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
20.01.2024р
Голова спеціалізованої
вченої ради
ДФ 26.133.056
д.т.н., проф. Г.М. Гулак

РЕЦЕНЗІЯ

СОКОЛОВА Володимира Юрійовича, кандидата технічних наук, доцента, доцента кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Київського столичного університету імені Бориса Грінченка, 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 дисертаційного дослідження

Збільшення кількості атак на критичну інфраструктуру, державні та комерційні інформаційні системи та мережі в умовах повномасштабної війни призводить до гострої необхідності в удосконаленні існуючих та розробці нових методів захисту таких систем. З іншого боку, збільшилася кількість зловживань персоналу, що призводить до компрометації підходу побудови контуру безпеки, демілітарізаційної зони та довіреної зони в середині однієї інформаційної системи. Методологія zero-trust (нульової довіри) як раз дозволяє побудувати систему, в якій відсутня довірена зона в загалі. Таким чином, кожна робоча сесія підчас відкриття має відповідати поточним налаштуванням рівня безпеки і валідується на права доступу до конкретного ресурсу. Звичайно, у такого підходу є обмеження: інформаційна система критичної інфраструктури має буде побудована на мікросервісній архітектурі, але значна більшість сучасних систем

використовують саме таких підхід.

Частковий чи повний перехід на хмарні технології при побудові комерційних інформаційних систем призводить до перманентного стану недовіри до будь-якого користувача, тому питання гармонізації процесів побудованих в традиційних і хмарних інформаційних системах вирішується вкрай легко. При нульовій довірі потають питання в адмініструванні та оновлені системи контролю доступу, а всі сервіси мають підтримувати однаковий протокол авторизації. Але незважаючи на збільшення складності системи, основні затрати приходяться лише на етап впровадження.

Тому вдосконалення політик безпеки інформаційних систем підприємств як критичної інфраструктури, так і комерційного напрямку за допомогою методології zero-trust є вкрай актуальним та своєчасним для побудови систем нового покоління.

2. Наукова новизна результатів дисертації

Новизна результатів дисертаційного дослідження **ВОРОХОБА Максима Віталійовича** зумовлена тим, що вперше розроблено метод автентифікації користувачів корпоративної мережі на основі стеганографічного протоколу обміну даними автентифікації згідно з політикою безпеки з урахуванням концепції zero-trust. А також були вдосконалені методика формування вихідних вимог щодо побудови безконтактного апаратного засобу автентифікації користувачів корпоративної мережі на основі RFID-технології та методика оперативної оцінки поточного стану корпоративної кіберкультури на основі анкетування персоналу.

3. Теоретичне і практичне значення результатів дисертації

Теоретичне значення дисертаційної роботи **ВОРОХОБА Максима Віталійовича** не викликає сумніву, оскільки автор пропонує застосувувати методологія zero-trust через кардинальну перетвореність парадигми кібербезпеки, що виявляється у відмові від традиційних моделей, заснованих на ідеї периметра, на користь більш динамічного та адаптивного підходу через

ключові фактори:

– зміна ландшафту кіберзагроз (зі збільшенням частоти та складності кібератак традиційні моделі безпеки, що розраховані на впевненість у надійності внутрішньої мережі, виявляються неадекватними, тому методологія zero-trust визнає необхідність неперервної перевірки та автентифікації кожного користувача та пристрою, незалежно від їхнього місцезнаходження чи мережевої інфраструктури);

– мобільна робоча сила та віддалений доступ (у бізнес-середовищі працівники мають можливість звертатися до ресурсів підприємства з різних місць та за допомогою різних пристроїв, але концепція zero-trust визнає необхідність постійної перевірки, що робить її особливо актуальною в умовах розповсюдження віддаленої роботи);

– порушення даних та внутрішні загрози (традиційні моделі безпеки нерідко демонструють непоодинокість у захисті від внутрішніх загроз в мережі, але zero-trust зменшу ризики внутрішніх загроз та несанкціонованого доступу через обов'язковість перевірки кожного користувача не залежно від місця його розміщення);

– впровадження хмарних служб (зростає необхідність у концепції безпеки, що виходить за межі звичайного периметра, і zero-trust відповідає цим вимогам, реалізуючи захист даних незалежно від їхнього місцезнаходження);

– вимоги відповідності (багато сфер діяльності підпорядковані строгим стандартам щодо захисту даних та конфіденційності, і впровадження моделі безпеки zero-trust може сприяти відповідності цим стандартам, надаючи вищий рівень контролю та видимості доступу до даних та їх обробки);

– безперервний моніторинг та адаптивна безпека (zero-trust базується на ідеї постійного моніторингу та адаптивної безпеки, що стає критично важливим в умовах стрімкого розвитку кіберзагроз, де загрози постійно змінюються, тому здатність динамічно налаштовувати заходи безпеки на основі даних у реальному часі є ключовою перевагою zero-trust);

– реагування на інциденти та виявлення загроз (zero-trust включає

ефективні механізми реагування на інциденти та розширені можливості виявлення загроз, що набуває стратегічного значення для оперативного виявлення та пом'якшення інцидентів безпеки, мінімізуючи можливий збиток).

