УДК 004.75:004.49
DOI https://doi.org/10.32782/IT/2024-4-14

Антоніна КАШТАЛЬЯН
кандидат технічних наук, доцент кафедри фізики та електротехніки, докторанка, Хмельницький національний університет, 11, вул. Інститутська, м. Хмельницький, Україна, 29016
***ORCID:** 0000-0002-4925-9713*
***Scopus Author ID:** 57218242499*

Бібліографічний опис статті: Каштальян, А. (2024). Характерні властивості централізації в архітектурі мультикомп'ютерних систем антивірусних комбінованих приманок і пасток. *Information Technology: Computer Science, Software Engineering and Cyber Security,* 4, 114–124, doi: https://doi.org/10.32782/IT/2024-4-14

ХАРАКТЕРНІ ВЛАСТИВОСТІ ЦЕНТРАЛІЗАЦІЇ В АРХІТЕКТУРІ МУЛЬТИКОМП'ЮТЕРНИХ СИСТЕМ АНТИВІРУСНИХ КОМБІНОВАНИХ ПРИМАНОК І ПАСТОК

В роботі здійснено аналіз систем попередження, виявлення і протидії зловмисному програмному забезпеченню та комп'ютерним атакам, зокрема обманних систем та систем з приманками і пастками. При розробленні таких систем в їх архітектуру часто закладають механізми, які забезпечують їх адаптивність, тобто пристосування до оточуючого операційного середовища та внутрішніх і зовнішніх впливів. Під цими механізмами першочергово розглядають механізми, які забезпечують перебудову архітектури систем в процесі їх функціонування з метою відповіді на зловмисні загрози. Одним з основних елементів при перебудові архітектури систем без втручання користувача є центри систем. Деталізації механізмів перебудови саме центрів систем приділено недостатньо уваги, зокрема про це не заявляють і розробники комерційних систем.

В роботі визначено характерні властивості централізації в мультикомп'ютерних системах та здійснено деталізацію характерних властивостей, їх поєднання та подання. Така деталізація характерних властивостей є основою для встановлення зв'язків між ними, синтезу систем з такими центрами, а також оцінювання ефективності варіантів централізації. Згідно розробленого подання варіантів централізації в архітектурі систем було оцінено потенційну кількість варіантів централізації, до яких може перейти система при виборі наступного варіанту централізації.

***Метою статті** забезпечення деталізації характерних властивостей централізації для визначення наступного варіанту центру в архітектурі мультикомп'ютерних систем попередження, виявлення та протидії зловмисному програмному забезпеченню і комп'ютерним атакам таким чином, щоб системи самостійно приховували свій центр, а також щоб забезпечувались ефективна взаємодія між їх вузлами і швидке прийняття рішень та підтримувалась цілісність системи в процесі експлуатації.*

***Методологія** полягає у застосуванні наукових методів: системного аналізу синтезу, порівняння. В роботі представлений аналіз характерних властивостей централізації для визначення наступного варіанту центру в архітектурі мультикомп'ютерних систем попередження, виявлення та протидії зловмисному програмному забезпеченню і комп'ютерним атакам. Згідно аналізу подано формальне представлення характерних властивостей згідно яких будуть синтезовані варіанти централізації в архітектурі систем.*

***Наукова новизна** полягає у розроблених моделях характерних властивостей централізації для використання їх в методі визначення наступного варіанту центру в архітектурі мультикомп'ютерних систем попередження, виявлення та протидії зловмисному програмному забезпеченню та комп'ютерним атакам, які на відмінну від відомих моделей згруповано за характерними властивостями і надають змогу формувати з них наступний варіант централізації без залучення користувача та уникнення повного або значного часткового перебору варіантів.*

***Висновки**. Розроблено характерні властивості централізації в архітектурі мультикомп'ютерних систем приманок та пасток для виявлення та протидії ЗПЗ та КА. Характерні властивості згруповано в множини характерних властивостей. Згідно такого визначення отримано показники для використання їх при визначенні наступного варіанту централізації в архітектурі мультикомп'ютерних систем, яке вони повинні здійснювати самостійно без залучення адміністратора. Аналіз запропонованого рішення підтвердив перспективність напряму досліджень. В роботі здійснено постановку експерименту для розробленої системи згідно поданої централізації. Результати проведеного експерименту підтверджують перспективність досліджень в напрямі перебудови центру систем.*

***Ключові слова:** централізація; захист інформації; обманні системи; мультикомп'ютерні системи; зловмисне програмне забезпечення; комп'ютерні атаки.*

Antonina KASHTALIAN
PhD, Associate Professor at the Department of Physics and Electrical Engineering, Doctoral Student, Khmelnytskyi National University, 11, Instytuts'ka Str., Khmelnytskyi, Ukraine, 29016, yantonina@ukr.net
ORCID: *0000-0002-4925-9713*
Scopus Author ID: *57218242499*

To cite this article: Kashtalian, A. (2024). Kharakterni vlastyvosti tsentralizatsii v arkhitekturi multykompiuternykh system antyvirusnykh kombinovanykh prymanok i pastok [Characteristic properties of centralization in the architecture of multi-computer systems of antiviral combined baits and traps]. *Information Technology: Computer Science, Software Engineering and Cyber Security*, 4, 114–124, doi: https://doi.org/10.32782/IT/2024-4-14

CHARACTERISTIC PROPERTIES OF CENTRALIZATION IN THE ARCHITECTURE OF MULTI -COMPUTER SYSTEMS OF ANTIVIRAL COMBINED BAITS AND TRAPS

The work analyzes the prevention, detection and counteraction systems of malicious software and computer attacks, including fraudulent systems and systems with baits and traps. When developing such systems, mechanisms that provide their adaptability, that is, adaptation to the surrounding operating environment and internal and external influences, are often laid in their architecture. These mechanisms first consider mechanisms that provide restructuring of systems architecture in the process of their functioning in order to respond to malicious threats. One of the main elements in the restructuring of the architecture of systems without user intervention is the centers of systems. The detail of the mechanisms of restructuring of the centers of systems is not given enough attention, in particular, the developers of commercial systems do not declare.

The work identifies the characteristic properties of centralization in multicomputer systems and detail the characteristic properties, their combination and presentation. Such detail of characteristic properties is the basis for establishing relationships between them, the synthesis of systems with such centers, as well as evaluating the effectiveness of centralization options. According to the developed submission of centralization options in the architecture of systems, the potential number of centralization options, which can be transferred when choosing the next centralization option, was evaluated.

