https://doi.org/10.31891/2219-9365-2025-82-48
УДК 004.8:004.056.53

ТАРАСЕНКО Ярослав
Державний науково-дослідний інститут випробувань і сертифікації озброєння та військової техніки
https://orcid.org/:0000-0002-5902-8628
e-mail: yaroslav.tarasenko93@gmail.com
ТУРОВСЬКИЙ Олександр
Державний університет інформаційно-комунікаційних технологій
https://orcid.org/0000-0002-4961-0876
e-mail: s19641011@ukr.net
ІВАНКІН Віктор
Державний університет інформаційно-комунікаційних технологій
https://orcid.org/0009-0000-9033-9187
e-mail: victorentino@gmail.com
МАТУСЯК Павло
Державний університет інформаційно-комунікаційних технологій
https://orcid.org/0009-0008-8923-3631
e-mail: pavelmatusyak@gmail.com
ТОМАШЕВСЬКИЙ Михайло
Державний університет інформаційно-комунікаційних технологій
https://orcid.org/0009-0004-9065-7408
e-mail: m.Tomashevskyi@stud.duikt.edu.ua

ЗАБЕЗПЕЧЕННЯ КІБЕРЗАХИСТУ КОРПОРАТИВНОЇ МЕРЕЖІ ПЕРЕДАЧІ ДАНИХ В ХОДІ ОРГАНІЗАЦІЇ ВЗАЄМОДІЇ МІЖ ПРИСТРОЯМИ IoT ДОСЛІДНИЦЬКИХ ЛАБОРАТОРІЙ

У роботі було проведено аналіз ефективності існуючих методів забезпечення кіберзахисту корпоративної мережі науково-дослідної лабораторії при взаємодією із пристроями IoT, які входять до складу сенсорної мережі лабораторних випробувань. Аналіз проводився з урахуванням перекриття кіберзагроз і конвергенції фізичної та інформаційної безпеки кіберфізичної системи, утвореної на основі їх взаємодії. Для отримання точного представлення взаємодії сенсорної та корпоративної мереж в умовах впливу кіберзагроз пристроїв IoT було визначено перелік спільних кіберзагроз обох мереж та кіберзагроз, характерних кожній з них в умовах виконання задач лабораторних випробувань. Визначено вектори впливу кіберзагроз сенсорної мережі на кіберзагрози корпоративній мережі. Досліджено методи кіберзахисту від кожної кіберзагрози з точки зору їх переваг і недоліків при застосуванні до кіберфізичної системи лабораторних випробувань та досліджено їх інтеграційний потенціал. Для кожної кіберзагрози визначено об'єкти потенційних кібератак зловмисників. На основі визначених кіберзагроз, методів кіберзахисту та об'єктів потенційних атак було сформовано принципову модель впливу кіберзагроз на області кіберзахисту корпоративної мережі. Враховано вплив в умовах перекриття кіберзагроз та подвійного бар'єру кіберзахисту. Визначено вплив характерних сенсорній мережі кіберзагроз на області кіберзахисту корпоративної мережі, що дозволило врахувати конвергенцію фізичної та інформаційної безпеки в кіберфізичній системі. Дослідження впливу кіберзагроз на основі побудованої принципової моделі дозволило довести підвищення коефіцієнту кіберзагроз корпоративної мережі для 5 з 8 об'єктів області кіберзахисту корпоративної мережі, що доводить зниження ефективності використання методів кіберзахисту та потребу врахування додаткових коефіцієнтів впливу при забезпеченні кіберзахисту корпоративної мережі при взаємодії з пристроями IoT в лабораторних випробуваннях.

Ключові слова: сенсорна мережа, корпоративна мережа, IoT, лабораторні випробування, автоматизовані лабораторії, кіберзахист корпоративної мережі, перекриття кіберзагроз, конвергенція безпеки.

TARASENKO Yaroslav
State Scientific Research Institute of Armament and Military Equipment Testing and Certification
TUROVSKY Oleksandr, IVANKIN Viktor,
MATUSYAK Pavlo, TOMASHEVSKYY Mykhailo
State University of Telecommunications

ENSURING CYBER PROTECTION OF THE CORPORATE NETWORK OF DATA TRANSMISSION DURING THE ORGANIZATION OF INTERACTION BETWEEN IoT DEVICES OF RESEARCH LABORATORIES

The paper analyzed the effectiveness of existing methods for protecting the corporate network of a research laboratory when interacting with IoT devices that are part of the sensor network of laboratory tests. The analysis was carried out taking into account the overlap of threats and the convergence of physical and information security of the cyber-physical system formed on the basis of their interaction. To obtain an accurate representation of the interaction of sensor and corporate networks under the influence of IoT device threats, a list of common threats of both networks and threats characteristic of each of them under the conditions of performing laboratory test tasks was determined. The vectors of influence of sensor network threats on threats to the corporate network were determined. Methods of protection against each threat were studied from the point of view of their advantages and disadvantages when applied to the cyber-physical system of laboratory tests and their integration potential was investigated. For each

threat, the objects of potential attacks by attackers were identified. Based on the identified threats, protection methods and objects of potential attacks, a principle model of the impact of threats on the areas of corporate network protection was formed. The impact in conditions of overlapping threats and a double barrier of protection was taken into account. The impact of threats characteristic of the sensor network on the areas of corporate network protection was determined, which allowed us to take into account the convergence of physical and information security in the cyber-physical system. Research into the impact of threats based on the constructed principle model allowed us to prove an increase in the corporate network threat coefficient for 5 out of 8 objects of the corporate network protection area, which proves a decrease in the effectiveness of the use of protection methods and the need to take into account additional impact coefficients when ensuring corporate network protection when interacting with IoT devices in laboratory tests.

Keywords: sensor network, corporate network, IoT, laboratory tests, automated laboratories, corporate network protection, threat overlap, security convergence.

Стаття надійшла до редакції / Received 12.04.2025
Прийнята до друку / Accepted 07.05.2025

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

На сьогоднішній день в умовах сучасних викликів під час процесу вступу України до Європейського Союзу все більшої актуальності набуває потреба контролю якості продукції різних галузей виробництва. Одним з найбільш ефективних шляхів підтвердження якості є лабораторні випробування. Дослідно-випробувальні лабораторії в Україні характеризуються рядом проблем, які потребують нагального вирішення. Такі проблеми та перспективи їх вирішення проаналізовано в роботі [1], з результатів якої можна виокремити вимоги до безпеки процесів вимірювань і випробувань в лабораторних умовах, питання забезпечення точності і відтворюваності результатів лабораторних вимірювань за умов мінімізації втручання людини в процеси випробувань та необхідність удосконалення лабораторної бази. Одним з найбільш важливих напрямків удосконалення лабораторної бази з урахуванням актуальних вимог є автоматизація лабораторних випробувань.

