ВІДГУК

офіційного опонента
декана факультету комп'ютерних наук та технологій
Національного авіаційного університету,
д.т.н., професора Гнатюка Сергія Олександровича,
на дисертаційну роботу
Василишина Святослава Ігоровича
«Розробка методу використання програмних приманок як елементів захисту комп'ютерних мереж на основі технології Blockchain»,
подану на здобуття наукового ступеня доктора філософії
за спеціальністю 125 «Кібербезпека та захист інформації»
(галузь знань 12 «Інформаційні технології»)

Актуальність теми дисертації

У дисертаційній роботі Василишини Святослава Ігоровича розглядається проблема захисту комп'ютерних мереж від кібератак, зокрема використання програмних приманок для залучення та виявлення зловмисників. Однак, існують певні виклики та обмеження, які потрібно вирішувати, щоб забезпечити ефективний захист.

Один з таких викликів – централізація. Для забезпечення властивості транслокації програмних приманок використовується більше одного хоста, а потрібен центральний механізм автоматизації. Однак, традиційний метод використовує центральний хост для підтримки властивості автоматизації. Якщо центральний хост вийде з ладу, то вся система може відмовити.

Другий виклик полягає у складності виявлення програмних приманок. Основна мета механізму динамічної транслокації полягає в тому, щоб приховати реальні ресурси. Однак, завдяки технології anti-honeypot підроблені або справжні ресурси можуть бути розпізнані.

Третій виклик пов'язаний з експертизою. Людина, яка здійснює напад, завжди виходить переможцем. Тому для подальшого розслідування необхідно зафіксувати достовірні докази нападу. Необхідно зафіксувати докази нападу для спеціалістів, які надалі будуть займатися розшуком порушника.

У роботі розглядаються переваги та недоліки захисту кіберсистем побудованих на технології Blockchain та розробляється концептуальне рішення з використанням програмних приманок побудованих на технології Blockchain, які використовують властивість децентралізації хоста.

Відповідно, актуальність дисертаційної роботи Василишина Святослава Ігоровича обумовлена необхідністю побудови комп'ютерної мережі на основі технології Blockchain, яка використовує розроблений метод використання програмних приманок як елементів захисту комп'ютерних мереж.

Зв'язок теми дисертації з державними програмами, науковими напрямами університету та кафедри

Дисертаційні дослідження Василишина С.І. виконувалися в межах держбюджетної науково-дослідної роботи «Розроблення та удосконалення методів та засобів захисту інформації для протидії несанкціонованому доступу в інформаційно-комунікаційних мережах» (№ державної реєстрації 0119U101690; терміни виконання – 2019-2022 рр.).

Наукова новизна одержаних результатів

Наукова новизна основних результатів дисертації полягає в розробленні методів використання програмних приманок як елементів захисту комп'ютерних мереж на основі технології Blockchain:

1. *Вперше розроблена* модель динамічної системи активних програмних приманок, що використовують Blockchain технологію. На відміну від відомих дана модель інтегрує децентралізовані та автоматично оновлювані атрибути пасток, що дало змогу підвищити ефективність захисту мережі шляхом зменшення навантаження на мережеву інфраструктуру та часу відгуку сервісів у разі атаки.
2. *Набув подальшого розвитку* математичний опис обчислення динамічних атрибутів програмних приманок, який, на відміну від відомих враховує динамічні та транс локаційні можливості Blockchain-технології Solana. Це дало змогу змоделювати та оптимізувати розподіл ресурсів мережі за рахунок адаптації до змінних умов, що в результаті сприяло підвищенню ефективності захисту, зокрема забезпеченню швидкого відгуку сервісів під час зовнішніх атак.
3. *Вперше*, на основі розробленої моделі динамічної системи програмних (активних) приманок, яка використовує Blockchain-технологію для підтримки безпеки, прозорості та адаптивності до зовнішніх атак, за рахунок плаваючих хостів в мережі та математичного апарату обчислення динамічних атрибутів програмних приманок, *розроблено метод* використання програмних приманок як елементів захисту комп'ютерних мереж на основі технології Blockchain. Цей метод, на відміну від відомих унеможливлює здійснення успішної сніфер атаки за рахунок шифрування, захищає від атаки сканування за рахунок динамічного відкривання та закривання портів, підвищує ефективність захищеності від DDoS атак та зберігає інформацію про атаки на систему на Blockchain-платформі, що забезпечує високий рівень збереження даних та гарантує їхню незмінність.

