ВІДГУК

офіційного опонента завідувача кафедри кібербезпеки та комп'ютерної інженерії Київського національного університету будівництва і архітектури, доктора технічних наук, професора, академіка Української академії наук Хлапоніна Юрія Івановича на дисертаційну роботу Бурмаки Івана Анатолійовича на тему «Інформаційна технологія виявлення та аналізу аномальних подій для захисту комп'ютерних мереж малих та середніх підприємств на основі blockchain», представлену на здобуття ступеня доктора філософії в галузі знань 12 Інформаційні технології за спеціальністю 122 Комп'ютерні науки

Актуальність теми дисертації.

Протягом останніх років кількість кібератак на інформаційну інфраструктуру підприємств безперервно зростає, а враховуючи використання кібератак в якості одного із засобів ведення гібридної війни, надійний захист від таких загроз є критично важливим для стабільного функціонування в складних умовах. Ситуація також ускладнюється постійною появою нових видів атак, розроблених для обходу актуальних, на момент їх застосування, захисних систем. Тому швидка реакція та адаптація до нових загроз є ключовими вимогами до сучасних систем захисту від вторгнень.

З огляду на високий інтерес кіберзлочинців до мереж малих та середніх підприємств, нижчу захищеність таких мереж, високу вартість комерційних захисних систем та потребу в кваліфікованих спеціалістах для їх обслуговування, ці мережі часто стають мішенню для кібератак. Щоб зменшити кількість таких інцидентів, необхідно забезпечити захист мереж незалежно від їх масштабу та завантаженості. Таким чином, розробка інформаційної технології для виявлення та аналізу аномальних подій з метою захисту мереж малих і середніх підприємств на основі технології blockchain є актуальним науковим завданням.

Зв'язок роботи з науковими програмами, планами, темами.

Представлена дисертаційна робота запланована та виконана в рамках міжнародного наукового проекту «Cyber Rapid Analysis for Defense Awareness of Real-time Situation – CyRADARS» за грантом NATO SPS, (grant agreement number: G5286)» та відповідно до плану науково – дослідної роботи Національного університету «Чернігівська політехніка» «Розробка моделей та

методів захисту системи від зовнішніх атак з використанням технологій штучного інтелекту» (№0120U101931).

Оцінка обґрунтованості наукових результатів дисертації, їх достовірності та новизни.

Наукова новизна результатів дисертаційного дослідження полягає в наступному:

- Вперше розроблена концептуальна модель розподіленої інформаційної системи виявлення та аналізу аномальних подій в комп'ютерних мережах малих та середніх підприємств, яка на відміну від існуючих містить blockchain компонент для виявлення, накопичення, збереження та спільного використання інформації про аномальні події та блок мультикласифікатора для визначення наявності загрози, що дозволяє підвищити швидкість реагування на невідомі атаки;
- Вперше запропоновано метод вибору протоколу консенсусу для розподіленої системи виявлення вторгнень на основі blockchain, який на відміну від існуючих враховує вимоги до обладнання, масштабування та керування учасниками систем виявлення вторгнень в комп'ютерні мережі, що забезпечує підтримку прийняття рішень при проектуванні систем захисту комп'ютерних мереж малих та середніх підприємств.
- Удосконалено метод консенсусу PoS blockchain технології, який на відміну від існуючих, використовує в якості значення ставки час роботи вузла в розподіленій системі і дозволяє використовувати blockchain для децентралізованого зберігання даних розподіленої системи виявлення вторгнень в комп'ютерні мережі малих та середніх підприємств.
- Набула подальшого розвитку функціональна модель розподіленої системи захисту комп'ютерних мереж на основі blockchain технології для виявлення, накопичення, збереження та спільного використання інформації про аномальні події, яка визначає основні вхідні, вихідні параметри, обмеження та ресурси з трьома рівнями деталізації та є основою для проектування систем захисту комп'ютерних мереж малих та середніх підприємств.

Основні результати дослідження полягають у розробці методів, моделей та алгоритмів захисту комп'ютерних мереж малих та середніх підприємств на основі blockchain.

