https://doi.org/10.31891/2307-5732-2025-349-50
УДК 004.7:004.75:004.49:004.62

КАШТАЛЬЯН АНТОНІНА
Хмельницький національний університет
https://orcid.org/0000-0002-4925-9713
e-mail: yantonina@ukr.net

МЕТОД ВИЯВЛЕННЯ ЗЛОВМИСНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА КОМП'ЮТЕРНИХ АТАК МУЛЬТИКОМП'ЮТЕРНИМИ СИСТЕМИ АНТИВІРУСНИХ КОМБІНОВАНИХ ПРИМАНОК ТА ПАСТОК

У межах дослідження розроблено новий метод виявлення зловмисного програмного забезпечення (ЗПЗ) та комп'ютерних атак (КА) мультикомп'ютерними системами на основі впровадження антивірусних комбінованих приманок і пасток. Запропоновано модель, що передбачає включення до складу системи множини приманок, відмінних за архітектурними характеристиками, функціональним призначенням і тактикою поведінки у віртуальному середовищі. Частина таких компонентів виконує роль інтелектуальних агентів, здатних до автономного прийняття рішень, взаємодії між собою та координації дій з центральним вузлом системи.

Формалізовано механізми функціонального розподілу завдань між приманками з урахуванням їх здатності до багатоцільового використання, що дозволяє підвищити ефективність використання ресурсів системи. Визначено, що кожна приманка може бути залучена до кількох етапів обробки подій, виконуючи як роль ініціатора реагування, так і елементу колективного аналізу.

Реалізовано трирівневу модель опрацювання подій у системі, що складається з: 1) первинного аналізу подій окремою приманкою; 2) групового узгодження результатів кількома приманками, які взаємодіють у рамках визначених сценаріїв; 3) комплексної обробки всією системою з урахуванням зібраної інформації на попередніх етапах. Такий підхід забезпечує гнучкість системи при реагуванні на загрози, а також дозволяє динамічно адаптувати поведінкові патерни залежно від типу і характеристик атакуючої дії.

Завдяки застосуванню варіативних обманних механізмів досягнуто підвищення рівня протидії сучасним типам ЗПЗ і КА. Продемонстровано, що така архітектура дозволяє не лише зменшити ймовірність успішного проникнення зловмисника до критичних елементів системи, але й сприяє накопиченню аналітичної інформації для подальшої ідентифікації та нейтралізації загроз.

Ключові слова: мультикомп'ютерні системи, приманки, пастки, комп'ютерні атаки, зловмисне програмне забезпечення, обманні системи

KASHTALIAN ANTONINA
Khmelnytskyi National University

METHOD OF DETECTING MALICIOUS SOFTWARE AND COMPUTER ATTACKS WITH MULTI -COMPUTER ANTIVIRAL COMBINED BAITS AND TRAPS

The study has developed a new method of detecting malicious software (RFS) and computer attacks (CA) with multi -computer systems based on the introduction of antiviral combined baits and traps. A model is proposed, which involves the inclusion in the system of many baits, different in architectural characteristics, functional purpose and tactics of behavior in the virtual environment. Some of these components acts as intellectual agents capable of autonomous decision -making, interaction with each other and coordinating actions with the central node of the system.

The mechanisms of functional distribution of tasks between baits are formalized, taking into account their ability to multi -purpose use, which increases the efficiency of system resources. It is determined that each bait can be involved in several stages of processing of events, performing both the role of the initiator of the response and the element of collective analysis.

A three -tier model of event processing in a system consisting of: 1) primary analysis of events with a separate lure was implemented; 2) group coordination of the results by several lures that interact in the framework of certain scenarios; 3) comprehensive processing by the whole system, taking into account the information collected in the previous stages. This approach provides the flexibility of the system when responding to threats, and also allows you to dynamically adapt behavioral patterns depending on the type and characteristics of the attacking action.

Due to the use of variational fraudulent mechanisms, an increase in the level of counteraction to modern types of RFS and CA has been achieved. It is demonstrated that such architecture not only reduces the likelihood of successful penetration of the attacker into the critical elements of the system, but also contributes to the accumulation of analytical information to further identify and neutralize threats.

