oplus,\oplus}$, а імовірність раундового цілочисельного диференціалу – параметром $\Delta^s_{+,+}$ замість $\Delta^s_{\oplus,+}$.

З метою перевірки положень було проведено моделювання на комп'ютері, під час якого за методом бесповторного набору були сгенеровані конкретні значення s-блоків S_1 - S_{10} (зразки наведені на рис. 1, 2), що задовольняють умові (8).

В таблиці 1 наведені параметри $\Delta^s_{+,\oplus}$ та $\Delta^s_{\oplus,\oplus}$, що визначатимуть максимальну імовірність раундового побітового диференціалу для сгенерованих s-блоків.

Таблиця 1

Параметри s-блоків S_1 - S_{10}, що задовольняють умові (8)

s-блок	$\Delta^s_{+,\oplus}$	$\Delta^s_{\oplus,\oplus}$	s-блок	$\Delta^s_{+,\oplus}$	$\Delta^s_{\oplus,\oplus}$
S_1	0,04296875	0,0390625	S_2	0,04296875	0,0390625
S_3	0,04296875	0,0390625	S_4	0,04296875	0,0390625
S_5	0,04296875	0,0390625	S_6	0,04296875	0,0390625
S_7	0,04296875	0,0390625	S_8	0,04296875	0,0390625
S_9	0,04296875	0,0390625	S_{10}	0,04296875	0,0390625

У підсумку моделювання на комп'ютері за методом бесповторного набору були сгенеровані значення s-блоків S_{11} - S_{20} (зразки наведені на рис. 3, 4), що задовольняють умові (9).

В таблиці 2 наведені обчислені їх параметри $\Delta^s_{+,+}$ та $\Delta^s_{\oplus,+}$, що визначатимуть імовірність раундового цілочисельного диференціалу.

B1	0D	F6	4B	AD	F3	D6	63	AC	FD	7A	EB	A1	C6	6C	06
B8	05	9B	7B	B0	18	45	A3	95	17	31	19	6D	73	59	83
DF	36	0B	71	41	68	C8	ED	26	21	B6	5A	4D	F4	E6	D5
B9	1C	09	44	12	D1	98	A4	CA	84	43	94	90	4C	C2	56
53	9E	54	6E	51	3A	23	D3	29	FB	10	3C	60	AF	9F	2E
CD	0C	82	46	91	27	99	DC	7D	FA	E4	74	5C	B5	BA	7C
4F	04	EF	8A	00	D0	2C	E9	81	F8	D7	BF	13	61	87	DA
4E	34	96	16	64	89	37	39	FF	6F	20	7F	B4	65	1A	F0
3D	24	C4	4A	A2	F1	42	DD	F2	EE	5B	8D	48	C5	50	B3
1D	E2	52	3B	C1	C3	B2	E8	BB	1B	1E	67	88	E1	57	CE
A0	69	35	A5	8B	0F	0A	1F	D8	78	38	B7	02	E0	2A	EC
79	72	AB	9A	AA	14	D9	62	5F	80	9C	C9	DB	BD	8E	E5
FE	D2	F7	A6	A9	C0	D4	32	77	15	3E	AE	28	CF	30	22
92	0E	9D	93	85	2F	6B	2B	5E	55	03	11	2D	F5	C7	6A
97	F9	49	E3	07	33	66	70	75	76	08	EA	BC	58	A7	CB
40	86	A8	7E	01	47	8C	FC	E7	DE	3F	5D	BE	8F	CC	25

3C	A9	95	E7	E5	4F	36	B8	3E	C1	B3	29	20	DC	F3	AB
6A	64	6E	85	D5	68	7F	87	CC	5C	80	E4	EB	93	BD	53
2A	81	50	7C	4D	CF	58	67	99	89	E2	3F	E6	CB	65	91
56	A8	42	1C	E1	A2	AC	5D	83	63	98	05	D7	B4	2B	61
C6	54	47	F1	D3	BC	9F	FD	7D	02	4C	FA	AD	F9	DF	0D
19	8E	A3	11	B0	FB	2F	07	B5	9C	23	9B	45	6B	00	94
D2	04	88	39	F5	E9	8F	1D	C2	EC	37	24	D6	3B	D0	35
51	C3	B2	21	1E	C9	C0	3A	48	13	0C	72	2E	40	43	BE
F0	82	74	34	A4	79	0A	4E	D1	7E	46	8A	52	59	26	09
BB	EA	DE	CE	ED	8D	15	A5	6F	C7	49	4B	E0	1F	25	BF
08	69	22	9E	2C	17	03	CA	77	8B	F6	FF	84	6C	BA	4A
F8	A6	73	30	92	0B	97	F2	12	B7	90	86	10	C8	27	E8
33	D8	1A	E3	06	01	31	AA	0F	A0	9A	16	66	A1	28	9D
0E	62	2D	EE	B6	60	70	57	FC	7A	6D	41	C4	5F	DA	71
7B	D9	8C	55	FE	B1	3D	5B	78	AF	CD	38	DB	32	C5	D4
44	DD	5E	96	B9	18	75	1B	14	A7	AE	EF	5A	76	F4	F7

Рис. 1. Значення S – блоків S_1 (зліва) та S_2

2A	A2	12	42	5E	1F	CA	2B	17	CE	3C	11	50	C0	CB	69
80	41	29	A7	06	87	DC	CD	DD	84	4C	EA	39	2F	34	58
81	0D	D8	6C	B4	4B	78	48	98	B2	AB	D9	43	B6	EC	25
F0	AE	F9	89	40	30	55	93	60	7A	AC	BC	F7	1A	8D	04
7B	F5	D4	0B	6F	0E	E9	B8	9D	45	BE	FD	F2	2D	B0	E2
96	D5	7C	90	B9	6E	18	FC	C9	82	00	22	DB	73	ED	64
E3	91	9E	71	24	26	4D	14	A8	19	36	0F	85	B3	03	B7
95	67	75	56	3A	AA	BF	3F	6D	0C	FB	23	A0	E6	3D	C7
10	BA	D2	BB	8A	C1	7D	F6	32	15	99	21	9C	B1	1B	05
61	EF	35	C8	44	F1	47	EB	38	63	C5	4E	E4	86	27	A1
BD	D1	01	52	09	70	F3	3E	FA	28	D3	3B	E0	C6	DA	2E
A6	F8	1E	02	D0	08	92	5B	FF	46	7F	59	CC	8C	D6	8F
F4	C2	13	1C	CF	16	9F	AF	5A	6A	D7	7E	4A	AD	57	5F
54	8E	A9	9A	EE	68	77	E8	62	94	97	88	DF	FE	2C	49
31	51	74	A4	20	A5	8B	76	53	9B	07	72	E1	0A	33	37
C4	5D	A3	5C	4F	C3	65	1D	79	DE	6B	E7	B5	66	E5	83

1B	41	C8	03	A2	77	34	42	68	F6	E4	8A	44	45	5D	40
6F	9B	5C	C3	E5	11	23	83	6C	E8	0B	74	B5	9A	C9	29
D0	54	13	FE	36	3B	6D	E9	71	BB	19	8D	4A	1A	DE	05
2C	F5	7E	4C	3A	B2	7B	50	3C	12	69	DB	62	38	2D	27
20	9C	F0	26	60	B7	14	00	33	CA	18	D6	B6	E6	1D	09
C2	E0	06	39	0C	02	78	63	92	4E	C4	3E	6A	B9	CC	DF
21	F1	C7	D9	D1	F9	0F	A5	9E	7D	73	37	0D	0E	5E	A0
A4	79	85	A8	87	CE	1F	16	E3	B3	58	89	BF	2B	E1	BC
28	81	52	7F	D2	56	D7	49	6E	82	72	25	8E	51	E7	FC
53	C6	8C	2E	7A	70	96	EF	65	A1	4D	98	DA	6B	CF	C0
BD	F7	EB	AD	CD	8F	BA	46	B1	80	59	3F	9D	AE	4B	07
F4	17	FA	2F	99	94	AC	10	84	43	B0	AA	97	FF	48	90
C5	08	C1	1E	35	64	F8	A6	F3	7C	8B	5B	A3	AB	CB	B4
88	24	B8	61	76	FD	2A	31	75	66	95	A9	D3	1C	AF	DC
93	22	3D	47	F2	32	5F	0A	D8	04	D4	15	4F	01	DD	67
BE	55	EC	5A	E2	9F	30	86	FB	D5	EA	A7	ED	91	EE	57

Рис. 2. Значення S – блоків S_3 (зліва) та S_4

99	15	E4	56	8C	AC	7B	95	6E	40	84	35	BB	68	FD	9D
A5	DD	B4	3B	D3	C6	6C	6F	CE	41	61	F5	25	0B	1E	CC
7E	54	78	B2	3C	AA	7F	5C	55	0D	02	CB	A6	B6	27	2B
F8	59	88	39	2D	C3	7D	4D	A8	89	36	EF	DA	EC	47	DB
7C	1D	DF	5F	5D	A1	23	57	10	FF	D0	00	11	BE	DE	B7
EA	07	18	69	4B	94	E8	C4	DC	29	67	C9	97	86	ED	32
D1	21	2A	8D	9A	8B	20	74	3E	52	5E	03	51	34	C2	0E
0F	C5	43	1F	D8	E7	D9	05	76	E5	B3	7A	B9	72	63	D6
4A	AF	FA	F3	5A	A3	2E	CD	65	F0	14	5B	F1	FC	A0	77
60	AE	66	C8	30	62	C0	BA	6D	08	37	33	80	D5	64	70
F9	1B	9C	53	82	9B	D7	50	42	CF	45	8A	31	06	58	48
91	BF	4E	BD	F6	E9	CA	F4	C7	EE	13	2C	46	6B	0A	F2
3A	A2	17	D4	44	E2	A9	AD	1A	A4	E1	92	24	BC	38	04
87	71	B8	1C	90	3F	19	D2	22	8E	E0	98	2F	6A	09	C1
93	96	EB	75	01	73	8F	79	9E	28	26	A7	B0	0C	F7	3D
49	E6	4F	12	9F	FE	B1	4C	81	AB	FB	E3	85	B5	83	16

27	4E	5F	89	3B	11	62	0F	23	B3	F2	E1	D8	DE	71	43
8E	E4	78	EA	FB	C2	E2	D7	60	0C	92	D2	91	D4	9C	A5
51	E6	54	1F	44	B8	84	82	9E	FC	C6	3F	56	1E	20	8A
E8	8D	AD	9F	B6	34	4D	31	28	AB	ED	D3	57	C9	8B	B9
4F	A1	CC	AE	35	F6	08	0B	F3	6C	CD	61	22	EE	A8	8C
83	DA	CB	C1	15	58	D1	EB	87	A3	21	7E	6B	97	4B	FA
B1	41	F4	F8	A7	C7	C8	4C	DB	25	09	3D	66	6A	07	C4
AC	67	F1	29	18	01	A0	72	2A	C0	C5	BD	DD	13	53	88
93	A2	F5	C3	1C	5E	B5	FE	1A	37	74	55	A9	5A	E5	BE
52	B0	1B	68	EC	64	04	45	CF	7B	38	19	2E	47	9D	DC
1D	99	6F	14	10	90	E3	F0	95	2F	7D	12	75	7A	39	F9
03	FD	26	3A	98	7C	F7	59	96	24	70	33	30	5C	46	40
81	D6	94	63	79	E0	B2	48	5B	06	5D	E9	50	BB	9A	8F
FF	76	CA	3C	32	BC	2B	A4	B4	AF	9B	EF	2C	DF	6D	6E
B7	00	E7	3E	77	0E	0D	CE	2D	D9	49	73	16	86	02	65
0A	7F	A6	42	80	AA	BA	BF	85	D5	D0	4A	05	69	17	36

Рис. 3. Значення S – блоків S_{11} (зліва) та S_{12}

73	27	92	DE	17	D7	6F	A4	21	FA	F0	1F	3A	71	78	F5
D9	23	34	0B	C5	B7	76	C7	CF	91	4B	99	AA	88	9E	DF
82	8F	7C	96	2F	35	16	E1	5C	7D	14	AB	B0	E8	F7	0A
98	F6	80	B1	ED	D6	8E	60	08	F9	8D	19	24	DC	A9	01
E3	EA	45	E0	B9	6C	F3	3D	2B	72	C6	FD	EE	8B	29	2A
E6	BF	77	D2	1A	51	A8	FF	31	44	38	6D	95	1B	48	47
37	E5	AD	74	86	FB	36	F2	2D	70	EC	46	A1	54	5B	90
05	39	D8	87	4A	A7	11	75	62	DD	6A	A5	E9	0F	12	58
B4	CE	61	79	40	A2	D3	4D	B2	69	94	97	E7	3F	DB	07
28	AF	EB	CC	CA	64	59	8A	89	C9	26	43	65	84	D5	2C
B6	42	9C	E4	BC	22	AE	5D	30	BD	DA	FC	15	BA	57	9D
BB	83	53	A3	02	13	93	85	C1	9F	1C	3E	C2	56	63	7F
1D	06	C4	4E	00	68	CB	5E	EF	10	C0	2E	55	52	4C	04
B5	4F	81	D4	8C	1E	D0	7A	25	C8	7B	03	C3	5A	D1	41
66	09	6B	49	A6	50	3C	33	6E	0E	F1	7E	F8	67	32	9A
E2	F4	3B	BE	CD	0D	FE	9B	18	0C	B8	B3	AC	5F	20	A0

1D	48	02	BA	DD	AE	C7	3E	08	21	72	35	06	15	2C	E1
2B	5F	94	0A	78	C0	BC	99	19	D5	1A	FF	9D	69	03	85
77	DF	8A	FB	55	74	36	46	14	47	DA	4B	F8	A1	D3	82
D2	5A	CF	61	D1	2F	E6	BD	84	34	24	D0	11	0C	81	59
86	12	1B	EC	2D	27	9F	07	EF	8E	33	F3	50	95	39	76
41	16	66	B0	6A	F1	AF	52	C6	71	F5	CC	B2	A7	8F	FA
26	ED	7F	DC	7B	CA	A2	CD	37	AA	C3	9A	DE	A4	B8	D9
BB	45	54	F4	7E	5E	3B	B1	4F	D8	CB	6C	EE	0D	80	E8
44	13	DB	67	00	B6	6B	7C	F7	E4	1E	09	05	0E	A5	FD
89	EA	7D	8C	38	9C	A3	E3	2A	04	4C	29	9B	C2	90	C8
01	A9	F2	0B	68	1C	5D	FC	FE	30	32	3D	17	91	D4	C5
83	70	92	28	18	B5	43	49	2E	3A	98	F6	3F	3C	5B	AB
C1	96	9E	4D	23	87	25	CE	BF	10	79	73	6D	B4	51	A6
6E	65	C9	1F	58	5C	B9	8B	D6	42	6F	E9	D7	57	B3	8D
F9	31	88	0F	63	4E	B7	A8	60	A0	56	75	97	7A	53	BE
F0	93	E7	64	E0	4A	C4	E5	AC	EB	20	62	22	40	E2	AD

Рис. 4. Значення S – блоків S_{13} (зліва) та S_{14}

Таблиця 2

Параметри s-блоків S_{11} - S_{20}, що задовольняють умові (9)

s-блок	$\Delta^s_{+,+}$	$\Delta^s_{\oplus,+}$	s-блок	$\Delta^s_{+,+}$	$\Delta^s_{\oplus,+}$
S_{11}	0,03515625	0,03125	S_{12}	0,03125	0,0234375
S_{13}	0,03125	0,0234375	S_{14}	0,03515625	0,03125
S_{15}	0,03125	0,02734375	S_{16}	0,03125	0,02734375
S_{17}	0,03125	0,02734375	S_{18}	0,03515625	0,02734375
S_{19}	0,03125	0,02734375	S_{20}	0,03125	0,02734375

Варіант 1б. Передбачає заміну ключового суматора з операції модульного додавання на операцію побітового додавання.

У разі малої обчислювальної потужності процесора проектантам для збільшення швидкодії процедур криптографічного перетворення, враховуючи достатню нелінійність s-блоків, уявляється є зайвим внесення нелінійності модульного додавання, до того ж суттєво уповільнюючим процес шифрування.

Потенційною загроза у цьому варіанті є зменшення стійкості до цілочисельного або класичного різницевого криптоаналізу.

Умовою реалізації загрози є наявність у раундовій функції таких s-блоків, для яких

$$\Delta^s_{\oplus,\oplus} > \Delta^s_{+,\oplus} \quad (10)$$

або

$$\Delta^s_{\oplus,+} > \Delta^s_{+,+}. \quad (11)$$

Обгрунтування: згідно [19], після такої заміни ключового суматора максимальна імовірність раундового побітового диференціалу буде визначатись параметром $\Delta^s_{\oplus,\oplus}$ замість $\Delta^s_{+,\oplus}$, а імовірність раундового цілочисельного диференціалу – параметром $\Delta^s_{\oplus,+}$ замість $\Delta^s_{+,+}$.

У підсумку моделювання на комп'ютері за методом бесповторного набору були сгенеровані значення s-блоків S_{21} - S_{30} (зразки наведені на рис. 5, 6), що задовольняють умові (10), а в таблиці 3 наведені їх параметри $\Delta^s_{\oplus,\oplus}$ та $\Delta^s_{+,\oplus}$ та, що визначатимуть максимальну імовірність раундового побітового диференціалу.

```
2B 4C 58 CB B9 D7 FD E4 5A F3 F1 07 ED B4 53 3A    BB 07 37 F3 95 FC EC A1 FE 0E F1 32 77 E2 D6 C0
8A 0D 19 DC 65 F7 4E CD BC DA 9C C9 5D 42 75 7D    81 06 39 3F 5C AC 53 1D 5E 03 CE 0C 8E 51 19 63
93 14 2D AD 54 EA 57 25 46 51 67 FF 82 41 8E FA    08 40 AA 58 BC 4C C6 E5 D9 D8 97 DF BE B7 29 1F
56 1C C8 3E 52 DB 5B 7E D6 61 0C C2 77 D4 E3 A8    27 8F 6A EE E3 4A 4B AB 2A 73 B6 A7 FB C2 7D F8
AF 28 C3 59 E2 50 4A 43 B7 AA B0 02 32 94 87 89    E7 13 35 A8 D2 9C 66 A9 E0 EF 67 A4 52 61 17 24
9A D2 A3 34 2C 63 2E C5 30 60 36 9D 2A 6A 39 74    18 93 45 05 3A B5 36 CC 12 1A FD 76 8C 56 D0 00
11 C7 1A CF 9F EE 99 81 7A D8 5C C0 BB 09 A1 9E    F0 F5 F9 5A FF B0 AF B2 C5 55 31 C3 7C E9 E6 2E
C4 3B 5F 91 1F FC 96 D0 BD 8D D3 00 10 E1 A7 DF    9D 9F DB 3D C7 44 92 6D 4D 78 CB 47 20 0B 1B 72
8C 12 2F 16 26 A2 F4 1E 33 A6 08 6B F6 35 F2 B5    79 CF 4E A0 B9 7B 54 A2 B1 34 D1 14 57 26 43 E8
70 3F 6F F5 CC 38 CE FE 3D 80 97 A5 31 98 A0 01    25 91 C8 87 94 4F EA D5 3E AD 30 42 B8 2C B4 C1
8F 55 E0 C1 64 0E 48 44 AB B8 1D 40 4B B6 73 D9    E4 7E 9E 2D 49 89 15 23 7F 80 CD D7 DD F6 85 28
83 69 0F 06 72 27 0B 7B 0A FB 6D A4 8B 4D 92 15    33 F4 BD 09 DE 9B D4 74 2B 0F FA 65 5F 59 84 41
88 E8 86 AC 78 03 E9 BE 85 04 18 49 62 45 BF D1    7A 71 EB 3C 60 A3 BA E1 6F 10 1E 98 6E DA 62 70
84 29 47 EB 6E 23 CA F9 66 C6 20 F8 21 76 3C 17    02 69 A6 BF A5 82 88 50 3B 16 C9 04 01 CA 8B 64
13 90 DD BA 37 F0 24 5E 7C B3 7F E6 4F 1B AE A9    5B 1C 90 F2 46 11 21 5D 8D 6B 9A F7 ED 0D 48 B3
E7 DE 6C D5 E5 05 EC 71 EF 68 22 B2 79 B1 95 9B    AE 0A C4 2F 8A DC 68 75 86 96 99 38 83 22 D3 6C
```

Рис. 5. Значення S – блоків S_{21} (зліва) та S_{22}

```
67 E0 61 D6 FC 35 24 08 1D 9F 8F A4 79 21 37 9A    FF 35 DC 04 9C 2A FB 6F 12 E5 47 C3 C2 0D 3A 01
71 3D F9 1F A1 EA 4A D3 9C 1E B0 50 B8 23 F7 80    BD FC A6 59 AC 09 D9 C0 D7 82 7A 92 9B 62 EF CD
5C 53 5B 56 C5 2A D0 CD AC EB 3E E6 0F 15 28 95    B1 21 7E 49 83 24 66 52 BB 3F 1F B0 44 D2 8C AA
04 2E 3A C6 7A 5A 84 31 C2 1B 10 86 AA 85 38 92    E2 E3 AF 43 F9 C4 CE 30 8A FD 07 31 E1 8F 27 CF
39 EC 9B 3F C8 4C 00 88 A8 90 82 2B 43 70 7C 7D    F4 74 0F 70 81 99 61 A2 F2 CA 9F 73 4C A3 41 B9
B4 AB F0 B9 E1 E8 D5 12 BD 93 BC B1 8A FE FB F3    05 02 00 19 B2 84 68 F0 77 B5 A1 87 D6 96 E8 BE
F5 D4 77 CA 91 BB 9D 8E 7F DA C9 D9 11 0D 57 6F    36 5E 4B 76 9E 79 B4 18 F3 7C A0 C1 32 69 A5 7F
8B 64 3C A2 68 F4 D8 EF B3 76 44 BE DD E5 07 01    9D E4 88 AD 13 53 D8 20 6A 2B 2D 80 39 4E 37 0E
DF 40 5D 62 0E ED E4 6E 75 E3 20 2F 9E EE F2 06    2E 3E F5 94 B7 15 42 11 22 28 FE A4 5C 51 2C 75
46 2D FD C3 42 98 89 09 72 74 D1 C1 1C B2 AD 59    4A 6B 33 E9 1A 1C 6D C7 3C BC 60 0A E7 DA 1D 78
6C 87 4F DC 16 6D C7 32 02 4D DE 2C 5F A6 F8 E9    E6 98 2F 71 50 E0 03 08 85 F6 C6 8B D0 64 BA F1
22 CF 97 7B 4E B7 D2 27 FF 03 E7 55 B5 BA 0C 25    5B 40 6E EE 10 14 4D 6C DF 86 FA 4F DE 23 0B EA
B6 52 1A F6 51 0A 6A 48 45 C0 83 73 58 C4 41 47    A9 5D 7B 55 C5 57 F8 ED D4 9A C9 48 46 06 3B D5
33 8C 78 D7 49 13 AF A3 4B 36 5E 96 DB A0 6B 30    CB 34 A7 DD 56 90 A8 38 1E 91 29 D1 AE 63 97 3D
99 F1 CC AE A5 0B 14 FA CB 69 05 26 18 3B 63 66    B8 5F 25 26 93 AB 8D EB B6 65 B3 1B 16 72 67 CC
54 60 17 29 19 34 81 CE 7E A7 94 E2 A9 BF 8D 65    F7 89 95 0C 45 17 8E 54 7D C8 58 BF EC DB 5A D3
```

Рис. 6. Значення S – блоків S_{23} (зліва) та S_{24}

Таблиця 3

Параметри s-блоків S_{21} - S_{30}, що задовольняють умові (10)

s-блок	$\Delta^s_{\oplus,\oplus}$	$\Delta^s_{+,\oplus}$	s-блок	$\Delta^s_{\oplus,\oplus}$	$\Delta^s_{+,\oplus}$
S_{21}	0,046875	0,03125	S_{22}	0,046875	0,03125
S_{23}	0,0390625	0,03125	S_{24}	0,0390625	0,03125
S_{25}	0,046875	0,03125	S_{26}	0,046875	0,02734375
S_{27}	0,046875	0,02734375	S_{28}	0,046875	0,02734375
S_{29}	0,046875	0,02734375	S_{30}	0,046875	0,03125

У підсумку моделювання на комп'ютері за методом бесповторного набору були сгенеровані значення s-блоків S_{31} - S_{40} (зразки наведені на рис. 7, 8), що задовольняють умові (11), а в таблиці 4 наведені параметри $\Delta^s_{\oplus,+}$ та $\Delta^s_{+,+}$, що визначатимуть імовірність раундового цілочисельного диференціалу.

