МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

**Петренко Тарас Анатолійович**

УДК 004.056.53 (043.3)

# МЕТОДИ ТА МОДЕЛІ ЕКСПЕРТНИХ СИСТЕМ РОЗПІЗНАВАННЯ КІБЕРАТАК НА ОСНОВІ КЛАСТЕРИЗАЦІЇ РЕАЛІЗАЦІЙ ОЗНАК

05.13.21 – Системи захисту інформації

**Автореферат**
дисертації на здобуття наукового ступеня
кандидата технічних наук

Київ – 2019

Робота виконана на кафедрі кібербезпеки та математичного моделювання Чернігівського національного технологічного університету Міністерства освіти і науки України.

Дисертацією є рукопис.

Науковий керівник: доктор технічних наук, професор
**Лахно Валерій Анатолійович**,
Національний університет біоресурсів і природокористування України, завідувач кафедри комп'ютерних систем і мереж.

Офіційні опоненти: доктор технічних наук, професор
**Грищук Руслан Валентинович,**
Житомирський військовий інститут ім. С.П. Корольова, начальник кафедри захисту інформації та кібербезпеки;

кандидат технічних наук, доцент
**Іванченко Євгенія Вікторівна,**
Національний авіаційний університет,
професор кафедри безпеки інформаційних технологій.

Захист відбудеться «02» липня 2019 р. о $16^{00}$ годині на засіданні спеціалізованої вченої ради Д 26.062.17 при Національному авіаційному університеті за адресою: 03058, м. Київ, просп. Космонавта Комарова, 1, ауд. 11-111.

З дисертацією можна ознайомитись у науково-технічній бібліотеці Національного авіаційного університету за адресою: 03058, м. Київ, просп. Космонавта Комарова, 1.

Автореферат розісланий «31» травня 2019 р.

Учений секретар спеціалізованої вченої ради, д.т.н, доцент Гнатюк С.О.

# ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

**Актуальність теми.** Останні десятиліття характеризуються швидким зростанням і розвитком комп'ютерних мереж та систем, з метою забезпечення кібербезпеки яких розроблено безліч систем, що використовують різні техніки опрацювання даних для виявлення нелегітимної діяльності. Більшість класичних систем виявлення кібератак характеризуються рядом недоліків (недостатня масштабованість, відсутність гнучкості тощо), що накладає додаткові обмеження на області їх застосування. Як показує досвід останніх років, кіберзлочинці все частіше використовують унікальні, ще не відомі IT-індустрії шкідливі програми, уразливості та способи кібератак.

Активне розширення інформаційно-комунікаційного середовища (ІКС) та критично-важливих інформаційних систем (КВІС) у багатьох державах світу, супроводжується виникненням нових загроз для кібербезпеки (КБ), про що свідчить зростання кількості інцидентів, пов’язаних із захистом інформації, а також виявлених уразливостей у КВІС. Зростання інтересу до проблематики КБ та інформаційної безпеки (ІБ), викликало за останнє десятиліття сплеск досліджень в області розроблення ефективних систем виявлення й запобігання кіберзагрозам.

Проблеми, пов'язані із захистом інформації й забезпеченням ІБ та кібербезпеки, успішно вирішують провідні вітчизняні й закордонні вчені: Блінцов В.С., Гайкович В.Ю., Герасименко В.А., Глова В.І., Грищук Р.В., Дудикевич В.Б., Клейменов С.А., Котенко В.І., Касперський К., Ахмад Д.М., Atighetchi M., Campbell R. H., Chapman C., Chi S.-D., Chien E., Dawkins J., Endler M., Erickson J., Halpin M., Hariri S., Jha S., Kaiser G., Kemmerer R., Kim P., Misra V., Nieh J., Silva F., Stolfo S. та ін.

Протистояти постійному зростанню кількості й складності деструктивних впливів на КВІС можна, зокрема, й використовуючи інтелектуальні системи розпізнавання кіберзагроз (СІРКЗ).

Отже, дослідження, спрямовані на подальший розвиток моделей та методів кіберзахисту на основі застосування, здатних до самонавчання систем інтелектуального розпізнавання кібератак, є актуальними.

**Зв’язок роботи з науковими програмами, планами, темами.** Розробка основних положень дослідження здійснювалася відповідно до планів НДР і договорів, що виконуються протягом 2015-2018 рр. у Чернігівському національному технологічному університеті, Приватному вищому навчальному закладі “Європейський університет”: 1) НДР “Методи та засоби забезпечення безпеки ресурсів інформаційних систем” (№ держ. реєстрації 0117U003187); 2) НДР “Інформаційне та програмне забезпечення, математичне моделювання складних систем” (№ держ. реєстрації 0114U005430). При виконанні робіт дисертант брав участь у розробці методів забезпечення ІБ і математичних моделей СЗІ, як виконавець окремих розділів.

**Мета дослідження** – підвищення ефективності систем інтелектуального розпізнавання кібератак для КВІС на основі створення здатної до самонавчання експертної системи (ЕС), яка враховує відомі статистичні параметри кластеризації реалізацій ознак кібератак, як об’єкта спостереження.

Для досягнення поставленої мети необхідно розв'язати *такі задачі:*

1) проаналізувати методи які використовуються для побудови систем інтелектуального розпізнавання кібератак в умовах зростання кількості та складності цільових атак, які характеризуються реалізаціями ознак, які важко пояснити, а також ураховують відомі статистичні параметри кластеризації реалізацій ознак кібератак;

2) розробити модель експертної системи та метод її навчання із використанням процедури нечіткої кластеризації реалізацій ознак кібератак та можливістю корекції вирішальних правил, що дозволить створювати адаптивні механізми самонавчання систем кіберзахисту;

3) удосконалити методи навчання експертної системи та визначити раціональну кількість кластерів у просторі реалізацій ознак кібератак, що дозволить зменшити час навчання;

4) розробити експертну систему розпізнавання кібератак (об’єктів розпізнавання – ОР), яка у взаємодії із іншими системами кіберзахисту дозволить підвищити рівень розпізнавання складних цільових кібератак із важко пояснюваними реалізаціями ознак;

5) провести імітаційні дослідження та натурну апробацію моделі експертної системи.

**Об’єкт дослідження:** процеси розпізнавання кібератак у критично важливих інформаційних системах.

**Предмет дослідження:** методи та моделі здатних до самонавчання експертних систем у складі комплексів виявлення вторгнень у критично важливих інформаційних системах.

**Методи дослідження:** у процесі дослідження, враховуючи особливості предметної галузі та сформульованих задач, використано: методи теорії захисту інформації та кластерного аналізу (для побудови алгоритму розбиття простору реалізацій ознак на кластери); методи прикладної статистики, оптимізації та комп'ютерного моделювання (для імітаційного моделювання); моделі інтелектуальних технологій машинного навчання (МНав) та теорію нечітких множин (для побудови моделі оціночного показника ефективності навчання та процедури нечіткої кластеризації реалізацій ознак розпізнавання у ЕС), принципи й методи об'єктно-орієнтованого програмування для створення ЕС у складі СІРКЗ; методологію тесту на проникнення (для експериментальної перевірки розроблених моделей).

**Наукова новизна одержаних результатів.** У межах виконаних досліджень отримані такі наукові результати:

*1. Уперше:*

– розроблено модель експертної системи у складі інтелектуальних систем виявлення вторгнень, у якій, на відміну від існуючих, застосовується процедура нечіткої кластеризації реалізацій ознак кібератак та наступна корекція вирішальних правил, що дозволяє створювати адаптивні механізми самонавчання систем інтелектуального розпізнавання кібератак;

– запропоновано застосовувати в якості оціночного показника ефективності навчання експертної системи модифіковану інформаційну умову функціональної результативності, яка ґрунтується на ентропійному та інформаційно-дистанційному

критерії Кульбака – Лейблера, та, на відміну від існуючих, дозволяє отримувати вхідну навчальну матрицю, яка використовується як об'єкт навчання, й будувати коректні вирішальні правила розпізнавання кібератак на критично важливі інформаційні системи.

*2. Удосконалено:*

– метод розбиття простору реалізацій ознак на кластери в ході реалізації процедури розпізнавання кібератак, який відрізняється від існуючих, одночасною оптимізацією при обчисленні контрольних допусків у ході аналізу експертною системою важко пояснюваних реалізацій ознак об'єктів спостереження, та дозволяє на кожному кроці навчання змінювати перевірочні допустимі відхилення для всіх реалізацій ознак кібератак одночасно;

– метод навчання експертної системи, який являє собою ітераційну процедуру пошуку глобального максимуму інформаційної умови функціональної результативності, та, на відміну від існуючих, дозволяє попереджати можливі випадки поглинання одним класом об'єктів розпізнавання базових реалізацій ознак іншого класу, враховує відомі статистичні параметри кластеризації реалізацій ознак об'єктів спостереження, а також помилки під час завдання на прийняття рішення в ході процедур машинного навчання.

*3. Набули подальшого розвитку:*

– імітаційні моделі для композитної побудови систем інтелектуального виявлення кібератак за рахунок одночасної оптимізації контрольних допусків в ході аналізу об'єктів розпізнавання, що дозволяє проводити їх дослідження, здійснювати вибір раціональних способів протидії і нейтралізації наслідків, аналізувати більш складні і раніше невідомі види кібератак на критично важливі інформаційні системи.

