МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ
ВІЙСЬКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ ТА ІНФОРМАТИЗАЦІЇ ІМЕНІ ГЕРОЇВ КРУТ
Код 24978555
«05» 04 2021 р.
№ 1/12/1/963
01101, м. Київ

Голові спеціалізованої вченої ради Д 26.861.06 Державного університету телекомунікацій

вул. Солом'янська, 7, м. Київ, 03110

ВІДГУК
офіційного опонента

начальника кафедри автоматизованих систем управління факультету інформаційних технологій Військового інституту телекомунікацій та інформатизації імені Героїв Крут, доктора технічних наук, старшого наукового співробітника полковника Сови Олега Ярославовича на дисертацію Охрімчука Володимира Васильовича на тему "Метод побудови шаблонів потенційно небезпечних кібератак на комп'ютерні системи та мережі військового призначення", поданої ним на здобуття наукового ступеня кандидата технічних наук за спеціальністю 21.05.01 – інформаційна безпека держави

Актуальність теми. Суттєве зростання ролі комп'ютерних систем та мереж військового призначення в сучасних війнах та локальних збройних конфліктах як в Україні, так і в світі висуває все новіші вимоги до забезпечення захищеності їх від кібератак.

Сьогодні для порушення нормальних умов функціонування об'єктів з критичною інфраструктурою держави, до яких також відносяться комп'ютерний системи та мережі Збройних Сил України, зловмисником або протиборчою стороною здійснюються кібератаки з використанням спеціальних зразків шкідливого програмного забезпечення – кіберзброї, яка як правило націлена на експлуатацію вразливості нульового дня "Zero-day". Для комп'ютерних систем та мереж військового призначення реалізація таких та інших потенційно небезпечних кібератак є неприпустимою, оскільки зрив процесів управління в таких системах призведе до невиконання ними завдання за призначенням.

Відомі на даний час технології, які покладені в основу функціонування систем інформаційної безпеки комп'ютерних систем та мереж військового призначення, ґрунтуються в більшості на сигнатурних підходах до побудови шаблонів кібератак. Такі технології характеризуються наявністю "ефекту запізнення" з вироблення потрібної сигнатури, що суттєво знижує захищеність комп'ютерних систем та мереж військового призначення від потенційно небезпечних кібератак, особливо тих з них, які мають високу технологічну складність.

Вхідний ДУТ № 502
«06» 04 2021 р.

Враховуючи вищезазначене, дисертаційне дослідження, пов'язане з розробкою методу побудови шаблонів потенційно небезпечних кібератак на комп'ютерні системи та мережі військового призначення, є актуальним на даному етапі розвитку систем та засобів кіберзахисту.

Наукова новизна одержаних здобувачем результатів полягає у наступному:

набула подальшого розвитку теоретико-множинна модель шаблону потенційно небезпечної кібератаки на комп'ютерну систему або мережу військового призначення, яка відрізняється від відомих технологією комплексування джерел первинних даних, таких як: бази шаблонів атак (KDD-99 та CAPEC), бази вразливостей і дефектів (CVE) – що дозволяє у формалізованому вигляді подати шаблон потенційно небезпечної кібератаки як булеву модель пошуку інформації, перетини множин якої відповідають множинам середовищ, об'єктів та суб'єктів кібератаки;

набула подальшого розвитку узагальнена диференціально-ігрова модель шаблону потенційно небезпечної кібератаки на комп'ютерну систему та мережу військового призначення, яка на відміну від відомої, ґрунтуючись на деннінговій моделі захисту інформації, враховує найслабшу ланку в складі СІБ – програмні засоби захисту – й дозволяє в умовах апріорної невизначеності з позицій атакуючого оцінити незахищеність від потенційно небезпечної кібератаки;

вперше розроблено метод побудови шаблонів потенційно небезпечних кібератак на комп'ютерні системи та мережі військового призначення, який ґрунтується на одночасному визначенні базових характеристик і параметрів (ознак) потенційно небезпечної кібератаки на основі всебічного аналізу стандартного функціонального профілю захищеності, реалізованого в комп'ютерних системах та мережах, й джерел первинних даних – баз шаблонів атак (KDD-99 та CAPEC), баз вразливостей і дефектів (CVE), – що дозволяє нівелювати вплив "ефекту запізнення" в ході їх створенні.

Ступінь обґрунтованості наукових положень, висновків і рекомендацій, сформульованих у дисертації, достовірність одержаних результатів. Обґрунтованість положень і висновків обумовлена вибором адекватних методів дослідження, використанням сучасного апробованого математичного апарата, ясним фізичним трактуванням результатів досліджень та їх несуперечністю відомим даним.