Ступінь обґрунтованості наукових положень дисертації і їх достовірність та новизна

Наведені в дисертації результати базуються на кваліфікованому підході до постановки завдань досліджень, логічно правильному обґрунтуванню прийнятих

допущень під час вибору математичних моделей і коректному використанні математичного апарату. Крім того, достовірність підтверджується результатами комп'ютерного моделювання і практичною реалізацією системи динамічних програмних приманок, а також збіжністю з результатами експериментальної верифікації.

Наукове значення виконаного дослідження із зазначенням можливих наукових галузей та розділів програм навчальних курсів, де можуть бути застосовані отримані результати

Наукові результати, отримані автором, можуть бути використані при розробці та побудові новітніх мережевих систем, які використовують технологію Blockchain та програмні приманки в якості активного захисту та для підсилення наявних систем захисту в приватних або державних компаніях

Практичне значення дисертаційного дослідження

Практичне значення одержаних результатів полягає у можливості їх безпосереднього застосування для підсилення наявних систем активного та пасивного захисту в корпоративних та державних підприємствах.

1. Розроблена модель динамічної системи активних пасток на основі програмних приманок побудованих на системі Blockchain, яка дала змогу в залежності від різних ситуацій моделювання (в залежності від атаки) до 54% підвищити пропускну здатність каналу та до 204% підвищити швидкість передачі даних під час проведення зовнішніх атак на систему в порівнянні з статичними аналогами.

2. Удосконалення математичного апарату програмних приманок за рахунок додавання та обчислення динамічних атрибутів програмних приманок дало змогу покращити час відгуку сервісів під час атаки типу DDOS на статичні хости, в межах таких значень – MSQL до 34%, NGNIX до 16%, APACHE до 1%, vsFTPd до 13%.

3. Підвищено ефективність захищеності каналів передачі даних в комп'ютерній мережі за рахунок впровадження розробленого методу динамічної системи активних пасток на основі програмних приманок побудованих на технології Blockchain з RSA 2048 - бітовим алгоритмом шифрування. Система активних пасток не дозволяє декодувати інформацію без відповідного ключа конфіденційності, що забезпечує захист каналу передачі даних та запобігає витоку даних через перехоплення та розшифрування інформації під час її передачі. Експеримент з сніфер атакою на розроблену модель системи показує, ефективність реалізації захисту від перехоплення на основі шифрування.

4. Удосконалення алгоритму визначення та передачі вузлових хостів в системі Blockchain, за рахунок впровадження плаваючих хостів в мережі,

підвищило загальну адаптивність мережі реагувати на зовнішні атаки. Цей алгоритм, на відміну від відомих дозволяє системі реагувати на атаки типу сканування та закривати порти доступу реагуючи на зловмисні дії. Результати експерименту під час атаки сканування на відкриті порти дозволили автоматизувати закриття портів, за рахунок зміни основного хоста, що ускладнює збір інформації та можливість доступитись до системи ззовні.

5. Розроблений метод використання програмних приманок, що побудований на основі використання технології Blockchain вимагає більше ресурсів від нападника для здійснення атаки на мережу: потужності комп'ютерів, серверів з яких здійснюється атака а також більше фізичного часу, що збільшує час для фахівців з кібербезпеки для реагування та контр дії нападу до 45%. Було проведено однакову кількість атак як на централізовану систему, яка використовує програмні приманки так і на динамічну систему, яка побудована на розробленому методі. Найбільшу різницю видно не на всіх сервісах: Apache та Nginx динамічної системи зазнають під час атаки майже однакового з центральним аналогом результатів. З тридцяти проведених атак розроблена модель успішно заблокувала 50% в той час як централізована всього 13%, що показує покращення захисних можливостей розробленої моделі. Загальний захист комп'ютерної мережі побудованої з використанням програмних приманок на основі технології Blockchain вищий на 37% в порівнянні з централізованим аналогом, що є підвищенням глобального рівня захисту комп'ютерної мережі в півтора рази.

Результати дослідження впроваджені у навчальний процес кафедри захисту інформації у курсі «Нормативно-правове забезпечення та міжнародні стандарти кібербезпеки» для студентів спеціальності 125 «Кібербезпека», а також впроваджено у технологічні процеси ТОВ «Н-ІКС СПЕЙС» (м. Львів) для підсилення наявних систем моніторингу та попередження несанкціонованого доступу в інформаційних мережах.

