https://doi.org/10.31891/2219-9365-2023-76-35
УДК 004.75:004.49:00.4.5

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

ПРИНЦИП СИНТЕЗУ МУЛЬТИКОМП'ЮТЕРНИХ СИСТЕМ З КОМБІНОВАНИХ АНТИВІРУСНИХ ПРИМАНОК І ПАСТОК ТА КОНТРОЛЕРУ ПРИЙНЯТТЯ РІШЕНЬ ДЛЯ ВИЯВЛЕННЯ ЗЛОВМИСНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА КОМП'ЮТЕРНИХ АТАК

В роботі наведено результати досліджень щодо deception-систем для виявлення зловмисного програмного забезпечення та комп'ютерних атак. З цією метою пропонується розробити принцип синтезу мультикомп'ютерних систем з комбінованих антивірусних приманок та пасток. Такий клас систем є одним з класів deception-систем. Для розроблення принципу синтезу було здійснено аналіз архітектури deception-систем. Поділ архітектури систем за внутрішньою будовою дав змогу визначити необхідні елементи та компоненти в архітектурі системи, яка міститиме контролер та спеціалізований функціонал, і є основою для розробки концепції та методологічних основ синтезу таких систем. На відміну від відомих принципів синтезу мультикомп'ютерних систем з комбінованими приманками і пастками та контролером прийняття рішень для виявлення та протидії зловмисному програмному забезпеченню та комп'ютерним атакам, розроблений принцип синтезу таких систем містить дві визначальні вимоги щодо архітектури систем. Контролер прийнятих рішень відокремлено від центру системи, що дає змогу формувати його архітектуру відокремлено від архітектури центру системи і, як наслідок, приймати рішення щодо напрацьованих в центрі системи рішень незалежно від нього. Це обумовлено специфікою системи та надає переваги системі безпосередньо перед зловмисниками чи їх засобами, бо формує різні остаточні відповіді системи за однакових початкових умов в різні проміжки часу, що заплутує зловмисників. Наявність спеціалізованого функціоналу, який впливатиме на внутрішні події в системі та зміну її архітектури, тобто взаємодія в системі підсистем, що забезпечують її безпосереднє функціонування та спеціалізований функціонал для виявлення та протидії ЗПЗ і КА, дає змогу покращити стійкість системи та оперативність в прийнятті рішень.

Ключові слова: deception-системи, принцип, контролер, зловмисне програмне забезпечення, комп'ютерні атаки, приманки, пастки.

KASHTALIAN Antonina
Khmelnytskyi National University

PRINCIPLE OF SYNTHESIS OF MULTI-COMPUTER SYSTEMS FROM COMBINED ANTI-VIRUS BAITS AND TRAPS AND A DECISION-MAKING CONTROLLER FOR THE DETECTION OF MALICE SOFTWARE AND COMPUTER ATTACKS

The work presents the results of research on deception systems for detecting malicious software and computer attacks. For this purpose, it is proposed to develop the principle of synthesis of multi-computer systems from combined antivirus baits and traps. This class of systems is one of the classes of deception systems. To develop the principle of synthesis, an analysis of the architecture of deception systems was carried out. The division of system architecture by internal structure made it possible to determine the necessary elements and components in the system architecture, which will contain a controller and specialized functionality, and is the basis for developing the concept and methodological foundations of the synthesis of such systems. In contrast to known principles of synthesis of multi-computer systems with combined decoys and traps and a decision-making controller for detecting and countering malicious software and computer attacks, the developed principle of synthesis of such systems contains two defining requirements for system architecture. The decision controller is separated from the center of the system, which makes it possible to form its architecture separately from the architecture of the system center and, as a result, to make decisions about the solutions developed in the center of the system independently of it. This is due to the specifics of the system and gives advantages to the system directly before the attackers or their means, because it forms different final responses of the system under the same initial conditions at different time intervals, which confuses the attackers. The presence of specialized functionality that will affect internal events in the system and changes in its architecture, i.e., interaction in the system of subsystems that ensure its direct functioning and specialized functionality for detecting and countering ZPZ and KA, makes it possible to improve the stability of the system and efficiency in decision-making.

Key words: deception systems, principle, controller, malicious software, computer attacks, decoys, traps.

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

Користувачам комп'ютерних мереж необхідні системи для виявлення зловмисного програмного забезпечення (ЗПЗ) та комп'ютерних атак (КА), які дадуть змогу, крім забезпечення безпеки на різних етапах можливого проникнення в комп'ютерні системи чи станції, що об'єднані в мережу, для етапу, коли на всіх попередніх етапах такі виявлення не були здійснені, але могли мати місце проникнення в систему. Серед різних за призначенням систем виявлення ЗПЗ та КА є системи, які крім виявлення загроз створюють в комп'ютерних мережах хибні об'єкти для атак, що надає змогу адміністраторам таких мереж можливість

відслідковувати процеси в мережах, які є зловмисними чи аномальними і потребують зупинки. Тому, перспективними для розробки є системи, які орієнтовані на виявлення ЗПЗ та КА, що пройшли певні етапи захисту, на яких використовувались традиційні засоби і системи попередження, виявлення та протидії, призначення яких та можливі варіанти конфігурування при використанні відомі зловмисникам. Серед таких систем особливе місце в класифікації займають системи попередження, виявлення та протидії із певною множиною приманок та пасток для ЗПЗ та КА. Їх використання створює хибні об'єкти атаки для зловмисника та дозволяє зберегти відомості про такі атаки та розповсюдження ЗПЗ в комп'ютерних станціях в мережі. Для покращення ефективності систем виявлення та протидії ЗПЗ та КА за рахунок використання приманок та пасток, необхідним є інтегрування цих засобів в складні системи із залученням всіх комп'ютерних станцій в мережі та організації функціонування їх таким чином, щоб вони могли реагувати на зловмисні та аномальні процеси сумісно та без втручання користувача. Таким чином, необхідним є побудова не однієї приманки та пастки в певній комп'ютерній станції, а мережі приманок та пасток для здійснення комплексного захисту комп'ютерної мережі на етапі коли КА змогли пройти через міжмережне екранування, а ЗПЗ змогло подолати перевірку антивірусними засобами і системами.

