МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ПОЛІСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет інформаційних технологій,
обліку та фінансів
Кафедра комп’ютерних технологій
і моделювання систем

Кваліфікаційна робота
на правах рукопису

Інжиєвського Олександра Олександровича

УДК 004.056.53

КВАЛІФІКАЦІЙНА РОБОТА

Підвищення ефективності методів протидії кібератакам на об'єкти критичної інфраструктури

125 - Кібербезпека

Подається на здобуття освітнього ступеня магістр

кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ Інжиєвський О. О.

Керівник роботи
Веретюк Сергій Михайлович
К.т.н.,старший викладач кафедри
комп’ютерних технологій і моделювання систем

Житомир – 2023

АНОТАЦІЯ

Інжиєвський О.О. Підвищення ефективності методів протидії кібератакам на об'єкти критичної інфраструктури– Кваліфікаційна робота на правах рукопису.

Кваліфікаційна робота на здобуття освітнього ступеня магістр за спеціальністю 125 – кібербезпека. – Поліський національний університет,

Житомир, 2023.

Магістерська робота присвячена дослідженню та підвищенню ефективності методів протидії кібератакам на об'єкти критичної інфраструктури. У роботі ретельно розглянуті основні методи протидії кіберзагрозам, виявлені їхні особливості та проаналізовані результати використання в реальних умовах. Також розглянуто та проаналізовано кіберінценденти на ОКІ України.

Основною частиною роботи є розробка математичної моделі синтезу оптимальної комплексної стратегії протидії кіберзагрозам для об'єктів критичної інфраструктури. В рамках моделі формалізовано поняття ефективності стратегії як співвідношення потенціалу методів, які входять до складу стратегії, вартості та часу реагування цих методів. Запропонована математична модель становить інноваційний підхід до формулювання комплексної стратегії протидії, що може бути застосована для різноманітних сценаріїв та типів кібератак.

Окремою частиною роботи є апробація розробленої моделі, підтверджуючи її ефективність в реальних умовах. Застосування моделі на практиці дозволило отримати переконливі результати щодо покращення рівня кібербезпеки об'єктів критичної інфраструктури. Апробація включала етапи тестування, аналізу та вдосконалення стратегій протидії на основі отриманих даних.

Загальна характеристика: кваліфікаційної роботи, 32 с., 1 табл., 3 рис., 1 дод., 17 джерел.

SUMMARY

Inzhyievskyi O.O. Increasing the effectiveness of methods of counteracting cyber attacks on critical infrastructure - Qualification work on the rights of the manuscript.

Qualification work for the degree of master's degree in specialty 125 - cybersecurity - Polissya National University, Zhytomyr, 2023.

The master's thesis is devoted to the study and improvement of the effectiveness of methods of countering cyberattacks on critical infrastructure. The work thoroughly examines the main methods of countering cyber threats, identifies their features and analyzes the results of their use in real conditions. Cyber incidents at the Ukrainian critical infrastructure are also considered and analyzed.

The main part of the work is the development of a mathematical model for the synthesis of an optimal comprehensive strategy for countering cyber threats to critical infrastructure. The model formalizes the concept of strategy effectiveness as the ratio of the potential of the methods that make up the strategy, the cost and response time of these methods. The proposed mathematical model is an innovative approach to formulating a comprehensive countermeasure strategy that can be applied to various scenarios and types of cyberattacks.

A separate part of the work is the testing of the developed model, confirming its effectiveness in real conditions. Applying the model in practice has provided convincing results in improving the level of cybersecurity of critical infrastructure facilities. The approbation included the stages of testing, analysis and improvement of counteraction strategies based on the data obtained.

General characteristics: qualification work, 32 p., 1 table, 3 figures, 1 appendix, 17 sources.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ 5
ВСТУП 6
Розділ 1. ОГДЯД ІСНУЮЧИХ КІБЕРАТАК НА ОКІ, МЕТОДІВ ЇХ РЕАЛІЗАЦІЇ ТА ПРОТИДІЇ 8
1.1 Кібератаки та джерела їх виникнення 8
1.2 Огляд реалізованих кібератак на ОКІ в Україні 10
1.3 Наслідки кібератак на об'єкти критичної інфраструктури 12
1.4 Методи протидії кібератакам 15
Висновок до 1 розділу 18
2 Розділ. МЕТОДИ ПОКРАЩЕННЯ ЕЛЕМЕНТІВ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ ОКІ 19
2.1 Методи підвищення ефективності методів протидії кібератакам на ОКІ 19
2.2 Розроблення математичної моделі вибору оптимальної стратегії застосування методів протидії кібератакам на ОКІ 20
Висновок до 2 розділу 24
Розділ 3 25
3.1 Визначення оптимальних значень параметрів стратегії протидії кіберзагрозі 25
3.2 Приклад застосування запропонованої моделі 26
Висновок до 3 розділу 28
ВИСНОВКИ 29
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 30
ДОДАТКИ .....

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАЧЕННЯ

КССД – Комплексна система санкціонованого доступу

ІКС – Інформаційно-комунікаційна система

ІзОД – Інформація з обмеженим доступом

ОІД – Об’єкт інформаційної діяльності.

СКУД – систем контролю та управління доступом

СУІБ – систем управління інформаційною безпекою

КСЗІ – комплексних систем захисту інформації

АС – автоматизована система

КТіМС – комп’ютерні технології і моделювання систем

ТЗ – технічні засоби

ОТЗ – основні технічні засоби

ІС – інформаційні системи

СВВ – системи виявлення вторгнень

СЗВ – системи запобігання вторгненням

ПІБ – політика інформаційної безпеки

КСЗІ – комплексна система захисту інформації

ОКІ – об'єкт критичної інфраструктури

ICS – industrial control systems

ВСТУП

Актуальність роботи Актуальність підвищення ефективності методів протидії кібератакам на об'єкти критичної інфраструктури надзвичайно висока в сучасних умовах, оскільки ці об'єкти відіграють ключову роль у забезпеченні стабільності суспільства. Зростання кількості та складності кіберзагроз, а також зміни в технологічному середовищі роблять необхідним постійне вдосконалення заходів з захисту від кібератак. Пошкодження чи втрата доступу до критичної інфраструктури може мати серйозні наслідки для економіки, безпеки та соціального благополуччя. Таким чином, розвиток та впровадження новітніх методів протидії кіберзагрозам є невід'ємною складовою стратегії забезпечення кібербезпеки об'єктів критичної інфраструктури.

