В умовах постійного зростання кількості дестабілізуючих впливів на стан кіберпезпеки критично-важливих комп'ютерних систем, потрібні подальші дослідження, спрямовані на розвиток методологічних та теоретичних засад інформаційного синтезу систем кіберзахисту, здатних до самонавчання. Розроблена категорійна модель та алгоритм інформаційно-екстремального навчання системи інтелектуального розпізнавання загроз з можливістю гіпереліпсоїдної корекції вирішальних правил на основі нечіткої кластеризації ознак для безпомилкового визначення класів аномалій, кіберзагроз або кібератак

Ключові слова: адаптивні системи розпізнавання кіберзагроз, ознаки кібератаки, кластеризація ознак, інформаційно-екстремальний алгоритм

В условиях постоянного роста количества дестабилизирующих воздействий на состояние кибербезопасности критически важных компьютерных систем, необходимы дальнейшие исследования, направленные на развитие методологических и теоретических основ информационного синтеза систем киберзащиты, способных к самообучению. Разработана категориальная модель и алгоритм информационно-экстремального обучения системы интеллектуального распознавания угроз с возможностью гиперэллипсоидной коррекции решающих правил на основе нечеткой кластеризации признаков для безошибочного определения классов аномалий, киберугроз или кибератак

Ключевые слова: адаптивные системы распознавания киберугроз, признаки кибератаки, кластеризация признаков, информационно-экстремальный алгоритм

УДК 004.056
DOI: 10.15587/1729-4061.2016.66015

ПОБУДОВА АДАПТИВНОЇ СИСТЕМИ РОЗПІЗНАВАННЯ КІБЕРЗАГРОЗ НА ОСНОВІ НЕЧІТКОЇ КЛАСТЕРІЗАЦІЇ ОЗНАК

В. А. Лахно
Доктор технічних наук, доцент
Кафедра організації комплексного захисту інформації
Європейський університет
бул. Академіка Вернадського, 16В, м. Київ, Україна, 03115
E-mail: lva964@gmail.com

1. Вступ

Ефективність функціонування сучасних систем та технологій виявлення кібератак істотно залежить від оперативності та достовірності моніторингової інформації про активність кіберзлочинців на попередніх стадіях реалізації атак на інформаційні ресурси, зокрема й критично важливі. Як показав світовий досвід, на сьогодні найбільш ефективним методологічним підходом до побудови інноваційних інтелектуальних моніторингових систем кібернападів є шлях створення ієрархічних багаторівневих структур розпізнавання кібератак на початкових стадіях їхньої реалізації. При цьому, ієрархічний підхід дає змогу розв'язувати складні задачі управління процесом захисту інформації від кібератак в розподілених критично важливих інформаційних системах (КВІС) як послідовність локальних задач, скоординованих між собою.

Таким чином, одним із перспективних та актуальних напрямів досліджень систем інтелектуального розпізнавання кіберзагроз (СІРКЗ) є надання їм властивості адаптивності. Зокрема, при цьому можна використовувати моделі та методи інформаційно-екстремальної технології, яка ґрунтується на максимізації інформаційної спроможності СІРКЗ шляхом використовування при навчанні додаткових інформаційних обмежень, які, наприклад, стосуються ознак аномалій в роботі або кібератак в межах відомих та нових класів вторгнень.

2. Аналіз літературних даних і постановка проблеми

Як правило, ієрархія більшості КВІС, інформаційних систем (ІС) або автоматизованих систем керування (АСК) включає чотири рівня [1, 2]: рівень прикладного програмного забезпечення; рівень СКБД; рівень ОС; рівень мережі, що забезпечує взаємодію вузлів КВІС (протоколи TCP/IP, IPS/SPX, SMB/NetBIOS та ін. [3, 4]). За статистикою [5] та даними досліджень окремих авторів [6–8], до найбільш поширених типів атак можна віднести несанкціонований доступ до паролю і конфіденційної інформації, несанкціоноване віддалене виконання команд внаслідок помилок типу «переповнення буфера», порушення прав доступу, атаки типу «відмова в обслуговуванні» і завантаження шкідливого програмного забезпечення (ПЗ, наприклад, програм типу «троянський кінь», ActiveX, вірусів). Труднощі ефективного динамічного формування параметрів оцінки кіберзагрози полягають у тому, що розмір зони пошуку експоненційно залежить від потужності початкових множин ознак аномалій, уразливостей, загроз та кібернападів [9, 10].

Складність застосування до СІРКЗ формалізованого апарату аналізу й синтезу КВІС полягає в тому, що конкретний інформаційний комплекс і його підсистема інформаційної безпеки (ІБ) складаються з різнорідних елементів, які можуть описуватися різними розділами теорії (системами масового обслуговування [1, 2, 9], кінцевими автоматами [11, 12], теорією ймовірностей [3, 4, 13, 14], теорією розпізнавання образів [8, 9, 15], та ін. [1, 2, 16, 17]), тобто розглянутий об'єкт дослідження є агрегативним.

В США, державах ЄС, Китаї, Південній Кореї та Японії дослідженням проблематики створення інтелектуальних систем виявлення кібератак приділяється багато уваги, про що свідчить велика кількість публікацій з цієї тематики, зокрема, роботи [18–21].

В роботах [1, 3, 4, 11] з позицій аналізу потенційно небезпечних деструктивних впливів на інформаційну безпеку, запропоновано окремо розглядати функціональну безпеку КВІС. При цьому у визначенні функціональної безпеки КВІС акцент було зроблено на правильність функціонування системи. Тобто, вважається, що вона в основному пов'язана з ненавмисними деструктивними факторами [2, 17, 21]. Однак складність та багатофакторність процесів у КВІС в більшості випадків [4, 5, 22] вказує на неможливість окремого оцінювання параметрів функціональної, інформаційної безпеки та кіберзахисту.

