ISSN 2225-5036 (Print), ISSN 2411-071X (Online)
http://infosecurity.nau.edu.ua; http://jrnl.nau.edu.ua/index.php/Infosecurity

КІБЕРБЕЗПЕКА ТА ЗАХИСТ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ / CYBERSECURITY & CRITICAL INFORMATION INFRASTRUCTURE PROTECTION (CIIP)

DOI: 10.18372/2225-5036.30.19234

МОДЕЛЬ ОЦІНЮВАННЯ КІБЕРСТІЙКОСТІ ІНФОРМАЦІЙНИХ СИСТЕМ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ПІД ВПЛИВОМ ГІБРИДНИХ КІБЕРАТАК З ВИКОРИСТАННЯМ АЛГОРИТМІВ МАШИННОГО НАВЧАННЯ

Володимир Шиповський

Національний університет оборони України

ШИПОВСЬКИЙ Володимир Володимирович, ад'юнкт
Рік та місце народження: 1981 рік, м Київ, Україна.
Освіта: Національний університет оборони України, 2019 рік.
Посада: ад'юнкт кафедри інформаційно-аналітичних технологій.
Наукові інтереси: інформаційна безпека, кіберзахист критичної інфраструктури, мультидоменні операції (MDO).
Публікації: більше 30 наукових публікацій, серед яких навчальні посібники, наукові статті, матеріали та тези доповідей на конференціях.
E-mail: v.shypovskyi@nuou.org.ua.
Orcid ID: 0000-0003-3743-3064.

Анотація. *У статті представлено модель оцінювання кіберстійкості інформаційних систем об'єктів критичної інфраструктури (ОКІ) під впливом комбінованих кібератак. Модель аналізує вплив десяти типів атак, таких як DoS, DDoS, фішинг, шкідливе програмне забезпечення та інші, на системи HMI та SCADA. Взаємодія між атаками та системами моделюється через метод Монте-Карло, генетичний алгоритм використовується для створення гібридних атак, а кластеризація за допомогою HDBSCAN дозволяє визначити стійкість систем до певних типів атак. Прогнозування наслідків атак та часу відновлення здійснюється за допомогою алгоритму Random Forest Regressor. Результати дослідження можуть бути використані для вдосконалення заходів кіберзахисту ОКІ та підвищення їх здатності до відновлення після кібератак.*

Ключові слова: *кіберстійкість, гібридні загрози, критична інфраструктура, HMI, SCADA, генетичний алгоритм, ОКІ, кібератака, інформаційні системи, відновлення, моделювання, симуляція, оцінювання, машинне навчання, кібербезпека.*

Постановка проблеми

Сучасний розвиток цифрових технологій та критична залежність об'єктів інфраструктури від інформаційних систем ставлять нові виклики у сфері кібербезпеки. Об'єкти критичної інфраструктури (ОКІ) України постійно стають цілями різноманітних кібератак з боку Російської Федерації, особливо в умовах російського військового вторгнення.

Кібератаки часто поєднуються з ракетними ударами по критичній інфраструктурі, що збільшує їхній руйнівний ефект і ускладнює процес відновлення. ОКІ, як енергетичні системи, водопостачання, транспорт та зв'язок, особливо вразливі до атак через свою критичну важливість для економіки і національної безпеки [1].

З початком повномасштабного вторгнення хакери рф активно використовують тактики DDoS-атак, фішингу та шкідливого програмного забезпечення для порушення роботи інформаційних систем критичної інфраструктури України, що координується з кінетичними ударами для підвищення ефективності. Наприклад, атаки на українську енергетичну систему супроводжувались фізичними ракетними ударами для посилення руйнівних наслідків [2].

До найбільш поширених типів кібератак належать DDoS, фішинг, шкідливе програмне забезпечення та SQL-ін'єкції.

Вони націлені на системи управління, такі як HMI та SCADA, які є ключовими елементами інфраструктур. Ці системи потребують постійної уваги до

їх кіберзахищеності та здатності до відновлення після атак [3].

Метою цього дослідження є розробка моделі оцінювання кіберстійкості ОКІ під впливом комбінованих кібератак. Для цього будуть враховані специфічні характеристики різних типів атак та об'єктів інфраструктури, що дозволить створити комплексний підхід до визначення рівня кіберстійкості кожного з компонентів системи.

Аналіз останніх досліджень та публікацій

У [4] зазначено, що російські хакери протягом 2022-2023 років активно атакували енергетичну інфраструктуру України, використовуючи DDoS-атаки і поєднуючи їх з ракетними ударами. Це показує новий рівень координації кібератак з військовими діями, що значно ускладнює відновлення після пошкоджень. У статті «Кібератака на Україну – не вперше і не востаннє?» обговорюється, що кіберпростір став важливим елементом військових дій поряд із землею, морем та повітрям. Особливо наголошується на ролі кібератак у війні РФ проти України, де вони використовуються як гібридна загроза для критичної інфраструктури [5] зазначено, що у 2023 році кількість кібератак на критичну інфраструктуру України зросла на 62%. Російські хакери продовжують націлюватись на об'єкти інфраструктури з метою дестабілізації. Аналіз різних джерел показує що проблеми кіберзахисту ОКІ лишаються вагомими та потребують нових підходів до вирішення.

Мета та постановка завдання

Метою дослідження є розробка моделі для оцінювання кіберстійкості інформаційних систем об’єктів критичної інфраструктури (ОКІ) під впливом комбінованих кібератак. Модель повинна враховувати особливості кібератак, які були застосовані проти ОКІ, таких як енергопостачання, водопостачання, транспорт, зв'язок та виробничі підприємства, ураження яких передбачає загрози національній безпеці. Завдання полягає в оцінці вразливості інфраструктури до заданих типів загроз, впливу загроз на об’єкти, їх стійкості та здатності до відновлення після атак. Розроблена модель дозволить оцінювати вплив одинарних і комбінованих атак, виявляти вразливості ОКІ та симулювати стійкість систем для покращення захисних заходів та підвищення кіберстійкості.