FC	01	BB	11	5F	0D	F7	87	96	1C	DA	CA	90	02	E7	A8
37	8B	D3	5A	59	46	3A	3F	72	32	CE	C5	93	8D	FB	41
22	4E	10	4A	D6	6A	C7	0E	B4	CF	DD	DF	76	CD	EB	BD
2A	27	13	25	18	EA	BA	9E	69	A9	F3	8F	99	05	E0	EE
66	B2	31	14	75	45	E2	0C	92	CC	9D	38	91	84	A0	55
68	8C	A4	4D	40	8A	88	A5	4C	AD	E5	80	86	D9	23	09
D0	C6	FE	C1	AC	D2	6D	65	C4	F5	B1	FA	3C	FF	24	36
D7	21	7D	07	B6	A2	C2	30	E9	3B	7F	AA	3E	97	79	71
7B	F0	E4	62	52	12	29	28	06	0F	20	95	04	AB	0B	4F
B9	4B	CB	7E	78	5D	D8	1E	16	E1	D5	EF	9C	E6	7A	67
73	B5	89	3D	34	35	AE	49	33	54	DC	03	58	C0	DE	2E
00	42	48	19	6F	63	85	77	F4	B7	56	81	6C	D4	26	B8
2F	F2	1D	2C	57	A1	74	F6	83	C8	A6	44	AF	8E	1B	A3
C3	5E	1A	BE	53	C9	BF	7C	D1	47	2D	51	B0	E3	70	9A
43	39	F9	A7	5B	82	17	F1	1F	60	2B	B3	50	DB	0A	9F
98	ED	61	F8	E8	5C	94	EC	6E	64	15	9B	08	6B	FD	BC

88	05	E8	52	53	66	F5	34	29	5B	C9	35	B5	E3	F7	06
1A	71	AD	02	92	E4	7B	43	2E	81	5A	A3	12	3F	A5	4B
28	41	2D	89	DF	BF	74	BE	C1	27	7A	20	3D	C5	97	D4
45	32	2A	5D	6A	CC	72	9B	49	94	3E	1F	B9	A6	87	E9
0A	2B	A9	CE	7D	ED	83	FD	21	57	3A	31	58	15	80	36
2C	38	75	98	4A	E1	54	04	AB	A2	69	11	BA	3C	09	84
7C	73	8D	07	78	B7	4F	B4	7F	D8	61	14	F6	BB	D2	47
77	0F	16	95	63	08	82	50	F4	EE	C4	DC	EF	1D	65	00
8C	D9	6D	6E	48	DA	0D	46	D6	B1	86	44	22	9D	F0	99
10	40	E5	1E	8B	F2	5C	A1	19	01	3B	93	BC	55	70	91
E6	1B	60	DD	62	EA	F3	B6	BD	96	51	E7	9E	03	0C	8A
67	37	6F	7E	18	C7	90	D5	8E	A8	33	56	6B	D1	68	B3
5F	AA	C8	CD	39	D0	9A	64	5E	26	4D	23	A4	9C	C3	25
30	D3	EB	76	0B	13	FE	2F	CA	AF	59	C0	B0	DE	4C	E0
FC	1C	CF	A0	AE	DB	F9	EC	B2	AC	FB	24	B8	17	85	C6
9F	FF	E2	F8	79	F1	D7	A7	42	6C	FA	CB	0E	C2	8F	4E

Рис. 7. Значення S – блоків S_{31} (зліва) та S_{32}

AA	F6	FF	52	A6	B3	9E	70	D6	81	12	00	4B	6D	DC	72
10	8D	18	F7	C5	AD	83	68	A8	FE	A7	3A	30	8F	99	A2
71	21	1D	17	A9	56	5F	A0	E9	2B	20	07	5D	55	4E	FA
1B	E5	B8	7E	02	1F	82	4A	75	BD	57	0C	BA	3E	AE	FB
76	94	EB	D5	C2	77	B6	38	16	EE	62	23	42	09	59	53
19	98	DB	27	B7	DE	22	B0	CA	F9	EA	31	05	11	50	5B
7A	28	B5	A1	92	E7	29	46	B4	33	25	D8	0B	49	85	6A
7F	EF	13	2D	54	A3	36	D7	58	8C	73	CF	35	BC	66	48
7D	BE	DF	80	E2	D3	F1	E1	F5	C7	74	69	91	E8	5A	1E
EC	34	E6	14	B9	C8	06	A5	60	08	1C	8B	9A	79	CC	CB
2C	86	6E	37	7C	AC	0E	93	0D	FC	84	D1	45	24	6B	CE
4D	B2	04	9F	61	CD	8A	C1	88	5C	F4	A4	C0	AF	26	4C
ED	39	44	8E	1A	2A	F8	F3	D9	AB	2E	BF	47	41	5E	97
C3	9B	C4	BB	96	6F	D4	DA	03	6C	B1	95	E0	4F	F0	0A
15	3F	E4	01	51	63	C9	40	D0	3B	64	87	43	78	9D	DD
3D	FD	7B	D2	67	89	65	3C	2F	F2	32	E3	90	9C	0F	C6

21	D4	1D	D9	7A	7B	FE	68	8A	8C	3B	1A	95	45	82	E7
36	49	CF	EE	05	75	C6	EA	2D	FC	4E	D0	46	6B	3C	E6
81	62	B0	61	35	66	4B	F0	67	A7	37	57	E2	E1	EF	65
BE	4D	8E	F2	07	69	B2	DF	5F	6C	71	0E	FA	41	04	43
48	BB	E4	27	9F	93	E8	AC	98	40	08	94	F3	54	03	1E
9B	EC	8B	F1	56	53	14	01	20	0C	2C	F5	BD	30	84	C9
10	5D	2F	6F	92	23	78	A9	26	52	F9	15	C7	72	8F	A1
D2	51	24	C3	89	B4	5B	87	B7	A3	CB	17	C0	55	FF	25
BC	29	3F	9C	BA	13	12	31	F8	9E	D3	44	E0	AA	AE	91
79	D8	39	F4	B1	E3	1C	2E	38	DD	88	90	19	22	F7	6E
A0	0D	99	74	AD	34	BF	C5	1B	5A	18	DB	3E	33	0B	32
B6	50	F6	83	B8	C2	5C	A4	59	85	64	4C	DE	47	9A	3D
C4	C1	8D	CD	DC	DA	5E	A2	D6	73	77	0F	86	CC	B5	6D
B9	A5	0A	CE	09	70	4A	63	58	C8	97	4F	9D	3A	E9	FB
02	06	1F	EB	7D	D7	7C	76	ED	FD	A8	D1	42	00	D5	28
E5	2A	6A	16	7E	96	80	11	AB	CA	A6	2B	60	7F	B3	AF

Рис. 8. Значення S – блоків S_{33} (зліва) та S_{34}

Таблиця 4

Параметри s-блоків S_{31} - S_{40}, що задовольняють умові (11)

s-блок	$\Delta^{s}_{\oplus,+}$	$\Delta^{s}_{+,+}$	s-блок	$\Delta^{s}_{\oplus,+}$	$\Delta^{s}_{+,+}$
S_{31}	0,03125	0,02734375	S_{32}	0,03125	0,02734375
S_{33}	0,03125	0,02734375	S_{34}	0,03515625	0,0234375
S_{35}	0,02734375	0,0234375	S_{36}	0,03125	0,02734375
S_{37}	0,03125	0,0234375	S_{38}	0,03125	0,02734375
S_{39}	0,02734375	0,0234375	S_{40}	0,03125	0,02734375

Загроза 2. Некоректна заміна s-блоків.

Відбувається заміна s-блоків з метою удосконалення шифру.

У цьому випадку метою заміни (реальною або замаскованою) є підвищення стійкості до побітового різницевого криптоаналізу.

Потенційною загрозою цього варіанту є зменшення стійкості до цілочисельного різницевого криптоаналізу.

Умовою реалізації загрози є наявність такого s-блоку s_1 у раундовій функції шифру та існування такого s-блоку s_2, для яких одночасно виконуються наступні умови:

якщо у ключовому суматорі шифру реалізовано операцію побітового додавання, то

$$\Delta^{s_1}_{\oplus,+} < \Delta^{s_2}_{\oplus,+},\ \Delta^{s_1}_{\oplus,\oplus} > \Delta^{s_2}_{\oplus,\oplus} \text{ та } \Delta^{s_1}_{\oplus,\oplus} < \Delta^{s_2}_{\oplus,+}; \quad (12)$$

якщо у ключовому суматорі шифру реалізовано операцію модульного додавання, то

$$\Delta^{s_1}_{+,+} < \Delta^{s_2}_{+,+},\ \Delta^{s_1}_{+,\oplus} > \Delta^{s_2}_{+,\oplus} \text{ та } \Delta^{s_1}_{+,\oplus} < \Delta^{s_2}_{+,+}. \quad (13)$$

Обґрунтування: згідно [19], максимальна імовірність раундового цілочисельного диференціалу після заміни s-блоку S_1 на s-блок S_2 буде визначатись параметром $\Delta^{s_2}_{\oplus,+}$ у першому випадку і $\Delta^{s_2}_{+,+}$ у другому випадку, і цей параметр буде більшим, ніж відповідні параметри, залежні від s_1, як для цілочисельного, так і для класичного диференціалу.

Для проведення експериментальних досліджень були обрані s-блоки, що наведені на рис. 9-13.

63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

$\Delta^{s_1}_{\oplus,\oplus} = 0{,}015625,\ \Delta^{s_1}_{\oplus,+} = 0{,}0234375,\ \Delta^{s_1}_{+,\oplus} = 0{,}02734375,\ \Delta^{s_1}_{+,+} = 0{,}02734375$

Рис. 9. S-блок для алгоритму AES (Federal Information Processing Standards Publication 197)

```
A8 43 5F 06 6B 75 6C 59 71 DF 87 95 17 F0 D8 09
6D F3 1D CB C9 4D 2C AF 79 E0 97 FD 6F 4B 45 39
3E DD A3 4F B4 B6 9A 0E 1F BF 15 E1 49 D2 93 C6
92 72 9E 61 D1 63 FA EE F4 19 D5 AD 58 A4 BB A1
DC F2 83 37 42 E4 7A 32 9C CC AB 4A 8F 6E 04 27
2E E7 E2 5A 96 16 23 2B C2 65 66 0F BC A9 47 41
34 48 FC B7 6A 88 A5 53 86 F9 5B DB 38 7B C3 1E
22 33 24 28 36 C7 B2 3B 8E 77 BA F5 14 9F 08 55
9B 4C FE 60 5C DA 18 46 CD 7D 21 B0 3F 1B 89 FF
EB 84 69 3A 9D D7 D3 70 67 40 B5 DE 5D 30 91 B1
78 11 01 E5 00 68 98 A0 C5 02 A6 74 2D 0B A2 76
B3 BE CE BD AE E9 8A 31 1C EC F1 99 94 AA F6 26
2F EF E8 8C 35 03 D4 7F FB 05 C1 5E 90 20 3D 82
F7 EA 0A 0D 7E F8 50 1A C4 07 57 B8 3C 62 E3 C8
AC 52 64 10 D0 D9 13 0C 12 29 51 B9 CF D6 73 8D
81 54 C0 ED 4E 44 A7 2A 85 25 E6 CA 7C 8B 56 80
```

$\Delta^{S_1}_{\oplus,\oplus} = 0{,}03125,\ \Delta^{S_1}_{\oplus,+} = 0{,}0234375,\ \Delta^{S_1}_{+,\oplus} = 0{,}0234375,\ \Delta^{S_1}_{+,+} = 0{,}03125$

Рис. 10. S-блок №1 для алгоритмів ДСТУ 7624:2014 та ДСТУ 7564:2014

```
CE BB EB 92 EA CB 13 C1 E9 3A D6 B2 D2 90 17 F8
42 15 56 B4 65 1C 88 43 C5 5C 36 BA F5 57 67 8D
31 F6 64 58 9E F4 22 AA 75 0F 02 B1 DF 6D 73 4D
7C 26 2E F7 08 5D 44 3E 9F 14 C8 AE 54 10 D8 BC
1A 6B 69 F3 BD 33 AB FA D1 9B 68 4E 16 95 91 EE
4C 63 8E 5B CC 3C 19 A1 81 49 7B D9 6F 37 60 CA
E7 2B 48 FD 96 45 FC 41 12 0D 79 E5 89 8C E3 20
30 DC B7 6C 4A B5 3F 97 D4 62 2D 06 A4 A5 83 5F
2A DA C9 00 7E A2 55 BF 11 D5 9C CF 0E 0A 3D 51
7D 93 1B FE C4 47 09 86 0B 8F 9D 6A 07 B9 B0 98
18 32 71 4B EF 3B 70 A0 E4 40 FF C3 A9 E6 78 F9
8B 46 80 1E 38 E1 B8 A8 E0 0C 23 76 1D 25 24 05
F1 6E 94 28 9A 84 E8 A3 4F 77 D3 85 E2 52 F2 82
50 7A 2F 74 53 B3 61 AF 39 35 DE CD 1F 99 AC AD
72 2C DD D0 87 BE 5E A6 EC 04 C6 03 34 FB DB 59
B6 C2 01 F0 5A ED A7 66 21 7F 8A 27 C7 C0 29 D7
```

$\Delta^{S_1}_{\oplus,\oplus} = 0{,}03125,\ \Delta^{S_1}_{\oplus,+} = 0{,}0234375,\ \Delta^{S_1}_{+,\oplus} = 0{,}02734375,\ \Delta^{S_1}_{+,+} = 0{,}0234375$

Рис. 11. S-блок №2 для алгоритмів ДСТУ 7624:2014 та ДСТУ 7564:2014

Тут в якості блоку S_1 може бути будь-який з s-блоків (№№ 1 – 4) алгоритмів ДСТУ 7624:2014 та ДСТУ 7564:2014 та AES.

Під час проведення експериментальних досліджень не вдалося отримати жодного s-блоку, який задовольняє умові (12).

В той же час існує досить багато s-блоків, що задовольняють умові (13). Зокрема, цій умові задовольняють майже всі s-блоки (крім s-блок №1) алгоритмів ДСТУ 7624:2014 та ДСТУ 7564:2014.

На рис. 14, 15 наведені конкретні значення s-блоків, що задовольняють умові (13), а в таблиці 3 наведені значення відповідних параметрів $\Delta^{S}_{+,\oplus}$ та $\Delta^{S}_{+,+}$.

```
93 D9 9A B5 98 22 45 FC BA 6A DF 02 9F DC 51 59
4A 17 2B C2 94 F4 BB A3 62 E4 71 D4 CD 70 16 E1
49 3C C0 D8 5C 9B AD 85 53 A1 7A C8 2D E0 D1 72
A6 2C C4 E3 76 78 B7 B4 09 3B 0E 41 4C DE B2 90
25 A5 D7 03 11 00 C3 2E 92 EF 4E 12 9D 7D CB 35
10 D5 4F 9E 4D A9 55 C6 D0 7B 18 97 D3 36 E6 48
56 81 8F 77 CC 9C B9 E2 AC B8 2F 15 A4 7C DA 38
1E 0B 05 D6 14 6E 6C 7E 66 FD B1 E5 60 AF 5E 33
87 C9 F0 5D 6D 3F 88 8D C7 F7 1D E9 EC ED 80 29
27 CF 99 A8 50 0F 37 24 28 30 95 D2 3E 5B 40 83
B3 69 57 1F 07 1C 8A BC 20 EB CE 8E AB EE 31 A2
73 F9 CA 3A 1A FB 0D C1 FE FA F2 6F BD 96 DD 43
52 B6 08 F3 AE BE 19 89 32 26 B0 EA 4B 64 84 82
6B F5 79 BF 01 5F 75 63 1B 23 3D 68 2A 65 E8 91
F6 FF 13 58 F1 47 0A 7F C5 A7 E7 61 5A 06 46 44
42 04 A0 DB 39 86 54 AA 8C 34 21 8B F8 0C 74 67
```

$\Delta^{S_1}_{\oplus,\oplus} = 0{,}03125,\ \Delta^{S_1}_{\oplus,+} = 0{,}02734375,\ \Delta^{S_1}_{+,\oplus} = 0{,}02734375,\ \Delta^{S_1}_{+,+} = 0{,}02734375$

Рис. 12. S-блок №3 для алгоритмів ДСТУ 7624:2014 та ДСТУ 7564:2014

```
68 8D CA 4D 73 4B 4E 2A D4 52 26 B3 54 1E 19 1F
22 03 46 3D 2D 4A 53 83 13 8A B7 D5 25 79 F5 BD
58 2F 0D 02 ED 51 9E 11 F2 3E 55 5E D1 16 3C 66
70 5D F3 45 40 CC E8 94 56 08 CE 1A 3A D2 E1 DF
B5 38 6E 0E E5 F4 F9 86 E9 4F D6 85 23 CF 32 99
31 14 AE EE C8 48 D3 30 A1 92 41 B1 18 C4 2C 71
72 44 15 FD 37 BE 5F AA 9B 88 D8 AB 89 9C FA 60
EA BC 62 0C 24 A6 A8 EC 67 20 DB 7C 28 DD AC 5B
34 7E 10 F1 7B 8F 63 A0 05 9A 43 77 21 BF 27 09
C3 9F B6 D7 29 C2 EB C0 A4 8B 8C 1D FB FF C1 B2
97 2E F8 65 F6 75 07 04 49 33 E4 D9 B9 D0 42 C7
6C 90 00 8E 6F 50 01 C5 DA 47 3F CD 69 A2 E2 7A
A7 C6 93 0F 0A 06 E6 2B 96 A3 1C AF 6A 12 84 39
E7 B0 82 F7 FE 9D 87 5C 81 35 DE B4 A5 FC 80 EF
CB BB 6B 76 BA 5A 7D 78 0B 95 E3 AD 74 98 3B 36
64 6D DC F0 59 A9 4C 17 7F 91 B8 C9 57 1B E0 61
```

$\Delta^{S_1}_{\oplus,\oplus} = 0{,}03125,\ \Delta^{S_1}_{\oplus,+} = 0{,}02734375,\ \Delta^{S_1}_{+,\oplus} = 0{,}02734375,\ \Delta^{S_1}_{+,+} = 0{,}02734375$

Рис. 13. S-блок №4 для алгоритмів ДСТУ 7624:2014 та ДСТУ 7564:2014

```
1B 95 9E 90 2A 26 FF F4 CE C2 7A 6E 75 DF C4 B5
5B 50 19 EB 4D 7C 1C 5E B6 7B ED 3A 1F B9 0E 64
CA A5 87 30 A4 01 92 12 1E 10 BE 2D 05 00 58 29
36 78 98 DE 11 70 AD 06 37 4E E0 07 65 34 EA D9
E5 97 16 35 CB 39 99 6C 8B 0C B0 B4 E4 03 A3 74
AA 24 C9 46 E3 B1 EC 18 BF 48 A0 86 BB D8 BD 42
C1 51 4A 69 2F 47 31 73 F9 A7 89 C0 A6 AC 2C A1
8A D3 17 AF AB 57 27 EF 5D F5 0F 2E 22 25 55 C6
52 20 A8 60 62 E7 CC 68 33 80 D6 28 7F AE B7 8F
82 D2 09 63 9D 14 4F 4B 96 7D D1 7E FB EE F8 76
BA D5 53 94 3F DD CF 9B 85 8C C7 1A 93 FA 3B 56
43 1D 6A D7 9A FC F0 88 38 D4 81 F3 54 F6 61 B3
9F B2 49 0B 21 3D 6B F1 59 C8 72 E8 F2 41 FE E2
DA 4C 9C 08 E9 91 5A 2B 44 A2 83 79 02 6D 23 FD
DC E1 77 DB 32 0D 5F 45 3E 6F 40 C3 B8 BC 66 3C
04 C5 8D D0 E6 A9 0A 67 84 8E CD 5C F7 13 71 15
```

```
9C 34 98 44 8B 45 8D 49 F6 46 04 CB FB B3 08 C5
43 EA 38 AB A7 E5 4A CA F7 5F B6 B1 CC D9 DB 02
CF 5C 75 BD 16 83 54 7B 14 73 36 4E 33 68 C3 26
01 3E A5 FE E0 94 C8 BF 37 B7 FA F1 FC 95 5B AD
15 7F C4 BB 52 11 5D 97 27 86 74 A6 B4 09 96 F4
20 07 3D 67 9A E9 5E AC FF 99 6B 1A 0E 17 D8 8F
61 30 10 7A 3B C1 D0 03 00 AF D6 BC D2 9B 79 CE
AE DC 40 32 DF A1 EF 41 66 6A 7E D4 B8 1E B2 C6
2B 3C 0F 84 9D D5 06 62 4F A3 F9 0D C7 93 ED 8C
B0 71 F5 63 48 F3 88 DD 23 EE 0B DA E8 7D 4B 22
1F 5A 31 4D EC 76 70 77 BE E4 A0 F0 69 65 57 13
DE 82 78 D1 72 C9 CD 05 12 D3 E3 47 FD E2 EB 60
0C 0A B5 1C 7C 80 2F 28 53 2E 8E 90 19 81 9F 50
9E E1 55 A8 42 1B C2 D7 89 E6 92 6D 64 3A 2C 35
59 18 B9 39 A9 21 E7 AA F2 BA 2A F8 A2 87 24 1D
29 25 8A 2D C0 6C 6E 4C 3F 58 51 6F 85 56 91 A4
```

Рис. 14. Значення S – блоків S_{41} (зліва) та S_{42}

```
EF 6E D7 68 3D 91 8D E2 6B 10 0E 35 CC 18 63 44
36 45 1E B6 43 7A 00 F3 12 B9 66 CF FF 07 4B 1C
1B 8E FB 9F 05 70 67 C8 5F 50 C9 BC 0B F5 C1 1A
46 65 C0 E5 F1 14 01 9A 0D 5E E4 88 6F AB 41 13
09 53 E9 A4 33 F7 95 79 06 84 A0 58 99 94 49 AE
A6 27 A8 BF E3 BE 4D 4C 57 EA 7C 42 DD 86 FD 87
A2 C4 EE A3 85 C3 64 93 DF 7F B0 76 C7 D3 ED AD
A9 E8 26 3A 38 B2 2C 73 CA 52 F0 31 19 39 4F D8
EC 81 89 74 E7 6C 69 15 CD 5A 8B B4 61 FE 3F DE
A5 E6 30 9B C2 0C F4 D9 08 C5 2E D6 8C FA 04 29
BA 3E 03 BB E0 0F 17 2D 9D 21 A7 D2 6D 82 4E 7D
2F 90 CB 92 D1 59 71 8A 6A A1 DC 34 5D D5 3B 83
98 AF 20 BD 5B AC 25 11 B7 FC EB 48 7E 77 8F D0
3C 40 56 47 72 F8 CE 55 4A F9 2B F2 75 80 60 7B
51 AA 62 D4 97 23 B8 96 2A 54 24 1F E1 9C C6 32
DA B5 37 16 F6 B1 B3 22 1D DB 0A 02 9E 78 5C 28
```

```
9F 95 69 3B 9E D3 99 93 2F E0 63 9B 94 2C 85 C0
56 82 E7 87 F1 8A 5F 00 97 1F 06 84 E5 EE CE 6A
71 F3 29 6B C7 43 F4 15 1C 8E 3D DE 40 01 C8 C9
51 B4 8F 12 20 96 3A F5 1A D9 59 D6 D5 67 C3 44
A2 A3 B9 7E 34 83 F2 5B A4 7B 58 45 92 BB F0 77
0D C2 D4 60 17 50 6C FB 3E 47 DD D2 6F 18 B0 CA
6E 27 54 FD AA 1E 2B BE 07 E2 3F 33 26 4D A0 10
CD 68 4C 37 49 A8 22 E4 39 64 ED 79 42 02 D0 4E
70 7D F8 0E AF C1 25 0C F9 9A AB B7 2E 38 41 B3
2D CF FC 21 4B A7 31 DF F7 52 89 81 13 E6 CB 23
B8 0B 32 A9 7C 72 5A 05 5D 28 0F B5 FE 16 4A 7A
61 BA 24 08 8B 98 AD 36 D7 EA 86 75 DC A1 C6 E1
53 AE B1 AC 74 55 48 EC 9D EF C4 35 19 62 A6 14
76 C5 5C BD 0A FF F6 91 7F 9C 04 11 E9 B2 30 1D
57 2A 66 BF 90 80 E8 FA B6 BC 09 E3 1B 78 73 4F
8C DB 03 6D 88 A5 CC 3C 8D 46 EB D1 D8 65 DA 5E
```

Рис. 15. Значення S – блоків S_{43} (зліва) та S_{44}

Таблиця 5

Параметри s-блоків S_{41} - S_{44} , що задовольняють умові (13)

s-блок	$\Delta^{s}_{+,\oplus}$	$\Delta^{s}_{+,+}$	s-блок	$\Delta^{s}_{+,\oplus}$	$\Delta^{s}_{+,+}$
S_{41}	0,0234375	0,03125	S_{42}	0,046875	0,03125
S_{43}	0,0390625	0,03125	S_{44}	0,0390625	0,03125

Висновки

Отримані результати свідчать про те, що імовірність співпадіння результатів модульного та покомпонентного додавання (віднімання) є дуже малою. Вона зменшується із зростанням довжини вектора (або ключового суматора) і прямує до нуля, коли довжина вектора прямує до нескінченості. Тому використання для аналізу стійкості блокового алгоритму такої його модифікації, в якій модульне додавання (віднімання) замінюється на покомпонентне, є некоректним, хоч і суттєво спрощує аналіз алгоритму.

