ВІДГУК

офіційного опонента про дисертаційну роботу Петренка Тараса Анатолійовича «Методи та моделі експертних систем розпізнавання кібератак на основі кластеризації реалізацій ознак», подану на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – системи захисту інформації

1. Актуальність теми дисертаційної роботи

Інформаційний вибух останніх років висунув на одне з перших місць проблему кібербезпеки та захисту критично важливих інформаційних систем (КВІС).

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

Відомі наукові праці, в яких доведено, що одним з перспективних напрямків забезпечення кібербезпеки КВІС є впровадження в контури кібербезпеки адаптивних інтелектуальних систем розпізнавання кібератак на основі кластеризації реалізацій ознак, які можуть належати різним класам атак.

Термін «адаптація» для СІРКЗ можна тлумачити як процес цілеспрямованої зміни структури, алгоритму або параметрів системи з метою підвищення ефективності її функціонування. Зокрема, при цьому можна використовувати методи інтелектуальних технологій машинного навчання. У свою чергу, ці технології машинного навчання можуть використовувати моделі, які, ґрунтуються на максимізації інформаційної спроможності СІРКЗ шляхом імплементації в їхній склад експертних систем, які дозволяють виконувати більш детальний аналіз атак на основі кластеризації реалізацій ознак кібератак в межах відомих та нових класів вторгнень.

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

2. Наукова новизна результатів роботи

У роботі досліджено новий підхід щодо підвищення ступеню захищеності КВІС шляхом впровадження в контури захисту експертних систем, здатних розпізнавати складні кібератаки за рахунок кластеризації реалізацій ознак.

Виходячи з того, що нові наукові результати – це нові знання в певній галузі фундаментальних чи прикладних наук, вважати основними науковими результатами дисертації можна наступне:

1. Вперше:

– розроблено модель експертної системи у складі інтелектуальних систем виявлення вторгнень, в 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 під час 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. Достовірність наукових результатів

Достовірність основних наукових результатів роботи підтверджується наведеною в розд. 2, 3 і 4 системою формальних методик і перетворень, що не містить принципових помилок, а також рядом прикладів, результатами комп'ютерного тестування з використанням загальновизнаних наборів тестів.

4. Цінність дисертаційної роботи для науки

Цінність дисертації полягає в тому, що в ній запропоновано нове рішення важливої науково-технічної 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. Наведені в роботі методи, моделі та алгоритми, що їх реалізують, не були відомі раніше.

5. Практична цінність роботи

Практична корисність роботи обумовлена тим, що використання запропонованих в ній моделей, формальних методів і конкретних рішень дозволяє отримувати більш досконалі, порівняно з відомими, засоби розпізнавання кібератак на критично важливі інформаційні систем.

Результати роботи впроваджено в науково-технічних розробках ТОВ «Захист інформації» (акт №134 від 16.11.2018р.) та у навчальний процес у Чернігівському національному технологічному університеті (акт №9 від 5.09.2018р.), а також у Національному авіаційному університеті (акт від 3.09.2018р.).

6. Структура роботи

Дисертаційна робота містить вступ, 4 розділи, висновки, перелік використаних джерел і додатки.

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.

У третьому розділі запропоновано метод навчання експертної системи (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.

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 атак у КВІС; отримувати експертну інформацію про стан

комп'ютерів у мережі та ін.

У додатках подано коди експертної системи «Analyzer of cyberthreats» та акти про впровадження результатів дисертаційного дослідження.

7. Публікації за темою дисертації

Наукові положення дисертації, що пов'язані з розробкою методів та моделей для експертних систем із розпізнавання кібератак на основі кластеризації реалізацій ознак, достатньо повно відображені в публікаціях автора і пройшли апробацію на міжнародних науково-технічних конференціях.

8. Автореферат дисертації

Автореферат дисертації за своїм змістом повністю відповідає дисертаційній роботі.

Оформлення дисертації та автореферату відповідає вимогам, що висуваються до наукових праць. Зміст автореферату відповідає принциповим положенням дисертації.

9. Зауваження щодо змісту дисертаційної роботи

1. У списку використаних джерел відсутні деякі відомі роботи із проблематики розпізнавання кібератак.

2. Автор використовує два поняття адаптивна система розпізнавання та система інтелектуального розпізнавання атак та загроз. Бажано навести більш ґрунтовні пояснення у чому полягає відмінність між цими термінами в контексті мети роботи.

3. У таблиці 2.4 наведено далеко не повний перелік основних джерел даних для адаптивних систем розпізнавання атак. При цьому немає роз'яснення до яких класів належать ці кібератаки.

4. У розділі 2 роботи немає прикладів, яким чином виконується процедура корекції вирішальних правил розпізнавання для атак, які належать для різних класів.

5. У табл. 3.4, яка містить базу знань експертної системи для об'єктів розпізнавання кібертатак, не вказано одиницю вимірювання наведених ознак атрибутів для відповідних класів атак, що не сприяє розумінню висунутих гіпотез для розпізнавання.

6. Наведена на рис. 3.3. схема для імітаційної моделі містить лише 3 робочі станції у складі сегменту критично важливої інформаційної системи. Не зрозуміло чому автор не збільшив цю кількість, наприклад, до 10-15 станції, що більш притаманне сегменту КВІС?

10. Загальна оцінка дисертації

Дисертаційна робота Петренка Т.А. є завершеною науковою працею, в якій отримані нові науково обґрунтовані результати, що в сукупності вирішують важливу науково-прикладну задачу підвищення ефективності систем інтелектуального розпізнавання кібератак на критично важливі інформаційні системи

Вважаю, що за актуальністю вибраної теми, обсягом і рівнем виконаних теоретичних і експериментальних досліджень, достовірністю і обґрунтованістю висновків, новизною досліджень, значенням отриманих результатів для науки і практики дисертаційна робота задовольняє вимогам п. 9, 10, 12 «Порядку присудження наукових ступенів», затвердженого постановою КМУ від 19 серпня 2015 року № 656, а її автор Петренко Тарас Анатолійович заслуговує присудження наукового ступеня кандидата технічних наук зі спеціальності 05.13.21 – системи захисту інформації.

Офіційний опонент:

Іванченко Є.В. к.т.н., доцент, професор кафедри
безпеки інформаційних технологій
Національного авіаційного університету

Підпис Іванченко Є.В.
засвідчую
Вчений секретар
Національного авіаційного університету
Сичева
06.06.2019р

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
01132330
МІСТО КИЇВ