Голові спеціалізованої вченої ради
ДФ 26.133.056 у Київському столичному університеті імені Бориса Грінченка
доктору технічних наук, професору
професору кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського столичного університету імені Бориса Грінченка
Гулаку Геннадію Миколайовичу

Отримано
22.01.2024
Голова спеціалізованої
вченої ради
ДФ 26.133.056
д.т.н., проф.
І.М. Гулак

ВІДГУК

офіційного опонента **ОППРСЬКОГО Івана Романовича**, доктора технічних наук, професора, завідувача кафедри захисту інформації Національного університету «Львівська політехніка», на дисертацію **ВОРОХОБА Максима Віталійовича «Моделі і методи вдосконалення політики інформаційної безпеки підприємства на основі методології Zero Trust»** подану на здобуття ступеня доктора філософії за спеціальністю 125 Кібербезпека та захист інформації

1. Актуальність теми дослідження.

Дослідження механізмів, методів та систем ефективного функціонування організацій з точки зору інформаційної безпеки є актуальною та важливою проблемою у сучасному інформаційному світі. Руйнування інформаційного ресурсу, його тимчасова недоступність або несанкціоноване використання можуть завдати організації значних матеріальних збитків, а складність мережевої інфраструктури, різноманіття даних і додатків призводять до того, що при реалізації системи інформаційної безпеки за межами уваги адміністраторів безпеки можуть виявитися багато загроз. Безпека мережі на основі периметра також є недостатньою, бо як тільки зловмисники порушують периметр, подальший бічний рух стає безперешкодним. Така ситуація вимагає більш надійних механізмів захисту інформації, забезпечення її конфіденційності, доступності та цілісності.

Нульова довіра (zero-trust) є відповіддю на тенденції корпоративної мережі, які включають віддалених користувачів, використання власного пристрою і хмарних активів, що розташовані за межами корпоративної мережі. Нульова довіра зосереджена на захисті ресурсів, а не на сегментах мережі, оскільки мережеве

розташування більше не вважається основним компонентом безпеки ресурсу. У разі нульової довіри засоби захисту зазвичай передбачають мінімізацію доступу до ресурсів, а також постійну автентифікацію та авторизацію ідентифікації та безпеки кожного запиту на доступ. Проте складна реалізація та використання ресурсів, а також громіздкі процеси входу та помилкові спрацьовування є перешкодою у широкому застосуванні на практиці. Тому дане дослідження може стати запорукою політики інформаційної безпеки підприємств та стимулом для формулювання нових стратегій управління ризиками інформаційної безпеки, які б відповідали викликам загроз, що постійно еволюціонують.

Таким чином, вивчення методів та моделей на основі методології zero-trust стає необхідним елементом методологічної основи концепції інформаційної безпеки підприємства.

2. Зв'язок теми дисертаційної роботи з науковими планами, програмами, фундаментальними та прикладними дослідженнями

Дисертація виконана на кафедрі інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Київського університету імені Бориса Грінченка відповідно до теми науково-дослідної роботи та індивідуального плану аспіранта Київського університету імені Бориса Грінченка. Напрям дисертаційного дослідження безпосередньо пов'язаний з реалізацією доктрини інформаційної безпеки України, Стратегії інформаційної безпеки та Стратегії кібербезпеки України. Дисертаційна робота виконана відповідно до планів наукової і науково-технічної діяльності Київського університету імені Бориса Грінченка в рамках науково-дослідної роботи: «Методи та моделі забезпечення кібербезпеки інформаційних систем переробки інформації та функціональної безпеки програмно-технічних комплексів управління критичної інфраструктури» (№ 0122U200483, КУБГ, м. Київ).

3. Ступінь обґрунтованості наукових положень, висновків і рекомендацій та їхня достовірність

Зміст дисертаційної роботи повною мірою розкриває тему наукового

дослідження та відповідає визначеним меті, завданням, об'єкту та предмету дослідження. Розроблені автором і викладені у дисертаційній роботі наукові положення, висновки та рекомендації є аргументованими та обґрунтованими, сформульовані чітко, логічно і послідовно.