Крім того, показано, що заміна операції у ключовому суматорі або блоку підстановки шифру недопустима без попередніх досліджень, що полягають в обчисленні і порівнянні відповідних параметрів. Якщо ж є додаткова інформація про те, що відбулись модифікації шифру, вказані у розділі 4, то модифікований шифр може бути більш вразливим до різницевих методів криптоаналізу. Аналогічно, якщо отримано додаткову інформацію про те, що під час дослідження криптографічної стійкості шифру розглядалась лише його відповідна модифікація, то сам шифр може виявитись вразливим до різницевих атак.

Література

[1]. A. Konheim, *Computer security and cryptography,* J.Wiley&Sons, Inc. Hoboken, New Jersey. 2007, 521 p.

[2]. M. Stamp, R. Low, *Applied cryptoanalysis: breaking ciphers in the real world*, J.Wiley&Sons, Inc. Hoboken, New Jersey, 2007, 401 p.

[3]. С. Панасенко, *Алгоритмы шифрования. Специальный справочник,* СПб.: БХВ-Петербург, 2009, 576 с.

[4]. А. Грушо, Э. Применко, Е. Тимонина, *Теоретические основы компьютерной безопасности: учеб. пособие для студентов высш. учеб. заведений*, М.: Изд.центр Академия, 2009, 272 с.

[5]. Г. Гулак, "Моделирование на этапе оценки безопасности шифраторов конфиденциальной информации", *Науково-практичний журнал «Сучасна спеціальна техніка»,* № 1(24), С. 73-81, 2011.

[6]. Г. Гулак, "Забезпечення безпеки засобів КЗІ у кіберпросторі", *Матеріали науково-технічної конференції «Сучасні інформаційно-телекомунікаційні технології», том ІУ Сучасні технології інформаційної безпеки*, К., С. 100-102, 2015.

[7]. Г. Гулак Г.М. "Оцінка інженерно криптографічних якостей під час тематичних досліджень криптосистем", *13 Міжнародна науково практична конференція «Математичне та імітаційне моделювання систем МОДС 2018» Київ, Чернігів Жукін, 25...29 червня 2018. Тези доповідей*. Чернігів ЧНТУ, С. 326-330, 2018.

[8]. Г. Гулак, П. Складанний, "Формування вимог щодо забезпечення гарантоздатності автоматизованих систем переробки інформації й управління критично-важливими об'єктами інфраструктури", *II Всеукраїнська науково-практична конференція «Кібербезпека в Україні: правові та організаційні питання» (Одесса, 17 листопада 2017р.),* Одесса: ОДУВС, С. 12-14, 2017.

[9]. К. Шеннон, "Теория связи в секретных системах", *Работы по теории информации и кибернетике*, М.: Издательство иностранной литературы, С. 333-402, 1963.

[10]. Ю. Горчинский, "О гомоморфизмах многоосновных универсальных алгебр в связи с криптографическими применениями", Труды по дискретной математике, Т. 1, М.: ТВП, С. 67– 84, 1997.

[11]. О. Шемякина, "О перемешивающих свойствах операций в конечном поле", *Труды Восьмой Общероссийской научной Конференции «Математика и безопасность информационных технологий» – (МаБИТ-09), 30 октября – 2 ноября 2009.*

[12]. Л. Ковальчук, О. Сиренко, "Анализ перемешивающих свойств операций модульного и побитового сложения, определенных на одном носителе", *Кибернетика и системный анализ*, № 5, С. 83-97, 2011.

[13]. Л. Ковальчук, О. Сиренко, "Анализ перемешивающих свойств операций в конечном кольце", *Сборник тезисов XIV Международной научно-практической конференции «Безопасность информации в информационно-телекоммуникационных системах», 17-20 мая 2011*, Киев, С. 45-46, 2011.

[14]. Л. Ковальчук, Н. Лысенко, Л. Скрыпник, "Перемешивающие свойства операций, определенных на множестве N-мерных векторов над простым конечным полем", *Кибернетика и системный анализ,* № 4, С. 135-145, 2014.

[15]. *ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования*. М.: Госстандарт СССР, 1989, 28 с.

[16]. И. Горбенко, М. Бондаренко, "Перспективний блоковий шифр «Мухомор» – основні положення та специфікація", *Прикладна радіоелектроніка*, Т. 6. №2, С. 147-157, 2017.

[17]. И. Горбенко, О. Тоцький, С. Казьміна, "Перспективний блоковий шифр «Калина» – основні положення та специфікація", *Прикладна радіоелектроніка*, Т. 6, №2, С. 195-208, 2007.

[18]. В. Галинский, "Вероятностные свойства переносов при сложении по модулю 2^n", *Обозрение прикладной и промышленной математики*, Т. 10, вып. 1, С. 129-130, 2003.

[19]. Л. Ковальчук, С. Пальченко, Л. Скрыпник, "Построение верхних оценок средних вероятностей целочисленных дифференциалов для композиции ключевого сумматора, блока подстановки и оператора циклического сдвига", *Труды Восьмой Общероссийской научной Конференции "Математика и безопасность информационных технологий" – (МаБИТ-09), Москва, 30 октября – 2 ноября 2009*, С. 74-87, 2010.

УДК 621.3.019.3+004.056

Гулак Г.Н. Анализ операций модульного и покомпонентного прибавления в блоковых шифрах

Аннотация. *В работе исследуются свойства операций модульного и покомпонентного сложения, которые используются в узлах блочных шифров и обеспечивают сложение ключевой информации (ключевые сумматоры), и их влияние на практическую криптографическую стойкость. Для этого получены вспомогательные*

результаты для функций распределения вероятностей обычных и модульных сумм независимых равномерно распределенных случайных величин. В основной части доказано, что последовательность битов переноса в следующий разряд при модульном сложении чисел образует однородную цепь Маркова с определенным начальным состоянием и соответствующей матрицей переходов, а также выведена формула вероятности того, что при модульном и покомпонентном сложении в результате образуется переходов между блоками, в которых все компоненты совпадают, и блоками, в которых все компоненты не совпадают. С учетом вспомогательных результатов в статье получены и сравнены вероятностные характеристики операций покомпонентного та модульного сложения, вычислены вероятности совпадения результатов этих операций, сделаны выводы о корректности (некорректности) использования соответствующих модификаций блочных шифров для получения оценок стойкости, приведены практически применимые образцы блоков замены для блочных шифров, которые соответствуют определенным условиям, определена возможность уязвимости шифра к определенным типам разностных атак при условии наличия дополнительной информации о том, что при оценке стойкости данного шифра использовалась его модификация, полученная путем замены операции в ключевом сумматоре на некоторую другую. В статье обоснован вывод, что замены операции в ключевом сумматоре или блоков подстановок шифра недопустима без предварительных исследований, суть которых в вычислении и сравнении соответствующих параметров.

Ключевые слова: *блочный шифр, блок замени, ключевой сумматор, операция модульного сложения, операция покомпонентного сложения, криптографическая стойкость.*

Hulak H. Analysis of modular and component addition operations in block codes

Abstract. *The paper investigates the properties of modular and componentwise addition operations, which are used in the nodes of block ciphers and provide the addition of key information (key adders), and their impact on practical cryptographic security. For this, auxiliary results are obtained for the probability distribution functions of ordinary and modular sums of independent uniformly distributed random variables. In the main part, it is proved that the sequence of carry bits in the next bit during modular addition of numbers is a homogeneous Markov chain with a certain initial state and the corresponding transition matrix, and also a formula for the probability that, during modular and componentwise addition, transitions between blocks are formed in which all components match, and blocks in which all components do not match. Taking into account the auxiliary results in the article, the probabilistic characteristics of the operations of componentwise and modular addition are obtained and compared, the probabilities of the coincidence of the results of these operations are calculated, conclusions are drawn about the correctness (incorrectness) of using the corresponding modifications of block ciphers to obtain security estimates, practically applicable samples of replacement blocks for block ciphers are given that correspond to certain conditions, the possibility of vulnerability of the cipher to certain types of differential attacks is determined, provided there is additional information that when assessing the strength of this cipher, its modification was used, obtained by replacing the operation in the key adder with some other. The article substantiates the conclusion that replacing an operation in a key adder or cipher substitution blocks is unacceptable without preliminary research, the essence of which is the calculation and comparison of the corresponding parameters.*

Keywords: *block cipher, substitute block, key adder, modular addition operation, component addition operation, cryptographic strength*

Гулак Геннадій Миколайович, кандидат технічних наук, доцент, завідувач лабораторії досліджень кібербезпеки Інституту проблем математичних машин і систем Національної академії наук України.
Гулак Геннадий Николаевич, кандидат технических наук, доцент, заведующий лаборатории исследований кибербезопасности Института проблем математических машин и систем Национальной академии наук Украины.
Hulak Hennadii, Candidate of Technical Sciences (Information security), Associate Professor, Head of the Cybersecurity Research Laboratory of the Institute for Problems of Mathematical Machines and Systems of the National Academy of Sciences of Ukraine.

Отримано 01 *серпня 2020 року*, затверджено редколегією *14 серпня 2020 року*

ISSN 2225-5036 (Print), ISSN 2411-071X (Online)
http://infosecurity.nau.edu.ua; http://jrnl.nau.edu.ua/index.php/Infosecurity

БЕЗПЕКА КОМП'ЮТЕРНИХ МЕРЕЖ ТА ІНТЕРНЕТ / NETWORK & INTERNET SECURITY

DOI: 10.18372/2225-5036.26.14917

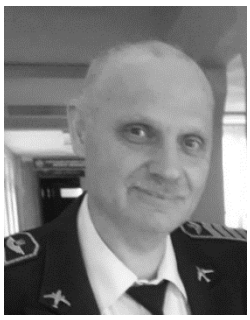
МЕТОДОЛОГІЧНІ ОСНОВИ СТВОРЕННЯ ЕЛЕМЕНТІВ КОМПЛЕКСНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ: ФІЗИЧНА МОДЕЛЬ ШТУЧНОЇ МОЛЕКУЛЯРНОЇ ПАМ'ЯТІ НА ОСНОВІ ДВОХ ТИПІВ ОРГАНІЧНИХ СПОЛУК

Олена Ключко, Володимир Шутко, Олена Колганова

Національний авіаційний університет

КЛЮЧКО Олена Михайлівна, к.б.н., доцент

Рік та місце народження: 1959, Київ.
Освіта: Національний університет ім. Тараса Шевченка, Київ, (1981); Національний Авіаційний університет, Київ (2003), Міжнародний університет лінгвістики та права (1999).
Посада: доцент кафедри електроніки, робототехніки, моніторингу та Інтернету речей Національного авіаційного університету.
Наукові інтереси: біоінформатика, біофізика, екологія, науки про мозок.
Публікації: більше 230, включно з монографіями, науковими та навчальними статтями, патентами.
E-mail: kelenaXX@ukr.net.
Orcid ID: 0000-0003-4982-7490.



ШУТКО Володимир Миколайович, д.т.н., професор

Рік та місце народження: 1970, Київ.
Освіта: повна вища, Московський державний технічний університет ім. Баумана, Москва, Росія, (1993).
Посада: завідувач кафедри електроніки, робототехніки, моніторингу та Інтернету речей Національного авіаційного університету.
Наукові інтереси: цифрова обробка сигналів та зображень.
Публікації: більше 160, включно з монографіями, науковими статтями, патентами.
E-mail: vnshutko@ukr.net.
Orcid ID: 0000 0002 9761 5583.

КОЛГАНОВА Олена Олегівна, к.т.н.

Рік та місце народження: 1979, Київ.
Освіта: повна вища: Національний авіаційний університет, Київ, Україна, (2007).
Посада: асистент кафедри інженерії програмного забезпечення Національного авіаційного університету.
Наукові інтереси: цифрова обробка сигналів та зображень.
Публікації: більше 50, включно з монографіями, науковими статтями.
E-mail: kolganovae79@gmail.com.
Orcid ID: 0000 0002 1301 9611.

Анотація. *У даній статті була описана розроблена гіпотетична фізична модель штучної молекулярної пам'яті на основі двох типів органічних сполук – похідних фенолу та індолу, які потенційно можуть бути застосовані для виконання функцій такої пам'яті у нано- електронних пристроях. Розроблена фізична модель демонструвала властивості штучної «пам'яті». Вона була подібною до інших прототипів, які виготовляли за допомогою молекул хіноліну та/або молекул-похідних нітро анілін оліго (фенілен етилену), однак нами було застосовано молекули інших типів – суміш похідних фенолу та індолу із замісниками - поліаміновими ланцюгами різної довжини та складності (JSTX-3, AR, ARN-1, ARN-2). Виготовлені нами системи були сформовані шляхом нашарування один на одного 2D та/або 3D наборів шарів органічних речовин, які можна було*

замінювати. Шари з ізотропними та анізотропними властивостями повинні чергуватися між собою. Випробування функціонування таких зразків проводили шляхом запису електричних іонних струмів, які проходили через них. Струми були асиметричними залежно від того, чи протікали вони по поліаміновому ланцюгу "до" чи "від" фенольного циклу. Для реєстрації та випробування таких елементарних електричних струмів використовували методи patch-clamp та реєстрації трансмембранних іонних струмів у режимі фіксації потенціалу. Деякі отримані дані носять попередній характер і для виготовлення промислових зразків необхідно виконати великий об'єм подальших робіт. Запропонований спосіб дозволяє модифікувати та утворювати нові елементи пам'яті природного та штучного походження, а також виконувати тестування їх функціонування шляхом реєстрації електричних струмів через утворений зразок. Зареєстровані струми мають асиметричний характер, демонструючи властивості пам'яті зразка. Розроблені методи та пристрої захищені патентами України на корисні моделі. Описано, які нові можливості кодування та захисту інформації на основі фізичної моделі відкриває виконана робота.

Ключові слова: *фізична модель, штучна молекулярна пам'ять, нано-електронна пам'ять, хімічні сполуки, похідні фенолу, похідні індолу.*

ВСТУП

Проблема створення запам'ятовуючих пристроїв у техніці на основі розробок штучної молекулярної пам'яті привертає останніми роками увагу все більшої кількості науковців та інженерів [1-6]. Такі роботи дозволяють вирішити як завдання мінімізації сучасної обчислювальної техніки, так і створюють нові можливості створення новітніх комп'ютерних пристроїв та систем на основі наших більш глибоких знань фізичного світу.

Однією із найбільш перспективних технічних ідей у цьому напрямку є створення так званої «штучної молекулярної пам'яті» (ШМП), або «нано- електронної пам'яті» (НЕП) [1-3]. Колективи професіоналів у галузях інформаційно-комп'ютерних технологій (ІКТ) у різних країнах світу (США, Китаї, країнах ЄС та ін.) працюють над різними аспектами вирішення цієї задачі – структурою елементарних комірок ШМП, підбором найбільш підходящих сполук-кандидатів для них, архітектурою компютерів на базі ШМП, іншими [1-3]. Застосовані у ШМП молекулярні структури відрізняються від тих, які задіяні для вирішення подібних задач у сучасних комерційних зразках техніки. Такі розробки вважаються достатньо перспективними, інформація про них є в університетських підручниках з ІКТ у США та країнах Західної Європи вже протягом останніх близько 10 років, у наших роботах ми також надавали інформацію про них [6]. Інтенсивні роботи у цьому напрямку виконують у тому числі і шляхом створення нових фізичних моделей відповідних пристроїв та їх нано- елементів.

У своїх попередніх публікаціях ми вже надавали попередню інформацію щодо своїх робіт у цьому напрямку, а саме щодо підбору деяких органічних сполук – вуглеводнів, похідних фенолу з поліаміновими замісниками різної довжини та ступеня розгалудженості, як кандидатів на функціональні елементи ШМП. Оскільки один з авторів протягом довгих років досліджувала функції молекул ароматичних вуглеводнів – похідних фенолу та амфіфільних сполук іншої будови у структурах природної пам'яті, то результати робіт, наведені нижче, є продовженням цих багаторічних робіт із досліджень речовин, потенційно придатних на роль елементів штучної молекулярної пам'яті та створення нових фізичних моделей відповідних пристроїв та їх нано- елементів.

Метою виконаної роботи було розробити методологічні основи створення штучної пам'яті на основі суміші двох типів молекул-похідних фенолу та індолу як елемента у складі комплексних систем захисту інформації; розробити фізичну модель такої штучної молекулярної пам'яті, а також пояснити переваги такого пристрою з точки зору захисту інформації.

ОСНОВНА ЧАСТИНА

Деякі прототипи, покладені в основу виконаної роботи. За означенням, «нанопам'ять, або молекулярна пам'ять» (відповідно «комірка нанопам'яті»...) є штучно створений запам'ятовуючий пристрій, асембльований із елементів нано- розмірів; вони застосовуються при розробці сучасних комп'ютерів супермалих (нано) розмірів. У нашому випадку та у ряді прототипів такими елементами є молекули – похідні фенолів та індолів [2-6]. Нижче наведемо опис деяких прототипів, які були покладено в основу виконаної нами роботи.

У прототипі [1] описано пристрій пам'яті та пам'ять для нього, яка включає в себе безліч пристроїв пам'яті. Кожний пристрій пам'яті містить відокремлені джерела та ділянки стоків, канал, бар'єрний ізоляційний шар, нанокристал або множину нанокристалів, контрольний бар'єрний шар та електрод входу. Нанокристал може бути квантовою крапкою, у ньому може бути «збереженим» один електрон чи дірка, або дискретне число електронів чи дірок. При кімнатній температурі при цьому забезпечується такий поріг зміни напруг, який перевищує величину теплових стрибків напруг для кожної із «записаних у пам'яті» характеристик відповідно електрона чи дірки. У цьому винаході використано кулонівську блокаду для електростатичного з'єднання одного або декількох «збережених» електронів чи дірок із каналом, уникаючи при цьому того, щоб «збережені» заряди не «відчували на собі» впливу провідності, контрольованої кулонівською блокадою.

Як інший приклад пристрою із нано-електронною пам'яттю необхідно розглянути той, що описано у способі створення елементів нано-електронної пам'яті у [2]. Цей спосіб базується на тому, що створюють нано-електронну матрицю пам'яті; фактично цей запам'ятовуючий пристрій містить масив комірок пам'яті, розташованих у рядах і стовпцях, сконструйованих над субстратом, кожна комірка пам'яті включає в себе перший сигнальний електрод, другий сигнальний електрод і наношар, розміщений в області перетину між першим сигнальним електродом і другим сигнальним електродом; при цьому утворюється множина смугових ліній, кожна з яких сполучає перші сигнальні електроди ряду комірок пам'яті; та

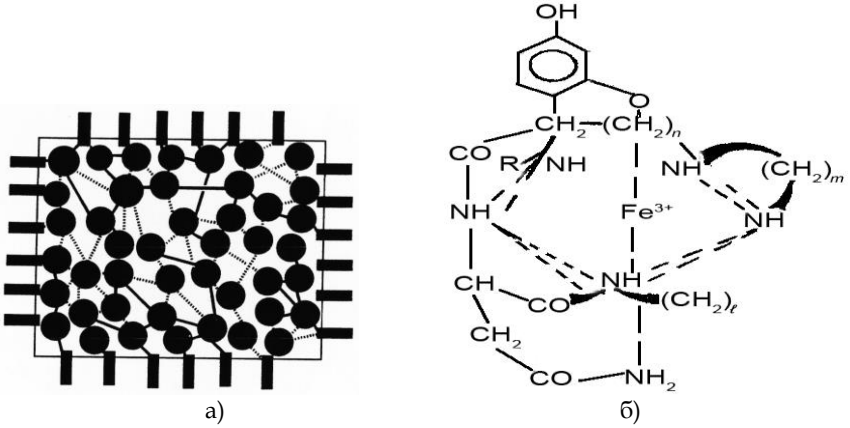
множина бітових ліній, кожна з яких з'єднує електроди другого сигналу зі стовпчика комірок пам'яті. Недоліками цього способу є те, що невідомі переконливі дані, чи функціонують (та чи справді добре функціонують) такі елементи саме як елементи пам'яті; це ставить під сумнів якість та ефективність роботи такої системи. У прототипі [2] описані елементи, які на мікро- та нанорівнях копіюють відповідні макроструктури, не використовуючи всіх переваг мікро- та нанотехнологій.

Нарешті, у якості іншого перспективного прототипу до виконаної розробки необхідно розглянути технічне рішення зі створенням наносумішей (нанокомпаундів) для пристроїв пам'яті із компонентів - органічних речовин [3]. Цей прототип являє собою наносуміш (нанокомпаунд) із компонентів, які мають властивості пам'яті. Описана суміш з нанокомпонентів включає в себе метал або його оксид та органічну сполуку, здатну окислювати і відновлювати зв'язок з металом або його оксидом; у прототипі використані органічні сполуки – хіноліни. Цей винахід відноситься також до запам'ятовуючого пристрою, який містить у собі розроблені органічні нанокомпоненти. Недоліками способу-прототипу [3] є те, що серед органічних речовин-нанокомпонентів цього пристрою недостатнє застосування знайшли похідні фенолів із замісниками – поліаміновими ланцюгами різної довжини й різного ступеня складності, застосування яких дозволяє покращити ряд характеристик молекулярної пам'яті. Це ставить під сумнів ефективність роботи системи пам'яті в прототипі [3] її якість і достовірність отриманих у [3] результатів.