**Практична значимість наукових результатів.**

1. Запропоновані в дисертації моделі та методи, у рамках розробленої ЕС з розпізнавання кібератак, доведені до практичної реалізації шляхом імплементації програмних модулів в MatLAB та Delphi, що дозволяє підвищити ефективність розпізнавання, залежно від класу кібератак, до 70–99 %, та на 15–20 % зменшити час налагодження проектів СЗІ КВІС (КВКС) за рахунок імітаційного моделювання кібератак.

2. Запропоновані в дисертації модель та метод, доведені до практичної реалізації шляхом створення відповідних програмних модулів здатної до самонавчання експертної системи «Analyzer of cyberthreats» («Аналізатор загроз»), що дозволяє враховувати відомі статистичні параметри кластеризації реалізацій ознак об'єктів розпізнавання, а також помилки під час завдання на прийняття рішення під час машинного навчання. Запропонована ЕС дозволяє підвищити результативність СІРКЗ, які працюють у складі СЗІ КВІС (КВКС) до 98 %. ЕС «Analyzer of cyberthreats» впроваджена в ТОВ «Захист інформації» (акт № 134 від 16.11.2018 р.).

3. Запропоновані програмні продукти можуть бути використані для забезпечення кіберзахисту державних КВІС, модернізації існуючих СІРКЗ.

4. Результати досліджень впроваджено в навчальний процес у Чернігівському національному технологічному університеті (акт № 9 від 5.09.2018 р.) та Національному авіаційному університеті (акт від 3.09.2018 р.).

*Достовірність і обґрунтованість наукових результатів підтверджується*: математичною адекватністю розробленої моделі ЕС; теоретичною та практичною верифікацією методів навчання ЕС; практичним впровадженням ЕС для інтелектуального розпізнавання кібератак на КВІС; збігом результатів імітаційного моделювання процедури розпізнавання кібератак і тестів на проникнення у КВІС.

**Особистий внесок здобувача.** Усі основні результати одержані здобувачем особисто. У роботах, опублікованих із співавторами, здобувачу належать: [6, 11] – аналіз загроз інформаційної безпеки бездротових мереж, [4, 10, 12, 13] – категорійна модель адаптивної системи розпізнавання кібератак; [5, 15] – модель та метод навчання адаптивної системи розпізнавання кібератак; [1] – структурна схема адаптивної експертної системи, категорійна модель для визначення інформаційного критерію функціональної результативності навчання експертної системи; [2, 14] – модель адаптивної системи розпізнавання, модифікована інформаційна умова функціональної результативності навчання експертної системи; [8, 9] – складові процесу управління інформаційною безпекою.

**Апробація результатів дисертації.** Основні результати роботи були представлені та обговорені на таких конференціях: 1) Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених «Новітні технології у науковій діяльності і навчальному процесі», м. Чернігів, 23-24 квітня 2014 р. та 28 квітня 2015р.; 2) VII Всеукраїнська науково-практична конференція «Стан та удосконалення безпеки інформаційно-комунікаційних систем «SITS-2015», м. Миколаїв, м. Коблево, 9-12 червня 2015 р.; 3) Науково-практична конференція «Безпека українського суспільства в концепції вступу в постіндустріальне суспільство ЄС», м. Київ, 16 грудня 2015р.; 4) II Міжнародної науково-практичної конференції «Актуальні питання забезпечення кібербезпеки та захисту інформації», с. Верхнє Студене, 24-27 лютого 2016 р.; 5) II міжнародна науково-практична конференція «Актуальні проблеми моделювання ризиків і загроз виникнення надзвичайних ситуацій на об'єктах критичної інфраструктури» м. Київ, 26-28 травня 2016р.; 6) The seventh world congress “Aviation in the XXI-st century” Safety in Aviation and Space Technologies, Kyiv, September 19-21 2016; 7) VII міжнародна науково-практична конференція «Комплексне забезпечення якості технологічних процесів та систем (КЗЯТПС – 2017», м. Чернігів, 24–27 квітня 2017р.; 8) VII міжнародна науково-технічна конференція «ITSEC: Безпека інформаційних технологій», м. Київ, 16-18 травня 2017 р.

**Публікації.** За результатами дослідження опубліковано 16 наукових праць в яких повністю відображені основні результати дисертації (з них 3 одноосібно). В їх число входять 2 статті що входять до наукометричної бази Scopus [1, 2], 1 стаття у наукових періодичних виданнях інших держав [3], 3 статті у фахових виданнях України [4-6] а також 10 матеріалів і тез доповідей на всеукраїнських та міжнародних конференціях [7-16].

**Структура і обсяг роботи.** Дисертація складається з анотації, вступу, чотирьох розділів, висновків, викладена на 240 сторінках друкованого тексту, в т. ч. основний текст на 167 сторінках, містить 49 рисунків, 24 таблиці, перелік цитованої літератури з 211 найменувань і 2-х додатків.

## ОСНОВНИЙ ЗМІСТ РОБОТИ

У **вступі** висвітлено актуальність теми дисертаційного дослідження, сформульовані мета і задачі, наукова новизна отриманих результатів та їх практична цінність, а також відомості про апробацію результатів роботи.

У **першому** розділі виконано огляд та аналіз попередніх досліджень у сфері вирішення завдань захисту КВІС та КВКС, підвищення стійкості інформаційно-обчислювальних процесів, схоронності й захищеності інформації. З'ясовано, що складність застосування до інтелектуальних систем розпізнавання цільових кібератак формалізованого апарату аналізу й синтезу СІРКЗ, полягає в тому, що конкретний інформаційний комплекс КВІС або КВКС та їх підсистеми ІБ складаються з різнорідних елементів, які описуються із використанням різних моделей. Показано, що застосування елементів адаптивного захисту інформації може бути засноване на використанні новітніх методів інтелектуального розпізнавання кібератак на КВІС.

На підставі аналізу стану ІБ КВІС та КВКС України формалізовано загальну наукову задачу досліджень, спрямованих на подальший розвиток моделей та методів захисту на основі інтелектуального розпізнавання кібератак в умовах збільшення кількості та складності дестабілізуючих впливів, формалізована мета роботи і групи задач, що її вирішують.

У **другому** розділі запропоновано структурну схему та подано модель здатної до самонавчання експертної системи із розпізнавання кібератак.

Вхідний нечіткий розподіл реалізацій об'єктів, які використовуються під час навчання (багатовимірні навчальні матриці реалізацій ознак кібератак), трансформується в чіткий розподіл під час оптимізації перевірочних допустимих відхилень на кожен клас кібератак. У результаті відбувається цілеспрямована зміна значень реалізацій ознак розпізнавання в ЕС для визначених об'єктів та побудова коректних вирішальних правил за багатомірною бінарною навчальною матрицею (ББНМ). Це дає змогу в межах ІІТ поєднати процес коригування об'єктів, які використовуються для навчання (ОВН), й безпосередній етап навчання. Під час останнього етапу відбувається синтез вирішальних правил.

Розв'язання завдання по формуванню вхідного математичного опису ЕС у складі СІРКЗ, полягає у створенні об'єкту, який використовується для навчання – ОВН (тобто багатовимірної навчальної матриці реалізацій ознак) – $\left\| lm_{m,i}^{(j)} \mid m=\overline{1,M}; i=\overline{1,N}, j=\overline{1,n} \right\|$. Для цього сформульовано словник реалізацій ознак для кожного класу кібератак, а також алфавіт класів у термінах об'єктів розпізнавання; визначено мінімальний обсяг репрезентативної навчальної матриці (ОВН); визначено граничні допустимі відхилення для реалізацій ознак розпізнавання нелегітимного втручання в роботу КВІС.

Алфавіт класів кібератак (об'єктів розпізнавання – ОР) для ЕС $\{lm_m^o\}$ формується на першому етапі розробником системи із залученням фахівців із ІБ. На другому етапі синтезу алфавіту, за допомогою ЕС, продовжується опрацювання вхідних даних із застосуванням методів кластеризації.

Формальна постановка задачі кластеризації кібератак на КВКС: потрібно розбити вибірку, що складається з реалізацій ознак різних класів кібератак (мережевих, вірусних, таргетованих, ін'єкція коду та ін.) на непересічні підмножини. Причому необхідно, щоб кожен кластер складався з об'єктів, близьких за метрикою (функція кодової відстані між об'єктами), а об'єкти різних кластерів істотно відрізнялися.