Мета роботи – розробити оптимальну за критерієм ефективності стратегію застосування комплексу заходів (методів) протидії для удосконалення комплексу заходів з завчасного реагування на кіберзагрози для ОКІ.

Завдання:

- Аналіз та дослідження кібератак на ОКІ.
- Аналіз методів протидії.
- Розроблення математичної моделі синтезу оптимальної за критерієм ефективності стратегії для протидії адаптивним кіберзагрозам.
- Проведення валідації і апробації розробленої моделі.

Об’єкт дослідження - процес протидії кібератакам на системи безпеки ОКІ.

Предмет дослідження - ефективність застосування методів протидії кібератакам на об'єкти критичної інфраструктури.

Методи дослідження: аналіз наукової літератури, аналіз звітів з кіберінциндентів, аналіз регламентів та стандартів кібербезпеки, системний аналіз, математичний аналіз, теорія прийняття рішень.

Наукова новизна: розроблено математичну модель синтезу оптимальної за критерієм ефективності стратегії як розв’язку задачі мінімізації методом Лагранжа потенційних втрат від кібератаки за умови апріорної інформації щодо обмежень на витрати, час реагування та здатності протидіяти кібератаці, що дає можливість

розробляти адаптивні підходи до реагування на кіберзагрози.

Перелік публікацій за темою дослідження:

1. Інжиєвський О. О., Веретюк С. М. Роль людського фактору у підвищенні ефективності заходів протидії кібератакам на об'єкти критичної інфраструктури. *Пріоритетні шляхи розвитку науки і освіти* : Міжнар. науково-практ. конф., м. Львів, 29–30 листоп. 2023 р. Львів, 2023. С. 44.
2. Інжиєвський О. О., Веретюк С. М. Роль інноваційних технологій у вдосконаленні заходів протидії кібератакам на об’єкти критичної інфраструктури. *Пріоритетні напрями досліджень в науковій та освітній діяльності:* : Міжнар. науково-практ. конф., м. Львів, 19–20 грудня. 2023 р. Львів, 2023. С 76.
3. Інжиєвський О. О., Веретюк С. М. Методи підвищення захисту об’єктів критичної інфраструктури від кібератак. *Безпека, Технології, Інновації: нові горизонти* : Міжфакультет. науково-практ. інтернет-конф., м. Житомир, 15 листоп. 2023 р. Житомир, 2023.

РОЗДІЛ 1. ОГДЯД ІСНУЮЧИХ КІБЕРАТАК НА ОКІ, МЕТОДІВ ЇХ РЕАЛІЗАЦІЇ ТА ПРОТИДІЇ

1.1 Кібератаки та джерела їх виникнення

Кібербезпека об’єктів критичної інфраструктури далі: «ОКІ» стає дедалі важливішою у зв'язку зі зростанням кількості та складності кіберзагроз. Ці атаки не лише ставлять під загрозу функціонування об'єктів критичної інфраструктури, таких як енергетичні системи, транспортні мережі та комунікаційні інфраструктури, але й можуть мати серйозні наслідки для економічної та соціальної стабільності. Далі наведемо перелік розповсюджених кібератак:

Фішинг та соціальна інженерія: Фішинг представляє собою форму обману, призначену для витягування особистої інформації від довірливих або необачних користувачів мережі. Основна мета шахраїв полягає в тому, щоб отримати особисті дані клієнтів. Шахраї намагаються змусити користувачів самостійно надати конфіденційну інформацію, наприклад, шляхом надсилання електронних листів із запитаннями підтвердження реєстрації облікового запису. Ці листи містять посилання на веб-сайти, зовнішній вигляд яких повністю копіює дизайн відомих ресурсів.[1]

Фішінг включає в себе використання психологічних та технічних методів для отримання конфіденційної інформації. Спам-повідомлення, які легко можуть виглядати як офіційні листи від інших співробітників, використовуються для перехоплення облікових даних та отримання доступу до систем.

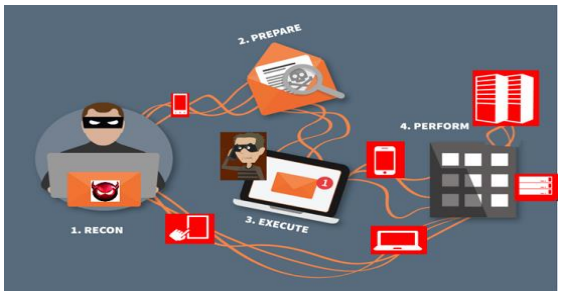

Рисунок 1.1 Ілюстрація механізму фішингової атаки

Соціальна інженерія – це спосіб зламу, в якому використовуються психологічні методи для обману людини.[2]

Шкідливе програмне забезпечення (malware) – це програмне забезпечення заважає нормальному функціонуванню комп'ютера, збирає конфіденційну інформацію або отримує несанкціонований доступ до приватних комп'ютерних систем. Його прояв може бути у вигляді коду, скрипта, активного контенту та іншого програмного забезпечення. Термін "шкідливий" використовується як загальна назва для опису різних форм ворожого або непроханого програмного забезпечення[3].

Атаки за допомогою вірусів, троянів та шкідливого програмного забезпечення стають все більш вдосконаленими. Атакуюча сторона може використовувати ці інструменти для здійснення шпигунства, вимагань викупу або призначення інших зловмисних дій.

DoS та DDoS атаки – це атака на комп'ютерну систему з метою зробити комп'ютерні ресурси недоступними для користувачів, для яких ця система була призначена.[4]

Ці атаки спрямовані на перевантаження мережевих ресурсів об'єкта, призводячи до тимчасової або повної відмови в обслуговуванні. Це може призвести до значних збитків та порушити нормальне функціонування критичної інфраструктури.