Keywords: multicomputer systems, baits, traps, computer attacks, malicious software, deception systems

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями

У сучасному цифровому світі, де кіберзагрози набувають усе складніших форм, одним із ефективних інструментів захисту є обманні системи з приманками, відомі як honeypots, honeynets та honeytokens [1]. Ці системи створюються з метою імітації вразливих або цінних ресурсів [2], на які зловмисники можуть звернути увагу. Основна їх мета — виявлення, ізоляція, аналіз шкідливої активності та отримання інформації про методи і стратегії нападників.

Проєктування таких систем пов'язане з низкою викликів [3]. Передусім необхідно визначити рівень інтерактивності. Низькоінтерактивні системи [3] простіші у реалізації та безпечніші, але менш привабливі для зловмисників, тоді як високоінтерактивні надають реалістичну взаємодію, але становлять вищий ризик бути використаними для справжніх атак. Іншим критичним аспектом є реалістичність. Якщо система виглядає неприродно або не відповідає типовій поведінці справжнього середовища, досвідчений

зловмисник може швидко виявити пастку [1]. Важливу роль відіграє також правильне логування та моніторинг усіх дій, що вимагає значних ресурсів і ефективних аналітичних інструментів [3].

Застосування обманних систем також не позбавлене труднощів. Недостатньо захищені honeypots можуть бути використані самими хакерами для проведення атак на інші об'єкти [3]. Додатковою проблемою є підтримка таких систем. Потрібно регулярно оновлювати програмне забезпечення, адаптувати середовище до нових загроз і виявляти нові методи приховання присутності. Попри це, переваги використання обманних систем суттєві. Вони дозволяють виявити вторгнення на ранньому етапі, отримати цінну інформацію про зловмисників, вдосконалити стратегії захисту мереж і використовуються як потужний інструмент навчання для спеціалістів у сфері кібербезпеки.

Таким чином, хоча впровадження обманних систем у комп'ютерних мережах супроводжується низкою проєктних та прикладних викликів, їх значення в сучасній кібероборі зростає [3], особливо в умовах постійного ускладнення кіберзагроз. Залишається актуальною проблемою покращення виявлення зловмисного програмного забезпечення та комп'ютерних атак з використанням приманок та пасток в комп'ютерних системах за рахунок організації їх функціонування та удосконалення внутрішньої будови.

Аналіз досліджень та публікацій

Сфера корпоративних обманних систем є активною сферою розробки та досліджень. Завдяки широкому різноманіттю обманних систем та різним методам їх застосування у кібербезпеці, класифікація таких систем не є простим завдання, і в ряді робіт пропонується класифікувати обманні системи за різними ознаками, які частково перетинаються. В роботі [1] проведено широкий огляд методів обману, із класифікаційних ознак запропоновано використовувати мету обману, одиницю обману, рівень обманних систем та спосіб розгортання. В цій роботі також запропоновано класифікацію моделей обманних систем відповідно до таких ознак: модель процесу, яка визначає бажаний процес та спосіб його виконання; ймовірнісна модель, яка використовує ймовірність для оцінки переваг та вартості обманних дій; практична модель, яка використовує графіки атак; теоретико-ігрова модель, яка дозволяє визначити оптимальну стратегію обману. Огляд проблематики приманок та стратегій захисту, які використовують обманні методи, проведено класифікацію приманок за різними категоріями проведено в [2]. В роботі [3] запропоновано модель кіберланцюга виявлення атак, який враховує етапи проведення атаки, запропоновано класифікацію за типом обману, стратегією розгортання приманок, рівнем обманні системи. Класифікація за типом обману також розглянута в роботі [4], в якій крім того використовується як класифікаційна ознака мета обманні системи. А також різні типи обману виділено в роботі [5], в якій запропоновано класифікацію методів обману відповідно до принципів теорії ігор. В роботі [6] запропоновано дворівневу класифікацію обманних систем, яка включає не тільки класифікацію приманок, а також класифікацію програмного забезпечення; приманки класифікуються за ознаками рівня взаємодії, масштабованості, адаптивності, ролі, рівня ресурсів, стратегії розгортання, типу ресурсів; програмне забезпечення класифікується за ознаками типу спостереження атак, запобігання атакам, виявлення атак, відповідь на атаку, профілювання атак.

