**CУЧАСНІ ЗАГРОЗИ ТА КІБЕРАТАКИ НА ВАЖЛИВІ ІНФОРМАЦІЙНІ СТРУКТУРИ**

**Махнов Я.Г1, Половенко Л.П. 2, Загоруйко Л.В.2,\***

*1,2,3Донецький національний університет імені Василя Стуса,*

*м. Вінниця, Україна*

1e-mail: makhnov.ya@donnu.edu.ua

2e-mail: l.polovenko@donnu.edu.ua

3e-mail: l.zahoruiko@donnu.edu.ua

На даний момент одна з самих 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 в 2023 році, згідно даних Держспецзв’язку, було зафіксовано близько 55 кібератак на енергооб’єкти [1]. Масштаби кібероперацій проти України неухильно зростають, причому в РФ на національному рівні запроваджується система масштабування кіберагресії. Із 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](https://www.cyberdaily.au/security/9285-3-things-you-need-to-know-about-state-sponsored-hackers" \t "_blank)). 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 в грудні 2023 року, згідно даних 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 дозволяє 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 дозволяють знизити цей рівень, підвищуючи точність виявлення.

Розглянемо модель виявлення вторгнень, яка базується на методах класифiкацiї та попереднього аналiзу даних.

Для реалiзацiї запропонованої моделi виявлення вторгнень використовувались такi алгоритми класифiкацiї: K–nearest Neighbors (KNN), Gaussian naive Bayes (GNB), Random Forest Classifier (RFC), Support V ector Machine (SV M). Цi алгоритми були вибранi в силу того, що в них достатньо рiзнi механiзми класифiкацiї й вiдповiдно до цього рiзнi результати аналiзу.

В табл. 1 представленi результати роботи алгоритмiв в метриках Precision, Recall та F1–score, для двох класiв – Normal, який вiдповiдає «нормальнiй» поведiнцi користувачiв, та Attacks, який вiдповiдає двом класам атак R2L та U2R.

Таблиця 1. Результати роботи алгоритмiв класифікацій

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | 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 |
| SV M | 0.93 | 0.89 | 0.91 | 0.82 | 0.76 | 0.81 |

З представлених в таблицi даних ми баччимо, що алгоритм GNB має досить високі результати в виявленнi Normal класу, але у випадку класу Attacks, алгоритм спрацював слабо i виявив дуже малу кiлькiсть атак. Низькі значення показників Precision i Recall вказують на те, що кiлькiсть помилок FP та FN достатньо велика вiдносно кiлькостi атак. Вiдмiтимо, що нашi данi не є збалансованими, саме тому для нас метрики Precision та Recall є набагато iнформативнiшими, нiж показник Accuracy алгоритмiв.

Аналіз представленіих в табл. 1 алгоритмів, дозволяє визначити, який з них показав кращi результати i найбільше пiдходить для вирiшення поставлених задач. В ходi дослiдження було виявлено, що кращим алгоритмом класифiкацiї для виявлення атак R2L та U2R є Random Forest. Цей алгоритм показав, як хорошi результати Precision та Recall, 99 % та 93 % вiдповiдно, так i маленький вiдсоток помилок FP та FN, 0.04 % та 0.07 % вiдповiдно.

Наступними за оцiнкою якостi, пiсля Random Forest Classifier, iдуть K–nearest Neighbors та Support Vector Machine.

Вибір моделі виявлення аномалій для дослідження обґрунтований її актуальністю, універсальністю, адаптивністю, здатністю знижувати false positive спрацювання, 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 мережi вцiлому.

**Перелік джерел посилання:**

1. Ольга Чайка. Російські хакери координують дії з військовими та посилюють атаки напередодні зими. Як Україна протистоїть кібератакам на енергосистему. 2023. URL: <https://forbes.ua/company/rosiyski-khakeri-koordinuyut-dii-z-viyskovimi-ta-posilyuyut-ataki-naperedodni-zimi-yak-ukraina-protistoit-kiberatakam-na-energosistemu-08112023-17242>
2. Злам федеральної податкової служби рф ― деталі чергової кіберспецоперації ГУР. 2023. URL: <https://gur.gov.ua/content/zlam-federalnoi-podatkovoi-sluzhby-rf-detali-cherhovoi-kiberspetsoperatsii-hur.html>
3. Ajit Abraham, Ravi Jain, Johnson Thomas, Sang Yang Han “D-SCIDS: Distributed softcomputing intrusion detection system”. *Journal of Network and Computer Applications*. 2007. Vol. 30, no. 1. Р. 81-98.
4. Susan M. Bridges and M. Vaughn Rayford. 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. and Luo J. Network Intrusion Detection Design Using Feature Selection of Soft Computing Paradigms. *Journal of Computaional Intelligence*. 2016. Vol. 4, no. 3. Р. 196-208.