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. Г.М. Гулак

ВІДГУК

офіційного опонента ТОЛЮПИ Сергія Васильовича, доктора технічних наук, професора, професора кафедри кібербезпеки та захисту інформації Київського університету імені Тараса Шевченка, 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

Цифрова трансформація спонукає компанії у всьому світі адаптувати свої мережі та стратегії безпеки. Останніми роками прискорилися дві ключові тенденції: впровадження хмарної інфраструктури та зростання розподіленої робочої сили. Разом ці тенденції призвели до реструктуризації мереж і безпеки. Тепер компаніям необхідно розгортати служби безпеки в будь-який час і в будь-якому місці на різноманітних архітектурах і кінцевих точках. Крім того, їм потрібно контролювати та захищати розподілену робочу силу, внутрішні ресурси та хмарну інфраструктуру. Оскільки традиційні проєкти мережевої безпеки важко або, навіть, неможливо перекласти на нові парадигми, потрібна нова модель безпеки. Компанії все частіше досліджують концепцію нульової довіри.

Нульова довіра – це набір парадигм кібербезпеки, які зміщують захист зі статичних мережевих периметрів до зосередження на користувачах, активах і ресурсах. Нульова довіра передбачає відсутність прихованої довіри

до активів або облікових записів користувачів виключно на основі їх фізичного чи мережевого розташування або на основі власності на активи. Нульова довіра усуває потребу у фізичних межах для розмежування довірених і ненадійних користувачів, пристроїв і мереж. І хоча рішення на основі нульової довіри мають багато переваг порівняно з традиційними рішеннями, компанії не готові повністю відмовитись від перевірених роками та добре знайомих технологій захисту на користь нових рішень.

Однією з проблем, що стримує інноваційні процеси в запровадженні концепції Zero-Trust, є недостатній рівень її розробленості та структуруванні. З цією метою необхідно напрацювати методи, засоби, технології та стратегічні програми побудови даної моделі. Саме це і зумовило вибір дисертантом важливої та актуальної теми даного дослідження.

2. 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 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, м. Київ).

Обрана тема дисертації безпосередньо пов'язана з реалізацією та виконанням доктрини інформаційної безпеки України, Стратегії інформаційної безпеки та Стратегії кібербезпеки України.

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

Отримані наукові результати та висновки дисертаційної роботи характеризуються належним рівнем обґрунтованості, що підтверджується аналізом значної кількості наукової та технічної літератури та використанням загальнонаукових та спеціальних методів дослідження, зокрема методів теорії ризиків в системах безпеки, теорії ймовірностей та математичної статистики, методів моделювання систем управління інформаційною безпекою.

Достовірність, отриманих в дисертації результатів, ґрунтується на комплексному, експериментальному й теоретичному вивченні моделей і методів вдосконалення політики безпеки підприємства на основі методології Zero-Trust. Перелік наукових праць дисертанта та довідки щодо

впровадження результатів дослідження засвідчують фаховий підхід здобувача до обрання дослідницької проблематики та високий рівень його наукової компетентності.

4. Мова та стиль викладення результатів

Дисертаційна робота написана українською мовою.

Дисертаційна робота є гарно структурованою, кількість розділів та підрозділів тексту дисертації адекватно відображає суть та логічну послідовність проведених наукових досліджень. Слід відзначити доступність викладення, а також професійне та коректне використання загальноприйнятої термінології.

Дисертація складається з вступу, 3 розділів, висновків, списку літератури до кожного розділу та 1 додатка. Загальний обсяг дисертації 164 сторінки.

У вступі обґрунтовується важливість й актуальність теми дисертаційного дослідження, сформульовано мету та задачі роботи, визначено основні положення, наукову та практичну цінність отриманих результатів роботи та наведено особистий внесок автора.

У першому розділі здійснено аналіз стану розробки методів забезпечення політики безпеки сучасного підприємства. Визначено ролі політики безпеки у забезпечення інформаційної безпеки підприємства, проаналізований поточний стан застосування політик безпеки, визначено основні аспекти, підходи та принципі застосування концепції Zero-Trust. Сформульовано актуально наукове завдання, яке полягає в подальшому розвитку методів вдосконалення політики інформаційної безпеки підприємства на основі інтегрування концептуальних принципів Zero-Trust, зокрема технічних аспектів їх забезпечення. Зокрема для його вирішення визначено мету роботи, яка полягає в підвищенні ефективності застосування політики інформаційної безпеки підприємства сформованої за принципами концепції Zero-Trust завдяки комбінуванню стенографічного та криптографічного підходів до побудови протоколів ідентифікації/автентифікації суб'єктів в ІКС.

У другому розділі визначено основні тренди загроз кібербезпеки та процеси управління кібербезпекою. Запропонована вдосконалена модель формування системи кібербезпеки та підходи щодо оцінки рівня культури кібербезпеки, що дало змогу створити формалізовану модель оцінки культури кібербезпеки.

