ВІДГУК ОФІЦІЙНОГО ОПОНЕНТА

доктора технічних наук, професора, завідувач відділу мікропроцесорної техніки №205, інституту кібернетики ім. В.М. Глушкова НАН України

Опанасенка Володимира Миколайовича

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.

Корпоративні мережі дедалі більше впроваджують IP-телефонію (VoIP) завдяки її гнучкості, масштабованості та економічним перевагам. Однак зростання її популярності супроводжується збільшенням кількості кіберзагроз, таких як спам, фішинг та DoS-атаки, що ставлять під загрозу конфіденційність, цілісність і доступність комунікацій. VoIP інтегрується з іншими інформаційними системами (CRM, ERP), але водночас стає привабливою ціллю для зловмисників, що використовують методи спуфінгу та перехоплення даних.

Дослідження у галузі безпеки VoIP були зроблені як зарубіжними, так і вітчизняними науковцями. В умовах гібридних загроз і цифрових трансформацій особливо важливим є підвищення ефективності виявлення зловмисних повідомлень у VoIP-мережах, що критично впливає на безпеку корпоративних систем і довіру клієнтів.

Існуючі методи не здатні оперативно виявляти зловмисну активність, оскільки не враховують зміни в поведінці трафіку та мають низьку адаптивність до нових загроз. Це підкреслює необхідність впровадження технологій штучного інтелекту, машинного навчання та аналізу аномалій для своєчасного виявлення атак. Створення інтелектуальної системи захисту VoIP, що враховує сучасні тенденції в кібербезпеці, дозволить підвищити рівень захищеності корпоративних мереж, забезпечити безперервність бізнесу та знизити ризики фінансових і репутаційних втрат.

Дисертаційне дослідження виконувалось в Західноукраїнському національному університеті відповідно до наукового напрямку “Математичне та комп’ютерне

моделювання об’єктів з розподіленими параметрами на основі поєднання онтологічного та інтервального аналізу”.

2. Аналіз змісту дисертації. Ступінь обґрунтованості наукових оложень, висновків і рекомендацій, сформульованих в дисертації

Дисертація є завершеною науково-дослідною роботою, яка містить вступ, чотири розділи, висновки, список використаних джерел.

У вступі обґрунтовано актуальність теми дисертації, сформульовано мету та завдання дослідження, визначено наукову новизну та практичне значення отриманих результатів, подано інформацію щодо апробацій та публікацій результатів дисертаційної роботи із зазначенням особистого внеску автора.

У першому розділі «Сучасний стан та перспективи розвитку виявлення зловмисних повідомлень IP-телефонії» досліджено структуру та особливості IP-телефонії, а також проведено аналіз існуючих методів виявлення зловмисних повідомлень у цій системі. Визначено, що незважаючи на економічні переваги IP-телефонії, її інтеграція з Інтернетом робить її вразливою до кіберзагроз, таких як DoS/DDoS, спуфінг, фішинг та інші атаки, що ставлять під загрозу конфіденційність і доступність голосових комунікацій.

Окремо розглянуто методи штучного інтелекту, зокрема машинне навчання та глибинне навчання, які мають значний потенціал у виявленні складних патернів аномальної поведінки та зловмисних повідомлень. Особливу увагу приділено виявленню нетипової поведінки при передачі голосу, що дає можливість ідентифікувати загрози, які не завжди фіксуються за допомогою традиційних сигнатур атак.

Попри успіхи, існуючі підходи мають проблеми з масштабованістю, високим рівнем хибно позитивних спрацьовувань і адаптацією до нових загроз. Подальші дослідження мають зосередитися на розробці гібридних методів, що поєднують сигнатурний аналіз і методи штучного інтелекту для підвищення ефективності виявлення зловмисних повідомлень, а також на розробці адаптивних систем з можливістю самонавчання та оперативного реагування на нові загрози. Це дозволить покращити безпеку та стійкість систем IP-телефонії.

У другому розділі «Інтелектуальні методи виявлення зловмисних повідомлень IP-телефонії в корпоративній мережі» обґрунтовано використання методів аналізу мовлення та обробки природної мови для підвищення ефективності систем виявлення аномального трафіку в VoIP, зокрема інтеграції інтелектуальних засобів для аналізу контенту. Запропоновано онтологію для опису VoIP-повідомлень в IP-телефонії, включаючи формалізацію основних понять та визначення зв’язків між ними. Введено метод виявлення аномалій у трафіку на основі групування повідомлень, що поєднує знання-орієнтовані підходи з онтологією та контекстно-частотним аналізом.