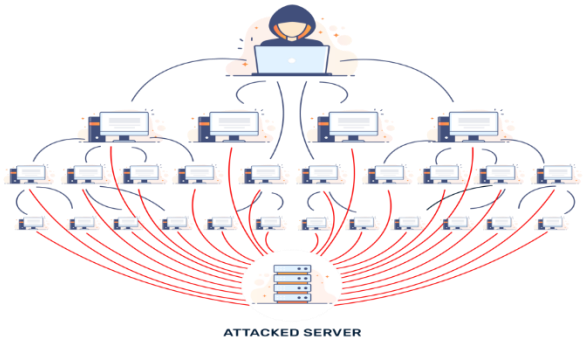

Рисунок 1.2 Ілюстрація DDOS атаки

Експлуатація вразливостей ПЗ: Атаки, спрямовані на використання вразливостей програмного чи апаратного забезпечення, можуть призвести до незаконного доступу та викрадення конфіденційної інформації. Важливо

регулярно оновлювати програмне забезпечення та встановлювати необхідні патчі для усунення потенційних вразливостей.

Віддалені мережеві атаки полягають в негативному впливі на розподілену обчислювальну систему через програмні засоби по зв'язкових каналах. [5].Ці атаки можуть включати в себе маніпулювання маршрутизацією та DNS-атаки з метою перенаправлення трафіку або заблокування доступу до ключових ресурсів.

Фізичні атаки: Такі атаки можуть включати в себе встановлення шкідливих пристроїв або фізичне знищення обладнання.

Компрометація довірених осіб: Атакуюча сторона може намагатися впливати на співробітників чи адміністраторів об'єкта для отримання доступу до конфіденційної інформації або виконання зловмисних дій.

1.2 Огляд реалізованих кібератак на ОКІ в Україні

У грудні 2016 року група хакерів, відома як Sandworm і пов'язана з російським ГРУ, використала програму під назвою Industroyer для виклику відключення електроенергії в Києві. Це призвело до тимчасового відсутності електропостачання в значній частині міста протягом години. Рік до цього, у 2015 році, тим самим методом було вимкнуто електроенергію для 225 000 українців протягом шести годин. У 2022 році з'явилася нова версія програми - Industroyer2. Деякі джерела вказують, що цю програму використали під час третьої атаки на українські електромережі, але вона була виявлена і зупинена, не досягнувши своєї мети.

Industroyer відзначався тим, що відмінно розумів секретні промислові процеси, що використовуються українськими операторами електромереж. Він взаємодіяв з цими системами, щоб викликати вимикання та повторне включення ліній підстанцій. Industroyer мав здатність відсилати команди на вимикачі, використовуючи будь-який з чотирьох промислових протоколів систем управління. Шкідливе програмне забезпечення також включало компонент для вимикання пристроїв безпеки, відомих як захисні реле, які автоматично

припиняють подачу електроенергії при виявленні небезпечних режимів, що можуть призвести до катастрофічних фізичних пошкоджень обладнанню. [8].

Атака на енергосистему України в жовтні 2022р

Інцидент складався з кількох етапів, а не був однією атакою. Група хакерів використовувала нові методи впливу на системи управління енергосистемою (ICS) та операційні технології (OT).

Згідно з проведеним аналізом, вторгнення почалося із проникнення в комп'ютерну систему та її вивчення у червні 2022 року або навіть раніше, і завершилося двома руйнівними подіями 10 і 12 жовтня 2022 року.

Спочатку група Sandworm вимкнула автоматичні вимикачі на підстанції, що спричинило неплановане відключення електроенергії, що збіглося з масовими ракетними ударами по об'єктах критичної інфраструктури по всій території України. Зловмисник використав образ оптичного диска (ISO) для запуску власного виконуваного файлу MicroSCADA, ймовірно, з метою викликати зловмисні команди для вимикання підстанцій. З огляду на часову мітку від 23 вересня, можливо, існував двомісячний проміжок часу від моменту, коли зловмисник отримав початковий доступ до SCADA-системи, до моменту реалізації можливостей OT.

Через два дні відбувся другий етап, коли група розгорнула новий варіант віруса-вайпера CADDYWIPER (призначений для стирання даних) в інформаційно-технічному середовищі компанії-жертви. Ймовірно, метою було викликати додаткові збої та видалити свої сліди. Розгортання віруса-стирача було обмежене інформаційно-технічним середовищем і не вплинуло на гіпервізор або віртуальну машину SCADA. Це було незвичайним, оскільки зловмисник раніше видалив інші "кримінальні артефакти", як їх називають дослідники, з SCADA-системи, можливо, намагаючись «замести сліди», що були б підсилені діяльністю вайпера. Це може вказувати на відсутність координації між різними особами або оперативними підгрупами, які приймали участь у цій атакі.[9].

Кібератака найбільшого оператора зв’язку України “Київстар”

Третій приклад який можна додати відбувся 12 грудня 2023 року. Цього разу під приціл ворожого хакерського угрупування попав оператор мобільного зв’язку “Київстар”.

Понад 12 годин мобільна мережа, сайт та додаток найбільшого в Україні оператора “Київстар” не працювали через хакерську атаку. Станом на 20:00 12 грудня «Київстар» частково відновив роботу послуг фіксованого зв’язку. Остаточно цю роботу планували завершити 13 грудня, але тільки 15 грудня мережа мобільного зв’язку запрацювала без перебоїв.

Оскільки результати офіційного розслідування не опубліковано, проте ймовірно доступ до внутрішньої мережі зловмисником отримано через обліковий запис працівника який має такий високий рівень доступу, або “заражений” вірусом комп'ютер який в свою чергу під'єднаний до корпоративної мережі та має доступ до конфеденційної інформації . Так як зображено на рис. 1.3