Фізична модель фрагменту штучної молекулярної пам'яті на основі молекул-похідних фенолу й індолу та "електронна пастка". При розгляді вищенаведених прототипів штучної молекулярної (нано) пам’яті привертає увагу ряд характерних рис, для їх аналізу звернемося до рис. 1. На ньому зображено фрагмент вже виготовленого зразка ШМП – вигляд згори (рис. 1,а). Видно, що як і у прототипі [1], фрагмент розділений на компартменти – різні функціональні зони. Серед них вирізняються прямокутні темні зони контактів та округлі темні кола – локуси кріплення молекул ароматичних вуглеводнів – наприкад, похідних фенолу (рис. 2).

Молекули таких вуглеводнів відіграють основну роль у перерозподілі електронів, що формують електричні нано-струми у обох напрямках вздовж лінійної ділянки поліаміну – «до» та «від» фенольного кільця. Механізм захоплення електронів у кільці фенолу, так звана «пастка електронів» лежить в основі механізму «запам'ятовування». А моделі пристроїв на основі цих ефектів можна розглядати як такі, що містять штучні "комірки пам'яті", зібрані з елементів на рівні молекул та молекулярних комплексів [2-6]. Такі фізичні явища та детальну розробку подібних пристроїв ми вже описували у попередніх публікаціях [4, 6].

При створенні власної версії фізичної моделі штучної молекулярної пам'яті раніше авторами було запропоновано застосувати молекули-похідні фенолу із замісниками – поліаміновими ланцюгами, лінійними або розгалудженими, різної довжини та складності [4, 6]. Була розроблена фізична модель молекулярних накопичувачів із властивостями штучної пам’яті, спираючись на вивчені нами механізми взаємодії ароматичних вуглеводнів з бішаровими ліпідними мембранами (рис. 2 та рис. 3). В основу запропонованої моделі можна покласти наступні факти, які були зареєстровані авторами та рядом інших дослідників-науковців [6]. 1. Вивчені хімічні сполуки (похідні ароматичних вуглеводнів із заступниками - лінійними поліамінами різної довжини та складності) є амфіфільними речовинами, їх ароматичні групи можуть бути розчинені у гідрофобній ліпідній фазі мембран у складі комірки пам’яті розроблюваного пристрою, а їх поліамінові ланцюги можуть стирчати у навколишній простір. 2. Молекули досліджених авторами органічних сполук можуть утворювати координаційні комплекси з металами, наприклад, з іонами заліза Fe^{3+}(у той час, як у прототипі – з атомами золота Au) (рис. 1,б). 3. Розраховане на основі отриманих авторами експериментальних даних, значення коефіцієнта Хілла становило 0,86, що свідчило про приєднання однієї молекули досліджених сполук (JSTX-3, AR, тощо) до однієї молекули на поверхні мембрани у складі розроблюваного запам’ятовуючого пристрою. Запропонована й описана фізична модель ШМП дозволяє виготовити і випробувати елементи нано-пам’яті - технічні пристрої з властивостями "штучної пам'яті" на основі сполук фенолу.



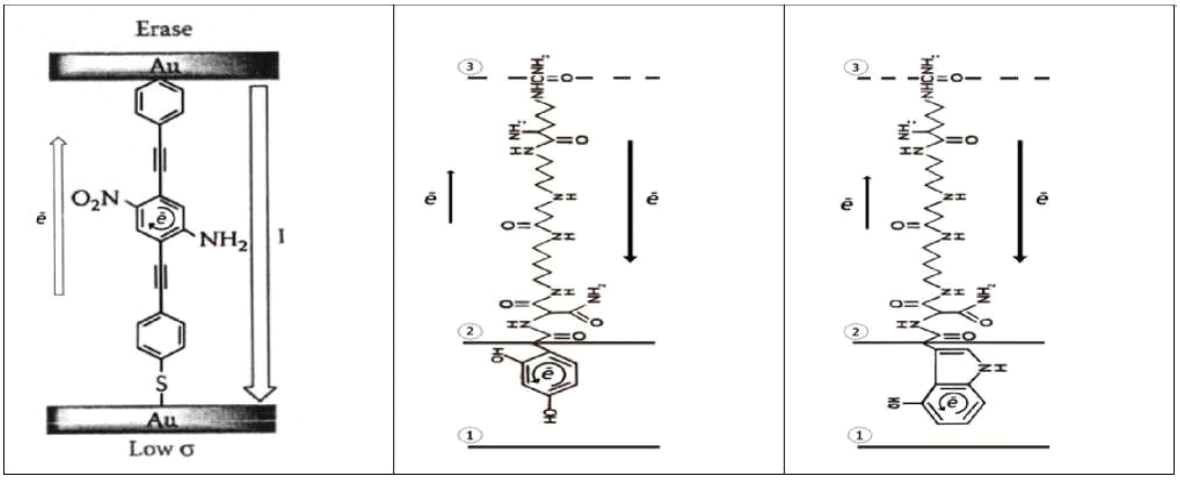
а) б)

Рис. 1. Прототип елементарного фрагменту нано-пам'яті із органічних молекул [2, 3, 6]
а) Прототип, вид згори. Видно, що як і у прототипі [1], фрагмент розділений на компартменти – різні функціональні зони. Прямокутні темні зони контактів та округлі темні кола – локуси кріплення молекул ароматичних вуглеводнів – похідних фенолу або індолу. б) Структура хелатного комплексу токсину JSTX-3 і катіона заліза Fe^{3+} (пояснення дивись у тексті)

Пізніше авторами була запропонована теоретично можлива фізична модель, у якій у якості елемента ШМП було застосовано хімічні сполуки, подібні до попередньо розглянутих: похідні індолу із замісниками – поліаміновими ланцюгами, лінійними або розгалудженими, різної довжини та складності [5, 6]. Тобто, на відміну від вищеописаних сполук, тут замість фенольного кільця є присутнім фрагмент індолу – поєднані разом 5- та 6-членні ароматичні кільця. У роботах автора були досліджені у біофізичних експериментах такі сполуки, як аргіопінін 1 (ARN-1) та аргіопінін 2 (ARN-2). В основу моделі на основі сполук-похідних індолів можна покласти такі ж факти, які викладені у попередньому абзаці та які були зареєстровані авторами та рядом інших дослідників-науковців [6]. У цьому відношенні властивості сполук були подібними, що дозволило описану гіпотетичну фізичну модель поширити і на цей клас сполук (рис. 2, 3).

Фрагмент штучної молекулярної пам'яті на основі суміші двох типів молекул-похідних фенолу та індолу. Поставлена задача була вирішена за рахунок того, що була створена та протестована фізична молекулярна пам'ять, що складається із матриці з комірок, утворених шарами – плоскими фрагментами ліпідної гідрофобної бішарової мембрани зі зв'язаними із ними органічними та неорганічними речовинами. Вирішення такої задачі було нами зареєстровано, як два винаходи (корисні моделі) в Україні [4, 5] та детально описано у статті [6]. Відповідний спосіб [4] характеризується тим, що при його здійсненні виконують такі елементи пам'яті шляхом формування (наслоювання) 2D та/або 3D шарів, які мають ізотропні та анізотропні властивості, причому шари з ізотропними та анізотропними властивостями чергують між собою, а до складу одного чи кількох таких шарів входять пов'язані із ним (ними) молекули похідних фенолу та індолу із замісниками – поліаміновими ланцюгами різної довжини та різного ступеня складності; такі молекули можуть бути однаковими або різних типів, штучного або природного походження. Для тестування функцій таких елементів пам'яті нами запропоновано виконувати реєстрацію електричних струмів через них застосовуючи методи patch-clamp та voltage-clamp, які були розроблені раніше у галузі біофізики для реєстрації трансмембранних електричних іонних струмів [6, 7].

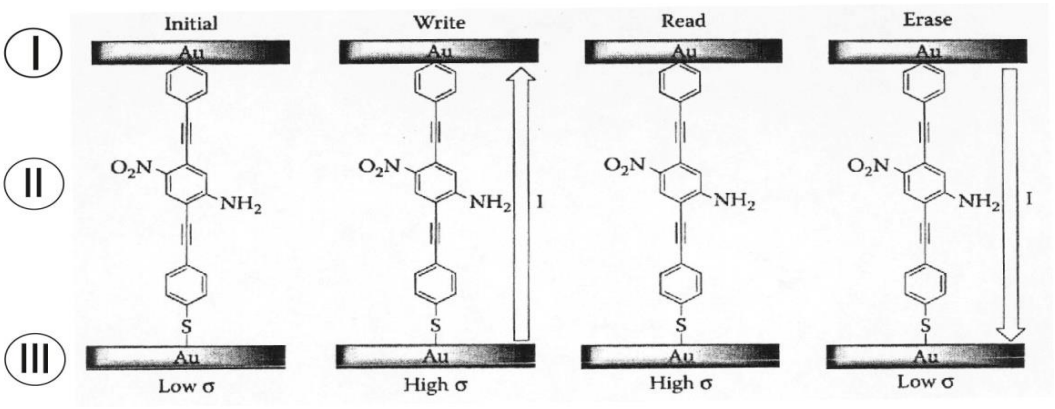
Для виготовлення описуваної системи нами було розроблено кількаетапний процес попередньої обробки ліпідних бішарових мембран та підготовку компонентів з органічних речовин-похідних фенолу та індолу. Виконавши послідовно необхідні етапи роботи, було отримано систему, яка є фізичною моделлю пристрою зберігання інформації. Розроблена фізична модель демонструвала властивості штучної «пам'яті» (рис. 2, 3). Вона була подібною до інших з прототипів, які готували за допомогою молекул хіноліну та/або молекул, одержуваних з оліго нітро аніліну (фенілен етилену) (рис. 2, 3). Однак у нашому випадку робота проводилася з використанням інших типів молекул - похідних фенолу та індолу (речовин JSTX-3, AR, ARN-1, ARN-2). Запропоновані нами речовини, а саме похідні фенолу та індолу із замісниками - поліаміновими ланцюгами різної довжини та складності, необхідно було наносити на поверхню мембран. Такі молекули могли бути однакового чи різного типу, штучного чи природного походження; а дослідні системи формували шляхом нашарування (наслоювання) один-на-один 2D та/або 3D шарів необхідних органічних та неорганічних речовин, які за потребою могли замінювати. Необхідною умовою функціонування такої системи із пам'яттю було те, щоб шари з ізотропними та анізотропними властивостями чергувалися між собою. Тестування придатності таких зразків до виконання функцій пам'яті проводили експериментальним шляхом. Записи електричних струмів через зразки було зареєстровано. Електричні струми, що протікали через зразок, були асиметричними залежно від того, чи протікали вони вздовж поліамінового ланцюга "до" або "від" фенольного кільця. Для реєстрації та тестування таких елементарних електричних струмів використовували методи patch-clamp та фіксації потенціалу на мембрані. Таким чином, у результаті проведених експериментів, нами було продемонстровано, що створена фізична модель мала властивості зберігання інформації - властивості "молекулярної пам'яті".



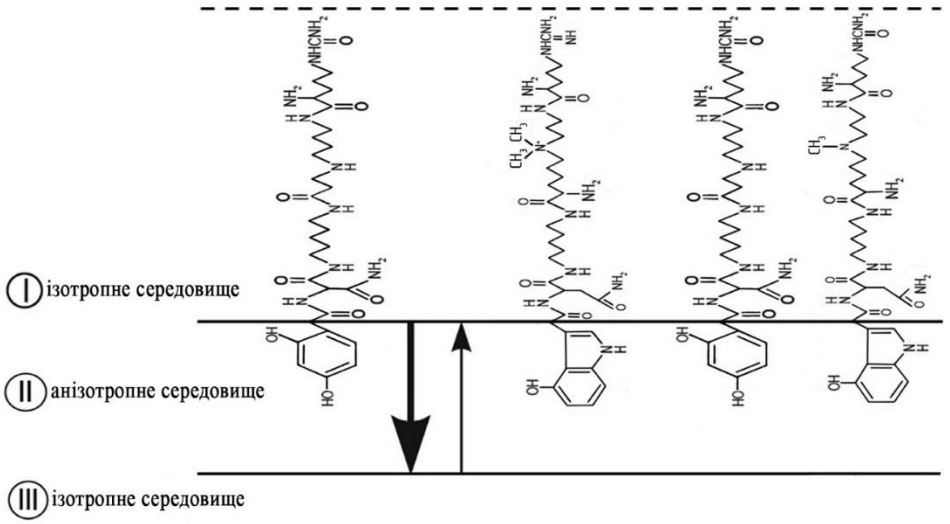
а) б) в)

Рис. 2. Елементи молекулярного пристрою штучної памяті [4, 5, 6]

а) Молекулярний елемент, реалізований у прототипі, б) запропонований елемент з похідним фенолу JSTX-3, б) запропонований елемент з похідним індолу ARN-1. Вертикальні асиметричні стрілки вказують різні величини електронних струмів в обох напрямках; товщина та довжина стрілок прямо пропорційні величині струму. Захоплення електронів у «пастку» схематично показано стрілками у 6-членних циклах



а)



б)

Рис. 3. Зборка елементарних фрагментів нано-пам'яті із органічних молекул [4, 5, 6]
а) Прототип у поперечному розрізі. б) Фрагмент запропонованого пристрою нано-пам'яті з органічними молекулами - похідними фенолу з лінійним замісником – поліаміном. Зображено випадок, у якому застосовано молекули JSTX-3 (але можливо застосування інших молекул з подібними властивостями). Елементарна система з "штучною пам'яттю" повинна бути зібрана з набору ізотропних та анізотропних шарів, які чергуються між собою. I, III - ізотропні середовища, II - анізотропне середовище (пояснення в тексті)

Описана вище система являла собою одиночний фрагмент - елемент, який було названо «коміркою» нано-пам'яті. Наступним логічним кроком розробки фізичного молекулярного пристрою зберігання інформації, було утворення ансамблю таких елементів, який складався з матриці з «комірок». Кожна із цих «комірок» була утворена з шарів - плоских фрагментів ліпідної гідрофобної двошарової мембрани із поєднаними із нею органічними та неорганічними речовинами. Як описано вище, кожен із цих елементів виконували шляхом формування (нашарування) 2D та/або 3D шарів, які мали ізотропні та анізотропні властивості. Шари з ізотропними та анізотропними властивостями чергувались між собою. Один або більше таких шарів містили молекули похідних фенолу із замісниками - поліаміновими ланцюгами різної довжини та складності. Такі молекули могли бути однакових або різних типів, штучного або природного походження. Зразок такого фрагмента штучної пам’яті наведено на Рис. 2 для похідних фенолу JSTX-3 (рис. 2,б) та індолу ARN-1 (рис. 2,в).

Запропоновані нами методи [4, 5, 6] створюють можливість модифікувати та створити нові типи молекулярних елементів природного та штучного походження для пристроїв молекулярної памяті, а також протестувати їх функції, зареєструвавши електричні струми через виконаний зразок методами patch-clamp та фіксації потенціалу на мембрані. Зареєстровані трансмембранні електричні струми мали асиметричний характер та продемонстрували властивості штучної пам'яті.

З метою створення зразків таких нано-пристроїв для штучного зберігання інформації, необхідно було виконати кілька етапів робіт. Цей робочий процес був описаний у наших попередніх публікаціях [4, 5, 6]; розроблені методи захищені патентами України [4, 5].

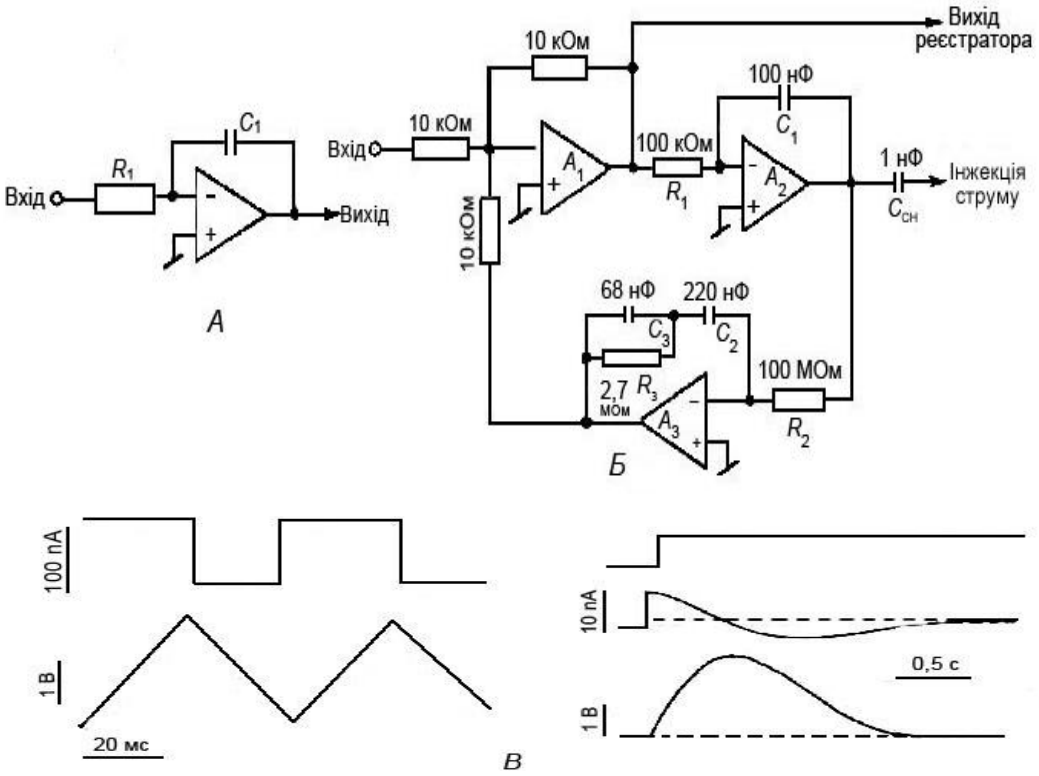


Рис. 4. Інтегратор для інжекції тестуючого сигналу для тестування виготовлених зразків нано-пам'яті методом patch-clamp. На вхід системи інформація надходить у вигляді електричних або хімічних сигналів, на виході інформацію реєструють у вигляді електричних сигналів [7]

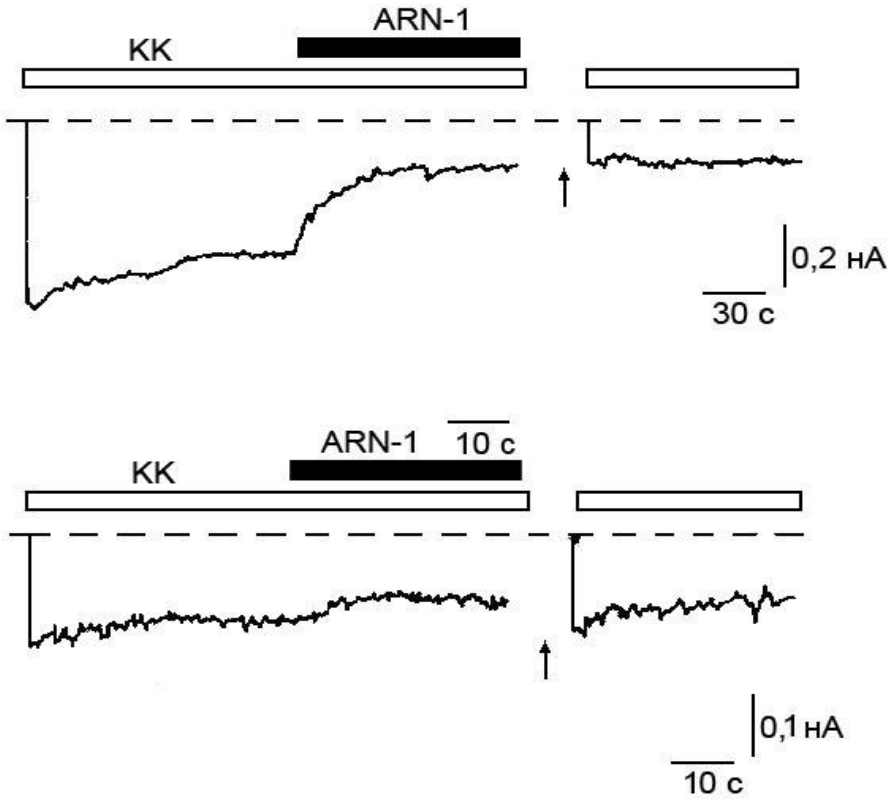


Рис. 5. Експериментальні підтвердження розробленого способу та відповідного зразка – реальні записи, зроблені під час експерименту з реєстрації електричних сигналів на виході біосенсорної технічної системи. Продемонстровано запис електричних трансмембранних струмів, що виникають при дії на БФ каінату (КК) при наступній дії на БФ сполуки ARN-1, похідної індолу з поліаміновим ланцюгом. Зареєстровано ефект необоротного блокування каінатактивованих струмів молекулою аргіопінін 1 (ARN-1), яка демонструє неоднакові електропровідні властивості при переміщенні електронів у зовнішньому електричному полі уздовж її поліамінового ланцюга у протилежних напрямках: до фрагмента індолу та від нього. Скорочення: КК – каїнат, ARN-1 одне з похідних індолу з поліаміновим ланцюгом.

Можливості кодування та захисту інформації на основі фізичної моделі молекулярної пам'яті. Після виконання робіт [4-6] стало можливим запропонувати фізичну модель штучної "молекулярної пам'яті", аналогічної прототипу з молекулами хіноліну [3]. На рис. 2,а та рис. 3,а, представлено фрагменти нано-пам'яті з молекул-похідних нітро анілін оліго (фенілен етилену). Такий прототип було запропоновано у США, натепер продовжуються роботи із пібору найбільш піходящих молекулярних елементів для реалізації таким зразком його функцій як наноелемента штучної пам'яті. На рис. 1 зображено вже готовий зразок цього прототипу пам'яті, а саме його вигляд згори.

Як зазначалося у наших перших публікаціях на цю тему [4, 6], нами запропоновано для цієї ж мети застосувати сполуки-похідні фенолу, наприклад, природні сполуки-токсини JSTX-3 та AR (рис. 2). Механізм пам'яті тут реалізується завдяки ефекту так званої «електронної пастки», який зображено на схемах на рис. 2. Електрони, які формують електричні нано-струми, можуть бути захоплені цією «пасткою електронів», якою тут виступає шестичленний цикл фенолу. Час перебування електронів у таких «пастках» був різним, залежно від їх переміщення у різних напрямках «до» або «від» фенольного циклу та від ряду інших факторів, наприклад, від асиметрії системи [6]. Отже, й елементарні опори електронним струмам в обох напрямках також були різними, реалізуючи "1" або "0" в такому елементарному пристрої зберігання інформації.

Можливості кодування інформації у системі із сумішшю двох типів похідних: фенолу та індолу. У перших описаних нами фізичних моделях [4] у якості елемента ШМП було обрано сполуки-похідні фенолу JSTX-3 та AR. Уявимо гіпотетичну фізичну модель, у якій у якості елемента ШМП застосовано суміш похідних двох типів циклічних сполук – фенолу та індолу (наприклад, природні сполуки-токсини JSTX-3 та ARN-1). У системі із сумішшю двох типів похідних – фенолу (1) та індолу (2) будемо спостерігати складніший ефект. Очікувано, час перебування електронів у «електронній пастці» індольної групи (2) буде довшим, ніж у випадку групи фенолу. Відповідно, електронна провідність потоку електронів у випадку (2) буде нижчою в N разів, аніж у випадку (1). Оскільки величина елементарних опорів дорівнює одиниці, поділеній на величини едементарних провідностей, то й опори перебуватимуть у взаємозалежності (але – оберненій). Тобто, те ж саме буде справедливим і для елементарних опорів електронним струмам в обох напрямках вздовж ланцюга поліаміну, Отже, якщо ми приймаємо для системи з похідними фенолу (1), що ми реалізуємо "1" або "0" у такому елементарному пристрої зберігання інформації, то при внесенні молекул – похідних індолу (2), отримаємо додатково ще й дробові значення інформаційних бітів (наприклад, ¼, ¾ і т.д.). Відповідно, зростають можливості для кодування інформації у системі (2).