Відповідно до підходів, запропонованих у [4, 7, 9], надійний інформаційний процес (ІП) у КВІС успішно протидіє існуючим кіберзагрозам при заданих зовнішніх умовах його функціонування. Це призводить до постійного вдосконалення як способів і засобів захисту інформації (ЗЗІ), так і способів і засобів реалізації загроз для інформаційної безпеки (ІБ), в результаті чого поява нових ЗЗІ призводить до появи нових засобів нападу [2, 7, 10, 22].

Причина лежить в принципових теоретичних труднощах моделювання технологій забезпечення кіберзахисту КВІС, що виникають при спробі з'єднати перспективний підхід до забезпечення надійності та захисту ІП від кібернападів з гнучкістю захисних механізмів [6, 9, 11, 16]. Тому, на думку авторів [1, 2, 5, 15], СІРКЗ повинна визначати, які завдання для КВІС є критично важливими.

У роботах [4, 6, 7, 22] проведено аналіз методів діагностики аномалій в комп'ютерних системах – сигнатурний, статистичний аналіз, використання інтелектуальних (експертних) систем, генетичних алгоритмів, нейромереж та ін.).

В Україні питанням розробки та створення СІРКЗ присвячені роботи [6–9, 16]. Однак, запропоновані в роботах моделі ґрунтуються на різнорідних підходах та носять точковий характер, відповідно до об'єктів кібернападу. Моделі та алгоритми розпізнавання кібернападів часто не взаємопов'язані [6, 8], що наразі ускладнює їх використання при створенні ефективних СІРКЗ.

Отже, потрібні подальші дослідження, спрямовані на розвиток методологічних та теоретичних засад інформаційного синтезу систем захисту інформації, здатних до самонавчання, зокрема, на основі нових моделей та алгоритмів для СІРКЗ із використанням процедури нечіткої кластеризації ознак аномалій, кіберзагроз або кібератак.

3. Мета і завдання дослідження

Метою роботи є розробка моделі та алгоритму навчання адаптивної системи розпізнавання кіберзагроз з можливістю нечіткої кластеризації ознак аномалій, кіберзагроз або кібератак, та корекцією вирішальних правил, що дозволяє скоротити час навчання системи кіберзахисту, в умовах зростання кількості та складності кібернападів.

Для досягнення мети роботи потрібно вирішити наступні завдання:

– розробити модель, яка дозволяє для конкретних КВІС, встановлювати відношення між елементами адаптивних систем кіберзахисту;

– розробити алгоритм навчання СІРКЗ із використанням процедури нечіткої кластеризації ознак аномалій або кібернападів та можливістю гіпереліпсоїдної корекції вирішальних правил, що дозволить створювати адаптивні механізми самонавчання системи розпізнавання загроз у КВІС;

– перевірити алгоритм інформаційно-екстремального навчання СІРКЗ і визначити раціональну кількість кластерів в просторі ознак аномалій або кібернападів для КВІС, а також потрібну кількість кроків для навчання.

4. Категорійна модель системи інтелектуального розпізнавання кіберзагроз

Оцінка загроз ІБ КВІС включає дві складові: ситуаційний аналіз і виявлення загроз [1, 6, 7, 9]. Ситуаційний аналіз являє собою детальний аналіз параметрів функціонування апаратно-програмного забезпечення КВІС. При проведенні даного аналізу доцільно згрупувати однотипні дані і оцінювати їх окремо по кожній групі. Приклад такого аналізу показаний на рис. 1, 2.

Виявлення загроз передбачає комплексний і детальний аналіз усіх факторів, які можуть впливати на безпеку функціонування КВІС. Загрози у відповідності до класів [6, 8, 13, 15] поділяються на три базові групи: «потенційні» – дії, які теоретично можуть становити небезпеку; «Реальні» – дії зловмисників по НСД; «Спрямовані» – ті, які спрямовані на реалізацію конкретних уразливостей в КВІС.

На думку багатьох фахівців, перспективним шляхом підвищення функціональної ефективності СРКЗ, що у деяких випадках функціонують за умов апріорної невизначеності та впливу зовнішніх дестабілізуючих неконтрольованих факторів, є впровадження інтелектуальних інформаційних технологій, основаних на методах та моделях машинного навчання [4, 8, 9, 15, 17, 20]. На початковому етапі навчання можуть бути використані методи та алгоритми кластерного аналізу для автоматизації процедури формування керованого процесу вхідного математичного опису задачі розпізнавання аномалій у роботі КВІС та кібернападів на основі бази знань, сформованої по відомим ознакам.

Трансформація апріорно нечіткого розбиття ознак O_b аномалій або кібератаки в чітке розбиття еквівалентності класів розпізнавання відомих та нових кібератак може бути успішно розв'язана у випадку використовування моделей, в якій контейнери класів розпізнавання кібератак, відновлюються в радіальному базисі бінарного простору ознак розпізнавання конкретної атаки.