Прийнято, що відомі алфавіт класів $\left\{CT_m^o \mid m=\overline{1,M}\right\}$ й ББНМ ОР (тип "об'єкт–властивість"), яка, відповідно, описує $m$-й стан, у якому перебуває система. При цьому, ББНМ ОР для класу розпізнавання $CT_m^o$, матиме такий вигляд:

$$\left\|lm_{m,i}^{(j)}\right\| = \begin{vmatrix} lm_{m,1}^{(1)} & lm_{m,2}^{(1)} & \cdots & lm_{m,k}^{(1)} & \cdots & lm_{m,N}^{(1)} \\ lm_{m,1}^{(2)} & lm_{m,2}^{(2)} & \cdots & lm_{m,k}^{(2)} & \cdots & lm_{m,N}^{(2)} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ lm_{m,1}^{(j)} & lm_{m,2}^{(j)} & \cdots & lm_{m,k}^{(j)} & \cdots & lm_{m,N}^{(j)} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ lm_{m,1}^{(n)} & lm_{m,2}^{(n)} & \cdots & lm_{m,k}^{(n)} & \cdots & lm_{m,N}^{(n)} \end{vmatrix}. \quad (1)$$

У матриці (1) прийнято такі позначення: рядок матриці – реалізація "подання" ОР $\left\{lm_{m,i}^{(j)} \mid i=\overline{1,N}\right\}$, $N$ – кількість ознак ОР; стовпчик – стохастична навчальна вибірка $\left\{lm_{m,i}^{(j)} \mid j=\overline{1,n}\right\}$ з обсягом $n$. Усі можливі значення кожної властивості ОР запропоновано кодувати у бінарній формі, де нуль відповідає невизначеному значенню властивості ОР. Об'єднуючи дані отримані в процесі попереднього моніторингу, в кластери, можна проводити аналіз типових представників кожного кластера й приймати рішення про те, чи є такі дані ознакою атаки чи ні. Потім це рішення переноситься на всіх представників досліджуваного кластера. Такий підхід суттєво скорочує обсяги необхідної для успішної класифікації атаки інформації (ОВН). ІУФР здатної до самонавчання ЕС з КБ подано так:

$$CE_m^* = \max_{IS} CE_m,, \quad (2)$$

де $CE_m$ – ІУФР процедури машинного навчання ЕС в ході розпізнавання класу ОР $CT_m^0$; $IS$ – допустимі значення параметрів КВКС.

Під час навчання ЕС та формування бази знань (БЗ) роботу системи регламентує фахівець з ІБ, який згідно з рекомендаціями ЕС формує керуючі команди – $\left\{CC\{hy_m\} \mid m=\overline{1,M}\right\}$. Для розробленої ЕС у складі СІРКЗ в якості інформаційних мір обґрунтовано застосування ентропійної міри та критерія Кульбака – Лейблера. Величину нормованої ентропійної ІУФР, враховуючи апріорну ймовірність схвалення гіпотези для розпізнавання ОР, можна подати таким чином

$$IND = 1 + \sum_{l=1}^{2}\sum_{m=1}^{2} HL \cdot \log_2 HL \Big/ 2, \qquad (3)$$

де $HL = p\left(hy_m / hy_l\right)\, p\left(hy_l\right)$ – апріорна ймовірність схвалення припущення (гіпотези) $hy_l$; $p\left(hy_m / hy_l\right)$ – апостеріорна ймовірність схвалення припущення $hy_m$ за умови, що була прийнята гіпотеза $hy_l$; $M = 2$ – кількість розглянутих припущень у процесі розпізнавання кібератаки.

Виходячи із завдання програмної реалізації експертної системи та парадигми ООП, клас ОР мусить відповідати таким основним вимогам: клас повинен служити контейнером для об'єктів; контейнер кластера (КК) має бути динамічно розширюваним та допускати типізування.

З урахуванням (2) та (3) нормована ентропійна ІУФР навчання, яка враховує помилки 1-го та 2-го роду, а також помилки під час завдань на прийняття рішення під час МНав ЕС, виглядає таким чином

$$CE_m^{(ls)} = 1 + \frac{\left(\begin{array}{l} HM1 \cdot \log_2 HM1 + HM2 \cdot \log_2 HM2 + HM3 \cdot \log_2 HM3 + \\ + HM4 \cdot \log_2 HM4 + HM5 \cdot \log_2 HM5 + HM6 \cdot \log_2 HM6 \end{array}\right)}{2}, \qquad (4)$$

де $HM1 = mis1_m^{(ls)}(cr) \Big/ \left(mis1_m^{(ls)}(cr) + AU_{2,m}^{(ls)}(cr)\right)$,

$HM2 = mis2_m^{(ls)}(cr) \Big/ \left(AU_{1,m}^{(ls)}(cr) + mis2_m^{(ls)}(cr)\right)$;

$HM3 = AU_{1,m}(cr) \Big/ \left(AU_{1,m}^{(ls)}(cr) + mis2_m^{(ls)}(cr)\right)$,

$HM4 = AU_{2,m}^{(ls)}(cr) \Big/ \left(mis1_m^{(ls)}(cr) + AU_{2,m}^{(ls)}(cr)\right)$;

$HM5 = mis1_m^{(ls)}(cr) \Big/ \left(mis1_m^{(ls)}(cr) + AU_{3,m}^{(ls)}(cr)\right)$;

$HM6 = AU_{3,m}^{(ls)}(cr) \Big/ \left(mis3_m^{(ls)}(cr) + AU_{3,m}^{(ls)}(cr)\right)$; $AU_{1,m}^{(ls)}(cr)$ – процедура першої валідації; $AU_{2,m}^{(ls)}(cr)$ – процедура другої валідації; $mis1_m^{(ls)}(cr)$ – помилки першого роду прийняття рішення для $ls - го$ кроку навчання ЕС; $mis2_m^{(ls)}(cr)$ – помилки другого роду прийняття рішення для $ls - го$ кроку навчання ЕС; $mis3_m^{(ls)}(cr)$ – помилки під час завдання на прийняття рішення в ході процедур МНав ЕС; $cr$ – радіус КК.

Забезпечення стійкого функціонування та надійного опрацювання даних про стан ІБ КВКС в довільний момент часу в умовах впливу кібератак досягається реалізацією відображення

$$SO : SS \times CA \to SS_{res} = \left\{SS_{res}^{\,i}\right\}, \qquad (5)$$

де $SS_{res}$ – множина дозволених станів КВКС; $CA = \left\{CA_0, CA_1, ..., CA_N\right\}$ – множина реалізації кібератак.

Функціонал, що визначає узагальнений показник ефективності протидії кібератакам, враховує показник ефективності розпізнавання, а також характеризує стійкість функціонування КВКС. З урахуванням зазначеного, його подано виразом

$$IE = F\left[(SCA, CE), (SS, T_s, VIL), (CO, CM, ME\right], \quad (6)$$

де $SCA$ – сценарії кібератак; $CE$ – критерій ефективності розпізнавання ОР; $SS$ – множина параметрів КС: $T_s$ – періоди часу виконання функціональних завдань у КС; $VIL$ – уразливості КС; множина параметрів протидії кібератакам: $CO$ – параметри регулювання КС; $CM$ – методи протидії кібератакам у КС; $ME$ – засоби попередження, виявлення, аналізу та активної протидії кібератакам.

У розділі визначено залежність інформаційної міри Кульбака – Лейблера від параметрів ЕС для варіанту застосування керуючих команд, які ґрунтуються на трьох альтернативах: перша – основна робоча гіпотеза (базова) – $hy_{\gamma_1}$: реалізація ознаки $rc_i$ ОР ($RS$) та показник $IE$ знаходиться у межах звичайного стану КВІС; друга – гіпотеза $hy_{\gamma_2}$: реалізація ознаки $rc_i$ ОР ($RS$) та показник $IE$ дозволяють зробити висновок, що значення показника $IE$ є меншими на норму; третя – гіпотеза $hy_{\gamma_3}$: показник $IE$ дозволяють зробити висновок, що значення показника $IE$ є більшими за норму.

Для прийнятих гіпотез отримано такий результат

$$CE_m^{(ls)} = \begin{Bmatrix} \left[AU_{1,m}^{(ls)} + AU_{2,m}^{(ls)} + AU_{3,m}^{(ls)}\right] - \\ -\left[mis1_m^{(ls)} + mis2_m^{(ls)} + mis3_m^{(ls)}\right] \end{Bmatrix} \cdot \log_2 \frac{AU_{1,m}^{(ls)} + AU_{2,m}^{(ls)} + AU_{3,m}^{(ls)}}{AU_{1,m}^{(ls)} + AU_{2,m}^{(ls)} + AU_{3,m}^{(ls)}} \Big/ 3. \quad (7)$$

де $AU_{1,m}^{(ls)} = p\left(hy_{\gamma_1} / hy_{\mu_1}\right)$ – перша валідація гіпотези базується на висновках; $AU_{2,m}^{(ls)} = p\left(hy_{\gamma_2} / hy_{\mu_2}\right)$ – друга валідація гіпотези базується на порівнянні відхилень від $\left\{ca_{K,i}^*\right\}$; $AU_{3,m}^{(ls)} = p\left(hy_{\gamma_3} / hy_{\mu_3}\right)$ – третя валідація гіпотези базується на результатах опрацювання предикатного вигляду обчислення кількості епізодів, коли встановлено, що реалізація атаки не належить до КК $C_{1,m}^o$ якщо дійсно $\left\{ct_1^{(j)}\right\} \in CT_1^o$ та кількість епізодів, коли встановлено, що реалізації атаки належать до КК $C_{1,m}^o$, якщо вони насправді належать класу $CT_2^o$; $mis1_{1,m}^{(ls)} = p\left(hy_{\gamma_2} / hy_{\mu_1}\right)$ та $mis1_{2,m}^{(ls)} = p\left(hy_{\gamma_3} / hy_{\mu_1}\right)$ – кількість помилкових спрацювань ЕС в процесі виявлення кібератак, відповідно; $mis1_{2,m}^{(ls)} = p\left(hy_{\gamma_3} / hy_{\mu_1}\right)$ та $mis2_{1,m}^{(ls)} = p\left(hy_{\gamma_1} / hy_{\mu_2}\right)$ – кількість невиявлених у ході роботи ЕС кібератак, відповідно; $mis3_{1,m}^{(ls)} = p\left(hy_{\gamma_1} / hy_{\mu_3}\right)$ та $mis3_{2,m}^{(ls)} = p\left(hy_{\gamma_2} / hy_{\mu_3}\right)$ – помилки під час завдання на прийняття рішення в ході процедур МНав, які виникають у тому разі, коли модель не враховує деякі алгоритми навчання (МІТН) ЕС; $hy_{\mu_1}$ – значення реалізації ознаки належить полю допустимих відхилень (ПДВ) $ca$, $hy_{\mu_2}$ – значення реалізації ознаки знаходиться лівіше за ПДВ; $hy_{\mu_3}$ – значення реалізації ознаки знаходиться правіше за ПДВ.