Аналіз останніх досліджень і публікацій

Deception-технології застосовують для виявлення зловмисних вторгнень в мережу. Це стратегія насамперед призначена для відволікання зловмисника від робочих сервісів та заманювання в пастку. Іншою важливою перевагою deception-технології є дослідження поведінки зловмисників та характеристик атак. Сьогоднішній ринок продуктів в сфері кібербезпеки пропонує сучасні рішення deception-систем.

CommVault [1] надає широкий набір рішень для захисту даних, їх менеджменту та оптимізації, аналіз ризиків і сканування загроз. Модуль системи побудовані таким чином, що надають можливості раннього попередження та швидкого реагування для нейтралізації атак. Labyrinth Deception Platform [2] створює обманне середовище для імітації реальної мережі, яке містить інтелектуальні хости, що імітують програмне забезпечення, контент, пристрої тощо робочих сервісів різного типу. Ці обманні точки виявляють зловмисну активність всередині мережі та забезпечують комплексний захист та відслідковування активності зловмисників. Rapid7 Deception Technology Solution [3] пропонує систему, яка містить чотири типи пасток, а саме приманки, honey користувачі, honey облікові дані, honey файли. Ці пастки швидко встановлюються та розгортаються, що дозволяє виконувати раннє виявлення зловмисників до того, як вони можуть пошкодити мережу або викрасти дані. Також система проводить постійне дослідження поведінки зловмисників. В системі CounterCraft Cyber Deception Platform [4] використовуються активні приманки, які є гнучкими до налаштувань і можуть бути використані як кінцеві точки і сервери. Система забезпечує швидке розгортання, взаємодію із зловмисниками та інтеграцію з існуючими системами захисту та менеджменту. Система Attivo ThreatDefend Deception and Response Platform [5] також надає можливість реагування, забезпечує взаємодію власних обманних об'єктів із зловмисниками, імітуючи очікувану реакцію. Система може бути розгорнута локально та в хмарному середовищі, і забезпечує захист мережі та дослідження атак та зловмисних дій.

Системи приманок та пасток є ефективними в тому випадку, коли вони застосовують обман таким чином, що зловмисник про нього не здогадується Це потребує застосування різноманітних обманних тактик. В роботі deception систем виділяють наявність двох фаз, а саме приховування та моделювання [6]. Приховування включає маскування, перепакування та засліплення. Моделювання передбачає створення хибних об'єктів, в тому числі імітацію, створення та перехоплення. Приховування та моделювання може застосовуватися до трьох рівнів, а саме наявності цільової інформації, її природи та її цінності.

Маскування передбачає приховування реальних даних та пристроїв таким чином, що вони не можуть бути виявлення, в тому числі маскування під виглядом приманки [7]. Зворотнім методом, що застосовується в deception системах, є імітація, тобто надання обманних об'єктам ознак і властивостей реальних об'єктів мережі [8]. Також одному об'єкту можуть надаватися властивості іншого об'єкта для його перепакування та надання вигляду як іншого об'єкта, який може бути менш привабливий для зловмисника [9]. З тією ж метою використовується засліплення, змішування цільових об'єктів з іншими об'єктами, таким чином ускладнюючи їх виявлення для атак [10].

Системи приманок та пасток можуть мати різну архітектуру на функціонал. Зокрема вони можуть бути спеціалізовані із вузьким функціоналом та багатофункціональні. Багатофункціональні системи містять фунціонал для розгортання різних класів приманок [11], які розроблені для різних типів операційних систем та пристроїв, архітектура таких приманок є динамічною і ресурси основної системи використовуються оптимально [12]. Deception системи може бути гнучкими також в межах певного класу, зокрема IoT пристроїв [13], хмарних сервісів [14], корпоративних мереж [15]. Системи приманок та пасток працюють на боці сервера або клієнта [16]. З боку клієнта використовуються системи приманок високого рівня взаємодії [17]. З боку сервера використовують приманки, які забезпечують розуміння атак на сервер [18].

Системи приманок здебільшого містять самі приманки та сенсори приманок. Сенсори приманок призначені для детектування, обману та перехоплення трафіку, власне приманки призначені для взаємодії та аналізу поведінки для виявлення атак. Сенсори приманок виконують функції виявлення сканування IP адрес

та TCP портів, підтримки виявлених ділянок мережі, підтримки ділянок мережі приманок, підтримки білого списку функцій обману, підтримки обману для пакетів з невідомими доменними іменами тощо [19]. Приманки забезпечують підтримку HTTP, SSH, SMB, RDP протоколів для глибокої взаємодії із зловмисниками, аналізу їх поведінки, ідентифікації атак, відправки логів взаємодії та сканування логів, отриманих від сенсорів приманок, завантаження файлів, імітації веб-сторінок тощо.

Класифікація deception-систем подана в табл. 1.