Практичним результатом дисертації є нова інформаційна технологія виявлення та аналізу аномальних подій для захисту комп'ютерних мереж на основі blockchain, що може бути використана як розробниками систем захисту комп'ютерних мереж, так і мережевими адміністраторами та ІБ спеціалістами малих та середніх підприємств. Також, розроблено програмний модуль blockchain підсистеми, що слугує основою для побудови децентралізованої

розподіленої системи виявлення вторгнень, а також програмний модуль мультикласифікатора, які є частиною інформаційної технології виявлення та аналізу аномальних подій.

Обґрунтованість та достовірність наукових положень, висновків та рекомендацій підтверджується глибоким аналізом наукових праць українських та зарубіжних науковців у відповідних сферах, нормативно-правових актів, аналітичних матеріалів міжнародних організацій, інформаційних ресурсів мережі Internet. Наукові результати дисертації були апробовані, доповідались на міжнародних конференціях та підтверджуються довідками про впровадження. Це загалом підтверджує достатній рівень практичної значимості та обґрунтованості дослідження.

Поставлене наукове завдання в дисертаційній роботі виконано повністю, здобувач повною мірою оволодів методологією наукової діяльності.

Оцінка змісту дисертації, її завершеність та дотримання принципів академічної доброчесності.

За своїм змістом дисертаційна робота здобувача Бурмаки І.А. повністю відповідає Стандарту вищої освіти зі спеціальності 122 Комп'ютерні науки та напрямкам досліджень відповідно до освітньої програми «Комп'ютерні науки».

Дисертаційна робота є завершеною науковою працею і свідчить про наявність особистого внеску здобувача у науковий напрям «Комп'ютерні науки».

Розглянувши звіт подібності за результатами перевірки дисертаційної роботи на текстові співпадіння, можна зробити висновок, що дисертаційна робота Бурмаки Івана Анатолійовича є результатом самостійних досліджень здобувача і не містить елементів фальсифікації, компіляції, фабрикації, плагіату та запозичень. Виявлений відсоток співпадінь пояснюється наведенням у дисертації фрагментів з опублікованих статей автора (на які вказані посилання) та використанням загальноприйнятої наукової термінології. Використані ідеї, результати і тексти інших авторів мають належні посилання на відповідне джерело.

Мова та стиль викладення результатів

Дисертаційна робота написана українською мовою.

Текст дисертації викладений логічно та послідовно, його оформлення відповідає чинним вимогам. Автор дотримується наукового стилю та використовує загальноприйняту термінологію.

Структура та зміст дисертації

Дисертаційна робота складається з вступу, 4 розділів висновків, переліку умовних скорочень, переліку посилань зі 129 джерел та 3 додатків. Загальний обсяг дисертації 231 сторінка.

У вступі дисертації обґрунтовано актуальність досліджуваної теми, сформульовано мету, завдання та методологію дослідження, а також розкрито його зв’язок із науковими програмами кафедри, а також наведено наукову новизну та практичне значення отриманих результатів.

У першому розділі проведено аналіз основних загроз інформаційній безпеці комп'ютерних мереж та факторів, що впливають на їх захищеність. Встановлено, що мережі малих та середніх підприємств особливо вразливі до атак і потребують засобів захисту, здатних швидко виявляти нові, раніше невідомі атаки та ефективно їх блокувати. Крім того, проведено огляд основних методів і засобів захисту комп'ютерних мереж, включаючи як комерційні рішення, так і рішення з відкритим вихідним кодом.

У другому розділі представлено модель розподіленої інформаційної системи для виявлення та аналізу аномальних подій на основі технології blockchain. Описано обґрунтування необхідності використання цієї технології для створення розподіленої системи виявлення вторгнень, для захисту комп'ютерних мереж малих та середніх підприємств. Також визначено основні методи класифікації аномальних подій, які можуть бути інтегровані як окремі модулі в систему виявлення вторгнень, утворюючи комплексний класифікатор для підвищення точності виявлення аномалій. Запропоновано метод вибору протоколу консенсусу для компонента blockchain у розподіленій системі виявлення вторгнень та адаптовано протокол консенсусу PoS для використання в цих системах.

У третьому розділі подано загальну функціональну модель розподіленої системи захисту комп’ютерних мереж, що базується на технології blockchain. Визначено основні вхідні та вихідні параметри, обмеження і ресурси на трьох рівнях деталізації. Архітектура системи представлена за допомогою UML діаграм, що відображають її структуру.