У третьому розділі визначено ключові організаційно-технічні положення політики безпеки підприємства на основі концепції Zero-Trust. Запропонована вдосконалена модель загроз безпеки на основі концепції Zero-Trust. Визначено вимоги до безконтактного апаратного засобу автентифікації, розроблено стеганографічний протокол обміну даними, визначено загрози й ризики використання штучного інтелекту «artificial intelligence» (ШІ), а також запропоновано структурно-логічну схему відповідної системи підтримки прийняття рішення (СППР) щодо відновлення пошкодженого програмного забезпечення внаслідок впливу кібератак. Зазначена технологія обробки інформації в СППР по відновленню пошкодженого програмного забезпечення внаслідок впливу кібератак, у подальшому дає можливість здійснювати прийняття рішень відносно розв'язання складних структурованих або неструктурованих задач з метою оптимального вибору способу відновлення дефектів та технологічних операцій по їх усуненню.

У розділі «Висновки» наведено основні результати дисертації.

У додатку представлено практичні рішення наукових досліджень які 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).

Дисертаційна робота оформлена відповідно до вимог наказу МОН України від 12 січня 2017 р. № 40 «Про затвердження вимог до оформлення дисертації».

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

Представлені в дисертації положення, концептуальні засади, структура, постановка завдань та їх вирішення, узагальнені висновки є результатом реалізації авторських ідей і самостійно виконаної наукової праці. У дисертаційній роботі Ворохоба М.В. обґрунтовано низку концептуальних положень, узагальнень та висновків, які відповідають критеріям наукової новизни, зокрема:

- 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.

Всі отримані автором результати можуть слугувати складовою частиною впровадження методології Zero-Trust для забезпечення конфіденційності, доступності та цілісності інформації.

6. Теоретична цінність і практична значущість наукових результатів

Наукові положення, висновки та рекомендації дисертаційної роботи Ворохоба М.В. мають теоретичну цінність і практичну значущість. Отримані результати є певним внеском у розвиток інформаційної та кібернетичної безпеки.

Теоретичне значення дослідження полягає в обґрунтуванні необхідності та дослідженні можливості впровадження методів захисту інформації на основі методології Zero-Trust, що дозволяє розширити та удосконалити політику безпеки на підприємстві.

Практична цінність дисертаційної роботи Ворохоб М.В. не викликає сумніву, оскільки вона присвячена дослідженню методів та моделей на основі методології Zero-Trust, що дозволяє вдосконалити системи захисту інформації на основі нових методик, які базуються не на моделі «безпеки периметра», а на повному інформаційному контролю щодо того, хто саме, коли й до яких активів отримував доступ, та на так званому ефекті мікросегментації, коли враження одного з об'єктів не призводить до враження всієї системи. Здобувачем розроблено метод 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).

Сформульовані в дисертації висновки та пропозиції можуть бути

7. Повнота викладення наукових результатів дисертації в опублікованих працях

Результати дисертації відображені у 11 публікаціях: восьми статтях у журналі, що входить до наукових фахових видань (Категорія "Б"), та трьох, які представлені на Workshop on Cybersecurity Providing in Information and Telecommunication Systems (Scopus).

Аналіз публікацій автора дозволяє зробити висновок про повноту викладення основних наукових положень дисертаційного дослідження у науковій літературі. Також зазначено особистий внесок здобувача у тих наробках, які виконано колективно.

8. Відсутність (наявність) порушення академічної доброчесності

У дисертації та наукових публікаціях Ворохоба М.В. відсутні порушення академічної доброчесності. Запозичень матеріалу без посилання на відповідне джерело не виявлено. Перевірка проводилася сертифікованою програмою Unichek.

9. Дискусійні положення та недоліки дисертаційної роботи

Відзначаючи позитивні сторони роботи Ворохоба М.В., слід звернути увагу на певні зауваження та дискусійні положення, які потребують додаткової аргументації.

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 обґрунтовано стегосистему для захисту інформаційного обміну в рамках реалізації процедур автентифікації на основі концепції нульової довіри, здійснено

висновок щодо швидкості її реалізації, проте самі обчислювальні дії з конкретними даними відсутні.

Вказані недоліки не носять принципового характеру та не впливають на загальну позитивну оцінку представленої до захисту дисертаційної роботи, оскільки в основному носять дискусійний характер та спрямовують дисертанта на дослідження зазначеної проблематики. Також слід зауважити, що наявність дискусійних питань, насамперед, характеризує складність, актуальність і багатоаспектність досліджуваної теми та власний підхід до її розгляду дисертантом.

10. 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,
професор кафедри кібербезпеки та захисту інформації
факультету інформаційних технологій
Київського національного університету
імені Тараса Шевченка Сергій ТОЛЮПА