УДК 004.056

МОДЕЛЮВАННЯ ЕФЕКТІВ КІБЕРАТАК НА ОБ'ЄКТИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ З УРАХУВАННЯМ ЇХ ЗАХИЩЕНОСТІ

О. Т. Музичка-Скрипка[1], І. В. Стьопочкіна[1]

[1] Навчально-науковий Фізико-технічний інститут

Анотація

У зв'язку з постійною загрозою кібернетичник атак, які спряжені із фізичними атаками на енергетичну інфраструктуру України стає актуальною задача моделювання взаємодії об'єктів критичної інфраструктури. Робота орієнтована на розробку методів комплексного моделювання за допомогою комплексних мереж для аналізу вразливостей і стійкості системи. Результати роботи відрізняються обчисленням ступеню захищеності кіберфізичних систем та ймовірності успішної атаки, що враховуються при моделюванні. Результати сприятимуть розробці стратегій захисту, підвищуючи кібернетичну стійкість енергетичної мережі.

Ключові слова: Моттера Леї, моделювання, оцінювання ступеню захищеності, класи заходів безпеки

Вступ

Практичне значення цього дослідження зумовлене необхідністю прогнозування сценаріїв, викликаних кібератаками на мережі критичної енергетичної інфраструктури. Важливо встановити показники стійкості мережі до таких шкідливих впливів. Використання комп'ютерного моделювання є ефективним методом для чисельної оцінки критеріїв класифікації об'єктів як критичної інфраструктури. Ці критерії включають тяжкість можливих негативних наслідків від перебоїв, тривалість усунення цих наслідків, а також подальший негативний вплив на інші сектори.

У цій роботі обґрунтовується використання моделей, що дозволяють моделювати та оцінювати негативні впливи на енергетичні об'єкти, прогнозувати тривалість усунення наслідків та масштаб негативних впливів, використовуючи результати теоретичних та прикладних досліджень інфраструктур інших країн. Удосконалено алгоритм, що працює на основі моделі Моттера-Лая (M-L), який тепер може враховувати ймовірнісну природу збоїв об'єктів, спричинених зловмисним втручанням.

1. Методика оцінювання ступеню захищеності

Методика базується на Наказі Адміністрації Держспецзв'язку, який вводить чотири категорії захисту (рис 1).

Рис. 1. Ступінь зрілості організації

Ці категорії описують "ступінь зрілості" організацій у впровадженні кіберзахисту, визначаючи їх готовність відбивати кібератаки.

Розробка методики оцінки. Методика включає в себе використання кілька класів заходів безпеки, кожен з яких включає різні компоненти:

1. **Клас ID (Ідентифікація ризиків кібербезпеки):**
   - Управління активами (ID.AM).
   - Надання життєво важливих послуг (ID.BE).
   - Управління безпекою (ID.GV).
   - Оцінки ризиків (ID.RA).
   - Стратегії управління ризиками (ID.RM).
   - Управління ризиками постачання (ID.SC).
2. **Клас PR (Кіберзахист):**
   - Управління доступом (PR.AC).
   - Обізнаність та навчання (PR.AT).
   - Безпека даних (PR.DS).
   - Процедури кіберзахисту (PR.IP).
   - Технічне обслуговування (PR.MA).
   - Технології кіберзахисту (PR.PT).
3. **Клас DE (Виявлення кіберінцидентів):**
   - Виявлення аномалій (DE.AE).
   - Моніторинг (DE.CM).
   - Процедури виявлення інцидентів (DE.DP).

Кожен з цих класів оцінюється за шкалою, що визначається кількістю елементів у кожному підкласі, і таким чином визначається загальний бал захищеності.

1.1. Класифікація та оцінка компонентів

Кожен клас кіберзахисту оцінюється на основі кількості підкласів і компонентів в кожному з них. Для порівняння вищенаведених методів були створені наступні критерії:

- **Клас ID:**

$$X_j^{\mathrm{ID}} = N_{\mathrm{ID.AM}} + N_{\mathrm{ID.BE}} + N_{\mathrm{ID.GV}} + \\ + N_{\mathrm{ID.RA}} + N_{\mathrm{ID.RM}} + N_{\mathrm{ID.SC}}$$
$$X_j^{\mathrm{ID}} = 6 + 5 + 4 + 6 + 3 + 5 = 29. \quad (1)$$