Таким чином, наукове обґрунтування вдосконалення політики безпеки підприємств на основі методології zero-trust набуває вагомості, оскільки вона гармонізується із сучасним ландшафтом кібербезпеки, розв'язує проблеми, пов'язані з віддаленим робочим процесом, впровадженням хмарних технологій та еволюцією характеру кіберзагроз. Цей підхід забезпечує прогнозовану та адаптивну реакцію на виклики, які виникають при захисті конфіденційної інформації в системах критичної інфраструктури та приватних підприємств.

4. Наукова обґрунтованість результатів дослідження, наукових положень, висновків і рекомендацій, сформульованих у дисертації, та їхня достовірність

Наукова обґрунтованість результатів дослідження зумовлена глибоким опрацюванням теоретичних джерел та їх аналізом. Наукові положення, висновки і результати, які представлено в дисертації **ВОРОХОБА Максима Віталійовича**, є теоретично і емпірично обґрунтованими та достовірними. Вони базуються на використанні загальнонаукових та спеціальних методів дослідження, таких як: системного аналізу, теорії ризиків, теорії ймовірностей та математичної статистики, методи моделювання систем управління інформаційною безпекою. Загальні висновки дисертації логічні та переконливі. Вони повністю висвітлюють хід дослідження, поставлені завдання та результати проведеної роботи.

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

Дисертаційна робота виконана відповідно до планів наукової і науково-технічної діяльності кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Київського столичного університету імені Бориса Грінченка в рамках науково-дослідної роботи №0122U200483 «Методи

та моделі забезпечення кібербезпеки інформаційних систем переробки інформації та функціональної безпеки програмно-технічних комплексів управління критичної інфраструктури» (КСУБГ, м. Київ). А також результати наукових досліджень впроваджені в Інституті програмних систем Національної академії наук України (акт від 18.09.2023 р.) та Інституті телекомунікацій та глобального інформаційного простору Національної академії наук України (акт від 20.09.2023 р.).

6. Рівень виконання поставленого наукового завдання та оволодіння здобувачем методологією наукової діяльності

Визначені в дисертації завдання здобувач виконав на високому рівні. Чітко сформульовано мету дослідження, точно сформульовано завдання та застосовано доцільні методи для її досягнення. Представлений текст дисертаційної роботи демонструє, що **ВОРОХОБ Максим Віталійович** опанував методологію наукової діяльності, уміло застосовує її на практиці, а отже, оволодів необхідними для рівня доктора філософії компетенціями.

7. Апробація результатів дисертації

Повнота викладу основних результатів дисертації у наукових публікаціях. У наукових публікаціях у повному обсязі висвітлено наукові результати дисертації відповідно до мети та поставлених завдань. Наукові результати дисертації висвітлено у 11 наукових працях (жодної одноосібної): 8 статті у наукових фахових виданнях України, 3 тези доповідей у періодичному науковому виданні, включеному до міжнародної наукометричної бази Scopus. Основні положення, висновки і результати дослідження викладались і у процесі виступів і обговорень на науково-практичній міжнародній конференції. В більшості робіт, опублікованих у співавторстві, зазначено особистий внесок здобувача.

8. Структура та зміст дисертації, її самостійність, завершеність, відповідність вимогам щодо оформлення й обсягу

Зміст дисертаційної роботи **ВОРОХОБА Максима Віталійовича** «Моделі

і методи вдосконалення політики інформаційної безпеки підприємства на основі методології Zero Trust» охоплює основні аспекти теми, відповідає меті та завданням дослідження. Робота містить анотацію, вступ, три розділи основної частини з підпунктами, висновки до розділів, загальні висновки, список використаних джерел з 176 найменувань (з них 167 є унікальними) та одного додатку. Робота містить 6 таблиць та 16 рисунків. Обсяг основного тексту дисертації складається з 162 сторінок друкованого тексту. Контекст дисертаційного дослідження вирізняється логічністю, індивідуальним і творчим авторським підходом до задуму дисертації, обізнаністю автора в методологічному інструментарії, підходах, методах, принципах, обґрунтованістю висновків, оригінальному баченні дискусійних проблем. У вступній частині авторкою обґрунтувано актуальність теми дослідження, її зв'язок із науковими програмами, планами, темами, сформульовано об'єкт, предмет, мету і завдання дослідження, інформаційну базу, методи дослідження, наукову новизну і практичне значення роботи, особистий внесок автора, дані про апробацію отриманих результатів та публікації за темою дисертації.