Можливості захисту інформації у системі із сумішшю двох типів похідних. Відповідно, можливості захисту інформації у системі із сумішшю двох типів похідних: фенолу та індолу також збільшуються. Це відбувається внаслідок того що, ідучи шляхом збільшення кількості значущих молекулярних елементів, які приймають участь у кодуванні, то на наступному етапі ми створюємо можливість заміни одного такого елемента іншим. Враховуючи те, що у природі існують мільйонів типів органічних молекул, можна отримати величезну кількість значущих їх комбінацій. «Зламати» такий молекулярний код стає практично неможливо.

На рис. 4 наведено схематичне зображення одного з блоків у схемі експериментальної установки для тестування виготовлених зразків нано-пам'яті методом patch-clamp. На рис. 5 наведено експериментальне підтвердження розробленого способу та пристрою: записи трансмембранних електричних струмів, які виконано із застосуванням методу реєстрації трансмембранних іонних струмів у режимі фіксації потенціалу [6, 7].

ВИСНОВКИ

У даній статті було запропоновано новий тип хімічних сполук ряду похідних індолу, які потенційно можуть бути застосовані для виконання функцій штучної молекулярної пам'яті у нано- електронних пристроях. Була описана розроблена гіпотетична фізична модель штучної молекулярної пам'яті на основі двох типів органічних сполук – похідних фенолу та індолу. Для виготовлення системи було розроблено кількаетапний процес обробки вихідних матеріалів - фрагментів двошарових мембран, поєднаних із набором органічних речовин. У результаті була отримана система, яка є фізичною моделлю нано-пам'яті. Розроблена фізична модель демонструвала властивості штучної «пам'яті» (рис. 2, 3). Вона була подібною до інших прототипів, які виготовляли за допомогою молекул хіноліну та/або молекул-похідних нітро анілін оліго (фенілен етилену). Однак у нашому випадку було застосовано молекули інших типів - похідні фенолу (JSTX-3, AR) та індолу (ARN-1, ARN-2). На поверхню мембран наносили такі речовини, які являють собою похідні фенолу та індолу із замісниками - поліаміновими ланцюгами різної довжини та складності. Такі молекули можуть бути однакового чи різного типу, штучного чи природного походження. Виготовлені нами системи були сформовані шляхом нашарування один на одного 2D та/або 3D наборів шарів органічних та неорганічних речовин, які можна було замінювати. Шари з ізотропними та анізотропними властивостями повинні чергуватися один з одним. Випробування функціонування таких зразків проводили шляхом запису електричних іонних струмів, які проходили через них. Струми були асиметричними залежно від того, чи протікали вони по поліаміновому ланцюгу "до" чи "від" фенольного циклу. Для реєстрації та випробування таких елементарних електричних струмів використовували методи patch-clamp та реєстрації трансмембранних іонних струмів у режимі фіксації потенціалу.

Запропонована нами гіпотетична фізична модель продемонструвала властивості зберігання інформації - властивості "молекулярної пам'яті". Проте деякі отримані дані носять попередній характер. Для виготовлення промислових зразків необхідно виконати великий об'єм подальших робіт.

Щодо прикладного значення виконаної фізичної моделі «комірки нанопам'яті» при розробці нових моделей сучасних комп'ютерів, то отриманий у роботі технічний результат полягає у наступному. Запропонований спосіб дозволяє модифікувати та утворювати нові елементи пам'яті природного та штучного походження, а також виконувати тестування їх функціонування шляхом реєстрації електричних струмів через утворений зразок. Зареєстровані струми мають асиметричний характер, демонструючи властивості пам'яті зразка. Необхідно зазначити, що розробники подібних нано пристроїв ведуть пошук в усьому світі речовин – потенційно здатних на виконання відповідних функцій, відповідні рішення розглядаються. Відповідно, автори запропонували та запатентували свої аналоги речовин - розроблені методи та пристрої захищені патентами України на корисні моделі [4, 5]. У фіналі статті описано, які нові можливості кодування та захисту інформації на основі фізичної моделі молекулярної пам'яті відкриває виконана робота.

References

[1]. W. Chen, T. Smith, S. Tiwari, *Nano-structure memory device. Patent US5714766A*. Priority: 1995-09-29. Assigned: 2015-10-05 to GLOBALFOUNDRIES INC.

[2]. B. Tran, *Nano-Electronic Memory Array. Patent US20080239791A1.* Priority: 2004-04-06. Applied: 2008-10-02; pending – 2018.

[3]. C. Chen, G. Hwang, C. Ting, Y. Chan, Z. Pei, C. Chang, C. Kung, *Nano compounds and organic memory devices comprising the same. Patent US7641820B2*. Priority: 2006-04-26. Applied: 2007-11-01; grant - 2010-01-05.

[4]. О. Ключко, А. Білецький, В. Шутко, *Спосіб виготовлення фізичної молекулярної пам'яті в анізотропних середовищах з молекулами-похідними фенолу. Патент UA 135531 U; B82Y 40/00, B82Y 10/00, H01B 1/12, C12Q 1/00, G11C 13/00* – Опубл: 10.07.2019, Бюл. 13, КМ, власник НАУ.

[5]. О. Ключко, А. Білецький, *Спосіб виготовлення фізичної молекулярної памя'ті в анізотропних середовищах з молекулами-похідними фенолу та індолу. Патент UA 141034 U; H01B 1/00, B82B 3/00, B82Y 10/00.* – Опубл: 25.03.2020, Бюл. 6, КМ, власник НАУ.

[6]. O. Klyuchko, "Aromatic hydrocarbons of Arthropodae species: mechanisms of action on biological membranes and perspectives of biomedical application", *Biotechnologia Acta*, K, V. 13, no. 2, pp. 12-31, 2020.

[7]. Ф. Сигворс, Б. Сакман, Э. Неер, *Регистрация одиночных каналов*, М.: Мир, 1987, 448 с.

УДК 004:591.5:612:616-006

Ключко О.М., Шутко В.Н., Колганова А.А. Физическая модель искусственной молекулярной памяти на основе двух типов органических соединений

Аннотация. *В данной статье была описана разработанная гипотетическая физическая модель искусственной молекулярной памяти на основе двух типов органических соединений - производных фенола и индола, которые могут быть применены для выполнения функций такой памяти в нано- электронных устройствах. Разработана физическая модель демонстрировала свойства искусственной «памяти». Она была подобна другим прототипам, которые изготавливали с помощью молекул хинолина и / или молекул производных нитро анилин олиго (фенилен этилена), однако нами были применены молекулы других типов - смесь производных фенола и индола с заместителями - полиаминовыми цепями различной длины и сложности (JSTX-3, AR, ARN-1, ARN-2). Изготовленные нами системы были сформированы путем наслоения друг на друга 2D и/или 3D наборов слоев органических веществ, которые можно было заменять. Слои с изотропными и анизотропными свойствами должны чередоваться между собой. Испытания функционирования таких образцов проводили путем записи электрических ионных токов, которые проходили через них. Токи были асимметричными в зависимости от того, протекали они по полиаминов цепи "до" или "от" фенольного цикла. Для регистрации и испытания таких элементарных электрических токов использовали методы patch-clamp и регистрации трансмембранных ионных токов в режиме фиксации потенциала. Некоторые полученные данные носят предварительный характер и для изготовления промышленных образцов необходимо выполнить большой объем дальнейших работ. Предложенный способ позволяет модифицировать и создавать новые элементы памяти естественного и искусственного происхождения, а также выполнять тестирование их функционирования путем регистрации электрических токов через выполненный образец. Зарегистрированные токи имеют асимметричный характер, демонстрируя свойства памяти образца. Разработанные методы и устройства защищены патентами Украины на полезные модели. Описано, какие новые возможности кодирования и защиты информации на основе физической модели открывает выполненная работа.*

Ключевые слова: *физическая модель, искусственная молекулярная память, нано-электронная память, химические соединения, производные фенола, производные индола.*

Klyuchko O., Shutko V., Kolganova O. Physical model of artificial molecular memory based on two types of organic compounds

Abstract. *This paper describes the developed hypothetical physical model of artificial molecular memory based on two types of organic compounds - phenol and indole derivatives, which can potentially be used to perform the functions of memory in nano-electronic devices. The developed physical model demonstrated the properties of artificial "memory". It was similar to other prototypes made with quinoline molecules and/or nitro aniline oligo derivatives (phenylene ethylene), but we used other types of molecules - a mixture of phenol and indole derivatives with substitutes - polyamine chains of different length and complexity (JSTX-3, AR, ARN-1, ARN-2). The systems we developed were formed by layering 2D and/or 3D sets of layers of organic substances that could be replaced. Layers with isotropic and anisotropic properties should alternate. Functional*

tests of such samples were performed by recording the electric ionic currents that passed through them. The currents were asymmetric depending on whether they flowed along the polyamine chain "to" or "from" the phenolic cycle. To record and test such elementary electric currents, patch-clamp methods and registration of transmembrane ionic currents in the potential fixation mode were used. Some of obtained data were preliminary and a great further work is necessary to produce the industrial samples. The proposed method allows to modify and create new memory elements of natural and artificial origin, as well as to test their functioning by the registration of electric currents through the formed sample. The recorded currents were asymmetric, demonstrating the memory properties of the sample. Developed methods and devices were protected by patents of Ukraine. New possibilities of coding and protection of information on the basis of physical model of obtained results were described as well.
Keywords: *physical model, artificial molecular memory, nano-electron memory, chemical compounds, phenol derivatives, indole derivatives.*

Ключко Олена Михайлівна, кандидат біологічних наук (біофізика), доцент кафедри електроніки, робототехніки, моніторингу та Інтернету речей Національного авіаційного університету.
Ключко Елена Михайловна, кандидат биологических наук (биофизика), доцент кафедры электроники, робототехники, мониторинга и Интернета вещей Национального авиационного университета.
Klyuchko Olena, Candidate of Science (Biophysics), Associate Professor of the Chair of electronics, robotics, monitoring and Internet of things of the National Aviation University.

Шутко Володимир Миколайович, доктор технічних наук, професор, завідувач кафедри електроніки, робототехніки, моніторингу та Інтернету речей Національного авіаційного університету.
Шутко Владимир Николаевич, доктор технических наук, профессор, заведующий кафедры электроники, робототехники, мониторинга и Интернета вещей Национального авиационного университета.
Shutko Volodymyr, Doctor of Sciences (Technique), Full Professor, Chair of Department of electronics, robotics, monitoring and Internet of things of the National Aviation University.

Колганова Олена Олегівна, кандидат технічних наук, асистент кафедри інженерії програмного забезпечення Національного авіаційного університету.
Колганова Елена Олеговна, кандидат технических наук, ассистент кафедры инженерии программного обеспечения Национального авиационного университета.
Kolganova Olena, Candidate of Sciences (Technique), Assistant Professor of Department of software engineering of the National Aviation University.

Отримано *23 червня 2020 року*, затверджено редколегією *19 липня 2020 року*

© Opirskyy I., Holovchak R., Moysiychuk I. Prospects of development of artificial intelligence in the context of information security // Ukrainian Scientific Journal of Information Security, 2020, vol. 26, issue 2, pp. 108-115.

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ / INFORMATION SECURITY MANAGEMENT

DOI: 10.18372/2225-5036.26.14757

ПЕРСПЕКТИВИ РОЗВИТКУ СИСТЕМ ШТУЧНОГО ІНТЕЛЕКТУ В КОНТЕКСТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Іван Опірський, Романа Головчак, Ірина Мойсійчук

Національний університет «Львівська політехніка»

ОПІРСЬКИЙ Іван Романович, д.т.н., доцент

Рік та місце народження: 1987 рік, м. Сімферополь, АР Крим, Україна.
Освіта: Національний університет «Львівська Політехніка», 2008 рік.
Посада: професор кафедри захисту інформації з 2019 року.
Наукові інтереси: методи і засоби технічного захисту інформації, охорона державної таємниці, проектування комплексних систем захисту інформації, лазерні системи акустичної розвідки, математичні методи та моделі захисту інформації, технічні канали витоку інформації, спецвимірювання .
Публікації: більше 120 наукових публікацій, серед яких наукові статті, монографії, навчальні посібники, тези та матеріали доповідей на конференціях.
E-mail: iopirsky@gmail.com.
Orcid ID: 0000-0002-8461-8996.

ГОЛОВЧАК Романа Василівна

Рік та місце народження: 2001 рік, м. Дрогобич, Львівська область, Україна.
Освіта: студент кафедри захисту інформації Національного університету «Львівська політехніка».
Наукові інтереси: інформаційна безпека держави, правове забезпечення інформаційної безпеки.
E-mail: romana.holovchak.kb.2018@lpnu.ua.
Orcid ID: 0000-0002-2932-3466.

МОЙСІЙЧУК Ірина Русланівна

Рік та місце народження: 2001 рік, с. Тур, Волинська область, Україна.
Освіта: студент кафедри захисту інформації Національного університету «Львівська політехніка».
Наукові інтереси: системи кіберзахисту інформаційних ресурсів, комп'ютерні науки.
E-mail: iryna.moisiichuk.kb.2018@lpnu.ua.
Orcid ID: 0000-0002-7531-5811.

Анотація. *Штучний інтелект – концепція, за якою машини здатні здійснювати деяку інтелектуальну діяльність, що властива людям або тваринам. Іншими словами можна сказати, що це поняття включає в себе будь-який пристрій, який має здатність сприймати його оточення та вживати дій, що збільшують шанс на успішне досягнення цілей. Проте, незважаючи на триваючий прогрес у швидкості комп'ютерної обробки та об'ємі пам'яті, до цих пір немає програм, які могли б зрівнятися з людською гнучкістю в більш широких областях або в завданнях, що вимагають великих повсякденних знань. З іншого боку, деякі програми досягли рівня продуктивності людських експертів і професіоналів у виконанні певних конкретних завдань, так що штучний інтелект в цьому обмеженому сенсі можна знайти в таких різноманітних додатках, як медична діагностика, комп'ютерні пошукові системи і розпізнавання голосу або почерку. Метою даної роботи є, власне, визначення позитивних та негативних аспектів застосування систем штучного інтелекту в галузі безпеки інформації. Визначено, що такі системи мають вагому роль в поточному та подальшому забезпеченні безпеки даних, а також наведено ряд недоліків таких систем для майбутнього їх врахування. У статті було розглянуто те, що штучний інтелект був розроблений шляхом вивчення того, як людський мозок думає,*

навчається і приймає рішення, а потім застосовує ці біологічні механізми до комп'ютерів. На відміну від класичних обчислень, де кодери забезпечують точні входи, виходи і логіку, штучний інтелект заснований на наданні машині вхідних даних і бажаного результату, дозволяючи машині розвивати свій власний шлях для досягнення поставленої мети. Штучний інтелект – це технологія, яка перетворює всі сфери життя. Це широкий інструмент, який дозволяє людям переосмислити, як ми інтегруємо інформацію, аналізуємо дані та використовуємо отримані результати для покращення процесу прийняття рішень. Вони змінюють спосіб, яким ми шукаємо інформацію, як ми спілкуємося один з одним, навіть як ми поводимося. Ця трансформація стосується багатьох областей, включаючи освіту. Основною метою даної статті є огляд вирішення проблем за допомогою штучних технологій. У представленому огляді літератури ми розглянули чотири категорії: індивідуальний освітній контент, інноваційні методи навчання, технологія розширеної оцінки, комунікація між студентом і викладачем. Розглянувши публікації на цю тему, ми представляємо тут можливу картину того, як штучний інтелект змінить ландшафт освіти. Починаючи з короткої історії штучного інтелекту, в даній статті представлений загальний огляд цієї технології.

Ключові слова: *штучний інтелект, машинне навчання, безпека інформації, системи машинного навчання, людина.*

Вступ

Не зважаючи на те, що алгоритми штучного інтелекту з'явилися ще в 60-их роках, інтерес до нього і його розвитку досі не згас. Оскільки сучасні як маленькі компанії, так і великі корпорації почали надавати надзвичайно великого значення інформаційній безпеці та безпосередньому захисту великого потоку даних, питання штучного інтелекту в галузі безпеки постало доволі гостро. Ні для кого не є секретом те, що, так звані, "чорні" хакери вже використовують алгоритми машинного навчання для своїх цілей, при чому доволі успішно. Експерти вже давно визначають необхідність створення "розумної" та автономної системи безпеки. Деякі з них схиляються до думки, що саме штучний інтелект буде запорукою успішності цієї системи. Звичайно, є і інша думка: для забезпечення повного захисту потрібні, власне, люди.

Поточний стан розвитку штучного інтелекту

Автоматизація з кожним роком набирає все більших обертів, а компанії все більше інвестують в її розвиток з метою замінити людську робочу силу, заявляє Forbes. Роботам не потрібно відпочивати, їм не потрібен час на обід чи на сон. Великі корпорації з колосальними кількостями найманих працівників однозначно будуть у виграшній ситуації від розвитку систем Штучного Інтелекту (ШІ). В свою чергу Білл Гейтс в своєму інтерв'ю для Time заявив, що серед усіх сучасних розробок, саме ШІ має найбільший потенціал змінити наші життя: зробити їх «продуктивнішими, ефективнішими, а загалом легшими».

Натан Бенайч та Ян Хогарт, які є серійними інвесторами галузі штучного інтелекту, заявляють, що штучний інтелект стане рушійною силою технічного прогресу в нашому все більш цифровому світі, керованому даними. Причиною цього вони визначають у тому, що нас оточують продукти людського інтелекту, незалежно чи культура це чи споживчі продукти. Ще у 2018 році ШІ досяг великого прогресу в сфері комп'ютерних ігор (зокрема StarCraft II, Quake III Arena (Capture the Flag), Dota2). Чому вибір середовища навчання для ШІ зупинився саме на іграх? Відповідь надзвичайно проста: саме там легко здійснити моніторинг процесу пристосування до мінливого середовища та варіації великої кількості змінних. Йдеться про системи ШІ, засновані на технології reinforcement learning. Автори звертають увагу на те, що виграш над реальним гравцем є менш важливим результатом, ніж вивченням методів досягнення цього результату. Системи ШІ можна порівняти з дітьми, які шляхом застосування комп'ютерних ігор здобувають нові навички, засвоюють невідомі раніше моделі поведінки без реальної загрози в житті. Мабуть, саме через вище вказану причину тестування систем машинного навчання є цілком доцільним в цьому середовищі (рис. 1).

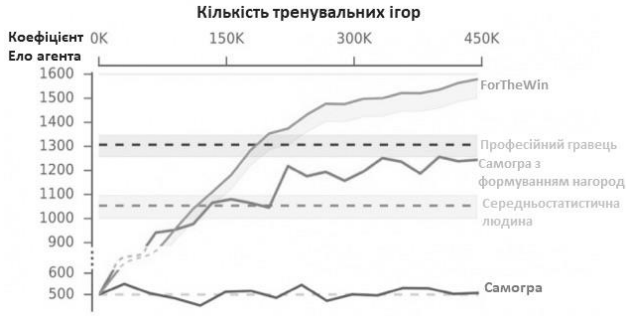


Рис. 1. Розробники компанії Deep Mind створили ШІ FTW (ForTheWin), який навчається під час гри і перемагає професійних кіберспортсменів

На діаграмі, поданій вище, неозброєним оком видно вражаючу стрімкість динаміки навчання ШІ. Авжеж, такий успіх в розвитку в комп'ютерних іграх зовсім не гарантує ідентичний результат при застосуванні в реальному житті, але можемо сказати, що це чудове місце для початку, проте однозначно не кінцева мета розвитку систем машинного навчання.

Зараз ШІ здатен навіть написати музику, відповідно до вподобань людини. Одним з перших творінь була колискова, яка за висновками медиків має заспокійливо-лікувальний ефект на людський мозок. Також, системи ШІ змогли написати цілий альбом в стилі black metal «Coditany of Timeness». Проаналізувавши інші композиції цього жанру, система змогла самостійно створити свій альбом з 5 творів.

Відповідно до результатів досліджень McKinsey & Company ШІ виявив здатність виявляти каталізатори виникнення емоцій та почуттів у людини. Це може свідчити про те, що з часом впливати на точки зору, принципи людини стане в рази легше. Таким чином недобродушні розробники нейронних мереж зможуть досягати своєї вигоди, незважаючи на думки простих людей.

Проблеми, які могли бути вирішеними за допомогою систем ШІ

Насправді, дуже важко сказати, як би закінчилась та чи інша історія, якби щось змінити, неможливо точно змоделювати ситуацію. Проте, зробити припущення ми в силі. Системи машинного навчання могли б змінити перебіг дуже багатьох значущих подій в історії як України, так і світу взагалі. Йдеться не лише про різноманітні кібератаки, які здійснюються щоденно(не беремо до уваги їх розмір та значущість нанесених збитків), а й про глобальні катастрофи, так як вибух на Чорнобильській Атомній Електростанції 1986 року, вибух на хімзаводі Phillips Petroleum Company 1989 року тощо.

Напевно доцільно буде розглядати аварію на ЧАЕС, оскільки саме ця подія стала світовим символом техногенної катастрофи. Уявіть собі, випробування реактора проводить не група людей, а ШІ, який попередньо пройшов навчання. Чи почала б така система випробування в умовах такого фізичного та техногідравлічного стану стабільності, який можна було порушити навіть незначними коливаннями? Важко сказати, проте скоріш за все, ні. Цей стан реактора і сам був викликаний некомпетентними діями персоналу, проте на цьому етапі цілком реально було запобігти катастрофі. Групі, котра проводила дану операцію, попросту не були доступні усі необхідні дані для визначення готовності реактора до випробування. Власне йде мова про вирішальний замір - оперативний запас реактивності. Чи помітила б система ШІ невідповідність значень змінних перед запуском випробування? Ми не можемо знати напевне, але маємо сміливість припустити, що так. Безпосереднім імпульсом для виникнення такої масштабної катастрофи стало введення в дії системи аварійної зупинки реактора, котра містила фатальну помилку в своїй конструкції і призвела до старту розгону потужності реактора. Ще в першій частині статті було зазначено: роботам не потрібен відпочинок, сон чи їжа. О 2 години ночі робот буде абсолютно такий же уважний та прискіпливий як і о 15 дня. Веду до того, що люди, які прийшли на зміну, цілком ймовірно приймали б зовсім інші рішення в екстремальній ситуації. Людей переповнювало почуття невідомості та страху, чого точно не може відчувати нейронна мережа. Не можна сказати точно, що за наявності такої мережі в роботі реактора в ту ніч, аварія б не відбулась чи наслідки могли б бути не настільки масштабними, але хочеться вірити в те, що дякуючи саме системам ШІ людство більше не зустрінеться з такою глобальною катастрофою.

Якщо говорити лише про забезпечення інформаційної безпеки засобами нейронних мереж, то можна згадати доволі багато різноманітних атак, яким можливо б дала відбій система ШІ. Наприклад злом Home Depot(2014), злом eBay(2014), атака на Ashley Madison(2015) тощо.