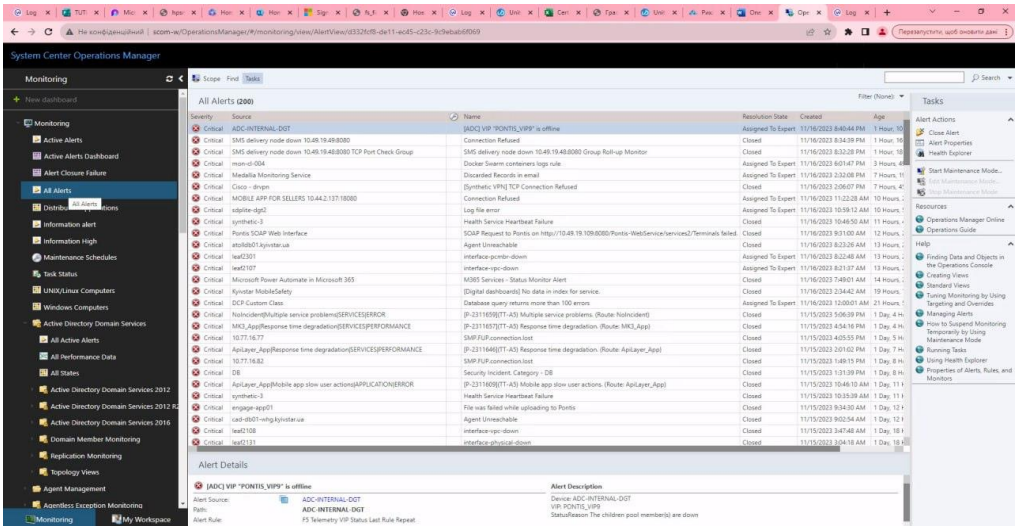

Рисунок 1.3 Скріншот робочої станції зловмисника

1.3 Наслідки кібератак на об'єкти критичної інфраструктури

Під терміном "наслідки" маємо на увазі розмір та характер завданої шкоди під час успішної кібератаки. Для точного визначення цих наслідків необхідно встановити конкретні параметри. Під поняттям "величина наслідків" розуміємо очікувану вартість завданих втрат протягом визначеного періоду часу при певному

виді нападу, який завдав шкоди певному об'єкту. Це може включати, наприклад, кількість постраждалих осіб, пошкодження майна та інше.

Деякі автори [6] вказують, що збитки від кіберзагроз можуть бути визначені у конкретних одиницях, таких як економічні втрати, витрати часу, обсяг втраченої або пошкодженої інформації. Збитки в ОКІ можуть бути розділені на прямі та непрямі.

Прямі збитки включають витрати, пов'язані з заміною активів. Це може відбутися через фізичне пошкодження активу, втрату його цілісності або доступності, порушення точної послідовності чи зміну характеру процесу. Зазначимо, що активи можуть мати низькі прямі збитки в порівнянні з їхньою корисністю, оскільки засіб для їхнього зберігання, як правило, має невисоку вартість. Малі пошкодження людських активів із швидким відновленням можуть мати невеликі прямі збитки для організації, навіть при довгострокових наслідках для постраждалої особи.

Непрямі збитки виникають внаслідок втрати активів і можуть включати в себе витрати на простій, переробці та інші виробничі витрати через втрату активів.

Для фізичних активів, зазвичай, непрямі збитки виникають внаслідок втрати компонентів. Випадкове пошкодження обладнання може призвести до необхідності проведення ремонту, реінжинірингу чи інших заходів для відновлення контролю над промисловим процесом. Одночасно непрямі збитки часто можуть мати значні розміри, включаючи втрату довіри громадськості, втрату ліцензії на діяльність, та втрату конкурентних переваг відносно випуску інтелектуальної власності, такої як конфіденційні процеси та нові технології.

У випадку автоматизованих систем управління технологічними процесами, збитки виникають через порушення конфіденційності, цілісності, доступності та неспростовності інформації у результаті деструктивних дій при реалізації кіберзагроз.

Основні категорії впливу деструктивних дій в автоматизованих системах управління технологічними процесами визначаються як [7]:

1. *Фізичний вплив*: включає в себе безліч прямих наслідків аварій в автоматизованих системах управління технологічними процесами. Найважливіші потенційні наслідки таких подій включають травми та загибель людей. Інші можливі наслідки охоплюють втрату майна (включаючи дані) та потенційні збитки для навколишнього середовища.

2. *Економічні впливи* - це наслідки другого порядку від фізичних впливів, що виникають внаслідок аварій в автоматизованих системах управління технологічними процесами. Фізичний вплив може призвести до наслідків для самої системи, що, в свою чергу, може призвести до більших економічних збитків для підприємства чи організації. На великому рівні ці наслідки можуть негативно вплинути на місцевий, регіональний, національний та, можливо, глобальний рівні економіки.

3. *Екологічний вплив* - це вплив на населення та природне середовище.

4. *Політичний вплив* - це вплив на впевненість та дієздатність влади.

5. *Соціальні впливи* - це наслідки другого порядку, які є виведеними з втрати державної та громадської довіри до організації.

Взаємозв'язок з іншими елементами критичної інфраструктури та тривалість впливу можливо розглядати, враховуючи наведені вище категорії впливу порушення безпеки інформації в автоматизованих системах управління технологічними процесами. Серед наслідків цих впливів можуть бути:

- *Порушення національної безпеки.*
- *Сприяння вчиненню актів тероризму.*
- *Втрата або скорочення виробництва.*
- *Травми або смерть людей.*
- *Пошкодження обладнання.*
- *Викид (витікання, випаровування) або крадіжка небезпечних матеріалів.*
- *Екологічні збитки.*
- *Кримінальні або цивільно-правові зобов'язання.*
- *Втрата приватної або конфіденційної інформації.*
- *Втрата іміджу бренду та довіри клієнтів.*

Слід зауважити, що елементи цього переліку взаємопов'язані, і один наслідок може призвести до іншого. Крім того, на сьогоднішній день визначається перелік інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави, враховуючи негативні наслідки, які можуть виникнути в результаті кібератак на інформаційно-телекомунікаційну систему. Дослідження інформації з відкритих джерел свідчить про збільшення спрямованості кібератак на комп'ютерні мережі енергетичного сектору, дипломатичного корпусу, силових відомств, оборонного комплексу, державних підприємств та медіа компаній. Мета таких кібератак, передусім, полягає в нанесенні шкоди критичній інфраструктурі держави. З урахуванням можливих негативних наслідків кібератак, ефективне функціонування системи кіберзахисту країни залишається пріоритетним завданням, що набуває все більшої актуальності з кожним роком

1.4 Методи протидії кібератакам

Основним засобом захисту інформаційних систем та мереж (ІС) від інформаційно-руйнівних впливів у формі кібернетичних вторгнень є системи виявлення та/або запобігання вторгненням (СВВ/СЗВ). Основна мета цих систем полягає в оперативному виявленні вторгнень, що означає встановлення відповідності між об’єктом та його ідентифікатором (унікальним атрибутом). У ідеальному випадку, ці системи ініціюють ефективні захисні сценарії для припинення порушення конфіденційності, доступності та цілісності інформаційних ресурсів та сервісів. Практика використання СВВ розглядає два основних напрями протидії кібернетичним вторгненням: виявлення зловживань (Misuse detection) та виявлення аномалій (Anomaly detection).