Таблиця 1

Класифікація deception-систем

Ознака	Типи систем
Функціонал	Вузькоспеціалізовані, багатофункціональні
Можливість модифікації архітектури	Статичні, динамічні (гнучкі)
Відкритість коду	Комерційні, відкриті
Сфера застосування	Корпоративні мережі, IoT, хмарні, автоматизовані системи керування
Функціонування	На боці сервера, на боці клієнта
Керування	Централізована, децентралізована

В статтях [20-23] наведено методи для виявлення ЗПЗ та КА, які можуть бути імплементовані в deception-системи. Таких методів відомо достатньо багато, але їх реалізація в системах, які б враховували особливості в своїй архітектурі, що поєднувала б виявлення згідно методу і реакцію системи на факт ідентифікації подано недостатньо.

Формулювання цілей статті

Метою роботи є розроблення принципу синтезу мультикомп'ютерних систем комбінованих антивірусних приманок та пасток в корпоративних мережах.

Виклад основного матеріалу

Для покращення ефективності систем виявлення та протидії ЗПЗ та КА за рахунок використання приманок та пасток, необхідним є інтегрування цих засобів в складні системи із залученням всіх комп'ютерних станцій в мережі та організації функціонування їх таким чином, щоб вони могли реагувати на зловмисні та аномальні процеси сумісно та без втручання користувача. Таким чином, необхідним є побудова не однієї приманки та пастки в певній комп'ютерній станції, а мережі приманок та пасток для здійснення комплексного захисту комп'ютерної мережі на етапі коли КА змогли пройти через міжмережне екранування, а ЗПЗ змогло подолати перевірку антивірусними засобами і системами. Така система з приманками та пастками включатиме приманки, які здійснюють моніторинг зловмисного трафіку, тому вона може забезпечити максимально швидке його виявлення, а також виявлення патернів нових атак. Пастки при поєднанні їх в мережі можуть імітувати тіньову комп'ютерну мережу. Така система з приманок і пасток може бути комбінованою з них системою і для досягнення ефективного результату повинна включати тіньові приманки та пастки, які дозволять встановити та відслідкувати поведінку зловмисника при атаці, а також виявити ЗПЗ та КА з більшою вірогідністю. Важливим завданням, яке має бути вирішене при використанні таких систем полягає не тільки у застосуванні приманок та пасток, але й в управлінні їх використанням. Ефективність таких засобів суттєво залежить від організаційної складової частини системи. Використовуючи такі засоби в реальних системах, покращення ефективності може бути досягнуто за рахунок заміни оператора чи користувача на відповідну підсистему, яка зможе забезпечити ефективну організацію. Побудова такої системи можлива з використанням мультиагентних систем та компонентів штучного інтелекту.

Мультиагентна система приманок і пасток може містити множину приманок та пасток різного типу та призначення. Крім того, самі приманки та пастки можуть бути побудовані з використанням компонентів штучного інтелекту. Приманки та пастки системи, які є інтелектуальними, мають ознаки інтелектуального агенту, володіють автономною та гнучкою поведінкою, що передбачає наявність в них таких характеристик:

1) реактивність – інтелектуальна приманка та пастка здатна сприймати середовище, в якому вона працює, та своєчасно реагувати на зміни, які в ньому відбуваються, відповідно до цілей функціонування;

2) проактивність – інтелектуальна приманка та пастка здатна проявляти цілеспрямовану поведінку, що передбачає прояв ініціативи, відповідно до цілей функціонування;

3) соціальні можливості – інтелектуальна приманка та пастка здатна взаємодіяти з іншими приманками (та іншими пристроями) та пастками системи відповідно до цілей функціонування.

Антивірусні приманки та пастки як окремі частини системи можуть окремо приманками чи пастками, але можуть бути скомбіновані разом як окремі частини системи. Взаємодія їх функціоналів між собою може бути здійснена за потреби. Також, їх інтелектуалізація може стосуватись окремо приманок і окремо пасток, коли вони поєднані, але може і бути віднесеною до обох з них одночасно.

Використання лише програмної системи одночасно в якості і приманок та системи, в якій будуть прийматись рішення щодо наступного опрацювання отриманих подій в мережі приманок та пасток і окремих приманках та пастках, є недостатнім. Це пов'язано з особливостями проведення КА та поведінкою

ЗПЗ при поширенні і виконанні деструктивних дій. Тобто, вплив ЗПЗ та КА відбувається програмними засобами і, тому, забезпечення протидії винятково програмними засобами не завжди забезпечує бажаний результат, що підтверджується і розробниками систем попередження і виявлення вторгнень та антивірусних засобів. Крім того, організація ефективної взаємодії між комп'ютерними станціями в корпоративних мережах для підтримки мережних застосунків суттєво залежить від часу передачі повідомлень і їх обробки. Враховуючи такі особливості при побудові приманок, пасток та мереж приманок і пасток необхідно синтезувати систему, в якій до процесу виявлення ЗПЗ та КА були б залучені, також, комп'ютерні станції в мережі. І така система могла б в процесі обробки отриманих даних з приманок та пасток приймати рішення про свої наступні кроки, зокрема і в частині зміни конфігурування та використання комп'ютерних станцій в мережі. Тому, синтезуємо мультикомп'ютерну систему комбінованих антивірусних приманок та пасток в корпоративних комп'ютерних мережах для виявлення ЗПЗ та КА включивши в неї такі складові: мультикомп'ютерну систему; мультиагентну систему; приманки та пастки для виявлення ЗПЗ та КА. А також, такі особливості і характерні властивості: адаптивність; гнучкість; самоорганізація; прийняття рішень; контролер прийнятих рішень; колективна робота агентів. Такі вимоги до архітектури мультикомп'ютерної системи комбінованих антивірусних приманок та пасток в корпоративних мережах дадуть змогу покращити ефективність її функціонування, бо не потребуватимуть втручання користувача при прийнятті рішень в різних поточних станах, та забезпечать спроможності користувачів корпоративних мереж до виявлення та протидії ЗПЗ та КА, покращивши ефективність виявлення та протидії.

