зйомки УФ-камерою: для цього дрон зависає в повітрі на 5–10 с, а лічильник імпульсів приладу видає усереднений показник розрядної активності.

Отже, впровадження технологій дистанційного моніторингу на основі квадрокоптерів значно покращує керування ЛЕП. Водночас квадрокоптери дають змогу швидко та безпечно обстежувати важкодоступні ділянки без ризику для персоналу, скорочуючи час і витрати на інспекцію. Їх можна використовувати без відключення ліній, що знижує ризики перебоїв енергопостачання.

СПИСОК ВИКОРИСТАНИХ ПОСИЛАНЬ

1. Зайцев Є. О., Кучанський В. В. Аналіз методів контролю втрат потужності на корону в лініях електропередавання. *Технічні науки в Україні: сучасні тенденції розвитку:* Всеукраїнська інтернет-конференція студентів, аспірантів та молодих вчених (20–21 листопада 2019 р., Київ, Україна). С. 14–16.
2. Кучанський В. В., Зайцев Є. О. Технічні засоби аеродіагностування високовольтного електроустаткування. *Відновлювана енергетика та енергоефективність у XXI столітті:* збірник матеріалів XX Міжнародної науково-практичної конференції (19–20 травня 2023 р., Київ). Київ: Інститут відновлюваної енергетики НАН України, 2023. С. 156–157.
3. Sensing method using multiple quantities for diagnostic of insulators in different ambient conditions / B. Dolník, L. Šárpataky, P. Havranet et al. *Sensors.* 2022. Vol. 22, № 4. P. 1376. DOI: 10.3390/s22041376.
4. Putra N. R. M., Sartika N., Rachmawati R. The study on leakage current waveform characteristics and computer simulation of ceramic insulator under artificial tropical condition. *2018 12th International Conference on the Properties and Applications of Dielectric Materials (ICPADM). IEEE, Xi'an.* 2018. P. 320–323. DOI: 10.1109/ICPADM.2018.8401273.
5. Stress control methods on a high voltage insulator: A review / A. Al-Gheilani, A. Rowe, W. Li et al. *Energy Procedia.* 2017. Vol. 110. P. 95–100. DOI: 10.1016/j.egypro.2017.03.112.

СУЧАСНІ ЗАГРОЗИ ТА КІБЕРАТАКИ НА ВАЖЛИВІ ІНФОРМАЦІЙНІ СТРУКТУРИ

Махнов Я. Г.[1*], Половенко Л. П.[2], Загоруйко Л. В.[3***]**

[1,2,3]*Донецький національний університет імені Василя Стуса, Вінниця (Україна)*

[*]e-mail: makhnov.ya@donnu.edu.ua

[**]e-mail: l.polovenko@donnu.edu.ua

[***]e-mail: l.zahoruiko@donnu.edu.ua

Сьогодні одна з найбільш серйозних загроз національній безпеці – кібератаки на важливі інформаційні структури. Такі атаки відбуваються постійно. З початку повномасштабної війни росія щомісяця проводить від 102 до 293 кібератак, левова частка яких припадає на критичну інфраструктуру. Під прицілом ворога постійно перебуває українська енергетика. Тільки у 2023 році, згідно з даними Держспецзв'язку, було зафіксовано приблизно 55 кібератак на енергооб'єкти [1]. Масштаби кібероперацій проти України неухильно зростають, причому в рф на національному рівні запроваджується система масштабування кіберагресії. З початку великої війни хакерів координує один центр. Активно залучаються студенти технічних та військових вишів, яких системно навчають хакерству, впроваджуються

технології синтетичного штучного інтелекту. Задіюються хакерські підрозділи Головного розвідувального управління російської армії – такі структури ще називають хакерами, спонсорованими державою (state-sponsored hackers). У 2024 році зафіксовано понад 800 спроб кібератак ворога на державні установи та сервіси.

Російські хакери використовують різні підходи: від сканування ІТ-периметру до, наприклад, DDoS-атак – перевантаження сервісу запитами для того, щоб його «покласти». Під час однієї з DDoS-атак на «Укренерго» кількість запитів могла перевищувати 5 млн за декілька годин. Росіяни комбінують атаки ракетами і дронами з кібератаками. Злам найбільшого в Україні мобільного оператора, який відбувся у грудні 2023 року, згідно з даними ГУР та СБУ, міг бути відповіддю на кібертатаку на податкову систему росії [2]. Це вкотре довело, що, окрім конвенційної війни, триває і кіберпротистояння.

