Метод та моделі адаптивних експертних систем розпізнавання кібератак на основі кластеризації ознак

УДК 004.056

Тарас Петренко[1], Валерій Лахно[2]

[1]Чернігівський національний технологічний університет,
[2]Європейський університет, [1]mail_taras@ukr.net,[2] valss21@ukr.net

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 ІТ-індустрії шкідливі програми, уразливості і 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.

Метою даної роботи є підвищення ефективності систем інтелектуального розпізнавання кібератак, аномалій та загроз для КВІС на основі створення здатної до самонавчання адаптивної експертної системи (АЕС), яка враховує відомі статистичні та дистанційні параметри кластеризації ознак кібернападів, а також, помилки третього роду під час процедури машинного навчання.

Під час досліджень, запропоновано структурну схему здатної до самонавчання адаптивної експертної системи з КБ та розпізнавання кібератак. Вхідний нечіткий розподіл реалізацій об'єктів, які використовуються під час навчання (багатовимірні навчальні матриці ознак), трансформується в чіткий розподіл під час оптимізації перевірочних допустимих відхилень на кожен клас аномалій або кібератак. У результаті відбувається цілеспрямована зміна значень ознак розпізнавання у АЕС для визначених об'єктів та побудова коректних вирішальних правил за багатомірною бінарною навчальною матрицею (ББНМ). Це дає змогу, у рамках 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 ознак) – $\left\| lm_{m,i}^{(j)} \mid m=\overline{1,M}; i=\overline{1,N}, j=\overline{1,n} \right\|$. Для цього: сформульовано словник ознак для кожного класу аномалій, кіберзагроз та атак, а також, алфавіт класів

в термінах об'єктів розпізнавання; визначено мінімальний обсяг репрезентативної навчальної матриці (ОВН); визначено нормовані допустимі відхилення для ознак розпізнавання нелегітимного втручання в роботу КВІС.

Алфавіт класів аномалій, загроз або 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.

Проведені дослідження дозволяють зробити наступні висновки:

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

2. Запропонована модель АЕС у складі СІРКЗ та метод її навчання із використанням процедури нечіткої кластеризації ознак аномалій або кібератак та можливістю гіпереліпсоїдної корекції вирішальних правил, що дозволить створювати адаптивні механізми самонавчання системи інтелектуального розпізнавання кібератак, аномалій та загроз у КВІС.

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