tse-znaty-i-iaki-operatsii-zaraz-provodyt-rosiia-proty-ukrainy/ (дата звернення: 26.04.2026).

3. Chamika Hiruni. Psychological Warfare in the Digital Age: The Role of Cyber Operations in Modern PsyOps. Psychological Warfare in the Digital Age. November 2024. DOI:10.13140 /RG.2.2.34079.37283.

4. Що таке ІПСО: сенс, загроза та як протидіяти. *Chernigivlisgosp.com.ua*. URL: https://chernigivlisgosp.com.ua/ shho-take-ipso-sens-zagroza-ta-yak-protidiyati/ (дата звернення: 26.04.2026).

КІБЕРБЕЗПЕКА ЯК ЕЛЕМЕНТ ІНФОРМАЦІЙНО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ ПІДРОЗДІЛІВ КРИМІНАЛЬНОЇ ПОЛІЦІЇ

Постолова Карина Юріївна
здобувачка вищої освіти 202 взводу
Навчально-наукового інституту підготовки фахівців
для підрозділів кримінальної поліції Національної поліції України
(Одеський державний університет внутрішніх справ)
Форос Ганна Володимирівна
завідувачка кафедри кримінального аналізу та інформаційних технологій, к.ю.н., доцент
(Одеський державний університет внутрішніх справ)
https://orcid.org/0000-0002-9504-3681

У сучасних умовах стрімкого розвитку інформаційних технологій та активної цифровізації всіх сфер суспільного життя особливого значення набуває питання забезпечення кібербезпеки. Постійне зростання обсягів інформації та розширення можливостей використання кіберпростору поряд із беззаперечними перевагами зумовлює появу нових викликів і загроз, пов’язаних із кіберзлочинністю, витоком даних та несанкціонованим втручанням у функціонування інформаційних систем. У зв’язку з цим підвищується роль правоохоронних органів, зокрема підрозділів кримінальної поліції, діяльність яких значною мірою залежить від ефективного інформаційно-аналітичного забезпечення та належного рівня кібербезпеки.

Правову основу кібербезпеки становить Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII. Відповідно до ст. 5 Закону, правоохоронні органи є суб'єктами забезпечення кібербезпеки та здійснюють запобігання використанню кіберпростору в протиправних цілях, виявлення, реагування на кіберінциденти та інформаційний обмін [2].

Національна поліція України відповідно до Закону України «Про Національну поліцію» від 02.07.2015 № 580-VIII наділена повноваженнями щодо запобігання, виявлення, припинення та розкриття кіберзлочинів, а також підвищення поінформованості громадян про безпеку в кіберпросторі [3, с. 374]. Департамент кіберполіції утворено постановою Кабінету Міністрів України від 13.10.2015 № 831 як міжрегіональний територіальний орган у структурі кримінальної поліції.

Важливе значення мають Будапештська конвенція про кіберзлочинність (ратифікована Україною у 2005 році), Закон України «Про критичну інфраструктуру» (2021) та Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури (Постанова КМУ від 19.06.2019 № 518). Кримінальний кодекс України містить статті 361–363-1, що передбачають відповідальність за комп'ютерні злочини.

Нормативна база створює підґрунтя для інтеграції кібербезпеки в діяльність поліції, проте законодавче регулювання має певні прогалини, зокрема в механізмах міжвідомчої взаємодії та процедурній роботі з цифровими доказами [1, с. 393].

Департамент кіберполіції входить до структури кримінальної поліції Національної поліції України та є міжрегіональним територіальним органом. Він забезпечує реалізацію державної політики у сфері протидії кіберзлочинності та здійснює оперативно-розшукову діяльність.

Основні завдання Департаменту включають: реалізацію державної політики протидії кіберзлочинності; завчасне інформування населення про новітні кіберзлочини; впровадження програмних засобів для систематизації та аналізу інформації про кіберінциденти, загрози та злочини; реагування на запити закордонних партнерів через Національну цілодобову мережу контактних пунктів (понад 90 країн); підвищення кваліфікації працівників поліції щодо застосування комп'ютерних технологій; участь у міжнародних операціях.