Всі розробники систем виявлення атак і організації, які використовують СВА, повинні бути знайомі з класифікацією цих систем. Це допомагає вибрати найкращі рішення для захисту інформаційних систем. Дослідження різних аспектів таксономії та використання різних варіантів може сприяти досягненню вищого рівня безпеки інформаційних систем. [10, 11].

Виявлення вторгнень активно вивчається протягом кількох десятиліть, і існує значна різноманітність методів та підходів для виявлення віддалених мережевих атак. Для захисту інформаційної системи використовують різні поширені засоби та методи, такі як встановлення політики безпеки корпоративної мережі, використання міжмережевих екранів, захист на рівні маршрутизаторів, проведення мережевого аудиту, використання систем виявлення вторгнень та розробка регламенту реагування на виявлені атаки.

Сьогодні для захисту інформації необхідно не лише розробляти індивідуальні механізми безпеки, але і впроваджувати системний підхід, який включає в себе комплекс взаємопов'язаних заходів. Основною метою будь-якої системи інформаційної безпеки є створення умов для ефективного функціонування підприємства, уникнення кіберзагроз його безпеки, захист законних інтересів підприємства від незаконних вторгнень, запобігання крадіжці фінансових ресурсів, уникнення розголошення, втрат, витоку, спотворення та знищення службової інформації, забезпечуючи це в межах діяльності установи.[12]

Забезпечення кібербезпеки об'єктів критичної інфраструктури включає в себе ряд стратегій та методів. Мережева безпека є ключовим елементом, забезпечуючи виявлення та блокування небажаних мережевих активностей. Використання фаєрволів і систем виявлення вторгнень сприяє контролю трафіку та обмеженню доступу.

Шифрування даних грає важливу роль у забезпеченні конфіденційності та цілісності інформації. Це ефективний захист від несанкціонованого доступу, хоча може створити додаткове навантаження на системи та вимагати управління ключами шифрування.

Безпека програмного забезпечення включає в себе оновлення та патчінг для усунення відомих уразливостей. Використання антивірусного програмного забезпечення допомагає захистити системи від шкідливого програмного забезпечення. Однак цей підхід не завжди ефективний проти нових, невідомих загроз.

Фізична безпека гарантує захист від фізичного вторгнення та несанкціонованого доступу. Застосування систем контролю доступу та відеоспостереження забезпечує додаткові рівні захисту, але вимагає значних витрат та управління.

Аудит безпеки є необхідним для виявлення потенційних уразливостей через регулярні перевірки. Проте, може виникнути ризик помилкових тривог та навантаження на системи, вимагаючи ресурсів для проведення аудитів.

Співпраця та інформаційний обмін з іншими організаціями підвищують здатність реагування на кіберзагрози. Проте, може бути важко координувати дії різних сторін, і існує ризик небажаного витоку інформації.

Планування та реагування на інциденти розробляються для швидкого та ефективного відновлення після кібератак. Проте, їх ефективність може зазнати втрат через зміни в інфраструктурі та вимагати постійного оновлення та тестування[20]

Навчання та підвищення рівня свідомості персоналу про кібербезпеку може зменшити ризик внутрішніх загроз. Але цей підхід вимагає часу та ресурсів для організації тренінгів, і не гарантує повного виконання політик безпеки всіма працівниками.

Перелік ще деяких методів протидії з описом, перевагами та недоліками подано таблицею у додатку А

Ці заходи є необхідними разом, як частина комплексної стратегії забезпечення кібербезпеки критичної інфраструктури. Кожен метод має свої переваги та недоліки, і їх взаємодія є критичною для створення ефективної системи захисту.

ВИСНОВОК ДО 1 РОЗДІЛУ

Розділ, присвячений огляду існуючих кібератак на об’єкти критичної інфраструктури (ОКІ), методів їх реалізації та заходів з протидії. Здобута інформація розкриває різноманітні сценарії атак, спрямованих на ОКІ, а також методи їхньої реалізації, що може послужити основою для розробки ефективних стратегій захисту.

Зокрема, аналіз наслідків кібератак вказує на серйозні загрози, які можуть виникнути внаслідок порушення безпеки. Втрати конфіденційності, цілісності та доступності інформації можуть мати серйозні соціальні, економічні та політичні наслідки. Тому необхідно невідкладно вдосконалювати заходи з протидії та підвищувати рівень кібербезпеки ОКІ.

Запропоновані у розділі методи захисту та протидії кібератакам надають цінні вказівки для розробки комплексних стратегій безпеки. Серед них можна виділити заходи з моніторингу та виявлення аномалій, шифрування даних, удосконалення систем аутентифікації та авторизації, а також постійне оновлення програмного забезпечення. Важливим елементом є також відповідальність всіх учасників інфраструктури за забезпечення безпеки та взаємодія між різними рівнями оборони.

Узагальнюючи, розділ надає необхідну основу для подальших досліджень та розробки стратегій кіберзахисту, а також акцентує важливість постійного вдосконалення систем безпеки.

2 РОЗДІЛ. МЕТОДИ ПОКРАЩЕННЯ ЕЛЕМЕНТІВ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ ОКІ

2.1 Методи підвищення ефективності методів протидії кібератакам на ОКІ

До основних методів підвищення ефективності кібербезпеки на ОКІ віднесено [15, 16]:

1. **Розвинення систем виявлення інцидентів (SIEM)**:

- Використання SIEM-систем дозволяє виявляти аномалії та надзвичайні події в мережі чи системі, що може сприяти швидкій реакції на потенційні загрози. Це включає аналіз журналів подій, виявлення атак та автоматизовані засоби реагування.

2. **Посилення кібергігієни:**

- Навчання персоналу: Проведення регулярних тренінгів з питань кібербезпеки для персоналу сприяє підвищенню рівня обізнаності та відповідальності в галузі кіберзахисту[18].
- Стандарти безпеки: Введення та забезпечення виконання стандартів безпеки, таких як ISO 27001, допомагає створити стійку систему захисту.

3. **Посилення мережевої безпеки:**

- Захист від DDoS-атак: Використання спеціальних пристроїв та послуг для захисту від розподілених атак на доступність.
- Розробка резервних планів: Створення і випробування планів відновлення після інциденту та резервних копій даних для мінімізації можливих збитків.

4. **Впровадження шифрування та аутентифікації:**

- Шифрування даних: Застосування шифрування для захисту конфіденційності даних під час їх передачі та зберігання.
- Аутентифікація двофакторна/багатофакторна: Використання додаткових етапів аутентифікації для ускладнення несанкціонованого доступу.

