ВІДГУК ОФІЦІЙНОГО ОПОНЕНТА
кандидата технічних наук, доцента, завідувача кафедри кібербезпеки
Хмельницького національного університету
Кльоца Юрія Павловича
на дисертаційну роботу Романця Ігоря Євгеновича
на тему «Інтелектуалізована комп'ютерна система виявлення зловмисних повідомлень IP-телефонії в корпоративній мережі»,
подану на здобуття наукового ступеня кандидата технічних наук
за спеціальністю 05.13.05 – комп'ютерні системи та компоненти

1. Актуальність теми дисертаційної роботи.

Перехід від традиційної телефонії до VoIP дозволив компаніям значно скоротити витрати та оптимізувати бізнес-процеси, однак водночас підвищив рівень ризиків інформаційної безпеки, оскільки ця технологія ґрунтується на інтернет-протоколах і є доступною для атак із будь-якої точки світу. З кожним роком спектр загроз для VoIP-інфраструктури розширюється. Існуючі методи захисту, зокрема шифрування трафіку, багатофакторна аутентифікація, контроль доступу та статичні системи фільтрації, мають низку суттєвих недоліків: вони характеризуються низькою адаптивністю до нових атак, не містять механізмів самонавчання та адаптації до змін у поведінкових патернах трафіку, відзначаються високим рівнем хибних спрацювань, а також мають обмежені можливості аналізу в реальному часі, що унеможливлює своєчасне реагування на інциденти.

У таких умовах виникає нагальна потреба у розробці та впровадженні інтелектуалізованих систем виявлення зловмисної активності, здатних аналізувати багатовимірні дані з трафіку та метаданих протоколів VoIP, виявляти аномалії у реальному часі, самонавчатись і швидко адаптуватись до нових загроз. Таким чином, розробка та впровадження адаптивних, самонавчальних, інтелектуалізованих систем захисту VoIP є критично важливою для забезпечення кіберстійкості корпоративних мереж та дозволить підвищити рівень інформаційної безпеки, зберегти конфіденційні дані, мінімізувати фінансові втрати та забезпечити безперервність бізнес-процесів в умовах зростаючих і технологічно складних кіберзагроз.

Вищеозначене обумовлює актуальність обраної теми дисертаційної роботи Романця І.Є., яка спрямована на вирішення актуальної науково-практичної задачі підвищення рівня безпеки IP-телефонії в корпоративних мережах шляхом створення

інтелектуалізованої комп'ютерної системи, що базується на онтологічній моделі функціонування VoIP-системи та методах інтелектуального аналізу даних.

Аналіз змісту дисертації. Ступінь обґрунтованості наукових положень, висновків і рекомендацій, сформульованих в дисертації забезпечується чітко визначеними метою і завданнями дослідження, оскільки їх постановка та послідовність дозволяють розкрити основний зміст теми дисертації. Об'єкт та предмет дослідження сформульовані достатньо чітко та зрозуміло, що і дозволило комплексно проаналізувати поставлену проблему, не виходячи за межі наукової спеціальності.

Дисертаційна робота складається зі вступу, чотирьох розділів, висновків, списку використаних джерел з 112 найменувань та додатків. Зміст та структура роботи у повній мірі відповідають завданню з викладення основних результатів вирішення поставленої наукової проблеми та сформульованим окремим задачам дослідження, які відповідають паспорту спеціальності 05.13.05 – комп'ютерні системи та компоненти.

У **вступі** обґрунтовано актуальність теми дисертації, сформульовано мету та завдання досліджень, відмічено наукову новизну та практичну цінність отриманих у роботі результатів, наведено дані про особистий внесок здобувача, публікації, апробацію результатів роботи, обсяг і структуру дисертації.

Перший розділ дисертації присвячений аналізу сучасного стану досліджень по проблематиці роботи, а саме: методів виявлення зловмисних повідомлень в IP-телефонії, аналізу структури та особливостей VoIP-систем, а також огляду інтелектуальних підходів, що застосовуються для забезпечення їх безпеки.