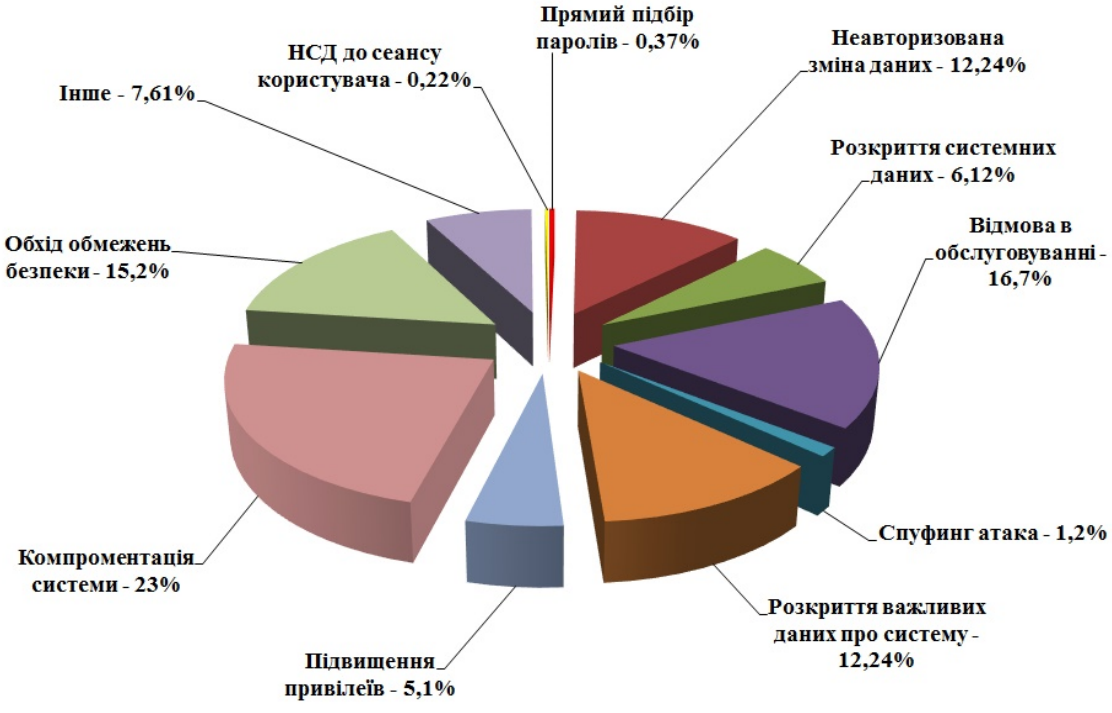

Рис. 1. Розподіл частки найбільших кіберзагроз для КВІС та АС підприємств [5, 7, 11, 18]

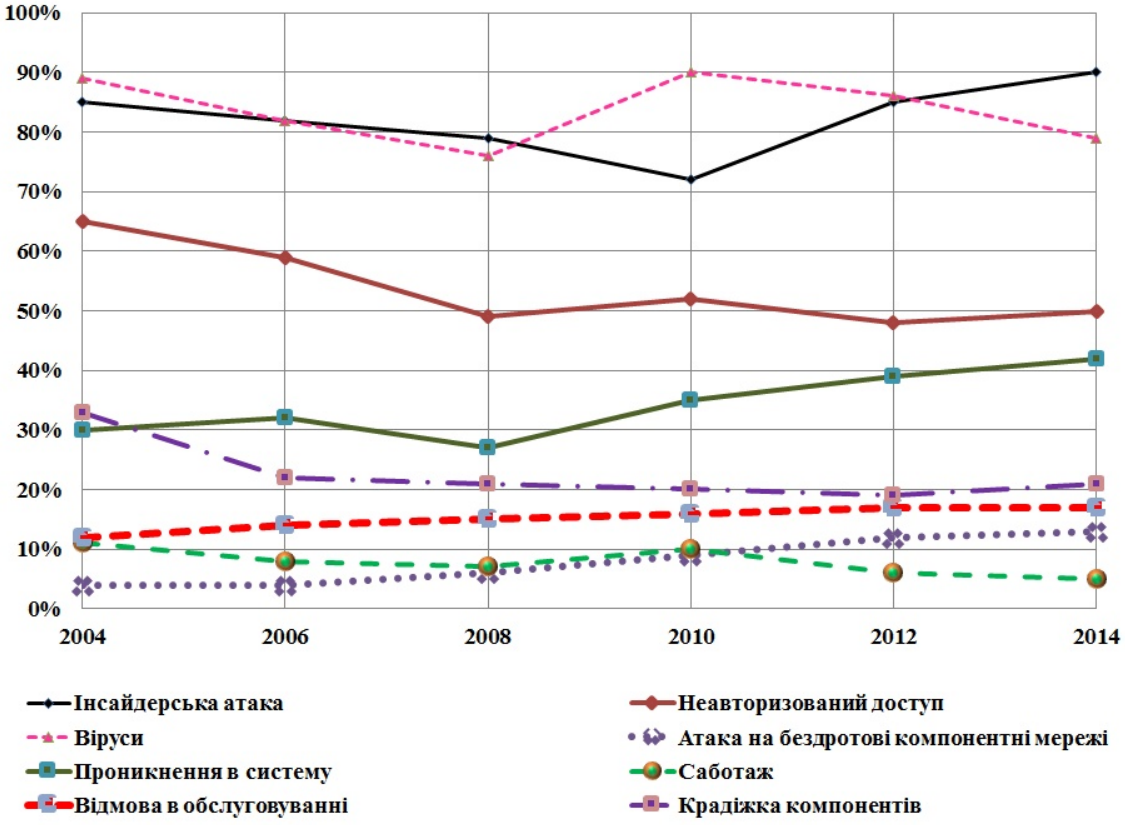

Рис. 2. Динаміка найбільших кіберзагроз для КВІС та АС підприємств [3–5, 7, 11, 18]

Наприклад, аналіз аномалій виявляє істотні відхилення трафіку мережевих пристроїв від «нормального» профілю трафіку для даного пристрою або групи пристроїв. Прикладами мережевих аномалій є раптове збільшення інтернет-трафіку робочої станції або зміна структури трафіку (зокрема, збільшення шифрованого SSL-трафіку) в порівняно зі звичайними щоденними показниками для даної ЕОМ у складі КВІС [4, 7, 15, 19, 21, 22].