Ряд досліджень присвячено окремим напрямкам обманних систем. В роботі [7] проведено огляд відкритого програмного забезпечення приманок, їх фрейморки, інструменти розробки та розгортання, системну архітектуру, методи виявлення та уникнення приманок, запропоновано класифікацію за типами приманок, сценаріями розгортання, рівнями взаємодії, методами виявлення. Окремим напрямом є динамічні обманні системи, в роботі [8, 9] проведено огляд динамічних приманок, розглянуто обманні системи, які мають мету виявлення, запобігання та реагування на атаки, а також взаємодія обманних систем із системами виявлення вторгнень. Окремі роботи присвячені таким обманним методам та засобам, як honey-x [10, 11] та захист рухомою ціллю. В роботі [12, 13] проведено огляд останніх досліджень в розвитку захисту рухомих цілей, класифіковано засоби захисту на різні підкласи в залежності від того, що, коли і як вони змінюють.

Обманні системи, що розробляються для певних типів цільових систем, потребують окремих класифікаційних ознак, зокрема це стосується веб-застосунків, IoT систем, хмарних сервісів, промислових систем та мереж, тощо. В роботі [14, 15] розглянуто застосування методів обману в контексті виявлення атак веб додатків. Проведено класифікацію приманок та їх систем в [16, 17]; системи, які використовуються в IoT пристроях та кіберфізичних системах класифікують за такими ознаками, як мета, роль, рівень взаємодії, масштабованість, рівень ресурсів, доступність вихідного коду, цільова система

Формулювання цілей статті

Метою роботи є покращення виявлення зловмисного програмного забезпечення та комп'ютерних атак мультикомп'ютерними системами антивірусних комбінованих приманок та пасток. Для хабехпечення покращення необхідно розробити метод організації функціонування мультикомп'ютерних систем антивірусних комбінованих приманок та пасток. Безпосередньо архітектура обманних систем на основі мультикомп'ютерних підходів була розроблена в [1, 3].

Виклад основного матеріалу

Обманні системи класифікують за набором ознак, серед яких: тип обману, мета обману, рівень системи, тип розгортання, рівень поведінки та відповідей системи, керування системою. Тип обману характеризується інформаційними структурами, діями та тривалістю. Типи обману, які використовують

обманні системи: honey-x об’єкти, захист рухомою ціллю, заплутування, збурення та залучення зловмисників. В сучасних обманних системах найбільш поширеними обманними об’єктами є honey-x та об’єкти захисту рухомою ціллю. До класу honey-x входять об’єкти, які прийнято називати термінами з початком honey-, це honeypots, honeynets, honeytokens, honeymails, honeyurs тощо. Статична та передбачувана поведінка цільових систем має значні переваги зловмисникам для планування успішних атак. Захист рухомої цілі змінює налаштування основної системи, зменшуючи рівень успішності кібератак. Зміни налаштувань, або кібермутації, засновані на захисті рухомих цілей, дозволяють системам автоматично змінювати свої параметри конфігурації в непередбачуваний, безпечний та адаптивний спосіб для проактивного обману зловмисників. Кібермутації включають мутацію хостів, маршрутів та віртуальних мереж.

Головна мета обманних систем, які вони намагається досягти, відповідає стадії боротьби з атакою. Відповідно до мети обманні системи призначені для: покращення запобігання атакам; вдосконалення виявлення атак; пом’якшення наслідків успішних атак.

Одиниця обману стосується рівня деталізації активу об’єкта, який використовується для здійснення обману. До одиниць обману відносяться рішення/вибір (наприклад, рішення про прийняття з’єднання від IP-адреси, яка не використовується), відповідь (наприклад, імітація мережної відповіді), сервіс (наприклад, сервіс приманки), діяльність (наприклад, обчислювальна активність приманки), слабкість (наприклад, імітована вразливість), продуктивність (наприклад, затримка відповіді), конфігурація (наприклад, імітація топології мережі) та дані (наприклад, обліковий запис). Одиниці обману можуть використовуватися як окремо, так і комбінуватися в різних поєднаннях.