Для синтезу систем з такими характеристиками та функційними можливостями потрібно розробити принцип їх синтезу, щоб вони містили комбіновані приманки і пастки та контролер прийняття рішень.

Такий принцип повинен визначати загальні вимоги до побудови елементів теорії створення мультикомп'ютерних систем з комбінованими приманками і пастками та контролером прийняття рішень для виявлення та протидії ЗПЗ і КА. При характеристиці таких систем принцип буде відображати ті суттєві характеристики, які відповідають за правильне функціонування системи. Саме без формалізації та подання правильного функціонування системи, вона не буде виконувати свого призначення. Крім того, принцип синтезу таких систем дасть змогу сформувати клас таких систем та буде розвивати елементи теорії мультикомп'ютерних систем в частині саме систем, в яких здійснено поєднання з контролером прийняття рішень спеціалізованого функціоналу для виявлення зловмисного програмного забезпечення з використанням комбінованих приманок і пасток. Такий принцип в контексті розвитку елементів теорії мультикомп'ютерних систем є систематичним принципом, бо відноситься до задання механізмів функціонування систем. При цьому в ньому потрібно задати такі особливості і характерні властивості систем, щоб відображалась найменша кількість факторів, які визначатимуть, як функціонуватиме система.

Принцип синтезу мультикомп'ютерних систем з комбінованими приманками і пастками та контролером прийняття рішень для виявлення та протидії ЗПЗ і КА задамо з врахуванням деталізації контролера прийняття рішень системи та спеціалізованого функціоналу для виявлення зловмисного програмного забезпечення з використанням комбінованих приманок і пасток. Архітектура мультикомп'ютерних систем з врахуванням принципу синтезу таких систем може бути централізованою, децентралізованою або гібридною з різними ступенями централізації. Відповідно, центр прийняття рішень таких мультикомп'ютерних системи може бути в одній або декількох компонентах системи і це, як і архітектура, не впливатиме на сам принцип синтезу систем та його не виконання. Центр може переміщуватись між компонентами в залежності від поточного стану системи. Також, архітектура таких систем може гнучко перебудовуватись за потреб при зміні зовнішнього середовища і впливів на систему, що характеризує специфіку виконуваних нею завдань. Але при цьому такі особливості не впливають на вимогу принципу синтезу таких систем. Особливістю пропонованого принципу синтезу систем є забезпечення контролю за прийнятими рішеннями в центрі прийняття рішень, тобто обов'язкова наявність контролера прийняття рішень. При цьому контролер прийнятих рішень повинен мати можливість впливати на їх імплементацію через затвердження до виконання або відхилення пропонованих наступних кроків системи, а також затвердження до виконання іншого близького або альтернативного рішення. Такі особливості контролера прийняття рішень вимагаються тим, що система призначена для виконання специфічних завдань, які пов'язані з взаємодією компонентів чи елементів системи із зловмисним програмним забезпеченням та комп'ютерними атаками. Відповідно, зловмисники можуть повторювати свої дії багатократно однаково, що буде переводити систему до одного і того ж стану та її відповідні компоненти. В результаті такого тестування системи зловмисник буде мати змогу вивчити її поведінку і за певний час зможе її обійти. Тому, контролер прийнятих рішень системи повинен здійснювати вплив на остаточне прийняття рішень через вибір наступних кроків системи, як реакцію на зміну зовнішнього середовища та стану системи і її компонент. Така зміна у виборі наступних кроків системи призведе до ускладнень для зловмисника в частині вивчення поведінки засобів виявлення протидії ЗПЗ та КА в корпоративних мережах.

Вимога поєднання в таких системах спеціалізованого функціоналу для опрацювання подій в корпоративній мережі, тобто розподілення в просторі, та наявність підсистеми прийняття рішень, в якій будуть напрацьовуватись рішення, причому їх втілення можливе тільки після затвердження контролером,

встановлює фактори для розроблення принципу синтезу мультикомп'ютерних систем з комбінованими приманками і пастками та контролером прийняття рішень для виявлення та протидії ЗПЗ і КА. Зокрема, формалізуємо системи, їх складові частини і їх властивості, які необхідні для виконання вимог принципу синтезу систем.

Позначимо символом $\mathfrak{P}$ принцип синтезу мультикомп'ютерних систем з комбінованими приманками і пастками та контролером прийняття рішень для виявлення та протидії ЗПЗ і КА. Тоді, ним як відображенням з усієї множини мультикомп'ютерних систем $\mathfrak{C}$ буде сформовано підмножину систем $\mathfrak{S}$, для яких буде виконуватись вимога принципу $\mathfrak{P}$. Тобто, задане відображення формулою $\mathfrak{C} \xrightarrow{\mathfrak{P}} \mathfrak{S}$ буде формувати клас систем із заданими принципом $\mathfrak{P}$ вимогами і потрібно деталізувати компоненти таких систем для подальшого їх синтезу. Задамо кожну з визначальних компонент та властивостей, що потребують імплементації в архітектурі таких систем, підмножиною $\mathfrak{V}_i$ $(i = 1,2, \dots, n_{\mathfrak{V}}$, $n_{\mathfrak{V}}$ – кількість підмножин). Наявність можливих варіантів серед $\mathfrak{V}_i$ $(i = 1,2, \dots, n_{\mathfrak{V}}$, $n_{\mathfrak{V}}$ – кількість підмножин) є допустимим. Наприклад, такі системи можуть бути централізованими, децентралізованими або гібридними з певним ступенем централізації, що теж може надати можливості для їх поділу на окремі типи, і, при цьому, вони відповідатимуть вимогам принципу $\mathfrak{P}$.