Сутність розбиття об'єктів які містять ознаки аномалій (кібератак) на клас однотипних з точки зору інформаційної безпеки або кіберзахисту множин по-

лягає в розбитті множини об'єктів на підмножини. Класичний підхід до вирішення цього завдання здійснюється в два етапи [2, 4, 8, 11].

На першому етапі визначається множина показників і їх параметрів, тобто простір ознак аномалій (або кіберзагрози), табл. 1. Якщо множину значень кожного з показників розбити за певними правилами на непересічні групи, то за кожним показником можуть бути закріплені виділені області його значень, в межах яких вимоги до стану ІБ (кіберзахисту) є незмінними. Для різних КВІС розбиття множини ознак на непересічні групи проводиться не по одному, а по багатьом показникам стану ІБ.

На другому етапі визначається функція близькості і критерій розбиття на множини ознак з використанням великої кількості показників і їх значень і визначається кількість класів типових кібернападів на КВІС.

Дане завдання може бути вирішено за допомогою методів кластерного аналізу [8, 17, 22]. Традиційні алгоритми нечіткої кластеризації використовують як вхідні параметри задану кількість кластерів розбиття, а деякі з них, також, заданий показник нечіткості кластерів в просторі ознак уразливостей [1, 2, 17], аномалій [7, 12, 19], загроз НСД [16, 18] та кібератак [18, 22]. На основі інформаційного критерію функціональної ефективності (ІКФЕ) СЗКЗ для КВІС можна реалізувати адаптивний механізм налаштування параметрів алгоритму кластеризації ознак аномалій, кібератак або загроз. Такий підхід дозволить обрати оптимальну в інформаційному розумінні кількість ознак і отримати вирішальні правила для оперативного прийняття рішень в робочому режимі СРКЗ.

Математичний опис СІРКЗ виглядає наступним чином:

$$\Delta = \left\langle G \times T \times O_b \times \Phi \times R, Z^{|2|}, X^{|2|}, B_1, B_2 \right\rangle, \quad (1)$$

де G – множина вхідних факторів (сигналів), які впливають на ІБ КВІС; T – множина моментів часу зняття інформації про стан ІБ (кіберзахищеності КВІС); O_b – простір ознак для розпізнавання кіберзагроз КВІС; Ф – простір можливих функціональних станів ІБ КВІС; R – база знань для ідентифікації аномалій, кіберзагроз або кібератак; $Z^{|2|}$ – навчальна матриця (еталон) для двох класів; $X^{|2|}$ – бінарна навчальна матриця; B_1, B_2 – оператори формування вхідної та бінарної навчальних матриць, відповідно.

Категорійна модель адаптивної системи інтелектуального розпізнавання загроз наведена на рис. 3.

Оператор $\Theta: X^{|2|} \to \Re^{|2|}$ використовується для розбиття простору ознак аномалій, кіберзагроз або кібератак на два класи розпізнавання. За допомогою параметра класифікації ψ перевіряється статистична гіпотеза про належність реалізацій до модельованого класу аномалій, кіберзагроз або кібератак. Шляхом оцінки статистичних гіпотез, за допомогою оператору γ, формується множина $\zeta^{|q|}$ яка характеризує точність розпізнавання СІРКЗ, відповідно, χ – кількість статистичних гіпотез, $q=\chi^2$ – кількість характеристик СІРКЗ. Оператор φ формує множину E, яка складається із значень інформаційного критерію функціональної ефективності (ІКФЕ) СІЗКЗ. Оператор β використовується для оптимізації системи контрольних відхилень СІРКЗ. Множина M, замикається послідовно оператором $\alpha_1: E \to M$ і оператором $\alpha_2: M \to Z$, який змінює реалізації ознак аномалій, кіберзагроз або кібератак в процесі навчання СІРКЗ.

Таблиця 1

Фрагмент навчальної матриці простору ознак аномалій та кібератак на КВІС

Тип аномалії (або кібератаки) [1, 4, 5, 7, 9, 16, 17, 19, 21] **Відомі загрози (Класи аномалій або атак)**	Ознаки аномалій або кібератаки (Простір ознак O_b) [2, 4, 5, 15, 17, 19, 22]
Відмова в обслуговуванні елементів КВІС	1 – не працюють штатні компоненти; 2 – зниження продуктивності системи; 3 – ін.
Викрадення інформації або компонентів КВІС	1 – об'єктивні ознаки (наприклад, поява конфіденційної інформації у ЗМІ); 2 – субуєктивні ознаки; 3 – ін.
Привласнення особистості у КВІС	1 – об'єктивні ознаки (наприклад, зафіксовані спроби роботи під чужим логіном); 2 – субуєктивні ознаки; 3 – ін.
Модифікація інформації у КВІС	1 – зміна контенту; 2 – зміна структури інформаційних масивів; 3 – ін.
Вірусна атака на КВІС	1 – незвичайні прояви в роботі ЕОМ; 2 – зміни заданої в передостанньому сеансі роботи з ЕОМ структури файлової системи; 3 – ін.
Несанкціонований запуск ПЗ КВІС	1 – незвичайні прояви в роботі ЕОМ; 2 – атипова поведінка ПЗ; 3 – ін.
Порушення доступності БД та ПЗ КВІС	1 – не працюють штатні компоненти КВІС (ІМ та ПЗ); 2 – ін.
Мережеві атаки	1 – незвичайний трафік; 2 – аномалії мережевого трафіку; 3 – ін.
Інші....	
Невідомі загрози (Класи аномалій або атак)	Невиявлені Ознаки аномалій або кібератаки