Існують різні шляхи автоматизації лабораторної бази в залежності від задач та очікуваного ефекту. Для виконання задач лабораторних випробувань перспективним напрямком є застосування технології Інтернету речей (IoT), що відображено в сучасних наукових працях як [2]. Технології IoT широко представлені у прикладному аспекті та мають широке застосування. У рамках розгляду задач лабораторних випробувань на базі технології IoT функціонують сенсорні мережі, до складу яких входять датчики широкого функціонального спектру та виконавчі механізми (актуатори). З метою проведення глибинного аналізу отриманих даних в ході лабораторних випробувань на наступному етапі після граничних обчислень, керування процесами у сенсорній мережі, збору і обробки даних для подальшого порівняння з попередніми результатами випробувань, для навчання штучного інтелекту при реалізації інтелектуальних сенсорних мереж, виникає необхідність застосування зовнішніх серверів. У даних умовах сенсорна мережа лабораторних випробувань інтегрується із корпоративною мережею. Така інтеграції породжує явище так званої конвергенції фізичного та цифрового середовища, описане в роботі [3]. Таке явище породжує ряд нових кіберзагроз безпеці корпоративної мережі при взаємодії з IoT пристроями під час лабораторних випробувань. Однією з таких кіберзагроз може бути отримання доступу до корпоративної мережі через компрометацію фізичного IoT пристрою.

Виникає потреба аналізу існуючих методів кіберзахисту сенсорних та корпоративних мереж в умовах конвергенції фізичного та цифрового середовища для визначення ефективності забезпечення кіберзахисту корпоративної мережі при взаємодії з IoT пристроями в лабораторних випробуваннях. Формується необхідність визначення шляхів підвищення ефективності існуючих методів забезпечення кіберзахисту корпоративної мережі та пошуку нових напрямків розвитку методів кіберзахисту, яка породжена явищем конвергенції фізичної та інформаційної безпеки.

АНАЛІЗ ДОСЛІДЖЕНЬ ТА ПУБЛІКАЦІЙ

Розвиток методів кіберзахисту в кіберфізичних системах, які передбачають інтеграцію процесів обчислень, мережевого функціоналу та фізичних засобів контролю [4] на сьогоднішній день характеризується широким спектром існуючих напрямків. Виходячи із сучасних наукових досліджень в області забезпечення кіберзахисту кіберфізичних систем, напрямки розвитку актуальних методів кіберзахисту можна класифікувати за технологічною ознакою. Інакше кажучи, використані базові технології формують групи методів кіберзахисту, які можуть бути застосовані до тієї чи іншої складової кіберфізичної системи. Можна виділити групу методів криптографічного кіберзахисту. У роботі [5] представлено алгоритм полегшеного шифрування для кіберзахисту даних, які передаються в мережі. Наступну групу утворюють методи з блокчейн технологією. У роботі [6] розглядаються способи контролю незмінності даних які надходять до та від фізичних пристроїв за допомогою технології блокчейн. Ще одну групу утворюють методи на основі штучного

інтелекту. У роботі [7] описується підхід виявлення аномалій і вторгнень в кіберфізичну систему на основі нейромережі.

Кожна розглянута група методів забезпечує кіберзахист на різних рівнях архітектури кіберфізичної системи. Результати, представлені у [5] доцільно використовувати для кіберзахисту каналу зв'язку, у [6] для кіберзахисту вхідних та вихідних даних актуаторів, у [7] для виявлення зовнішніх кіберзагроз. Недостатньо приділено уваги дослідженням щодо інтегрованого використання методів кіберзахисту, які функціонують на різних рівнях архітектури та ґрунтуються на різних технологіях. Роботи [8-9] розглядають питання багаторівневого кіберзахисту в кіберфізичних системах, основаних на IoT технологіях, але не надають дані дослідження впливу кіберзагроз, які виникають у фізичній системі на цифрову систему, зокрема не розглядається корпоративна мережа як складова кіберфізичної системи та не досліджується одна із сфер її можливого застосування – лабораторні випробування.

У сучасних публікаціях, присвячених проблемам кіберзахисту кіберфізичних систем не розглядається питання перекриття кіберзагроз та вплив кіберзагроз фізичної системи на цифрову в умовах забезпечення кіберзахисту цифрової системи, якою виступає корпоративна мережа, що не дозволяє оцінити ефективність різних груп методів в умовах застосування до однієї кіберфізичної системи. Варто відзначити недостатність наукових праць, присвячених забезпеченню кіберзахисту кіберфізичних систем, які ґрунтуються на технології IoT та забезпечують виконання задач лабораторних випробувань.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Метою статті є аналіз ефективності існуючих методів забезпечення кіберзахисту корпоративної мережі при взаємодії з пристроями IoT з урахуванням конвергенції фізичної та інформаційної безпеки, утвореної цією взаємодією у кіберфізичній системі лабораторних випробувань.

Для досягнення мети в статті необхідно вирішити наступні задачі:

1) аналіз спільних та унікальних кіберзагроз безпеки для корпоративної та сенсорної мереж в умовах виконання задач лабораторних випробувань;

2) аналіз методів кіберзахисту від існуючих кіберзагроз;

3) формування принципової моделі впливу кіберзагроз на області кіберзахисту корпоративної мережі з урахуванням перекриття кіберзагроз і конвергенції фізичного та цифрового середовища;

4) дослідження впливу кіберзагроз з урахуванням принципової моделі.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Кіберфізичною системою у сфері лабораторних випробувань виступає система, елементами якої є сенсорна мережа, що відповідає за фізичну взаємодію з навколишнім середовищем і об'єктами випробувань та корпоративна мережа лабораторії, що відповідає за цифрову обробку інформації та інтерпретацію результатів при взаємодії з працівниками. Забезпечення кіберзахисту такої системи є складним багаторівневим процесом. Забезпечення кіберзахисту акцентується саме на корпоративній мережі, що зумовлено критичною важливістю цілісності даних, які надходять до мережі з метою подальшої обробки і зберігання від сенсорів, та які впливають на подальші процеси управління лабораторними випробуваннями. Ефективність наявних методів та засобів кіберзахисту кіберфізичних систем у випадку організації кіберфізичної системи лабораторних випробувань є непередбачуваною. Визначення впливу різних методів кіберзахисту сенсорної мережі, яка функціонує на базі технології IoT на ефективність методів кіберзахисту корпоративної мережі лабораторії передбачає дослідження явища перекриття кіберзагроз при застосуванні спільних методів до різних елементів кіберфізичної системи. Проведення дослідження методів кіберзахисту передбачало аналіз взаємозв'язків спільних та унікальних кіберзагроз безпеки для корпоративної та сенсорної мереж в умовах виконання задач лабораторних випробувань (рис. 1). Описані в роботі [10] кіберзагрози для сенсорної мережі та описані в роботі [11] кіберзагрози для корпоративної мережі розглядались у контексті проведення автоматизованих лабораторних випробувань.

