Державна наукова установа «Інститут інформації, безпеки і права
Національної академії правових наук України»

Науково-дослідний інститут інтелектуальної власності
Національної академії правових наук України

УКРАЇНА В УМОВАХ СОЦІАЛЬНОЇ ТА ЦИФРОВОЇ ТРАНСФОРМАЦІЇ: ТЕОРЕТИЧНІ МОДЕЛІ ПРАВОВОГО РЕГУЛЮВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ

МАТЕРІАЛИ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

Київ, 5 листопада 2025 року

Київ-Одеса

2025

УДК 340.132:004.8(477)
У 45

Рекомендовано до друку

Вченою радою Державної наукової установи «Інститут інформації, безпеки і права Національної академії правових наук України». Протокол № 10 від 09.12.2025 р.

У 45 **Україна в умовах соціальної та цифрової трансформації: теоретичні моделі правового регулювання штучного інтелекту :** матеріали наук.-практ. конф. (Київ, 5 листоп. 2025 р.) [Електронне видання] / упоряд.: М. В. Дубняк, С. О. Дорогих, І. Ф. Корж, В. М. Фурашев. Київ; Одеса : Фенікс, 2025. 240 с. Режим доступу: https://ippi.org.ua/sites/default/files/zbirnik_tez_05.11.2025_1.pdf

ISBN 978-617-8430-97-9

Збірник містить матеріали щодо стратегічних напрямів правового регулювання штучного інтелекту в Україні; розвитку національної LLM та впровадження агентних ШІ-рішень у державні сервіси; формування цифрових прав і оновлення цивільного законодавства; проблем використання ШІ в умовах воєнного стану, забезпечення кібербезпеки, захисту персональних даних та інтелектуальної власності; етичних і методологічних засад застосування ШІ у сфері освіти та науки.

Доповіді учасників конференції можуть бути корисними для фахівців, експертів і вчених, науково-педагогічних працівників та здобувачів вищої освіти.

УДК 340.132:004.8(477)

Матеріали подано у авторській редакції.

ISBN 978-617-8430-97-9

З М І С Т

БЕЗПЕКА, ОБОРОНА, КІБЕРЗАХИСТ ТА ВОЄННИЙ КОНТЕКСТ ПРИ РЕГУЛЮВАННІ ШІ

ЦИФРОВИЙ СУВЕРЕНІТЕТ І НАЦІОНАЛЬНА СТРАТЕГІЯ РОЗВИТКУ У СФЕРІ ШТУЧНОГО ІНТЕЛЕКТУ

ПРАВА ЛЮДИНИ, ПРИВАТНІСТЬ ТА ПИТАННЯ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ

СОЦІАЛЬНИЙ ВИМІР ШТУЧНОГО ІНТЕЛЕКТУ:

ОСВІТА, ПРАЦЯ, ІНКЛЮЗІЯ

Ганна Форос
кандидат юридичних наук, доцент, завідувачка кафедри кримінального аналізу та інформаційних технологій
Одеський державний університет внутрішніх справ
ORCID: https://orcid.org/0000-0002-9504-3681

АВТОМАТИЗОВАНИЙ МОНІТОРИНГ КІБЕРЗАГРОЗ ЗА ДОПОМОГОЮ СИСТЕМ МАШИННОГО НАВЧАННЯ

Активна цифровізація економічних процесів, державного управління та соціальної взаємодії зумовила суттєве зростання залежності суспільства від стабільного функціонування інформаційних систем. Збільшення кількості пристроїв, що підключені до мережі, формування розподілених хмарних середовищ і розвиток Інтернету речей призвели до різкого ускладнення ландшафту кіберзагроз. Кіберзлочинність набуває все більш структурованого та технологічно оснащеного характеру, а її інструменти швидко еволюціонують. У цих умовах питання забезпечення кібербезпеки перетворюється на ключовий аспект інформаційної політики держави та корпоративного управління.

Традиційні методи виявлення атак, що ґрунтуються на сигнатурному аналізі або фіксованих правилах реагування, поступово втрачають ефективність. Причиною є динамічність появи нових шкідливих кодів, варіативність поведінки зловмисників і використання складних технік ухилення. Тому виникає потреба у впровадженні адаптивних інтелектуальних систем, здатних виявляти відхилення від нормальної поведінки та прогнозувати потенційні інциденти без необхідності попереднього знання сигнатур атак.

Автоматизований моніторинг кіберзагроз є процесом безперервного збору, фільтрації, аналізу й кореляції подій у мережевому трафіку, системних журналах та інших джерелах телеметрії з метою своєчасного виявлення підозрілої активності. Системи машинного навчання забезпечують новий рівень аналітики, оскільки здатні опрацьовувати великі масиви даних, визначати приховані залежності між подіями та виявляти аномальні патерни,

що можуть свідчити про спробу несанкціонованого доступу або порушення політики безпеки.

Одним із найбільш результативних підходів є застосування алгоритмів класифікації, які дозволяють віднести вхідні дані до певної категорії ризику. До них належать Random Forest [1], Decision Trees [2], Support Vector Machines [3], а також ансамблеві методи, які комбінують результати кількох моделей для підвищення точності прогнозування. Для задач виявлення складних, багатоступеневих атак ефективно використовуються методи глибинного навчання, що базуються на штучних нейронних мережах. Автоенкодери допомагають ідентифікувати невідомі раніше типи загроз, а рекурентні мережі застосовуються для аналізу послідовностей подій у часових рядах журналів безпеки.

