Міністерство внутрішніх справ України
Харківський національний університет внутрішніх справ
Національна академія правових наук України
Організація з безпеки та співробітництва в Європі

ОБСЄ Організація з безпеки та співробітництва в Європі

БЕЗПЕКА У КІБЕРСФЕРІ

Збірник матеріалів
Міжнародної науково-практичної конференції
(м. Кам’янець-Подільський, 28 травня 2025 року)

Кам’янець-Подільський 2025

УДК [351.74:004](477)(08)
Б39

Друкується згідно з рішенням оргкомітету
за дорученням Харківського національного університету внутрішніх
справ від 26.02.2025 № 19

Б39 **Безпека** у кіберсфері : зб. матеріалів Міжнарод. наук.-практ. конф. (м. Кам'янець-Подільський, 28 трав. 2025 р.) / МВС України, Харків. нац. ун-т внутр. справ ; Нац. акад. правових наук України ; Організація з безпеки та співробітництва в Європі. – Кам'янець-Подільський : ХНУВС, 2025. – 246 с.

У матеріалах конференції окреслено найбільш актуальні проблеми безпеки у кіберсфері на сучасному етапі; проаналізовано окремі питання правового та організаційного забезпечення безпеки у кіберсфері; використання інформаційних технологій і технічних засобів у протидії правопорушенням; забезпечення кібербезпеки на об'єктах інформаційної діяльності; інформаційної безпеки суспільства та держави.

УДК [351.74:004](477)(08)

Матеріали викладено в авторській редакції з незначними коректорськими правками.
За достовірність наукового матеріалу, професійного формулювання,
фактичних даних, цитат, власних назв, географічних назв,
а також за розголошення фактів, що не належать відкритому друку, тощо
відповідають автори публікацій та їх наукові керівники.
Електронна копія збірника розміщується
у відкритому доступі на сайті Харківського національного
університету внутрішніх справ (http://www.univd.edu.ua) у розділі «Наука»,
сторінка «Конференції, семінари та круглі столи»,
а також у репозитарії ХНУВС (http://dspace.univd.edu.ua/xmlui/).

Windows Defender Firewall – ефективний засіб блокування зовнішніх мережевих загроз, хоча й вимагає додаткового налаштування для повного циклу чинності.

Malwarebytes Browser Guard – фільтр або блокувальник шкідливих сайтів, а також абонентської реклами та фішингу під час відвідування інтернет-ресурсів. Необхідно використовувати комплексний підхід, поєднуючи антивірус системний, брандмауер мережевий та засіб захисту від блокувальників. Це дозволяє підвести під відповідну захист ризики як з боку шкідливого ПЗ, так і з боку фішингу або дестабілізаці потенційних мережних атак.

Отже у процесі тестування всі три засоби продемонстрували високу ефективність у своїх напрямках. Для повного захисту персонального комп'ютера рекомендую використовувати їх у комплексі. Це дозволить захиститися від більшості сучасних кіберзагроз, забезпечивши безпеку як на рівні системи, так і під час роботи в мережі.

Список використаних джерел

1. Avast antivirus URL: https://blog.avast.com/avast-is-awarded-product-of-the-year-title-avast (дата звернення 01.05.2025)

2. 2. Firewall. URL: https://selabs.uk/reports/endpoint-security-eps-home-2023-q4/#product-factsheets (дата звернення 01.05.2025)

3. Malwarebytes. URL: https://arxiv.org/abs/1506.04200 (дата звернення 01.05.2025)

4. Perrotta R., Hao F. Botnet in the Browser: Understanding Threats Caused by Malicious Browser Extensions. *IEEE Security & Privacy.* 2018. Vol. 16, Issue 4. P. 66-81.

Одержано 29.04.2025

УДК 004.67

ГОРЕЛОВ Юрій Петрович,
кандидат технічних наук, доцент,
доцент кафедри кібербезпеки та DATA-технологій
навчально-наукового інституту № 5
Харківського національного університету внутрішніх справ;

КОБЗЕВ Ігор Володимирович,
кандидат технічних наук, доцент,
доцент кафедри інформатики та комп'ютерної техніки
Харківського національного економічного університету ім. Семена Кузнеця

ВИКОРИСТАННЯ ТЕХНОЛОГІЙ BIG DATA ДЛЯ АНАЛІЗУ ЗЛОЧИННОСТІ

Технології Big Data займають центральне місце у сучасних підходах до аналізу та запобігання злочинності. Завдяки можливості аналізувати великі обсяги різнорідних даних, Big Data надає правоохоронним органам інструменти для виявлення закономірностей у злочинній діяльності, прогнозування злочинів та ефективнішого управління ресурсами.

Застосування великих даних для аналізу злочинності активно досліджується у світі. Наприклад, дослідження [1] показало, що Big Data дозволяє покращити процеси патрулювання шляхом ідентифікації "гарячих точок" злочинності. Також в роботі [2] підкреслюється, що машинне навчання у поєднанні з великими даними допомагає прогнозувати злочини та поведінку правопорушників. Впровадження цих технологій підвищує швидкість аналізу та точність передбачень, зменшуючи кількість наслідкових злочинів.