Спільні кіберзагрози для сенсорних та корпоративних мереж:

1) таки на шлюзи передбачають атаки на вузли, що з'єднують сенсорну мережу датчиків та актуаторів з корпоративною мережею лабораторії;

2) кіберзагрози інсайдерських атак передбачають як фізичну модифікацію вузла сенсорної мережі чи його прошивки, так і компрометацію даних чи програмного забезпечення в лабораторії співробітниками цієї лабораторії;

3) кіберзагрози програмному забезпеченню можуть бути реалізовані за рахунок шкідливого програмного забезпечення чи атак на вже встановлене як на рівні граничних обчислень лабораторних датчиків та актуаторів чи іншого випробувального обладнання, так і на рівні обробки чи збереження результатів випробувань на сервері чи робочих станціях лабораторної корпоративної мережі;

4) кіберзагрози цілісності та конфіденційності даних передбачають підміну чи викрадення даних, які надходять від датчиків під час випробувань, так і даних, які зберігаються чи оброблюються в базі даних чи на робочих станціях;

ISSN 2219-9365

5) кіберзагрози інфраструктурі є спільними і полягають у виведенні з ладу лабораторного обладнання в сенсорній мережі або серверного обладнання чи робочих станцій опрацювання результатів випробувань.

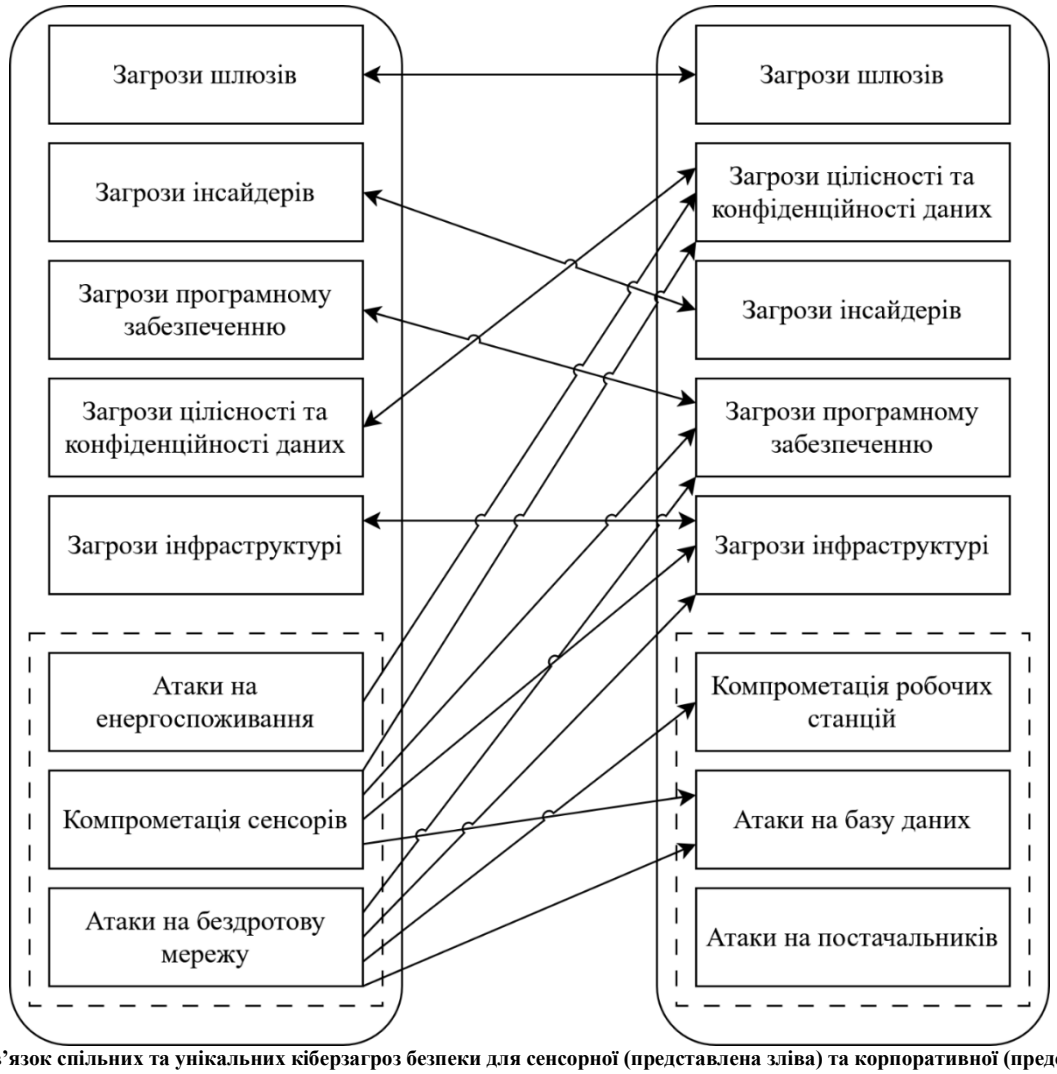

Рис. 1 Зв'язок спільних та унікальних кіберзагроз безпеки для сенсорної (представлена зліва) та корпоративної (представлена справа) мереж в умовах виконання лабораторних випробувань

Атаки характерні сенсорним мережам лабораторних випробувань:

1) атаки на енергоспоживання полягають у виснаженні акумуляторної батареї сенсорів чи лабораторного обладнання з подальшою відмовою проведення лабораторних випробувань, що може нанести шкоду цілісності даних випробувань при передачі цих даних у корпоративну мережу для подальшої обробки;

2) компрометація сенсорів включає захоплення або підміну лабораторного датчика з метою отримання доступу до корпоративної мережі лабораторії, що може вплинути на кіберзагрозу передачі недостовірних чи пошкоджених даних випробувань, дозволяє провести атаку на спеціалізоване програмне забезпечення корпоративної мережі щодо обробки результатів лабораторних випробувань, надає можливість зловмиснику отримати доступ до облікових записів користувачів чи до бази даних, де зберігаються дані про випробування;

3) кіберзагроза атак на бездротову мережу датчиків відкриває доступ до внутрішньої корпоративної мережі лабораторії та несе кіберзагрозу спеціалізованому лабораторному програмному забезпеченню та програмному забезпеченню загального призначення корпоративної мережі, підвищує імовірність вторгнень у робочі станції, дозволяє виконувати запити до бази даних корпоративної мережі лабораторії та несе кіберзагрозу інфраструктурним елементам, оскільки сенсорна мережа науково-дослідної випробувальної лабораторії є бездротовою в той час, як корпоративна мережа Intranet може не використовувати бездротові з'єднання.