Виклад основного матеріалу дослідження

Кібератаки на об'єкти критичної інфраструктури (ОКІ) є вагомою загрозою, для національної безпеки України. Енергетичний сектор, водопостачання та інші критично важливі об’єкти регулярно стають мішенню для кібератак з боку рф. Згідно з численними звітами, зокрема від Державної служби спеціального зв'язку та захисту інформації України (ДССЗЗІ) та CERT-UA, найбільш поширеними кібератаками на ОКІ є: DoS, DDoS, фішинг, SQL-ін’єкції, шкідливе програмне забезпечення (Malware), атаки методом грубої сили (Brute Force), атаки «людина посередині» (MitM), програми-вимагачі (Ransomware), атаки нульового дня (Zero-day exploit) та соціальна інженерія. Один із найвідоміших прикладів — це атака на енергетичну інфраструктуру України у 2015 році, коли кіберзлочинці використали шкідливе програмне забезпечення BlackEnergy для відключення електроенергії, атакуючи SCADA-системи енергетичних компаній [1].

Також яскравим прикладом є атака NotPetya у 2017 році, спрямована на українські підприємства та об’єкти критичної інфраструктури, що призвела до масштабних збоїв у роботі підприємств і державних установ [2]. Інформаційні системи ОКІ складаються з систем HMI (людино-машинний інтерфейс) та SCADA (системи диспетчерського контролю та збору даних) однаково під загрозою деструктивних кібервпливів з боку росії. Зовнішні атаки спрямовані на вразливості в мережі, програмному забезпеченні або периметрі системи, тоді як внутрішні атаки можуть здійснюватися інсайдерами або через компрометацію внутрішніх компонентів.

Наприклад, у 2022 році CERT-UA повідомила про зростання кількості інсайдерських загроз в енергетичному секторі України [3].

У таблиці 1 відобржажені можливі види зовнішніх деструктивних впливів на системи HMI та SCADA, у таблиці 2 представлені впливи які є результатом внутрішніх кібератак (табл. 1, 2).

Для створення моделі в статті пропонується вважати що внутрішні та зовнішні кібератаки можуть впливати як HMI на так і SCADA системи, що відображає реальність комбінованих загроз та спростить подальші розрахунки.

Таблиця 1

Вплив зовнішніх кібератак

Атака	Вплив на HMI	Вплив на SCADA
DoS	Обмежений, мережеві збої	Перешкоджає моніторингу та керуванню
DDoS	Системний збій HMI	Виводить з ладу SCADA
Phishing	Викрадення облікових даних	Менший вплив на SCADA
SQL Injection	Збої в доступі до даних	Мінімальний вплив
Zero-Day Exploit	Вразливості в ПЗ HMI	Вплив на SCADA-контролери

Таблиця 2

Вплив внутрішніх кібератак

Атака	Вплив на HMI	Вплив на SCADA
Malware	Віруси впливають на HMI	Віруси впливають на SCADA
Ransomware	Шифрування даних HMI	Шифрування SCADA
Brute Force	Доступ до HMI через підбір	Доступ до SCADA
MitM	Перехоплення даних HMI	Модифікація даних SCADA
Social Engineering	Маніпуляції користувачами	Мінімальний вплив

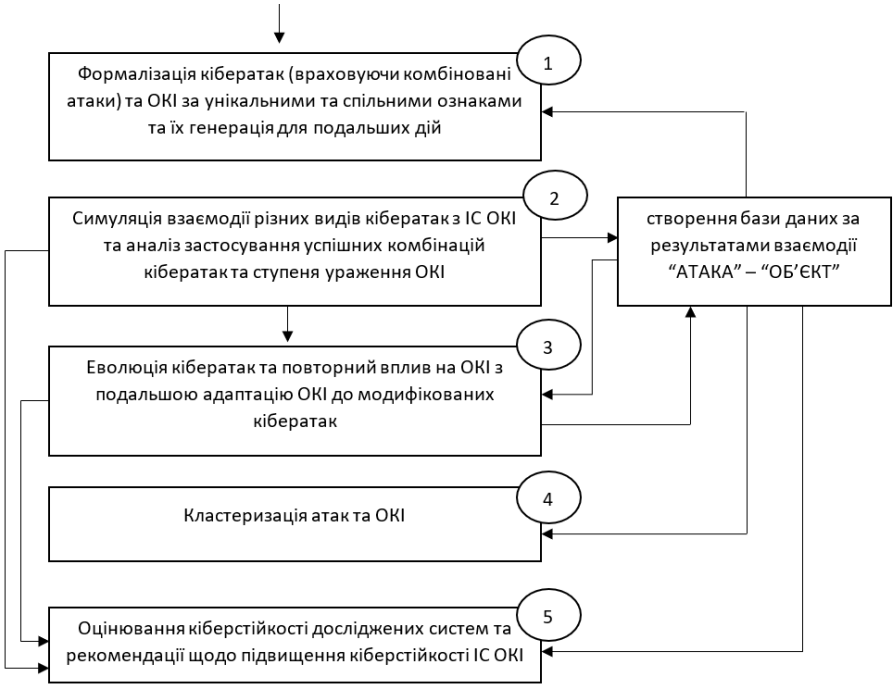

Рис.1 Орієнтовна блок-схема роботи моделі «атака» - «об'єкт»

Представлені елементи моделі оцінювання кіберстійкості інформаційних систем об'єктів критичної інфраструктури в умовах гібридних кібератак та послідовність їх застосування (рис. 1). Для практичної реалізації та моделювання процесів буде використовуватись мова програмування PHYTON.

