Рішення разової спеціалізованої вченої ради ДФ 26.133.056
про присудження ступеня доктора філософії

Разова спеціалізована вчена рада ДФ 26.133.056 Київського столичного університету імені Бориса Грінченка виконавчого органу Київської міської ради (Київської міської державної адміністрації), місто Київ, прийняла рішення про присудження ступеня доктора філософії з галузі знань 12 Інформаційні технології на підставі прилюдного захисту дисертації Ворохоба Максима Віталійовича «Моделі і методи вдосконалення політики інформаційної безпеки підприємства на основі методології Zero Trust» за спеціальністю 125 Кібербезпека та захист інформації 13 лютого 2024 року.

Ворохоб Максим Віталійович, 1995 року народження, громадянин України, освіта вища: 2019 році закінчив магістратуру Державного університету телекомунікацій за спеціальністю «Телекомунікації та радіотехніка».

З 2023 року і дотепер працює на посаді викладача кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського столичного університету імені Бориса Грінченка.

Дисертацію виконано в Університеті Грінченка.

Науковий керівник: Складанний Павло Миколайович, кандидат технічних наук, доцент, завідувач кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського столичного університету імені Бориса Грінченка.

Здобувач має 11 наукових публікацій за темою дисертації, із них усі у співавторстві: 8 статтей – у наукових виданнях, включених на дату

опублікування до переліку наукових фахових видань України; 3 статті (Scopus), у яких додатково висвітлено результати дисертації.

1. Літвінчук, І., Корчомний, Р., Коршун, Н., & Ворохоб, М. (2020). Підхід до оцінювання ризиків інформаційної безпеки для автоматизованої системи класу «1». Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(10), 98–112. https://doi.org/10.28925/2663-4023.2020.10.98112

2. Літвінчук, І., Коршун, Н., & Ворохоб, М. (2020). Спосіб оцінювання інтегрованих систем безпеки на об'єкті інформаційної діяльності. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(10), 135–143. https://doi.org/10.28925/2663-4023.2020.10.135143

3. Черненко, Р., Рябчун, О., Ворохоб, М., Аносов, А., & Козачок, В. (2021). Підвищення рівня захищеності систем мережі інтернету речей за рахунок шифрування даних на пристроях з обмеженими обчислювальними ресурсами. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(11), 124–135. https://doi.org/10.28925/2663-4023.2021.11.124135

4. Скітер, І., & Ворохоб, М. (2021). Модель оцінки рівня культури кібербезпеки в інформаційній системі. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(13), 158–169. https://doi.org/10.28925/2663-4023.2021.13.158169

5. Добришин, Ю., Сидоренко, С., & Ворохоб, М. (2023). Автоматизована система підтримки прийняття рішення щодо відновлення пошкодженого програмного забезпечення внаслідок впливу кібератак. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 4(20), 174–182. https://doi.org/10.28925/2663-4023.2023.20.174182

6. Ворохоб, М., Киричок, Р., Яскевич, В., Добришин, Ю., & Сидоренко, С. (2023). Сучасні перспективи застосування концепції Zero Trust при побудові політики інформаційної безпеки підприємства. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(21), 223–233. https://doi.org/10.28925/2663-4023.2023.21.223233

7. Скіцько, О., Складанний, П., Ширшов, Р., Гуменюк, М., & Ворохоб, М. (2023). Загрози та ризики використання штучного інтелекту. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(22), 6–18. https://doi.org/10.28925/2663-4023.2023.22.618

8. Крючкова, Л., Складанний, П., & Ворохоб, М. (2023). Передпроєктні рішення щодо побудови системи авторизації на основі концепції Zero Trust. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(19), 226–242. https://doi.org/10.28925/2663-4023.2023.13.226242

У дискусії взяли участь голова і члени разової спеціалізованої вченої ради:

Гнатюк Сергій Олександрович – доктор технічних наук, професор, декан Факультету комп'ютерних наук та технологій, Національний авіаційний університет.

1. Перший розділ дисертації традиційно присвячений критичному аналізу сучасних підходів (висвітлених у працях вітчизняних і закордонних науковців) до вирішення поставленого завдання. Проте, вкінці аналізу відсутнє порівняння зазначених підходів, що у певній мірі ускладнює оцінку та розуміння поточного стану справ у предметній області та доцільність розроблення нових методів та моделей.

2. Другий розділ дисертаційної роботи починається з аналізу трендів загроз кібербезпеки, який, на мою думку, мав би бути здійснений у першому розділі роботи. У другому і наступних розділах, як правило, представляються наукові та практичні результати дисертанта.

3. Наукова новизна сформульована не у повній мірі відповідно вимог та рекомендацій. Наприклад, не у кожному пункті зрозуміло аз рахунок чого досягається вказаний ефект, а також в пп.2-3 «методика» вказана як науковий результат, хоча це не зовсім коректно.

4. В моделі формування системи кібербезпеки на підсистему кадрового забезпечення впливають вимоги R2 щодо побудови підсистем кіберзахисту - не зрозуміло, який характер вимог (динамічний чи статичний).