Розглянемо можливі варіанти компонентів та визначальних властивостей для класу систем $\mathfrak{S}$: $\mathfrak{V}_1$ – тип архітектури системи (централізована, децентралізована, гібридна (змішана, комбінована)); $\mathfrak{V}_2$ – типи та кількість центрів в архітектурі системи (цілісний в одній компоненті, поділений на рівнозначні частини в різних компонентах, поділений ієрархічно в різних компонентах, цілісний ієрархічний в різних компонентах); $\mathfrak{V}_3$ – адаптивність системи при зміні зовнішніх умов (зміна алгоритмів свого функціонування, зміна архітектури системи, зміна алгоритмів функціонування та зміна архітектури системи); $\mathfrak{V}_4$ – характер змін в центрі системи (зміна значень параметрів, зміна в архітектурі центру, зміна значень параметрів і зміна в архітектурі центру); $\mathfrak{V}_5$ – самоорганізація системи (створення організації функціонування складної системи, відтворення організації функціонування складної системи, вдосконалення організації функціонування складної системи), $\mathfrak{V}_6$ – гнучкість системи (швидке переналаштування системи під впливом зовнішніх подій, латентне переналаштування системи, повільне переналаштування системи); $\mathfrak{V}_7$ – самостійність у прийнятті рішень (прийняття рішень всім центром системи, прийняття рішення частиною центру системи); $\mathfrak{V}_8$ – вплив на систему (внутрішні події, зовнішні події, внутрішні і зовнішні події); $\mathfrak{V}_9$ – наявність агентів в системі для прийняття рішень (мультиагентність, один агент, відсутність агентів); $\mathfrak{V}_{10}$ – контроль прийнятих рішень в системі (наявність контролера, відсутність контролера); $\mathfrak{V}_{11}$ – наявність спеціалізованого функціоналу в системі (формування спеціалізованим функціоналом внутрішніх подій в системі за результатами виконання завдань, вплив результатів виконання завдань спеціалізованим функціоналом на зміну в архітектурі системи, формування внутрішніх подій в системі та відсутність зв'язку впливу результатів виконання завдань спеціалізованим функціоналом на зміну архітектури системи, відсутність зв'язку впливу результатів виконання завдань спеціалізованим функціоналом на зміну архітектури системи та формування внутрішніх подій в системі). Кожна з характеристик $\mathfrak{V}_i$ $(i = 1,2, \dots, n_{\mathfrak{V}}$, $n_{\mathfrak{V}}$ – кількість підмножин) є множиною, в якій наявні типові елементи, що відносяться до систем $\mathfrak{C}$. При застосуванні принципу $\mathfrak{P}$ синтезуються системи типу $\mathfrak{S}$. Для здійснення синтезу систем згідно принципу $\mathfrak{P}$, тобто формування множини визначальних характеристик для системи типу $\mathfrak{S}$ в їх архітектурі згідно визначення прямого добутку множин $\mathfrak{V}_i$ $(i = 1,2, \dots, n_{\mathfrak{V}}$, $n_{\mathfrak{V}}$ – кількість підмножин) задамо так:

$$\mathfrak{S} = \left\{ \left(\mathfrak{v}_1, \mathfrak{v}_2, \dots, \mathfrak{v}_{10,1}, \mathfrak{v}_{11} \right) \middle| \left(\mathfrak{v}_1, \mathfrak{v}_2, \dots, \mathfrak{v}_{10,1}, \mathfrak{v}_{11} \right) \in \mathfrak{V}_1 \times \mathfrak{V}_2 \times \dots \times \mathfrak{V}_{10,1} \times \mathfrak{V}_{11} \right\}, \quad (1)$$

де $\mathfrak{V}_i$ $(i = 1,2, \dots, n_{\mathfrak{V}}$, $n_{\mathfrak{V}}$ – кількість підмножин) – підмножини з елементами, що характеризують особливості архітектури систем; $\mathfrak{v}_{10,1}$ – елемент, що визначає наявність контролера в системі; $\mathfrak{v}_{10,1} \in \mathfrak{V}_{10,1}$; множина $\mathfrak{V}_{10,1}$ – одноелементна множина; $\mathfrak{v}_1, \mathfrak{v}_2, \dots, \mathfrak{v}_9, \mathfrak{v}_{11}$ – позначення елементів в множинах $\mathfrak{V}_1, \mathfrak{V}_2, \dots, \mathfrak{V}_9, \mathfrak{V}_{11}$ відповідно.

Граф відображення визначальних характеристик для систем типу $\mathfrak{S}$ в їх архітектурі у вершинах, що відповідають елементам множин $\mathfrak{V}_i$ $(i = 1,2, \dots, n_{\mathfrak{V}}$, $n_{\mathfrak{V}}$ – кількість підмножин), зображено на рис. 1.