5. **Інтеграція технологій штучного інтелекту (ШІ) та машинного навчання (МН):**

- Аналіз поведінки: Використання ШІ та МН для виявлення аномалій в поведінці системи та автоматичного реагування на нові типи атак.
- Прогнозування загроз: Застосування аналітики та алгоритмів прогнозування для передбачення потенційних кіберзагроз та їх викриття до виникнення інциденту[19.

Ці методи у поєднанні створюють комплексний підхід до кібербезпеки об'єктів критичної інфраструктури, забезпечуючи високий рівень захисту та швидку реакцію на динаміку еволюції кіберзагрозр].

2.2 Розроблення математичної моделі вибору оптимальної стратегії застосування методів протидії кібератакам на ОКІ

Нехай є набір методів протидії кібератаці на ОКІ:

$M = \{ m_i \}, i \in [1;N],$

Кожний метод описується трьома параметрами *{P, T, C}:*

P_i – потенціал протидії (тобто здатність методу адекватно протидіяти конкертній кібератаці, або її складовій) і-того методу протидії загрозі;

T_i – час запровадження *i*-того методу (або час перехідного процесу від початку дії метода);

C_i – витрати застосування *i*-того методу.

Називатимемо стратегією протидії $S_j=\{m_{j,i}\}$ довільний набір методів, який ефективно протидіє загрозі Z_j. Загрозу Z_j характеризуємо параметром збитків L_j.

$$S_j \subseteq M, \tag{1}$$

Називатимемо ефективністю *i*-того метода E_i співвідношення:

$$E_i = \frac{P_i}{T_i \ C_i}, \tag{2}$$

Тоді ефективністю стратегії буде S_j величина:

$$E_{s_j} = \sum E_{ij}$$

де E_{i_j} – ефективність i-того методу в j-тій стратегії,

$$E_{s_i} = \sum \frac{P_{ij}}{T_{ij}\, C_{ij}}, \tag{3}$$

Нехай потік атак описується пуассонівським потоком подій:

$$P_{(A)} = \frac{(\lambda\tau)^m}{m!} e^{-\lambda\tau}, \tag{4}$$

де **λ** - інтенсивність потоку атак, m- кількість атак (подій) за час τ (реалізації потоку для різних значень **λ** та m наведено на рис.2.1)

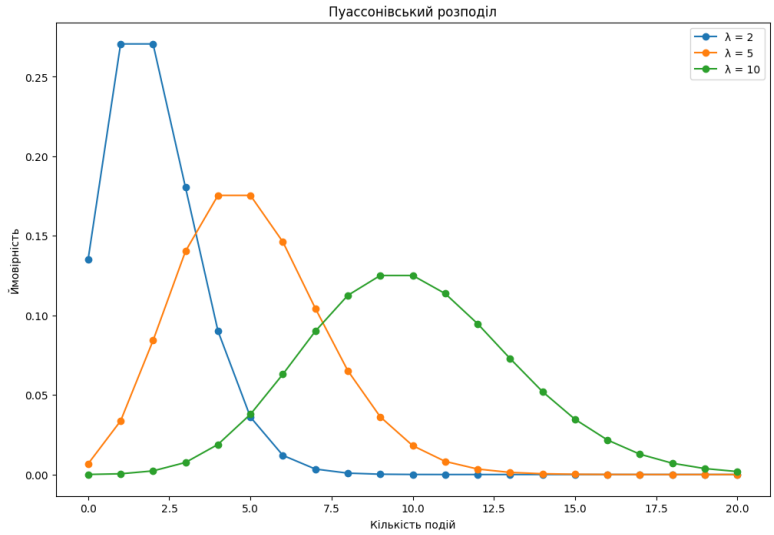

Рисунок 2.1 Реалізація пуассонівського потоку подій для різних значень **λ** (2, 5, 10)

Нехай середні втрати від атаки становлять L_a тоді можна подати, що математичне очікування втрат за час **τ** становить:

$$< \sum L_A > = L_A \sum_m \lambda\tau \frac{(\lambda\tau)^m}{m!} e^{-\lambda\tau} = L_{A\lambda\tau} e^{-\lambda\tau} \sum_{m=0}^{\infty} \frac{(\lambda\tau)^m}{m!}$$

Оскільки ряд $\frac{(\lambda\tau)^m}{m!}$ сходиться та $\sum \frac{(\lambda\tau)^m}{m!} = e^{\lambda\tau}$,то

$$< \sum L_A > = L_{A\lambda\tau}, \tag{5}$$

Опишемо загальні втрати від потоку атак таким співвідношенням:

$$L_{\text{заг}} = L_{A\lambda\tau}\left(1 - E_j^*\right), \quad (6)$$

де E_j^*- нормована до 1 ефективність обраної стратегії

Тоді принцип вибору стратегії має забезпечувати мінімалізацію $L_{\text{заг}}$

$$L_{A\lambda\tau}\left(1 - E_j^*\right) \to min, \quad (7)$$

за таких обмежень:

$$\begin{gathered} C_j = \sum C_i < C_{max} \text{ (обмеження на витрати)} \\ P_j = \sum P_i < P_{max} \text{ (обмеження на потенціал)} \\ T_j < T_{max} \text{ (обмеження по часу)} \\ C_j < \lambda L_{A\tau}, \text{ (}\textbf{принцип доцільності: використовувати стратегію, якщо вартість її реалізації менша за втрати від атак}\text{)} \end{gathered} \quad (8)$$

Вираз (7) можемо переписати як:

$$L_{A\lambda\tau}\left(1 - \frac{E_j}{E_{max}}\right) \to min,$$

де E_{max}- максимальна можлива ефективність стратегії.

$$L_{A\lambda\tau}\left(1 - \frac{E_j}{E_{max}}\right) = \frac{L_{A\lambda\tau}}{E_{max}}\left(E_{max} - E_j\right),$$

за фіксованих значень $L_A, \lambda, \tau, E_{max}$ задача зводиться до мінімізації співвідношення:

$$E_{max} - E_j \to min$$

$$E_{max} - \frac{P_j}{T_j C_j} \to min, \text{за обмежень 8.}$$

Для вирішення скористаємось методом Лагранжа [17], отже синтезуємо рівняння Лагранжа:

$$L_1 = E_{max} - \frac{P_j}{T_j C_j} - M_1\left(P_{max} - P_j\right) - M_2\left(T_{max} - T_J\right) - M_3\left(C_{max} - C_j\right) - M_4(\lambda L\tau - C_J)$$

