Голові спеціалізованої вченої ради
ДФ 26.133.056 у Київському столичному
університеті імені Бориса Грінченка,
д.т.н., 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 **ГНАТЮКА Сергія Олександровича**,
доктора технічних наук, професора, декана факультету комп'ютерних наук та технологій Національного авіаційного університету 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

Політика інформаційної безпеки підприємства традиційно сконцентрована на захисті периметру своєї мережі у припущенні відсутності загроз зсередини (інсайдерських загроз). Але в останні роки вона переглянута у бік суворішої авторизації користувачів та пристроїв незалежно від їх розташування відносно меж периметру в рамках концепції нульової довіри. Ця концепція втілилася у нову модель IT-безпеки Zero trust, згідно якої перед кожною операцією довіра до будь-якого користувача відсутня.

Сьогодні модель IT-безпеки Zero trust дозволяє підвищити ефективність застосування політики інформаційної безпеки підприємств, які використовують хмарні технології та віддалений доступ до своїх ресурсів оскільки вона результативно протистоїть загрозам і ризикам, що несуть в собі такі технології.

З розвитком цифрових технологій традиційні підходи до забезпечення інформаційної безпеки підприємства вже не можуть бути поєднані із винахідливістю сучасних загроз, внаслідок чого корпоративна мережа вважається зоною недовіри. У зв'язку з цим, модель Zero trust привернула до себе широку увагу у дослідженнях та практиці, оскільки вона може відповідати новим вимогам до безпеки мережі. Однак застосування Zero trust все ще знаходиться в зародковому стані, і підприємства, організації та окремі особи не до кінця усвідомлюють переваги та недоліки цієї методології. Тому подальший розвиток досліджень у цьому напрямку має надати методи для аналізу технологій, що застосовуються у Zero trust, узагальнення переваг та недоліків, можливих теперішніх проблем та майбутніх тенденцій.

Отже, вивчення моделей і методів вдосконалення політики безпеки підприємства на основі методології Zero trust є доцільним компонентом сучасних наукових і прикладних досліджень в інформаційній безпеці, а, як наслідок, тема дисертації М. Ворохоба є актуальною та важливою.

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 факультету інформаційних технологій та математики Київського університету імені Бориса Грінченка відповідно до плану науково-дослідних робіт. Дослідження здійснене відповідно до наукової роботи зазначеної кафедри «Методи та моделі забезпечення кібербезпеки інформаційних систем переробки інформації та функціональної безпеки програмно-технічних комплексів управління критичної інфраструктури» (реєстраційний номер 0122U200483, термін виконання 2022-2027 рр.)

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

Автор розробив і представив у своїй дисертації наукові положення, висновки та рекомендації, які мають достатню обґрунтованість. Дисертант провів детальний аналіз літературних джерел зарубіжних та вітчизняних учених та приділив увагу дослідженню і можливій адаптації зарубіжного досвіду. У процесі вирішення завдань, поставлених у дисертації, автор критично оцінював досягнення вітчизняних та зарубіжних учених, висловлюючи свою думку та демонструючи високий рівень наукової культури. Висновки та рекомендації, представлені в дисертації, логічні та є результатом всебічного та об'єктивного аналізу досліджуваних явищ з використанням сучасного наукового інструментарію. У ході дослідження було використано загальнонаукові та спеціальні методи пізнання, що дозволило дисертантові обґрунтувати теоретичні, методичні та практичні аспекти вдосконалення політики безпеки сучасного підприємства на основі методології Zero-trust

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

У рамках дисертаційного дослідження сформульовано та обґрунтовано низку наукових положень, висновків та рекомендацій, що відрізняються наявністю наукової новизни.

1. Вперше 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. На відміну від існуючих методів при вирішенні завдання автентифікації приховується зміст і обсяг інформаційного трафіку, клієнт і сервер отримують можливість обирати контейнери для доставки даних, замість складних фіксованих логінів клієнт отримує доступ до візуалізованого подання його особистої автентифікаційної інформації. Це дозволяє приховувати від зловмисника чутливу інформацію,

яка може бути використана для реалізації атак, включаючи її руйнування, що в свою чергу знижає ймовірність помилкової автентифікації клієнта або сервера у випадку реалізації цільових атак.

2. Вдосконалений метод формування вихідних вимог щодо побудови безконтактного апаратного засобу автентифікації користувачів корпоративної мережі на основі технології RFID., що за рахунок переведення в площину створення дослідного зразка відповідного багатофункціонального засобу автентифікації, дозволяє підвищити ефективність підсистеми ідентифікації і автентифікації.

3. Подальшого розвитку набув метод оперативного оцінювання поточного стану корпоративної кіберкультури на основі анкетування персоналу та математичного апарату обробки даних анкетування, що за рахунок синтезу з методикою оцінювання трендів загроз кібербезпеки, дає можливість оперативного реагування з боку менеджменту безпеки в частині корегування політики безпеки та впровадження організаційних і навчальних заходів.

5. Теоретична цінність і практична значущість наукових результатів

Результати аналізу дисертаційної роботи та опублікованих праць свідчать про важливість отриманих результатів проведеного дослідження. Основним досягненням є можливість сформувати теоретико-методичний підхід до підвищення ефективності впровадження політики інформаційної безпеки на підприємстві, яка базується на принципах концепції zero-trust завдяки комбінуванню стенографічного та криптографічного підходів до побудови протоколів ідентифікації/автентифікації суб'єктів в інформаційно-комунікаційних системах, а також впровадженню заходів управління кіберкультурою на підприємстві.

Зазначені теоретичні положення становлять основу для створення системного та уніфікованого підходу до управління інформаційною безпекою підприємства, що підтверджує вагомість проведеної роботи.

Висновки та пропозиції дисертаційного дослідження мають практичне значення і прийняті до впровадження в діяльність Інституту програмних систем Національної академії наук України (акт від 18.09.2023), Інституту телекомунікацій та глобального інформаційного простору Національної академії наук України (акт від 20.09.2023).

6. Повнота викладення наукових результатів дисертації в опублікованих працях

За темою дослідження опубліковано 11 наукових праць, із них: у фахових виданнях, затверджених МОН України – 8; у Scopus – 3 (кожна має підтверджений ISSN-номер). За матеріалами виступів на науково-технічних конференціях опубліковано 3 тез доповідей.

У публікаціях розкрито ключові результати проведеного дослідження та його наукову новизну, що дозволяє стверджувати, що висновки та пропозиції, викладені у дисертаційній роботі, є достатньо апробованими.

7. Відсутність (наявність) порушення академічної доброчесності

За результатами перевірки дисертаційної роботи Ворохоба М.В. на наявність ознак академічного плагіату встановлено коректність посилань на першоджерела для текстових та ілюстративних запозичень; навмисних спотворень не виявлено. Звідси можна зробити висновок про відсутність порушень академічної доброчесності.

8. Дискусійні положення та зауваження до дисертації

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 за 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 з боку 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 з 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»).

Проте, я вважаю, що зазначені недоліки не знижують ступінь наукової новизни та практичного значення одержаних в дисертації наукових результатів і, відповідно, позитивну оцінку роботи у цілому.

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.

Підпис Гнатюка С.О.
засвідчую
Вчений секретар
Національного авіаційного університету
М. Мелешкевич

Офіційний опонент:
декан факультету комп'ютерних наук та технологій
Національного авіаційного університету,
доктор технічних наук, професор Сергій ГНАТЮК