Рівень обманної системи відображає рівень цільової системи, яка захищається. Відповідно до рівня цільової системи виділяють такі рівні обманних систем: рівень мережі; рівень системи; рівень застосунку; рівень даних. Тип розгортання обманних систем характеризує шлях, яким обманні системи інтегруються в цільові системи. Залежно від рівня інтеграції обманні системи можуть бути вбудовані, додані під час функціонування цільової системи, встановлені перед цільовою системою та ізольовані. Вбудовані системи мають найвищий рівень інтеграції та інтегруються в захист цільових систем на етапі планування та розробки. Системи, що додаються під час функціонування, передбачають динамічне конфігурування обманних об'єктів в процесі функціонування цільової системи. Обманні системи, встановлені, перед цільовою системою, та ізольовані мають найменший ступінь інтеграції. Рівень поведінки та відповідей обманних систем характеризує рівень обману, який може забезпечити система відповідно до відповідей на сервісні запити. Відповідно до рівня інтелектуальності відповідей поведінка обманної системи може бути правдива, наївно оманлива та інтелектуально оманлива. В системах з правдивою поведінкою відповіді на будь-який запит завжди відображають дійсні внутрішні стани системи. В системах з наївно оманливою поведінкою процеси намагаються обманути користувача з яким взаємодіють, штучними відповідями. Однак, якщо користувачу відома ця оманлива поведінка з попередньої взаємодії, обман може бути виявлений та попередить зловмисника про наявність обманні системи. Найвищий рівень захисту цільової системи забезпечує система з інтелектуально оманливою поведінкою, завдяки чому функціонування такої обманні системи для користувача не відрізняється від функціонування цільової системи навіть за умови попередньої взаємодії. Така поведінка системи передбачає використання інтелектуальних методів обробки запитів користувачів, в тому числі методів машинного навчання та штучного інтелекту.

Організація керування обманною системою характеризує взаємодію між компонентами обманної системи та взаємодію із цільовою системою. В залежності від рівня централізації обманні система може бути централізована, частково централізована, частково децентралізована та децентралізована.

Топологія обманні системи може бути статичною та динамічною. Обсяг обманних дій, що використовуються обманні системами, може змінюватися від низького рівня до високого. Час обманних дій може змінюватися від короткотривалого то тривалого. Обманні системи містять механізми для протидії різним типам атак, включаючи: DoS атаки; розподілені DDoS атаки; атаки, що маніпулюють логікою; атаки, що використовують прогалини в протоколах; атаки; що використовують переповнення буфера тощо. Тип цільової системи, для якої захисту якої призначена обманна система, характеризує власне цільову систему. Спектр вразливостей сучасних систем постійно розширюється із розвитком сучасних технологій, відповідно додається різновидів систем, для яких розробляють обманні системи. Зростання використання пристроїв IoT, що піддаються атакам, вимагає застосування механізмів захисту на основі приманок для різних типів таких пристроїв, зокрема пристроїв відеоспостереження та відеокамер, інфраструктури вимірювальних приладів тощо.

В сучасних обманних системах honey-x є найбільш поширеними обманними об'єктами, призначеними для моніторингу та аналізу дій зловмисників та взаємодії із ними. До класу honey-x входять об'єкти, які називаються термінами з початком honey-, це honeypots, honeynets, honeytokens, honeymails, honeyurl, тощо (табл. 2). Об'єкти honey-x використовуються як в самостійних, так і в комбінованих стратегіях захисту.