Для прикладу розглянемо злам Home Depot. Як повідомляє керівництво платформи, зловмисники ввійшли в мережу під обліковим записом так званого «продавця». Вже звідти хакери отримали доступ до «особливих» прав, що надало їм можливість завантажувати свій унікальний код в систему, який забезпечував саморозгортання на платформах самообслуговування сайту. Оскільки шкідливе програмне забезпечення ніколи не використовувалось раніше, воно доволі довгий проміжок часу не було виявленим. Як наслідок, було викрадено близько 56 мільйонів платіжних даних та 54 мільйонів електронних адрес з баз даних сервісу. Як відомо, атака сталася через вразливість операційної системи Windows(згодом був випущений «патч», який закривав прогалину в безпеці, проте було вже пізно). Неможливо точно підрахувати збиток нанесений цією вразливістю, але важливий факт - це одна з наймасовіших крадіжок даних користувача в історії. Чи могли системи ШІ не допустити цього? Навряд, проте однозначно могли зменшити розмір нанесених збитків, як мінімум завдяки більш своєчасному виявленню атаки.

Переваги ШІ над людською роботою очевидні. Така система однозначно є в рази уважнішою та прискіпливішою до процесів, які відбуваються. Враховуючи швидкість «самонавчання» нейронних мереж, можна сказати, що у вчасному виявленні загроз (за умови коректного формування завдань мережі), їм не буде рівних. Можливо, на даній стадії розвитку ШІ не може забезпечити необхідну реакцію на негативні процеси, проте однозначно зможе.

Аналіз заяв авторитетних компаній, фахівців та їх аргументів щодо подальшого використання штучного інтелекту в області безпеки

Замість того щоб служити заміною людському інтелекту і винахідливості, штучний інтелект зазвичай розглядається як допоміжний інструмент. Хоча штучний інтелект в даний час насилу справляється з завданнями здорового глузду в реальному світі, він вміє обробляти і аналізувати величезні масиви даних набагато швидше, ніж це може зробити людський мозок. Програмне забезпечення штучного інтелекту може потім повернутися з синтезованими курсами дій і представити їх користувачеві-людині. Таким чином, люди можуть використовувати штучний інтелект, щоб допомогти згладити можливі наслідки кожної дії та спростити процес прийняття рішень.

За словами Аміра Хусейна, засновника і генерального директора компанії машинного навчання SparkCognition., штучний інтелект - це свого роду друге пришестя програмного забезпечення. Це така форма програмного забезпечення, яка сама приймає рішення і здатна діяти навіть у ситуаціях, не передбачених програмістами. Штучний інтелект володіє більш широкими можливостями прийняття рішень на відміну від традиційного програмного забезпечення.

Ці риси роблять штучний інтелект дуже цінним у багатьох галузях промисловості, будь то просто допомога відвідувачам і співробітникам ефективно пересуватися по корпоративному корпусу або виконання такого складного завдання, як моніторинг вітряної турбіни, щоб передбачити, коли вона буде потребувати ремонту.

Машинне навчання часто використовується в системах, які захоплюють величезні обсяги даних. Наприклад, інтелектуальні системи управління енергією збирають дані з датчиків, прикріплених до різ-

них активів. Потім масиви даних контекстуалізуються алгоритмами машинного навчання і передаються особам, які приймають рішення, щоб краще зрозуміти вимоги до використання енергії та технічного обслуговування.

Хусейн вважає, що штучний інтелект є незамінним союзником, коли мова заходить про пошук дірок в захисті комп'ютерних мереж. Ми дійсно не можете мати достатньо експертів з кібербезпеки, щоб розглянути ці проблеми, через масштаб і зростаючу складність.

Штучний інтелект також змінює системи управління взаємовідносинами з клієнтами (CRM). Програмне забезпечення, таке як Salesforce або Zoho, вимагає інтенсивного втручання людини, щоб залишатися актуальним і точним. Але коли ми застосовуємо штучний інтелект до цих платформ, звичайна CRM-система перетворюється на автокорегуючу систему, яка залишається на вершині нашого управління відносинами.

Ще один приклад універсальності штучного інтелекту - це фінансовий сектор. Доктор Хосейн Рахнама, засновник і генеральний директор консьєрж-компанії штучного інтелекту Flybits і запрошений професор Масачусецького технологічного інституту, працював з TD Bank над інтеграцією штучного інтелекту в звичайні банківські операції, такі як іпотечні кредити.

У Salesforce вважають, що штучний інтелект має величезний потенціал для поліпшення роботи організації. Ця наступна хвиля штучного інтелекту дозволить компаніям постійно адаптувати процеси, засновані на минулому досвіді, що призведе, наприклад, до значного поліпшення таргетингу клієнтів, оскільки алгоритми глибокого навчання зможуть виявляти патерни поведінки, які з більшою ймовірністю приведуть до продажів. У ланцюжках поставок і виробництві потенційні вигоди включатимуть прогнозоване технічне обслуговування обладнання, а також оптимізацію прибутковості і запасів.

Експерти в галузі штучного інтелекту розглядають охорону здоров'я, юриспруденцію, освіту і навіть дослідження в області штучного інтелекту як кращі ранні можливості для помічників на робочому місці. На думку керівник досліджень IBM Cognitive Solutions Костаса Бекаса, якщо ми можемо використовувати штучний інтелект для автоматичного читання 400 000 наукових робіт, систематизувати знання, а потім об'єднати свою інтуїцію з машинним навчанням, ми зможемо загострити область досліджень. Це те, що, на нашу думку, дійсно змінить світ для досліджень в майбутньому.

Здатність людей ефективно взаємодіяти з системами штучного інтелекту за допомогою вербального, контекстуального спілкування дозволить вченим впровадити технологію в об'єкти навколо нас, незалежно від того, чи є у них екран чи ні.

Головний вчений IBM Watson Грейді Буч уявляв штучний інтелект і когнітивну силу в аватарці, об'єкті у вашій руці, роботі або навіть в стінах операційної, конференц-залу або космічного корабля. Якби ми були психологами і хотіли визначити, хто знаходиться в кімнаті, хто дивиться на кого, хто знаходиться в клітці один з одним або розмовляє один з одним, у нас був би в стінах когнітивний асистент.

Кемпбелл з IBM погоджувався, що системи штучного інтелекту, які розробляються, матимуть сильні та слабкі сторони. І у людей є сильні і слабкі сторони. Таким чином, потрібно способувати змусити людей і комп'ютери добре працювати разом.

Аналіз штучного інтелекту як гаранта повної безпеки даних в майбутньому

У все більш оцифрованому світі кібератаки зростають в обсязі, стаючи все більш складними. Оскільки все більше компаній використовують Інтернет для власних цілей, кіберзлочинці шукають способи проникнути у ваші захисні системи. Завдяки ШІ, машинному навчанню та розвідуванню кіберзагроз, підприємства можуть реагувати на загрози з підвищеною впевненістю та більшою швидкістю. Використання штучного інтелекту може допомогти розширити горизонти існуючих рішень в області кібербезпеки і прокласти шлях до створення нових. У міру того як мережі стають все більші і складніші, штучний інтелект може стати величезним благом для кіберзахисту організацій. Простіше кажучи, зростаюча складність мереж виходить за рамки того, з чим люди здатні впоратися самостійно.

Також штучний інтелект може вчитися і адаптуватися через досвід. В даний час Машинне навчання дозволяє машинам навчати самих себе. Це означає, що вони можуть створювати моделі для розпізнавання образів, а не покладатися на людей, щоб побудувати їх.

Штучний інтелект навчений споживати велику кількість даних, як блоги і новинні сюжети, що дає зрозуміти – він краще розуміє загрози кібербезпеки. Звідси, штучний інтелект в кібербезпеці використовує дані для виявлення загроз (дивні файли, підозрілі адреси тощо), перш ніж почати відповідь на законну загрозу.

Як уже згадувалося раніше, штучний інтелект і машинне навчання знижують ризик людської помилки. Люди можуть втомлюватися і відчувати нудьгу при виконанні монотонного завдання. Команди кібербезпеки намагаються працювати під вагою всіх даних, необхідних для оцінки ризиків, але ШІ може швидко розпізнати всі загрозливі фактори. Однак штучний інтелект і людський інтелект повинні працювати разом. Крім того, людські експерти забезпечують здоровий глузд, якого немає у машин, і все ж краще справляються з рішенням, які дії зробити.

Ми можемо подолати багато ризикованих ситуацій, розробивши робота з штучним інтелектом, який, у свою чергу, може робити ризиковані речі для нас. Нехай він відправляється на Марс, знешкоджує бомбу, досліджує найглибші частини океанів, видобуває вугілля і нафту, його можна ефективно використовувати в будь-яких природних або техногенних катастрофах.

Переваги, описані вище, є лише малою частиною потенціалу ШІ в наданні допомоги кібербезпеки, але є і обмеження, які заважають машині стати основним інструментом, використовуваним в цій галузі. Для того, щоб побудувати і підтримувати систему

штучного інтелекту, компаніям буде потрібно величезна кількість ресурсів, включаючи пам'ять, дані і обчислювальну потужність. Крім того, оскільки системи штучного інтелекту навчаються за допомогою навчальних наборів даних, фірмам з кібербезпеки необхідно отримати в свої руки безліч різних наборів даних про шкідливі коди, нешкідливі коди і аномаліях. Отримання всіх цих точних наборів даних може зайняти дуже багато часу та ресурсів, які деякі компанії не можуть собі дозволити.

Штучний інтелект надає дивовижні можливості для задоволення самих спеціалізованих потреб клієнтів і створення абсолютно нових бізнес-моделей. Вона має здатність вирішувати деякі з найбільш гострих соціальних проблем. Але, оскільки рішення на основі штучного інтелекту починають мати все більший вплив на людське життя, виникають етичні питання про те, як технологія впливає на суспільство. Як ми можемо гарантувати, що ШІ ставиться до всіх справедливо, і в якій мірі організація несе відповідальність за захист конфіденційності?

Однак системи штучного інтелекту розроблені людьми і вони будуть ідеальними настільки, наскільки в них надходять дані. Навіть коли один алгоритм створює інший, початковий алгоритм був створений людьми і тому схильний до людських упереджень. Інсайт або передбачення не є більш чесним просто тому, що його згенерував бот.

На думку Тімніта Гебру, наукового співробітника команди етичного штучного інтелекту в Google, нам ще багато чого належить зробити, щоб навчити моделей міркувати розсудливо. Їх можна навчити тільки знаходити закономірності в історичних даних. Проблема полягає в тому, що ці навчальні дані не є нейтральними — вони можуть легко відображати упередження людей, які їх зібрали. Це означає, що він може кодувати тенденції та моделі, які відображають і увічнюють забобони та шкідливі стереотипи.

Оскільки вище ми описували в основному переваги систем ШІ, хочемо окремо виділити їх конкретні недоліки:

1.Моделі машинного навчання часто навчаються за даними з потенційно недостовірних джерел, включаючи інформацію про натовп, дані соціальних медіа та створені користувачем дані, такі як рейтинг задоволеності клієнтів, історія покупок або веб-трафік. Супротивники можуть впроваджувати на задньому плані або «троянців» у моделі машинного навчання шляхом отруєння навчальними наборами зі шкідливими зразками.

2.У традиційній системі компрометація впровадження бекдор означає створення секретного способу доступу до системи, не будучи авторизованим користувачем. Зазвичай це проявляється у формі програміста, який вручну кодує бекдор в систему, яку вони будують, або хакера, що впроваджує фрагмент коду, який відкриває систему для доступу з іншого засобу. Може бути дивним дізнатися, що такі чорні ходи можуть бути імплантовані в глибокі нейронні мережі для досягнення бажаних результатів від небажаних або спеціальних вхідних даних.

3.Можливість атак, які не потребують зміни моделі чи тренувальних даних, що дозволяє зовнішнім зловмисникам використовувати цей підхід. Це суперечлива атака. Візьміть два зображення нижче, візуально для людського ока вони виглядають як однакові зображення червоної лисиці. Перше зображення дійсно є незмінним зображенням червоної лисиці, однак друге зображення було змінено нейронною мережею атакуючих нападів таким чином, що класифікуюча нейронна мережа здатна класифікувати це зображення майже досконалою мірою точності, як Дональд Трамп. Природно, це створює проблему для Дональда Трампа (і перевага для спільноти лисиць), якщо системи безпеки Білого дому для розпізнавання обличчя покладаються на DCNN (рис. 2), (рис. 3).

Рис. 2. Оригінальне зображення лисиці, проаналізоване ШІ

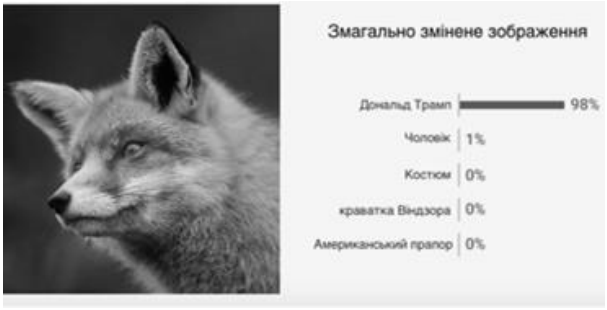


Рис. 3. Змінене зображення лисиці, проаналізоване ШІ

4.Навіть якщо припустити, що набір даних без спотворень і високоточна модель, цей успіх супроводжується дуже важливим застереженням: моделі, «засвоєні» сучасними моделями машинного навчання, є відносно крихкими. В результаті модель працює тільки з даними, які за своєю природою є такими самими, використовуваним в процесі навчання. Якщо використовувати дані, які навіть трохи відрізняються за своїм характером від типів змін, які він бачив у вихідному наборі даних, модель може повністю потерпіти невдачу. Це серйозне обмеження, яке можуть використовувати зловмисники: вводячи штучні зміни, такі як шматочок стрічки або інші відхиляються шаблони, зловмисник може порушити модель і контролювати її поведінку на основі введеного штучного шаблону.

5.Іншим викликом є той факт, що роботу деяких систем ШІ неможливо пояснити повністю. Припускають, що ця відсутність пояснень може підвищити сприйняття ризику та обмежити використання ШІ для деяких застосувань, наприклад, у критично важливих для безпеки умовах та з високою регламентацією.

Такі деякі переваги і недоліки штучного інтелекту. Кожен новий винахід або прорив буде мати і те, і інше, але ми, люди, повинні піклуватися про це і використовувати позитивні сторони винаходу для створення кращого світу. Штучний інтелект володіє

величезними потенційними перевагами. Ключ для людей буде гарантувати, що" повстання роботів " не вийде з-під контролю. Деякі люди також кажуть, що штучний інтелект може знищити людську цивілізацію, якщо він потрапить в чужі руки. Але все ж жодне з додатків штучного інтелекту, створених в такому масштабі, не може знищити або поневолити людство.

Що ж, давайте порівняємо людину і штучний інтелект, коли справа доходить до обробки інформації. Один повний аналіз безпеки, який читає машина, в середньому становить лише 10 слів, прочитаних людиною (рис. 4).

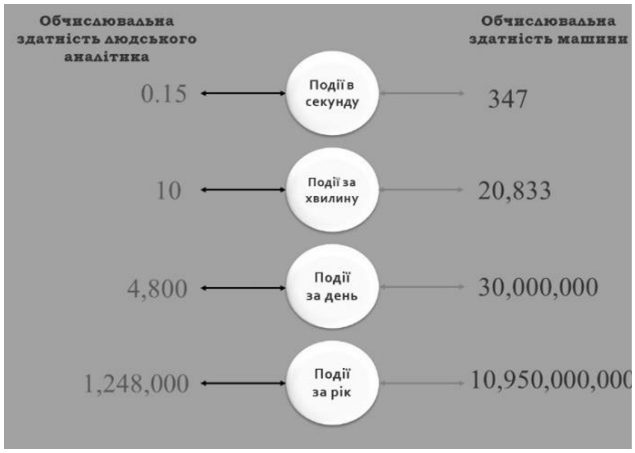


Рис. 4. Обробка даних людини та машини

Навіть найменша затримка може означати різницю між атакою і дією (рис. 5).

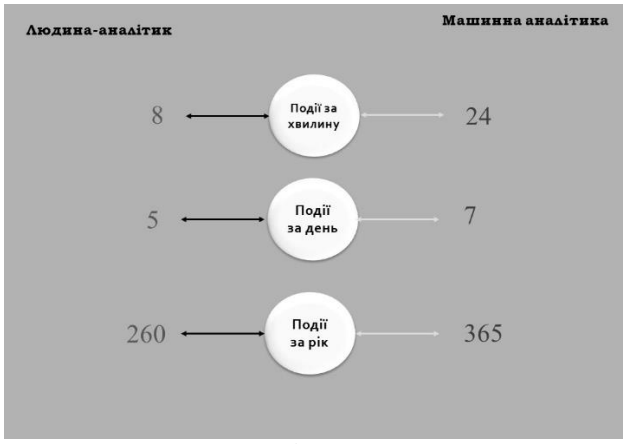


Рис. 5. Атака і дія

Бути аналітиком з кібербезпеки у великій компанії сьогодні - все одно що шукати голку в стозі сіна, якби цей стіг мчав до вас зі швидкістю оптоволокна. У кібербезпеки недостатньо часу; це не може зайняти години або навіть дні, щоб зрозуміти, чому відбувається атака. Ось чому отримання аналітиком можливості створювати і налаштовувати моделі машинного навчання є найбільш важливим аспектом системи. Розмах і масштаб сьогоднішніх загроз кібербезпеки-це нова норма. На щастя, наявні в даний час інструменти, такі як штучний інтелект і машинне навчання, все більшою мірою здатні впоратися з цим завданням. Щоб успішно використовувати нові, передові технології для боротьби з сьогоднішнім постійно мінливим ландшафтом загроз, взаємодія людини і машини-це те, над чим ми повинні працювати.

Висновок

Штучний інтелект дозволяє машинам вчитися на досвіді, пристосовуватися до нових вхідних даних і виконувати людські завдання. Більшість прикладів штучного інтелекту, про які ви чуєте сьогодні – від комп'ютерів, що грають в шахи, до самокерованих автомобілів - значною мірою залежать від глибокого навчання та обробки мови. Використовуючи ці технології, комп'ютери можуть бути навчені виконувати певні завдання, обробляючи великі обсяги даних і розпізнаючи закономірності в даних. Штучний інтелект збирається змінити кожну галузь, але ми повинні зрозуміти його межі. Принципове обмеження ШІ полягає в тому, що він навчається на основі отриманих даних. Немає іншого способу, за допомогою якого можна було б інкорпорувати знання. Це означає, що будь-які неточності в даних будуть відображені в результатах. І будь-які додаткові шари прогнозу або аналізу повинні бути додані окремо.

Сучасні системи штучного інтелекту навчені виконувати чітко визначені завдання. Система, яка грає в покер, не може грати в пасьянс або шахи. Система, яка виявляє шахрайство, не може керувати автомобілем або давати вам юридичні консультації. Насправді, система штучного інтелекту, яка виявляє шахрайство в сфері охорони здоров'я, не може точно виявити податкове шахрайство. Іншими словами, ці системи дуже і дуже спеціалізовані. Вони зосереджені на одному завданні і поводяться далеко не так, як люди. Аналогічним чином, самонавчальні системи не є автономними системами. Уявні технології штучного інтелекту, які ми бачимо в кіно і телебаченні, все ще є науковою фантастикою. Але комп'ютери, які можуть досліджувати складні дані для вивчення та вдосконалення конкретних завдань, стають досить поширеними.

Література

[1]. *Сучасний стан та перспективи розвитку робототехніки в Україні*. [Електронний ресурс]. Режим доступу: http://oldconf.neasmo.org.ua/node/2298.

[2]. *Як прогресує штучний інтелект: звіт про останні досягнення*. [Електронний ресурс]. Режим доступу: https://www.epravda.com.ua/publications/2019/07/15/649648/.

[3]. *10 прикладів, як штучний інтелект може змінити ваш спосіб життя*. [Електронний ресурс]. Режим доступу: https://www.radiosvoboda.org/a/29015231.html.

[4]. *Найбільші кібератаки проти України з 2014 року. Інфографіка*. [Електронний ресурс]. Режим доступу: https:// nv. ua/ ukr/ ukraine/ events/ najbilshi-kiberataki-proti-ukrajini-z-2014-roku-infografika-1438924.html.

[5]. *Апокаліпсис у мережі. 7 найбільших хакерських атак в історії.* [Електронний ресурс]. Режим доступу: https://nv.ua/ukr/techno/gadgets/apokalipsis-v-merezhi-7-najbilshih-hakerskih-atak-v-istoriji-1393066.html.

[6]. *Десять найстрашніших техногенних катастроф, які увійшли в історію людства*. [Електронний ресурс]. Режим доступу: https://khm.depo.ua/ukr/khm/ desyat – naystrashnishih – tehnogennih - katastrof-v-istoriyi-lyudstva-10022016200100.

[7]. *Чорнобильська атомна електростанція*. [Електронний ресурс]. Режим доступу: https://ru.wikipedia.org/wiki/Чернобыльская_АЭС.

[8]. *Home Depot: Вследствие взлома в сентябре были похищены 53 миллиона адресов электронной почты*. [Електронний ресурс]. Режим доступу: https://www.securitylab.ru/news/461601.php.

[9]. *Причини та масштаби аварії.* [Електронний ресурс]. Режим доступу: https://chnpp.gov.ua/ua/uk/component/content/article/42-about/accident-of-1986/175-2012-02-01-08-01-38529.

[10]. *A look at the positive side of AI and drones*. [Електронний ресурс]. Режим доступу: https://borgenproject.org/a-look-at-the-positive-side-of-ai-and-drones/.

[11]. *Positive & Negative Effects of Artificial Intelligence*. [Електронний ресурс]. Режим доступу: https:// www.koganpage.com/ article/ positive-negative-effects-of-artificial-intelligence.

[12]. *Advantages of Artificial Intelligence*. [Електронний ресурс]. Режим доступу: https://www.educba.com/advantages-of-artificial-intelligence/.

[13]. *Benefits & risks of artificial intelligence*. [Електронний ресурс]. Режим доступу: https://futureoflife.org/ background/benefits-risks-of-artificial-intelligence/.

[14]. *What is the future of artificial intelligence?* [Електронний ресурс]. Режим доступу: https://www.quora.com/What-is-the-future-of-artificial-intelligence-1.

[15]. *Implications of Artificial Intelligence for Cybersecurity: Proceedings of a Workshop.* [Електронний ресурс]. Режим доступу: https://www.nap.edu/read/25488/chapter/6.

[16]. *Attacking Artificial Intelligence: AI's Security Vulnerability and What Policymakers Can Do About It*. [Електронний ресурс]. Режим доступу: https://www.belfercenter.org/publication/AttackingAI.

[17]. I. Nicolae, M. Sinn, *The Adversarial Robustness Toolbox v0.3.0: Closing the Backdoor in AI Security*. [Електронний ресурс]. Режим доступу: https://www.ibm.com/blogs/research/2018/08/art-v030-backdoor/.

[18]. J. Aungiers, *AI security neural network backdoors.* [Електронний ресурс]. Режим доступу: https://www.altumintelligence.com / articles / a / AI-Security-Neural-Network-Backdoors.