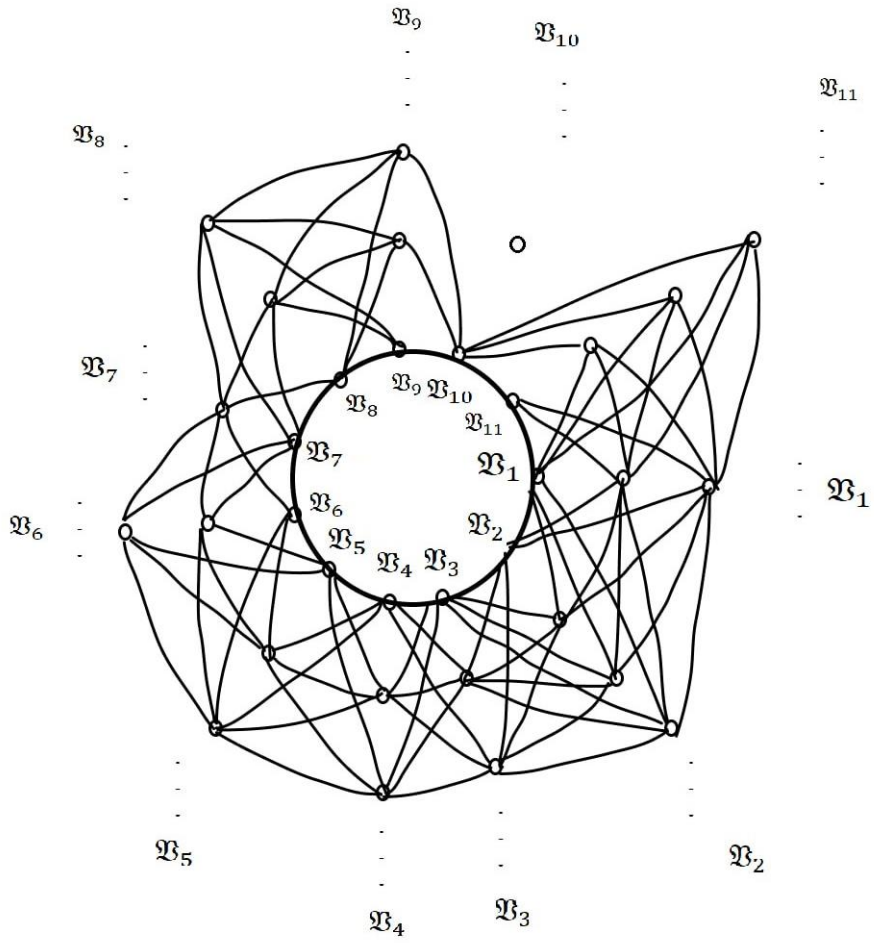

Рис. 1. Граф відображення визначальних характеристик в архітектурі систем типу $\mathfrak{S}$

Будь-який замкнений маршрут в графі відображення визначальних характеристик в архітектурі систем типу $\mathfrak{S}$ з рис. 1 буде завжди включати вершину $\mathfrak{v}_{10,1} \in \mathfrak{V}_{10,1}$ з множини $\mathfrak{V}_{10,1}$. Це означає, що граф відображає архітектуру різних систем згідно принципу синтезу $\mathfrak{P}$. Вершини, які відповідають елементам певної множини $\mathfrak{V}_i$ ($i = 1,2, \dots, n_{\mathfrak{V}}$, $n_{\mathfrak{V}}$ – кількість підмножин) при визначенні замкненого маршруту можуть йому належати, тобто з однієї множини до маршруту можуть включатись декілька елементів, а не тільки один. Це відображає інші варіанти в архітектурі систем типу $\mathfrak{S}$. Наприклад, система може мати не винятково централізовану, або децентралізовану, або змішану архітектури. Але вона у варіанті змішаної щодо централізації архітектури може мати централізовану і децентралізовану теж, наприклад з певними інтервалами часу тип архітектури може змінюватись на змішану, потім на централізовану і далі повертатись до змішаної або переходити до децентралізованої. Також, може бути рівень централізації і його особливість різними. Аналогічно і решта визначальних характеристик в архітектурі систем типу $\mathfrak{S}$ можуть мати такі ж особливості. Тобто, в системах типу $\mathfrak{S}$ може бути декілька елементів з певної множини $\mathfrak{V}_i$ ($i = 1,2, \dots, 9, 11, \dots, n_{\mathfrak{V}}$, $i \neq 10$, $n_{\mathfrak{V}}$ – кількість підмножин). Граф з рис. 1 поза межами наявних ребер і вершин може містити інші вершини і ребра. Але замкнений маршрут так само буде їх охоплювати і, відповідно, включати вершини і ребра. В результаті охоплені маршрутом вершини будуть відображати визначальні характеристики синтезовані в системах типу $\mathfrak{S}$. З множини $\mathfrak{V}_{10}$ в маршрут буде включатись лише одна вершина, що належатиме цій множині. Решта вершин будуть ізольованими і в жоден маршрут не будуть включені.

Таким чином, кількість систем типу $\mathfrak{S}$ згідно принципу $\mathfrak{P}$ є різною, але згідно формули (1) всіх їх поєднує наявність в їх архітектурі контролера. Кількість підмножин $\mathfrak{V}_i$ ($i = 1,2, \dots, n_{\mathfrak{V}}$, $n_{\mathfrak{V}}$ – кількість підмножин) може бути різною, зокрема і менше, ніж $n_{\mathfrak{V}}$, але наявність одноелементної множини $\mathfrak{V}_{10,1}$ та множини $\mathfrak{V}_{11}$ в прямому добутку множин є обов'язковим.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі

Такий поділ архітектури систем за внутрішньою будовою дає змогу визначити необхідні елементи та компоненти в архітектурі системи, яка міститиме контролер та спеціалізований функціонал, і є основою для розробки концепції та методологічних основ синтезу таких систем. На відміну від відомих принципів синтезу мультикомп'ютерних систем з комбінованими приманками і пастками та контролером прийняття рішень для виявлення та протидії ЗПЗ і КА, розроблений принцип синтезу таких систем містить дві визначальні вимоги щодо архітектури систем. Контролер прийнятих рішень відокремлено від центру системи, що дає змогу формувати його архітектуру відокремлено від архітектури центру системи і, як наслідок, приймати рішення щодо напрацьованих в центрі системи рішень незалежно від нього. Це обумовлено специфікою системи та надає переваги системі безпосередньо перед зловмисниками чи їх засобами, бо формує різні остаточні відповіді системи за однакових початкових умов в різні проміжки часу, що заплутує зловмисників. Наявність спеціалізованого функціоналу, який впливатиме на внутрішні події в системі та зміну її архітектури, тобто взаємодія в системі підсистем, що забезпечують її безпосереднє функціонування та спеціалізований функціонал для виявлення та протидії ЗПЗ і КА, дає змогу покращити стійкість системи та оперативність в прийнятті рішень.

