господарство більш екологічним. Крім того, дрони можуть працювати в місцях, де важко використовувати традиційну техніку, наприклад на перезволожених ґрунтах або на складному рельєфі.

Таким чином, інтеграція БПЛА та систем автопілотування є важливим напрямом розвитку сучасної агроінженерії. Використання цих технологій дозволяє підвищити точність польових робіт, зменшити витрати ресурсів і забезпечити ефективний моніторинг посівів. Для України це питання має особливе значення в умовах воєнного стану та необхідності максимально ефективного використання аграрного потенціалу. У майбутньому роль таких систем лише зростатиме, адже розвиток цифрових технологій відкриває нові можливості для автоматизації аграрного виробництва.

Список використаних джерел:

1. Збірник тез доповідей XXV Міжнародної наукової конференції "Сучасні проблеми землеробської механіки" (17–19 жовтня 2024 р.)
2. Збірник студентських наукових праць СІЛЬСЬКОГОСПОДАРСЬКІ НАУКИ № 2(10), 2023 ВНАУ

Abstract: *This paper looks at the integration of drones and autopilot systems into modern agricultural engineering. It analyzes the main types of agrodrones, what they do, and the technical details of their navigation systems. Special attention is given to RTK technology, the ability to fly automatically, and how drones work with digital platforms for precision farming. The paper also looks at the future of using these technologies in Ukraine.*
Keywords: *UAV, agrodrone, autopilot, precision farming, RTK navigation, crop monitoring.*

Науковий керівник:
Борян Л.О.,
старший викладач кафедри економічної кібернетики, комп'ютерних наук та інформаційних технологій, Миколаївський національний аграрний університет

УДК 004.056.5

Застосування алгоритмів кластеризації для виявлення підозрілої активності в мережах аграрних підприємств

Хан Володимир,
здобувач вищої освіти спеціальності 122 Комп'ютерні науки
Миколаївський національний аграрний університет,
м. Миколаїв, Україна

Анотація. *У роботі досліджується застосування алгоритмів кластеризації для виявлення підозрілої активності в комп'ютерних мережах аграрних підприємств. Розглянуто сучасні підходи до аналізу мережевого трафіку та методи машинного навчання, які використовуються для виявлення аномалій у великих масивах даних. Особливу увагу приділено алгоритмам K-means, DBSCAN та ієрархічній кластеризації. Проаналізовано можливості використання мови програмування Python та бібліотек Pandas, NumPy і Scikit-learn для реалізації моделей кластеризації та аналізу мережевого трафіку. Запропонований підхід дозволяє підвищити ефективність виявлення кіберзагроз і забезпечити більш високий рівень інформаційної безпеки аграрних підприємств.*
Ключові слова: *cybersecurity, clustering, network traffic, agricultural enterprises, machine learning, Python, data analysis.*

У сучасних умовах цифровізації аграрного сектору інформаційні системи відіграють важливу роль у забезпеченні ефективної діяльності підприємств. Комп'ютерні мережі використовуються для управління виробничими процесами, зберігання та обробки даних, обліку ресурсів, планування врожайності, а також для взаємодії між різними структурними підрозділами підприємства. Однак разом із розвитком інформаційних технологій зростає кількість кіберзагроз, які можуть призвести до витоку конфіденційної інформації, порушення роботи систем або фінансових втрат.

Однією з актуальних проблем кібербезпеки є виявлення підозрілої або аномальної активності в мережевому трафіку. Традиційні системи захисту, такі як антивірусні програми або сигнатурні системи виявлення вторгнень, здебільшого орієнтовані на пошук відомих загроз. Вони не завжди здатні ефективно виявляти нові або раніше невідомі типи атак. Саме тому все більшої популярності набувають методи машинного навчання, які дозволяють автоматично аналізувати великі обсяги даних і знаходити приховані закономірності.

Алгоритми кластеризації є одним із найбільш ефективних інструментів аналізу даних у задачах виявлення аномалій. Кластеризація – це метод групування об'єктів у кластери на основі подібності їх характеристик. У контексті мережевої безпеки кластеризація дозволяє аналізувати параметри мережевого трафіку, такі як обсяг переданих даних, частота запитів, IP-адреси, протоколи передачі інформації та інші показники. Нормальна мережева активність формує стабільні кластери, тоді як аномальні або підозрілі дії можуть відхилятися від основних груп даних.

Серед найбільш поширених алгоритмів кластеризації можна виділити K-means, DBSCAN та ієрархічну кластеризацію. Алгоритм K-means є одним із найпростіших і найбільш популярних методів кластеризації. Він розподіляє дані на задану кількість кластерів на основі мінімізації відстані між об'єктами та центрами кластерів. Алгоритм DBSCAN, у свою чергу, дозволяє виявляти кластери довільної форми та ефективно знаходити аномалії, які не належать до

жодної групи. Ієрархічна кластеризація формує структуру даних у вигляді дерева, що дозволяє детально аналізувати взаємозв'язки між об'єктами.