- **Клас PR:**

$$X_j^{\mathrm{PR}} = N_{\mathrm{PR.AC}} + N_{\mathrm{PR.AT}} + N_{\mathrm{PR.DS}} + \\ + N_{\mathrm{PR.IP}} + N_{\mathrm{PR.MA}} + N_{\mathrm{PR.PT}}$$
$$X_j^{\mathrm{PR}} = 5 + 6 + 7 + 4 + 4 + 5 = 31. \quad (2)$$

- **Клас DE:**

$$X_j^{\mathrm{DE}} = N_{\mathrm{DE.AE}} + N_{\mathrm{DE.CM}} + N_{\mathrm{DE.DP}}$$
$$X_j^{\mathrm{DE}} = 4 + 5 + 6 = 15. \quad (3)$$

Визначення важливості класів. Вага кожного класу PN_j визначається за допомогою методу відносного ранжування, де сума всіх ваг дорівнює одиниці:

$$PN_j = \frac{1}{n}\sum_{i=1}^{n} P_j, \quad (4)$$
$$\sum_{j=1}^{n} PN_j = 1.$$

2. Розрахунок універсальної множини

Зміни параметра X_j, що варіюється від 0 до N_j, відображаються на універсальну множину:

$$U = [0, L-1] \quad (5)$$

$$U_j' = \frac{(L-1)\cdot(X_j' - \underline{X}_j)}{(\overline{X}_j - \underline{X}_j)} \quad (6)$$

де X_j' — фактичне значення балів, отримане під час оцінки.

2.1. Функції приналежності

Функції приналежності для нечітких термів визначаються як:

$$\mu_i^j(U_j') = \frac{1}{\left(1 + (U_i' - i + 1)^2\right)^{PN_j}}, \quad (7)$$

де i — номер терма, j — номер класу. У формулі U_j' відіграє роль нормалізованої оцінки, яка враховує відстань між фактичним значенням показника і базовим рівнем $\underline{X}_j$.

Показник рівня захищеності. Загальний показник рівня захищеності розраховується шляхом агрегування значень функцій приналежності по всім класам і термам:

$$\mu_S(X_j') = MAX_i = 1^L MIN_j = 1^n \mu_i^{j(j)}, \quad (8)$$

де операції $\vee$ та $\wedge$ знаходяться як максимальне та мінімальне значення відповідно.

Таблиця 1. Коефіцієнти важливості класів та відповіді експертів

№ зап.	1	2	3	4	$P_j,\ j = 1\ldots4$	$PN_j,\ j = 1\ldots4$	$X_j',\ j = 1\ldots4$
1	5/5	3.1	3.8	4.8	12.7	0.37	1.5
2	1.9	5/5	3.6	3.9	10.4	0.31	3.5
3	1.2	1.4	5/5	4.2	7.8	0.23	2
4	0.2	1.1	0.8	5/5	3.1	0.09	3.6

Приклад. Нехай ми розглядаємо чотири класи з різними шкалами оцінки. Визначення важливості запитань проводиться групою з п'яти експертів. В результаті аналізу формуються кінцеві показники рівня захищеності для конкретного об'єкта.

Розглядаємо 4 класи (табл. 1):

- 1-й клас оцінюється по шкалі 0...3,
- 2-й клас оцінюється по шкалі 0...5,
- 3-й клас оцінюється по шкалі 0...10,
- 4-й клас оцінюється по шкалі 0...4.

В табл. 1 експертами розподіляються їхні 5 голосів між кожними двома відповідями, відповіді одержуються експертами, які проводять оцінку об'єкта критичної інфраструктури.

В результаті ми визначаємо, якого рівня є захищеність об'єкта критичної інфраструктури, який розглядається.

У відповідності до цього рівня будемо встановлювати імовірність у алгоритмі каскадних відключень за методом Моттера-Леі.

Для цього будемо припускати, що максимально висока ймовірність атаки відповідає Низькому рівню захищеності, а максимально низька — Високому рівню. При цьому припустимо, що така ймовірність коливається у межах від 5% до 95%. Тоді співставимо одержаним результатам ймовірність відповідно до табл. 2, де відповідні ймовірності зазначені з рівним інтервалом у діапазоні від 5% до 95%.