З аналізу витікає, що сучасні методи захисту IP-телефонії, незважаючи на їх різноманіття, часто виявляються недостатньо ефективними. Вони не завжди здатні своєчасно виявляти та локалізувати нові вектори кібератак через низьку адаптивність і обмежені можливості самонавчання. Як наслідок, це призводить до підвищеного ризику успішних атак, що можуть спричинити значні фінансові та репутаційні втрати для організацій

З другого боку, існуючі інтелектуальні підходи, хоча й демонструють потенціал, не повною мірою враховують специфіку трафіку IP-телефонії та можуть бути обчислювально складними, що обмежує їх застосування на ресурсообмежених

платформах або в умовах високошвидкісних комунікацій. Це обмежує рівень захисту, який вони можуть забезпечити, та можливість для більш тісної інтеграції механізмів виявлення аномалій у загальну систему безпеки.

Таким чином, результати першого розділу підтверджують, що проблема забезпечення ефективного виявлення зловмисних повідомлень IP-телефонії в корпоративній мережі, особливо у контексті протидії новим і адаптивним загрозам за допомогою інтелектуалізованих методів, залишається актуальною та невирішеною. Саме це підкреслює важливість і своєчасність теми даного дисертаційного дослідження.

Другий розділ дисертації присвячено дослідженню інтелектуальних методів виявлення зловмисних повідомлень у IP-телефонії. У розділі обґрунтовується доцільність застосування методів аналізу мовлення та обробки природної мови для підвищення точності й ефективності систем виявлення аномального трафіку у VoIP-системах.

Виділено перспективний напрямок використання інтелектуальних засобів аналізу контенту на основі онтологічного підходу, у межах якого формалізовано знання про структуру VoIP-повідомлень та розроблено онтологічну модель, яка відображає ключові поняття VoIP та їх взаємозв'язки, що є вагомим внеском у систематизацію предметної області.

Також автором запропоновано, а в наступних розділах апробовано, метод автоматизованого наповнення онтології тематичних повідомлень, який базується на формалізованому представленні повідомлень у вигляді деревоподібних структур та операцій алгебри кортежів, та дозволяє суттєво оптимізувати процес формування онтологічної бази знань, підвищуючи ступінь автоматизації та швидкість обробки інформації.

Отримані результати створюють ґрунтовну теоретичну та практичну базу для подальшого розвитку адаптивних систем безпеки VoIP, здатних ефективно протидіяти сучасним кіберзагрозам шляхом самонавчання і гнучкого реагування на нові вектори атак.

Третій розділ присвячено розробці архітектури та алгоритмічних рішень інтелектуалізованої системи виявлення зловмисних повідомлень IP-телефонії в корпоративних мережах. Побудовано узагальнену структуру системи, яка включає комплекс взаємодіючих підсистем, що реалізують повний цикл обробки даних - від

перехоплення та попередньої обробки трафіку VoIP до поглибленого аналізу та ухвалення рішень щодо виявлення аномалій. Запропонована структурно-функціональна схема та узагальнений алгоритм формалізують послідовність операцій, забезпечуючи прозорість і керованість процесів виявлення.

Автором розроблено механізми виявлення та моніторингу аномалій на основі онтологічного підходу, що дозволяє сформувати комплексний підхід до захищеності VoIP-систем від різноманітних векторів атак.

У розділі представлено багаторівневу архітектуру програмного забезпечення для захисту IP-телефонії, яка охоплює апаратний, комутаційний, серверний, безпековий та моніторингово-управлінський рівні. Архітектура демонструє взаємодію компонентів від фізичних пристроїв і мережевої інфраструктури до інтелектуальних засобів виявлення атак і централізованого керування. Програмний комплекс реалізований як об'єктно-орієнтована система на базі PHP та MySQL, інтегрована з платформою Asterisk під Linux, що забезпечує узгоджену роботу всіх модулів та ефективний захист у корпоративних середовищах.