The purpose of the article *is to detail the characteristic properties of centralization to identify the next version of the center in the architecture of systems of prevention, detection and counteraction to malicious software and computer attacks so that the systems are concealed their center independently, as well as to ensure effective interaction between their nodes And the rapid decision -making and the integrity of the system was maintained during operation.*

The methodology *is to apply scientific methods: systematic analysis of synthesis, comparison. The work presents an analysis of the characteristic properties of centralization to determine the next version of the center in the architecture of the Milty -Computer Systems Preventing, Detection and Combating Mallen software and computer attacks. According to the analysis, a formal representation of the characteristic properties according to which will synthesize the variants of centralization in the architecture of systems.*

Scientific novelty *lies in the designed models of characteristic properties of centralization to use them in the method of determining the next variant of the center in the architecture of multi-computer systems of prevention, detection and counteraction Able to form the following centralization option without involving the user and avoiding a complete or significant partial interview of options.*

Conclusions. *The characteristic properties of centralization in the architecture of multi-computer baits and traps to detect and counteract the RFS and Ka. The characteristic properties are grouped into the set of characteristic properties. According to this definition, the indicators were obtained to use them in determining the following centralization in the multi -computer architecture, which they must be carried out independently without involving the administrator. The analysis of the proposed solution confirmed the prospect of the research. The experiment was staged for the developed system according to the submitted centralization. The results of the experiment confirm the prospect of research in the direction of restructuring of the center of systems.*

Key words: *centralization, protection of information, fraudulent systems, multicomputer systems, malicious software; Computer attacks.*

Вступ. При розробленні мультикомп'ютерних систем (A. Kashtalian et al., 2023) для виявлення та протидії зловмисному програмному забезпеченню (ЗПЗ) і комп'ютерним атакам (КА), зокрема і систем з приманками та пастками, а також обманних систем, потрібно забезпечити такі системи механізмами перебудови (B. Savenko et al., 2023, O. Savenko et al., 2020) їх архітектури таким чином, щоб ускладнити зловмисникам процес виявлення центру систем. При здійсненні синтезу мультикомп'ютерних систем антивірусних комбінованих приманок і пасток згідно різних характеристичних властивостей та принципів (A. Kashtalian et

al., 2023, A. Kashtalian et al., 2024) потрібно враховувати особливості централізації, тобто архітектуру та функційні можливості центрів таких систем. Ефективність функціонування муьтикомп'ютерних систем антивірусних комбінованих приманок і пасток залежить від організації та особливостей функціонування центру в архітектурі таких систем, оскільки це впливає на комунікацію між вузлами. Вузли системи розподілені, тоді час на прийняття рішень та надсилання відповідних повідомлень є важливими характеристиками. Крім того, приховування центру мультикомп'ютерних систем антивірусних комбінованих приманок і пасток для уникнення його виявлення зловмисниками, які діють ззовні або з середини периметру корпоративної мережі, є важливою характеристикою та спроможністю систем класу $\mathfrak{S}$ (A. Kashtalian et al., 2023, A. Kashtalian et al., 2024). Тому, потрібно на архітектурному рівні при синтезі систем класу $\mathfrak{S}$ (A. Kashtalian, 2023) забезпечити їх централізацію таким чином, щоб системи самостійно приховували свій центр, а також щоб забезпечувались ефективна взаємодія між їх вузлами і швидке прийняття рішень та підтримувалась цілісність системи в процесі експлуатації.

Аналіз останніх досліджень і публікацій. Обманні системи із приманками є сучасними засобами запобігання та виявлення зловмисних дій (S. Suratkar et al., 2022), які можуть виконувати глибокий аналіз даних атак (S. Lysenko et al., 2022). Існуючі системи приманок піддаються постійним спробам детектування зловмисниками та виявлення їх вразливості. Приманки та їх системи, які мають постійні характеристики, не можуть протистояти виявленню. Ще одним недоліком статичних схем розгортання приманок є неможливість адаптації мережі після розгортання. Подолати ці недоліки дозволяють мережі приманок, які мають динамічні властивості (S. Leyi et al., 2019). В роботі (W. Fan et al., 2015) запропоновану гнучку систему керування віртуальною мережею приманок. Також при використанні систем приманок має досягатися компроміс щодо функціональних можливостей та супутніх витрат, що неможливо забезпечити маючи незмінну конфігурацію приманок. В роботі (J.C. Acosta et al., 2021) запропонований підхід, що дозволяє приманкам динамічно вводити ресурси відповідно до виявлених дій зловмисника. Приманки з динамічними характеристиками забезпечують кращий обман зловмисників, в тому числі завдяки динамічному розташуванню. В роботі (Y.Li et al., 2019) запропонована розподілена мережа з динамічно розташованими приманками, яка виконує періодичну зміну сервісів, заплутуючи зловмисника та розпізнаючи його дії. Для забезпечення динамічних властивостей обманних систем використовують можливості програмно керованих мережа, зокрема в роботі (W. Han et al., 2016) запропоновану мережу приманок HoneyMix, що дозволяє уникати виявлення зловмисником, в роботі (M. Baykara et al., 2019) рознлянуто централізований підхід на основі приманок із програмно-визначеним перемиканням для зменшення хибно позитивних спрацювань.

Для оптимізації роботи обманних систем використовують комбіновані системи приманок різного рівня взаємодії Комбіновані системи приманок динамічно конфігуруються, збалансовують використання двох рівнів складності приманок, приманок з високим рівнем взаємодії для більш досвідчених зловмисників, та низького рівня взаємодії для менш досвідчених (A. Anwar et al., 2022) та забезпечують передачу трафіку між різними рівнями (S. Schindler et al., 2015). В роботі (M. Wegerer et al., 2016) пропонується архітектура на основі програмно керованої мережі, застосованої до комбінованої приманки для моделювання топології мережі та пере направлення трафіку атаки, використовується розширюваність та керованість контролера програмно керованої мережі для імітації великої та реалістичної мережі для залучення зловмисників та пере направлення атак на приманку з високим рівнем взаємодії.

Важливою тактикою для обманних систем є їх невизначеність для зловмисників, що збільшує витрати зловмисників на атаки і зменшує їх успішність (S. Achleitner et al., 2016). В обманних системах має забезпечуватися розгортання обманних об'єктів, яке дозволяє інтегрувати обманні вузли в робочі, що дозволяє виявляти нові атаки з мінімальними втратами для засобу захисту (M. Zaman et al., 2023). Невизначеність системи досягається динамічними змінами, в роботі (C.J. Chiang et al., 2016) пропонується обманна система, що динамічно змінює вигляд мережі хостів в реальному часі. В роботі (A.S. Ehab, 2016) запропоновано методи кібермутації, які дозволяють змінювати динамічно конфігурацію системи, що забезпечує відволікання зловмисників та збільшення їх витрат на проведення атак.