У четвертому розділі розроблено імітаційну модель розподіленої системи захисту комп’ютерних мереж, призначену для тестування компонентів системи в різних умовах і оцінки її продуктивності. Експерименти проведені як у віртуальному середовищі, так і на фізичному обладнанні, з отриманням аналогічних результатів.

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

Оприлюднення результатів дисертаційної роботи

Наукові результати дисертації висвітлені у 10 наукових публікаціях здобувача, серед яких: 1 стаття у науковому виданні, включеному на дату опублікування до переліку наукових фахових видань України; 3 статті у періодичних наукових виданнях, проіндексованих у базі даних Scopus, з яких 2 статті у виданнях, віднесених до третього квартилю (Q3) відповідно до класифікації SCImago Journal and Country Rank або Journal Citation Reports.

Також результати дисертації були апробовані на 4 наукових фахових конференціях.

У наведених публікаціях достатньо повно представлено результати дисертаційної роботи. Порушення академічної доброчесності в них не виявлено. Особистий внесок здобувача у публікаціях, зазначений у дисертації, свідчить про його авторство у відповідних наукових досягненнях.

Таким чином, наукові результати описані в дисертаційній роботі повністю висвітлені у наукових публікаціях здобувача.

Недоліки та зауваження до дисертаційної роботи.

1. Концептуальна модель розподіленої системи виявлення вторгнень на основі blockchain для комп'ютерних мереж малих та середніх підприємств наведена на рисунку 2.1 містить модуль конфігурації, структура якого не деталізована.
2. Наведені в розділі 2.2 класифікатори в основному прості класифікатори (регресійні класифікатори, калсифікатори на основі опорних векторів та інші) але не розглянуто застосування більш складних класифікаторів які можуть забезпечити більш високу точність виявлення аномалій (нейронні мережі, нечітка логіка та інші).
3. При оцінюванні ефективності запропонованого адаптованого протоколу консенсусу (розділ 2.5) бажано було б навести порівняння швидкодії та використання системних ресурсів блокчейн підсистемою з іншими протоколами консенсусу.
4. Не в повній мірі деталізовані характеристики та джерела походження тестового набору даних трафіку який використовувався для тестування запропонованих класифікаторів в пункті 4.2.3 дисертаційної роботи.
5. В пункті 4.3 при тестуванні системи використовувались два типи атак: сканування портів та SYN Flood, але не зовсім зрозуміла поведінка системи при інших видах атак (наприклад CGI Request attack або ARP Storming) які також зустрічаються в комп’ютерних мережах малих та середніх підприємств.
6. В роботі зустрічаються орфографічні та стилістичні помилки.

Вважаю, що висловлені зауваження не є визначальними і не зменшують загальну наукову новизну та практичну значимість результатів та не впливають на позитивну оцінку дисертаційної роботи.

Висновок про дисертаційну роботу

Вважаю, що дисертаційна робота здобувача ступеня доктора філософії Бурмаки Івана Анатолійовича на тему «Інформаційна технологія виявлення та аналізу аномальних подій для захисту комп'ютерних мереж малих та середніх підприємств на основі blockchain» є завершеною науковою працею, в якій отримані обґрунтовані наукові результати.

Диссертація відповідає вимогам, які висуваються до дисертаційних робіт, зокрема зміст дисертації загалом відповідає галузі знань 12 "Інформаційні технології", спеціальності 122 "Комп'ютерні науки", та «Вимогам до оформлення дисертації», затвердженим Наказом Міністерства освіти і науки України від 12.01.2017 р. № 40 (із змінами, внесеними згідно з Наказом Міністерства освіти і науки України від 31.05.2019 № 759) та «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», затвердженому Постановою Кабінету Міністрів України від 12 січня 2022 р. № 44 (в редакції постанови Кабінету Міністрів України від 19 травня 2023 р. № 502), а її автор Бурмака Іван Анатолійович заслуговує на присудження наукового ступеня доктора філософії зі спеціальності 122 «Комп'ютерні науки».

Офіційний опонент:

завідувач кафедри кібербезпеки та комп'ютерної інженерії

Київського національного університету будівництва і архітектури

доктор технічних наук, професор Юрій ХЛАПОНІН

Підпис Хлапоніна Ю.І. засвідчую:

Секретар вченої Ради

Київського національного університету будівництва і архітектури

Микола КЛИМЕНКО

М.П. « 12 » серпня 2024 року