Таблиця 1

Класифікація обманних систем

Характеристика	Типи	Характеристика	Типи
Тип обману	- збурення (perturbation); - захист рухомої цілі (moving target defense); - заплутування (obfuscation); - змішування (mixing); - honey-x; - залучення зловмисника (attacker engagement) honey-x об'єкти призначені для залучення	Цільова система	- IoT; - промислова системи та мережі; - цифрові двійники; - бази даних; - веб-застосунки; - хмарні сервіси
Мета обманних систем	- покращити запобігання атаці; - вдосконалити виявлення атаки; - пом'якшити наслідки успішної атаки	Типи атак	- DoS атака; - DDoS атака; - атаки, що маніпулюють логікою; - атаки, що використовують прогалини в протоколі; - атаки, що використовують переповнення буфера
Одиниця обману	- рішення; - відповідь; - сервіс; - діяльність; - слабкість; - продуктивність; - конфігурація; - дані	Розмір обманних систем	- обсяг при розгортанні на хості; - обсяг при розгортанні в корпоративних мережах
Рівень обманних систем	- мережа; - система; - застосунок; - дані	Обсяг обману можливо застосовувати до обманних об'єктів	- низького рівня; - високого рівня
Розгортання обманних систем	- вбудована обманні система; - обманні рішення, додане під час функціонування цільової системи; - обманні система, встановлена перед цільовою системою; - ізольована обманні система	Час обману можливо застосовувати до обманних об'єктів	- короткочасний обман; - тривалий обман
Рівень поведінки та відповідей системи	- правдива; - наївно оманлива; - інтелектуально оманлива	Периметр захисту цільової системи	- зовнішній; - внутрішній; - зовнішній та внутрішній
Організація керування обманними системами	- централізована; - частково централізована; - частково децентралізована; - децентралізована	Доступність використання	- open-source; - комерційні
Топологія мережі обманних систем	- статична; - динамічна		

Таблиця 2

Приклади honey-х об'єктів, які використовуються в обманних системах [9, 13]

Метод	Обманна сутність	Домен	Хост (host-based)	Мережа (network-based)
honeypot	приманка	сервер		+
honeyentry	таблиця, набір даних	база даних	+	
honeyword	пароль	аутентифікація	+	
honeyaccount	користувацький обліковий запис	аутентифікація	+	
honeyfile ‘honey’-файл	файл (файл в хмарному середовищі)	файлова система	+	+
honeynet	множина приманок	мережа		+
honeyfarm	множина приманок та інструментів аналізу	система, мережа	+	+
honeytoken	об'єкт цифрових даних	база даних, файлова система	+	

Метод виявлення ЗПЗ та КА мультикомп’ютерними системами

Для виявлення ЗПЗ та КА мультикомп’ютерними системи антивірусних комбінованих приманок та пасток розробимо відповідний метод, в якому буде враховано виявлення саме мультикомп’ютерниими системами, до складу яких потрібно залучати множину приманок різної архітектури та призначення і, при цьому, частина з них можуть взаємодіяти між собою як інтелектуальні агенти, а також залучення приманок до складу мультикомп’ютерних систем повинно бути здійснено на основі їх поділу між завданнями системи. Для виконання певного завдання можуть бути залучені приманки різних типів, тобто частина приманок може мати декілька функцій і виконувати декілька завдань. Крім того, певна частина приманок для виконання завдань може здійснювати комунікацію між собою з інформуванням центру системи та опрацювання подій сумісно.

Основні кроки методу виявлення ЗПЗ та КА мультикомп’ютерними системи антивірусних комбінованих приманок та пасток

1) активізація приманок після увімкнення комп’ютерних станцій;

2) встановлення зв’язків з компонентами мультикомп’ютерної системи;

3) включення приманок до складу мультикомп’ютерної системи;

4) ідентифікація та поділ приманок на групи за їх призначенням;

5) ідентифікація та поділ приманок на групи за їх типами внутрішньої архітектури;

6) визначення групи приманок, які можуть взаємодіяти між собою та мати функції інтелектуальних агентів;

7) встановлення відповідності між завданнями мультикомп’ютерної системи і приманками та їх групами;

8) отримання зовнішніх та внутрішніх впливів на приманки з групи, в якій приманки можуть опрацьовувати такі події, і надсилання інформації про події до центру мультикомп’ютерної системи;

9) виконання кроку 8) *методу [3] організації функціонування мультикомп’ютерних систем з вибору приманки чи приманок для виконання завдань із обов’язковим врахуванням їх функцій винагороди;*

10) фіксування мультикомп’ютерною системою подій, які не зафіксовані приманками, їх опрацювання і виконання кроку 9) із залученням приманок з групи тіньових приманок;