Таким чином, проведений аналіз досліджень підтверджує необхідність розроблення нових підходів для забезпечення систем механізмами перебудови їх центру в процесі функціонування системи без втручання адміністратора. Це дасть змогу створювати системи, які буде

складно зрозуміти зловмисникам в процесі їх функціонування в частині знаходження та будови їх центру.

Методологія дослідження. Серед визначальних властивостей для систем класу $\mathfrak{S}$ було виділено в [4] таку властивість як $\mathfrak{V}_2$, яка характеризує типи та кількість центрів в архітектурі системи. В загальному випадку ця властивість щодо центру системи може буде реалізована так: цілісний центр в одній компоненті; центр поділений на рівнозначні частини в різних компонентах; центр поділений ієрархічно і міститься в різних компонентах; центр є цілісним, ієрархічним та міститься в різних компонентах. З використанням такої стратегії щодо синтезу центру в архітектурі систем класу $\mathfrak{S}$ можуть бути різні варіанти та варіації, які будуть основою при функціонуванні центру системи в поточний момент часу. Наприклад, центр систем класу $\mathfrak{S}$ в поточний момент часу може бути в одному вузлі, а далі протягом певного інтервалу часу вже бути розподілений в декількох компонентах системи у різних вузлах корпоративної мережі. Також, зловмисник з середини мережі може відімкнути обладнання і корпоративна розділиться на два або більше сегментів. Таку модель зловмисної поведінки потрібно враховувати при організації функціонування центру системи.

Для реалізації в архітектурі систем класу $\mathfrak{S}$ таких властивостей центру розподілимо на підмножини всі можливі варіанти та їх варіації, а також здійснимо дослідження центру на предмет відповідності його очікуваним результатам з ефективності його приховування, прийняття рішень, організації комунікації між компонентами системи в різних вузлах корпоративної мережі та забезпечення підтримки цілісності системи, враховуючи гнучкі переходи центру системи до різних варіантів.

Виділимо спочатку потенційні варіанти організації центру системи, а потім їх варіації. У системах з більше ніж однією компонентою, які розміщені у різних вузлах корпоративної мережі, можна синтезувати в архітектурі системи центр чотирма різними варіантами: централізована архітектура; частково централізована архітектура; частково децентралізована архітектура; децентралізована архітектура. Позначимо ці варіанти в множині варіантів централізації так:

$$M_{\mathfrak{V}_2,centr,v_1}=\left\{m_{\mathfrak{V}_2,centr,v_1,1},m_{\mathfrak{V}_2,centr,v_1.2},m_{\mathfrak{V}_2,centr,v_1,3},m_{\mathfrak{V}_2,centr,v_1,4}\right\}, \quad (1)$$

де елемент $m_{\mathfrak{V}_2,centr,v_1,1}$ відображає централізовану архітектуру систем класу $\mathfrak{S}$; елемент $m_{\mathfrak{V}_2,centr,v_1.2}$ – частково централізовану архітектуру системи; $m_{\mathfrak{V}_2,centr,v_1,3}$ – частково децентралізовану архітектуру системи; $m_{\mathfrak{V}_2,centr,v_1,4}$ – децентралізовану архітектуру системи.

Наступним параметром, який потребує врахування, буде варіант з розподіленням центру системи між її компонентами в різних вузлах корпоративної мережі. Задамо його множиною $M_{\mathfrak{V}_2,centr,v_2}$ так:

$$M_{\mathfrak{V}_2,centr,v_2}=\left\{m_{\mathfrak{V}_2,centr,v_2,1},m_{\mathfrak{V}_2,centr,v_2.2}\right\}, \quad (2)$$

де елемент $m_{\mathfrak{V}_2,centr,v_2,1}$ відображає поділ центру системи між компонентами в різних вузлах для систем класу $\mathfrak{S}$; елемент $m_{\mathfrak{V}_2,centr,v_2.2}$ відображає неподільність центру системи між компонентами в різних вузлах для систем класу $\mathfrak{S}$, тобто перебування його в одній компоненті.

Для варіанту, який задано множиною за формулою (2), потрібно врахувати можливість тимчасового розділення системи на дві або декілька частин. Причини розділення можуть бути різними. Але їх потрібно врахувати. Бо при наявності центру в одній із частин після розділення системи, решта частин системи повинні підтримувати своє функціонування. Інакше після повернення до повноцінного функціонування системи в цілісному поданні, довіра до частин, які функціонували без центру системи буде знижена і потребуватимуть повного дослідження її компоненти та вузли корпоративної мережі. Також, можуть бути і інші причини, але всі вони за відсутності центру системи в її частинах, які відокремились, знижують довіру до результатів її роботи. Тому, параметром, який потребує врахування, буде варіант з розподіленням центру системи між її компонентами в різних вузлах корпоративної мережі при розподіленні її на незв'язні частини. Навіть для централізованої архітектури систем класу $\mathfrak{S}$ при її розділенні на незв'язні частини вважатимемо, що центр системи буде в кожній з таких частин. Задамо такий варіант з наявністю центру системи в незв'язних частинах систем класу $\mathfrak{S}$ множиною $M_{\mathfrak{V}_2,centr,v_3}$ так:

$$M_{\mathfrak{V}_2,centr,v_3}=\left\{m_{\mathfrak{V}_2,centr,v_3,1},m_{\mathfrak{V}_2,centr,v_3.2}\right\}, \quad (3)$$

де елемент $m_{\mathfrak{V}_2,centr,v_3,1}$ відображає наявність центру системи в незв'язних частинах систем класу $\mathfrak{S}$ після їх розділення; елемент $m_{\mathfrak{V}_2,centr,v_3.2}$ відображає наявність центру системи лише в одній з незв'язних частин систем класу $\mathfrak{S}$ після їх розділення, тобто в решті частин системи центр відсутній.

У варіантах з розділенням центру системи між компонентами у різних вузлах корпоративної мережі потрібно враховувати задані зв'язки між компонентами центру системи. Вони

впливатимуть на швидкість прийняття рішень, бо будуть залежати від часу витраченого на обмін повідомленнями між собою. Ці зв'язки можуть бути встановлені між всіма компонентами, в яких буде міститись центр системи, а можуть бути задані лише частково, тобто не повністю і, відповідно, не формуватимуть відношення «всі до всіх». Між компонентами, в яких міститься центр системи, може бути організована ієрархічна підпорядкованість. Такі особливості в архітектурі центрів систем класу $\mathfrak{S}$ потрібно врахувати. Тому, задамо множиною $M_{\mathfrak{V}_2,centr,v_4}$ особливості зв'язків між компонентами при його розподілені між компонентами в різних вузлах корпоративної мережі так:

$$M_{\mathfrak{V}_2,centr,v_4}=\left\{m_{\mathfrak{V}_2,centr,v_4,1},m_{\mathfrak{V}_2,centr,v_4.2},\ldots,m_{\mathfrak{V}_2,centr,v_4,n_{centr,v_4}}\right\}, \quad (4)$$