Атаки характерні корпоративним мережам лабораторії:

1) компрометація робочих станцій передбачає викрадення облікових записів чи підміну інформації, яка оброблюється працівниками лабораторії в межах робочої станції;

2) атаки на базу даних передбачають застосування ін'єкцій шкідливого програмного коду для отримання прав адміністратора, або внесення завідома хибних даних про результати випробувань;

3) атаки на постачальників .можуть включати атаки на постачальників програмного забезпечення чи послуг обслуговування офісного обладнання.

На основі проаналізованих кіберзагроз було проведено дослідження підходів та методів кіберзахисту від усіх потенційних кіберзагроз сенсорної IoT системи лабораторних випробувань та корпоративної мережі лабораторії з огляду їх переваг і недоліків та можливості інтеграції. Вибір методів ґрунтувався на сукупності сучасних методів кіберзахисту кіберфізичних систем, які можливо використовувати в автоматизованій науково-дослідній випробувальній лабораторії.

Кіберзагрози шлюзів – метод (B_1, B_1^*) запропонований в [12] ґрунтується на сегментації мережі та підходить як сенсорним IoT мережам, так і корпоративним. Дозволяє проводити глибокий аналіз ризиків, але залежить від оновлення шаблонів та не враховує соціальну інженерію.

Кіберзагрози інсайдерським атакам – метод (B_2, B_2^*) запропонований в [13] дозволяє виявляти кіберзагрози інсайдерів в режимі реального часу. Його перевагою є низьке навантаження на обчислювальні ресурси, що дозволяє використовувати підхід і до сенсорної мережі лабораторних випробувань. Недоліком є залежність від якості записів журналу подій. У разі компрометації журналу подій через зовнішній доступ до бездротової сенсорної мережі ускладнюється подальше виявлення інсайдерських атак.

Кіберзагрози програмному забезпеченню – метод (B_3, B_3^*) запропонований в [14] ґрунтується на механізмах виявлення та запобігання вразливостей і не висуває жорстких вимог до продуктивності. До недоліків слід віднести обмежену адаптивність та обмежену кількість типів атак, які враховуються.

Кіберзагрози цілісності і конфіденційності даних – метод (B_4, B_4^*) запропонований в [15] оснований на криптографічному кіберзахисті інформації. До переваг використання підходу в сенсорній та корпоративній мережі лабораторних випробувань можна віднести полегшене навантаження на обчислювальні ресурси та високу ефективність в порівнянні з аналогічними рішеннями. Недоліком є складність масштабування мережі, що може ускладнити розширення мережі при розширенні сфери акредитації лабораторії або при зміні обладнання.

Кіберзагрози інфраструктурі – метод (B_5, B_5^*) запропонований в [16] ґрунтується на використанні системи виявлення вторгнень, яка функціонує за рахунок поєднання сигнатурного і аномального підходів та надає функціонал для гнучкої адаптації та масштабованості, що робить метод ефективним у поєднанні з іншими методами кіберзахисту лабораторних сенсорної і корпоративної мережі. Недоліком є потреба в навчанні моделей, що може стати потенційною уразливістю особливо на початкових етапах впровадження.

Атаки на енергоспоживання – метод (B_6) запропонований в [17] дозволяє за рахунок використання блокчейн технології дозволяє кіберзахистити пристрої IoT від атаки на виснаження енергії. Недоліком роботи є складність реалізації блокчейн у лабораторних сенсорах з обмеженою пам'яттю та відсутністю врахування атак мережевого рівня.

Компрометація сенсорів – метод (B_7) запропонований в [18] функціонує на базі машинного навчання та дозволяє прогнозувати значення датчиків, які отримані з мережевих пакетів Недоліком можна вважати низьку ефективність у випадку обізнаності зловмисника щодо кодування даних, які передаються.

Атаки на бездротову мережу – метод (B_8) запропонований в [19] ґрунтується на генетичному алгоритмі та характеризується гнучкістю і можливістю ефективної взаємодії з іншими методами, що важливо в умовах використання кіберфізичної системи лабораторних випробувань. Недоліком є висока обчислювальна складність, що може вплинути на виникнення затримок в роботі вузлів мережі, від яких залежить зниження точності лабораторних вимірювань в процесі випробувань.

Компрометація робочих станцій – метод (B_6^*) запропонований в [20] ґрунтується на принципі найменших привілеїв та надає можливість для масштабування з метою врахування особливостей різних випробувальних лабораторій. Недоліком можна вважати високі вимоги до базових характеристик інформаційної інфраструктури лабораторії для впровадження методу.

Атаки на базу даних – окрім вбудованих засобів існує потреба забезпечення кіберзахисту від атак можливих при використанні корпоративної мережі у випробувальних лабораторіях. У роботі [21] представлено метод (B_7^*) кіберзахисту від SQL-ін'єкцій на основі підходу глибинного навчання нейромережі. Перевагою є висока точність виявлення атак. До недоліків можна віднести можливі труднощі інтерпретації, що пов'язано із складністю навчання нейромережі в умовах постійних запитів до бази даних в процесі лабораторних випробувань.

Атаки на постачальників – у роботі [22] аналізується підхід нульової довіри (B_8^*). Відповідно до результатів аналізу, методи, основані на підході нульової довіри дозволяють мінімізувати шкоду у випадку успішної атаки, що вкрай важливо в процесі лабораторних випробувань у зв'язку з високою вартістю обладнання та об'єкта випробувань. Такі методи дозволяють виявити аномалії в поведінці, спричинені атаками на ланцюги поставок. До недоліків слід віднести складність та високу вартість впровадження, а також можливі труднощі для взаємодії із замовниками лабораторних випробувань.

Проаналізовані методи можуть бути використані в рамках забезпечення кіберзахисту корпоративної мережі та сенсорної мережі лабораторії. Важливою задачею при цьому є визначення ефективності методів забезпечення кіберзахисту корпоративної мережі при взаємодії з пристроями IoT.

У роботі [23] представлено методику аналізу та оцінки захищеності систем кіберзахисту інформації, що дозволяє врахувати ефект перекриття кіберзагроз. Необхідною умовою оцінки ефективності забезпечення кіберзахисту корпоративної мережі проаналізованими методами кіберзахисту за умов її взаємодії з пристроями IoT є врахування конвергенції фізичної та інформаційної безпеки через вплив кіберзагроз, характерних сенсорній мережі на кіберзагрози корпоративної мережі лабораторії.