УДК 654.071

Опирский И.Р., Головчак Р.В., Мойсийчук И.Р. Перспективы развития искусственного интеллекта в контексте информационной безопасности

Аннотация. *Искусственный интеллект - концепция, согласно которой машины способны осуществлять некоторую интеллектуальную деятельность, которая присуща людям или животным. Другими словами, можно сказать, что это понятие включает в себя любое устройство, обладающий способностью воспринимать его окружения и предпринимать действия, увеличивающие шанс на успешное достижение целей. Однако, несмотря на продолжающийся прогресс в скорости компьютерной обработки и объеме памяти, до сих пор нет программ, которые могли бы сравниться с человеческой гибкостью в более широких областях или в задачах, требующих больших повседневных знаний. С другой стороны, некоторые программы достигли уровня производительности человеческих экспертов и профессионалов в выполнении определенных конкретных задач, так что искусственный интеллект в этом ограниченном смысле можно найти в таких разнообразных приложениях, как медицинская диагностика, компьютерные поисковые системы и распознавания голоса или почерка. Целью данной работы является, собственно, определение положительных и отрицательных аспектов применения систем искусственного интеллекта в области безопасности информации. Определено, что такие системы имеют весомую роль в текущем и последующем обеспечении безопасности данных, а также приведен ряд недостатков таких систем для будущего их учета. В статье были рассмотрены то, что искусственный интеллект был разработан путем изучения того, как человеческий мозг думает, учится и принимает решение, а затем применяет эти биологические механизмы к компьютерам. В отличие от классических вычислений, где кодеры обеспечивают точные входы, выходы и логику, искусственный интеллект основан на предоставлении машине входных данных и желаемого результата, позволяя машине развивать свой собственный путь для достижения поставленной цели. Искусственный интеллект - это технология, которая превращает все сферы жизни. Это широкий инструмент, который позволяет людям переосмыслить, как мы интегрируем информацию, анализируем данные и используем полученные результаты для улучшения процесса принятия решений. Они меняют способ, которым мы ищем информацию, как мы общаемся друг с другом, даже если мы ведем себя. Эта трансформация касается многих областей, включая образование. Основной целью данной статьи является обзор решения проблем с помощью искусственных технологий. В представленном обзоре литературы мы рассмотрели четыре категории: индивидуальный образовательный контент, инновационные методы обучения, технология расширенной оценки, коммуникация между студентом и преподавателем. Рассмотрев публикации на эту тему, мы представляем здесь возможную картину того, как искусственный интеллект изменит ландшафт образования. Начиная с краткой истории искусственного интеллекта, в данной статье представлен общий обзор этой технологии.*

Ключевые слова: *искусственный интеллект, машинное обучение, безопасность информации, системы машинного обучения, человек.*

Opirskyy I., Holovchak R., Moysiychuk I. Prospects of development of artificial intelligence in the context of information security

Abstract. *Artificial intelligence is a concept in which machines are capable of performing some intellectual activity that is inherent in humans or animals. In other words, this concept includes any device that has the ability to perceive its environment and take actions that increase the chance of successfully achieving goals. However, despite ongoing progress in computer processing speed and memory, there are still no programs that can match human flexibility in broader areas or in tasks that require extensive daily knowledge. On the other hand, some programs have reached the level of productivity of human experts and professionals in performing certain specific tasks, so that artificial intelligence in this limited sense can be found in such*

diverse applications as medical diagnostics, computer search engines and voice or handwriting recognition. The purpose of this work is, in fact, to determine the positive and negative aspects of the use of artificial intelligence systems in the field of information security. It is determined that such systems have an important role in the current and future data security, as well as a number of shortcomings of such systems for their future consideration. The paper discusses that artificial intelligence was developed by studying how the human brain thinks, learns, and makes decisions, and then applies these biological mechanisms to computers. Unlike classical computing, where encoders provide accurate inputs, outputs, and logic, artificial intelligence is based on giving the machine input and the desired result, allowing the machine to develop its own path to achieve its goal. Artificial intelligence is a technology that transforms all spheres of life. It is a broad tool that allows people to rethink how we integrate information, analyze data, and use the results to improve decision-making. They change the way we look for information, how we communicate with each other, even how we behave. This transformation affects many areas, including education. The main purpose of this article is to review the solution of problems using artificial technologies. In the presented literature review, we considered four categories: individual educational content, innovative teaching methods, advanced assessment technology, communication between student and teacher. Having considered publications on this topic, we present here a possible picture of how artificial intelligence will change the landscape of education. Starting with a brief history of artificial intelligence, this article provides an overview of this technology.
Keywords: *artificial intelligence, machine learning, information security, machine learning systems, humans.*

Опірський Іван Романович, д.т.н., доц., професор кафедри захисту інформації Національного університету «Львівська політехніка».
Опирский Иван Романович, д.т.н., доц., профессор кафедры защиты информации Национального университета «Львовская политехника».
Opirskyy Ivan, Doctor of Technical Sciences, Associate Professor, Professor of the Department of Information Protection of the National University "Lviv Polytechnic".

Головчак Романа Василівна, студент кафедри захисту інформації Національного університету «Львівська політехніка».
Головчак Романа Васильевна, студент кафедры защиты информации Национального университета «Львовская политехника».
Holovchak Romana, student of the Department of Information Protection of the National University "Lviv Polytechnic".

Мойсійчук Ірина Русланівна, студент кафедри захисту інформації Національного університету «Львівська політехніка».
Мойсийчук Ирина Руслановна, студент кафедры защиты информации Национального университета «Львовская политехника».
Moysiychuk Iryna, student of the Department of Information Protection of the National University "Lviv Polytechnic".

Отримано *13 червня 2020 року*, затверджено редколегією *11 липня 2020 року*

© Tsurkan V. Method of information security management system structure synthesizing // Ukrainian Scientific Journal of Information Security, 2020, vol. 26, issue 2, pp. 116-122.

DOI: 10.18372/2225-5036.26.14926

МЕТОД СИНТЕЗУВАННЯ СТРУКТУРИ СИСТЕМ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Василь Цуркан

Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України

ЦУРКАН Василь Васильович, к.т.н., доцент

Рік та місце народження: 1982 рік, м. Харків, Україна.
Освіта: Національний технічний університет України «Київський політехнічний інститут» (з 2016 року - Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського)», 2005 рік.
Посада: старший науковий співробітник з 2019 року.
Наукові інтереси: інформаційна безпека, кібербезпека, теорія ризику, системні дослідження.
Публікації: понад 100 наукових публікацій, серед них монографії, наукові статті.
E-mail: v.v.tsurkan@gmail.com.
Orcid ID: 0000-0003-1352-042X.

Анотація. *Розглянуто потреби, очікування та пов'язані з ними обмеження зацікавлених сторін як вхідні дані для специфікування вимог до систем управління інформаційною безпекою. Вони доповнюються встановленням внутрішніх і зовнішніх обставин, що впливають або можуть впливати на діяльність організацій. За специфікацією вимог визначається множина взаємопов'язаних функцій з внутрішніми та зовнішніми інтерфейсами. Кожна з них розкладається відповідно до структурних елементів систем управління інформаційною безпекою на функції підсистем, комплексів, компонентів. При цьому показується недостатність визначення структурних елементів і властивих їм функцій. Це обмежується необхідністю з'ясування сутності систем управління інформаційною безпекою з огляду на потреби, мету, процеси, структуру організацій. Тому вони розглядаються як сукупність підсистем, комплексів, компонентів, так і відношень між ними. Загалом цією сукупністю утворюється структура систем управління інформаційною безпекою. Для її представлення використовуються діаграми в графічній нотації SysML. За нею структурні елементи відображаються блоками як модульними одиницями. Тому системи управління інформаційною безпекою представляються деревом модульних одиниць. Характерні для них ознаки визначаються властивостями. Серед властивостей виокремлюються спеціальні класи – порти та обмеження. Їхнє використання дозволяє акцентувати на обмеженнях і особливостях взаємодії блоків між собою. Тоді як особливості такої взаємодії враховуються типами відношень. Тож методом синтезування структури систем управління інформаційною безпекою визначаються її структурні елементи (підсистеми, комплекси, компоненти) та відношення між ними. Завдяки цьому можливе встановлення властивостей даних систем стосовно конкретних варіантів розроблення і демонстрування вірогідних напрямів досягнення поставленої мети. Зокрема, збереження конфіденційності, цілісності та доступності інформації в організаціях шляхом оцінювання ризиків. Цим гарантується досягненість системами управління інформаційною безпекою запланованих результатів впровадження. Насамперед надання впевненості зацікавленим сторонам належного управління ризиками з прийнятним рівнем.*

Ключові слова: *блок, властивість, відношення, структурний елемент, структура, система управління інформаційною безпекою, діаграма структури, SysML.*

Вступ

Вхідними даними для розроблення систем управління інформаційною безпекою є потреби, очікування і пов'язані з ними обмеження з боку зацікавлених сторін. Вони доповнюються встановленням внутрішніх і зовнішніх обставин, що впливають або можуть впливати на діяльність організацій. На основі їхнього аналізування визначаються вимоги до систем управління інформаційною безпекою. Завдяки цьому встановлюються відповідності індивідуальним, груповим характеристикам, систематизуються, виявляються відношення між ними і, як наслідок, специфікуються вимоги. За такою специфікацією розробляється функціональна архітектура систем управління інформаційною безпекою. Це досягається визначенням множини взаємопов'язаних функцій шляхом їх функціонального аналізування. Кожна з них характеризується наявністю внутрішніх і зовнішніх інтерфейсів. Такі інтерфейси виникають унаслідок взаємодії функцій між собою. Відповідно до структурних елементів систем управління інформаційною безпекою вони розкладаються на функції. Так встановлюється послідовність виконання функцій системами управління інформаційною безпекою на рівнях їхніх структурних елементів [1-3].

Однак, при розробленні систем управління інформаційною безпекою недостатньо визначити структурні елементи та властиві їм функції. Це пов'язано з необхідністю з'ясування сутності таких систем з огляду на потреби, мету, процеси, структуру організацій. Тому вони представляються як сукупність підсистем, комплексів, компонентів, так і відношень між ними. Таке представлення тлумачиться

як структура. Нею визначаються властивості систем управління інформаційною безпекою стосовно конкретних варіантів розроблення. Як наслідок, демонструються вірогідні напрями досягнення поставленої мети – збереження конфіденційності, цілісності та доступності інформації в організаціях шляхом оцінювання ризиків. Цим гарантується досягненість системами управління інформаційною безпекою запланованих результатів впровадження. Насамперед надання впевненості зацікавленим сторонам належного управління ризиками з прийнятним рівнем. Тому синтезування структури систем управління інформаційною безпекою є актуальним завданням [1, 4, 5].

Аналіз існуючих досліджень

Розроблення систем управління інформаційною безпекою регламентується вимогами та настановами, імплементованих в Україні, міжнародних стандартів ISO/IEC 27000, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27003 [1]. Відповідно до їхніх положень дослідження і публікації орієнтовані на розкриття окремих аспектів, наприклад [6-12]. У [6] акцентується на складнощах усвідомлення і забезпечення відповідності міжнародному стандарту ISO/IEC 27001. Для їх подолання пропонується метод оцінювання ризиків ISMS-CORAS. Ним визначаються технічні прийоми та рекомендації встановлення відповідності систем управління інформаційною безпекою. Інженерне середовище даних систем розглянуто в [7]. Зокрема, оцінюється ефективність його використання для підтримання організацій при розробленні систем управління інформаційною безпекою за вимогами ISO/IEC 27001. Аспекти забезпечення неперервності діяльності організацій розглянуто в [8]. Зокрема, розроблено фреймворк системи управління інформаційною безпекою. Він використовується для оцінювання рівня зрілості організацій і надання рекомендацій з впровадження процесів забезпечення інформаційної безпеки та управління відповідно до вимог ISO/IEC 27001. Рольову структуру системи управління інформаційною безпекою наведено в [9]. Визначено ролі працівників організації (на прикладі патентного відомства) стосовно забезпечення цілісності та доступності її інформаційних активів (заявок на винаходи, патентів). Розроблення, впровадження, контролювання та вдосконалення системи управління інформаційною безпекою на основі моделі зрілості представляється у [10]. Досягнення бажаного її рівня здійснюється створенням плану вдосконалення. Вхідними даними для нього є результати оцінювання зрілості організації стосовно забезпечення інформаційної безпеки. Конфіденційність, цілісність, доступність, загрозу, вразливість виокремлено як первинні параметри системи управління інформаційною безпекою у [11]. Значення кожного з них встановлюються методом контрольних списків. Його використання дозволяє оцінити відповіді розпорядників інформаційних активів і більш ефективно обрати засоби забезпечення інформаційної безпеки. Завдання формування прийнятних варіантів організаційного складу та структури автоматизованої системи управління різнорідними засобами захисту інформації вирішено в [12].

Отже, за результатами аналізування останніх досліджень і публікацій з'ясовано їхню орієнтованість на встановлення відповідності систем управління інформаційною безпекою вимогам і настановам міжнародних стандартів, зокрема, ISO/IEC 27001. По-перше, визначенням технічних прийомів та рекомендації методом оцінювання ризиків ISMS-CORAS [6]. По-друге, розробленням і впровадженням систем управління інформаційною безпекою за рівнем зрілості [8, 10]. По-третє, визначенням ролей працівників організації стосовно забезпечення цілісності та доступності її інформаційних активів [9]. По-четверте, виокремленням і встановленням значень первинних параметрів систем управління інформаційною безпекою методом контрольних списків [11]. По-п'яте, формуванням і управлінням прийнятними варіантами різнорідних засобів захисту інформації [12]. Однак, поза увагою залишається аспект виокремлення структурних елементів (підсистем, комплексів, компонентів), відношень між ними. Для цього запропоновано використання діаграм структури в графічній нотації SysML [3].

Метою даної роботи є визначення структурних елементів, відношень між ними систем управління інформаційною безпекою методом синтезування їхньої структури.

Основна частина дослідження

Структурні елементи систем управління інформаційною безпекою у графічній нотації SysML відображаються блоками [3]. Блок тлумачиться як модульна одиниця структури (див. рис. 1) [13, 14], якою моделюються підсистеми, комплекси, компоненти. Наприклад [15, 16]: оцінювання ризику, оброблення ризику; ідентифікування ризику, визначення оцінок ризику; ідентифікування вірогідності (ймовірності) реалізації загроз, ідентифікування наслідків реалізації загроз. Тому системи управління інформаційною безпекою представляються деревом модульних одиниць. Таке представлення дозволяє враховувати потреби, мету, процеси та структуру організацій. Воно реалізується шляхом визначення типів блоків, типів відношень між ними та способів їх поєднання відповідно до мети розроблення систем управління інформаційною безпекою. Зокрема, забезпечення інформаційної безпеки з прийнятним рівнем ризику та, як наслідок, гарантування зацікавленим сторонам належності управління ним в організації.

Для досягнення даної мети блоком визначається або одна, або декілька функцій відповідно до їхньої архітектури [16]. Структурні ознаки даного визначення характеризуються властивостями. Ними представляються тип і вказуються значення блоків, частин або посилання на інші блоки. Серед властивостей виокремлюються спеціальні класи – порти та обмеження. Портами відображаються прийнятні типи відношень між структурними елементами систем управління інформаційною безпекою. Зокрема, деталізуються місця підключення зовнішніх сутностей до блоків та способи взаємодії між ними. Наприклад, до блоку "Аналізування ризику" зовнішньою сутністю є інший блок "Зіставлення (атестування) ризику". Межі використання властивостей встановлюються обмеженнями. Наприклад, для блоку "Зіставлення (атестування) ризику" задається умова прийнятності / неприйнятності оцінок ризику для прийняття рішення про необхідність його оброблення [3, 13, 15].

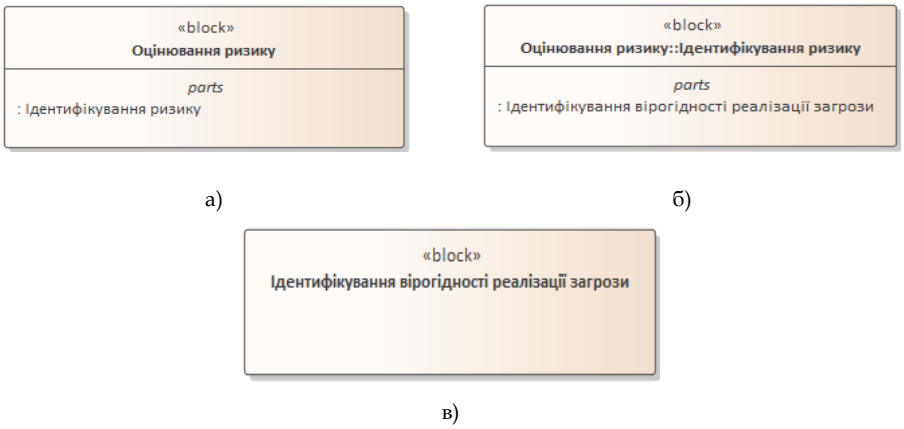


Рис. 1. Зображення структурних елементів систем управління інформаційною безпекою [3, 13, 17]:
а) підсистеми; б) комплексу; в) компоненту

Крім цього, для відображення структурних ознак блоків структури систем управління інформаційною безпекою у графічній нотації SysML виокремлюються три категорії властивостей [16]:

Частина – характеризує розкладання блоку на окремі складники. Взаємозв'язки між ними встановлюються за допомогою відношення композиціювання. Його використання орієнтоване на встановлення основних і додаткових властивостей блоку-частини в межах блоку-цілого. При цьому їхня кількість характеризується кратністю складника, що задається:

1) нижньою межею як мінімальною кількістю складників блоку-цілого. Задається нулем або будь-яким додатнім числом, наприклад: "0" – немає або "1" – один. Однак, при відображенні властивості "Частина" визначається тільки "0" або "1". Це обумовлено тим, що відношення композиціювання може встановлюватися тільки між двома блоками – цілим і його частиною. У цьому випадку встановлення "0" як нижньої межі означає існування блоку-частини без блоку цілого або його відсутність;

2) верхньою межею як максимальною кількістю складників блоку цілого. Задається або одиницею, або будь-яким додатнім числом, або "*" за великої кількості частин. При встановлені верхньої межі враховується умова, що вона рівна або більша за нижню. Тому верхня межа може визначатися лише "1". Це обумовлено існуванням блоку-частини тільки в межах одного блоку-цілого.

Властивість "Частина" відображається всередині блоку-цілого. Для цього відводиться окреме поле, що позначається словом "parts" (див., наприклад, рис. 1, б)). У такому полі кожному блоку-частині виділяється окремий запис. Зокрема, блок "Ідентифікування вірогідності реалізації загрози" є частиною блоку "Ідентифікування ризику". Тоді як останній є складником для цілого "Оцінювання ризику".

Посилання – характеризує включення до блоку інших блоків як його складників. Особливістю використання цієї властивості є можливість існування блоків-частин при знищенні цілого. Крім того воно застосовується для описання логічної ієрархії блоків структури систем управління інформаційною безпекою, що визначається блоками як елементами інших ієрархічних частин. За аналогією з властивістю "Частина" вказується всередині блоку-цілого в окремій секції. Для його позначення уживається слово "references" і виділяються окремі рядки для кожного посилання. Відношення між блоками задається типом "Агрегування" з визначенням кратності за аналогією з властивістю "Частина". Це означає, що нижня межа може дорівнювати "0" або "1", а верхня - "1". Наприклад, якщо розглядати як блок-ціле "Визначення оцінок ризику", то до нього можуть включатися блоки "Визначення якісних оцінок ризику", "Визначення кількісних оцінок ризику", "Визначення якісно-кількісних оцінок ризику". З огляду на характеризування взаємозв'язку між ними типу "Агрегування", кожна з цих частин може реалізовуватися як окремий структурний елемент, так і агрегуватися у межах блоку-цілого. Тоді його секція "references" визначатиметься трьома записами ": визначення якісних оцінок ризику", ": визначення кількісних оцінок ризику" ": визначення якісно-кількісних оцінок ризику".

Значення – використовуються для визначення характеристик структурних елементів систем управління інформаційною безпекою. До таких характеристик належать, наприклад: вірогідність (імовірність) реалізації загрози, наслідки реалізації загрози, оцінка ризику. Основою використання цієї властивості є встановлення діапазону її прийнятних значень при описанні блоку. Ці значення можуть бути типовими або, наприклад, визначатися законом розподілу ймовірності. Структура даних характеристик блоків описується типом значень на основі типів графічної нотації SysML або нових. Серед них виокремлюються:

1) примітивний тип – підтримуються скалярні значення, а саме: цілі, символьні, логічні та дійсні;

2) перелічуваний тип – визначається множина іменованих значень, що називаються літералами;

3) структурований тип – специфікується структура даних зі значеннями одного типу.

Оскільки типами представляються значення, то вони на відміну від блоків не характеризуються ідентичністю. Це означає, що їхня ідентичність визначається рівністю відповідних значень. Для задання властивостей "Значення" виділяється окрема секція блоку з ключовим словом "valueType". Тому при син-

тезуванні структури систем управління інформаційною безпекою важливо забезпечувати узгодженість типів значень характеристик її елементів.

Взаємозв'язок між структурними елементами систем управління інформаційною безпекою визначається відношеннями [16]. Встановленням їхнього типу враховуються його характер і особливості, наприклад [3, 16, 18, 19]: довільність, наслідуваність, узагальненість, структурність. Тож для визначення взаємозв'язку між структурними елементами систем управління інформаційною безпекою графічною нотацією SysML використовуються відношення асоціювання, узагальнення, агрегування, композиціювання [15, 16, 18, 19].

Асоціювання – тип відношення, яким визначається наявність взаємозв'язку між структурними елементами систем управління інформаційною безпекою (див., наприклад [3, 13, 17], рис. 2). Його використання вказує на довільність взаємодії або двох, або декількох блоків між собою. Рис. 2 демонструється приклад встановлення відношення типу "Асоціація" між блоками "Ідентифікування ризику" та "Визначення оцінок ризику". Цим ілюструється необхідність ідентифікування, зокрема, вірогідності (ймовірності) та наслідків реалізації загрози. Отримані результати комбінуються при визначенні оцінок ризику [20].

Рис. 2. Відношення асоціювання між блоками "Ідентифікування ризику" та "Визначення оцінок ризику"

Узагальнення – тип відношення, яким визначається взаємозв'язок між більш загальним ("батьком") і спеціалізованим стосовно нього ("нащадком") блоками (див., наприклад [3, 13, 17], рис. 3). З одного боку, це означає, що властивості батьківського блоку наслідуються блоками-нащадками. З іншого – ним можливе встановлення обмежень для блоків-нащадків при наслідуванні. Водночас останні можуть мати й додаткові властивості стосовно батьківського блоку. Направленість даного типу відношення дозволяє встановлювати ієрархічні взаємозв'язки тільки між двома структурними елементами систем управління інформаційною безпекою. Так, прикладом на рис. 3 демонструється наслідування блоком-нащадком "Визначення якісних оцінок ризику" властивостей батьківського блоку "Визначення оцінок". Насамперед атрибутів вірогідність (імовірність) реалізації загрози, наслідки реалізації загрози, оцінка ризику; операції визначення оцінок. Водночас блоку-нащадку властиві додаткові характеристики представлення результатів за порядковою шкалою [3]: низька, середня, висока.

Рис. 3. Відношення узагальнення між батьківським блоком "Визначення оцінок ризику" та блоком- нащадком "Визначення якісних оцінок ризику"

Агрегування – тип відношення, яким визначається взаємозв'язок між блоком та його складовими частинами (див., наприклад [3, 13, 17], рис. 4). Воно використовується для відображення системних зв'язків. Це означає, що структурні елементи систем управління інформаційною безпекою зіставляються як "ціле – частина". Тобто підсистеми ("ціле") можуть складатися з комплексів ("частина") або комплекс ("ціле") – з компонентів ("частина"). Їх використання дозволяє встановлювати відношення тільки між двома блоками. При цьому частини на відміну від відношення "Узагальнення" можуть мати відмінні властивості порівняно з цілим. Приклад встановлення взаємозв'язків "ціле-частина" показано на рис. 4. На ньому блок "Визначення оцінок ризику" зображується як "ціле". Тоді як його частинами є "Визначення якісних оцінок ризику" та "Визначення кількісних оцінок". Цим демонструються властивості блоку-цілого, якими враховується визначення оцінок залежно від обсягу даних про реалізації загроз і їхні наслідки для організації.