де елемент $m_{\mathfrak{V}_2,centr,v_4,1}$ відображає зв'язки між компонентами з центром системи архітектури систем класу $\mathfrak{S}$ згідно відношення «всі до всіх»; елемент $m_{\mathfrak{V}_2,centr,v_4.2}$ відображає зв'язки між компонентами з центром системи архітектури систем класу $\mathfrak{S}$ згідно відношення «один до всіх» архітектуру систем класу $\mathfrak{S}$; $m_{\mathfrak{V}_2,centr,v_4,3}$ відображає зв'язки між компонентами з центром системи архітектури систем класу $\mathfrak{S}$ згідно послідовної топології; $m_{\mathfrak{V}_2,centr,v_4,4}$ відображає зв'язки між компонентами з центром системи архітектури систем класу $\mathfrak{S}$ згідно топології «кільце»; $m_{\mathfrak{V}_2,centr,v_4,5}$ відображає зв'язки між компонентами з центром системи архітектури систем класу $\mathfrak{S}$ згідно топології «решітка»; $m_{\mathfrak{V}_2,centr,v_4,6}$ відображає зв'язки між компонентами з центром системи архітектури систем класу $\mathfrak{S}$ згідно топології «тор»; $m_{\mathfrak{V}_2,centr,v_4,7}$ відображає зв'язки між компонентами з центром системи архітектури систем класу $\mathfrak{S}$ згідно топології «куб»; n_{centr,v_4} – кількість варіантів зв'язків між компонентами з центром системи архітектури систем класу $\mathfrak{S}$.

Введемо, також, множину $M_{\mathfrak{V}_2,centr,v_5}$, елементи якої будуть характеризувати ієрархію компонентів, що містять центр системи, або будуть вказувати на те, що всі компоненти з центром системи є рівнозначними. Рівнів ієрархії компонентів з центром системи може бути декілька і не обов'язково два, як їх мінімальна кількість. Тобто, частина елементів може бути на вищому рівні ієрархії, а частина на нижчому рівні ієрархії. Більша кількість рівнів ієрархії може передбачати встановлення певної топології для таких компонентів, а також визначення для компонентів центру системи з певних рівнів ієрархії заданої функційної спроможності в ієрархії прийняття рішення. Ієрархія для компонентів центру системи може і не стосуватись обмеженої функційної спроможності, а може бути введена лише для оптимізації зв'язків між компонентами. Задамо *множину* $M_{\mathfrak{V}_2,centr,v_5}$ переліком таких елементів:

$$M_{\mathfrak{V}_2,centr,v_5}=\left\{m_{\mathfrak{V}_2,centr,v_5,1},m_{\mathfrak{V}_2,centr,v_5.2},m_{\mathfrak{V}_2,centr,v_5.3},\ldots,m_{\mathfrak{V}_2,centr,v_5,n_{centr,v5}}\right\}, (5)$$

де елемент $m_{\mathfrak{V}_2,centr,v_5,1}$ відображає один рівень ієрархії, тобто фактично відображає відсутність ієрархічних рівнів; елемент $m_{\mathfrak{V}_2,centr,v_5,2}$ відображає два рівні ієрархії; елемент $m_{\mathfrak{V}_2,centr,v_5.3}$ відображає три рівні ієрархії між компонентами з центром системи архітектури систем класу $\mathfrak{S}$; $m_{\mathfrak{V}_2,centr,v_5,n_{centr,v5}}$ відображає $n_{centr,v_5}-1$ рівнів ієрархії між компонентами з центром системи архітектури систем класу $\mathfrak{S}$; n_{centr,v_5} – кількість елементів множини $M_{\mathfrak{V}_2,centr,v_5}$.

Напрям передачі повідомлень між компонентами систем згідно встановлених ***зв'язків*** може бути одностороннім, двостороннім або комбінованим. Тобто, передача повідомлень при організації комунікації між частинами центру системи може мати обмеження. Без обмежень буде двостороння комунікація. З обмеженнями буде одностороння комунікація, при якій повідомлення можуть переміщуватись за встановленим маршрутом. Наприклад, якщо є перехід від однієї компоненти до другої, то зворотного переходу може не бути, а для того, щоб реалізувати передачу в зворотньому напрямі потрібно надсилати повідомлення за маршрутом, який преведе у вказану компоненту проходячи через певні компоненти. Аналогічно, для змішаної комунікації частина компонент буде забезпечена двосторонньою комунікацією, а частина односторонньою. Задамо множиною $M_{\mathfrak{V}_2,centr,v_6}$ варіанти передачі повідомлень з різними типами комунікації так:

$$M_{\mathfrak{V}_2,centr,v_6}=\left\{m_{\mathfrak{V}_2,centr,v_6,1},m_{\mathfrak{V}_2,centr,v_6.2},m_{\mathfrak{V}_2,centr,v_6.3}\right\}, \quad (6)$$

де елемент $m_{\mathfrak{V}_2,centr,v_6,1}$ відображає двосторонню комунікацію між компонентами; елемент $m_{\mathfrak{V}_2,centr,v_6.2}$ відображає односторонню комунікацію між компонентами; елемент $m_{\mathfrak{V}_2,centr,v_6.3}$ відображає змішану комунікацію між компонентами.

Дійсно, при різних варіантах в архітектурі систем з частковою централізацією переважатиме змішана комунікація між *компонентами*. У варіантах централізованої або децентралізованої архітектури, якщо не встановлено додаткових обмежень, переважатиме двостороння комунікація. Встановлення обмежень на здійснення комунікації між компонентами центру системи може бути необхідним, враховуючи специфіку завдань системи, потребу в заплутуванні зловмисників та приховуванні компонент центру системи.

Центр системи може бути в частині компонент, а не точно в усіх компонентах системи. Тобто, центр системи може бути розподіленим між певною частиною компонент, а в частині компонент його може не бути взагалі. Також, можливі варіанти, коли центр системи розподілено в усі компоненти. *Задамо множиною* $M_{\mathfrak{V}_2,centr,v_7}$ варіанти передачі повідомлень з різними типами комунікації так:

$$M_{\mathfrak{V}_2,centr,v_7} = \left\{ m_{\mathfrak{V}_2,centr,v_7.1}, m_{\mathfrak{V}_2,centr,v_7.2} \right\}, \quad (7)$$

де елемент $m_{\mathfrak{V}_2,centr,v_7.1}$ відображає наявність розподілених частин центру системи в усіх компонентах систем класу $\mathfrak{S}$; елемент $m_{\mathfrak{V}_2,centr,v_7.2}$ відображає наявність розподілених частин центру системи в певних компонентах систем класу $\mathfrak{S}$, тобто не в усіх компонентах.