За відсутності реальних даних, припустимо, що кожен об'єкт інфраструктури та кожна кібератака може однозначно визначатись своїм певним набором параметрів. Відповідно чим більше атак та систем ми створимо синтетичним чином – тим вища ймовірність того, що з-поміж них виявляться й реальні системи. Відповідно чим більше ми згенеруємо атак – тим вища ймовірність, що новостворена реальна атака буде схожою на одну з тих, які ми моделюємо. Відповідно знаючи оцінку параметрів атаки, ми зможемо якісно відреагувати на неї змінивши атрибути системи. Для моделі визначені 5 видів ОКІ, на які ймовірно будуть спрямовані деструктивні впливи з їх атрибутами.

1. Система енергопостачання **(Energy Supply).**

Специфічні Атрибути: кількість вузлів **(`num_nodes`)**, кількість з'єднань **(`num_connections`)**, рівень надмірності **(`redundancy_level`)**, типи захисту **(`physical_protection`, `cyber_protection`)**, резервні джерела енергії **(`backup_power_sources`)**.

2. Система водопостачання **(Water Supply).**

Специфічні Атрибути: кількість насосних станцій **(`num_pump_stations`)**, резервуари **(`reservoirs`)**, рівень автоматизації **(`automation_level`)**, протоколи зв'язку **(`communication_protocols`)**, системи очищення води **(`water_treatment_systems`)**.

3. Система транспорту **(Transportation).**

Специфічні Атрибути: кількість станцій **(`num_stations`)**, маршрути **(`routes`)**, системи керування трафіком **(`traffic_control_systems`)**, рівень захищеності сигналів **(`signal_protection_level`)**, транспортні засоби **(`vehicles`)**.

4. Система зв'язку **(Communication).**

Специфічні Атрибути: кількість базових станцій **(`num_base_stations`)**, типи мереж **(`network_types`)**, рівень надмірності **(`redundancy_level`)**, методи шифрування **(`encryption_methods`)**, пропускна здатність **(`bandwidth`)**.

5. Виробничі підприємства **(Manufacturing Enterprises).**

Специфічні Атрибути: площа забрудненої території **(`polluted_area `)**, кількість населення, яке відчує наслідки впливу на OKI **(`numb_affected_population`)**, рівень ураження **(`level_ impact`)**, масштаби загрози національній безпеці **(`national_importance`)**.

Також визначаємо 10 видів кібератак з їх атрибутами для моделювання подальшої кластеризації за унікальними ознаками:

1.**DoS** (Denial of Service). Високий обсяг трафіку, короткий інтервал між запитами, однакові адреси джерела. Специфічні Атрибути: **`high_traffic`, `short_interval`, `same_source_ip`**;

2. **DDoS** (Distributed Denial of Service). Високий обсяг трафіку з різних IP-адрес, короткий інтервал між запитами.Специфічні Атрибути: **`high_traffic`, `short_interval`, `multiple_source_ips`**;

3. **Phishing**. Зазвичай включає підроблені посилання або вкладення, часто відправляється через електронну пошту. Специфічні Атрибути: **`fake_links`, `attachments`, `email_based`**;

4.**SQL Injection**. Включення SQL команд у введені дані користувачів. Специфічні Атрибути: **`sql_commands_in_input`**;

5.**Malware**. Зловмисне програмне забезпечення, яке може викрадати дані або пошкоджувати систему. Специфічні Атрибути: **`malicious_software`, `data_theft`, `system_damage`**;

6. **Brute Force**. Велика кількість невдалих спроб авторизації за короткий час. Специфічні Атрибути: **`multiple_failed_logins`, `short_interval`**;

7. **MitM** (Man-in-the-Middle). Перехоплення та можливе змінення даних між двома сторонами. Специфічні Атрибути: **`data_interception`, `data_modification`**;

8. **Ransomware.** Блокує доступ до системи або даних, вимагаючи викуп. Специфічні Атрибути: **`data_encryption`, `ransom_demand`**;

9. **Zero-day Exploit.** Використання невідомих вразливостей у програмному забезпеченні. Специфічні Атрибути: **`unknown_vulnerabilities`**;

10. **Social Engineering**. Маніпулювання користувачами для отримання конфіденційної інформації. Специфічні Атрибути: **`user_manipulation`, `information_theft`.**

Для формалізації даних моделей використовуємо математичний апарат описаний у [4], але об'єднаємо внутрішні та зовнішні впливи, тоді вектор атрибутів захисту можна в час t можна визначити як – $S_{IC\_OKI}(\vec{x})$, та вектор атрибутів атаки як – $A(t)$. Тоді зміни в захисті системи можна виразити через наступне диференціальне рівняння (1):

$$\frac{dS_{IC\_OKI}(t)}{dt} = -\alpha S_{IC\_OKI}(t) + \beta A(t), \quad (1)$$

де a - параметр, що відповідає за внутрішню деградацію системи під час атаки. β - параметр, що відображає силу впливу атаки на систему. Тоді моделювання зміни інтенсивності атаки можна зробити за наступною формулою (2):

$$\frac{dA(t)}{dt} = -\varpi A(t) + \psi S_{IC\_OKI}(t), \quad (2)$$

де ω – параметр, що відповідає за зниження ефективності атаки через протидію системи. ψ - параметр, що відображає силу впливу атаки на систему.

