

**МАТЕРІАЛИ**  
**III Міжнародної науково-практичної конференції**  
**“КІБЕРБЕЗПЕКА ДЕРЖАВНИХ ІНСТИТУЦІЙ**  
**ТА ПОДОЛАННЯ КРИЗОВИХ СТАНІВ”**

**(Том 1)**

**14 листопада 2024 року**

**Київ – Прага – Таллінн – Тернопіль**

Oleksandr KOVALENKO; Olha SHEVCHUK	
Reducing the number of false alerts in SOC using machine learning algorithms....	121
Володимир КОЗЕМАСЛОВ; Оксана КУБАЙЧУК	
Аналіз та застосування тригонометричного шифру.....	122
Вікторія КОЗЯЙКІНА; Микола КОНОТОПЕЦЬ	
Аналіз сучасного стану фотоприймачів ГЧ-діапазону, що застосовуються в тепловізорах.....	123
Yvacheslav KOLODIICHUK; Ivan HORNIICHUK	
Method for monitoring local networks and managing connections of new devices	125
Іван КОНДРИЧ; Александра МАТІЙКО; Олексій ГЛУШКОВ	
Життєвий цикл кіберрозвідки .....	127
Вікторія КОМАРОВСЬКА; Олександр ШАПОВАЛ	
Програмний модуль запобігання роботі несанкціонованих ДНСР-серверів у комп'ютерній мережі.....	128
Богдан КОНОНЕНКО; Дмитро ЛАНДЕ	
Програмний модуль виявлення та прогнозування інцидентів кібербезпеки у соціальних мережах .....	129
Bohdan KONONENKO; Artem MYKYTIUK	
Modern solutions for detecting and responding to cyber threats to the network perimeter.....	130
Данило КОПИЧ; Володимир СОКОЛОВ	
Підсистема підтримки процесу розробки програмного забезпечення на основі штучного інтелекту .....	132
Денис КОРНУСЬ; Валерій БЛІЙ	
Аналіз та моніторинг кіберзагроз на основі стандартів кібернетичного захисту .....	134
Артем КОРОБЧУК; Василь ЦУРКАН	
Тенденції кіберзахисту об'єктів критичної інформаційної інфраструктури.....	135
Євгеній КОРОПЕЦЬКИЙ; Дмитро ШАРАДКІН	
Автоматизація рефакторингу програмного коду із застосуванням технологій генеративних мовних моделей .....	136
Іліа КОТІАІ; Olha SHEVCHUK	
A software tool for detecting military objects in images.....	138
Андрій КОЧЕРГІН; Вячеслав РЯБЦЕВ	
Архітектура підсистеми ведення електронних залікових книжок інформаційної системи військового навчального підрозділу закладу вищої освіти.....	139

## ПРОГРАМНИЙ МОДУЛЬ ВИЯВЛЕННЯ ТА ПРОГНОЗУВАННЯ ІНЦИДЕНТІВ КІБЕРБЕЗПЕКИ У СОЦІАЛЬНИХ МЕРЕЖАХ

**Анотація.** Розвиток технологій соціальних мереж став каталізатором зростання інцидентів кібербезпеки, що підвищує необхідність виявлення та прогнозування загроз. У дослідженні розглядається програмний модуль, який використовує методи машинного навчання для виявлення аномалій у поведінці користувачів, що дозволяє досягати високої точності в ідентифікації потенційних кіберінцидентів.

**Summary.** The development of social network technologies has catalyzed an increase in cybersecurity incidents, highlighting the need for detecting and predicting threats. The study examines a software module that employs machine learning methods to identify anomalies in user behavior, achieving high accuracy in identifying potential cyber incidents.

**Ключові слова:** інциденти кібербезпеки, соціальні мережі, виявлення, прогнозування, машинне навчання.

Генерація та обробка даних у соціальних мережах створюють нові виклики для безпеки інформації. Подроблені профілі, шахрайські активності та інші загрози ставлять під загрозу приватність та безпеку користувачів. У рамках дослідження було розглянуто методи виявлення інцидентів, зокрема використання алгоритмів машинного навчання для аналізу поведінки користувачів і виявлення аномалій. Комбінування статистичних методів та сучасних технологій, таких як нейронні мережі, дозволяє досягати високих результатів у виявленні кіберзагроз.

Модуль, розроблений у рамках дослідження, здатний адаптуватися до різних сценаріїв атак і використовує великі набори даних для навчання. Це забезпечує його стійкість до нових форм маніпуляцій. Результати показали, що комбінований підхід до виявлення та прогнозування інцидентів є ефективним, що підкреслює важливість інновацій у кібербезпеці.

**Висновки.** Розробка програмного модуля для виявлення та прогнозування інцидентів кібербезпеки в соціальних мережах є важливим кроком у забезпеченні інформаційної безпеки. Використання нейронних мереж допомагає покращити роботу застосунку.