Згідно множини, яку задано формулою (7), можуть бути варіації щодо перебування розподілених частин центру системи в компонентах в активному та неактивному станах. Введемо для визначення цих варіацій множину $M_{\mathfrak{V}_2,centr,v_8}$ *так:*

$$M_{\mathfrak{V}_2,centr,8} = \left\{ m_{\mathfrak{V}_2,centr,v_8.1}, m_{\mathfrak{V}_2,centr,v_8.2}, m_{\mathfrak{V}_2,centr,v_8.3} \right\}, \quad (8)$$

де елемент $m_{\mathfrak{V}_2,centr,v_8.1}$ відображає наявність розподілених частин центру системи в компонентах, які для нього задані, винятково в активному стані; елемент $m_{\mathfrak{V}_2,centr,v_8.2}$ відображає наявність розподілених частин центру системи в компонентах, які для нього задані, в двох станах (активний стан, пасивний стан); елемент $m_{\mathfrak{V}_2,centr,v_8.3}$ відображає наявність всіх розподілених частин центру системи в компонентах, які для нього задані, винятково в пасивному стані.

Активний стан розподіленої частини центру системи в певній компоненті означає його функціонування в поточний момент часу. Пасивний стан розподіленої частини центру системи в певній компоненті означає його перебування в поточний момент часу в очікуванні вказівки про перехід до активного стану.

Центр системи може бути розподілений так, що в усіх компонентах системи, в яких передбачено його наявність, буде однаковий функціонал. Тобто, всі компоненти, в яких буде наявний функціонал центру системи, будуть мати однакові функціонали. Якщо центр системи біде характеризуватись елементом $m_{\mathfrak{V}_2,centr,v_5.1}$ з формули (5), то всі компоненти з центром системи будуть фактично формувати децентралізовану архітектуру центру системи. Але центр системи може не бути в контексті ієрархії згідно формули (5), а може мати розділення таким чином, що декілька основних функцій будуть в окремих компонентах і матимуть вищий пріоритет порівняно з рештою функцій, які будуть перебувати в решті компонент, в яких задано функціонал з центром системи. В цьому варіанті центр системи складається з функцій, які розподілено між різними компонентами, і частина з них або одна є основними чи основною. Таким чином, центр розподілений за його частинами. Також, може бути варіант розподілу центру системи таким чином, що частина компонент міститиме основні функції центру системи, а решта компонент, в яких задано центр системи, другорядні. При цьому варіанті частина компонент з основними функціями центру системи буде рівнозначною між собою. Це важливо у випадку розпаду системи на декілька частин через розділення вузлів корпоративної мережі на певний інтервал часу. Тоді, буде збережено стійкість системи і вона зможе продовжити свою роботу. Введемо для визначення цих варіантів з розподіленням функцій центру системи множину $M_{\mathfrak{V}_2,centr,v_9}$ так:

$$M_{\mathfrak{V}_2,centr,9} = \left\{ m_{\mathfrak{V}_2,centr,v_9.1}, m_{\mathfrak{V}_2,centr,v_9.2}, m_{\mathfrak{V}_2,centr,v_9.3} \right\}, \quad (9)$$

де елемент $m_{\mathfrak{V}_2,centr,v_9.1}$ відображає випадок, коли всі компоненти, в яких наявний функціонал центру системи, будуть мати однакові функціонали; елемент $m_{\mathfrak{V}_2,centr,v_9.2}$ відображає випадок, коли центр системи має розділення таким чином, що декілька основних функцій будуть в окремих компонентах і мають вищий пріоритет порівняно з рештою функцій, які перебувають в решті компонент, в яких задано функціонал з центром системи; елемент $m_{\mathfrak{V}_2,centr,v_9.3}$ відображає випадок, коли варіант розподілу центру системи такий, що частина компонент містить основні функції центру системи, а решта компонент, в яких задано центр системи, другорядні, і, при цьому варіанті частина компонент з основними функціями центру системи буде рівнозначною між собою.

Функціонал центру системи може бути сформовано таким чином, що він буде складатись з незалежних підсистем. Для їх запуску в різних вузлах корпоративної мережі можна використовувати процедуру віддаленого запуску. Тоді, такий функціонал розподіленої частини центру системи може міститись в різних компонентах, в який задано функціонал центру системи, і буде формуватись з різних незалежних підсистем різних компонент. Головною незалежною підсистемою буде та підсистема, яка при встановлені функціоналу центру системи визначена і закріплена за відповідною компонентою. Таку організацію функціоналу компоненти центру системи

вважатимемо динамічною. Якщо ж функціонал компоненти центру системи складається з незалежних підсистем і всі вони встановлені в одну компоненту та запускаються в ній при виклику з головної підсистеми, то таку організацію функціоналу компоненти центру системи вважатимемо статичною. У випадку наявності одночасно двох варіантів з динамічною та статичною організацією функціоналу компоненти центру системи, тоді вважатимемо таку організацію змішаною. Для систем *класу* $\mathfrak{S}$ змішана організація може виникнути після повернення системи до цілісної, якщо перед цим було розділення. Під час її розділення в одній частині могла бути задіяна модель із динамічною організацією, а в решті частин – модель з статичною організацією. Після об'єднання фактично стає змішана організація. Задамо ці випадки множиною $M_{\mathfrak{M}_2,centr,v_{10}}$ *так:*

$$M_{\mathfrak{M}_2,centr,10} = \left\{ m_{\mathfrak{M}_2,centr,v_{10},1}, m_{\mathfrak{M}_2,centr,v_{10}.2}, m_{\mathfrak{M}_2,centr,v_{10}.3} \right\}, \quad (10)$$

де елемент $m_{\mathfrak{M}_2,centr,v_{10},1}$ відображає динамічну організацію функціоналу розподіленої частини центру системи*; елемент* $m_{\mathfrak{M}_2,centr,v_{10}.2}$ відображає статичну організацію функціоналу розподіленої частини центру системи; елемент $m_{\mathfrak{M}_2,centr,v_{10}.3}$ відображає змішану організацію функціоналу розподіленої частини центру системи.

Розглянемо введені множини та їх елементи згідно формул (1)-(10) в поєднанні для забезпечення централізації в системах класу $\mathfrak{S}$. Таке поєднання множин та їх елементів між собою забезпечить відображення особливостей центру системи за різновидами його архітектури, які необхідно використовувати при функціонуванні систем класу $\mathfrak{S}$ з метою приховування центру системи та заплутування зловмисників. Фактично, перебуваючи в одному із визначених центром системи можливих варіантів централізації, система перебуває в заданому стані, який характеризує її архітектуру в поточний момент часу. Протягом часу функціонування системи можуть самостійно змінювати варіанти централізації, переходячи при цьому до іншого стану.