Для створення синтетичних даних імпортуємо бібліотеки '**numpy'**, **'pandas'** та присвоюємо атрибути визначеним 10 типам атак. Додаємо функцію генерації даних для кожного виду атак, після цього додаємо функцію для комбінації різних типів кібератак. Відображений результат нижче (рис. 2).

	timestamp	source_ip	destination_ip	source_port	destination_port	protocol	payload_size	attack_type
0	2023-01-01 00:00:00	192.168.0.157	10.0.0.139	48881	7228	UDP	1229	DoS
1	2023-01-01 00:01:00	192.168.0.29	10.0.0.30	35428	25489	ICMP	760	DoS
2	2023-01-01 00:02:00	192.168.0.102	10.0.0.159	13385	46080	UDP	1104	DoS
3	2023-01-01 00:03:00	192.168.0.73	10.0.0.34	1655	49833	TCP	1329	DoS
4	2023-01-01 00:04:00	192.168.0.141	10.0.0.247	39939	58832	TCP	924	DoS
...	...	...	...	...	...	...	...	...
4995	2023-01-01 08:15:00	192.168.0.251	10.0.0.28	4392	52380	UDP	565	Social Engineering
4996	2023-01-01 08:16:00	192.168.0.173	10.0.0.225	27836	19282	UDP	565	Social Engineering
4997	2023-01-01 08:17:00	192.168.0.56	10.0.0.88	27696	25180	UDP	297	Social Engineering
4998	2023-01-01 08:18:00	192.168.0.220	10.0.0.6	54249	61191	ICMP	1111	Social Engineering
4999	2023-01-01 08:19:00	192.168.0.152	10.0.0.46	29162	38428	TCP	577	Social Engineering

Рис. 2 Результат генерації різних типів кібератак

Визначаємо типи OKI та присвоюємо унікальні атрибути кожному з об'єктів (вразливості і вагомі наслідки) та виводимо результат (рис. 3).

```
     system_type            timestamp  num_nodes  num_connections  \
0  Energy Supply  2023-01-01 00:00:00       67.0             72.0
1  Energy Supply  2023-01-01 01:00:00       74.0             67.0
2  Energy Supply  2023-01-01 02:00:00       80.0             94.0
3  Energy Supply  2023-01-01 03:00:00       49.0             49.0
4  Energy Supply  2023-01-01 04:00:00       62.0             26.0

   redundancy_level  physical_protection  cyber_protection  \
0              51.0                 37.0              22.0
1              25.0                 50.0               8.0
2              97.0                 98.0              94.0
3              47.0                 57.0              81.0
4              54.0                  3.0              16.0
```

Рис. 3 Результат генерації різних типів OKI

Складовими кіберстійкості є кіберзахищеність та здатність системи відновлюватись (відновлюваність).

У статті [5] представлена Система показників кіберстійкості інформаційних систем об'єктів критичної інфраструктури, яка надає можливості для оцінювання рівня кіберзахисту та дозволяє проводити комплексне оцінювання кіберстійкості інформаційних систем, враховуючи різноманітні технічні та організаційні особливості будь-якого OKI (рис. 4).

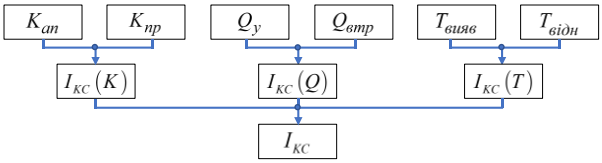

Рис. 4 Система показників кіберстійкості інформаційних систем ОКІ

Складові системи:

- показник кількості відбиття деструктивних кібервпливів – $I_{кс}\ K$;

- вартісний показник – $I_{кс}\ Q$;

- часовий показник – $I_{кс}\ T$.

Індекс відбиття деструктивних кібервпливів представляє собою відношення суми кількостей "успішно відбитих" атак K_{an} і усунутих внутрішніх порушень безпеки K_{np} до їх загальної кількості $K_{заг}$:

$$I_{кс}(K) = \frac{K_{an} + K_{np}}{K_{заг}}. \quad (3)$$

Вартісний показник кіберстійкості системи може бути виражений наступним чином:

$$I_{кс}(Q) = \frac{\sum_{y=1}^{Y} Q_y}{Q_{втр}}, \quad (4)$$

де Q_y – вартість реалізації у-го заходу забезпечення кіберзахисту системи; Y – кількість заходів забезпечення безпеки – може бути представлена як апаратним або програмним заходом підвищення кібербезпеки системи, так і підвищенням кваліфікації персоналу (інструктаж, освітній захід); $Q_{втр}$ – загальна вартість втрат у разі ураження ОКІ.

Часовий показник кіберстійкості представляє собою наступне відношення:

$$I_{кс}(T) = \frac{T_{вияв}}{T_{відн}}, \quad (5)$$

де $T_{вияв}$ – термін виявлення порушення безпеки – інтервал часу від моменту реалізації деструктивного впливу противника до його виявлення; $T_{відн}$ – термін відновлення роботи системи після порушення безпеки – часовий інтервал від моменту реалізації деструктивного впливу противника до усунення його впливу на мережу або систему.

Система показників кіберстійкості інформаційних систем ОКІ поверхнево враховує відновлюваність системи, яка є складовою кіберстійкості разом з кіберзахищеністю. Для моделі введемо додаткові показники відновлюваності інформаційної системи:

- показник випадкового впливу на ІС – $R_{ri} \in (0.5-1.5)$;

- показник здатності ІС до відновлюваності– $V_{sr} \in (0-1)$;

- показник складності відновлюваності – $V_{rc} \in (0-1)$.

Для генерації гібридних атак використовуємо Еволюційний алгоритм (генетичний алгоритм) – це алгоритм, який імітує біологічний процес еволюції, має в собі генетичні оператори та фітнес-функцію. Генетичні операції – мутація та схрещення. *Мутація* – на вхід один об'єкт, на вхід модифікований цей об'єкт (6). *Схрещення* – на вхід два об'єкти (батьки), на вихід один об'єкт (7):

$$x_{child} = \alpha \cdot x_{parent} + (1-\alpha) \cdot x_{parent2}, \quad (6)$$

$$x' = x + \varepsilon,\ \varepsilon \sim N(0,\sigma), \quad (7)$$

де σ – стандартне відхилення; α – коефіцієнт для кросовера, що визначає частку спадковості.