Достовірність наукових положень дисертаційної роботи підтверджується:

коректною постановкою наукового завдання та часткових наукових задач дисертаційного дослідження (с. 23, 67-70);

використанням в роботі теоретично обґрунтованих та широко апробованих на практиці методів системного аналізу, експертних оцінок, методів теорії графів, диференціальних перетворень, математичного та комп'ютерного модулювання;

збіжністю результатів моделювання та експериментальних перевірок з відомими експериментальними даними інших академічних досліджень, відповідністю отриманих теоретичних результатів з результатами експерименту (с. 117–130);

несуперечністю наукових положень основним законам і явищам природи.

Практичне значення отриманих результатів полягає в наступному:

застосування булевої моделі пошуку для визначення ознак потенційно небезпечних кібератак дає змогу автоматизувати даний процес шляхом програмної реалізації алгоритмів пошуку;

застосування диференціально-ігрової моделі шаблону потенційно небезпечної кібератаки на практиці дає змогу підвищити оперативність її виявлення в комп'ютерних системах та мережах військового призначення до 1,6 раза (з $0{,}58 \cdot T$ с до $0{,}37 \cdot T$ с);

розроблений метод дає змогу до 15% підвищити ефективність виявлення потенційно небезпечних кібератак на комп'ютерні системи та мережі військового призначення військового призначення в порівнянні з найкращими з діючих зразків СІБ, які застосовуються на практиці, зокрема *NOD32 Eset*.

Практична значущість одержаних результатів і достовірність наукових положень підтверджені актами впровадження (копії – с. 161–164). Зазначені факти підтверджують особистий внесок здобувача в науку.

Мова та стиль викладення дисертації та автореферату дозволяють зрозуміти суть розроблених наукових положень і одержаних практичних результатів. Дисертація у цілому відповідає вимогам, які ставляться до її оформлення відповідно до Порядку присудження наукових ступенів, затвердженого Постановою Кабінету Міністрів України від 24 липня 2013 р. № 567 (зі змінами) та Вимог до оформлення дисертації, затверджених наказом Міністерства освіти і науки України від 12.01.2017 р. № 40. Зміст дисертації викладено послідовно та логічно.

Повнота викладу основних результатів дисертації в наукових фахових виданнях. За напрямом дисертаційного дослідження здобувачем опубліковано 25 праць, з яких, 10 статей (9 статей у фахових наукових виданнях України, 1 – у міжнародному рецензованому виданні, яке входить до наукометричної бази SCOPUS, 3 статті написані без співавторів), 15 публікацій у матеріалах і збірниках тез міжнародних і регіональних конференцій.

Перелічені публікації з достатньою повнотою відбивають наукові та практичні результати дисертації та у цілому відповідають вимогам до публікацій результатів дисертації на здобуття наукового ступеня кандидата технічних наук, які висуваються згідно Порядку присудження наукових ступенів, затвердженого Постановою Кабінету Міністрів України від 24 липня 2013 р. № 567 (зі змінами). З праць, що їх опубліковано у співавторстві, у дисертації використано лише ті результати, які отримано здобувачем самостійно.

Оцінка змісту дисертації, її завершеність в цілому, відповідність встановленим вимогам оформлення дисертації. Дисертація Охрімчука В.В., подана на здобуття наукового ступеня кандидата технічних наук, за своїм змістом та отриманими науковими результатами, відповідає спеціальності 21.05.01 – інформаційна безпека держави (п. 6: науково-методичне забезпечення функціонування системи інформаційної безпеки держави. Рівні захищеності інформаційних систем. Розробка моделей загроз, критеріїв та показників оцінки уразливості інформаційних систем і мереж, дослідження

джерел загроз. Розробка методик та інструментарію оцінки стану інформаційної безпеки як складової національної безпеки України).

В ході вирішення поставленого наукового завдання автор дотримувався системного підходу, який передбачає: аналіз методів та моделей, покладених в основу функціонування сучасних систем інформаційної безпеки; розробку нових та розвиток існуючих моделей та методу побудови шаблонів потенційно небезпечних кібератак на комп'ютерні системи та мережі військового призначення; верифікацію розроблених моделей та методу.

Дисертація виконана на достатньо високому науковому рівні, відповідає вимогам Міністерства освіти і науки України щодо написання кандидатських дисертацій. Зміст автореферату відповідає основним положенням, рекомендаціям та висновкам дисертації. Автореферат написано лаконічно та в стислій формі.