На рисунку 2 представлена принципова модель впливу кіберзагроз на області кіберзахисту корпоративної мережі з урахуванням перекриття кіберзагроз і конвергенції фізичного та цифрового середовища.

Перекриття кіберзагроз передбачає проходження через два бар'єри кіберзахисту для спільних кіберзагроз корпоративній та сенсорній мережам: кіберзагроз шлюзів (U_1); кіберзагроз інсайдерів (U_2); кіберзагроз програмному забезпеченню (U_3); кіберзагроз цілісності і конфіденційності даних (U_4) і кіберзагроз інфраструктурі (U_5). Конвергенція фізичного та цифрового середовища зумовлює вплив характерних сенсорним мережам кіберзагроз: атак на енергоспоживання (U_{11}); компрометації сенсорів (U_{12}); атак на бездротову мережу (U_{13}) на кіберзагрози корпоративній сенсорній мережі з урахуванням характерних саме такій мережі кіберзагроз: компрометації робочих станцій (U_{21}); атак на базу даних (U_{22}) та атак на постачальників (U_{23}). Такий вплив відбувається саме при взаємодії областей кіберзахисту корпоративної мережі з областями кіберзахисту пристроїв IoT сенсорної мережі.

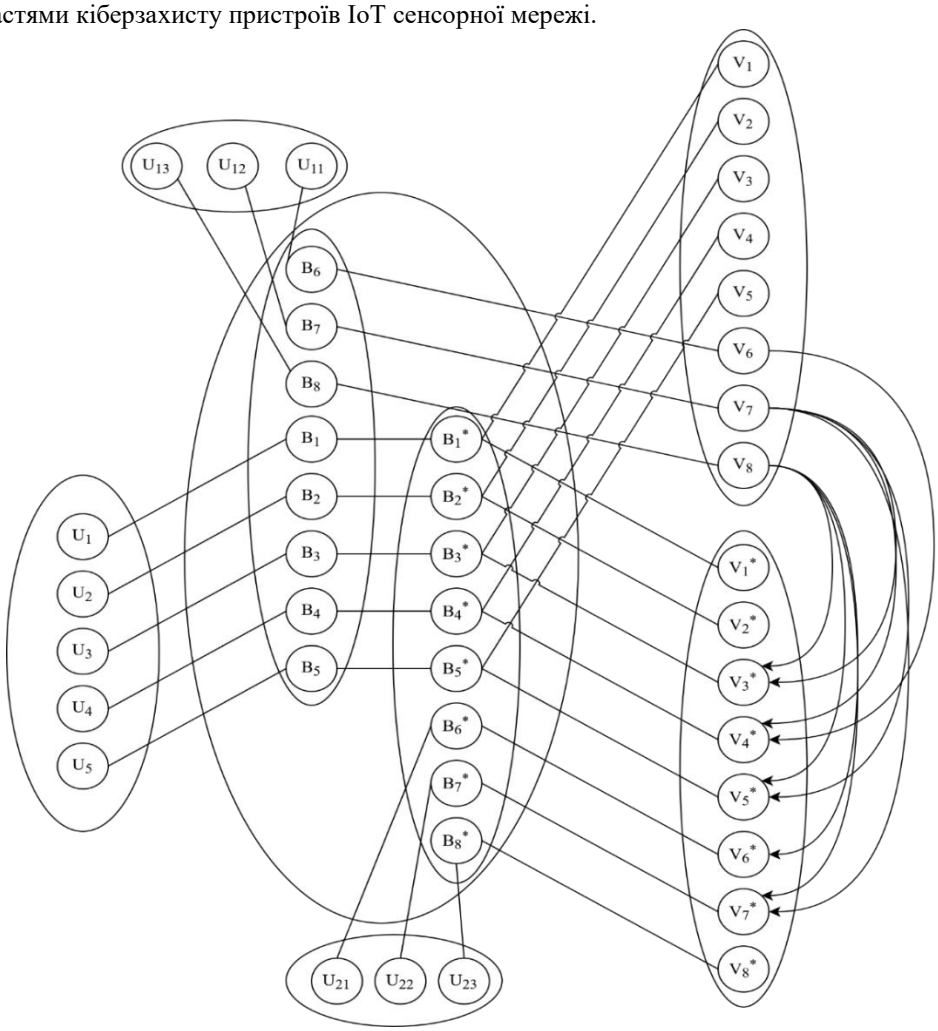

Рис.2. Принципова модель впливу кіберзагроз на області кіберзахисту корпоративної мережі з урахуванням перекриття кіберзагроз і конвергенції фізичного та цифрового середовища

Об'єктами впливу кіберзагроз є області кіберзахисту сенсорної та корпоративної мереж. Для сенсорної мережі: програмне забезпечення шлюзу і мережеві інтерфейси (V_1); датчики та актуатори, конфігурація мережі (V_2); прошивка сенсорів (V_3); дані, які передаються між датчиками та актуаторами, пам'ять сенсорів (V_4); точки доступу, системи охолодження для лабораторного обладнання (V_5); сенсори із

живленням батарейного типу, мобільні вузли (V_6); датчики та ауктатори (V_7); протоколи передачі даних, канали зв'язку (V_8). Для корпоративної мережі: маршрутизатор лабораторії (V_1^*); дані попередніх лабораторних досліджень, дані поточних вимірювань, які надходять від датчиків (V_2^*); сервери, бази даних (V_3^*); офісне та спеціалізоване випробувальне програмне забезпечення (V_4^*); сервери, робочі станції (V_5^*); дані та програмне забезпечення робочих станцій (V_6^*); сервери, бази даних (V_7^*); програмне забезпечення, офісне обладнання (V_8^*).

На рисунку 2 символами B_1-B_8 позначено методи кіберзахисту сенсорних мереж, символами B_1^*- B_8^* – методи кіберзахисту корпоративних мереж.

Аналіз та оцінка захищеності корпоративної на основі використання принципової моделі впливу кіберзагроз на області кіберзахисту корпоративної мережі з урахуванням перекриття кіберзагроз і конвергенції фізичного та цифрового середовища надала можливість оцінити захищеність корпоративної мережі з урахуванням перекриття кіберзагроз. Вплив кіберзагроз на об'єкти області кіберзахисту корпоративної мережі без урахування явища конвергенції фізичної та інформаційної безпеки двох мереж зображено на рисунку 3.