Подамо в табл. 1 фрагмент варіантів централізації з особливостями, які відображені елементами в формулах (1)-(10).

Таким чином, здійснено подання характерних властивостей варіантів централізації в системах класу $\mathfrak{S}$ множинами, які задано за формулами (1)-(10), та встановлено кількість можливих варіантів. Отриманий результат щодо кількості варіантів відображає потенційну складність при здійсненні вибору наступного варіанту централізації. Розроблене подання через характерні властивості необхідне для формування правил визначення наступного варіанту централізації в архітектурі систем класу $\mathfrak{S}$, враховуючи потенційно велику кількість можливих варіантів.

Дослідження ефективності застосування теоретико-множинного подання характерних властивостей для подання централізації в архітектурі мультикомп'ютерних систем. Розглянемо ефективність розроблених характерних властивостей та їх поділ на множини в контексті досягнення поставленої мети щодо

Таблиця 1

Фрагмент варіантів централізації в архітектурі систем

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	$M_{\mathfrak{S}_2,centr,v_1}$				$M_{\mathfrak{S}_2,centr,v_3}$		$M_{\mathfrak{S}_2,centr,v_5}$		$M_{\mathfrak{S}_2,centr,v_7}$				$M_{\mathfrak{S}_2,centr,v_9}$					$M_{\mathfrak{S}_2,centr,v_{11}}$			$M_{\mathfrak{S}_2,centr,v_{13}}$		$M_{\mathfrak{S}_2,centr,8}$			$M_{\mathfrak{S}_2,centr,9}$			$M_{\mathfrak{S}_2,centr,10}$		
	$m_{\mathfrak{S}_2,centr,v_1,1}$	$m_{\mathfrak{S}_2,centr,v_1,2}$	$m_{\mathfrak{S}_2,centr,v_1,3}$	$m_{\mathfrak{S}_2,centr,v_1,4}$	$m_{\mathfrak{S}_2,centr,v_3,1}$	$m_{\mathfrak{S}_2,centr,v_3,2}$	$m_{\mathfrak{S}_2,centr,v_5,1}$	$m_{\mathfrak{S}_2,centr,v_5,2}$	$m_{\mathfrak{S}_2,centr,v_7,1}$	$m_{\mathfrak{S}_2,centr,v_7,2}$	...	$m_{\mathfrak{S}_2,centr,v_7,n_{centr,v_7}}$	$m_{\mathfrak{S}_2,centr,v_9,1}$	$m_{\mathfrak{S}_2,centr,v_9,2}$	$m_{\mathfrak{S}_2,centr,v_9,3}$	...	$m_{\mathfrak{S}_2,centr,v_9,n_{centr,v_9}}$	$m_{\mathfrak{S}_2,centr,v_{11},1}$	$m_{\mathfrak{S}_2,centr,v_{11},2}$	$m_{\mathfrak{S}_2,centr,v_{11},3}$	$m_{\mathfrak{S}_2,centr,v_{13},1}$	$m_{\mathfrak{S}_2,centr,v_{13},2}$	$m_{\mathfrak{S}_2,centr,8,1}$	$m_{\mathfrak{S}_2,centr,8,2}$	$m_{\mathfrak{S}_2,centr,8,3}$	$m_{\mathfrak{S}_2,centr,9,1}$	$m_{\mathfrak{S}_2,centr,9,2}$	$m_{\mathfrak{S}_2,centr,9,3}$	$m_{\mathfrak{S}_2,centr,v_{10},1}$	$m_{\mathfrak{S}_2,centr,v_{10},2}$	$m_{\mathfrak{S}_2,centr,v_{10},3}$
1	1	0	0	0	0	1	1	0	1	0	0	0	1	0	0	0	0	1	0	0	1	0	1	0	0	1	0	0	1	0	0
2	1	0	0	0	0	1	1	0	1	0	0	0	0	1	0	0	0	1	0	0	1	0	1	0	0	1	0	0	1	0	0
3	1	0	0	0	0	1	1	0	1	0	0	0	0	0	1	0	0	1	0	0	1	0	1	0	0	1	0	0	1	0	0
4	1	0	0	0	0	1	1	0	1	0	0	0	0	0	0	1	0	1	0	0	1	0	1	0	0	1	0	0	1	0	0
5	1	0	0	0	0	1	1	0	1	0	0	0	0	0	0	0	1	1	0	0	1	0	1	0	0	1	0	0	1	0	0
6	1	0	0	0	0	1	1	0	1	0	0	0	1	0	0	0	0	0	1	0	1	0	1	0	0	1	0	0	1	0	0
7	1	0	0	0	0	1	1	0	1	0	0	0	0	1	0	0	0	0	1	0	1	0	1	0	0	1	0	0	1	0	0
8	1	0	0	0	0	1	1	0	1	0	0	0	0	0	1	0	0	0	1	0	1	0	1	0	0	1	0	0	1	0	0
9	1	0	0	0	0	1	1	0	1	0	0	0	0	0	0	1	0	0	1	0	1	0	1	0	0	1	0	0	1	0	0
10	1	0	0	0	0	1	1	0	1	0	0	0	0	0	0	0	1	0	1	0	1	0	1	0	0	1	0	0	1	0	0
11	1	0	0	0	0	1	1	0	1	0	0	0	1	0	0	0	0	0	0	1	1	0	1	0	0	1	0	0	1	0	0
12	1	0	0	0	0	1	1	0	1	0	0	0	0	1	0	0	0	0	0	1	1	0	1	0	0	1	0	0	1	0	0

синтезу систем, які можуть в процесі свого функціонування перебудовувати свою архітектуру без залучення адміністратора. Основною частиною мультикомп'ютерних систем, яка потребує дослідження щодо перебудови є центр системи. Задані характерні властивості централізації в архітектурі таких систем за формулами (1)-(10) дають змогу визначити не тільки потенційну кількість варіантів централізації, але й визначити стійкість та ймовірність виявлення зловмисником центру системи.