Четвертий розділ підсумовує впровадження запропонованих методів і засобів захисту IP-телефонії, що забезпечують зниження ризиків основних кіберзагроз від підбору паролів і фроду до DoS/DDoS-атак та перехоплення даних. Реалізовані рішення, зокрема шифрування голосового трафіку та сигналізації, інтеграція інструменту Fail2Ban, а також систем моніторингу Wazuh і Grafana, забезпечують комплексний захист, автоматичне блокування підозрілих дій та своєчасне виявлення аномалій.

Запропоновані методи та засоби дозволяють адаптувати Dialplan під специфіку конкретної інфраструктури, що значно підвищує ефективність управління безпекою. Експериментальні дослідження підтвердили результативність цих методів, зокрема шляхом успішної імплементації програмної підсистеми виявлення аномальних повідомлень, яка базується на онтологічному підході, в реальне корпоративне середовище.

Висновки дисертаційної роботи підкреслюють наукову новизну та практичну цінність проведених досліджень. Основні результати мають як теоретичну, так і практичну складову, створюючи в сукупності цілісну концепцію побудови та

впровадження ефективних методів і засобів захисту IP-телефонії, здатних адаптуватися до динамічних та еволюційних кіберзагроз, з одночасним забезпеченням високого рівня конфіденційності, доступності та цілісності переданих даних.

У **додатках** містяться документи, що підтверджують впровадження результатів дисертаційної роботи, лістинги розроблених програмних кодів, а також список публікацій здобувача за темою дисертації.

Отже, достовірність отриманих даних і обґрунтованість сформульованих пропозицій визначається правильно обраним методологічним підходом до проведеного дослідження, всебічним використанням автором коректного аналітичного та числового апарату досліджень, підтверджується результатами апробації на наукових конференціях, а також публікаціями у фахових виданнях, та виданнях, що індексуються у Scopus та Web of Science. Вказане дає підстави стверджувати, що сформульовані в дисертації наукові положення, висновки і рекомендації мають достатню міру обґрунтованості та достовірності.

2. Наукова новизна одержаних результатів

Наукові положення, результати та висновки, викладені в дисертації, отримані здобувачем самостійно, відзначаються новизною, належним обґрунтуванням і підтверджуються результатами експериментальних досліджень та апробацією на всеукраїнських і міжнародних наукових конференціях. Їх достовірність забезпечена коректним і доцільним застосуванням математичного апарату, положень теорії управління, принципів системного підходу, методів інтелектуального аналізу даних, технологій захисту комп'ютерних систем, методології проєктування інформаційних систем, а також успішною апробацією отриманих результатів.

Подана дисертаційна робота визначається науковою новизною, яка полягає в тому, що в ній:

Отримані в дисертаційній роботі наступні результати, які мають наукову новизну:

1. Вперше розроблено онтологічну модель опису VoIP повідомлень у системі IP-телефонії, що включає формалізацію основних понять через окремі концепти та опис зв'язків між ними, що дозволило створити нові ефективні методи виявлення аномалій у трафіку IP-телефонії.

2. Вперше розроблено метод виявлення аномалій у трафіку IP-телефонії, що базується на поєднанні методів групування VoIP повідомлень та контекстно-частотного аналізу, що забезпечило значне підвищення ефективності виявлення аномальних повідомлень.

3. Удосконалено підсистему захисту від термінації трафіку в IP-телефонії, яка відрізняється від відомих тим, що здатна гнучко адаптуватися до змінних умов і приймати рішення на основі нечітких даних. Такий підхід дозволяє враховувати численні критерії, зокрема IP-адресу клієнта, час здійснення дзвінка, часовий пояс та якість зв'язку, що, в свою чергу, сприяє підвищенню безпеки та якості зв'язку.