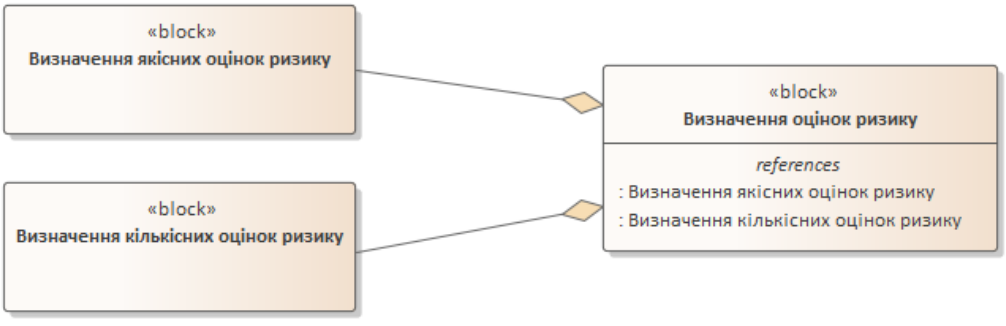


Рис. 4. Відношення агрегування між блоком-цілим "Визначення оцінок ризику" та блоками- частинами "Визначення якісних оцінок ризику", "Визначення кількісних оцінок ризику"

Композиціювання – тип відношення, яким визначається сильний взаємозв'язок між блоком-цілим та його складовими частинами (див., наприклад [3, 13, 17], рис. 5). Це означає, що видалення структурного елементу як цілого системи управління інформаційною безпекою призводить до знищення його складників. При цьому блок-частина може належати тільки одному композиту. Композиціювання розглядається як окремий випадок відношення "Агрегування". Його використання зображується на рис. 5. Як композит або блок-ціле показується "Аналізування ризику". Він складається з двох блоків-частин – "Ідентифікування ризику" та "Визначення оцінок ризику". Кожен з них може змінюватися до або після змінення цілого. Тому композит "Аналізування ризику" припиняє існувати внаслідок його видалення або окремих складників.

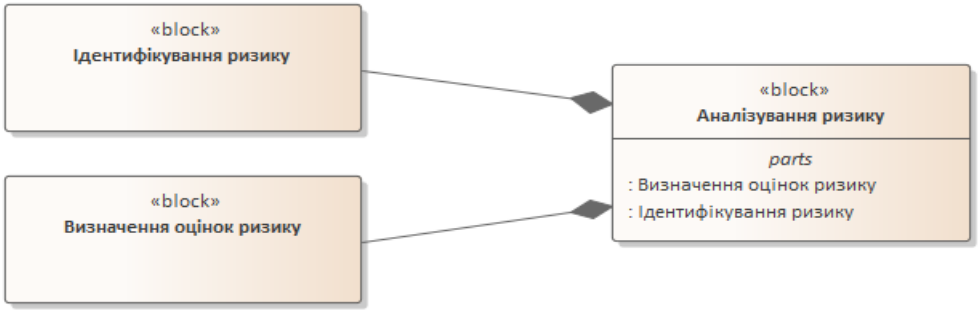


Рис. 5. Відношення композиціювання між блоками "Аналізування ризику" та блоками- частинами "Ідентифікування ризику ", "Визначення кількісних оцінок ризику"

Використання блоків і відношень між ними дозволяє синтезувати як структурні елементи систем управління інформаційною безпекою, так і встановити особливості їхнього представлення, взаємозв'язки блоків один з одним. Це узагальнюється завдяки використанню діаграм структури в графічній нотації SysML – визначення блоків і внутрішніх блоків [3]. Діаграмою визначення блоків відображається структура систем управління інформаційною безпекою зважаючи на її особливості (див., наприклад [13, 17], рис. 6). Тоді як для розкриття складових частин окремого структурного елементу використовується діаграма внутрішніх блоків.

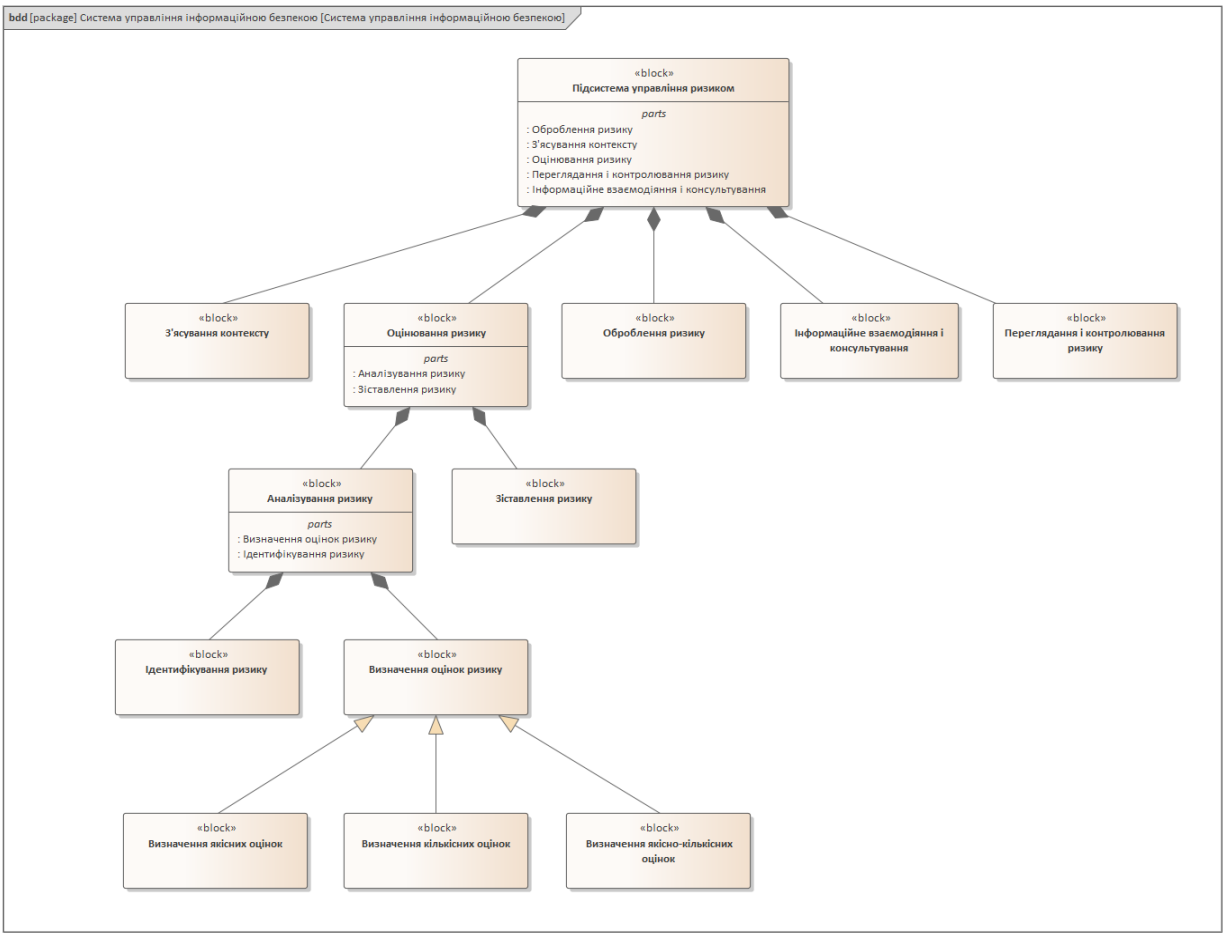


Рис. 6. Приклад синтезу структури систем управління інформаційною безпекою

Висновки

Отже, використання методу синтезування структури систем управління інформаційною безпекою дозволяє визначити її структурні елементи та відношення між ними. Для їхнього представлення застосовано діаграми структури в графічній нотації SysML. Воно реалізується шляхом визначення типів блоків, типів відношень між ними та способів їх поєднання. Завдяки цьому встановлюються властивості систем управління інформаційною безпекою стосовно конкретних варіантів розроблення і демонстрування вірогідних напрямів досягнення поставленої мети. Зокрема, збереження конфіденційності, цілісності та доступності інформації в організаціях шляхом оцінювання ризиків.

Література

[1]. *ISO/IEC 27001:2013, Information technology. Security techniques. Information security management systems. Requirements.* [Electronic resource]. URL: https://www.iso.org/standard/54534.html.

[2]. *ISO/IEC/IEEE 24748-4:2016. Systems and software engineering. Life cycle management. Part 4: Systems engineering planning*. [Electronic resource]. URL: https://www.iso.org/standard/56887.html.

[3]. В. Мохор, В. Цуркан, "Структурні елементи системи управління інформаційною безпекою", *Проблеми кібербезпеки інформаційно-телекомунікаційних систем*: *збірник матеріалів доповідей та тез міжнар. наук.-практ. конф., м. Київ, 12 черв. 2020 р.,* С. 332–334, 2020.

[4]. И. Прангишвили, *Системный подход и общесистемные закономерности. Серия "Системы и проблемы управления"*, Москва : СИНТЕГ, 2000, 528 с.

[5]. А. Антонов, *Системный анализ*, Москва: Высшая школа, 2004, 454 с.

[6]. K. Beckers, M. Heisel, B. Solhaug, K. Stolen, "ISMS-CORAS : A Structured Method for Establishing an ISO 27001 Compliant Information Security Management System", *Engineering Secure Future Internet Services and Systems: Lecture Notes in Computer Science*, vol. 8431, Springer, Cham, pp. 315–344, 2014. DOI: 10.1007/978-3-319-07452-8_13.

[7]. A. Suhaimi, D. Bao, H. Chen, J. Cheng, "Usefulness of ISMEE for Supporting Organizations with ISMSs", *Computer Science and its Applications : Lecture Notes in Electrical Engineering*, vol. 330, Springer, Berlin, Heidelberg, pp. 1331-1336, 2015. DOI: 10.1007/978-3-662-45402-2_185.

[8]. A. Aginsa, I. Edward Matheus, W. Shalannanda, "Enhanced information security management system framework design using ISO 27001 and Zachman framework – A study case of XYZ company", *Wireless and Telematics (ICWT) : 2nd International Conference, Yogyakarta, 1–2 Aug. 2016, Yogyakarta*, pp. 62–66, 2016. DOI: 10.1109/ ICWT. 2016. 7870853.

[9]. В. Сиротюк, "Модели, методы и средства разработки и внедрения эффективной системы управления информационной безопасностью патентного ведомства", *Науковедение*, Т. 9, № 6, С. 1-19, 2017.

[10]. D. Proença, J. Borbinha, "Information Security Management Systems – A Maturity Model Based on ISO/IEC 27001", *Business Information Systems. BIS 2018 : Lecture Notes in Business Information Processing*, vol. 320, Springer, Cham, pp. 102-114, 2018. DOI: 10.1007/978-3-319-93931-5_8.

[11]. S. Mortazavi, F. Safi-Esfahani, A checklist based evaluation framework to measure risk of information security management systems", *International Journal of Information Technology,* Vol. 11, Iss. 3, pp. 517-534, 2019. DOI: 10.1007/s41870-019-00302-0.

[12]. В. Селифанов, Р. Мещеряков, "Методика формирования допустимых вариантов организационного состава и структуры автоматизированной системы управления информационной безопасностью", *Моделирование, оптимизация информационные технологии*, Том 8, вып. 1, С. 1-13, 2020. DOI: 10.26102/2310-6018/2020.28.1.001.

[13]. *ISO/IEC 27005:2018, Information technology. Security techniques. Information security risk management.* [Electronic resource]. URL: https://www.iso.org/ru/standard/75281.html.

[14]. В. Цуркан, "Метод функціонального аналізування систем управління інформаційною безпекою", *Кібербезпека: освіта, наука, техніка*, Том 4, № 8, С. 192-201, 2020. DOI: 10.28925/2663-4023.2020.8.192201.

[15]. *OMG Systems Modeling Language (OMG SysML™).* [Electronic resource]. URL: https://sysml.org/res/docs/specs/OMGSysML-v1.6-19-11-01.pdf.

[16]. A. Moore, R. Steiner, *A Practical Guide to SysML. The Systems Modeling Language,* Waltham: Elsevier, 2015, 640 p.

[17]. *Model based systems engineering with Sparx Systems Enterprise Architect*. [Electronic resource]. URL: https://sparxsystems.com/resources/user-guides/.

[18]. А. Леоненков, *Самоучитель UML 2*, Санкт-Петербург : БХВ-Петербург, 2007, 576 с.

[19]. *Unified Modeling Language® (OMG UML®).* [Electronic resource]. URL: https://www.omg.org/spec/UML/2.5.1/PDF.

[20]. *ISO Guide 73:2009. Risk management. Vocabulary*. [Electronic resource]. URL: https://www.iso.org/standard/44651.html.

УДК 004[056.53+413.4]::303.732.4

Цуркан В.В. Метод синтезирования структуры систем управления информационной безопасностью

Аннотация. *Рассмотрены потребности, ожидания и связанные с ними ограничения причастных сторон как входящие данные для спецификации требований к системам управления информационной безопасностью. Они дополняются установлением внутренних и внешних обстоятельств, которые влияют или могут влиять на деятельность организаций. По спецификации требований определяется множество взаимосвязанных функций с внутренними и внешними интерфейсами. Каждая из них раскладывается в соответствии со структурными элементами систем управления информационной безопасностью на функции подсистем, комплексов, компонентов. При этом показывается недостаточность определения структурных элементов и свойственных им функций. Это ограничивается необходимостью выяснения сущности систем управления информационной безопасностью учитывая потребности, цель, процессы, структуру организации. Поэтому*

они рассматриваются как совокупность подсистем, комплексов, компонентов, так и отношений между ними. В общем этой совокупностью образуется структура систем управления информационной безопасностью. Для ее представления используются диаграммы в графической нотации SysML. За ней структурные элементы отображаются блоками как модульными единицами. Поэтому системы управления информационной безопасностью представляются деревом модульных единиц. Характерные для них признаки определяются свойствами. Среди свойств выделяются специальные классы – порты и ограничения. Ихние использование позволяет акцентировать на ограничениях и особенностях взаимодействия блоков между собой. Тогда как особенности такого взаимодействия учитываются типами отношений. Таким образом, методом синтезирования структуры систем управления информационной безопасностью определяются ее структурные элементы (подсистемы, комплексы, компоненты и отношения между ними. Благодаря этому возможно установление свойств данных систем относительно конкретных вариантов разработки и демонстрация возможных направлений достижения поставленной цели. В частности, сохранение конфиденциальности, целостности и доступности информации в организациях путем оценивания рисков. Этим гарантируется достигаемость системами управления информационной безопасностью запланированных результатов внедрения. Прежде всего представление уверенности заинтересованным сторонам надлежащего управления рисками с приемлемым уровнем.
Ключевые слова: *блок, свойство, отношение, структурный элемент, структура, система управления информационной безопасностью, диаграмма структуры, SysML.*

Tsurkan V. Method of information security management system structure synthesizing
Abstract. *The requirements, expectations, and related restrictions of interested parties are considered as input data for the specification of requirements for information security management systems. They are complemented with the establishment of internal and external factors that influence or can influence the activity of the organizations. According to the requirements specification, many interrelated functions with internal and external interfaces are defined. Each of them is decomposed according to the structural elements of information security management systems into the functions of subsystems, complexes, components. This shows the insufficiency of the definition of structural elements and their inherent functions. This is limited by the need to clarify the essence of information security management systems, taking into account the needs, goals, processes, structure of organizations. Therefore, they are considered as a set of subsystems, complexes, components, and relations between them. In general, this combination forms the structure of information security management systems. To represent it, diagrams in SysML graphic notation are used. Behind it, structural elements are reflected in blocks as modular units. Therefore, information security management systems are represented by a tree of modular units. Characteristics for them are determined by properties, among the properties stand out special classes - ports and restrictions. Their use allows to focus on the limitations and features of the interaction of blocks with each other. While the features of such interaction are taken into account by the types of relations. Therefore, by synthesizing the structure of information security management systems, its structural elements (subsystems, complexes, components) and the relationship between them are determined. Due to this, it is possible to set the properties of these systems regarding specific options for developing and demonstrating possible directions for achieving the goal. In particular, confidentiality, integrity and availability of information in organizations through risk assessment. This ensures that information security management systems achieve the planned implementation results. First of all, providing confidence to stakeholders to properly manage risks at an acceptable level.*
Keywords: *block, property, relationship, structural element, structure, information security management system, structure diagram, SysML.*

Цуркан Василь Васильович, кандидат технічних наук, доцент, старший науковий співробітник, Інститут проблем моделювання в енергетиці імені Г.Є. Пухова Національної академії наук України.
Цуркан Василий Васильевич, кандидат технических наук, доцент, старший научный сотрудник, Институт проблем моделирования в энергетике имени Г.Е. Пухова Национальной академии наук Украины.
Tsurkan Vasyl, candidate of technical sciences, associate professor, senior researcher, Pukhov Institute for Modeling in Energy Engineering of National Academy of Sciences of Ukraine.

Отримано *13 червня 2020 року*, затверджено редколегією *11 липня 2020 року*

125 Кібербезпека (1. Управління інформаційною безпекою; 2.Системи та технології кібербезпеки) *– приймаються особи з повною загальною середньою освітою та особи, які здобули освітньо-кваліфікаційний рівень молодшого спеціаліста (на 2-й курс за умови ліквідації академічної заборгованості). Зарахування проводиться за конкурсом – сертифікат УЦОЯО з таких дисциплін: 1) українська мова та література; 2) математика; 3) іноземна мова або фізика.*

та магістратури:

125 Кібербезпека (Адміністративний менеджмент у сфері захисту інформації)

124 Системний аналіз (Консолідована інформація)

Навчальний процес на кафедрі безпеки інформаційних технологій (БІТ) проходить у сучасних спеціалізованих навчальних та навчально-наукових лабораторіях, комп'ютерних класах та полігонах, де студенти отримують ґрунтовні знання з гуманітарних, соціально-економічних, математичних, природничо-наукових та професійних дисциплін. Протягом навчання ***студент оволодіє*** сучасними інформаційними технологіями, що дозволить йому досконало знати конструкцію та принципи функціонування і захисту сучасних комп'ютерів та операційних систем, організовувати захищений електронний документообіг, адмініструвати та захищати комп'ютерні мережі, проектувати комплексні системи захисту інформації та системи управління інформаційною безпекою тощо. ***Випускник кафедри БІТ*** здатний вирішувати завдання теоретичного та практичного характеру, що безпосередньо пов'язані з усіма без винятку аспектами захисту інформації. Випускники займають керівні посади у державних комітетах, службах та міністерствах, авіапідприємствах, банківських та ін. державних і недержавних установах. Крім того, кращі випускники можуть продовжити навчання в аспірантурі (докторантурі). Іногородні студенти на час навчання ***забезпечуються гуртожитками.***

Викладачі кафедри БІТ є досвідченими фахівцями у галузі інформаційної та авіаційної безпеки, вони набували досвіду в престижних навчальних закладах Європи та світу. Більшість викладачів є дійсними членами Міжнародної організації електротехніки та електроніки (IEEE), а їх висока кваліфікація підтверджена професійними сертифікатами та дипломами. Викладачі кафедри активно займаються науковою діяльністю і залучають студентів зокрема до участі у наукових конгресах, симпозіумах, конференціях та семінарах. З метою обміну досвідом та поглиблення освітнього рівня фахівців, ***кафедра тісно співпрацює*** з *СБУ, Державною службою спеціального зв'язку та захисту інформації України, Академією СБУ, Одеською національною академією зв'язку ім. О.С. Попова, Харківським національним університетом радіоелектроніки, Національним університетом «Львівська політехніка», Інститутом фізики НАН України, Інститутом проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, Інститутом кібернетики ім. В.М. Глушкова НАН України, Державним науково-дослідним інститутом спеціального зв'язку та захисту інформації, Вірменським державним інженерним університетом (м. Єреван, Вірменія), Казахським національним технічним університетом ім. К.І. Сатпаєва (м. Алмати, Казахстан), Центрально-азіатським університетом (м. Алмати, Казахстан), Університетом у Бельсько-Бялій (Польща), Державною вищою технічною школою у Новому Сончі (Польща), компаніями Аххоп Soft, SI BIS, D-Link, Сайфер, Криптон, Арт-мастер, Нові пошукові технології та ін*

НАУКОВЕ ВИДАННЯ

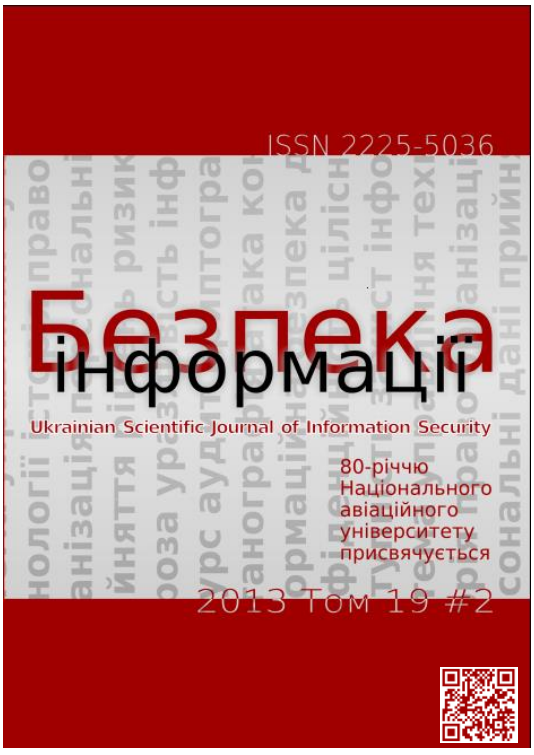
БЕЗПЕКА ІНФОРМАЦІЇ

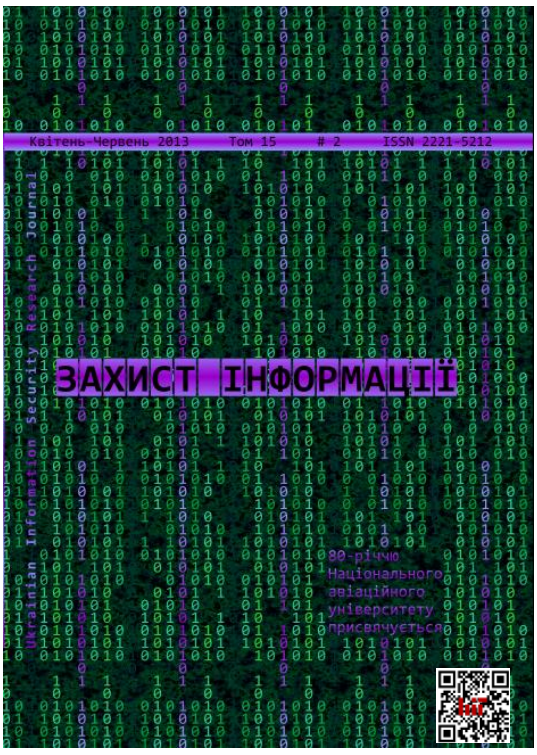
Ukrainian Scientific Journal of Information Security

Міжнародним центром ISSN (Париж, Франція) журналу присвоєно міжнародний стандартний номер для періодичних видань (International Standard Serial Number):
ISSN 2225-5036 (Print), ISSN 2411-071X (Online)
У міжнародний Реєстр ISSN журнал занесено під такими назвами:
Ключова назва (Key title): ***Bezpeka ìnformacìì***
Скорочена ключова назва (Abbreviated key title): ***Bezpeka ìnf.***

У авторській редакції
Комп'ютерне макетування: Людмила Павлівна РИБАЛКА
Дизайн обкладинки та логотипу: Кирило Петрович АНУФРІЄНКО

Підписано до друку 25.08.2020 р. Формат 60 × 84/8 Офс. друк Ум. друк. арк. 5,0. Обл. вид. арк. 5,4. Наклад 300 прим. Замовлення №_____ Віддруковано у типографії «Наш формат» 00105, м. Київ, пр. Миру 7.





Передплатний індекс та вартість річної підписки:

68979	**89539**
549 грн./рік	***732 грн./рік***
(виходить 3 рази на рік – у квітні, серпні та грудні)	*(виходить 4 рази на рік – у березні, червні, вересні та грудні)*