Вираз (7) враховує модифіковані ентропійний критерій та міру Кульбака – Лейблера. Він є функціоналом від характеристик рішень, які приймаються під час розпізнавання відповідних кібератак на КВКС.

Тестування ЕС із визначенням належності реалізації класу $CT_m^o$ до ОР здійснюється за таким вирішальним правилом:

$$if\left(1-\frac{\sum\limits_{1}^{N}\left(\mathrm{cov}_{m,i}\oplus\mathrm{cov}_{e,i}\right)}{cr_{1,m}^{*}}\geq 0\right)\ then\ hy_m=1-\frac{\sum\limits_{i=1}^{N}\left[\left(\mathrm{cov}_{m,i}\oplus\mathrm{cov}_{e,i}\right)\cdot cop_{m,i}^{*}\right]}{cr_{2,m}^{*}},\qquad(8)$$

де $\mathrm{cov}_{e,i}-$значення $i-й$ координати отриманої під час тестування; $cr_{1,m}^{*}-$ оптимальний радіус КК ОВН для $CT_m^o$; $cop_{m,i}^{*}-i-me$ значення координати вектора, який є ортогональним вісі, що проходить через вершину еталонного $CT_m$; $cr_{2,m}^{*}-$ оптимальний радіус КК для $CT_m^o$, що підлягає розпізнаванню;

За допомогою такого виразу визначається можливість віднесення вектору параметрів реалізації відомих або невідомих сценаріїв кібератак $SCA_m^{CT}$ для $m$-го об'єкту та $ct$-го класу до одного з відомих класів ОР $RS_{m_j}^{CT}$ на $j$-му кроці роботи засобів кіберзахисту

$$P\left(RS_{m_i}^{CT}\right)\cdot P\left(SCA_m^{CT}\Big/RS_{m_i}^{CT}\right)\geq P\left(RS_{m_k}^{CT}\right)\cdot P\left(\overline{SCA_m^{CT}}\Big/RS_{m_k}^{CT}\right),$$

де $P\left(RS_{m_i}^{CT}\right)$ – ймовірність віднесення ЕС ОР до класу відомих $RS_{m_i}^{CT}$; $P\left(\overline{SCA_m^{CT}}/RS_{m_i}^{CT}\right)$ – щільність умовної ймовірності віднесення ЕС виявленого ОР до відомого класу $RS_{m_i}^{CT}$; $P\left(RS_{m_k}^{CT}\right)$ – ймовірність віднесення ЕС ОР до класу невідомих ОР $RS_{m_k}^{CT}$; $P\left(\overline{SCA_m^{CT}}/RS_{m_k}^{CT}\right)$ – щільність умовної ймовірності віднесення ЕС виявленого ОР до невідомого класу $RS_{m_k}^{CT}$.

На основі критерію Байеса визначено середню “ціну” ризику прийняття у ЕС рішення щодо віднесення вектору параметрів невідомих ОР до класу $RS_{m_k}^{CT}$

$$PR\left(RUL_i/\overline{SCA_m^{CT}}\right)=\sum_{j=1}^{\gamma}np\left(\frac{RUL_i}{RS_{m_k}^{CT}}\right)\cdot P\frac{RS_{m_k}^{CT}}{\overline{SCA_m^{CT}}},\qquad(9)$$

де $RUL_i$ – вирішальне правило, за яким бінарний навчальний вектор (БНВ) ОР $\overline{SCA_m^{CT}}$ визначає приналежність об’єкту до $RS_{m_k}^{CT}$; $np\left(RUL_i/RS_{m_k}^{CT}\right)$ – умовна «ціна» прийняття ЕС рішення $RUL_i$; $P\left(RS_{m_k}^{CT}/\overline{SCA_m^{CT}}\right)$ – умовна ймовірність того, що $\overline{SCA_m^{CT}}$ віднесений ЕС до класу $RS_{m_k}^{CT}$.

Для випадку коли ЕС виконує порівняльний аналіз двох БНМ, вирішальне правило із використанням критерію Байєса подано так

$$\left(P\left(\overline{SCA_m^{CT}}\Big/RS_{m_1}^{CT}\right)\right)\Big/\left(P\left(\overline{SCA_m^{CT}}\Big/RS_{m_2}^{CT}\right)\right)\geq\left(P(RS_{m_2}^{CT})\right)\Big/\left(P(RS_{m_1}^{CT})\right). \quad (10)$$

Пошук глобального екстремуму, доповнений оцінкою на основі критерію Байєса, дозволяє уникнути локального максимуму і зациклення алгоритму навчання системи.

Запропонована модель, на відміну від відомих, враховує відомі статистичні критерії оптимізації процедури кластеризації реалізацій ознак ОР на попередньому етапі функціонування здатних навчатися ЕС у складі СІРКЗ.

**У третьому** розділі запропоновано метод навчання ЕС у складі СІРКЗ, який дозволяє підвищити результативність кластеризації реалізацій ознак при виявленні складних кібератак, а також виконано імітаційне моделювання модулів ЕС з метою перевірки запропонованих методів та моделей.

На першому етапі процедуру розбиття простору реалізацій ознак (ПОЗ) та наступної кластеризації, для будь-якого класу ОР $CT_m^o$, запропоновано здійснювати шляхом перетворення ПОЗ у гіперсферичну форму. Оскільки основним етапом кластеризації під час розбиття ПОЗ на групи є збільшення радіусу ($cr_m$) КК на кожному кроці навчання, то для цього використано рекурентний вираз

$$cr_m(ls)=\left[cr_m(ls-1)+\xi \mid cr_m(ls)\in IS_m^{cr}\right], \quad (11)$$

де $ls$ – кількість кроків збільшення радіуса КК $C_m^o$; $\xi$ – прийняті для вибраних реалізацій ознак кількість кроків збільшення КК; $IS_m^{cr}$ –допустима величина радіуса КК.

Метод навчання ЕС у складі СІРКЗ являє собою ітераційну процедуру пошуку глобального ІУФР у допустимому діапазоні визначення його функції

$$ca^*=\arg\max_{IS_{ca}}\{\max_{IS_{CE}\cap IS_{cr}}\overline{CE}\}, \quad (12)$$

де $IS_{ca}$ – допустимий діапазон величин контрольних відхилень $ca$ для класу ОР $\left\{CT_m^o\right\}$; $IS_{CE}$ – робочий діапазон визначення ІУФР $\overline{CE}$; $IS_{cr}$ – допустимий діапазон величини $cr$.

На другому етапі реалізації методу, перевіряється можливість корекції вирішальних правил, що дозволило створити адаптивний механізм самонавчання системи розпізнавання кібератак. При цьому використано такі обмеження

$$\left(\forall\, CT_{m,\xi}^{o}\in RC^{|M|}\right)\left\lfloor CT_{m,\xi}^{o}\neq\varnothing,\ m=\overline{1,M}\right\rfloor, \quad (13)$$

$$\left(\forall CT^{o}_{m,\xi} \in RC^{|M|}\right)\left(\forall CT^{o}_{c,\xi} \in RC^{|M|}\right)\begin{bmatrix} CT^{o}_{m,\xi} \neq \\ \neq CT^{o}_{c,\xi} \rightarrow BCT^{o}_{m,\xi} \cap BCT^{o}_{c,\xi} = \varnothing \end{bmatrix}, \quad (14)$$

$$\left(\forall CT^{o}_{m,\xi} \in RC^{|M|}\right)\left(\forall CT^{o}_{c,\xi} \in RC^{|O|}\right)\begin{bmatrix} CT^{o}_{m,\xi} \neq CT^{o}_{c/\xi} \rightarrow \\ \rightarrow \left(cr'_{m,\xi} < cr\left(ct_{m,\xi} \oplus ct_{c,\xi}\right)\right) \wedge \\ \wedge \left(cr'_{c,\xi} < cr\left(ct_{m,\xi} \oplus ct_{c,h}\right)\right) \end{bmatrix}, \quad (15)$$

$$\bigcup_{CT^{o}_{m,\xi} \in RC} CT^{o}_{m,\xi} \subseteq RS, \quad (16)$$

де $B\,CT^{o}_{m,\xi}$, $B\,CT^{o}_{c,\xi}$ – центри двох найближчих (сусідніх) кластерів $CT^{o}_{m,\xi}$ та $CT^{o}_{c,\xi}$, відповідно; $\xi$ – крок збільшення радіуса КК; $cr'_{m,\xi}$, $cr'_{c,\xi}$ відповідно, оптимізовані радіуси КК $CT^{o}_{m,\xi}$та $CT^{o}_{c,\xi}$; $cr\left(ct_m \oplus ct_c\right)$ – міжцентрова кодова відстань кластерів $CT^{o}_{m,\xi}$ та $CT^{o}_{c,\xi}$.