Фітнес функція – цільове значення, яке потрібно мінімізувати чи максимізувати за допомогою виведення нового об'єкту шляхом мутації та схрещення попередніх. (Виконується за допомогою пакета **DEAP**). На виході маємо наступний результат (рис.5).

```
Attack: ['Phishing', 'DDoS'], Fitness: (6.0, 1.3555793319735554, 0.05269044148171553, 0.6354028394681497)
Attack: ['Malware', 'Phishing'], Fitness: (6.0, 1.0954404792461538, 0.03215253359629067, 0.04747275258527006)
Attack: ['Phishing', 'Malware'], Fitness: (6.0, 0.825147090796888, 0.5219851421324894, 0.9463919402666732)
Attack: ['Malware', 'Phishing'], Fitness: (6.0, 0.8049371418406605, 0.09122240383925284, 0.47950410174714464)
Attack: ['Malware', 'DoS'], Fitness: (6.0, 0.7530602375092097, 0.2713589623300978, 0.13404796389701212)
Attack: ['DoS', 'Phishing'], Fitness: (6.0, 0.7410808921640454, 0.07414874378645275, 0.631461952152524)
Attack: ['Malware', 'Phishing'], Fitness: (6.0, 0.741007475804296, 0.06695159704398601, 0.20202940531985647)
Attack: ['DoS', 'Malware'], Fitness: (6.0, 0.7106673024607195, 0.027390151897267456, 0.16672288817337)
Attack: ['Phishing', 'DDoS'], Fitness: (6.0, 0.6727231696608563, 0.34732175969263734, 0.1676062103751771)
Attack: ['Malware', 'DDoS'], Fitness: (6.0, 0.5964164763123708, 0.967817181137165, 0.40753497911768033)
```

Рис. 5. Виведення найкращих результатів

Для проведення симуляції впливів кібератак на ОКІ використовуємо основи алгоритму Монте-Карло (8). Симуляції Монте Карло – алгоритм, який якісно враховує випадковість та варіативність для моделювання різноманітних сценаріїв атак, оскільки загрози можуть мати випадкові та непередбачувані характеристики. Підходить для моделювання складних систем і процесів в умовах невизначеностей, до того ж результати роботи можна використати для проведення статистичного аналізу через надзвичайно велику

кількість змодельованих сценаріїв і варіантами поведінки та впливу на систему.

$$\mu \approx \frac{1}{N}\sum_{i=1}^{N} f(x_i), \quad (8)$$

де N – кількість симуляцій; x_i – випадкове значення на *i*-ому кроцісимуляції.

Повторно вводимо атрибути атак та OKI, проводимо симуляції та візуалізуємо результати за допомогою модуля **'pyplot'** з бібліотеки **'Matplotlib'** та бібліотеки **'seaborn'** та отримуємо наступний результат:

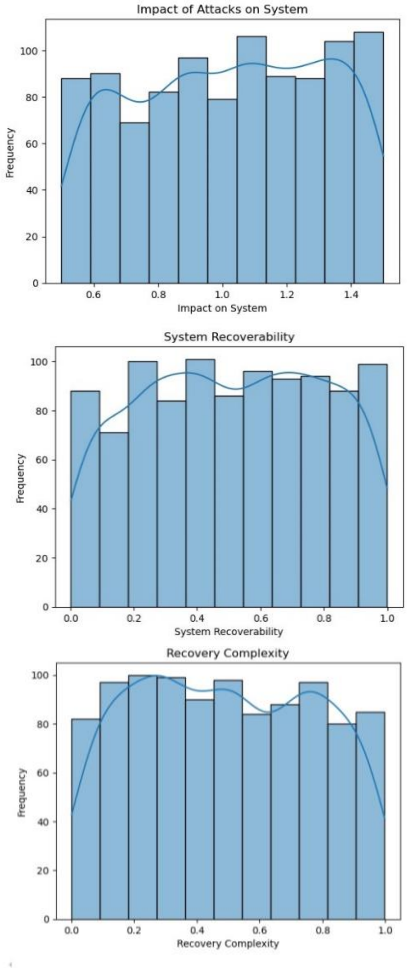

Рис. 6. Візуалізація відновлюваності систем після атаки

Наступним кроком ділимо дані на окремі кластери: за результатами проведеної симуляції можемо поділити системи на множини за схожістю, оскільки певні типи систем виявились одночасно вразливими до певних типів атак, або навпаки, одночасно стійкими. Що дає нам змогу якісно оцінити ті атрибути, які вплинули на вразливість чи які спонукали до стійкості. Для реалізації використовуємо метод **Mutual Information Score** який визначає залежності між змінними та допомагає покращувати моделі, визначаючи важливі ознаки. Чим вища взаємна інформація, тим сильніший взаємозв'язок між змінним). Потім дані передаються на вхід в алгоритм HDBSCAN (*Hierarchical Density-Based Spatial Clustering of Applications with Noise*) – це розширення алгоритму DBSCAN, який забезпечує краще визначення кластерів у разі даних з нерівномірною щільністю. HDBSCAN автоматично визначає кількість кластерів, дозволяє виявляти кластери будь-якої форми та може обробляти шум у даних, що робить його підходящим для кластеризації атак з різними атрибутами (Виконується за допомогою пакета **hdbscan**), який на вихід дає нам множини систем за схожістю та множини атак за схожістю (рис. 7). Відповідно, якщо приходить нова атака з якимось набором атрибутів –з високою ймовірністю можна визначити до якої множини атак вона належить та знайти відповідну множину систем, які до неї мають бути стійкими.