11) отримання зовнішніх та внутрішніх впливів на приманки з групи, в якій приманки можуть опрацьовувати такі події, і надсилання інформації про події до центру мультикомп’ютерної системи та опрацювання подій самостійно з повідомленням в центр системи або із залученням певних приманок та інформуванням про це центр системи;

12) повідомлення в центр системи про неможливість виконати завдання в зв’язку з вимкненням комп’ютерної станції чи пристрою;

13) повідомлення в центр системи про неможливість виконати завдання приманкою;

14) повідомлення в центр системи про вимкнення комп’ютерної станції чи пристрою і, відповідно, від’єднання приманки з мультикомп’ютерної системи.

Суть методу виявлення ЗПЗ та КА мультикомп’ютерними системи антивірусних комбінованих приманок та пасток полягає в тому, що до складу мультикомп’ютерних систем залучається множина

приманок різної архітектури та призначення і, при цьому, частина з них можуть взаємодіяти між собою як інтелектуальні агенти, а також залучення приманок до складу мультикомп'ютерних систем здійснюється на основі їх поділу між завданнями системи, для виконання яких можуть бути залучені приманки різних типів, тобто частина приманок може мати декілька функцій і виконувати декілька завдань. Частина приманок в процесі виконання завдань з опрацювання подій в системі може здійснювати комунікацію між собою з інформуванням центру системи та опрацювання подій сумісно. В результаті такої конфігурації при опрацюванні подій застосовується трьохетапний аналіз подій, який включає опрацювання на першому етапі безпосередньо приманкою, на другому етапі – групою приманок, на третьому етапі – системою з приманками. Це дає змогу системі здійснити різні обманні дії щодо зловмисних дій, зловмисного програмного забезпечення та комп'ютерних атак завдяки урізноманітненню варіантів відповідей.

Експерименти

Було сформовано експериментальне середовище з метою оцінювання ефективності мережі комбінованих антивірусних приманок у процесі виявлення ЗПЗ та КА мультикомп'ютерними системами. Для цього створено віртуалізовану мультикомп'ютерну мережу, яка імітує інфраструктуру організації середнього рівня складності, що включає 15–20 вузлів. До складу моделюваної мережі входили сервери загального призначення (файлові, поштові, веб), робочі станції з різними операційними системами (Windows, Linux), а також вузли безпеки, до яких інтегровано приманки різного функціонального типу: сервісні, файлові, системні та мережеві. Керування мережею приманок здійснювалося через централізований контролер обробки подій. Приманки були впроваджені з урахуванням гетерогенності системи і поділялися на пасивні, активні та інтелектуальні. Пасивні приманки фіксували спроби сканування портів та несанкціонованих підключень. Активні моделі імітували поведінку вразливих сервісів, вступаючи в інтеракцію зі зловмисним ПЗ, тоді як інтелектуальні агенти реалізовували механізми міжвузлової комунікації, аналізу подій і передачі інформації до центрального елементу системи. У конфігурації системи передбачалася можливість виконання приманками кількох функцій одночасно, залежно від контексту подій у мережі. У межах експерименту було змодельовано серію типових атак, серед яких: мережне сканування, спроби отримання несанкціонованого доступу, розгортання ЗПЗ, а також міжвузлове поширення зловмисного коду. Приманки реагували на ці події відповідно до трирівневої моделі аналізу: спочатку подію обробляла окрема приманка, далі інформація передавалася до групи приманок для колективного аналізу, і на завершальному етапі здійснювалася інтегральна обробка події всією системою. Для кожного сценарію фіксувалися такі параметри: час реагування окремої приманки, кількість виявлених загроз на кожному етапі, частка хибнопозитивних і хибнонегативних спрацювань, ефективність комунікації між приманками, а також рівень навантаження на центральний вузол.

Оцінювання ефективності проводилося за множиною показників, зокрема точністю виявлення загроз (true positive rate, false positive rate), середнім часом реагування системи, коефіцієнтом узгодженості рішень між елементами системи та ефективністю обманних механізмів, що оцінювалася за здатністю приманок відволікати дії шкідливого програмного забезпечення від реальних вузлів мережі.