Таблиця 2. Відповідність захищеності ймовірності атаки

Рівень захищеності	Модельна ймовірність P успішної атаки
Н	95%
НС	72.5 %
С	50%
ВС	27.5 %
В	5 %

3. Моделювання

Приклад коду для реалізації розрахунків. Наведемо приклад вихідного коду програми, що реалізує розрахунки з попереднього розділу.

Вхідні дані до нього наведено на лістінгу 1, вихідний код програми та результати його виконання — на лістінгах 2 та 3 відповідно.

```
# Grades for each class
scores = {
 'ID': [20, 18, 17, 15, 19, 16], # для ID класу
 'PR': [18, 17, 20, 18, 15, 17], # для PR класу
 'DE': [15, 16, 15] # для DE класу
}

# Maximum points for each subclass
max_scores = {
 'ID': [30, 30, 30, 30, 30, 30],
 'PR': [25, 25, 25, 25, 25, 25],
 'DE': [20, 20, 20]
}

# Weights for each class (assumedly calculated by experts)
weights = {
 'ID': 0.5,
 'PR': 0.3,
 'DE': 0.2
}

# Number of terms (L)
L = 5
```

Лістинг 1. Вихідні дані моделювання

```
# Розрахунок нормованих значень U для кожного класу
U = {cls: (np.array(scores[cls]) / np.array(max_scores[
    cls])) * (L - 1) for cls in scores}

# Виведення нормованих значень U
print("Normalized U values for each class:")
for cls, values in U.items():
 print(f"{cls}: {values}")

# Функція приналежності
def membership_function(U, i, weight):
 return 1 / (1 + (U - i + 1)**2 * weight)

# Розрахунок функцій приналежності для кожного терму і класу
mu = {cls: np.array([membership_function(u, i, weights[
    cls]) for u in U[cls]]) for cls in U for i in range
    (L)}

# Виведення функцій приналежності
print("\nMembership functions for each class and term")
for cls, matrix in mu.items():
 print(f"{cls}:")
 print(matrix)

# Розрахунок загального показника рівня захищеності
overall_protection_level=np.min([np.max(mu[cls], axis=0)
     for cls in mu])

# Виведення загального показника рівня захищеності
print("\nGeneral indicator of security level:",
    overall_protection_level)
```

Лістинг 2. Розрахунок функцій приналежності

```
Normalized U values for each class:
ID: [2.66666667 2.4 2.26666667 2. 2.53333333 2.13333333]
PR: [2.88 2.72 3.2 2.88 2.4 2.72]
DE: [3. 3.2 3. ]

Membership functions for each class and term
ID:
[0.94736842 0.84745763 0.78809107 0.66666667 0.90180361
    0.726979 ]
PR:
[0.99569858 0.97702048 0.98814229 0.99569858 0.90252708
    0.97702048]
DE:
[1. 0.99206349 1. ]

General indicator of security level: 0.9473684210526315
```

Лістинг 3. Результати виконання програми

Підготовка для моделювання. Візьмемо стару карту енергосистеми України, яку отримано з офіційного сайту Міненерго (рис. 2). Проаналізуємо новини та карту deepstatemap на сьогоднішній день та врахуємо це при моделюванні.

В результаті було сформовано граф взаємодії об'єктів критичної інфраструктури, наведений на рис. 3.

Моделі для каскадних ефектів у мережах об'єктів. При моделюванні розвитку подій внаслідок атак, в тому числі і кібернетичних, необхідно враховувати каскадні ефекти, які виникають в комплексній мережі. Розглянемо, яким чином це може бути зроблено.

У статті [1] запропоновано модель Моттера-Лая каскадного процесу відключень електроенергії в мережі критичної запропоновано модель каскадного процесу відключень в мережі критичної інфраструктури. Модель використовує топологічні особливості досліджуваної мережі і дозволяє моделювати процес знеструмлення з урахуванням можливості впливу на всю множину вузлів мережі, а не тільки на вузлів мережі, а не тільки на сусідні. Основна ідея моделі полягає в дослідженні результуючої зв'язності мережі в кінці процесу каскадного відключення.

У статті [2] розглянуто питання оцінки та пом'якшення наслідків каскадних відмов розглянуто питання оцінки та пом'якшення наслідків каскадних відмов. Автори пропонують метод оцінки ризиків, який враховує залежності між інфраструктурами.