Якщо ми бачимо, що система, яку атакують в режимі реального часу за симуляціями провалила більшість тестів на стійкість – задачею буде видозмінити чим її атрибути, які перемістять цю систему з множини *Вразливих* у множину *Стійких*. Алгоритм HDBSCAN працює в наступній послідовності:

1. Підготовка даних;
2. Виконання HDBSCAN кластеризації;
3. Побудова дендрограми для візуалізації ієрархії кластерів;
4. Виявлення точок, які не належать до жодного кластера;
5. Оцінка стійкості кожного кластера.

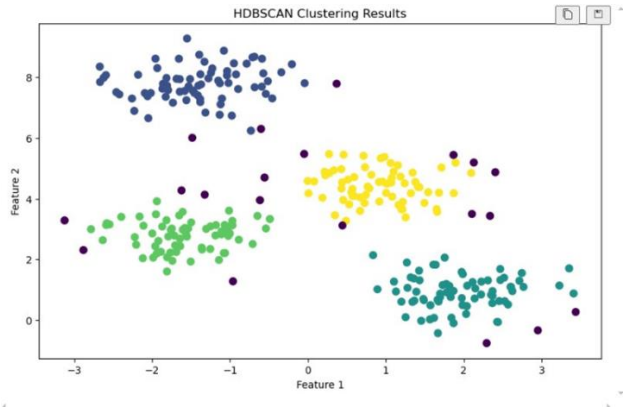

Рис. 7. Візуалізація поділу на кластери.

HDBSCAN автоматично позначає точки, які не належать до жодного кластера, як "шум". Це дозволяє виявляти аномалії у даних, тобто виявити властивості, які відрізняються від основних кластерів (рис. 7).

Заключним блоком моделі Побудова моделей оцінювання з використанням машинного навчання. За результатами симуляцій може будуватись оцінка систем щодо кіберстійкості, вразливості та здатності до відновлюваності. Для цього будується модель класифікації нової системи чи атаки, і ведеться пошук схожої на неї в множині синтезованих даних, аналізується результат симуляцій взаємодій цієї атаки з усіма системами, чи цієї системи з усіма атаками, і будується передбачення результату їх взаємодії, що дає оцінку до відновлюваності, та відповідно стійкість до загрози. Регресійна модель - алгоритм, який здатен передбачати неперервну змінну в залежності від набору атрибутів. Використовується для оцінки впливу довільної атаки на довільну систему шляхом побудови апроксимації кінцевої величини через наявні

параметри. На вхід маючи атрибути системи і атрибути атаки – застосовується метод підрахунку "Величини Впливу" атаки на систему, та рахується "Час відновлюваності".

Маючи у наступному циклі атрибути системи, величину впливу тієї чи іншої атаки та час відновлюваності – можна передбачити з певною точністю величину впливу та час відновлюваності для довільної іншої системи за тієї чи іншої атаки. Для цієї задачі використаємо **Random Forest Regressor,** алгоритм машинного навчання, який використовується для вирішення задач регресії. Він базується на методі ансамблювання і складається з багатьох дерев рішень. Алгоритм поєднує результати кількох дерев рішень, щоб покращити точність передбачень та знизити ризик переобчислення (overfitting):

$$\lambda \approx \frac{1}{N}\sum_{i=1}^{N} T_i(x), \qquad (9)$$

де $T_i(x)$ – прогноз *i*-ого дерева для вхідного значення *x*; N – кількість гілок у лісі.

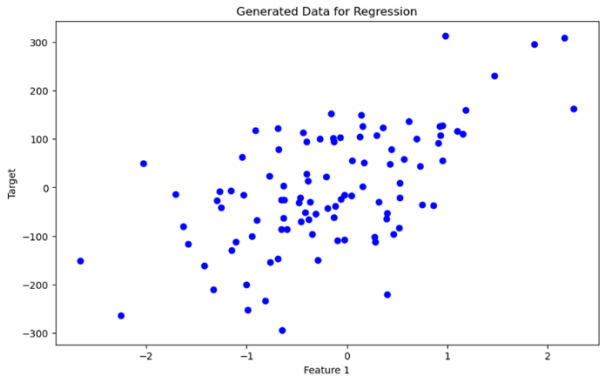

Рис. 8. Генерація даних

Послідовність роботи алгоритму наступна:

1.Підготовка даних (рис. 8);

2.Тренування Random Forest на навчальній вибірці (навчання моделі);

3.Візуалізація одного з дерев у лісі;

4.Визначення важливості ознак для прогнозування;

5.Оцінка моделі.