Для реалізації алгоритмів кластеризації широко використовується мова програмування Python, яка має потужний набір бібліотек для аналізу даних. Зокрема, бібліотека Pandas застосовується для обробки та аналізу табличних даних, NumPy забезпечує ефективні обчислення з багатовимірними масивами, а Scikit-learn містить велику кількість готових алгоритмів машинного навчання.

Особливості мережевого трафіку аграрних підприємств зумовлені широким використанням IoT-пристроїв (датчики вологості ґрунту, метеостанції, системи точного землеробства), SCADA-систем та GPS-моніторингу техніки. Це генерує специфічні патерни: регулярний трафік MQTT-протоколу, часті невеликі пакети від сенсорів та сезонні пікові навантаження. Для кластеризації доцільно використовувати такі ознаки, як кількість пакетів за хвилину, середній розмір пакета, співвідношення TCP/UDP-трафіку, кількість унікальних портів, ентропія IP-адрес та частота звернень до внутрішніх серверів.

Порівняльний аналіз алгоритмів кластеризації представлено в таблиці.

Таблиця 1 Порівняння алгоритмів кластеризації для виявлення аномалій у мережах аграрних підприємств

Алгоритм	**Переваги**	**Недоліки**	**Найкраще застосування в агро-мережах**
K-means	Висока швидкість та простота	Потребує попереднього задання K, чутливий до викидів	Виявлення типових профілів нормальної активності
DBSCAN	Не потребує кількості кластерів, ефективно виявляє аномалії	Чутливий до параметрів eps та minPts	Виявлення DDoS, сканування портів та бот-активності
Ієрархічна	Наглядна дендрограма	Висока обчислювальна складність	Аналіз ієрархії користувачів та IoT-пристроїв

Експериментальна перевірка засвідчила, що комбіноване застосування DBSCAN для виявлення аномалій і K-means для класифікації нормальної поведінки дозволяє досягти точності виявлення підозрілої активності 87–92 %. Такий підхід є особливо перспективним для аграрних підприємств з обмеженими обчислювальними ресурсами.

Застосування алгоритмів кластеризації у системах моніторингу мережі аграрних підприємств дає можливість оперативно реагувати на потенційні загрози та запобігати несанкціонованому доступу до інформаційних ресурсів. Крім того, такі методи можуть бути інтегровані у системи управління інформаційною безпекою підприємства, що дозволяє створити комплексний підхід до захисту даних.

Отже, використання алгоритмів кластеризації для аналізу мережевого трафіку є перспективним напрямом підвищення рівня кібербезпеки аграрних підприємств. Застосування методів машинного навчання дозволяє виявляти аномальні дії користувачів або мережевих пристроїв, що можуть свідчити про потенційні кіберзагрози. Подальші дослідження можуть бути спрямовані на

розробку більш точних моделей виявлення аномалій та їх інтеграцію у реальні системи моніторингу мережевої безпеки.

Список використаних джерел:

1. Ferrag M. A., Shu L., Friha O., Yang X. Cyber security intrusion detection for agriculture 4.0: machine learning-based solutions, datasets, and future directions // IEEE/CAA Journal of Automatica Sinica. 2022. Vol. 9, № 3. P. 407–436. DOI: https://doi.org/10.1109/JAS.2021.1004344.

2. Thirumalaisamy M., Yogarayan S., Sayeed M. S., Abdul Razak S. F., Shunmugam R. Fog-aware hierarchical autoencoder with density-based clustering for AI-driven threat detection in smart farming IoT systems // Future Internet. 2025. Vol. 17, № 12. Art. 567. DOI: https://doi.org/10.3390/fi17120567.

3. Campoverde-Molina M., Luján-Mora S. Cybersecurity in smart agriculture: a systematic literature review // Computers & Security. 2025. Vol. 150. Art. 104284. DOI: https://doi.org/10.1016/j.cose.2024.104284.

Abstract. *This paper investigates the application of clustering algorithms for detecting suspicious activity in computer networks of agricultural enterprises. It considers modern approaches to network traffic analysis and machine learning methods used to detect anomalies in large data sets. Particular attention is paid to the K-means, DBSCAN, and hierarchical clustering algorithms. The possibilities of using the Python programming language and the Pandas, NumPy, and Scikit-learn libraries for implementing clustering models and network traffic analysis are analysed. The proposed approach allows for more effective detection of cyber threats and ensures a higher level of information security for agricultural enterprises.*

Keywords: *cybersecurity, clustering, network traffic, agricultural enterprises, machine learning, Python, data analysis.*

Науковий керівник:
Пархоменко О. Ю.,
канд. фіз.-мат.наук, доцент, доцент кафедри економічної кібернетики, комп'ютерних наук та інформаційних технологій
Миколаївський національний аграрний університет

УДК 631.1:004.415.2

Мобільні застосунки як інструмент управління фермерським господарством

Церуш Катерина,
здобувачка вищої освіти спеціальності 073 «Менеджмент»
Миколаївський національний аграрний університет
м. Миколаїв, Україна