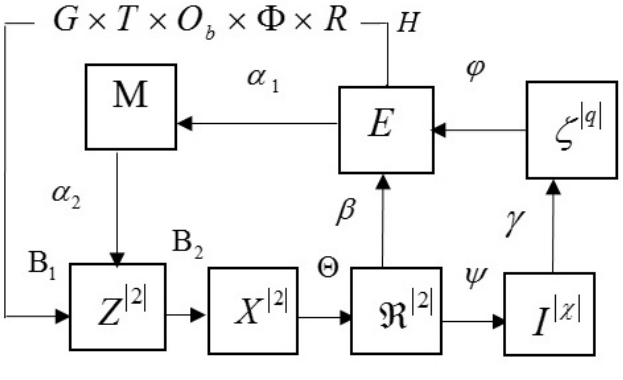

Рис. 3. Категорійна модель СІРКЗ для КВІС

5. Алгоритм навчання адаптивної системи розпізнавання кіберзагроз із використанням процедури нечіткої кластеризації ознак

Розглянемо процес формування апріорно нечіткої класифікованої навчальної матриці з метою побудови вирішальних правил в процесі навчання СІРКЗ. Припустимо, що відома апріорно некласифікована багатовимірна навчальна матриця для СІРКЗ $\left\|z_i^{(j)}\right\|, i=\overline{1,N}, j=\overline{1,n},$ де N,n – відповідно, кількість ознак розпізнавання аномалій або кіберзагрози (кібератаки) та випробувань. Постановка задачі:

1) в режимі кластерного аналізу необхідно перетворити вхідну некласифіковану навчальну матрицю ознак у нечітку класифіковану;

2) в режимі навчання побудувати чітке розбиття простору ознак розпізнавання аномалій, кіберзагроз або кібератак на класи $\left\{R_c^0 \,|\, c=\overline{1,C}\right\}$, які відповідно характеризують функціональні стани керованого процесу кіберзахисту, шляхом оптимізації координат вектора параметрів функціонування системи ІБ для КВІС

$$h=\left\langle C,s,\delta,r_{c1},r_{c2},O_b,a_c\right\rangle, \tag{2}$$

де C – кількість кластерів або потужність алфавіту класів розпізнавання аномалій в роботі КВІС або кіберзагроз; s – показник нечіткості для алгоритму; δ – поля допусків на ознаки розпізнавання аномалії, загрози або атаки; r_{c1}, r_{c2} – двійкові вектори, що визначають координати першого та другого фокусів гіпереліпсоїдного контейнеру для класу аномалій, кіберзагроз (кібератак) в бінарному просторі ознак O_b; a_c – піввісь контейнеру класу в просторі ознак O_b.

Введемо такі обмеження

$$\begin{cases} 2\le C\le n/n_{min}; n_c\ge n_{min}; s>1; a_c>d_c; d_c\le N/2; \\ a(r_{d1}\oplus r)+a(r_{d2}\oplus r)-d_d>0, \\ \forall r\in\left\{r: a(r_{c1}\oplus r)+a(r_{c2}\oplus r)=2a_c\right\}; \\ \delta\in\left[0,\delta_n/2\right], \end{cases} \tag{3}$$

де n_{min} – мінімальний обсяг навчальної вибірки для кожного класу ознак аномалій або кібератак (вибірка обов'язково повинна бути репрезентативною); n_c – кількість реалізацій в межах класу R_c^0; d_c – відстань до центра гіпе-реліпсоїдного контейнера в межах класу R_c^0; $a(r_{d1}\oplus r)$, $a(r_{d2}\oplus r)$ – відповідно, кодові відстані від першого та другого фокусів контейнера сусіднього класу R_c^0; r – вектор-реалізація бінарного простору ознак O_b; d_d – відстань до центра гіпереліпсоїдного контейнера в межах класу R_c^0 в просторі ознак O_b; $a(r_{c1}\oplus r)$, $a(r_{c2}\oplus r)$ – відповідно, кодові відстані від першого та другого фокусів контейнера класу R_c^0; δ_n – нормоване поле допусків.

В процесі навчання СІРКЗ визначаються координати вектора параметрів терму (2) при обмеженнях (3). Це, у свою чергу, дає змогу забезпечити max значення усередненого за алфавітом класів ІКФЕ розпізнавання аномалій, загроз або кібератак у КВІС, відповідно:

$$\overline{E}^*=(1/C)\cdot\sum_{c=1}^{C}\max_{\{w\}}E_c, \tag{4}$$

де E_c – значення ІКФЕ навчання СІРКЗ для реалізації класу аномалій або кібератак R_c^0; $\{w\}$ – множина кроків для навчанні СІРКЗ.

У режимі тестової перевірки СІРКЗ приймається рішення про належність реалізацій еталонних образів, що характеризують поточний функціональний стан інформаційної безпеки, до відповідного класу із сформованого на етапі навчання СІРКЗ алфавіту. Тобто, на цьому етапі виконується дефазіфікація нечітких даних – $\left\{R_c^0 \,|\, c=\overline{1,C}\right\}$.

Ініціалізація вхідних некластеризованих даних про ознаки аномалій або кібератак подано у вигляді (векторної) матриці $\left\{z_i^{(j)}, i=\overline{1,N}, j=\overline{1,n}\right\}$.