4. Удосконалено архітектуру системи виявлення зловмисних повідомлень IP-телефонії в корпоративній мережі, яка містить блоки та процедури для виявлення аномальних повідомлень у трафіку IP-телефонії на основі онтологічного підходу і розподілу доступу в режимі реального часу з використанням нечіткої логіки, що дозволило зменшити час обробки повідомлень.

4. Оформлення дисертації, дотримання вимог академічної доброчесності та повнота викладу наукових результатів в опублікованих працях.

4.1. Оформлення дисертації. Дисертаційна робота містить 170 сторінок друкованого тексту, з яких 138 сторінок складає основний текст, що включає 68 рисунків та 1 таблицю. Список використаних джерел налічує 112 найменувань.

Робота виконана українською мовою, у тексті використано загальновизнані наукові терміни, стиль викладення результатів теоретичних і практичних досліджень, нових наукових положень, висновків і рекомендацій забезпечує доступність їх сприйняття та використання. Оформлення дисертації відповідає усім необхідним атестаційним вимогам.

4.2. Дотримання вимог академічної доброчесності. Проведена перевірка дисертації на наявність академічного плагіату, отримані результати свідчать про хорошу індивідуальність роботи. По всьому тексту дисертації простежується авторський стиль. У дисертації не виявлено текстових запозичень і використання результатів інших науковців без посилань на відповідні джерела.

4.3. Основні результати дисертаційного дослідження представлені у 14 наукових публікаціях, зокрема: 3 одноосібні статті у фахових наукових виданнях України,

рекомендованих МОН України, 4 статті у журналах, індексованих у міжнародних наукометричних базах Scopus та Web of Science, а також 7 тез доповідей на міжнародних конференціях, які також входять до баз Scopus/Web of Science.

5. Наукове та практичне значення результатів дисертаційної роботи

Дисертаційна робота вирізняється розробкою оригінальних підходів, які підвищують ефективність захисту IP-телефонії в корпоративних мережах. Зокрема, вперше створена онтологічна модель для опису VoIP-повідомлень, що є принципово новим інструментом для аналізу трафіку та виявлення аномалій. На її основі розроблено метод виявлення аномалій, що поєднує групування повідомлень із контекстно-частотним аналізом, що значно підвищує точність і ефективність виявлення загроз.

Крім того, запропоновані вдосконалення архітектури системи та підсистеми захисту вирізняються тим, що вони здатні гнучко адаптуватися до змінних умов, приймати рішення на основі нечіткої логіки та спрощувати адміністрування. Це демонструє високий рівень інноваційності та прагнення до створення універсальних і надійних рішень.

Практична цінність результатів дисертації підтверджується її спрямованістю на вирішення конкретних проблем кібербезпеки. Розроблена система не лише забезпечує високий рівень виявлення зловмисних повідомлень, а й мінімізує кількість хибних спрацьовувань, що веде до прямої економії коштів і підвищення надійності зв'язку в корпоративних мережах.

Реалізований програмний прототип для платформи Asterisk з відкритим інтерфейсом є вагомим доказом практичної значущості роботи, оскільки це рішення може бути легко впроваджене та адаптоване під потреби підприємств різного масштабу. Більш того, запропоновані методи можуть слугувати основою для технічних рекомендацій та галузевих стандартів, що свідчить про їхній потенціал для широкого застосування.

6. Зауваження та дискусійні положення щодо змісту дисертації

Загалом позитивно оцінюючи дисертацію І. Є. Романця «Інтелектуалізована комп'ютерна система виявлення зловмисних повідомлень IP-телефонії в корпоративній мережі», варто зазначити, що деякі її положення є дискусійними та потребують додаткової аргументації:

1. У роботі стверджується, що запропонований метод виявлення аномальних повідомлень у трафіку IP-телефонії має низькі хибнопозитивні спрацьовування, але відсутній їх конкретний рівень (false positive rate), а також ситуації, в яких система може некоректно трактувати повідомлення (хибнонегативні). Було б доцільно надати статистичну оцінку цих показників.