Методи кластеризації, зокрема k-means, DBSCAN і Hierarchical Clustering, дозволяють групувати схожі події, виділяючи потенційні аномалії без попереднього маркування даних. Це особливо важливо для систем із великим обсягом трафіку, де ручне маркування або формування навчальних вибірок є неможливим. Таким чином, поєднання різних алгоритмічних підходів забезпечує створення багаторівневої системи аналізу даних, здатної адаптуватися до змін кіберсередовища.

Окрему роль відіграють методи обробки природної мови (Natural Language Processing) [4], що використовуються для автоматичного аналізу текстових повідомлень, звітів про вразливості та відкритих джерел інформації. Завдяки цим технологіям система може виявляти згадки про нові експлойти, індикатори компрометації або ознаки підготовки кібератаки ще до її фактичної реалізації. Це суттєво підвищує проактивність реагування та дозволяє прогнозувати потенційні ризики.

Побудова автоматизованої системи моніторингу кіберзагроз потребує розроблення архітектури, що включає кілька взаємопов’язаних рівнів. Перший рівень забезпечує збір та агрегацію даних із мережевих сенсорів, систем контролю доступу, журналів безпеки, SIEM-платформ [5] і зовнішніх джерел. Другий рівень відповідає за попередню обробку, нормалізацію та очищення даних від шумів. Третій рівень реалізує аналітичні моделі машинного навчання, які виконують класифікацію, прогнозування та детектування аномалій. Четвертий рівень охоплює компоненти візуалізації, формування звітів і автоматизоване інформування про потенційні інциденти безпеки.

Інтеграція автоматизованих систем моніторингу з іншими компонентами кіберзахисту — міжмережевими екранами, IDS/IPS, платформами керування інцидентами — забезпечує створення єдиного інформаційного простору, у якому рішення приймаються на основі комплексного аналізу даних. Це дозволяє значно скоротити час виявлення атак і зменшити навантаження на аналітиків безпеки.

Подальші дослідження у цьому напрямі орієнтовані на створення гібридних моделей, що об'єднують алгоритми класичного машинного навчання, глибинних нейронних мереж та генеративних моделей. Використання генеративно-змагальних мереж (Generative Adversarial Networks, GAN) відкриває можливість імітації поведінки зловмисників і формування навчальних вибірок із синтетичних даних, що сприяє підвищенню стійкості систем до нових типів атак. Особливої уваги заслуговує аспект інтерпретованості результатів — здатність пояснити рішення, прийняті моделлю. Це критично важливо для забезпечення довіри до автоматизованих систем кіберзахисту та для впровадження їх у критичну інфраструктуру.

Отже, автоматизований моніторинг кіберзагроз на основі методів машинного навчання формує нову парадигму забезпечення кібербезпеки, орієнтовану на аналітичну обробку великих обсягів даних, самонавчання та адаптацію до змін середовища. Реалізація подібних систем дозволяє підвищити точність виявлення загроз, зменшити час реагування на інциденти, оптимізувати використання ресурсів служби безпеки й створити динамічну модель захисту інформаційних ресурсів у мінливому кіберпросторі.

Список використаних джерел

1. Salman, Hasan Ahmed, Ali Kalakech, and Amani Steiti. "Random Forest Algorithm Overview." *Babylonian Journal of Machine Learning* (June 2024): 69–79. https://doi.org/10.58496/BJML/2024/007. 2024. Вип. 30. С. 67–77. DOI: https://doi.org/10.32447/20784643.30.2024.07

2. «Decision Tree – an Overview». *ScienceDirect Topics: Computer Science*. https://www.sciencedirect.com/topics/computer-science/decision-tree-model

3. «Support Vector Machine». *ScienceDirect Topics: Engineering.* Accessed October 30, 2025. https://www.sciencedirect.com/topics/engineering/support-vector-machine

4. Abuya, Teresa Kwamboka, Christal Anto V, Alexander Mutiso Mutua, and Richard Rimiru. *Natural Language Processing.* August 2025. Zenodo. https://doi.org/10.5281/zenodo.16917578. ISBN 978-93-6786-839-3.

5. Mahajan, Shilpa. «The Role of SIEM in Modern Cybersecurity: A Comprehensive Analysis». In *Cybersecurity and Privacy in the Era of Smart Technologies*, September 2025. https://doi.org/10.4018/979-8-3373-2282-7.ch010

НАУКОВЕ ВИДАННЯ

УКРАЇНА В УМОВАХ СОЦІАЛЬНОЇ ТА ЦИФРОВОЇ ТРАНСФОРМАЦІЇ: ТЕОРЕТИЧНІ МОДЕЛІ ПРАВОВОГО РЕГУЛЮВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ

МАТЕРІАЛИ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

Київ, 5 листопада 2025 року

Електронне видання

Макет збірника та комп'ютерна верстка:
М. Дубняк, С. Дорогих

Упорядкування:
І. Корж, В. Фурашев

Ум-друк. арк. 12.
Зам. № 2512-03.

Видавець ПП «Фенікс»
(Свідоцтво суб'єкта видавничої справи ДК № 1044 від 17.09.02).
Україна, м. Одеса, 65009, вул. Зоопаркова, 25.
e-mail: fenix-izd@ukr.net