Прирівняємо часткові похідні до нуля:

$$\begin{cases} \dfrac{\partial L}{\partial P_j} = -\dfrac{1}{T_j C_j} + M_1 = 0 \\ \dfrac{\partial L}{\partial T_j} = \dfrac{P}{T^2 C} + M_2 = 0 \\ \dfrac{\partial L}{\partial C_j} = \dfrac{P}{T C^2} + M_3 + M_4 = 0 \\ \dfrac{\partial L}{\partial M_1} = P_{max} - P_j = 0 \\ \dfrac{\partial L}{\partial M_2} = T_{max} - T_j = 0 \\ \dfrac{\partial L}{\partial M_3} = C_{max} - C_j = 0 \\ \dfrac{\partial L}{\partial M_4} = \lambda L \tau - C_j = 0, \end{cases} \quad (9)$$

Отже, розв’язок рівняння 9 надасть можливість визначити параметри (P, T, C) оптимальної стратегії S для протидії загрозі Z за критерієм ефективності як сукупності показників (потенціалу методів, що входять до стратегії, вартості та часу реагування цих методів)

ВИСНОВОК ДО 2 РОЗДІЛУ

Проаналізовано основні методи протидії кібератакам на ОКІ. Зазначено, що максимальної ефективності комплексна протидія кібератакам набуває за умови застосування сукупності методів (тобто застосування конкретних методів окремо не дозволяє забезпечити максимальну ефективність). Це відповідає системному підходу до вирішення проблеми забезпечення кібербезпеки, а саме застосування синергетичного ефекту від використання сукупності методів одночасно, як певної стратегії протидії кіберзагрозам.

Математично формалізовано процес вибору оптимальної стратегії як множини методів протидії кібератакам за критерієм найбільшої ефективності. Запропоновано формалізувати ефективність стратегії як співвідношення потенціалу методу, часу реакції та вартості застосування.

3 РОЗДІЛ. РОЗРАХУНКИ Й ЕКСПЕРИМЕНТАЛЬНІ ДАНІ, ЩО ПІДТВЕРДЖУЮТЬ ПРАВИЛЬНІСТЬ ПРОГРАМНИХ РІШЕНЬ.

3.1 Визначення оптимальних значень параметрів стратегії протидії кіберзагрозі

Для визначення оптимальних параметрів стратегії, а саме потенціалу набору методів, вартості та часу застосування (реакції) необхідно вирішити рівняння 9 (р.2.2). Розв'язок рівняння 9 виконано в середовищі Google Colaboratory на мові програмування Python із застосуванням бібліотеки sympy

Лістинг програми:

```
from sympy import symbols, solve, Eq
# Символьні змінні
P, C, T, lambda_, mu, nu, loss_mu = symbols('P C T lambda mu nu loss_mu')
# Значення
Pmax = 10
Cmax = 1
Tmax = 1
Emax=5
L=3
# Функція Лагранжа
L = Emax - P / (C * T) - lambda_ * (Pmax - P) - mu * (Cmax - C) - nu * (Tmax - T) - loss_mu* (L - C)
# Умови
conditions = [Eq(Pmax - P, 0),Eq(Cmax - C, 0), Eq(Tmax - T, 0),Eq(L-C, 0)]
# Часткові похідні
partials = [L.diff(var) for var in (P, C, T, lambda_, mu, nu, loss_mu)]
print (partials)
# Додаємо умови
partials.extend(conditions)
# Розв'язуємо систему рівнянь
solution = solve(partials, (P, C, T, lambda_, mu, nu, loss_mu))
# Виводимо результати
print(solution)
```

Розв’язки для різних значень обмежень

№пп	Значення вхідних параметрів моделі				Розв'язок		
	Pmax	Cmax	Tmax	L	P	C	T
1	100	100	100	50	70	20	15
2	80	30	30	75	50	10	20
3	50	20	5	80	Не має розв’язку		

Для третього сценарію розв'зок відсутній через неможливість сформувати стратегію, оскільки втрати від загрози більше за потенціал (тобто за можливість попередити збитки) методів, які в арсеналі, додатково унеможливлює вимога швидкого реагування. З практичної точки зору це можна інтерпретувати як необхідність розширити арсенал методів.

3.2 Приклад застосування запропонованої моделі

Нехай в результаті застосування моделі встановлено такі параметри стратегії табл. 3.1

Таблиця 3.1 Параметри стратегії встановлені в результаті застосування моделі та параметри статичної стратегії

Параметр стратегії	S_1 (змодельовані дані)	S_2 (статичні дані)
Потенціал (сума потенціалів методів, які входять до обраної стратегії)	50	80
Час реакції (сума реакцій методів)	20	30
Витрати (витрати на одиницю часу)	10	20

Розрахуємо ефективності стратегій

$$E_1 = \frac{P_1}{T_1\ C_1} = \frac{50}{20 * 10} = 0.25$$

$$E_2 = \frac{P_2}{T_2\ C_2} = \frac{80}{30 * 20} = 0.13$$

Вочевидь, стратегія S_1 демонструє вищу ефективність. Наступним кроком є формування набору методів, які відповідають показникам обраної стратегії.

ВИСНОВОК ДО 3 РОЗДІЛУ

Наведено послідовність визначення параметрів оптимальної стратегій за критерієм ефективності, що дозволяє в подальшому формувати набір методів для комплексної протидії кіберзагрозі

Проведено порівняльний аналіз стартегії через визначення показника ефективності, показано, що запропонований підхід дозволяє визначати ефективність стратегій, а отже дає можливість адаптивно реагувати на кібератаки.

ЗАГАЛЬНІ ВИСНОВКИ

Проаналізовано основні види кібератаки на об’єкти критичної інфраструктури, встановлено основні особливості таких кібератак, які полягають у тому, щоб завдати максимальних збитків на державному рівні. Втрата конфіденційності, цілісності та доступності інформації може мати серйозні соціальні, економічні та політичні наслідки.