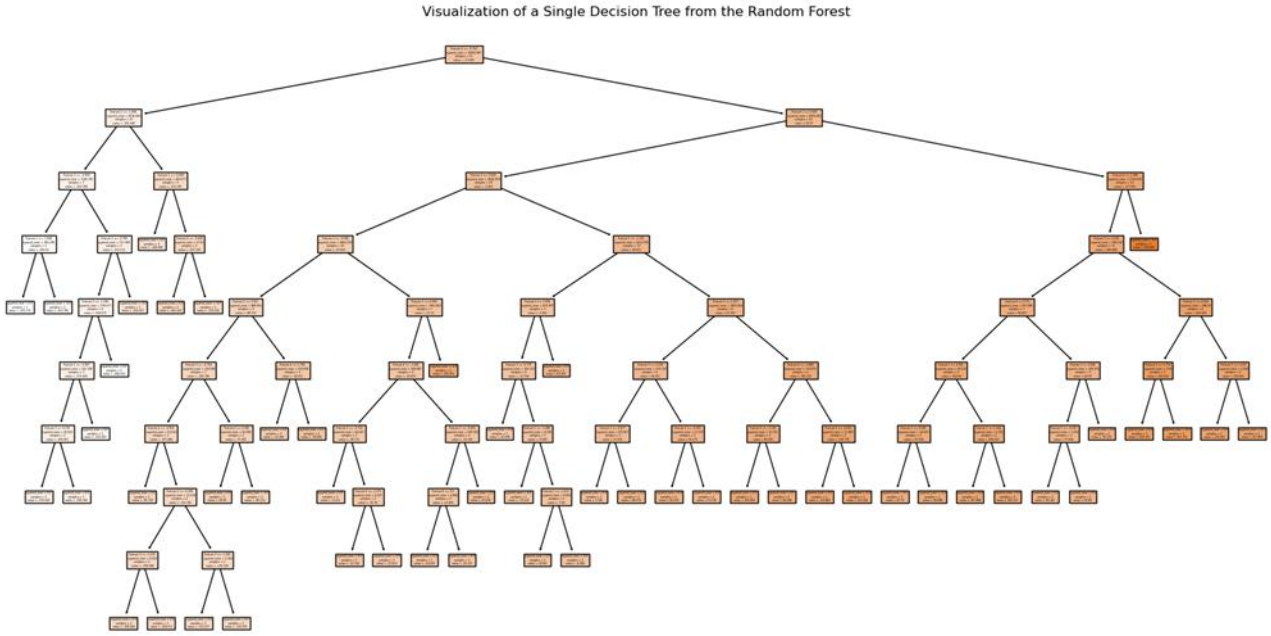

Рис. 9. Random Forest

Рис. 10. Цикл моделювання функціональних процесів

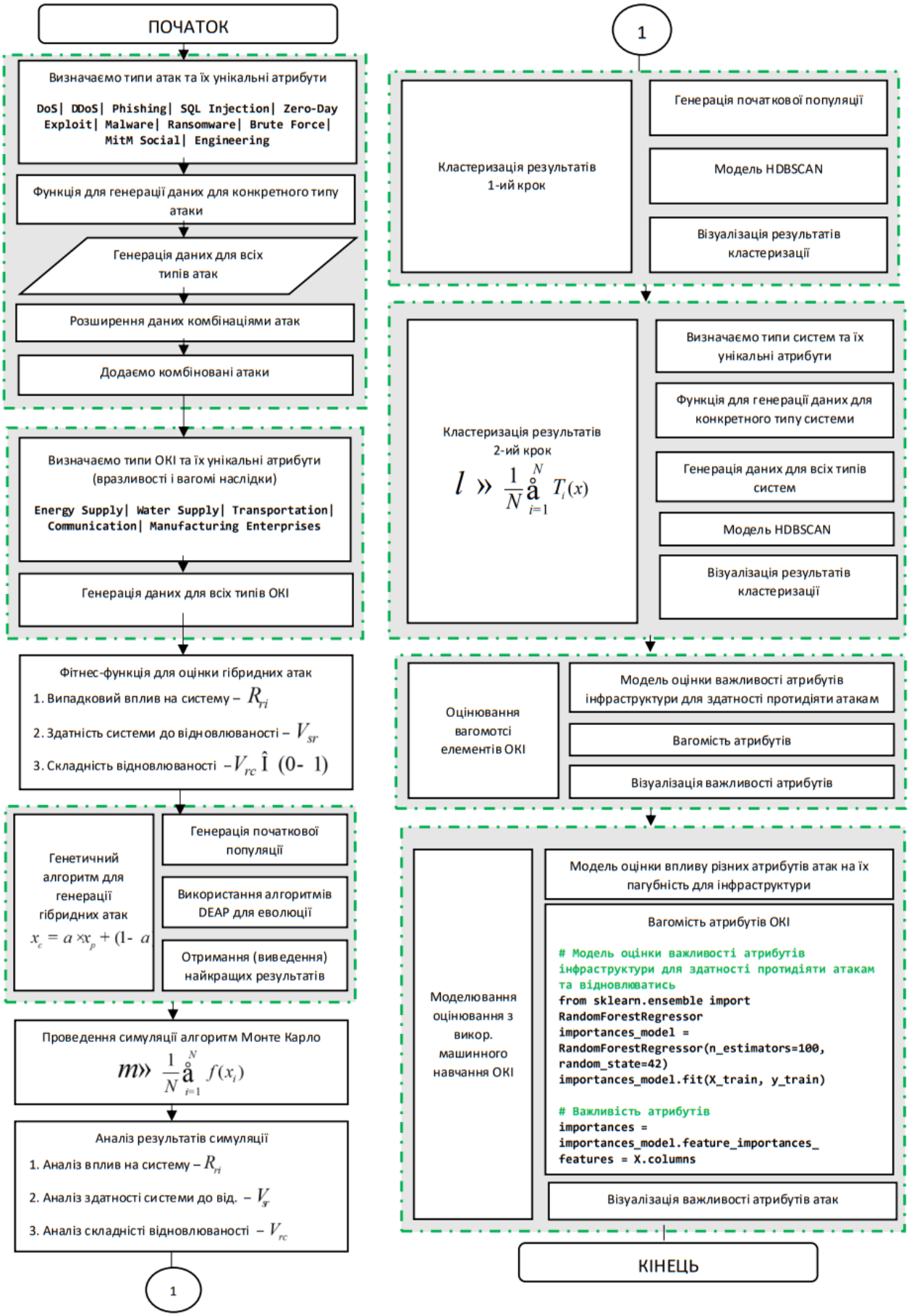

Рис. 11. Блок-схема моделі оцінювання кіберстійкості ІС ОКІ з використанням Random Forest Regressor

На рис. 9 одна гілка дерева Random Forest. Після побудови кожного дерева алгоритм об'єднує їх передбачення. У випадку регресії, результати обчислюються як середнє значення прогнозів усіх дерев. На рис.10 представлений спрощена послідовність основних елементів моделі, замкнених циклічно.

На рис.11 представлена модель оцінювання кіберстійкості ІС ОКІ з використанням Random Forest Regressor та всі її елементи (рис. 11).