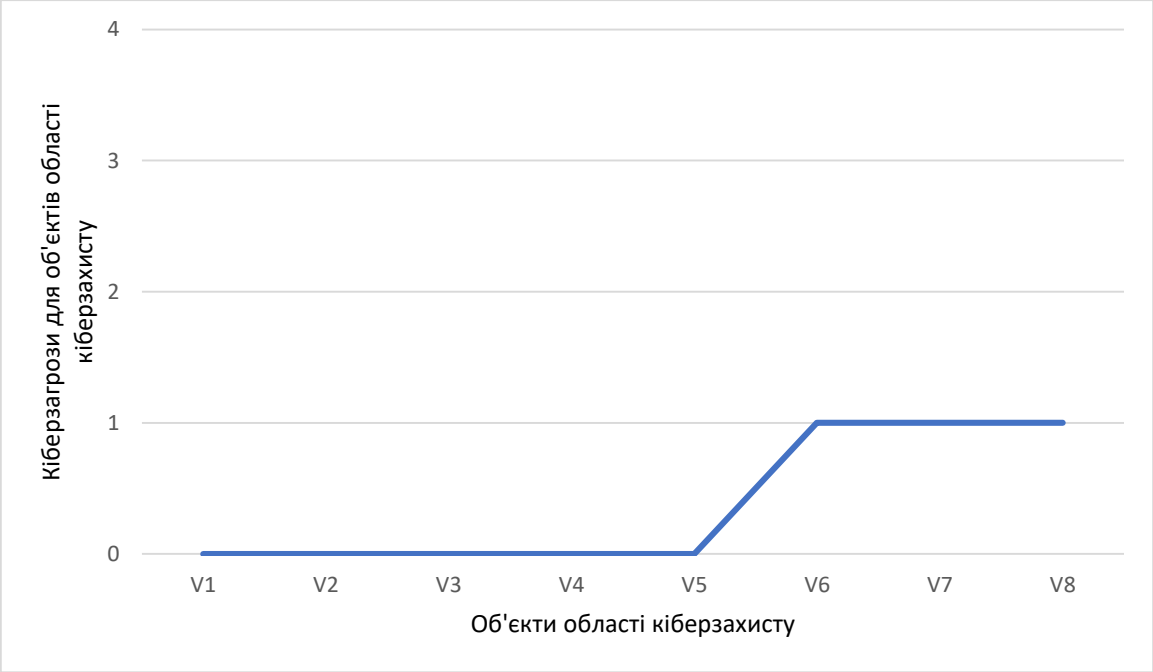

Рис.3. Графік впливу кіберзагроз на об'єкти області кіберзахисту з урахуванням перекриття кіберзагроз

Аналіз впливу кіберзагроз на об'єкти області кіберзахисту корпоративної мережі доводить підвищену ефективність використання методів кіберзахисту для об'єктів області кіберзахисту від 1 по 5. Така ситуація спричинена явищем перекриття кіберзагроз.

При взаємодії корпоративної мережі науково-дослідної лабораторії з пристроями IoT потребує уваги дослідження впливу кіберзагроз на об'єкти області кіберзахисту корпоративної мережі з урахуванням конвергенції фізичного та цифрового середовища (рис. 4).

Як видно з графіку, ефективність використання методів кіберзахисту для об'єктів 3-7 області кіберзахисту корпоративної мережі знижується через явище конвергенції фізичного та цифрового середовища. Ефективність методів кіберзахисту B_3-B_7 та B_3^*- B_7^* знижена за через явище конвергенції навіть за умови перекриття кіберзагроз, що вимагає подальшого пошуку шляхів удосконалення цих методів, розробки нових та розвитку механізмів їх інтеграції у кіберфізичну систему лабораторних випробувань.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

У роботі було проведено аналіз ефективності сучасних методів кіберзахисту корпоративної та сенсорної мережі на основі методики аналізу та оцінки захищеності систем кіберзахисту інформації з урахуванням перекриття кіберзагроз і конвергенції фізичного та цифрового середовища шляхом оцінювання впливу кіберзагроз на об'єкти області кіберзахисту корпоративної мережі, що надало можливість визначити методи, які функціонують зі зниженою ефективністю при забезпеченні кіберзахисту корпоративної мережі, яка взаємодіє з пристроями IoT у кіберфізичній системі лабораторних випробувань.

Було досліджено зв'язок спільних та унікальних кіберзагроз безпеки для сенсорної та корпоративної мереж в умовах виконання лабораторних випробувань.

Сформовано принципову модель впливу кіберзагроз на області кіберзахисту корпоративної мережі з урахуванням перекриття кіберзагроз і конвергенції фізичного та цифрового середовища.

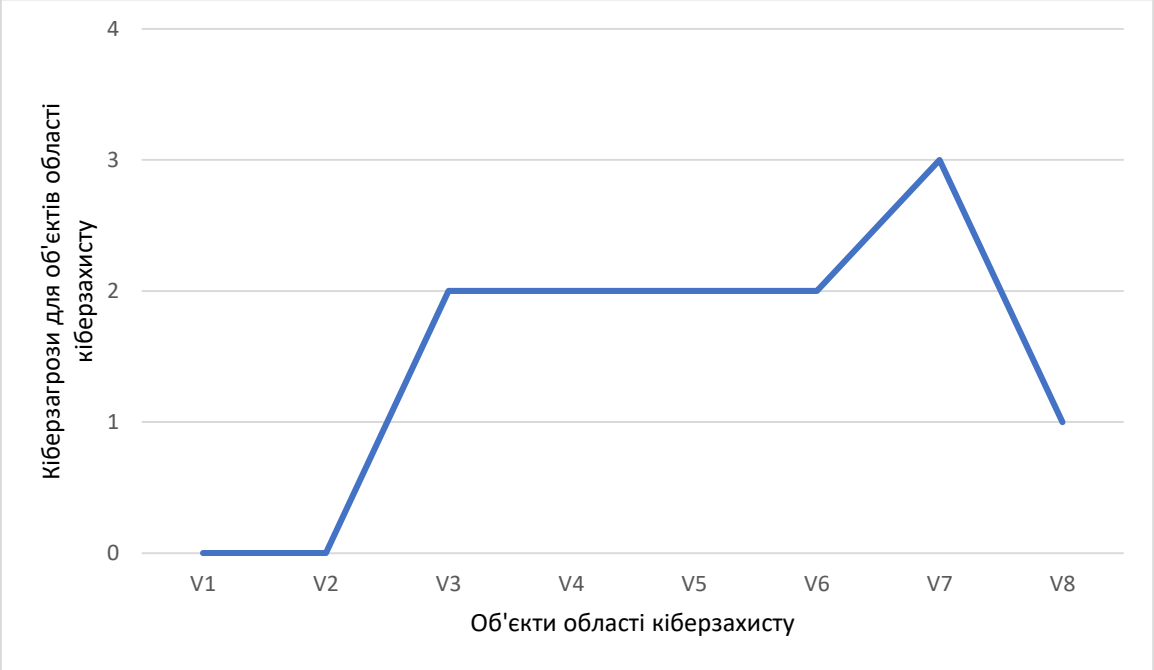

Рис.4. Графік впливу кіберзагроз на об'єкти області кіберзахисту з урахуванням перекриття кіберзагроз і конвергенції фізичного та цифрового середовища

Досліджено вплив кіберзагроз на об'єкти області кіберзахисту корпоративної мережі з урахуванням перекриття кіберзагроз і конвергенції фізичного та цифрового середовища, що дало змогу виявити знижену ефективність 5 методів кіберзахисту від кіберзагроз: програмному забезпеченню, цілісності та конфіденційності даних, інфраструктурі, компрометації робочих станцій та базі даних.