У першому розділі «Аналіз стану та постановка завдання розробки методу вдосконалення політики безпеки сучасного підприємства» **ВОРОХОБОМ Максимом Віталійовичем** було проведено аналіз поточного рівня розробки методів забезпечення безпеки на сучасних підприємствах. Визначено ключові ролі політики безпеки у гарантуванні інформаційної безпеки підприємств, розглянуто застосування політик безпеки та висвітлено основні аспекти, підходи та принципи концепції zero-trust. Сформульовано актуальне наукове завдання, яке полягає у подальшому розвитку методів удосконалення політики інформаційної безпеки підприємства за допомогою інтеграції концептуальних принципів zero-trust, зокрема технічних аспектів їх забезпечення. Для вирішення цього завдання визначено мету роботи - підвищення ефективності застосування політики інформаційної безпеки підприємства, сформованої на основі принципів zero-trust за допомогою поєднання стенографічного та криптографічного підходів до розробки протоколів ідентифікації/автентифікації суб'єктів в

інформаційно-комунікаційних системах.

У другому розділі «Аналіз трендів розвитку кіберінцидентів та управління культурою кібербезпеки організації» здобувачем були визначені основні тенденції кіберзагроз та процеси управління кібербезпекою. Розроблено удосконалену модель формування системи кібербезпеки та підходи до оцінки рівня культури кібербезпеки, що призвело до створення формалізованої моделі оцінки культури кібербезпеки. З урахуванням результатів, отриманих у попередньому розділі, у наступному розділі планується акцентувати увагу на організаційно-технічних аспектах політики безпеки підприємства на основі методології zero-trust.

Третій розділ роботи «Ключові організаційно-технічні положення політики безпеки підприємства на основі концепції zero-trust» містить ключові організаційно-технічні аспекти політики безпеки підприємства на базі методології zero-trust. Розроблено удосконалену модель загроз безпеки, визначено вимоги до безконтактних апаратних засобів автентифікації, розроблено стеганографічний протокол обміну даними, визначено загрози та ризики використання штучного інтелекту. Також запропоновано структурно-логічну схему системи підтримки прийняття рішень щодо відновлення пошкодженого програмного забезпечення внаслідок кібератак. Технологія обробки інформації в системі підтримки прийняття для відновлення пошкодженого програмного забезпечення внаслідок кібератак дозволяє здійснювати прийняття рішень щодо розв'язання складних структурованих або неструктурованих задач з метою оптимального вибору методу відновлення дефектів та технологічних операцій для їх усунення.

9. Дотримання академічної доброчесності у дисертації та наукових публікаціях. Відсутність (наявність) академічного плагіату, фабрикації, фальсифікації

Аналіз тексту дисертаційного дослідження та публікацій дозволяє стверджувати, що **ВОРОХОБ Максим Віталійович** дотримувався правил академічної доброчесності, в тексті не знайдено некоректного цитування, ознак

плагіату, фабрикації чи фальсифікації. Дисертаційна робота є оригінальним завершеним науковим дослідженням, що відповідає вимогам, які висуваються Міністерством освіти і науки України до оформлення дисертацій на здобуття наукового ступеня доктора філософії.

10. Дискусійні положення, недоліки та зауваження до дисертації

Принципових зауважень щодо структури, основних положень та концепції дисертації **ВОРОХОБА Максима Віталійовича** немає. Оцінюючи загалом позитивно наукове і практичне значення отриманих дисертанткою результатів, дозволю собі висловити зауваження і рекомендації до окремих положень дисертації.

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 б винести в додаток.

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.

10. Також присутні незначні зауваження до розділових знаків і узгодженості словосполучень: розірвані рядки в змісті, неузгодження з чисельником «6 таблиці», пропущені пробіли в списку літератури «&Korn, T. M.», вирівнювання по центру формули (3.12) тощо.

11. Загальний висновок про рівень набуття здобувачем теоретичних знань, відповідних умінь, навичок та компетентностей

ВОРОХОБ Максим Віталійович на високому рівні оволодів методологією наукової діяльності, набув теоретичних знань, умінь, навичок та компетентностей. Здобувач вільно володіє матеріалом дослідження та має достатній досвід для проведення самостійних дослідницьких робіт.

12. Загальна оцінка дисертації і наукових публікацій щодо їхнього наукового рівня з урахуванням дотримання академічної доброчесності та щодо відповідності 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.

Рецензент:

кандидат технічних наук, доцент
доцент кафедри інформаційної
та кібернетичної безпеки
імені професора Володимира Бурячка
Київського столичного університету
імені Бориса Грінченка

Володимир СОКОЛОВ

Власноручний підпис
Володимира Соколова
засвідчую
Начальник ВК
Н. Тимура