Покращення якості VoIP-зв'язку досягається завдяки розвитку мережевих технологій та протоколів, що забезпечують зростання мобільності через мобільні додатки і інтеграцію з іншими комунікаційними технологіями. Окремо відзначено важливість забезпечення безпеки VoIP-зв'язку через шифрування, аутентифікацію, управління доступом та системи виявлення вторгнень.

У розділі також розглянуто методи безпеки, такі як шифрування VoIP-трафіку за допомогою протоколів SRTP та TLS, використання брандмауерів, регулярне оновлення програмного забезпечення, а також застосування інтелектуальних засобів для аналізу контенту. Використання алгоритмів машинного навчання та обробки природної мови для виявлення злочинної інформації в текстових і голосових повідомленнях продовжує бути актуальним напрямом досліджень у забезпеченні безпеки VoIP.

Подальше вдосконалення методів безпеки передбачає застосування адаптивних систем, здатних до самонавчання і реагування на нові загрози, що підвищить стійкість систем IP-телефонії до сучасних кіберзагроз.

У третьому розділі «Архітектура інтелектуалізованої системи виявлення зловмисних повідомлень IP-телефонії в корпоративній мережі» розроблено архітектуру інтелектуалізованої системи для виявлення зловмисних повідомлень у системі IP-телефонії корпоративної мережі. Описано узагальнену структуру системи, яка включає взаємодію кількох підсистем. Розроблено алгоритм і структурно-функціональну схему, що дозволяє формалізувати процеси виявлення аномалій, підвищуючи їх прозорість та керованість.

Запропоновано механізм взаємозв’язку модулів для виявлення аномальних повідомлень, заснований на онтологічному підході. Механізм автоматизованого наповнення онтології тематичних повідомлень дозволяє системі постійно оновлювати свої знання щодо нормальних і аномальних патернів комунікації. Крім того, детально розглянуто метод виявлення аномалій у трафіку IP-телефонії за допомогою кластеризації та класифікації повідомлень.

Для забезпечення безпеки IP-телефонії розроблено узагальнений алгоритм, який включає управління доступом, моніторинг трафіку, аналіз загроз, автоматизоване прийняття рішень щодо безпеки та формування звітності. Алгоритм забезпечує ефективне автоматизоване реагування на загрози.

Архітектура програмного комплексу для захисту IP-телефонії має на меті мінімізацію ризиків від зовнішніх та внутрішніх загроз, забезпечуючи безперебійну роботу системи. Розроблена система інтегрована з Asterisk, використовує PHP та MySQL, і працює під управлінням Linux, забезпечуючи комплексний захист голосового трафіку та конфіденційності інформації в корпоративній мережі.

У четвертому розділі «Реалізація запропонованих методів та засобів» досліджено розроблені методи та засоби для підвищення ефективності захисту IP-телефонії в корпоративних мережах. Одним із ключових аспектів є застосування нечіткої логіки для розподілу доступу в реальному часі, враховуючи різноманітні критерії. Моделювання нечіткої системи виконано в середовищі MATLAB з використанням Fuzzy Logic Toolbox. Вхідні змінні включають рівень довіри клієнта за його IP-адресою, час дзвінка, часовий пояс адресата та якість зв’язку. Для кожної змінної визначені функції належності, зокрема дзвоноподібні для вхідних змінних і трапецевидні для вихідної змінної (доступ).

Для побудови бази знань використано правила типу «якщо-то», що визначають поведінку в умовах заданих вхідних змінних. Кількість правил досягла 255, що дозволяє забезпечити точний контроль доступу в IP-телефонії. Запропонований метод демонструє ефективність у реальних умовах через швидке виявлення аномальних повідомлень, що підтверджено проведеними експериментами.

Інтеграція розробленої системи в корпоративну VoIP мережу показала високу масштабованість та здатність до адаптації, що дозволяє ефективно обробляти великі обсяги даних з мінімальними витратами ресурсів. Програмне забезпечення на основі цієї системи інтегровано з підсистемою контролю трафіку, що забезпечує безперебійне функціонування мережі.

Результати експериментів підтвердили значне скорочення часу обробки повідомлень — до 8.3 рази швидше порівняно з ручною обробкою. Розроблена система також має переваги в плані адаптивної інтеграції, багатопотокової обробки та інтелектуального аналізу даних, що робить її потужним інструментом для підвищення рівня кібербезпеки в IP-телефонії.

Висновки по роботі повністю висвітлюють отримані результати та за своїм рівнем відповідають вимогам, які висуваються до результатів дисертаційного дослідження.

Структура дисертації повністю відповідає логіці й послідовності рішення поставлених задач.