Теоретичне значення полягає у визначенні переліку методів, які потребують подальшого розвитку для забезпечення кіберзахисту корпоративних мереж в умовах взаємодії із пристроями IoT та утворенні кіберфізичної системи лабораторних випробувань.

Практичне значення отриманих у роботі результатів полягає у застосуванні переліку об'єктів області кіберзахисту корпоративної мережі для впровадження додаткових методів кіберзахисту чи модифікації моделі та стратегії при забезпеченні кіберзахисту корпоративних мереж, які взаємодіють з пристроями IoT в лабораторних випробуваннях.

Подальших досліджень потребує формалізація процесу оцінювання ефективності кожного окремого методу при інтеграції у кіберфізичну систему лабораторних випробувань для забезпечення кіберзахисту корпоративної мережі лабораторії.

Література

1. Bedratyuk, O., Yemelyanenko, S., Marych, V., Petrovskyi, V., & Rudyk, Y. (2022). НОВІ ПЕРСПЕКТИВИ ДЛЯ РОБОТИ ДОСЛІДНО-ВИПРОБУВАЛЬНИХ ЛАБОРАТОРІЙ. *Вісник Львівського державного університету безпеки життєдіяльності*, *26*, 55-66. https://doi.org/https://doi.org/10.32447/20784643.26.2022.07

2. S. Viswanadh Kandala et al., (2025,). Engineering End-to-End Remote Labs Using IoT-Based Retrofitting," in IEEE Access, vol. 13, pp. 1106-1132, doi: 10.1109/ACCESS.2024.3523066.

3. Li, K., Cui, Y., Li, W., Lv, T., Yuan, X., Li, S., ... & Dressler, F. (2022). When internet of things meets metaverse: Convergence of physical and cyber worlds. *IEEE Internet of Things Journal*, *10*(5), 4148-4173.

4. Yuriy Zacchia Lun, Alessandro D'Innocenzo, Francesco Smarra, Ivano Malavolta, Maria Domenica Di Benedetto, (2019) State of the art of cyber-physical systems security: An automatic control perspective, Journal of Systems and Software, Volume 149, Pages 174-216, ISSN 0164-1212, https://doi.org/10.1016/j.jss.2018.12.006.

5. 5. D. Tiwari et al (2023) Lightweight encryption for privacy protection of data transmission in cyber physical systems /. *Cluster Computing*. Vol. 26. P. 2351-2365. URL: https://doi.org/10.1007/s10586-022-03790-1.

6. Rathore H., Mohamed A., Guizani M. (2020) A survey of blockchain enabled cyber-physical systems. *Sensors*. Vol. 20, Issue 1. URL: https://doi.org/10.3390/s20010282

7. Kasoju A. (2024) AI-driven anomaly detection in Cyber-Physical systems: a technical approach to real-time threat mitigation. *Iconic Research and Engineering Journals*. Vol. 8, Issue 4. P. 804-817.

8. Ning X., Jiang J. (2022.) Defence-in-depth against insider attack in cyber-physical systems. *Internet of Things and Cyber-Physical Systems*. Vol. 2. P. 203-211. URL: https://doi.org/10.1016/j.iotcps.2022.12.001

9. Дудикевич В., Б. та ін. (2024) Методологія безпеки кіберфізичних систем та Інтернету речей в інтелектуалізації об'єктів інфраструктури. *Комп'ютерні системи та мережі*. Вип. 6, № 1. С. 44-53. URL: https://doi.org/10.23939/csn2024.01.044

10. Коваленко, О., Є. (2023) Моделі безпеки Інтернету речей. *Математичні машини і системи*. № 4. С. 43-50. URL: https://doi.org/10.34121/1028-9763-2023-4-43-50

11. Крючкова Л., П., Ємельяненко М.О. (2024) Кіберзахист WEB-ресурсу Intranet від зовнішніх і внутрішніх кіберзагроз. *Кібербезпека: освіта, наука, техніка*. № 3 (23). С. 318-327. URL: https://doi.org/10.28925/2663-4023.2024.23.318327

12. Alabbad M., Mhaskar N., Khedri R. (2024) Hardening of network segmentation using automated referential penetration testing. *Journal of Network and Computer Applications*. Vol. 224. URL: https://doi.org/10.1016/j.jnca.2024.103851

13. Ali A., Husain M., Hans P. (2025) Real-time detection of insider threats using behavioral analytics and deep evidential clustering. *ArXiv*. URL: https://doi.org/10.48550/arXiv.2505.15383

14. Le-Thanh P., Le-Anh T., Le-Thung Q. (2023) Research and development of a smart solution for runtime web application self-protection. *Information and communication technology* : proceedings of the 12th International Symposium, Ho Chi Minh, Vietnam, 7-8 December / Association for Computing Machinery, New York : 2023. P. 304-311. URL: https://doi.org/10.1145/3628797.3628901

15. K. Wang et al. (2024) Lightweight identity-based network coding scheme for Internet of medical things / *Electronics*. Vol. 13, Issue 7. URL: https://doi.org/10.3390/electronics13071316

16. Alharbi S. Khan A. (2024) Ensemble defence system: a hybrid ADS approach for effective cyber threat detection. *ArXiv*. URL: https://doi.org/10.48550/arXiv.2401.03491

17. A. Alsirhani et al. (2023) Securing low-power blockchain-enabled IoT devices against energy depletion attack. *ACM Transactions on Internet Technology*. Vol. 23, Issue 3. № 43. P. 1-17. URL: https://doi.org/10.1145/3511903

18. Y. Chen et al. (2005) Active Fuzzing for testing and securing cyber-physical systems. *ArXiv*. URL: https://doi.org/10.48550/arXiv.2005.14124

19. Singh A., Dr. Singh D. (2023) Genetic algorithm-based secure routing protocol for wireless sensor networks. *International Research Journal on Advanced Engineering Hub*. Vol. 1, № 1. P. 46-52. URL: https://doi.org/10.47392/IRJAEH.2023.007