Отримані наукові результати та висновки дисертаційної роботи характеризуються належним рівнем обґрунтованості та достовірності, оскільки при її підготовці:

1) опрацьовано значну кількість літературних джерел зарубіжних і вітчизняних вчених, проаналізовано нормативно-правове забезпечення та приділено значну увагу дослідженню та можливості впровадження іноземного досвіду;

2) використано широкий спектр загальнонаукових і спеціальних методів дослідження – індукції і дедукції, логічного узагальнення, аналізу і синтезу, наукового абстрагування та системного підходу, а також методи теорії ризиків, теорії ймовірностей та математичної статистики; методи моделювання систем управління інформаційною безпекою;

3) вміло використано значний масив статистичного і фактологічного матеріалу, який якісно опрацьовано і подано в таблицях;

4) здійснена солідна апробація результатів дослідження, про що свідчить перелік наукових праць здобувача;

5) результати наукових досліджень прийняті до впровадження в діяльність Інституту програмних систем Національної академії наук України, та Інституту телекомунікацій та глобального інформаційного простору Національної академії наук.

Дисертаційна робота Ворохоба М.В. є оригінальною науковою працею, яка виконана на належному теоретичному та методичному рівнях. Робота має послідовну та логічну структуру і є комплексним, завершеним науковим дослідженням. Зміст роботи та багатогранність висвітленої проблеми свідчать про високий рівень наукової компетентності автора.

Викладене вище дає можливість висловити позитивний висновок стосовно наукового рівня, достовірності подання в дисертації матеріалу, теоретичних

обґрунтувань і аргументації всіх положень, практичного значення висновків і рекомендацій.

4. Новизна наукових положень, висновків і рекомендацій, сформульованих у дисертації

У дисертаційній роботі Ворохоба М.В. сформульовано та обґрунтовано ряд наукових положень, висновків і рекомендацій, які відзначаються наявністю наукової новизни. До положень, що відображають наукову новизну дисертаційного дослідження, можна віднести результати, отримані дисертантом самостійно, а саме:

- запропоновано та математично обґрунтовано метод автентифікації користувачів корпоративної мережі на основі стеганографічного протоколу обміну даними автентифікації згідно з політикою безпеки з урахуванням концепції zero-trust;

- вдосконалена методика формування вихідних вимог щодо побудови безконтактного апаратного засобу автентифікації користувачів корпоративної мережі на основі технології RFID;

- подальшого розвитку набула методика оперативної оцінки поточного стану корпоративної кіберкультури на основі анкетування персоналу та математичного апарату обробки даних анкетування.

Слід підкреслити, що отримані результати розширюють попередні наукові дослідження проблем захисту інформації на основі методології zero-trust.

5. Теоретична цінність і практична значущість наукових результатів.

Проведене Ворохобом М.В. дослідження має як теоретичне, так і прикладне значення, що є певним внеском дисертанта в кібербезпеку, а саме, в частині проблематики захисту інформації на основі методології zero-trust.

Теоретичне значення розробок визначається в розширенні та уточненні політик безпеки підприємства, систематизації загроз безпеки інформаційних активів підприємства на основі концепції zero-trust та визначенні вимог до оцінки рівня культури кібербезпеки.

Практична значущість дослідження полягає у розробці методу автентифікації користувачів корпоративної мережі на основі стеганографічного протоколу обміну даними автентифікації згідно з політикою безпеки з урахуванням концепції zero-trust. Практичні рішення наукових досліджень прийняті до впровадження в діяльність Інституту програмних систем Національної академії наук України (акт від 18.09.2023 року), Інституту телекомунікацій та глобального інформаційного простору Національної академії наук України (акт від 20.09.2023 року).

Запропоновані рішення можуть використовуватися для таких галузей як телемедицина, дистанційне управління засобами фізичної безпеки та охорони, систем дистанційної освіти тощо.

6. Повнота викладення наукових результатів дисертації в опублікованих працях.

Результати дисертаційної роботи, висновки та рекомендації знайшли відображення в іноземних та вітчизняних наукових виданнях.