Для оцінювання оптимальності ЕС у складі СІРКЗ, застосовано метод Парето. Ступінь приналежності найкращого, з точки зору ЕС або експерта, варіанта Парето оптимального рішення щодо обраних стратегій, визначається за формулою

$$\max\left[\sum_{j=1}^{h}\sum_{l=1}^{d}\widetilde{z}_{ij} \otimes \widetilde{p}_j \otimes \widetilde{p}_l^{SS}\right] = \max_{W_i \in W} CE(W_i(x)), \quad (17)$$

де $\otimes$ – триангулярна норма (Т–норма); $W_i(x)$ – остаточний вибір варіанта рішення ЕС (або експерта); $\widetilde{z}_{ij}$ – нечітка оцінка корисності *i*-го варіанта вирішення завдання розпізнавання ОР ЕС; $\widetilde{p}_j$ – оцінка станів КВІС у процесі розпізнавання ОР; $\widetilde{p}_l^{SS}$ – оцінки станів ЕС у процесі розпізнавання.

Визначення ступеня приналежності найкращого варіанту Парето оптимального нечіткого рішення для формування БЗ для ЕС виконано із застосуванням модифікованого критерію Вальда і критерію Севіджа.

У розділі представлені результати імітаційного моделювання (ІМ) з визначення залежності ІУФР навчання ЕС. Усереднене значення оптимального радіуса *cr* дорівнює у кодових одиницях для класів ОР, поданих у таблиці 1.

Таблиця 1

*Значення оптимального радіуса КК $cr$ для імітаційних моделей навчання ЕС*

| № | Прийняті гіпотези для ОР | Значення оптимального радіусу КК $cr$ | | | | |
|---|---|---|---|---|---|---|
| | | DoS/DDoS | Probe | R2L | U2R | BA |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| **Основі гіпотези** | | | | | | |
| 1 | Основна робоча $hy_{\gamma 1}$: реалізація ознаки (РОЗ) $rc_i$ ОР (*RS*) та показник *IE* знаходиться у межах звичайного стану КВІС | $cr_1^{onm} = 4-5$ | $cr_1^{onm} = 3-4$ | $cr_1^{onm} = 4-5$ | $cr_1^{onm} = 4-5$ | $cr_1^{onm} = 5-6$ |
| 2 | Гіпотеза $hy_{\gamma 2}$ – РОЗ $rc_i$ ОР (*RS*) дозволяє зробити висновок, що *IE* є меншими на норму | $cr_2^{onm} = 2-3$ | $cr_2^{onm} = 1-2$ | $cr_2^{onm} = 1-2$ | $cr_2^{onm} = 1-2$ | $cr_2^{onm} = 2-3$ |
| 3 | Гіпотеза $hy_{\gamma 3}$ дозволяє зробити висновок, що *IE* є більшими за норму | $cr_3^{onm} = 3-4$ | $cr_3^{onm} = 3-4$ | $cr_3^{onm} = 2-3$ | $cr_3^{onm} = 2-3$ | $cr_3^{onm} = 3-4$ |
| **Додаткові гіпотези для імітаційної моделі** | | | | | | |
| 4 | Гіпотеза $hy_{\gamma 1}^{D}$ – вузол $u$ демонструє підвищену мережеву активність | $cr_{D1}^{onm} = 4$ | $cr_{D1}^{onm} = 4$ | $cr_{D1}^{onm} = 3$ | $cr_{D1}^{onm} = 3$ | – |
| 5 | Гіпотеза $hy_{\gamma 2}^{D}$ – вузол демонструє підвищену мережеву активність | $cr_{D2}^{onm} = 3$ | $cr_{D2}^{onm} = 3$ | $cr_{D2}^{onm} = 3$ | $cr_{D2}^{onm} = 2$ | – |

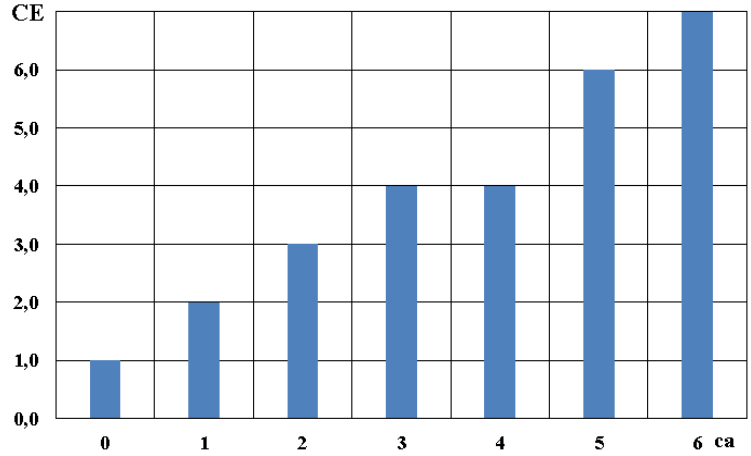


Рис. 1. Графік усередненого показника ІУФР навчання від ПДВ для реалізацій ознак розпізнавання мережевих атак

Під час імітаційного моделювання ІУФР навчання ЕС встановлено, що квазіоптимальне значення параметра $ca_{n,i}$ системи перевірочних / контрольних допустимих відхилень (СКДВ) дорівнює СКДВ = 8 – 16% при максимальному значенні $CE_{\max} = 6{,}16$ (рис. 1 та табл. 2).

За результатами ІМ зроблено такі висновки. Усереднене максимальне значення ІУФР навчання ЕС дорівнює: для атак класу DoS/DDoS $\overline{CE} = 3{,}19$; для атак класу Probe $\overline{CE} = 3{,}15$; для атак класу R2L $\overline{CE} = 2{,}84$; для атак класу U2R $\overline{CE} = 3{,}27$; для вірусних атак (ВА) $\overline{CE} = 2{,}56$. Результатами ІМ підтверджено, що запропоновані модель та метод кластерізації реалізацій ознак ОР, які ґрунтуються на ентропійному та інформаційно-дистанційному критерії Кульбака – Лейблера, дозволяють отримувати вхідні навчальні матриці для ЕС у складі СІРКЗ.

Таблиця 2

*Результати імітаційного моделювання*

| № | Параметр | Класи об'єктів розпізнавання | | | | |
|---|---|---|---|---|---|---|
| | | DoS/DDoS | Probe | R2L | U2R | ВА |
| 1 | Кількість реалізацій | 65 | 50 | 60 | 50 | 60 |
| 2 | Кількість ознак спостереження (загальна/розглянута) | 41/20 | 41/15 | 41/15 | 41/15 | 20/10 |
| 3 | Кількість сформованих БНМ | 20 | 15 | 15 | 15 | 10 |
| 4 | Середня кількість кроків навчання ЕС для формування БНМ (ОВН) | 700 | 900 | 900 | 1000 | 800 |
| 5 | Усереднене максимальне значення ІУФР навчання ЕС (гіпотеза $hy_{\gamma 1}$) | $\overline{CE}_{\max} = 3{,}19$ | $\overline{CE}_{\max} = 3{,}15$ | $\overline{CE}_{\max} = 2{,}84$ | $\overline{CE}_{\max} = 3{,}27$ | $\overline{CE}_{\max} = 2{,}56$ |
| 6 | Квазіоптимальне значення контрольних допустимих відхилень для РОЗ | СКДВ = 8 – 14% | СКДВ = 9 – 15% | СКДВ = 9 – 16% | СКДВ = 8 – 16% | СКДВ = 7 – 14% |

У **четвертому** розділі наведено результати програмної реалізації розробки та тестування ЕС «Analyzer of cyberthreats». Для розробки інтерфейсів та функціональних модулів ЕС використовувалася мова та середовище програмування Delphi. Для проектування ЕС обрана програма-оболонка CLIPS. Відповідно до цих завдань у склад ЕС імплементовані модулі, які дозволяють автоматизувати процедуру проведення аудиту ІБ КС; покращити процедуру розпізнавання загроз ІБ у КС; отримувати експертну інформацію про стан комп'ютерів у мережі; сканувати запущені програми на ЕОМ; визначати рівнів ІБ окремих ЕОМ у складі КС; полегшити роботу експертів з ІБ; використовувати накопичений раніше досвід з оцінювання стану ІБ; оцінювати поточні ризики НСД до ІС підприємства; представити рекомендації із підвищення рівня захищеності ІС; зменшити час на проведення перевірок та аудиту стану ІБ КС.