20. Plachkinova M., Knapp K. (2023.) Least privilege across people, process and technology: endpoint security framework. *Journal of Computer Information Systems*. Vol. 63, Issue 5. P. 1153-1165. URL: https://doi.org/10.1080/08874417.2022.2128937

21. Liu Y., Dai Y. (2024) Deep learning in cybersecurity: a hybrid BERT-LSTM network for SQL injection attack detection. *IET Information Security*. Vol. 2024. URL: https://doi.org/10.1049/2024/5565950

22. Ghasemshirazi S., Shirvani G., Alipour M.A. (2023) Zero trust: applications, challenges and opportunities. *ArXiv*. URL: https://doi.org/10.48550/arXiv.2309.03582

23. Пепа Ю., В. (2024) Методика аналізу та оцінки захищеності систем кіберзахисту інформації з урахуванням ступеня перекриття кіберзагроз / та ін. *Сучасний кіберзахист інформації*. № 1. С. 69-76. URL: https://doi.org/10.31673/2409-7292.2024.010008

References

1. Bedratyuk, O., Yemelyanenko, S., Marych, V., Petrovskyi, V., & Rudyk, Y. (2022). NEW PERSPECTIVES FOR THE WORK OF RESEARCH AND TESTING LABORATORIES. Bulletin of the Lviv State University of Life Safety, 26, 55-66. https://doi.org/https://doi.org/10.32447/20784643.26.2022.07

2. S. Viswanadh Kandala et al., (2025,). Engineering End-to-End Remote Labs Using IoT-Based Retrofitting," in IEEE Access, vol. 13, pp. 1106-1132, doi: 10.1109/ACCESS.2024.3523066.

3. Li, K., Cui, Y., Li, W., Lv, T., Yuan, X., Li, S., ... & Dressler, F. (2022). When internet of things meets metaverse: Convergence of physical and cyber worlds. IEEE Internet of Things Journal, 10(5), 4148-4173.

4. Yuriy Zacchia Lun, Alessandro D'Innocenzo, Francesco Smarra, Ivano Malavolta, Maria Domenica Di Benedetto, (2019) State of the art of cyber-physical systems security: An automatic control perspective, Journal of Systems and Software, Volume 149, Pages 174-216, ISSN 0164-1212, https://doi.org/10.1016/j.jss.2018.12.006.

5. 5. D. Tiwari et al (2023) Lightweight encryption for privacy protection of data transmission in cyber physical systems /. Cluster Computing. Vol. 26. P. 2351-2365. URL: https://doi.org/10.1007/s10586-022-03790-1.

6. Rathore H., Mohamed A., Guizani M. (2020) A survey of blockchain enabled cyber-physical systems. Sensors. Vol. 20, Issue 1. URL: https://doi.org/10.3390/s20010282

7. Kasoju A. (2024) AI-driven anomaly detection in Cyber-Physical systems: a technical approach to real-time threat mitigation. Iconic Research and Engineering Journals. Vol. 8, Issue 4. P. 804-817.

8. Ning X., Jiang J. (2022.) Defence-in-depth against insider attack in cyber-physical systems. Internet of Things and Cyber-Physical Systems. Vol. 2. P. 203-211. URL: https://doi.org/10.1016/j.iotcps.2022.12.001

9. Dudykevych V., B. et al. (2024) Methodology of security of cyber-physical systems and the Internet of Things in the intellectualization of infrastructure objects. Computer systems and networks. Vol. 6, No. 1. P. 44-53. URL: https://doi.org/10.23939/csn2024.01.044

10. Kovalenko, O., E. (2023) Security models of the Internet of Things. Mathematical machines and systems. No. 4. P. 43-50. URL: https://doi.org/10.34121/1028-9763-2023-4-43-50

11. Kryuchkova L., P., Emelyanenko M.O. (2024) Protection of the Intranet WEB resource from external and internal threats. Cybersecurity: education, science, technology. No. 3 (23). P. 318-327. URL: https://doi.org/10.28925/2663-4023.2024.23.318327

12. Alabbad M., Mhaskar N., Khedri R. (2024) Hardening of network segmentation using automated referential penetration testing. Journal of Network and Computer Applications. Vol. 224. URL: https://doi.org/10.1016/j.jnca.2024.103851

13. Ali A., Husain M., Hans P. (2025) Real-time detection of insider threats using behavioral analytics and deep evidential clustering. ArXiv. URL: https://doi.org/10.48550/arXiv.2505.15383

14. Le-Thanh P., Le-Anh T., Le-Thung Q. (2023) Research and development of a smart solution for runtime web application self-protection. Information and communication technology: proceedings of the 12th International Symposium, Ho Chi Minh, Vietnam, December 7-8 / Association for Computing Machinery, New York: 2023. P. 304-311. URL: https://doi.org/10.1145/3628797.3628901

15. K. Wang et al. (2024) Lightweight identity-based network coding scheme for Internet of medical things / Electronics. Vol. 13, Issue 7. URL: https://doi.org/10.3390/electronics13071316

16. Alharbi S. Khan A. (2024) Ensemble defense system: a hybrid ADS approach for effective cyber threat detection. ArXiv. URL: https://doi.org/10.48550/arXiv.2401.03491

17. A. Alsirhani et al. (2023) Securing low-power blockchain-enabled IoT devices against energy depletion attack. ACM Transactions on Internet Technology. Vol. 23, Issue 3. No. 43. P. 1-17. URL: https://doi.org/10.1145/3511903

18. Y. Chen et al. (2005) Active Fuzzing for testing and securing cyber-physical systems. ArXiv. URL: https://doi.org/10.48550/arXiv.2005.14124

19. Singh A., Dr. Singh D. (2023) Genetic algorithm-based secure routing protocol for wireless sensor networks. International Research Journal on Advanced Engineering Hub. Vol. 1, No. 1. P. 46-52. URL: https://doi.org/10.47392/IRJAEH.2023.007

20. Plachkinova M., Knapp K. (2023.) Least privilege across people, process and technology: endpoint security framework. Journal of Computer Information Systems. Vol. 63, Issue 5. P. 1153-1165. URL: https://doi.org/10.1080/08874417.2022.2128937

21. Liu Y., Dai Y. (2024) Deep learning in cybersecurity: a hybrid BERT-LSTM network for SQL injection attack detection. IET Information Security. Vol. 2024. URL: https://doi.org/10.1049/2024/5565950

22. Ghasemshirazi S., Shirvani G., Alipour M.A. (2023) Zero trust: applications, challenges and opportunities. ArXiv. URL: https://doi.org/10.48550/arXiv.2309.03582

23. Pepa Y., V. (2024) Methodology for analyzing and assessing the security of information protection systems taking into account the degree of threat overlap / et al. Modern Information Security. No. 1. P. 69-76. URL: https://doi.org/10.31673/2409-7292.2024.010008