Кіберполіція виконує функції попередження, виявлення, фіксації кіберзлочинів та розслідування інцидентів у кіберпросторі. Вона забезпечує інформаційно-аналітичну підтримку підрозділів кримінальної поліції шляхом моніторингу кіберінцидентів, аналізу загроз, збору індикаторів компрометації (IoC) та передачі аналітичних даних. Ефективна протидія серйозним інцидентам потребує спільної роботи CERT-UA і поліції: технічні фахівці швидко інформують правоохоронців, якщо атака має ознаки злочину, що дозволяє трансформувати технічний інцидент у кримінальне провадження [1, с. 399–401; 4].

Кібербезпека визначається як стан захищеності життєво важливих інтересів людини, суспільства та держави під час використання кіберпростору, за якого забезпечуються сталий розвиток інформаційного суспільства та своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз [2; 3, с. 375].

Для підрозділів кримінальної поліції кібербезпека є елементом інформаційної безпеки, що включає захист баз даних, систем документообігу, сервісу «102», автоматизованих диспетчерських систем від внутрішніх і зовнішніх загроз. Вона забезпечує: виявлення та нейтралізацію кіберзагроз під час оперативно-розшукових заходів; дотримання принципів конфіденційності, цілісності та доступності інформації; збір, обробку та використання цифрових доказів; координацію з CERT-UA для оперативного обміну даними [1, с. 398–401; 3, с. 376].

Впровадження сучасних програмно-аналітичних платформ для моніторингу кіберінцидентів і аналізу загроз дозволяє перетворювати розрізнені дані на якісну аналітичну інформацію, що підвищує ефективність управлінських рішень та профілактичної роботи в кримінальній поліції [1, с. 400].

Серед основних проблем виокремлюються: низький рівень цифрової зрілості та технічної спроможності правоохоронних органів порівняно зі швидкістю розвитку кіберзагроз; недостатня підготовка кадрів, брак фінансування та сучасного програмно-аналітичного забезпечення; фрагментарність координації між поліцією, CERT-UA та приватним сектором; проблеми збору цифрових доказів у транснаціональних атаках; правові колізії в питаннях юрисдикції та процедурної взаємодії [1, с. 393–394; 3, с. 374–375].

Перспективи вдосконалення пов’язані з:

- гармонізацією української правової бази з положеннями Директиви ЄС NIS2 та Будапештської конвенції;

- створенням Національної телекомунікаційної платформи кібербезпеки для оперативного обміну інформацією та індикаторами компрометації;
- підвищенням кадрового потенціалу через постійну професійну підготовку;
- впровадженням сучасних технологій (Big Data, штучний інтелект);
- розвитком партнерства з приватним сектором та посиленням міжнародної співпраці через мережі Інтерполу та Європолу [1, с. 402–403].

Отже, кібербезпека є невід'ємним елементом інформаційно-аналітичного забезпечення підрозділів кримінальної поліції. Вона забезпечує захист інформаційних ресурсів, оперативне реагування на загрози, збір цифрових доказів та ефективну протидію кіберзлочинності в умовах гібридної війни. Аналіз нормативної бази, ролі Департаменту кіберполіції та практичних аспектів свідчить про необхідність системного підходу до її розвитку. Вирішення виявлених проблем шляхом кадрового, технічного та нормативного вдосконалення сприятиме підвищенню стійкості кримінальної поліції до кіберзагроз і зміцненню національної безпеки України.

Список використаних джерел:

1. Василенко В. М. Національна кібербезпека в умовах диджиталізації суспільства: роль поліції в захисті критичної інфраструктури. *Науковий вісник. 2025.* С. 392–403.

2. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII. Офіційний вебпортал Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

3. Мамедова Е. А. Кібербезпека патрульної поліції: підходи до визначення поняття науковцями та практиками. *Науковий вісник. 2023*. С. 374–377.

4. Кіберполіція. Кібербезпека України. Legal Aid Wiki. URL: https://legalaid.wiki/index.php/Кіберполіція._Кібербезпека_України