Тестування ЕС «Analyzer of cyberthreats» було проведено для КС декількох підприємствах м. Києва та м. Чернігова. На рис. 2 показані основні результати, отримані в ході моделювання показника $CE$ для мережевих класів кібератак.

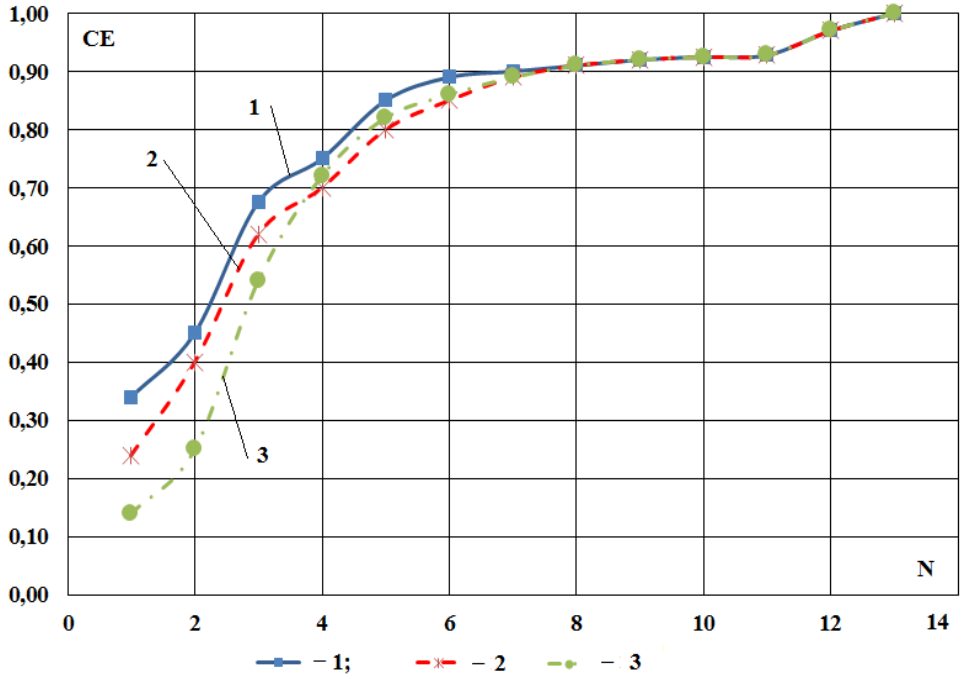


Рис. 2. Графік залежності ІУФР (IND) навчання здатної до самонавчання ЕС від кількості реалізацій ознак (N) які використовуються для навчання:
1 – модель гібридної нейронної мережі;
2 – модель інтелектуальної технології навчання (МІНТ) експертної системи з кібербезпеки КВКС;
3 – метод опорних векторів

Під час дослідження встановлено, що в моделі «голосування» МІТН за представницькими наборами реалізацій ознак кібератак досить обмежитися побудовою представницьких наборів довжини 5–7 реалізацій ознак.

У порівнянні з методом опорних векторів, МІТН для невеликої кількості реалізацій ознак ОР (2–4) має суттєву перевагу показника *CE* на 25–50 %, але поступається на 20–55 % показнику *CE*, отриманому для моделі гібридної нейронної мережі.

Порівняльний аналіз, рис. 3 та таблиця 3, здійснено на підставі даних, отриманих під час тестових випробувань ЕС «Analyzer of cyberthreats», та даних для систем виявлення мережевих вторгнень (СВВ) AIDS – application based IDS, комбінованих рішень IDS & IPS (Intrusion prevention system).

Запропонований підхід розпізнавання кібератак, заснований на МІТН, дозволяє підвищити рівень виявлення мережевих кібератак у КС. Виявлення різних типів атак за допомогою ЕС відбувається з ймовірністю 77–99 %. Крім цього, запропонований метод не вимогливий до ресурсів ІС і здатний виявляти невідомі типи кібератак у КС.

У результаті означеного експерименту для розробленої ЕС та методу інтелектуального розпізнавання кібератак, були отримані наступні результати для атак: DoS/DDoS – для помилок 1-го роду (кількість помилкових спрацьовувань) – 10–11 %) і помилок 2-го роду (кількість невиявлених атак) – 2–3%; Probe – для помилок 1-го роду – 12–14 і помилок 2-го роду – 3–4%; для атак R2L – для помилок 1-го роду – 9–11% і помилок 2-го роду – 2–4 %; U2R – для помилок 1-го роду – 11–12% і помилок 2-го роду – 3–5%.

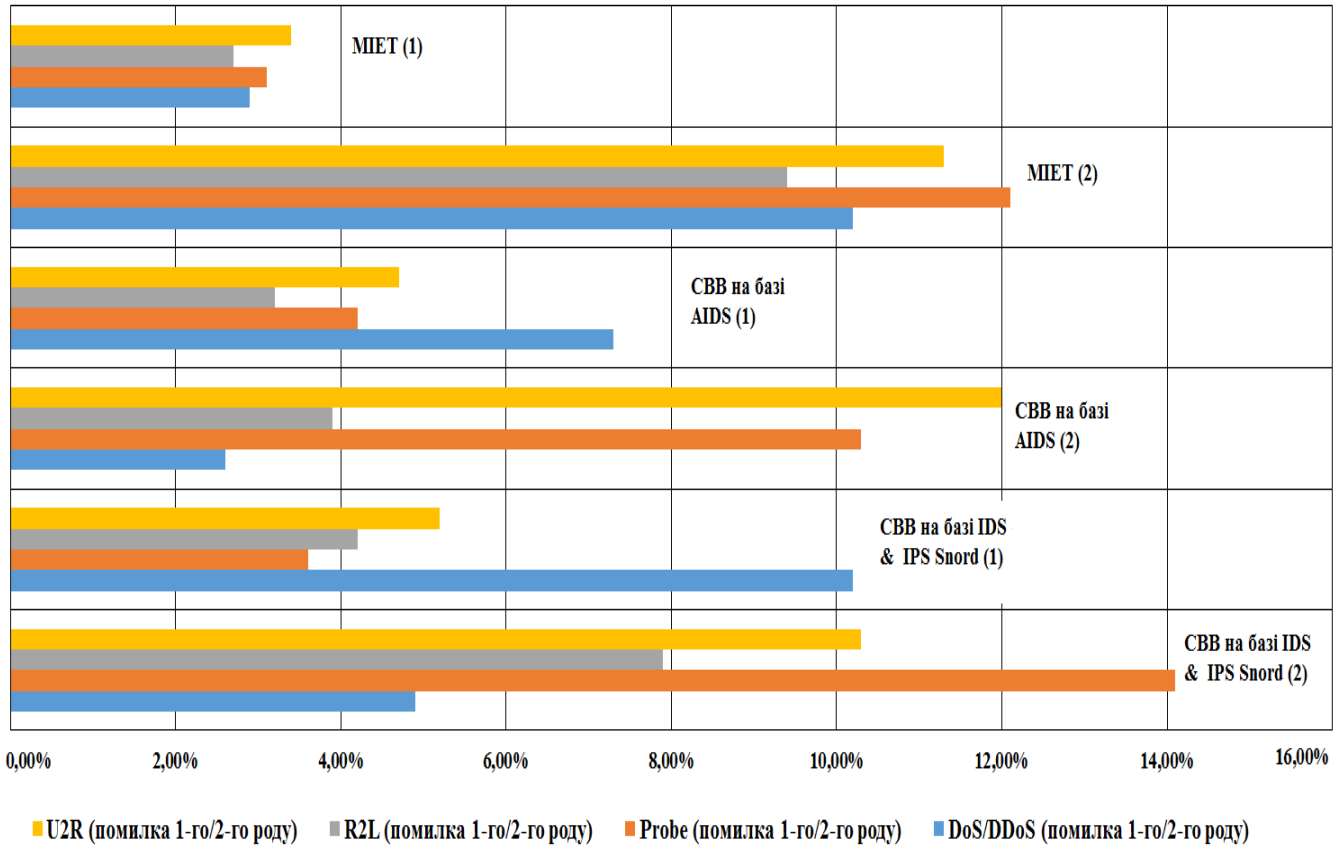


Рис. 3. Порівняння ймовірності виникнення помилок першого (**1**) та другого (**2**) роду при виявленні кібератак різними системами

Таблиця 3

*Порівняльна характеристика методів виявлення кібератак (КА)*

| № | Математичний апарат | Нечіткі КА можливість адаптації до помилок під час завдання на прийняття рішення в ході процедур МНав | База даних | Кількість вхідних параметрів | Пошук вторгнень та нормальної поведінки, % | Пошук нових ознак |
|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 1 | Ієрархічна самоорганізуюча карта | – | KDD– 99 | 41 | Norm–96,4; DoS–96,2; U2R–37,1; R2L–43,1; Probe–94,3 | – |
| 2 | Метод опорних векторів | – | | | Norm–99,8; DoS–97,5; U2R–86,6; R2L–81,3; Probe–92,8 | – |

Закінчення табл. 3

| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|
| 3 | Кластерні моделі на основі алгоритму DBSCAN | – | | | Norm–96,2; DoS–98,2; U2R–72,2; R2L–84; Probe–81,0 | + |
| 4 | Гібридна нейрона мережа | + | | | Norm–96; DoS–98,8; U2R–72,8; R2L–33,45; Probe–86,2 | + |
| 5 | МІТН та модель кластеризації реалізацій ознак для ЕС | + | | 10–12 | Norm–98,7; DoS–99,1; U2R–76,5; R2L–90; Probe–84,2 | + |

У ході досліджень встановлена оптимальна кількість кластерів для визначення $\max$ значення показника ІУФР при навчанні ЕС, яка дорівнює 3.