Потенційну кількість варіантів централізації визначимо згідно врахування характерних властивостей кожної множини, які визначені формулами (1)-(10). Оскільки, з кожної множини може бути взято тільки по одній характерній властивості, тоді кількість таких характерних властивостей буде дорівнювати 10 з 31 можливої характерної властивості. Тоді, 21 характерна властивість буде відсутня в системі. Взагалі допустимо, що система може вибирати довільних варіант централізації з різними характерними властивостями, як подано фрагментом потенційних варіантів в табл. 1. Наявність певної характерної властивості позначено в табл. 1 одиницею, а відсутність – нулем. Кількість виборів однієї характерної властивості з першої множини буде дорівнювати кількості перестановок без повторень з чотирьох елементів по одному елементу. Аналогічно визначаємо для решти дев'яти множин. Отримані значення для кожної характерної властивості з кожної з десяти множин за правилом добутку перемножуємо і отримуємо потенційно можливу кількість варіантів централізації, тобто

$$K_{centr} = \prod_{i=1}^{10} C_1^{N^{centr}_{M_{\mathfrak{M}_2,\,centr,i}}}, \qquad (11)$$

де $N^{centr}_{M_{\mathfrak{M}_2,\,centr,i}}$ – кількість елементів в множині характерних властивостей $M_{\mathfrak{M}_2,\,centr,i}$; $i = 1,2,\ldots,10$.

Подані за формулами (1)-(10) множини характерних властивостей дають змогу, також, встановити варіанти централізації, в які неможливо перейти з попереднього поточного варіанту централізації. Кількість таких варіантів є невеликою і пов'язана переважно з станом системи, коли вона розподіляється на дві непорожні незв'язні частини, а потім при поверненні до повноцінного варіанту пробує вибрати наступний варіант централізації.

Ймовірність виявлення центру мультикомп'ютерної системи є оберненою величиною до кількості компонент в системі. Для такого визначення можуть обиратись тільки активні в поточний момент часу компоненти. Щодо компонент, в яких міститься функціонал з центром системи можливі варіанти. Наприклад, система в поточний момент часу повністю централізована у варіанті без розподілення центру між декількома компонентами. Також, може бути варіант децентралізованої архітектури, тоді всі компоненти системи містять функціонал центру системи. Але у варіантах децентралізованої архітектури чи частково децентралізованої, частково централізованої або централізованої з певною кількістю компонент з функціоналом центру вважатимемо, що вихід з ладу однієї з компонент системи не призведе до виходу з ладу центру системи. Тому, ймовірність пошуку центру системи буде визначатись так:

$$P_{zl} = \frac{1}{K_{komp}}, \qquad (12)$$

де K_{komp} – кількість компонент в системі.

Якщо припустити, що всі процеси в корпоративній мережі будуть спрощеними щодо дій зловмисника і пошук центру системи для виведення його з ладу буде відповідати моделі, яка описана з припущення за формулою (12), тоді розроблення різної кількості варіантів щодо централізації в системі недоцільне. Але поведінка зловмисника переважно визначається його цілеспрямованістю та набором певних інструментів досягнення мети. Наприклад, після пошуку однієї компоненти з центром системи, він як правило переходить до іншої компоненти, потім до наступної компоненти, продовжуючи захоплювати або виводити з ладу компоненти системи чи комп'ютерні станції. В процесі таких дій зловмисник як правило постійно виконує шаблонні дії з використанням наявних інструментів. Система проти якої спрямовані дії зловмисника повинна мати набір інструментів для відповіді на прояви зловмисних дій. Одним з варіантів на повторювані дії зловмисника є варіант з перебудовою архітектури системи і її центру. В такому випадку ймовірність виявлення центру системи зловмисником буде суттєво менше значення, яке отримується за формулою (12). Тому, запропоноване рішення щодо зміни централізації в архітектурі мультикомп'ютерних систем згідно характерних властивостей, які задано множинами за формулами (1)-(10), покращує стійкість таких систем щодо зловмисних впливів на їх центр.

Висновки. Розроблено характерні властивості централізації в архітектурі мультикомп'ютерних систем приманок та пасток для виявлення та протидії ЗПЗ та КА. Характерні властивості згруповано в множини характерних властивостей. Згідно такого визначення отримано

показники для використання їх при визначенні наступного варіанту централізації в архітектурі мультикомп'ютерних систем, яке вони повинні здійснювати самостійно без залучення адміністратора. Аналіз запропонованого рішення підтвердив перспективність напряму досліджень.

Напрямом подальших досліджень буде деталізація механізмів централізації в архітектурі мультикомп'ютерних систем для формування зв'язків між ними та на їх основі правил, які будуть забезпечувати перехід систем до наступного варіанту централізації.

ЛІТЕРАТУРА:

1. Kashtalian A., Lysenko S., Savenko B., Sochor T., Kysil, T. Principle and method of deception systems synthesizing for malware and computer attacks detection. *Radioelectronic and Computer Systems,* (023. 0(4), 112–151. doi:https://doi.org/10.32620/reks.2023.4.10

2. B. Savenko, A. Kashtalian, S. Lysenko and O. Savenko, "Malware Detection By Distributed Systems with Partial Centralization," *2023 IEEE 12th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, Dortmund, Germany, 2023, pp. 265–270, doi: 10.1109/IDAACS58523.2023.10348773.

3. Savenko O., Sachenko A., Lysenko S., Markowsky G., Vasylkiv N. BOTNET DETECTION APPROACH BASED ON THE DISTRIBUTED SYSTEMS. *International Journal of Computing*, 2020. 19(2), 190–198. https://doi.org/10.47839/ijc.19.2.1761

4. Kashtalian A., Lysenko S., Savenko O., Nicheporuk A., Sochor T., Avsiyevych V. 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

5. Каштальян А. С. Концептуальна модель архітектури мультикомп'ютерних систем із приманками та пастками для виявлення та протидії зловмисному програмному забезпеченнюю *Information Technology: Computer Science, Software Engineering and Cyber Security*, 2023, № 3, С. 22

6. Suratkar S., Shah K., Sood A. An adaptive honeypot using Q-Learning with severity analyzer. *J Ambient Intell Human Comput*, 2022, 13, P.4865–4876.

7. 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.

8. Leyi S., Yang L., Liu T., Liu J., Shan B., Chen H. Dynamic Distributed Honeypot Based on Blockchain. *IEEE Access*, 2019. P. 1–1. 10.1109/ACCESS.2019.2920239.

9. Fan W., Fernández D., Du Z. Adaptive and Flexible Virtual Honeynet. 2015. 10.1007/978-3-319-25744-0_1.

10. 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*, 2021, vol. 441.

11. Li Y, Shi L, Feng H. A Game-Theoretic Analysis for Distributed Honeypots. *Future Internet*, 2019. 11(3), 65.

12. Han W., Zhao Z., Doupé A., Ahn G.-J. HoneyMix: Toward SDN-based Intelligent Honeynet. 2016. 10.1145/2876019.2876022.

13. Baykara M., Das R. oftSwitch: a centralized honeypot-based security approach usingsoftware-defined switching for secure management of VLAN networks. *Turkish journal of electrical engineering & computer sciences*, 2019, 27, P.3309–3325

14. Anwar A. H., Zhu M., Wan Z., Cho J. -H., Kamhoua C. A., Singh M. P. Honeypot-Based Cyber Deception Against Malicious Reconnaissance via Hypergame Theory. *GLOBECOM 2022 – 2022 IEEE Global Communications Conference, Rio de Janeiro, Brazil*, 2022, P. 3393–3398.