У статті [3] аналізується каскадний вплив кібератак на системи безпечного водопостачання, водоочистки та розподілу води, враховуючи взаємозалежність критично важливих підгалузей та об'єктів інфраструктури. Пропонуються моделі зловмисника та атаки, інваріанти нормальних процесів, а також аномалії. Для дослідження каскадних ефектів використовуються програмні інструменти. Алгебраїчний підхід до моделювання каскадних та взаємодійних ефектів описаний у [4].

Каскадні ефекти в складних системах з різною мережевою топологією досліджено в [5].

Автори використовують графовий підхід і наводять співвідношення важливих показників, порівнюються набори моделей (зокрема, модель Уатта, деревоподібний аналітичний підхід, модель Ньюмана та інші). Обґрунтовано, що SIR-подібні епідеміологічні моделі можуть бути використані для моделювання каскадних ефектів моделювання каскадних ефектів у різних мережах.

У статті [6] розглянуто питання стійкості до збоїв та атак. Основна увага приділяється зроблено на статистичній механіці мережевої динаміки, яка вимагає наявності великої кількості даних для для дослідження еволюції мережі.

У роботі [7] досліджено топологічну структуру та стійкість електроенергетичної мережі. Було введено деякі метрики для оцінки ефективності та стійкості. Розрахунок цих метрик може бути використа-

