Волобоєва Злата Олегівна

студентка навчально-наукового інституту права та соціального менеджменту Донецького державного університету внутрішніх справ

Габорець Ольга Андріївна

доцент кафедри оперативно-розшукової діяльності та інформаційної безпеки навчально-наукового інституту підготовки фахівців для підрозділів кримінальної поліції імені Е.О. Дідоренка Донецького державного університету внутрішніх справ, доктор філософії, доцент

ІНФОРМАЦІЙНО-АНАЛІТИЧНА ПІДТРИМКА ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

В умовах гібридної війни кіберзлочинність трансформується з переважно економічно мотивованої протиправної діяльності у складовий елемент системного деструктивного впливу на національну безпеку, державне управління та суспільну стабільність. Цифровий простір використовується не лише як середовище вчинення злочинів, а й як інструмент реалізації інформаційно-психологічних операцій, саботажу критичної інфраструктури, підриву довіри до органів влади та правоохоронної системи. За таких умов ефективна протидія кіберзлочинності неможлива без розвиненої інформаційно-аналітичної підтримки, здатної забезпечити випереджувальне виявлення загроз, глибоке осмислення їх природи та обґрунтоване прийняття управлінських і процесуальних рішень.

Інформаційно-аналітична підтримка протидії кіберзлочинності в умовах гібридної війни набуває міждисциплінарного характеру, поєднуючи інструменти кримінального аналізу, кібербезпеки, цифрової криміналістики, розвідки з відкритих джерел та аналітики великих даних [1]. Її сутність полягає у системному зборі, верифікації, інтеграції та інтерпретації різнорідної інформації з метою формування цілісної картини кіберзагроз, ідентифікації суб'єктів протиправної діяльності, їх інфраструктури, мотивації та зв'язків. На відміну від традиційного аналізу кіберінцидентів, сучасна аналітична діяльність повинна враховувати гібридну

природу загроз, коли межі між кримінальними угрупованнями, хактивізмом і керованими ззовні кібератаками стають дедалі більш розмитими.

Особливе значення в цьому контексті має перехід від реактивної моделі реагування до проактивної аналітики, орієнтованої на прогнозування та попередження кіберзлочинних проявів. Аналіз поведінкових патернів зловмисників, кореляція технічних індикаторів компрометації з фінансовими, комунікаційними та соціальними слідами дозволяють виявляти підготовчі стадії атак, оцінювати потенційні наслідки та визначати найбільш уразливі об'єкти впливу. У цьому аспекті інформаційно-аналітична підтримка виконує не лише допоміжну, а стратегічну функцію, формуючи підґрунтя для розроблення державної політики у сфері кібербезпеки та кримінальної юстиції.

Важливою складовою аналітичного забезпечення є використання стандартизованих моделей опису кіберзлочинної діяльності, що забезпечують уніфікацію підходів до фіксації, аналізу та інтерпретації даних. Формалізація тактик, технік і процедур зловмисників підвищує якість міжвідомчої взаємодії, спрощує міжнародний обмін інформацією та сприяє підвищенню доказової спроможності матеріалів кримінальних проваджень. Водночас у гібридній війні аналітика має виходити за межі суто технічного аналізу, доповнюючись оцінкою інформаційного ефекту кібератак, їх впливу на громадську думку, соціальні настрої та легітимність державних інститутів.

Додатковим викликом для інформаційно-аналітичної підтримки стає активне використання штучного інтелекту та автоматизованих інструментів у кіберзлочинній діяльності. Масштабування фішингових кампаній, створення переконливого синтетичного контенту, автоматизований підбір жертв і адаптація сценаріїв соціальної інженерії суттєво ускладнюють виявлення та атрибуцію злочинів. У відповідь аналітичні підрозділи змушені впроваджувати методи поведінкового аналізу, графових моделей взаємозв'язків, контент-аналізу та машинного навчання, поєднуючи технологічні можливості з правовими гарантіями захисту прав і свобод людини.

Не менш важливим є організаційно-правовий вимір інформаційно-аналітичної підтримки, який передбачає чітке регламентування доступу до даних, забезпечення цілісності та допустимості цифрових доказів, а також налагодження стійкої взаємодії між правоохоронними органами, спеціальними службами та приватним сектором. Умови гібридної війни об'єктивно зумовлюють необхідність міжнародної координації, оскільки кіберзлочинні екосистеми мають транснаціональний характер, а їх інфраструктура часто розміщується поза межами однієї юрисдикції.

Узагальнений науковий висновок полягає в тому, що інформаційно-аналітична підтримка протидії кіберзлочинності в умовах гібридної війни є ключовим інструментом забезпечення національної безпеки, який інтегрує технологічні, аналітичні та правові механізми у єдину систему протидії. Її ефективність визначається здатністю трансформувати великі обсяги різнорідних даних у науково обґрунтовані аналітичні продукти, орієнтовані на прогнозування, превенцію та доказове реагування, що в сукупності дозволяє зменшити деструктивний вплив кіберзлочинності та підвищити стійкість держави в умовах гібридного протистояння.

Література

1. Габорець О. А., Пекарський С. П. Кіберзлочини як об'єкт правової класифікації. Українська поліцеїстика: теорія, законодавство, практика. 2025. № 2 (серп.). С. 100-105. DOI: https://doi.org/10.32782/2709-9261-2025-2-14-18