На наступному етапі роботи алгоритму генеруються матриці нечіткого розбиття:

$$V=\begin{bmatrix} v_{11}\, v_{12}\ldots v_{1n} \\ v_{21}\, v_{22}\ldots v_{2n} \\ \ldots \\ v_{C1}\, v_{C2}\ldots v_{Cn} \end{bmatrix}$$

за умов

$$v_{cj}\in\{0,1\}; \sum_{c=1}^{C}v_{cj}=1; 0<\sum_{j=1}^{n}v_{cj}<n,$$

де v_{cj} – ступінь належності j-го об'єкта до кластеру – с.

Розрахунок центрів кластерів ознак аномалій та кібернападів здійснюється за наступною формулою:

$$z_c=\sum_{j=1}^{n}(v_{cj}^{(l-1)})^s\cdot z^{(j)}\Big/\sum_{j=1}^{n}(v_{cj}^{(l-1)})^s, \tag{5}$$

де l – лічильник кількості ітерацій.

У результаті роботи алгоритму мінімізується цільова функція:

$$J=\sum_{c=1}^{C}\sum_{j=1}^{n}v_{cj}^s\cdot a^2_{K^{(c)}}(z^{(j)},z_c),$$

де

$$K^{(c)}=\frac{\sum_{j=1}^{n}(v_{cj}^{(l-1)})^s\cdot(z^{(j)}-z_c)^T\cdot(z^{(j)}-z_c)}{\sum_{j=1}^{n}(v_{cj}^{(l-1)})^s},$$

де $K^{(c)}$ – коваріація для кластеру – с; T – множина моментів часу зняття інформації.

У разі потреби, виконується переобчислення елементів матриці нечіткого розбиття виконується за наступною формулою:

$$v_{cj}^{(l)}=1\Big/\left[\sum_{w=1}^{C}\left(\frac{a^2_{K^{(c)}}(z^{(j)},z_c)}{a^2_{K^{(c)}}(z^{(j)},z_w)}\right)^{\frac{1}{w-1}}\right]. \tag{6}$$

Перевірку моделі виконано для 5 класів поширених кібератак на КВІС – «відмова в обслуговуванні», «завантаження ворожого ПЗ», «несанкціоноване виконання команд», «порушення прав доступу», «несанкціонований доступ до паролю».

При цьому кількість ознак розпізнавання варіювалась в межах $N=9-15$. Оптимальна кількість кластерів обиралась за max ІКФЕ навчання СІРКЗ, рис. 4. Як показав аналіз результатів, оптимальна кількість кластерів дорівнює $C=3$.

На рис. 5 наведена показана гістограма залежності значення max ІКФЕ для варіантів словників ознак аномалій та кібератак від кількості кроків алгоритму навчання СІРКЗ $\{w\}$, а на рис. 6 наведено залежність ІКФЕ від кількості ознак які використовуються для навчання СІРКЗ.

Аналіз рис. 5 та 6 показує, що досить ефективним в СІРКЗ є використання алгоритму із 5–10 ознаками навчання, тобто для цього випадку ІКФЕ досягає свого максимального значення, що свідчить про побудову безпомилкових за навчальною матрицею вирішальних правил. В режимі тестового навчання СІРКЗ достатня кількість кроків $\{w\}$ для безпомилкового визначення класів аномалій, кіберзагроз або кібератак для КВІС склала $w = 2500 - 3000$.

При побудові алгоритму розпізнавання додавалися представницькі набори більшої довжини, ефективність алгоритму виявлялася такою ж. При додаванні представницьких наборів меншої довжини ефективність алгоритму знижувалася.

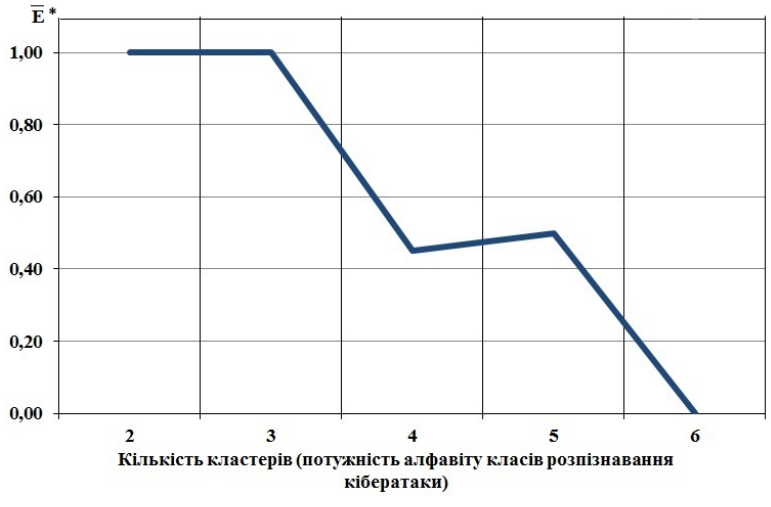

Рис. 4. Оптимальна кількість кластерів для max значення ІКФЕ в процесі навчання СІРКЗ

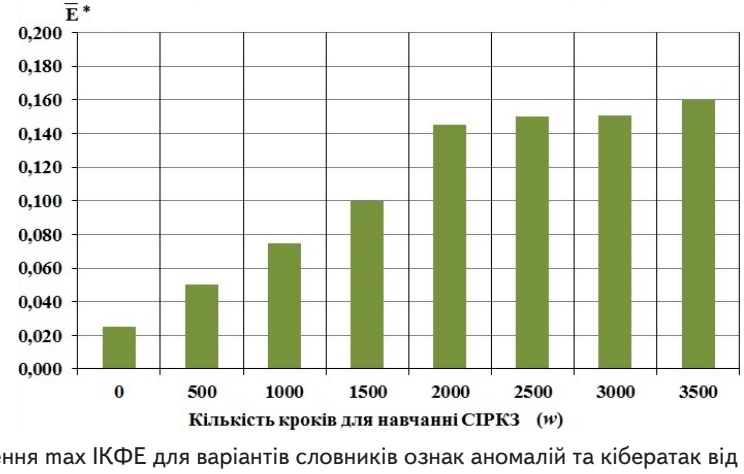

Рис. 5. Залежність значення max ІКФЕ для варіантів словників ознак аномалій та кібератак від кількості кроків алгоритму навчання СІРКЗ