Одержані результати дозволяють зробити висновок, що, на відміну від існуючих, запропоновані метод та моделі інтелектуального розпізнавання кібератак, не потребують значного часу для систематизації та переведення у форму ББНМ шаблонів кібератак з наступним їх заведенням у ЕС.

## ВИСНОВКИ

У дисертації запропонований новий підхід до розв'язання актуальної науково-прикладної задачі підвищення ефективності систем інтелектуального розпізнавання кібератак на критично важливі інформаційні системи на основі розроблених моделей та методології створення здатної до самонавчання експертної системи, яка дозволяє враховувати відомі статистичні параметри кластеризації реалізацій ознак кібератак. Це дозволяє оперативно виявляти нові види складних комбінованих атак при обмежених обчислювальних ресурсах та варіативності умов застосування. Проведені дослідження дозволяють зробити такі висновки:

1. З’ясовано, що складність застосування до інтелектуальних систем розпізнавання цільових кібератак формалізованого апарату аналізу й синтезу СІРКЗ, полягає в тому, що конкретний інформаційний комплекс КВІС або КВКС та їх підсистеми ІБ складаються з різнорідних елементів, які описуються із використанням різних моделей. Показано, що застосування елементів адаптивного захисту інформації може бути засноване на використанні новітніх методів інтелектуального розпізнавання кібератак.

2. Запропонована модель ЕС у складі СІРКЗ із використанням процедури нечіткої кластеризації реалізацій ознак кібератак та можливістю корекції вирішальних правил, що дозволить створювати адаптивні механізми самонавчання системи інтелектуального розпізнавання кібератак на КВІС.

3. Запропоновано для оцінки якості розбиття простору реалізацій ознак об'єктів розпізнавання у ЕС застосовувати в якості оціночного показника модифіковану ІУФР, здатної до самонавчання системи розпізнавання. Доведено, що застосування моделі та методу кластерізації реалізацій ознак ОР, які ґрунтуються на ентропійному та інформаційно-дистанційному критерії Кульбака – Лейблера, дозволяє отримувати вхідну навчальну матрицю, яка використовується як об'єкт навчання, та в рамках інтелектуальних технологій та методів навчання АСР будувати коректні вирішальні правила розпізнавання кібератак на КВІС. Встановлено, що збільшення кількості векторів–реалізацій класів ОР при виявленні кібератак проти КВІС призводить до збільшення максимального значення інформаційної умови функціональної результативності, а також дозволяє отримувати коректні правила для здатної до самонавчання системи розпізнавання. Доведено, що оцінка якості розбиття простору реалізацій ознак кібератак та інших варіантів легітимного втручання в роботу КВІС, може бути ефективно вирішена на основі ІУФР та можливої корекції вирішальних правил розпізнавання, що дозволяє зменшити кількість попередньої інформації, яка підлягає опрацюванню аналітиками служб ІБ КВІС.

4. Удосконалено метод навчання ЕС у складі СІРКЗ для запропонованих етапів паралельної оптимізації контрольних відхилень для реалізацій ознак розпізнавання кібератак проти КВІС. Розроблено метод навчання ЕС у складі СІРКЗ, який являє собою ітераційну процедуру пошуку глобального максимуму ІУФР у допустимому діапазоні визначення його функції. Запропоновані уточнення до методу навчання ЕС дозволяють попереджати можливі випадки поглинання одним класом ОР базових реалізацій ознак іншого класу, враховує відомі статистичні параметри кластеризації реалізацій ознак об'єктів розпізнавання, а також помилки під час завдання на прийняття рішення в ході процедур машинного навчання. Отримано відповідні предикатні вирази для ЕС здатної до самонавчання.

5. Запропоновано уточнення до методу розбиття простору реалізацій ознак на кластери в ході реалізації процедури розпізнавання ОР, який відрізняється від існуючих одночасною оптимізацією при обчисленні контрольних допусків у ході аналізу ЕС важко пояснюваних реалізацій ознак ОР та дозволяє на кожному кроці навчання змінювати перевірочні допустимі відхилення для всіх ознак одночасно.

6. Проведено дослідження за допомогою імітаційного моделювання для моделі та методу кластерізації реалізацій ознак ОР, які ґрунтуються на ентропійному та інформаційно-дистанційному критерії Кульбака – Лейблера, а також алгоритму оптимізації контрольних допусків на реалізації ознак розпізнавання ОР. Встановлено, що квазіоптимальне значення параметра системи контрольних допустимих відхилень дорівнює 8–16 % при максимальному значенні ІУФР $CE_{\max} = 6{,}16$.

7. Проведено тести на проникнення в ІС та АСК підприємств Замовників, та виконано дослідження продуктивності ЛОМ і ІС, а також поведінки всієї інфраструктури в звичайних умовах і при різних варіантах кібератак (DoS/DDoS, Probe, R2L, U2R). Апробована методологія тестування ЕС «Analyzer of cyberthreats», яка дозволяє на етапі аналізу та синтезу СІРКЗ для конкретних КВІС, встановлювати відношення між елементами адаптивних систем кіберзахисту. Експериментально підтверджена ефективність запропонованого методу навчання ЕС та СІРКЗ з можливістю корекції вирішальних правил, що дозволило створити адаптивний механізм самонавчання системи розпізнавання кібератак на КВІС. Протестована розроблена ЕС «Analyzer of cyberthreats». Встановлено, що запропонований метод навчання ЕС «Analyzer of cyberthreats» та відповідного поповнення БЗ для СІРКЗ, є найбільш ефективним для 3 кластерів у завданнях розбиття простору реалізацій ознак ОР для досліджених КВІС. При цьому в режимі тестового навчання ЕС та СІРКЗ достатня кількість кроків для безпомилкового визначення класів кібератак склала $k = 2500 - 3000$.

8. Виконано порівняння розроблених методів навчання (МІЕТ) з існуючими та доведено, що запропоновані рішення, дозволяють досягнути результатів розпізнавання типових класів кібератак на рівні 70 – 99%, що знаходиться на рівні ефективності розпізнавання гібридних нейронних мереж та генетичних алгоритмів.

## СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. V. Lakhno, Yu. Tkach, T. Petrenko, S. Zaitsev and V. Bazylevych, “Development of adaptive expert system of information security using a procedure of clustering the attributes of anomalies and cyber attacks”, *Eastern-European Journal of Enterprise Technologies,* no. 6/9 (84), pp. 32–44, 2016.

2. V. Lakhno, S. Zaitsev, Yu. Tkach, T. Petrenko, “Adaptive expert systems development for cyber attacks recognition in information educational systems on the basis of signs’ clustering”, *Advances in Intelligent Systems and Computing*, v. 754. pp. 673–682, 2018.

3. T. Petrenko, “Design of adaptive system for detection of cyber-attacks”, *MEST Journal: Management, Education, Science & Society, Technologies,* v. 5, pp. 78–85, 2017.

4. В.А. Лахно, Т.А Петренко і М.В. Пирог, “Моделювання роботи адаптивної системи розпізнавання кібератак в умовах неоднорідних потоків запитів в модулях e-business”, *Безпека інформації*, т. 22, № 2, с. 135–142, 2016.

5. В.А. Лахно, А.М. Терещук и Т.А. Петренко, “Совершенствование киберзащиты информационных систем за счет адаптивных технологий распознавания кибератак”, *Захист інформації,* т.18, № 2, с. 99–106, 2016.

6. Д.Б. Мехед, Ю.М. Ткач Ю.М., В.М. Базилевич і Т.А. Петренко, “Аналіз загроз інформаційної безпеки в мережах стандарту IEEE 802.11”, *Захист інформації*, т. 17, №4. с. 285–291, 2015.

7. Т.А. Петренко, “Прикладні аспекти захисту конфіденційної інформації на підприємстві”, *Новітні технології у науковій діяльності і навчальному процесі: матеріали Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених (Чернігів, 23-24 квітня 2014 р.): тези доповідей,* Ч., 2014, С. 26–28.

8. Ю.В. Козинець та Т.А. Петренко “Дослідження процесу управління інформаційною безпекою”, *Новітні технології у науковій діяльності і навчальному процесі: матеріали Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених (Чернігів,28 квітня 2015 р.): тези доповідей*, Ч., 2015, С. 26–27.

9. Д.Б. Мехед, В.М. Базилевич і Т.А. Петренко, “Оцінка ризиків інформаційної безпеки на підприємстві”, *Стан та удосконалення безпеки інформаційно-комунікаційних систем “SITS-2015”: матеріали VII Всеукраїнської науково-практичної конференції (Миколаїв-Коблево, 9-12 червня 2015 р.): збірник тез доповідей*, Миколаїв-Коблево, 2015, С. 59 – 61.