Повнота висвітлення результатів в опублікованих працях, апробація роботи

Основні результати дисертаційного дослідження апробовано на міжнародних наукових та науково-практичних конференціях, наукових школах та консорціумах, семінарах:

- VII Міжнародна науково-технічна конференція «Захист інформації і безпека інформаційних систем» (30-31 травня 2019 року, Львів 2019, Україна);
- VIII Міжнародна науково-технічна конференція «Захист інформації і безпека інформаційних систем» (10-11 листопада 2021 року, Львів 2021, Україна);

- The 15th IEEE International Conference on Computer Sciences and Information Technologies (23-26 вересня, 2020 року, Збараж, Україна);
- IV Всеукраїнська науково-практична конференція молодих учених, студентів і курсантів (26 листопада 2020 року, Київ 2020 р, Україна);
- VI Міжнародна науково-технічна конференція «Захист інформації і безпека інформаційних систем» (01-02 червня 2017 року, Львів 2017, Україна);
- Міжвідомчі міжрегіональні семінари Наукової Ради НАН України "Технічні засоби захисту інформації" (11 квітня 2018 року, 11 квітня 2019 року, 10 грудня 2020 року, Львів, Україна);
- Наукові семінари кафедри захисту інформації (2018-2023 рр.).

Основні результати дисертаційної роботи Василишина С.І. достатньо повно відображені у 19 наукових публікаціях, з яких 7 статей у наукових фахових виданнях України, 4 статті у наукових виданнях інших держав, які входять до міжнародної наукометричної бази Scopus, та 8 матеріалів конференцій.

Загальна характеристика структури та змісту дисертаційної роботи

Структура дисертації цілком відповідає логіці й послідовності вирішення поставлених задач. Наукова робота складається з анотації, змісту, переліку скорочень, вступу, чотирьох основних розділів, списку використаних джерел та додатків.

У вступі зазначено актуальність теми дисертації, сформульовано мету і задачі досліджень, заявлено наукову новизну та практичне значення отриманих результатів, представлено зв'язок роботи з науковими програмами, планами і темами, особистий внесок здобувача, перелік публікацій і апробації результатів.

Перший розділ присвячено вивченню досліджень та публікацій, що стосуються актуальної тематики Blockchain та програмних приманок. У цьому розділі проводиться детальний огляд технології програмних приманок, розглядаються їх потенційні можливості, значні переваги, неминучі недоліки, різні рівні взаємодій між компонентами, особливості внутрішнього дизайну та відповідні перешкоди, які можуть виникнути під час їх розгортання. Також у даному розділі звертається увага на актуальні проблеми, пов'язані з використанням приманок та обманок у контексті захисту даних у комп'ютерних мережах.

У другому розділі дисертації досліджуються можливості застосування Blockchain для захисту даних в різних кібер-областях, зокрема на об'єктах інфраструктури. Розглядаються сфери впливу, в яких дана технологія може розповсюджуватись, та як вона потенційно може використовуватись на об'єктах інфраструктури. Вивчаються можливості використання технології Blockchain в таких актуальних структурах, як урядові та військові організації, а також

перспективи та можливості в комбінуванні з штучним інтелектом, великими даними та іншими передовими технологіями.

У третьому розділі дисертації акцентується увага на методі, моделюванні та архітектурі динамічної системи, яка використовує програмні приманки та динамічні властивості Blockchain. У цьому розділі детально вивчається динамічна розподілена система управління, яка використовує динамічні властивості Blockchain та представляється розроблений метод використанні цієї системи.

У четвертому розділі проводиться дослідження стійкості розробленої системи до різних видів атак, експериментальний аналіз рівня безпеки та оцінка ефективності системи в порівнянні з існуючими рішеннями. Досліджено рівень безпеки системи та рішення щодо її захисту від трьох видів атак: атак сканування, сніфер та DDoS.

У висновках сформульовані основні результати дисертаційної роботи.

Відсутність (наявність) порушення академічної доброчесності

У дисертаційній роботі відсутні порушення академічної доброчесності. Використанні ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

Зауваження щодо змісту і результатів роботи:

1. У першому розділі дисертаційної роботи автор досліджує більшість робіт закордонних колег, проте бажано було б звернути більше уваги на дослідження українських науковців, які працюють у даній галузі. Приклади досліджень з українських джерел допоможуть показати наявність та внесок національних науковців у розвиток даної тематики, а також більш повно оцінити стан справ у цій галузі та оцінити рівень отриманих результатів.