Рис. 6. Графік залежності ІКФЕ від кількості ознак які використовуються для навчання СІРКЗ

6. Обговорення результатів тестування моделі та алгоритму навчання СІРКЗ

Розроблені модель та алгоритм навчання СІРКЗ не тільки становлять самостійний практичний інтерес, але є прикладом створення адаптивних систем кіберзахисту. Зокрема, у порівнянні з результатами отриманими для моделей на основі кінцевих автоматів [11, 12], випадкового відбору [3, 4, 13, 14], нейронних мереж [8, 9] розроблені модель та алгоритм, забезпечують істотно меншу кількість потрібних ознак для класифікації загроз, скорочуючи при цьому час навчання адаптивної СІРКЗ. Також, на відміну від алгоритмів які використовуються для навчання для кінцевих автоматів [11], та випадкового відбору [14], запропонований алгоритм здатен автоматично визначати розміри навчальної та тестової матриць ознак аномалій, кіберзагроз або кібератак, не вимагаючи участі експертів.

Апробація алгоритму здійснювалась лише для відомих класів аномалій та кібератак. Це є певним недоліком дослідження. Для більш складних кібератак та аномалій, вочевидь, потрібно збільшення кількості ознак, а також, кроків алгоритму навчання адаптивної СІРКЗ $w > 3500$, що у свою чергу, підвищує рівень вимог до обчислювальних ресурсів.

Перспективи подальших досліджень полягають у тому, щоб удосконалити базу знань уразливостей, аномалій та кіберзагроз, а також дослідити запропоновані модель та алгоритм на більш широкому класі розпізнавання кібернападів на КВІС.

6. Висновки

В результаті виконаних досліджень:

– розроблена категорійна модель, яка дозволяє на етапі аналізу СІРКЗ для конкретних КВІС, встановлювати відношення між елементами адаптивних систем кіберзахисту;

– розроблено алгоритм навчання СІРКЗ з можливістю гіпереліпсоїдної корекції вирішальних правил, що дозволило створити адаптивний механізм самонавчання системи розпізнавання аномалій, загроз та кібератак у КВІС;

– встановлено, що запропонований алгоритм інформаційно-екстремального навчання СІРКЗ є найбільш ефективним для 3 кластерів в завданнях розбиття простору ознак аномалій та кіберзагроз. При цьому, в режимі тестового навчання СІРКЗ достатня кількість кроків для безпомилкового визначення класів аномалій, кіберзагроз або кібератак склала $w = 2500 - 3000$.

Література

1. Jegede, A. J. Information Security Policy: Relevance, Creation and Enforce-ment [Text] / A. J. Jegede, G. I. O. Aimufua, H. O. Salami // International Journal of Soft Computing. – 2007. – Vol. 2, Issue 3. – p. 408–410.
2. Abidar, R. Intelligent and Pervasive Supervising Platform for Information System Security Based on Multi-Agent Systems [Text] / R. Abidar, K. Moummadi, F. Moutaouakkil, H. Medromi // international review on computers and software. – 2015. – Vol. 10, Issue 1. – p. 44–51. doi: 10.15866/irecos.v10i1.4699
3. Alcaraz, C. Critical Control System Protection in the 21st Century [Text] / C. Alcaraz, S. Zeadally // Computer. – 2013. – Vol. 46, Issue 10. – p. 74–83. doi: 10.1109/mc.2013.69
4. Hassani, A. Integrity-OrBAC: a new model to preserve Critical Infrastructures integrity [Text] / A. A. El Hassani, A. A. El Kalam, A. Bouhoula, R. Abassi, A. A. Ouahman // International Journal of Information Security. – 2015. –Vol. 14, Issue 4. – P. 367–385. doi: 10.1007/s10207-014-0254-9
5. 2015 Attacks Statistics [Electronic resource]. – Available at: http://www.hackmageddon.com/2016/01/11/2015-cyber-attacks-statistics/
6. Дудикевич, В. Б. Проблеми оцінки ефективності систем захисту [Текст] / В. Б. Дудикевич, І. А. Прокопишин, В. Ф. Чекурін // Вісник Національного університету «Львівська політехніка». Сер.: Автоматика, вимірювання та керування. – 2012. – № 741. – С. 118–122.
7. Грищук, Р. В. Атаки на інформацію в інформаційно-комунікаційних системах [Текст] / Р. В. Грищук // Сучасна спеціальна техніка – 2011. – № 1 (24). – С. 61–66.
8. Корченко, А. А. Система формирования нечетких эталонов сетевых параметров [Текст] / А. А. Корченко // Захист інформації. – 2013. – Т. 15, № 3. – С. 240–246.
9. Lahno, V. Ensuring of information processes' reliability and security in critical application data processing systems [Text] / V. Lahno // MEST Journal. – Belgrade. – 2014. –Vol. 2, Issue 1. – P. 71–79. doi: 10.12709/mest.02.02.01.07
10. Manap, N. A. Legal Issues of Data Protection in Cloud Computing [Text] / N. Manap, S.Basir, S. Hussein, P. Tehrani, A. Rouhani // International Journal of Soft Computing. – 2013. – Vol. 8, Issue 5. – P. 371–376.
11. George, J. A. Improving Authentication and Authorization for Identity Based Cloud Environment Using OAUTH with Fuzzy Based Blowfish Algorithm [Text] / J. A. George, M. Hemalatha // international review on computers and software. – 2015. – Vol. 10, Issue 7. – p. 783–788. doi: 10.15866/irecos.v10i7.7062
12. Li, H.-H. Study of Network Access Control System Featuring Collaboratively Interacting Network Security Components [Text] / H.-H. Li, C.-L. Wu // international review on computers and software. – 2013. – Vol. 8, Issue 2. – P. 527–532.
13. Geuna K.Applying Need Pull and Technology Push Theory to Organizational Information Security Management [Text] / K. Geuna, K. Sanghyun // International Business Management. – 2015. – Vol. 9. Issue 4. – p. 524–531.
14. Geetha, R. Secure Communication Against Framing Attack in Wireless Sensor Network [Text] / R. Geetha, E. Kannan // international review on computers and software. – 2015. – Vol. 10, Issue 4. – p. 393–398. doi: 10.15866/irecos.v10i4.5520