Зауваження щодо змісту та оформлення дисертації. Не зважаючи на високий науковий та практичний рівень, дисертаційна робота має низку недоліків:

1. Під час оформлення тексту дисертації та автореферату здобувач не зовсім коректно оперує категорією "потенційно небезпечна кібератака". На наш погляд, в роботі доцільно було б привести обґрунтування даної категорії, або використовувати загальновживане поняття – кібератака нульового дня.

2. У другому розділі, на с. 71, здобувач приводить досить велику кількість баз первинних даних для побудови шаблону потенційно небезпечної кібератаки. При цьому автор не обґрунтовує критерій або правило вибору серед них тих, які покладено в основу подальших досліджень, а саме KDD-99, CVE, CAPEC та відомості про стандартні функціональні профілі захищеності. Також в дисертації та в авторефераті у другому розділі не знайшла місце відповідь на питання, яким чином комплексуються різноформатні вхідні дані.

3. З дисертації дещо проблемно встановити, який конкретно клас систем інформаційної безпеки розглядається у якості механізму захисту комп'ютерних систем та мереж військового призначення від потенційно небезпечних кібератак адже, як відомо, їх на сьогодні досить багато, зокрема, засоби антивірусного програмного забезпечення, міжмережеві екрани, системи виявлення атак, системи виявлення вторгнень або інші.

4. Визначаючи елементи кортежу на с. 95 дисертації, здобувач застосовує низку правил та критеріїв до елементів множини (2.17). При цьому він не розкриває ні правила, ні критерії. Таке подання моделі суттєво ускладнює її практичне застосування, адже побудова шаблона потенційно небезпечної кібератаки тоді зведеться до використання методу проб та помилок. Враховуючи значну небезпеку від кібератаки нульового дня, вважається за доцільне більш ґрунтовне розкриття правил визначення елементів кортежу, щоб звести кількість помилок першого роду і другого роду до мінімуму.

5. При викладенні результатів другого розділу здобувач спирається на модель захисту інформації Деннінга, що на наш погляд є цілком закономірним та правильним. Але, на с. 99, при подальшій побудові узагальненої диференціально-ігрової моделі шаблону потенційно небезпечної кібератаки з усієї множини розглянутих рівнів захисту розглядає лише один з них –

програмні засоби системи інформаційної безпеки. Як наслідок залишається низка питань: чому обраний саме цей рівень; як зміниться шаблон потенційно небезпечної кібератаки, якщо буде розглянуто інші рівні моделі Деннінга. Даний недолік характерний і автореферату.

Разом з тим, зазначені недоліки не впливають на якість подання дисертації, а їх наявність не знижує практичної, а тим паче наукової цінності одержаних здобувачем результатів.

Загальний висновок. Отже, на основі критичного вивчення дисертації та праць здобувача, опублікованих за темою, об'єктивно встановлено:

дисертаційна робота Охрімчука В.В. на тему "Метод побудови шаблонів потенційно небезпечних кібератак на комп'ютерні системи та мережі військового призначення" відповідає вимогам Порядку присудження наукових ступенів, затвердженого Постановою Кабінету Міністрів України від 24.07.2013 № 567 (із змінами), а також вимогам наказу Міністерства освіти і науки України від 12 січня 2017 р. № 40 "Про затвердження Вимог до оформлення дисертації";

дисертаційна робота відповідає паспорту спеціальності 21.05.01 – інформаційна безпека держави та профілю спеціалізованої вченої ради Д 26.861.06;

використання чужих наукових результатів без посилань на авторів у дисертації не виявлено, що свідчить про особистий внесок здобувача в науку. Автореферат ідентичний дисертації;

дисертація Охрімчука В.В. є завершеною кваліфікаційною науковою працею, що місить нові науково обґрунтовані результати проведених ним досліджень, які вирішують конкретне наукове завдання, що полягає у підвищенні рівня захищеності комп'ютерних систем та мереж військово призначення від потенційно небезпечних кібератак шляхом розроблення методу побудови їх шаблонів;

автор дисертації, Охрімчук Володимир Васильович, заслуговує присудження наукового ступеня кандидата технічних наук за спеціальністю 21.05.01 – інформаційна безпека держави.

Офіційний опонент –
начальник кафедри автоматизованих систем управління
факультету інформаційних технологій
Військового інституту телекомунікацій та інформатизації імені Героїв Крут
доктор технічних наук, старший науковий співробітник

Олег СОВА

05.04.2021

Підпис офіційного опонента О. Сови засвідчую.
Начальник відділу персоналу та стройового

Сергій ЛИСЕНКО

05.04.2021