2. У другому розділі дисертаційної роботи зосереджено увагу на дослідженні використання технології Blockchain та її динамічних атрибутів у контексті кіберзахисту. Однак, варто було б розглянути різні методи та підходи, які використовують технологію Blockchain у наведених дисертантом сферах. Пояснення відмінностей та переваг різних підходів надало б змогу краще зрозуміти можливості технології в контексті захисту.

3. У другому розділі, на стор. 95, представлено рис. 2.3, який відображає методологію використання Blockchain для виявлення зловмисників на полі бою. Але сама методика, що представлена на зазначеному рисунку, не була достатньо відображена у роботі. Необхідно було детальніше описати розроблену методологію та як саме технологія Blockchain допомагає виявляти зловмисників

(у порівнянні з аналогами), а також які механізми використовуються для цієї мети.

4. У четвертому розділі, на стор. 143-144, наведено табл. 4.3, яка порівнює розроблений прототип системи з іншими системами, що мають встановлені програмні приманки. Проте у самій дисертаційній роботі автором не описано обґрунтування обраних критеріїв для порівняння. Розгорнуті пояснення для кожного з критеріїв підвищили б ґрунтовність переваг розробленого методу над існуючими аналогами.

5. Тестування розробленого методу використання програмних приманок проводилося з використанням зовнішніх атак, проте у роботі не було розглянуто внутрішні загрози для побудованої мережі. Додаткове включення інших видів атак, включаючи внутрішні, допоможе більш повно оцінити ефективність розробленого методу у різних сценаріях.

6. На мою думку, пункти наукової новизни сформульовані дисертантом не у повній мірі відповідно вимогам і рекомендованим підходам – це дещо ускладнює розуміння результатів і шляхів їх досягнення.

7. Другий науковий результат, я вважаю, необхідно було б замість «набув подальшого розвитку математичний опис обчислення динамічних атрибутів програмних приманок…» сформулювати так: «набула подальшого розвитку математична модель обчислення динамічних атрибутів програмних приманок…».

8. Відсутній інтегрований кількісний показник, що згідно мети дисертації характеризує «підвищення ефективності захисту комп'ютерних мереж…», це дещо ускладнює розуміння її досягнення. Проте, варто відмітити, присутність значної кількості кількісних параметрів у висновках роботи.

9. У дисертаційній роботі зазначено наявність великої кількості скорочень, не досить вдалих стилістичних речень, різної термінології для опису одних і тих самих речей та граматичних помилок. Однак, після ретельного перегляду та редагування тексту можна забезпечити єдність термінології та стиль, що сприятиме більш гармонійному викладенню ідей та допоможе зрозуміти дослідження більш чітко й логічно.

Проте зазначені зауваження не носять принциповий характер і не знижують цінності проведеного здобувачем дослідження, актуальності, новизни та практичної значущості дисертаційної роботи.

Висновки щодо відповідності дисертації встановленим вимогам

Дисертаційна робота за актуальністю, науковою новизною, практичним значенням, особистим внеском автора, обсягом і рівнем публікацій,

достовірністю відповідає встановленим вимогам до дисертації. Результати роботи викладені чітко, послідовно і логічно, висновки за розділами та загальні висновки дисертації містять якісні і кількісні наукові та практичні результати. За поставленою метою та вирішеними задачами, об'єктом та предметом досліджень, отриманими результатами робота Василишина Святослава Ігоровича відповідає вимогам до дисертаційних досліджень спеціальності 125 «Кібербезпека та захист інформації».

Загальні висновки щодо дисертаційної роботи

За результатами аналізу змісту дисертації вважаю, що дисертація Василишина Святослава Ігоровича є завершеним науковим дослідженням, у якому розв'язана важлива науково-практичне завдання підвищення ефективності виявлення кіберзлочинів та покращення стійкості захисної системи за рахунок розробки системи приманок на основі динамічних атрибутів Blockchain.

Враховуючи актуальність, наукову новизну і практичне значення одержаних результатів, вважаю, що дисертаційна роботи «Розробка методу використання програмних приманок як елементів захисту комп'ютерних мереж на основі технології Blockchain» цілком відповідає вимогам пп. 6,7,8,9, які встановлені у «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», який затверджений Постановою Кабінету Міністрів України від 12.01.2022 р. №44, а її автор Василишин Святослав Ігорович заслуговує на присудження наукового ступеня доктора філософії за спеціальністю 125 «Кібербезпека та захист інформації».

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

«04» серпня 2023 року

ВІДДІЛ КАДРІВ
ПОСВІДЧУЮ