За результатами експериментального дослідження функціонування мережі комбінованих антивірусних приманок у мультикомп'ютерній системі було отримано низку кількісних та якісних показників, що засвідчують ефективність запропонованої архітектури. У ході моделювання 50 сценаріїв атак різної складності (у тому числі типові мережеві сканування, атаки з використанням експлойтів, спроби несанкціонованого доступу та поширення шкідливого ПЗ) фіксувались ключові метрики на кожному з трьох рівнів обробки подій.

Середній час реагування окремої приманки на подію становив **1,4 с**, при цьому час узгодженого реагування групи приманок був **3,2 с**, а повний цикл обробки події на рівні системи — **4,8 с**. Такий показник підтверджує допустимий рівень латентності для оперативного реагування в реальному часі.

Загальна точність виявлення загроз становила **96,2%**, при цьому частка хибнопозитивних спрацювань (FPR) не перевищувала **2,8%**, а хибнонегативних (FNR) — **1,0%**. У 94% випадків саме інтелектуальна взаємодія між приманками дозволила підтвердити загрозу, яку окрема приманка ідентифікувала з невисоким рівнем впевненості. Це свідчить про доцільність використання колективної обробки та розподілу завдань між приманками різного типу.

Коефіцієнт узгодженості рішень між приманками (узгодженість між локальним і груповим аналізом) склав **92,7%**, що вказує на ефективну синхронізацію процесів виявлення на різних рівнях. Оцінка ефективності обманних механізмів показала, що у **87%** атакуючих сесій зловмисне програмне забезпечення було залучене в імітоване середовище, що дало змогу відволікти його від реальних вузлів і отримати повну сесію взаємодії для подальшого аналізу.

Особливо високу ефективність виявлено для атак, що базувалися на ручному проникненні та використанні експлойтів: 100% таких спроб були зафіксовані вже на першому рівні реагування, що засвідчує високу чутливість системи до активних вторгнень. У випадках застосування поліморфного ЗПЗ точність виявлення була трохи нижчою (91,5%), однак після колективного аналізу вона зростала до 97,8%.

Загалом експеримент підтвердив гіпотезу про ефективність використання мережі комбінованих приманок з розподіленими функціями аналізу подій. Запропонована архітектура дозволяє не лише виявляти загрози з високою точністю, а й здійснювати ефективне управління реагуванням завдяки

скоординованій роботі елементів системи, здатних до обміну інформацією і прийняття рішень в умовах невизначеності.

Висновки з даного дослідження
і перспективи подальших розвідок у даному напрямі

Таким чином, виявлення зловмисного програмного забезпечення та комп'ютерних атак у мультикомп'ютерних системах з використанням антивірусних комбінованих приманок і пасток ґрунтується на інтеграції до їх складу множини приманок, що відрізняються за архітектурою та функціональним призначенням. Частина таких приманок функціонує як інтелектуальні агенти, здатні до взаємодії між собою з метою колективної обробки подій та інформування центрального вузла системи. Формування зазначеної множини здійснюється з урахуванням принципу розподілу задач між приманками різних типів, причому окремі з них можуть мати багатофункціональний характер, виконуючи декілька завдань одночасно.

У процесі аналізу подій така система реалізує трирівневий підхід: на першому етапі – первинна обробка подій окремою приманкою, на другому – колективний аналіз групою взаємодіючих приманок, і на третьому – інтегральна обробка всією системою. Така архітектура забезпечує гнучке реагування на шкідливі дії за рахунок варіативності поведінкових сценаріїв, що дозволяє реалізовувати ефективні методи обману зловмисників і підвищує загальний рівень протидії ЗПЗ та КА.

Напрямами подальших досліджень є деталізація архітектури приманок різного призначення та особливо тих, які можуть виконувати функції інтелектуальних агентів для забезпечення комунікації між ними при виконанні завдань системи.