5. В онтологічній моделі формування вимог в системі управління інформаційною безпекою наявні корегуючі впливи на політику безпеки збоку концепції Zero Trust та з боку процедур оцінки відповідності не описано чи ці процеси можуть мати конфліктний характер.

6. З метою покращення безпекової ситуації та нейтралізації існуючих уразливостей автором запропоновано розглянути низку рішень, зокрема, застосовувати чинники особистості співробітника, які не потребують складних технологій, але не запропоновано конкретного рішення.

7. У підрозділі 3.4 запропоновано використання системи штучного інтелекту для управління ризиками, які виникають внаслідок використання системи штучного інтелекту, проте у тексті дисертації не описано питання яким чином має бути створена початкова безпечна система штучного інтелекту, яка буде контролювати ризики інших систем.

8. У висновках до роботи відсутні кількісні показники, що ускладнює оцінювання ефективності запропонованих методів і моделей у порівнянні з раніше відомими. Наприклад, не зрозуміло на скільки дисертанту вдалось підвищити ефективність підсистеми ідентифікації і автентифікації (п. 2 наукової новизни).

9. У роботі наведено багато статистичних даних кібербезпеки 2020-2021 років, проте від початку повномасштабного вторгнення російської федерації (з лютого 2022 року) в галузі кібербезпеки багато що змінилось, як в Україні так і в світі.

10. У дисертації присутня не значна кількість орфографічних, пунктуаційних та лексичних помилок (наприклад, на стор. 16, стор. 75, стор. 162 тощо). Для прикладу, використовується термін «чутлива інформація», який не є стандартизованим і загальноприйнятим у нашій

державі (замість нього варто було б вживати термін «конфіденційна інформація»).

Опірський Іван Романович – доктор технічних наук, професор, завідувач кафедри захисту інформації, Інституту комп'ютерних технологій, автоматики та метрології Національного університету «Львівська політехніка».

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.

Толюпа Сергій Васильович – доктор технічних наук, професор, професор кафедри кібербезпеки та захисту інформації Факультету інформаційних технологій Київського національного університету імені Тараса Шевченка.

1. У розділі 2.1 дисертантом здійснена спроба математичної обробки кількості кіберінцидентів в світі за 2019-2022 роки з метою визначення їх розподілу рівномірного чи нормального. Було б доцільніше у рамках проблеми дослідження висвітлити саме ті кіберінциденти, які пов'язані з внутрішніми порушниками, з інсайдерською діяльністю на підприємстві.

2. У розділі 2.2 автором представлено засоби підвищення кіберкультури на підприємстві. Дослідження мало б більш завершеним у цьому питання, якщо спочатку була б представлена технологія підвищення кіберкультури на підприємстві виходячи з концепції нульової довіри, а потім деякі складові були б деталізовані, що і представлено у дослідженні.

3. У висновках до розділу 2 здобувач описує під номером 4 «Формалізована модель оцінки рівня культури кібербезпеки в інформаційній системі дає можливість коректної обробки даних анкетування персоналу та формування висновків щодо її покращення», проте у самому дослідженні не представлено, як здійснювати цю обробку даних.

4. У розділі 3.3 автором детально теоретично обгрунтовано стегосистему для захисту інформаційного обміну в рамках реалізації процедур

автентифікації на основі концепції нульової довіри, здійснено висновок щодо швидкості і реалізації, проте самі обчислювальні дії з конкретними даними відсутні.

Соколов Володимир Юрійович – кандидат технічних наук, доцент, доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка, Факультету інформаційних технологій та математики Київського університету імені Бориса Грінченка.

1. В першому розділі було би гарно привести статистичні дані для підприємств приблизно однакого розміру, які використовують класичну схему та які перейшли на використання методології zero-trust.
2. В списку «Опублікованих праць за темою дисертації» не зрозуміло, яку категорію мають періодичні наукові видання.
3. Рис. 2.3 містить англійські оператори, які не пояснені у тексті.
4. Посилання на рис. 2.4 відсутнє в тексті пояснювальної записки до цього рисунку.
5. У табл. 2.5 шапка відірвалася і залишилася на попередній сторінці. Сама таблиця займає цілу сторінку, тому її краще було бвинести вдодаток.
6. Заголовок «відірваний від основного тексту в розділі «2.6. Формалізована модель оцінки культури кібербезпеки».
7. Електрична схема представлена на рис. 3.3 сильно контрастує з основною тематикою роботи. Її використання недостатньо обґрунтоване.
8. Рис. 3.6 складається з суцільного тексту, його доцільно привести в вигляді нумерованого списку.
9. Також присутні незначні зауваження до розділових знаків і узгодженості словосполучень: розірвані рядки в змісті, неузгодження з чисельником «б таблиці», пропущені пробіли в списку літератури «&Korn, T. M.», вирівнювання по центру формули (3.12) тощо.

Результати відкритого голосування:

«За» – 5 членів ради,

«Проти» – немає,

«Утримались» – немає.

На підставі результатів відкритого голосування разова спеціалізована вчена рада ДФ 26.133.056 присуджує Ворохобу Максиму Віталійовичу ступінь доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека та захист інформації.

Голова разової спеціалізованої вченої ради ДФ 26.133.056 Геннадій ГУЛАК