Для деталізації архітектури мультикомп'ютерних систем з комбінованими приманками і пастками та контролером прийняття рішень для виявлення та протидії ЗПЗ і КА, яка відповідає запропонованому принципу синтезу таких систем, потрібно розробити концептуальну модель її архітектури.

Література

1. *The Commvault Data Protection Platform*. Available at: https://www.commvault.com/ (accessed 06.08.2023).
2. *Labyrinth Deception Platform. Datasheet*. Available at: https://labyrinth.tech/assets/media/pdf/labyrinth-data-sheet.pdf (accessed 06.08.2023).
3. *Rapid7 Deception Technology Solution/* Available at: https://www.rapid7.com/solutions/deception-technology/ (accessed 06.11.2023).
4. *Counter Craft Security*. Available at: https://www.countercraftsec.com/ (accessed 06.11.2023).
5. *SentinelOne*. Available at: https://www.sentinelone.com/surfaces/identity/ (accessed 06.11.2023).
6. Onyekware U. Oluoha, Terungwa S. Yange, George E. Okereke, Francis S. Bakpo. *Cutting Edge Trends in Deception Based Intrusion Detection Systems—A Survey. Journal of Information Security*. 2021. 12. P. 250-269.
7. Aggarwal P., Du Y., Singh K., Gonzalez C. Decoys in Cybersecurity: An Exploratory Study to Test the Effectiveness of 2-sided Deception. https://arxiv.org/pdf/2108.11037.pdf.
8. Ehab A.-S., Jinpeng W., Kevin W. H., Cliff W. Autonomous Cyber Deception. Reasoning, Adaptive Planning, and Evaluation of HoneyThings. *Springer Nature Switzerland AG (eBook)*. 2019. https://doi.org/10.1007/978-3-030-02110-8.
9. Rowe, N.C. (2019). Honeypot Deception Tactics. In: Al-Shaer, E., Wei, J., Hamlen, K., Wang, C. (eds) Autonomous Cyber Deception. Springer, Cham. https://doi.org/10.1007/978-3-030-02110-8_3.
10. V. E. Urias, W. M. S. Stout, J. Luc-Watson, C. Grim, L. Liebrock and M. Merza, "Technologies to enable cyber deception," 2017 International Carnahan Conference on Security Technology (ICCST), Madrid, Spain, 2017, pp. 1-6.
11. Kumar S., Janet B., Eswari R. Multi Platform Honeypot for Generation of Cyber Threat Intelligence. *2019 IEEE 9th International Conference on Advanced Computing (IACC), Tiruchirappalli, India*. 2019. P. 25-29.
12. Acosta J.C., Basak A., Kiekintveld C., Kamhoua C. Lightweight On-Demand Honeypot Deployment for Cyber Deception. *In: Gladyshev, P., Goel, S., James, J., Markowsky, G., Johnson, D. (eds) Digital Forensics and Cyber Crime. ICDF2C 2021. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering. Springer, Cham.* 2022. Vol. 441.
13. Rabzelj M.; Južnič L.Š.; Volk M.; Kos A.; Kren M.; Sedlar U. Designing and Evaluating a Flexible and Scalable HTTP Honeypot Platform: *Architecture, Implementation, and Applications. Electronics*. 2023. 12. 3480.
14. Aydeger A., Saputro N., Akkaya K. Cloud-based Deception against Network Reconnaissance Attacks using SDN and NFV. *2020 IEEE 45th Conference on Local Computer Networks (LCN, Sydney, NSW. Australia*. 2020. P. 279-285.
15. Anjum I., Zhu M., Polinsky I., Enck W., Reiter M.K., Singh M.P. Role-Based Deception in Enterprise Networks. *In Proceedings of the Eleventh ACM Conference on Data and Application Security and Privacy (CODASPY '21). Association for Computing Machinery, New York, NY, USA*. P. 65–76.
16. Biswas J. Analysis of Client Honeypots. *(IJCSIT) International Journal of Computer Science and Information Technologies.* 2014. Vol. 5 (4). P. 5776-5780
17. Shukla R., Singh M.P. PythonHoneyMonkey: Detecting malicious web URLs on client side honeypot systems. *Proceedings of 3rd International Conference on Reliability, Infocom Technologies and Optimization.* 2014. P. 1-5.

18. Mukti, F.S., & Sukmawan, R. Integration of Low Interaction Honeypot and ELK Stack as Attack Detection Systems on Servers. *Jurnal Penelitian Pos dan Informatika*. 2021.

19. Yamin, M.M., Katt, B., Sattar, K., & Ahmad, M.B. Implementation of Insider Threat Detection System Using Honeypot Based Sensors and Threat Analytics. *Lecture Notes in Networks and Systems*. 2019.

20. Lysenko S., Savenko O., Bobrovnikova K. DDoS Botnet Detection Technique Based on the Use of the Semi-Supervised Fuzzy c-Means Clustering. CEUR-WS 2018, 2104, 688–695.

21. G. Markowsky, O. Savenko, S. Lysenko, A. Nicheporuk, The Technique for Metamorphic Viruses' Detection Based on its Obfuscation Features Analysis, CEUR Workshop Proceedings, Vol. 2104, 2018, pp. 680-687.

22. Bobrovnikova K., Lysenko S., Savenko B., Gaj P., Savenko O. Technique for IoT malware detection based on control flow graph analysis. Radioelectron. Comput. Syst. 2022, 1, 141–153.

