

3. Про розвідку : Закон України від 17.09.2020 № 912-IX : станом на 31.03.2023. URL: <https://zakon.rada.gov.ua/laws/show/912-20#Text>.

4. В Україні з'явився Ситуаційний центр, що відбиватиме кібератаки: веб сайт. URL: <https://www.ukrinform.ua/rubric-technology/2389847-v-ukraini-zavivsa-situacijnij-centr-so-vidbivatime-kiberataki.html>.

5. Корнейко О.В., Худенко Д.М. Підготовка кримінальних аналітиків у національній академії внутрішніх справ: історія та досвід. *Актуальні питання та перспективи розвитку кримінального аналізу в правоохоронній системі України [Текст] : матеріали міжвідом. наук.-практ. конф. (Київ, 11 серп. 2022 р.) / [редкол.: С. С. Чернявський, Д. І. Овсянюк, В. В. Корольчук]. – Київ : Нац. акад. внутр. справ, 2022. С. 90—93.*

6. Тіхонов С. В., Василичук В. І. Аналітична робота у боротьбі з кримінальними правопорушеннями: шляхи удосконалення. *Актуальні питання удосконалення загальнодержавної системи боротьби з тероризмом в умовах функціонування режиму воєнного стану : зб. Матер. Круглого столу (м. Київ, 31 серпня 2022 року). – Київ: НА СБУ, 2022. С. 127—131.*

**Ткачук Маргарита Геннадіївна,**

слухач магістратури навчально-наукового інституту № 1 Національної академії внутрішніх справ

*Науковий керівник:*

кандидат юридичних наук, старший

викладач кафедри кримінології

та інформаційних технологій

Національної академії внутрішніх справ

**Яровий К. В.**

## **КІБЕРЗЛОЧИННІСТЬ ТА ЇЇ ВПЛИВ НА ПРАВООХОРОННУ ДІЯЛЬНІСТЬ УКРАЇНИ**

Проблематика кіберзлочинності в Україні є особливо актуальною з огляду на її стрімкий розвиток та зростання впливу на правоохоронну діяльність. Сучасні кібератаки та загрози комп'ютерного тероризму визнані одними з ключових чинників, що становлять реальну та потенційну загрозу національній безпеці та суспільній стабільності держави.

Протягом останніх років проблема кіберзлочинності стала вкрай важливою на державному рівні, адже її вплив на правоохоронну систему відчутно зріс.

Серед найуразливіших об'єктів, які найчастіше стають мішенями для кібератак, є критична інфраструктура країни, що включає енергетичні системи, транспортну інфраструктуру та банківський сектор. Інтенсивність та частота кібератак на ці об'єкти підкреслюють необхідність посилення захисту й адаптації правоохоронної системи до сучасних викликів у сфері кібербезпеки. Така ситуація вимагає не лише активного впровадження новітніх методів протидії кіберзагрозам, а й тісної міжвідомчої співпраці та міжнародної взаємодії.

Кіберзлочинність, що вперше згадується в літературі 1960-х років, визначається як порушення прав у сфері автоматизованих систем обробки даних. Зазначене поняття охоплює всі види злочинів у сфері інформаційних технологій включаючи злочини, вчинені у кіберпросторі з використанням комп'ютерних систем, мереж або інших засобів доступу [1, с. 98].

Кіберзлочин (комп'ютерний злочин) – суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України [2].

На нашу думку, протидія кіберзлочинності потребує спільних зусиль державного і приватного секторів, вдосконалення міжнародного та національного законодавства, а також створення ефективного інституційного механізму. Дослідники поділяють кіберзлочини на два типи: нові, зумовлені сучасними технологіями, та традиційні, вчинені за допомогою комп'ютерів і Інтернету. Водночас другий тип чітко не визначений, а державна статистика щодо нього відсутня.

З метою розгляду та порівняння кіберзлочинності в правоохоронній діяльності України, варто звернутися до статистичних даних Офісу Генерального прокурора за 2022 рік, органами правопорядку зареєстровано 3415 кримінальних правопорушень у сфері інформаційних технологій, у 2021 році – 3187 кримінальних правопорушень та у 2020 році – 2498, що свідчить про суттєве зростання вчинення кримінальних правопорушень у сфері інформаційних технологій [3].

Вважаємо за доцільне також звернути увагу на офіційну сторінку Кіберполіції у Facebook, де відображено результати розслідувань кримінальних проваджень за 2023 рік, а саме:

- виявлено понад 3600 кіберзлочинів;
- за оперативного супроводу кіберполіції оголошено підозру понад 1700 особам за вчинення понад 3700 злочинів, що на 59 % перевищує аналогічний показник у 2022 році;
- направлено до суду матеріали щодо 42 організованих злочинних груп, у тому числі 7 злочинних організацій, що на 83% перевищує аналогічний показник у 2022 році;
- проведено 18 міжнародних спецоперацій спільно з правоохоронцями з Грузії, Швейцарії, Чехії, Ізраїлю, Норвегії, Нідерландів, Франції, Німеччини та США;
- за оперативного супроводу кіберполіції направлено до суду обвинувальні акти щодо вчинення понад 4000 злочинів [6].

Підсумовуючи, можна зазначити, що розвиток правоохоронної системи України сприяє швидшому розкриттю кіберзлочинів. Водночас ефективність протидії кіберзагрозам вимагає постійного контролю, підвищення правової грамотності населення, удосконалення законодавства та регулярного навчання фахівців. Кібербезпека є пріоритетом державної політики, що потребує узгоджених дій між державою, суспільством і міжнародною спільнотою.

#### ***Список використаних джерел***

1. Кудінов В. А., Яровий К. В. Інформаційне забезпечення правоохоронної діяльності: навч.-практ. посіб. Київ: Нац. акад. внутр. справ, 2024. 120 с.
2. Про основні засади забезпечення кібербезпеки України. Закон України від 05.10.17 р. № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/term/39984>.
3. Офіційний сайт Офісу Генерального прокурора. URL: <https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravororushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2> (дата зведення: 30.10.2024).
4. Офіційна сторінка Кіберполіції України в Facebook URL: <https://www.facebook.com/cyberpoliceua/videos/722135096772255>.