За темою дослідження опубліковано 11 наукових праць, з них 8 опубліковані у спеціалізованих фахових виданнях, затверджених наказом МОН України та 3 опубліковано у закордонному науковому виданні, що входить до наукометричної бази Scopus.

Слід відзначити належний рівень апробації досліджень на та їх представлення на конференціях та семінарах, зокрема на чотирьох Workshop on Cybersecurity Providing in Information and Telecommunication Systems (Scopus) та 3 конференціях.

Обсяг і зміст опублікованих праць свідчать, що в них висвітлені основні положення проведеного наукового дослідження, які були апробовані й отримали позитивну оцінку на наукових заходах різних рівнів. У роботах, опублікованих у співавторстві, зазначено особистий внесок здобувача.

7. Відсутність (наявність) порушення академічної доброчесності.

Аналіз тексту дисертації, а також публікації здобувача свідчать про відсутність ознак порушення вимог академічної доброчесності. Зокрема, дисертаційна робота містить посилання на джерела інформації у випадку

використання ідей, розробок, тверджень, відомостей; відповідає нормам законодавства про авторське право і суміжні права; відображає прагнення автора надати достовірну інформацію про результати власної наукової діяльності, використані методики досліджень та інформаційні ресурси. Посилання на першоджерела є коректними, навмисних спотворень не виявлено.

8. Дискусійні положення та недоліки дисертаційної роботи.

1. Автором проведений аналіз переваг та недоліків впровадження методології zero-trust у політику безпеки організацій. Водночас дослідження набуло б більшого науково-практичного значення, якби дисертант узагальнив отримані результати в частині виокремлення конкретних проблем організацій, які застосовували дану методологію.

2. Безумовно актуальними та практично спрямованими є пропозиції автора щодо оцінки поточного стану корпоративної кіберкультури на основі анкетування персоналу та математичного апарату обробки даних анкетування. Такі пропозиції автора носили б більш завершений формат, якщо б було чітко визначено, які саме структури мали б виконувати ці функції та нести відповідальність за надання своєчасної та якісної інформації, а також при проведенні анкетування використовувати психологічні методи для профілювання особистості.

3. У третьому розділі дисертаційної роботи абсолютно вірно наголошено про загрози та ризики в системі захисту, які може нести штучний інтелекту. Проте ця теза не набула подальшого розвитку та належного обґрунтування в частині механізму функціонування на основі методології zero-trust.

4. Текст дисертаційної роботи містить ряд помилок і зауважень технічного характеру:

- у твердженні 2 на ст. 129 стверджується про рівномірний розподіл бітів та відповідну оцінку, а в наступному твердженні визначається, що ця оцінка не залежить від розподілу;
- на рис 3.4 блок-схема представлена англійською мовою;
- формула 3.13 містить у дужках невірний знак, останній одночлен має містити знак мінус;

- схеми виконані не в одному стилі.

Наведені зауваження і дискусійні моменти вказують на деякі суперечливі аспекти дослідження, проте загалом вони засвідчують складність і багатогранність обраної теми, її практичну важливість та актуальність і суттєво не впливають на якісні характеристики дисертаційної роботи.

9. Загальна оцінка дисертаційної роботи, її відповідність встановленим вимогам.

Дисертаційна робота Ворохоба Максима Віталійовича на тему «Моделі і методи вдосконалення політики інформаційної безпеки підприємства на основі методології Zero Trust» є завершеним науковим дослідженням, яке за актуальністю, достовірністю отриманих результатів, їхньою науковою новизною і практичною цінністю відповідає вимогам «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», затвердженого Постановою Кабінету Міністрів України від 12 січня 2022 року №44, а її автор, Ворохоб Максим Віталійович, заслуговує на присудження ступеня доктора філософії за спеціальністю 125 Кібербезпека та захист інформації.

Офіційний опонент:
доктор технічних наук, професор
завідувач кафедри захисту інформації
Національного університету
«Львівська політехніка» Іван ОПІРСЬКИЙ

Підпис професора Опірського І.Р. засвідчую
Вчений секретар Національного університету
«Львівська політехніка», к.т.н., доцент Роман БРИЛИНСЬКИЙ