Кіберзагрози постійно еволюціонують, і зловмисники використовують все більш витончені методи для обходу традиційних систем безпеки. Модель виявлення аномалій дає змогу виявляти нові, невідомі типи атак, які ще не мають сигнатур, здатна адаптуватися до змін у поведінці системи та користувачів, що робить її актуальною та перспективною у сучасних умовах навіть у динамічних середовищах.

Хоча моделі виявлення аномалій можуть мати вищий рівень false positive спрацьовувань, порівняно з моделями на основі сигнатур, сучасні методи машинного навчання та аналізу даних дають змогу знизити цей рівень, підвищуючи точність виявлення.

Розглянемо модель виявлення вторгнень, яка базується на методах класифікації та попереднього аналізу даних. Для реалізації запропонованої моделі виявлення вторгнень використовувались такі алгоритми класифікації: k–nearest neighbors (KNN), Gaussian Naive Bayes (GNB), Random Forest Classifier (RFC), Support vector machine (SVM). Ці алгоритми були вибрані через те, що в них доволі різні механізми класифікації й відповідно різні результати аналізу.

У табл. 1 представлені результати роботи алгоритмів у метриках Precision, Recall та F1 score: для двох класів – Normal, який відповідає «нормальній» поведінці користувачів, та Attacks, який відповідає двом класам атак – R2L та U2R.

Таблиця 1. Результати роботи алгоритмів класифікацій

Name	**Normal**			**Attacks**		
	precision	*recall*	*F1 score*	*precision*	*recall*	*F1 score*
KNN	0.99	0.99	0.99	0.95	0.91	0.94
GNB	0.98	0.97	0.97	0.08	0.09	0.08
RFC	0.99	0.99	0.99	0.99	0.93	0.96
SVM	0.93	0.89	0.91	0.82	0.76	0.81

Із представлених у таблиці даних бачимо, що алгоритм GNB має доволі високі результати у виявленні класу Normal, але у випадку класу Attacks алгоритм спрацював слабо і виявив дуже малу кількість атак. Низькі значення показників Precision і Recall вказують на те, що кількість помилок FP та FN достатньо велика відносно кількості атак. Зазначимо, що наші дані не є збалансованими, тому для нас метрики Precision та Recall є набагато інформативнішими, ніж показник алгоритмів Accuracy.

Аналіз представлених у табл. 1 алгоритмів дає змогу визначити, який з них показав кращі результати і найбільше підходить для вирішення поставлених задач. Під час дослідження було виявлено, що кращим алгоритмом класифікації для виявлення атак R2L та U2R є Random Forest. Цей алгоритм показав і хороші результати Precision та Recall, 99 % та 93 % відповідно, і низький відсоток помилок FP та FN, 0.04 % та 0.07 % відповідно.

Наступними за оцінкою якості, після Random Forest Classifier, ідуть k–nearest neighbors та Support vector machine.

Вибір моделі виявлення аномалій для дослідження обґрунтований її актуальністю, універсальністю, адаптивністю, здатністю знижувати спрацювання false positive, виявляти складні атаки та перспективами розвитку. Ця модель є потужним інструментом у боротьбі з кіберзагрозами та має потенціал для подальшого вдосконалення та застосування у різних сферах. Запропонована модель може бути хорошим доповненням до стандартних IDS, що може покращити систему безпеки мережі загалом.

СПИСОК ВИКОРИСТАНИХ ПОСИЛАНЬ

1. Ольга Чайка. Російські хакери координують дії з військовими та посилюють атаки напередодні зими. Як Україна протистоїть кібератакам на енергосистему. *Журнал Forbes Ukraine.* 2023. URL: http://surl.li/wlzsgw
2. Злам федеральної податкової служби рф – деталі чергової кіберспецоперації *ГУР.* 2023. URL: https://gur.gov.ua/content/zlam-federalnoi-podatkovoi-sluzhby-rf-detali-cherhovoi-kiberspets-operatsii-hur.html
3. D-SCIDS: Distributed softcomputing intrusion detection system / A. Ajit, J. Ravi, T. Johnson, Y. H. Sang. *Journal of Network and Computer Applications*. 2007. Vol. 30, № 1. P. 81–98.
4. Bridges S. M., Rayford M. V. Fuzzy data mining and genetic algorithms applied to intrusion detection. *National Institute of Standards and Technology*. 2003. URL: https://www.researchgate.net/publication/2481632_Fuzzy_Data_Mining_And_Genetic_Algorithms_Applied_To_Intrusion_Detection
5. Chou T. S., Yen K. K., Luo J. Network Intrusion Detection Design Using Feature Selection of Soft Computing Paradigms. *Journal of Computaional Intelligence.* 2016. Vol. 4, № 3. P. 196–208.