Література

1. Kashtalian, A., Lysenko, S., Savenko, O., Nicheporuk, A., Sochor, T., & Avsiyevych, V. (2024). Multi-computer malware detection systems with metamorphic functionality. Radioelectronic and Computer Systems, 2024(1), 152-175. doi:https://doi.org/10.32620/reks.2024.1.13
2. Lysenko S, Bobrovnikova K, Kharchenko V, Savenko O. IoT Multi-Vector Cyberattack Detection Based on Machine Learning Algorithms: Traffic Features Analysis, Experiments, and Efficiency. *Algorithms*. 2022; 15(7):239. https://doi.org/10.3390/a15070239
3. Kashtalian, A., Lysenko, S., Kysil, T., Sachenko, A., Savenko, O., & Savenko, B. (2025). Method and Rules for Determining the Next Centralization Option in Multicomputer System Architecture. *International Journal of Computing*, *24*(1), 35-51. https://doi.org/10.47839/ijc.24.1.3875
4. Han, X., Kheir, N., Balzarotti, D. (2018). Обманні Techniques in Computer Security. ACM Computing Surveys (CSUR), 51, 1 - 36.
5. Zobal, L., Kolář, D., R. Fujdiak. (2019). Current State of Honeypots and Обманні Strategies in Cybersecurity," 2019 11th International Congress on Ultra-Modern Telecommunications and Control Systems and Workshops (ICUMT), Dublin, Ireland, 1-9. doi: 10.1109/ICUMT48472.2019.8970921.
6. Zhang, L., Thing, V. L. L. (2021) Three Decades of Обманні Techniques in Active Cyber Defense -- Retrospect and Outlook. https://doi.org/10.48550/arXiv.2104.03594.
7. Oluoha, O., Yange, T., Okereke, G., Bakpo, F. (2021). Cutting Edge Trends in Обманні Based Intrusion Detection Systems—A Survey. Journal of Information Security, 12, 250-269. 10.4236/jis.2021.124014.
8. Pawlick, J., Colbert, E., Zhu, Q. (2017). A Game-theoretic Taxonomy and Survey of Defensive Обманні for Cybersecurity and Privacy. ACM Computing Surveys (CSUR), 52, 1 - 28.
9. Fan, W., Du, Z., Fernández, D., Villagrá, V.A. (2017). Enabling an Anatomic View to Investigate Honeypot Systems: A Survey. IEEE Systems Journal, 12, 3906-3919.
10. Ilg, N., Duplys, P., Germek, D., Menth, M. (2023). Survey of contemporary open-source honeypots, frameworks, and tools. Journal of Network and Computer Applications. 220. 103737. 10.1016/j.jnca.2023.103737.
11. Mohammadzadeh, H. (2012). A Survey on Dynamic Honeypots. International Journal of Information and Electronics Engineering. 10.7763/IJIEE.2012.V2.89.
12. Qin, X., Jiang, F., Cen, M., Doss, R. (2022). Hybrid Cyber Defense Strategies Using Honey-X: A Survey. SSRN Electronic Journal. 10.2139/ssrn.4302960.
13. Sengupta, S., Chowdhary, A., Sabur, A., Alshamrani, A., Huang, D., Kambhampati, S. (2020). A Survey of Moving Target Defenses for Network Security. IEEE Communications Surveys & Tutorials, 22, 3, 1909-1941. doi: 10.1109/COMST.2020.2982955.
14. Efendi, M.A., Ibrahim, Z.B., Zawawi, M.N., Rahim, F.A., Pahri, N.A., & Ismail, A. (2019). A Survey on Обманні Techniques for Securing Web Application. 2019 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS), 328-331.
15. Franco J., Aris A., Canberk B., Uluagac A.S. (2021) A Survey of Honeypots and Honeynets for Internet of Things, Industrial Internet of Things, and Cyber-Physical Systems arXiv:2108.02287v1 [cs.CR] 4 Aug 2021.
16. L. Bedratyuk, O. Savenko, *MATCH Commun. Math. Comput. Chem.* 2018, 79, 407–414.
17. Fraunholz, D., Duque Anton, S., Lipps, C., Reti, D., Krohmer, D., Pohl, F., Tammen, M., Schotten, H.. (2018). Demystifying Обманні Technology:A Survey. 10.48550/arXiv.1804.06196.