2.2. Достовірність та обґрунтованість отриманих результатів та запропонованих автором рішень, висновків, рекомендацій забезпечується коректним використанням аналітичного та числового апарату досліджень; адекватністю теоретичних розрахункових результатів і результатів перевірки; відповідністю висновків і отриманих результатів фізичній суті досліджуваних явищ; порівнянням рішень з відомими у літературі; зіставленням отриманих результатів з даними інших авторів і узгодженням з поставленими завданнями. Результати досліджень ілюстровані таблицями, графіками і рисунками. Прийняті в дисертації рішення мають наукову новизну і обґрунтовані та вирішують поставлені задачі досліджень, у ході розв’язання яких розроблено інтелектуалізовану комп'ютерну систему своєчасного виявлення зловмисних VoIP-повідомлень в корпоративній мережі.

3. Наукова новизна одержаних результатів

Основні наукові положення, результати та висновки дисертації отримані здобувачем самостійно, є новими, достатньо обґрунтованими та підтверджуються даними експериментальних досліджень та апробацією основних положень на

всеукраїнських та міжнародних конференціях. Достовірність наукових положень, висновків і результатів, отриманих здобувачем, обумовлена коректними та доцільним використанням математичного апарату, теорії управління, принципах системного підходу, методах інтелектуального аналізу даних, засобах захисту комп'ютерних систем, методології проектування інформаційних систем, успішною апробацією отриманих результатів.

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

Вперше розроблено:

1. 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. 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.

Удосконалено:

1. 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.

2. 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. Це дозволяє спростити функції адміністратора та значно зменшити час обробки повідомлень.

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

4.1. Оформлення дисертації. Дисертаційну роботу викладено на 170 сторінках друкованого тексту, з них 138 сторінок основного тексту, де наведено 68 рисунків та 1 таблиця, список використаних джерел складає 112 найменувань.

Дисертаційну роботу написано українською мовою грамотно, на хорошому стилістичному рівні. Застосована в роботі наукова термінологія є загальновизнаною, стиль викладення результатів теоретичних і практичних досліджень, нових наукових положень, висновків і рекомендацій забезпечує доступність їх сприйняття та використання. Зміст дисертації дозволяє скласти уявлення про основні положення, висновки і рекомендації, запропоновані автором. Стиль викладу матеріалів досліджень і наукових положень забезпечує їх належне сприйняття. 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 достатньо повно викладені в 14 наукових працях, серед яких: 3 одноосібних статті у наукових фахових виданнях України, рекомендованих МОН України, 4 – у виданнях, що індексуються в міжнародних наукометричних базах Scopus/Web of Science, 7 тез доповідей на міжнародних конференціях, що індексуються в міжнародних наукометричних базах Scopus/Web of Science.

5. Наукове та практичне значення результатів дисертаційної роботи

Наукове значення виконаного дослідження полягає в запропонованій онтології для опису VoIP-повідомлень у системах IP-телефонії, яка формалізує ключові поняття в окремі концепти з чіткими визначеннями та атрибутами, що забезпечує однозначність інтерпретації. Ця онтологія є основою для подальшої адаптації до конкретних завдань, зокрема для виявлення аномалій, аналізу повідомлень та захисту від VoIP-атак, а також для інтеграції з інструментами аналізу даних у мережевій безпеці. Її використання

підвищує інтероперабельність та автоматизацію процесів контролю і реагування на події.

Окрім того, запропоновано метод автоматизованого наповнення онтології для тематичних повідомлень у корпоративних системах IP-телефонії, що значно підвищує ефективність аналізу трафіку. Метод базується на деревовидних структурах для представлення повідомлень, що дозволяє проводити семантичний аналіз із врахуванням стандартних протоколів IP-телефонії. Операції порівняння, фільтрації та трансформації повідомлень у відповідні концепти онтології автоматизують процес ідентифікації нових сутностей, зменшуючи час на наповнення бази знань.

Розроблено також метод виявлення аномалій у трафіку IP-телефонії, заснований на групуванні повідомлень з використанням онтологічного підходу та контекстно-частотного аналізу. Це дозволяє підвищити точність виявлення нестандартної або шкідливої активності, підвищуючи ефективність виявлення аномальних повідомлень.

Задля захисту від термінації трафіку в IP-телефонії розроблено підсистему на основі нечіткої логіки, яка адаптується до змінних умов і враховує різноманітні критерії для підвищення безпеки та якості зв’язку.

Практична цінність результатів дослідження полягає в тому, що розроблено систему, яка значно підвищує ефективність виявлення зловмисних повідомлень у корпоративних мережах, при цьому знижуючи кількість хибних спрацьовувань. Це забезпечує суттєве зменшення фінансових втрат від VoIP-шахрайства та підвищує надійність зв’язку. Створено прототип програмного рішення для Asterisk із відкритим інтерфейсом налаштування правил реагування, що спрощує впровадження та адаптацію рішення для підприємств різного масштабу. Запропоновані методи нечіткого виведення та онтологічного аналізу можуть бути використані як окремі модулі в існуючих системах безпеки мережі, що покращує масштабованість та гнучкість рішення.