15. Shamshirband, S. An appraisal and design of a multiagent system based cooperative wireless intrusion detection computational intelligence technique [Text] / S. Shamshirband, N. B. Anuar, M. L. Kiah, A. Patel, // Engineering Applications of Artificial Intelligence. – 2013. – Vol. 26, Issue 9. – p. 2105–2127. doi: 10.1016/j.engappai.2013.04.010
16. Мірошник, М. А. Розробка методів оцінки ефективності захисту інформації в розподілених комп'ютерних системах [Текст] / М. А. Мірошник // Інформаційно-керуючі системи на залізничному транспорті: науково-технічний журнал. – 2015. – № 4 (113). – С. 39–43.
17. Keunsoo, L. DDoS attack detection method using cluster analysis [Text] / L. Keunsoo, J. Kim, K. Hoon Kwon, Y. Han, S. Kim // Expert Systems with Applications. – 2008. – Vol. 4, Issue 3. – p. 1659–1665. doi: 10.1016/j.eswa.2007.01.040
18. Dilek, S. Applications of artificial intelligence techniques to combating cyber crimes: A review [Text] / S. Dilek, H. Çakır, M. Aydın // International Journal of Artificial Intelligence & Applications. – 2015. – Vol. 6, Issue 1. – P. 21–39. doi: 10.5121/ijaia.2015.6102
19. Patel, A. M. An intrusion detection and prevention system in cloud computing: A systematic review [Text] / A. Patel, M. Taghavi, K. Bakhtiyari, J. Celestino Junior // Journal of Network and Computer Applications. – 2013. – Vol. 36, Issue 1. – P. 25–41. doi: 10.1016/j.jnca.2012.08.007
20. Barman, D. K. Design of Intrusion Detection System Based On Artificial Neural Network and Application of Rough Set [Text] / D. K. Barman, G. Khataniar // International Journal of Computer Science and Communication Networks. – 2012. – Vol. 2, Issue 4. – P. 548–552.
21. Raiyn, J. A survey of Cyber Attack Detection Strategies [Text] / J. Raiyn // International Journal of Security and Its Applications. – 2014. – Vol. 8, Issue 1 –P. 247–256. doi: 10.14257/ijsia.2014.8.1.23
22. Kotenko, I. Integrated repository of security information for network security evaluation [Text] / I. Kotenko, A. Fedorchenko, A. Chechulin // Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA). – 2015. – Vol. 6, Issue 2. – P. 41–57.

Проаналізовано фактори невизначеності у процесі прийняття стратегічних рішень і проведено порівняльний аналіз традиційних статистичних моделей і методів прогнозування. Сформульовано основні завдання прогностичного забезпечення та обґрунтовано необхідність розробки моделі прогностичного забезпечення підтримки прийняття стратегічних рішень для потреб організації. Запропоновано чотирирівневу модель системи із принципами її методичного насичення, а також інструменти її налаштування

Ключові слова: прогностичне забезпечення, підтримка прийняття управлінських рішень, прогнозування, комплексування прогнозних оцінок

Проанализированы факторы неопределённости в процессе принятия стратегических решений и проведён сравнительный анализ традиционных статистических моделей и методов прогнозирования. Сформулированы основные задачи прогностического обеспечения и обоснована необходимость разработки модели прогностического обеспечения поддержки принятия стратегических решений для нужд организации. Предложена четырёхуровневая модель системы с принципами её методического насыщения, а также инструменты её настройки

Ключевые слова: прогностическое обеспечение, поддержка принятия управленческих решений, прогнозирование, комплексирование прогнозных оценок

UDC 658.5:004.94
DOI: 10.15587/1729-4061.2016.66306

FORMATION OF PROGNOSTIC SOFTWARE SUPPORT FOR STRATEGIC DECISION-MAKING IN AN ORGANIZATION

Yu. Romanenkov
PhD, Associate Professor*
E-mail: KhAI.management@ukr.net
V. Vartanian
Doctor of Technical Sciences, Professor*
E-mail: vartanyan_vm@ukr.net
*Department of management
M. E. Zhukovsky National Aerospace University «Kharkiv Aviation Institute»
Chkalova str., 17, Kharkiv, Ukraine, 61070

1. Introduction

The advanced development of modern information technologies and communications systems facilitates a continuous increase of various types of data for monitoring organizational and technical as well as socioeconomic systems that become accumulated in specialized databases, including time series. To various extents, these data reflect the dynamics of multifactor