10. Т.А. Петренко, В.А. Лахно, Г.С. Григорян, “Розробка адаптивної системи розпізнавання кіберзагроз”, *Безпека українського суспільства в концепції вступу в постіндустріальне суспільство ЄС: Наукові доповіді та тези учасників науково-практичної конференції (м. Київ, 16 грудня 2015 р.),* К., 2015. С. 66–76.

11. Ю.М. Ткач, Д.Б. Мехед, В.М. Базилевич і Т.А. Петренко, “Аналіз загроз інформаційної безпеки в WI-FI мережах”, *Актуальні питання забезпечення кібербезпеки та захисту інформації: тези доповідей учасників II Міжнародної науково-практичної конференції (Закарпатська область, Міжгірський район, село Вернє Студене, туристичний комплекс «Едельвейс», 24-27 лютого 2016 року)*, К., 2016, С. 151–155.

12. В.А. Лахно, А.М. Терещук и Т.А. Петренко “Адаптивные системы распознавания кибератак на критически важные компьютерные системы”, *II міжнародна науково-практична конференція “Актуальні проблеми моделювання ризиків і загроз виникнення надзвичайних ситуацій на об'єктах критичної інфраструктури”: Наукові доповіді та тези учасників науково-практичної конференції ( м. Київ, 26-28 травня 2016р.)*, К., 2016, С. 136-141.

13. T. Petrenko and V. Lakhno, “A model developed for teaching an adaptive system of recognising cyberattacks in information systems”, *The seventh world congress “Aviation in the XXI-st century” Safety in Aviation and Space Technologies, Kyiv, NAU, September 19-21*, 2016, pp. 406-408.

14. В.А. Лахно и Т.А. Петренко, “Система интеллектуальной поддержки принятия решений в слабо формализуемых задачах обеспечения кибербезопасности”, *Комплексне забезпечення якості технологічних процесів та систем (КЗЯТПС – 2017): матеріали тез доповідей VII міжнародної науково-практичної конференції (м. Чернігів, 24–27 квітня 2017 р.)*, Ч., 2017, Т. 2, С. 107-108.

15. Т.А. Петренко та В.А. Лахно, “Метод та моделі адаптивних експертних систем розпізнавання кібератак на основі кластеризації ознак”, *ITSEC: Безпека інформаційних технологій: VII міжнародна науково-технічна конференція, 16-18 травня 2017 р.*, м. Київ, НАУ, 2017, С. 77-78.

16. Т.А. Петренко, “Інформаційна безпека в сучасних умовах”, *Вісник Чернігівського державного інституту права, соціальних технологій та праці,* №2, с. 98–102, 2009.

## АНОТАЦІЯ

**Петренко Т. А. Методи та моделі експертних систем розпізнавання кібератак на основі кластеризації реалізацій ознак**. – Рукопис.

Дисертації на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – Системи захисту інформації. Національний авіаційний університет Міністерства освіти і науки України, Київ, 2019.

Дисертаційна робота містить результати досліджень, які спрямовані на подальший розвиток методів та моделей для адаптивних систем розпізнавання кібератак на основі кластеризації реалізацій ознак. Запропоновано структурну схему здатної до самонавчання експертної системи (ЕС) з інформаційної безпеки. Розроблено модель ЕС у складі системи інтелектуального розпізнавання кіберзагроз (СІРКЗ) та метод її навчання, у яких застосовується процедура нечіткої кластеризації реалізацій ознак кібератак та корекції вирішальних правил, що дозволяє створювати адаптивні механізми самонавчання СІРКЗ. Запропоновано застосовувати в якості оціночного показника ефективності навчання ЕС модифіковану інформаційну умову функціональної результативності (ІУФР), яка ґрунтується на ентропійному та інформаційно-дистанційному критерії Кульбака-Лейблера. Удосконалено метод розбиття простору реалізацій ознак на кластери в ході реалізації процедури розпізнавання кібератак, а також метод навчання ЕС, які являють собою ітераційну процедуру пошуку глобального максимуму ІУФР. Проведені тестові дослідження ЕС та порівняльний аналіз із існуючими методами та моделями, які використовуються у інтелектуальних системах розпізнавання кібератак.

**Ключові слова**: захист інформації, інформаційна безпека, інтелектуальне розпізнавання кібератак, кластеризація реалізацій ознак.

## ABSTRACT

**Petrenko T.A. Methods and models of adaptive expert systems of recognition of cyber attacks on the basis of clustering of features. –** Manuscript.

Thesis for a candidate degree in technical sciences by specialty 05.13.21. – Information security systems. National Aviation University of the Ministry of Education and Science of Ukraine, Kyiv, 2019.

The dissertation contains the results of researches aimed at further development of methods and models for adaptive systems of recognition of cyber attacks on the basis of clusterization of the implementation of features. A structural scheme of an expert system for information security capable of self-education is proposed.

On the basis of the analysis of available scientific publications, it was found that the complexity of application to intelligent recognition systems of target cyber attacks of the formalized apparatus of analysis and synthesis is that a specific information complex and their subsystems of information security consist of heterogeneous elements that are described using different models. It is shown that the application of elements of adaptive information protection can be based on the use of advanced methods of intelligent recognition of cyber attacks.

For the first time, an expert system model has been developed as part of intelligent intrusion detection systems, in which, unlike existing ones, the procedure of fuzzy clusterization of the implementation of cyber attacks and the subsequent correction of decisive rules is applied, which allows for the creation of adaptive self-learning mechanisms for intelligent cyber attacks detection systems.

For the first time, it is suggested to use the modified informational condition of functional effectiveness as an estimator of the effectiveness of the training of the expert system based on the entropy and informational-remote criterion of the Kulbak-Leibler, and, unlike the existing one, allows to receive the entrance educational matrix, which is used as an object of study , and build correct decisive rules for recognizing cyber attacks on critical information systems.

The method of partitioning the realization of features into clusters in the course of implementing the cyber attacks recognition procedure, which differs from existing, is simultaneously optimized when calculating control tolerances during the analysis by an expert system of difficult explanatory implementations of the objects of observation, and allows for each step of the training to change the test tolerance deviations for all implementations of cyber attacks simultaneously.

The method of teaching the expert system is improved, which is an iterative procedure for finding the global maximum of the information condition of functional efficiency, and, unlike the existing one, prevents possible cases of one object acquisition of objects of recognition of basic realizations of signs of observation objects, as well as errors during the task of making decisions in the course of machine learning procedures.

Further development of simulation models for the composite construction of intelligent detection systems for cyber attacks by simultaneously optimizing control tolerances during the analysis of recognition objects, allowing them to conduct research, to select rational methods of counteraction and neutralization of consequences, to analyze more complex and previously unknown types of cyber attacks on critical information systems.

The practical significance of the results is that the dissertation developed a software implementation of the expert system for the recognition of cyber attacks, which allows to increase the efficiency of recognition, depending on the class of cyber attacks, up to 70-99%, and reduce the time of debugging of the information security systems projects by 15-20% CYIS at the expense of simulation of a cyber attacks. An EU-based self-learning tool, "Analyzer of Cyberthreats", allows you to take into account the known statistical parameters of clustering implementations of features of recognition objects, as well as errors during the decision making task during machine learning. The proposed expert system allows to increase the efficiency of functioning of cybersecurity systems.

The results of the work have been implemented in the scientific and technical developments of "Protection of Information" Ltd. and in the educational process at the Chernihiv National Technological University, as well as at the National Aviation University.

**Key words:** protection of information, information security, intellectual recognition of cyber attacks, clustering of the implementation of features.

# АННОТАЦИЯ

**Петренко Т.А. Методы и модели экспертных систем распознавания кибератак на основе кластеризации реализаций признаков**. – Рукопись.

Диссертация на соискание ученой степени кандидата технических наук по специальности 05.13.21 – Системы защиты информации. Национальный авиационный университет Министерства образования и науки Украины, Киев, 2019.

Диссертационная работа содержит результаты исследований, направленных на дальнейшее развитие методов и моделей для адаптивных систем распознавания кибератак на основе кластеризации реализаций признаков. Предложена структурная схема способной к самообучению экспертной системы (ЭС) в задачах информационной безопасности. Разработана модель для ЭС в составе интеллектуализированных систем распознавания кибератак и угроз (СИРКА) и метод ее обучения. Метод основан на процедуре нечеткой кластеризации реализаций признаков кибератак и коррекции решающих правил. Разработанный подход позволяет создавать адаптивные механизмы самообучения СИРКА. Предложено применять в качестве оценочного показателя эффективности обучения ЭС модифицированное информационное условие функциональной результативности распознавания атаки (ИУФР). Данное условие основано на энтропийном и информационно-дистанционном критерии Кульбака-Лейблера. Усовершенствован метод разбиения пространства реализаций признаков кибератак на кластеры в ходе реализации процедуры распознавания. Также усовершенствован метод обучения ЭС, который представляют собой итерационную процедуру поиска максимума ИУФР. Проведены тестовые исследования ЭС и сравнительный анализ с существующими методами и моделями, которые используются в интеллектуальных системах распознавания кибератак.

**Ключевые слова:** защита информации, информационная безопасность, интеллектуальное распознавание кибератак, кластеризация реализаций признаков.