Результати дослідження можуть лягти в основу технічних рекомендацій для IT-відділів корпоративних замовників, а також бути враховані при формуванні політик інформаційної безпеки в галузевих стандартах.

6. Зауваження та дискусійні положення щодо змісту дисертації

Загалом дисертаційне дослідження здійснено на високому науково-прикладному рівні. Проте, оскільки деякі його положення є дискусійними, що пов’язано з складністю досліджуваної предметної області, варто зробити певні уточнення, зауваження та рекомендації з метою подальшого удосконалення досліджуваної проблематики.

1. У тексті дисертації представлено низку математичних співвідношень (формули 2.18–2.27), що відображають реалізацію методу виявлення аномалій в трафіку IP-телефонії на основі групування повідомлень. Хоча теоретична побудова є коректною і логічно обґрунтованою, включення прикладу умовного розрахунку або стислої інтерпретації отриманих результатів дозволило б повніше розкрити прикладне значення запропонованого підходу в контексті виявлення аномалій в трафіку. Такий підхід сприяв би кращому розумінню потенціалу математичного апарату з боку адміністраторів мереж та інших IT-спеціалістів.

2. У роботі описано застосування нечіткої логіки для захисту від термінації трафіку в IP-телефонії, проте не проведено достатньо досліджень для оцінки ефективності запропонованого підходу, зокрема в питаннях підвищенню рівня безпеки та якості зв'язку, що задекларовано у науковій новизні.

3. У четвертому розділі дисертаційного дослідження наведено ряд рисунків, зокрема 4.1.-4.7, 4-19-4.22, які описують відому систему функціонування комп’ютерної мережі університету і які не носять науково-прикладної цінності, їх доцільно було б представити у першому розділі роботи, або винести в додатки. Було б цікавіше побачити як впливає інтеграція запропонованої інтелектуальної системи на функціонування корпоративної мережі в цілому.

4. У четвертому розділі роботи для підтвердження ефективності запропонованого методу виявлення аномальних повідомлень було проведено порівняння з традиційними підходами, зокрема, з методами «ручної ідентифікації», що не дозволяє повністю оцінити досягнуті результати. Для більш комплексної оцінки ефективності доцільно було б здійснити порівняння з відомими інтелектуальними системами, що застосовуються в цій галузі.

5. Висновок щодо методу автоматизованого наповнення онтології тематичних повідомлень у корпоративній системі IP-телефонії, що є суттєвим внеском у підвищення

ефективності побудови онтологічних баз знань для аналізу комунікаційного трафіку потребує додаткової верифікації та подальших досліджень для повного наукового обґрунтування.

6. У тексті дисертаційного дослідження зустрічаються стилістичні неточності при формулюванні деяких тверджень, а також граматичні помилки.

Однак, наведені вище зауваження не зменшують наукової та практичної цінності дисертаційного дослідження в цілому.

7. Висновки

7.1. Дисертаційна робота Романця Ігоря Євгеновича є самостійним, оригінальним, завершеним науковим дослідженням, у якій отримано нові науково-обгрунтовані результати. У дисертації розв’язано актуальне наукове завдання, яке полягає у розробці інтелектуалізованої комп'ютерної системи своєчасного виявлення зловмисних сповідомлень в корпоративній мережі з метою підвищення ефективності захисту IP-телефонії, що базується на онтологічній моделі її функціонування та методах інтелектуального аналізу даних.

7.2. Одержані наукові та практичні результати є вагомим внеском у розвиток теорії та практики розробки та реалізації методів та засобів захисту VoIP-систем в корпоративних мережах . Зміст роботи повністю відповідає спеціальності 05.13.05 – комп'ютерні системи та компоненти.

7.3. Отже, дисертаційна робота «Інтелектуалізована комп'ютерна система виявлення зловмисних повідомлень IP-телефонії в корпоративній мережі» за актуальністю обраної теми, обсягом та рівнем виконаних досліджень, повнотою вирішення поставлених наукових та практичних задач, новизною і ступенем обґрунтованості отриманих результатів, практичних висновків та рекомендацій, повноти викладу в наукових публікаціях, зарахованих за темою дисертації, відсутності порушень академічної доброчесності, відповідає вимогам чинного законодавства України, що передбачені в пп. 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:
завідувач відділу мікропроцесорної техніки №205,
інституту кібернетики
ім. В.М. Глушкова НАН України,
доктор технічних наук, професор Володимир ОПАНАСЕНКО