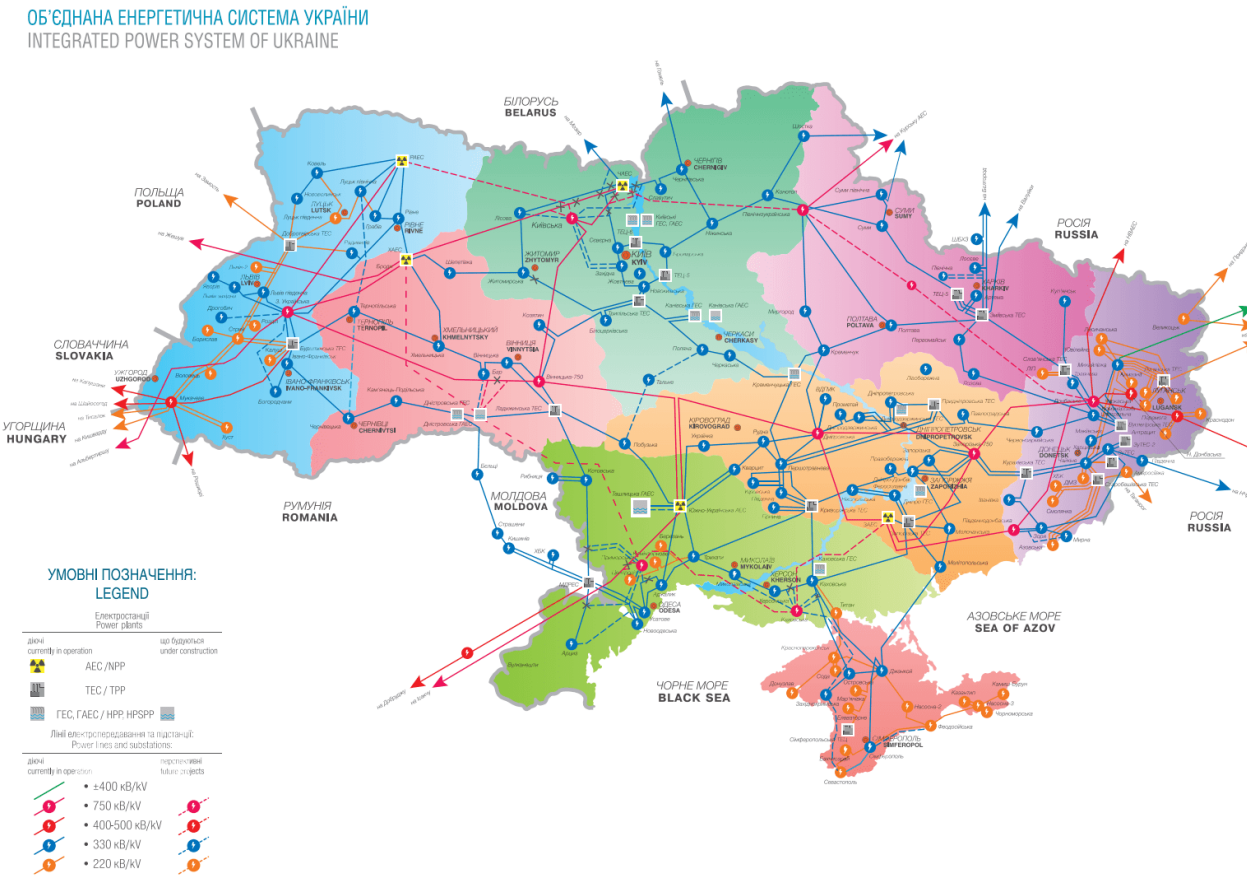

Рис. 2. Карта енергосистеми України
(https://mev.gov.ua/storinka/nabory-vidkrytykh-danykh-haluzi)

ний для отримання цих метрик може бути використаний для отримання вхідних параметрів для інших моделей. В роботі [8] розглянуто структурну вразливість Північноамериканської електромережі. Автори стверджують, що мережа є стійкою до більшості видів збурень.

В [9] автори представляють нову модель динаміки поширення каскаду відмов. Модель враховує враховує затримки взаємодії між вузлами. Також автори розглядають питання зменшення шкоди, що є перевагою роботи.

Робота [10] досліджує штучні мережі, зокрема випадкові графи ER та безмасштабні мережі, аналізуючи стратегію випадкового видалення вузлів на прикладі Інтернету. Більшість моделей, що розглядалися, використовують великий набір параметрів, що значно впливає на результати моделювання. Через невизначеність характеристик атак та брак спостережень, ідентифікація всіх параметрів часто є неможливою. Тому ми обрали моделі, зокрема Моттера-Лая та SIS з сімейства SIR-подібних моделей, параметри яких можна отримати в практичних ситуаціях.

Моттера Леї. Метод Моттера-Леї є ключовим інструментом у вивченні стійкості складних мереж, зокрема енергосистем. Модифікація цього алгоритму була запропонована в роботі [11]. Ця робота дає методику для розрахунку імовірності p, необхідної в модифікації даного алгоритму, на основі вітчизняної нормативної бази.

Висновки

У роботі було представлено комплексне дослідження взаємодії об'єктів критичної інфраструктури в галузі енергопостачання. Методика оцінювання була використана для визначення вразливих місць у енергетичній інфраструктурі, що можуть стати мішенями для атак. Дослідження підкреслює важливість комплексного підходу в аналізі стійкості енергетичної інфраструктури та необхідність безперервного вдосконалення методів оцінки та управління кіберзахистом на всіх рівнях.

Запропонована методика врахування захищеності об'єктів критичної інфраструктури базується на рекомендаціях нормативних додкументів, та дозволяє підвищити точність оцінювання імовірності успішної кібернетичної атаки на об'єкт. У комплексі з підходом на основі алгоритма Моттера-Лая, це дозволяє виявити наявність вразливих місць у енергетичній інфраструктурі, що можуть стати мішенями для атак. Прогнозування та моделювання стійкості енергетичної інфраструктури з урахуванням цих факторів може передбачити поріг стійкості енерге-