15. Schindler S., Schnor B., Scheffler T. Sven Schindler. Hyhoneydv6: A hybrid Honeypot Architecture for Ipv6 Networks. *International Journal of Intelligent Computing Research (IJICR)*, 2015, June, Volume 6, Issue 2, P. 562–570

16. Wegerer M., Tjoa S. Defeating the Database Adversary Using Deception – A MySQL Database Honeypot. 2016 *International Conference on Software Security and Assurance (ICSSA), Saint Pölten, Austria*, 2016, P. 6–10.

17. Achleitner S., Porta T., McDaniel P., Sugrim S., Krishnamurthy S., Chadha R. Cyber Deception: Virtual Networks to Defend Insider Reconnaissance. 2016. P.57–68. 10.1145/2995959.2995962.

18. Zaman M., Tao L., Maldonado M., Liu C., Sunny A., Xu S., Chen L. Optimally Blending Honeypots into Production Networks: Hardness and Algorithms. Science of Cyber Security : 5th International Conference,

SciSec 2023, Melbourne, VIC, Australia, July 11–14, Proceedings. Springer-Verlag, Berlin, Heidelberg, 2023, P.285–304.

19. Chiang C. J., Gottlieb Y. M., Sugrim S., Chadha R., Serban C., Poylisher A., Marvel L. M., Santos J. ACyDS: *An adaptive cyber deception system. MILCOM 2016 – 2016 IEEE Military Communications Conference*, P. 800–805.

20. Ehab Al-Shaer. A Cyber Mutation: Metrics, Techniques and Future Directions. *In Proceedings of the 2016 ACM Workshop on Moving Target Defense (MTD '16). Association for Computing Machinery, New York, NY, USA,* 2016, 1.

REFERENCES:

1. Kashtalian, A., Lysenko, S., Savenko, B., Sochor, T., & Kysil, T. (2023). Principle and method of deception systems synthesizing for malware and computer attacks detection. *Radioelectronic and Computer Systems,* 0(4), P.112–151.

2. Savenko, B., Kashtalian, A., Lysenko, S. & Savenko, O. (2023). "Malware Detection By Distributed Systems with Partial Centralization," *2023 IEEE 12th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, *Dortmund, Germany*, P. 265–270.

3. Savenko, O., Sachenko, A., Lysenko, S., Markowsky, G., & Vasylkiv, N. (2022). Botnet detection approach based on distributed systems. *International Journal of Computing*, P.190–198

4. 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*, (1), P.152–175. doi:https://doi.org/10.32620/reks.2024.1.13

5. Kashtalian, A. (2023). A conceptual model of the architecture of multi-computer systems with decoys and traps for detecting and countering malware and computer attacks. *Information Technology: Computer Science, Software Engineering and Cyber Security*, № 3, P. 22–31.

6. Suratkar, S., Shah, K., Sood, A. (2022). An adaptive honeypot using Q-Learning with severity analyzer. *J Ambient Intell Human Comput*, 13, P. 4865–4876.

7. Lysenko, S., Bobrovnikova, K., Kharchenko, V., Savenko, O. (2022). IoT Multi-Vector Cyberattack Detection Based on Machine Learning Algorithms: Traffic Features Analysis, Experiments, and Efficiency. *Algorithms*, 15(7), 239.

8. Leyi, S., Yang, L., Liu, T., Liu, J., Shan, B., Chen, H. (2019). Dynamic Distributed Honeypot Based on Blockchain. *IEEE Access*, P. 1–1. 10.1109/ACCESS.2019.2920239.

9. Fan, W., Fernández, D., Du, Z. (2015). Adaptive and Flexible Virtual Honeynet. 10.1007/978-3-319-25744-0_1.

10. Acosta, J. C., Basak, A., Kiekintveld, C., Kamhoua, C. (2021). 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*, vol. 441.

11. Li, Y, Shi, L, Feng, H. (2019). A Game-Theoretic Analysis for Distributed Honeypots. *Future Internet*, 11(3), 65.

12. Han, W., Zhao, Z., Doupé, A., Ahn, G.-J. (2016). HoneyMix: Toward SDN-based Intelligent Honeynet. 10.1145/2876019.2876022.

13. Baykara, M., Das, R. (2019). oftSwitch: a centralized honeypot-based security approach usingsoftware-defined switching for secure management of VLAN networks. *Turkish journal of electrical engineering & computer sciences*, 27, P.3309–3325

14. Anwar, A. H., Zhu, M., Wan, Z., Cho, J. -H., Kamhoua, C. A., Singh, M. P. (2022). Honeypot-Based Cyber Deception Against Malicious Reconnaissance via Hypergame Theory. *GLOBECOM 2022 – 2022 IEEE Global Communications Conference, Rio de Janeiro, Brazil*, P. 3393–3398.

15. Schindler, S., Schnor, B., Scheffler, T. (2015). Sven Schindler. Hyhoneydv6: A hybrid Honeypot Architecture for Ipv6 Networks. *International Journal of Intelligent Computing Research (IJICR)*, June, Volume 6, Issue 2, P. 562–570

16. Wegerer, M., Tjoa, S. (2016). Defeating the Database Adversary Using Deception – A MySQL Database Honeypot. 2016 *International Conference on Software Security and Assurance (ICSSA), Saint Pölten, Austria*, P. 6–10.

17. Achleitner, S., Porta, T., McDaniel, P., Sugrim, S., Krishnamurthy, S., Chadha, R. (2016). Cyber Deception: Virtual Networks to Defend Insider Reconnaissance. P.57–68. 10.1145/2995959.2995962.

18. Zaman, M., Tao, L., Maldonado, M., Liu, C., Sunny, A., Xu, S., Chen, L. (2023). Optimally Blending Honeypots into Production Networks: Hardness and Algorithms. Science of Cyber Security: 5th International Conference, SciSec 2023, Melbourne, VIC, Australia, July 11–14, Proceedings. Springer-Verlag, Berlin, Heidelberg, P.285–304.

19. Chiang, C. J., Gottlieb, Y. M., Sugrim, S., Chadha, R., Serban, C., Poylisher, A., Marvel, L. M., & Santos, J. ACyDS: *An adaptive cyber deception system. MILCOM 2016 – 2016 IEEE Military Communications Conference*, P. 800–805.

20. Ehab, Al-Shaer. (2016). A Cyber Mutation: Metrics, Techniques and Future Directions. *In Proceedings of the 2016 ACM Workshop on Moving Target Defense (MTD '16). Association for Computing Machinery, New York, NY, USA,* 1.