Проаналізовано основні методи протидії кібератакам на ОКІ. Зазначено, що максимальної ефективності комплексна протидія кібератакам набуває за умови застосування сукупності методів (тобто застосування конкретних методів окремо не дозволяє забезпечити максимальну ефективність). Це відповідає системному підходу до вирішення проблеми забезпечення кібербезпеки, а саме застосування синергетичного ефекту від використання сукупності методів одночасно, як певної стратегії протидії кіберзагрозам.

Математично формалізовано процес вибору оптимальної стратегії як множини методів протидії кібератакам за критерієм найбільшої ефективності. Запропоновано формалізувати ефективність стратегії як співвідношення потенціалу методу, часу реакції та вартості застосування.

Наведено послідовність визначення параметрів оптимальної стратегій за критерієм ефективності, що дозволяє в подальшому формувати набір методів для комплексної протидії кіберзагрозам. Проведено порівняльний аналіз стратегії через визначення показника ефективності, показано, що запропонований підхід дозволяє визначати ефективність стратегій, а отже дає можливість адаптивно реагувати на кібератаки.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Учасники проектів Вікімедіа. Фішинг – Вікіпедія. *Вікіпедія*. URL: https://uk.wikipedia.org/wiki/Фішинг (дата звернення: 17.12.2023).

2. Учасники проектів Вікімедіа. Соціальна інженерія (безпека) – Вікіпедія. *Вікіпедія*.
URL: https://uk.wikipedia.org/wiki/Соціальна_інженерія_(безпека) (дата звернення: 10.11.2023).

3. Учасники проектів Вікімедіа. Шкідливий програмний засіб – Вікіпедія. *Вікіпедія*.
URL: https://uk.wikipedia.org/wiki/Шкідливий_програмний_засіб (дата звернення: 10.11.2023).

4. Учасники проектів Вікімедіа. Віддалені мережеві атаки – Вікіпедія. *Вікіпедія*.
URL: https://uk.wikipedia.org/wiki/Віддалені_мережеві_атаки (дата звернення: 11.11.2023).

5. В.В. Домарев, Безопасность информационных технологий. Методология создания систем защиты. Київ, Україна: ООО “ТИД “ДС”, 2002.

6. Council of the European Union. (2008, Dec. 08). Directive 2008/114/EC, On the identification and designation ofEuropean critical infrastructures and the assessment of the need to improve their protection. [Online]. Available: http://eur-1ex.europa.eu/1ega1-content/EN/ALL/?uri= celex:32008L0114. Accessed оп: Dec. 18, 2015.

7. Гайдамашко О. Дослідники виявили шкідливе ПЗ CosmicEnergy, яке Кремль використовує для навчання хакерів. *24 Канал*. URL: https://24tv.ua/tech/fahivtsi-mandiant-proanalizuvali-programu-dlya-navchannya-kremlivskih_n2321784 (дата звернення: 30.11.2023).

8. Гайдамашко О. Російські хакери кілька місяців мали доступ до української енергосистеми, перш ніж атакувати її. *24 Канал*. URL: https://24tv.ua/tech/pidrozdil-google-rozpoviv-pro-rosiyski-kiberataki-proti-ukrayini_n2428873 (дата звернення: 02.12.2023).

9. Павлов І. М., Толюпа С. В., Ніщенко В. І. Аналіз таксономії систем виявлення атак у контексті сучасного рівня розвитку інформаційних систем. Сучасний захист інформації. 2014. № 4. С. 44–52.

10. Толюпа С. В., Штаненко С. С., Берестовенко Г. Класифікаційні ознаки систем виявлення атак та напрямки їх побудови. Збірник наукових праць Військового інституту телекомунікацій та інфор- матизації імені Героїв Крут. 2018. Вип. № 3. С. 56–66.

11. Гулак Г. М. Методологія захисту інформації. Аспекти кібербезпеки: підручник. Київ: Видавництво НА СБ України, 2021. 256 с.

12. Учасники проектів Вікімедіа. Діпфейк – Вікіпедія. *Вікіпедія*. URL: https://uk.wikipedia.org/wiki/Діпфейк (дата звернення: 08.12.2023).

13. Мельник Т. «Це найбільша у світі хакерська атака на телеком-інфраструктуру». Перше інтерв'ю президента «Київстару» після кібератаки, яка паралізувала оператора – Forbes.ua. *Forbes.ua | Бізнес, мільярдери, новини, фінанси, інвестиції, компанії*. URL: https://forbes.ua/innovations/pro-kiberataku-na-kiivstar-vidnovlennya-zvyazku-ta-dopomogu-microsoft-cisco-ericsson-blits-intervyu-prezidenta-kompanii-komarov-12122023-17855 (дата звернення: 15.12.2023).

14. В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа. «Інформаційна та кібербезпека: соціотехнічний аспект». - 2015.

15. О.Г. Трофименко Законодавча база забезпечення кібербезпеки держави. Кібербезпека в Україні: правові та організаційні питання: матер. ІІ всеукр. наук.-практ. конф., 17 листопада 2017 р., Одеса: ОДУВС, С. 55–56.

16. Основи кіберпростору, кібербезпеки та кіберзахисту / В. Богуш та ін. Ліра-К, 2021. 554 с.

17. Книга: Обчислення (OpenStax). *LibreTexts - Ukrayinska*. URL: https://ukrayinska.libretexts.org/Математика/розрахунку/Книга:_Обчислення_(OpenStax) (дата звернення: 12.12.2023).

18. Інжиєвський О. О., Веретюк С. М. Роль людського фактору у підвищенні ефективності заходів протидії кібератакам на об'єкти критичної

інфраструктури. *Пріоритетні шляхи розвитку науки і освіти* : Міжнар. науково-практ. конф., м. Львів, 29–30 листоп. 2023 р. Львів, 2023. С. 44.

19. Інжиєвський О. О., Веретюк С. М. Роль інноваційних технологій у вдосконаленні заходів протидії кібератакам на об’єкти критичної інфраструктури. *Пріоритетні напрями досліджень в науковій та освітній діяльності:* : Міжнар. науково-практ. конф., м. Львів, 19–20 грудня. 2023 р. Львів, 2023. С 76.
20. Інжиєвський О. О., Веретюк С. М. Методи підвищення захисту об’єктів критичної інфраструктури від кібератак. *Безпека, Технології, Інновації: нові горизонти* : Міжфакультет. науково-практ. інтернет-конф., м. Житомир, 15 листоп. 2023 р. Житомир, 2023. С