Метою доповіді є дослідження можливостей використання технологій Big Data для аналізу злочинності, визначення її переваг у порівнянні з традиційними методами, а також аналіз основних викликів, що стоять на шляху ефективного впровадження цих технологій у правоохоронній сфері.

Технології Big Data дозволяють збирати й аналізувати великі обсяги даних про злочини, такі як час, місце, тип правопорушення, соціально-економічні фактори. Використання геопросторових даних та алгоритмів кластеризації допомагає виявляти "гарячі точки" злочинності — райони з підвищеним рівнем правопорушень. Це дозволяє правоохоронним органам краще планувати патрулі та зосереджувати ресурси на найбільш небезпечних зонах.

Технології Big Data у поєднанні з алгоритмами машинного навчання допомагають прогнозувати ймовірність виникнення злочинів у певних районах. На основі історичних даних можна визначати фактори ризику та прогнозувати майбутні злочини, що дозволяє вчасно вживати запобіжних заходів.

Аналіз соціальних мереж та комунікаційні дані дають змогу виявляти зв’язки між злочинцями та групами, що діють у регіоні. Big Data використовується для ідентифікації структур злочинних організацій та відстеження їхньої діяльності, що сприяє боротьбі з організованою злочинністю.

Камери спостереження генерують величезні обсяги відео-даних, що можуть бути оброблені за допомогою технологій штучного інтелекту та великих даних. Аналіз зображень та відео дозволяє відслідковувати підозрілу поведінку та ідентифікувати правопорушників. Крім того, дані з соціальних мереж можуть бути використані для виявлення злочинних намірів або аналізу поведінки потенційних правопорушників.

Завдяки автоматизованим алгоритмам обробки даних, аналіз великих масивів інформації відбувається швидше та точніше порівняно з ручними методами. Big Data допомагає краще розподіляти ресурси правоохоронних органів, зосереджуючи увагу на найбільш проблемних районах або групах. Прогнозування злочинів на основі історичних даних дозволяє вживати проактивних заходів для їхнього запобігання.

Одним із ключових викликів використання Big Data у правоохоронній сфері є захист приватності громадян. Аналіз даних про пересування людей, їхні комунікації або активність у соціальних мережах може порушувати права на приватність, тому важливо розробляти етичні норми використання цих даних.

Щоб забезпечити точність результатів, необхідно гарантувати, що дані є достовірними, повними та актуальними. Використання неперевірених або недостовірних даних може призвести до хибних висновків або несправедливих звинувачень. Не всі правоохоронні органи мають необхідну інфраструктуру та

технічні можливості для обробки великих даних. Це вимагає інвестицій у розвиток технічної бази та підготовку фахівців.

Використання нових технологій, таких як Інтернет речей (IoT) та 5G, відкриває нові можливості для збору даних, які можуть бути корисними у боротьбі зі злочинністю. Важливо продовжувати роботу над створенням стандартів використання Big Data, що будуть відповідати вимогам приватності та безпеки громадян.

Технології Big Data відкривають нові можливості для аналізу та запобігання злочинності. Їхнє використання дозволяє покращити точність прогнозування, ефективніше використовувати ресурси правоохоронних органів та підвищити рівень безпеки громадян. Однак для повного впровадження Big Data в аналіз злочинності необхідно подолати технічні, етичні та організаційні виклики. Розвиток нових технологій і міжнародна співпраця дозволять використовувати цей інструмент максимально ефективно.

Список використаних джерел

1. Kumar R., Nagpal B. Analysis and prediction of crime patterns using big data. *Int. j. inf. tecnol.* 11, 799–805 (2019). https://doi.org/10.1007/s41870-018-0260-7

2. Hussam Hashim Hussein, Ahmed Talib Abdulamee. Crime Prediction Using Big Data Analysis. *EUDL - European Union Digital Library*. IMDC-IST 2021, September 07-09, Sakarya, Turkey Copyright © 2022 EAI DOI 10.4108/eai.7-9-2021.2314943 URL: https://eudl.eu/pdf/10.4108/eai.7-9-2021.2314943

Одержано 30.04.2025

УДК 343.102:004.056:355.02

ДАНІЛЮК Світлана Богданівна,
курсантка 3 курсу
навчально-наукового інституту № 1
Харківського національного університету внутрішніх справ
https://orcid.org/0009-0001-2845-8991;

ДЕРЕВЯГІН Олексій Олександрович,
кандидат юридичних наук, старший науковий співробітник,
професор кафедри оперативно-розшукової діяльності та розкриття злочинів
навчально-наукового інституту № 2
Харківського національного університету внутрішніх справ
https://orcid.org/0000-0003-1622-5549

ОСОБЛИВОСТІ ЗАСТОСУВАННЯ ОПЕРАТИВНО-РОЗШУКОВИХ ЗАХОДІВ ПІДРОЗДІЛАМИ КРИМІНАЛЬНОЇ ПОЛІЦІЇ З МЕТОЮ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ НА ОБ'ЄКТАХ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ В УМОВАХ ВОЄННОГО СТАНУ

Забезпечення кібербезпеки на об'єктах інформаційної діяльності в умовах воєнного стану є критично важливим завданням для правоохоронних органів, зокрема підрозділів кримінальної поліції. В умовах активізації кібератак, спрямованих на державні установи, критичну інфраструктуру та приватний сектор,