2. Під час обговорення практичного значення отриманих результатів автор зазначає про розробку методів виведення (пункт 3, ст. 12). Втім, з тексту дисертаційної роботи не зрозуміло що це за методи та яке їх призначення, що ускладнює оцінку їх практичної значущості та внеску у досліджувану проблематику.

3. У роботі підкреслюється, що система має властивість самонавчання та адаптації до нових типів загроз. Однак немає чіткої інформації, як саме це реалізовано у програмній моделі: чи є оновлення моделей у роботі (online learning), яка частота навчання, який механізм зворотного зв'язку від користувача або адміністратора.

4. З роботи не зрозуміло, як здійснюється захоплення та обробка VoIP-потоку, а також декодування аудіо, що є основою для роботи запропонованого автором методу виявлення аномалій в трафіку IP-телефонії на основі групування повідомлень у якому аудіосигнал конвертується в текст.

5. У тексті дисертації рис. 1.2 та рис.1.4 є ідентичними, однак мають різні назви.

6. Відомо, що у VoIP-системах зазвичай застосовують спеціальні кодеки, оптимізовані для передачі мовлення у реальному часі. При розробці модуля автоматичної обробки голосових записів у режимі реального часу та їх конвертації у текст у системі IP-телефонії (лістинг, додаток В) автор реалізував функцію перетворення аудіо з формату MP3 у WAV. Проте використання формату MP3 в цьому контексті не є доцільним, оскільки MP3 орієнтований на збереження аудіо для прослуховування та має досить високу затримку кодування\декодування, що є критичним для VoIP-систем.

7. У роботі доцільно було навести приклади типових відомих атак на розроблену інтелектуалізовану комп'ютерну систему та оцінити їх вплив на якість обслуговування, безпеку автентифікації та цілісність передачі даних.

8. Для оцінки ефективності методу виявлення аномалій в трафіку IP-телефонії доцільно було застосувати метрики (precision, recall, F1-score), які дозволяють

збалансовано оцінити точність, повноту та узагальнену якість класифікації аномальних та нормальних повідомлень.

9. Деякі висновки по роботі мають якісних характер, їх слід було б замінити кількісними співвідношеннями.

10. В дисертаційній роботі зустрічаються деякі термінологічні та технічні неточності, а також стилістичні та граматичні помилки.

Втім, висловлені зауваження мають дискусійний характер та не впливають на загальну позитивну оцінку проведеного дослідження, його новизну та практичне значення отриманих результатів. Вони радше визначають потенційні вектори майбутніх наукових досліджень у цій сфері.

7. Висновки

Дисертаційна робота Романця Ігоря Євгеновича на тему «Інтелектуалізована комп'ютерна система виявлення зловмисних повідомлень IP-телефонії в корпоративній мережі» є самостійною та завершеною науковою роботою, виконаною особисто дисертантом у вигляді кваліфікаційної наукової праці на правах рукопису. Дисертаційне дослідження містить науково обґрунтовані теоретичні та практичні результати, характеризується єдністю змісту та свідчить про особистий внесок автора. Крім того, дисертація за своєю актуальністю, ступенем новизни, постановкою та способом вирішення поставлених питань, теоретичним та практичним підґрунтям та обґрунтованістю одержаних результатів відповідає вимогам п. 9, 11-13 Порядку присудження наукових ступенів, затвердженого постановою Кабінету Міністрів України від 24.07.2013 р. № 567, а її автор, Романець Ігор Євгенович, заслуговує присудження йому наукового ступеня кандидата технічних наук за спеціальністю 05.13.05 – комп'ютерні системи та компоненти.

Офіційний опонент:
кандидат технічних наук, доцент,
завідувач кафедри кібербезпеки
Хмельницького національного університету Юрій КЛЬОЦ

Підпис засвідчую:
кандидат економічних наук, доцент,
проректор з науково-педагогічної роботи
Хмельницького національного університету Віктор ЛОПАТОВСЬКИЙ