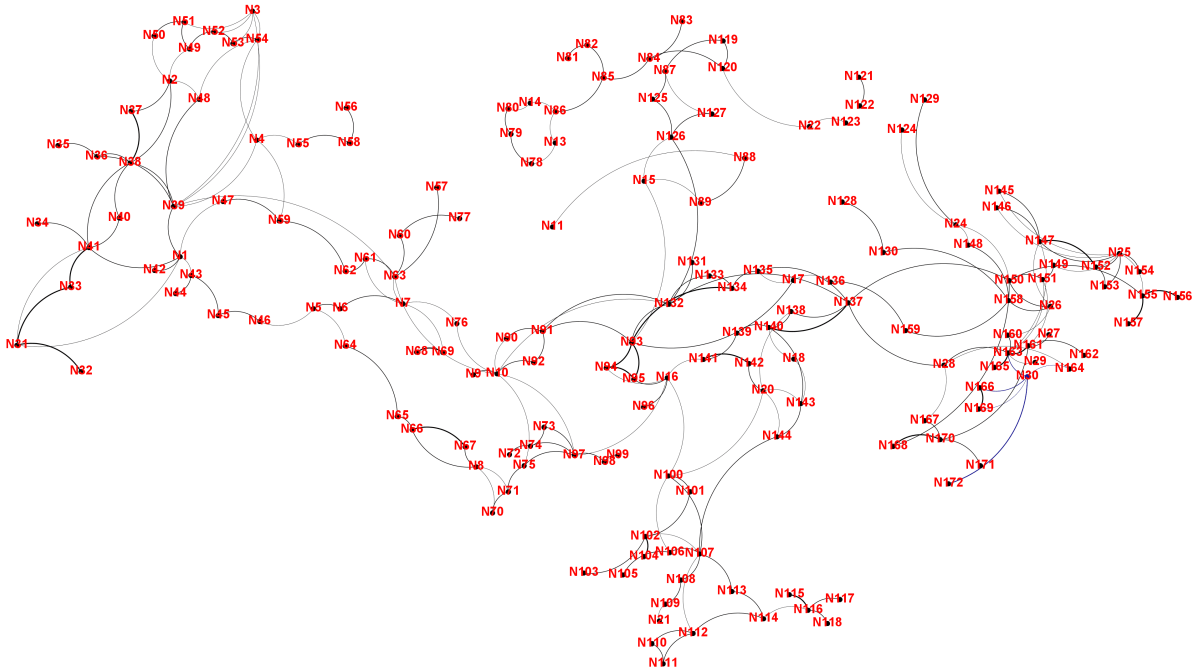

Рис. 3. Граф, який відповідає енергосистемі України

тичної системи та інші показники, які дозволять зробити заходи захисту більш зосередженими та успішними.

Перелік використаних джерел

1. *Motter A., Lai Y.-C.* Cascade-based Attacks on Complex Networks // Physical review. E, Statistical, nonlinear, and soft matter physics. — 2003. — Jan. — Vol. 66. — P. 065102. — DOI: 10.1103/PhysRevE.66.065102.
2. *Kotzanikolaou P., Theoharidou M., Gritzalis D.* Cascading Effects of Common-Cause Failures in Critical Infrastructures // International Conference on Critical Infrastructure Protection. — 2013. — DOI: 10.1007/978-3-642-45330-4_12.
3. Cascading effects of cyber-attacks on interconnected critical infrastructure / V. Palleti, S. Adepu, V. Kumar Mishra, A. Mathur // Cybersecurity. — 2021. — Dec. — Vol. 4. — DOI: 10.1186/s42400-021-00071-z.
4. *Adam E. M., Dahleh M. A.* On the mathematical structure of cascade effects and emergent phenomena. — 2019. — Nov. — DOI: 10.48550/arXiv.1911.10376.
5. *Hackett A. W.* Cascade dynamics on complex networks // University of Limerick. — 2011.
6. *Albert R., Barabasi A.-L.* Statistical Mechanics Of Complex Networks // Reviews of Modern Physics. — 2001. — June. — Vol. 74. — DOI: 10.1103/RevModPhys.74.47.
7. Power grid vulnerability: A complex network approach / S. Arianos, E. Bompard, A. Carbone, F. Xue // Chaos: An Interdisciplinary Journal of Nonlinear Science. — 2009. — Лют. — Т. 19, № 1. — С. 013119. — ISSN 1054-1500. — DOI: 10.1063/1.3077229.
8. *Albert R., Albert I., Nakarado G.* Structural vulnerability of the North American power grid. // Physical review. E, Statistical, nonlinear, and soft matter physics. — 2004. — Vol. 69 2 Pt 2. — P. 025103. — DOI: 10.1103/PhysRevE.69.025103.
9. Modelling of cascading effects and efficient response to disaster spreading in complex networks / K. Peters, L. Buzna, D. Helbing, [et al.] // Int. J. Critical Infrastructures. — 2008. — Vol. 4. — DOI: 10.1504/IJCIS.2008.016091.
10. *Crucitti P., Latora V., Marchiori M.* Model for cascading failures in complex networks // Physical review. E, Statistical, nonlinear, and soft matter physics. — 2004. — Трав. — Т. 69. — С. 045104. — DOI: 10.1103/PhysRevE.69.045104.
11. Cyber Attacks Cascading Effects Simulation for Ukraine Power Grid / O. Novikov, G. Vedmedenko, I. Stopochkina, M. Ilin // Selected Papers of the XXI International Scientific and Practical Conference "Information Technologies and Security" (ITS 2021). — 2021. — Dec. — URL: http://ceur-ws.org/Vol-3241.