23. Savenko B., Lysenko, S., Bobrovnikova K., Savenko O. Markowsky G. Detection DNS Tunneling Botnets. In Proceedings of the 2021 IEEE 11th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, Cracow, Poland, 22–25 September 2021; Volume 1, pp. 64–69.

References

1. *The Commvault Data Protection Platform*. Available at: https://www.commvault.com/ (accessed 06.08.2023).

2. *Labyrinth Deception Platform. Datasheet*. Available at: https://labyrinth.tech/assets/media/pdf/labyrinth-data-sheet.pdf (accessed 06.08.2023).

3. *Rapid7 Deception Technology Solution/* Available at: https://www.rapid7.com/solutions/deception-technology/ (accessed 06.11.2023).

4. *Counter Craft Security*. Available at: https://www.countercraftsec.com/ (accessed 06.11.2023).

5. *SentinelOne*. Available at: https://www.sentinelone.com/surfaces/identity/ (accessed 06.11.2023).

6. Onyekware U. Oluoha, Terungwa S. Yange, George E. Okereke, Francis S. Bakpo. *Cutting Edge Trends in Deception Based Intrusion Detection Systems—A Survey. Journal of Information Security*. 2021. 12. P. 250-269.

7. Aggarwal P., Du Y., Singh K., Gonzalez C. Decoys in Cybersecurity: An Exploratory Study to Test the Effectiveness of 2-sided Deception. https://arxiv.org/pdf/2108.11037.pdf.

8. Ehab A.-S., Jinpeng W., Kevin W. H., Cliff W. Autonomous Cyber Deception. Reasoning, Adaptive Planning, and Evaluation of HoneyThings. *Springer Nature Switzerland AG (eBook)*. 2019. https://doi.org/10.1007/978-3-030-02110-8.

9. Rowe, N.C. (2019). Honeypot Deception Tactics. In: Al-Shaer, E., Wei, J., Hamlen, K., Wang, C. (eds) Autonomous Cyber Deception. Springer, Cham. https://doi.org/10.1007/978-3-030-02110-8_3.

10. V. E. Urias, W. M. S. Stout, J. Luc-Watson, C. Grim, L. Liebrock and M. Merza, "Technologies to enable cyber deception," 2017 International Carnahan Conference on Security Technology (ICCST), Madrid, Spain, 2017, pp. 1-6.

11. Kumar S., Janet B., Eswari R. Multi Platform Honeypot for Generation of Cyber Threat Intelligence. *2019 IEEE 9th International Conference on Advanced Computing (IACC), Tiruchirappalli, India*. 2019. P. 25-29.

12. Acosta J.C., Basak A., Kiekintveld C., Kamhoua C. Lightweight On-Demand Honeypot Deployment for Cyber Deception. *In: Gladyshev, P., Goel, S., James, J., Markowsky, G., Johnson, D. (eds) Digital Forensics and Cyber Crime. ICDF2C 2021. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering. Springer, Cham.* 2022. Vol. 441.

13. Rabzelj M.; Južnič L.Š.; Volk M.; Kos A.; Kren M.; Sedlar U. Designing and Evaluating a Flexible and Scalable HTTP Honeypot Platform: *Architecture, Implementation, and Applications. Electronics*. 2023. 12. 3480.

14. Aydeger A., Saputro N., Akkaya K. Cloud-based Deception against Network Reconnaissance Attacks using SDN and NFV. *2020 IEEE 45th Conference on Local Computer Networks (LCN, Sydney, NSW. Australia*. 2020. P. 279-285.

15. Anjum I., Zhu M., Polinsky I., Enck W., Reiter M.K., Singh M.P. Role-Based Deception in Enterprise Networks. *In Proceedings of the Eleventh ACM Conference on Data and Application Security and Privacy (CODASPY '21). Association for Computing Machinery, New York, NY, USA.* P. 65–76.

16. Biswas J. Analysis of Client Honeypots. *(IJCSIT) International Journal of Computer Science and Information Technologies.* 2014. Vol. 5 (4). P. 5776-5780

17. Shukla R., Singh M.P. PythonHoneyMonkey: Detecting malicious web URLs on client side honeypot systems. *Proceedings of 3rd International Conference on Reliability, Infocom Technologies and Optimization.* 2014. P. 1-5.

18. Mukti, F.S., & Sukmawan, R. Integration of Low Interaction Honeypot and ELK Stack as Attack Detection Systems on Servers. *Jurnal Penelitian Pos dan Informatika*. 2021.

19. Yamin, M.M., Katt, B., Sattar, K., & Ahmad, M.B. Implementation of Insider Threat Detection System Using Honeypot Based Sensors and Threat Analytics. *Lecture Notes in Networks and Systems*. 2019.

20. Lysenko S., Savenko O., Bobrovnikova K. DDoS Botnet Detection Technique Based on the Use of the Semi-Supervised Fuzzy c-Means Clustering. CEUR-WS 2018, 2104, 688–695.

21. G. Markowsky, O. Savenko, S. Lysenko, A. Nicheporuk, The Technique for Metamorphic Viruses' Detection Based on its Obfuscation Features Analysis, CEUR Workshop Proceedings, Vol. 2104, 2018, pp. 680-687.

22. Bobrovnikova K., Lysenko S., Savenko B., Gaj P., Savenko O. Technique for IoT malware detection based on control flow graph analysis. Radioelectron. Comput. Syst. 2022, 1, 141–153.

23. Savenko B., Lysenko, S., Bobrovnikova K., Savenko O. Markowsky G. Detection DNS Tunneling Botnets. In Proceedings of the 2021 IEEE 11th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, Cracow, Poland, 22–25 September 2021; Volume 1, pp. 64–69.