Висновки. У статті запропоновано модель оцінювання кіберстійкості інформаційних систем об'єктів критичної інфраструктури в умовах комбінованих кібератак. Модель враховує різноманітні типи атак, такі як DoS, DDoS, фішинг, SQL-ін'єкції, шкідливе програмне забезпечення, атаки грубої сили, атаки «людина посередині», програми-вимагачі, атаки нульового дня та соціальна інженерія. Розроблена модель дозволяє оцінювати вплив атак на системи HMI та SCADA, які є основними компонентами критичної інфраструктури. За допомогою методу Монте-Карло здійснюється симуляція впливу атак, що дозволяє враховувати варіативність та випадковість атак. Генетичний алгоритм використовується для генерації гібридних атак, що дозволяє оптимізувати їхній вплив на системи. Модель також включає кластеризацію атак та систем за допомогою алгоритму HDBSCAN, що дозволяє ефективно оцінювати стійкість систем до певних типів атак. Застосування Random Forest Regressor дозволяє прогнозувати вплив атак та здатність систем до відновлення, що робить цю модель корисною для практичного використання в оцінці кіберстійкості критичної інфраструктури. Результати дослідження можуть бути використані для розробки заходів підвищення захищеності інформаційних систем об'єктів критичної інфраструктури та поліпшення їх здатності до відновлення після атак.

Список літератури.

[1]. Кібератаки Росії на Україну: критичні об'єкти під загрозою. / УКРІНФОРМ / URL: https://www.ukrinform.ua/rubric-ato/3579698-rosia-gotue-masovani-kiberataki-na-obekti-kriticnoi-infrastrukturi-ukraini-rozvidka.html (дата звернення: 19.07.2024).

[2]. російські війська поєднують кібернетичні та кінетичні атаки впродовж усієї війни — Держспецзв'язку / АРМІЯІНФОРМ / URL: https: // armyinform.com.ua/2023/11/10/rosijski-vijska-poyednuyut-kibernetychni-ta-kinetychni-ataky-vprodovzh-usiyeyi-vijny-derzhspeczzvyazku / (дата звернення: 20.08.2024).

[3]. Кібербезпека критичних інфраструктур: закордонний досвід та українські реалії. / DOI https: //doi.org/10.32850/sulj.2022.4.3.38 / URL: https://doi.org/10.32850 / sulj.2022.4.3.38 (дата звернення: 17.09.2024).

[4]. Російські хакери координують дії з військовими та посилюють атаки напередодні зими. / FORBES / URL: https://forbes.ua/company/rosiyski-khakeri-koordinuyut-dii-z-viyskovimi-ta-posilyuyut-ataki-naperedodni-zimi-yak-ukraina-protistoit-kiberata-kam-na-energosistemu-08112023-17242 (дата звернення: 22.08.2024).

[5]. Кібератака на Україну – не вперше і не востаннє? / Радіо Свобода / URL: https://www.radiosvoboda.org/a/kiberataka-na-ukrayinu-khto-ta-yak-protydiye/31655457.html (дата звернення: 21.09.2024)]. У звіті ДЦКЗ [2023 року кількість зареєстрованих кіберінцидентів зросла на 62,5% / Звіт оперативного центру реагування на кіберінциденти ДЦКЗ / URL: https: //ain.ua (дата звернення: 11.07.2024).

[6]. BlackEnergy: атака на енергетичну систему України / ESET / URL: https://www.eset.com/int/blackenergy-cyberattack (дата звернення: 19.07.2024).

[7]. Атака NotPetya: наслідки для України / CERT-UA / URL: https://cert.gov.ua/notpetya-attack (дата звернення: 16.07.2024).

[8]. CERT-UA: інсайдерські загрози та кіберзахист енергетики України / CERT-UA / URL: https:// cert.gov.ua/insider-threats (дата звернення: 19.08.2024)

[9]. V.Shypovskyi / Journal of Scientific Papers "Social Development and Security", Vol. 13, No. 3, –2023/ Decision-making process model for cybersecurity protection of critical infrastructure objects under the hybrid threats influence / DOI: https://doi.org/10.33445/sds. 2023.13.3.3.

[10]. Шиповський В.В. / Захист інформації. Том 25 № 1 (2023)/ Система показників оцінювання кіберстійкості інформаційних систем об'єктів критичної інфраструктури / DOI: https: // doi.org /10.18372/ 2410-7840.25.17597.

УДК 004.056 (477)

Shypovsky V. Cyber resilience assessment model information systems of critical objects infrastructures under the influence of hybrids cyber-attack using algorithms machine learning

Abstract. *The article presents a model for assessing the cyber resilience of information systems of critical infrastructure objects (CIO) under the influence of combined cyber-attacks. The model analyzes the impact of ten types of attacks, such as DoS, DDoS, phishing, malware, and others, on HMI and SCADA systems. The interaction between attacks and systems is modeled using the Monte Carlo method; a genetic algorithm is used to create hybrid attacks, and clustering with HDBSCAN allows for determining the resilience of systems to certain types of attacks. Prediction of attack consequences and recovery time is carried out using the Random Forest Regressor algorithm. The research results can be used to improve cyber defense measures of CIOs and enhance their ability to recover after cyber-attacks.*

Keywords*: cyber resilience, hybrid threats, critical infrastructure, HMI, SCADA, genetic algorithm, CIO, cyber-attack, information systems, recovery time, modeling, simulation, assessment, machine learning, cyber security.*

Шиповський Володимир Володимирович, ад'юнкт кафедри інформаційно-аналітичних технологій Національного університету оборони України.

Volodymyr Shipovskyi, adjunct professor of the Department of Information and Analytical Technologies of the National Defense University of Ukraine.

Отримано *25 травня 2024 року*, затверджено редколегією *26 червня 2024 року*