Романів Р.
аспірант,
Західноукраїнський національний університет,
Пивоварчук Л.
студентка групи ПД-33 юридичного факультету,
Західноукраїнський національний університет

ІНФОРМАЦІЙНА ЗЛОЧИННІСТЬ ЯК ВИКЛИК НАЦІОНАЛЬНІЙ БЕЗПЕЦІ

У сучасному цифровому середовищі інформаційні злочини набули системного та транснаціонального характеру. Йдеться не лише про несанкціонований доступ до інформаційних систем чи розповсюдження шкідливого програмного забезпечення, а й про маніпулювання масовою свідомістю через фейкові кампанії, кібершпигунство та атаки на критичну інфраструктуру. Ці загрози вимагають не просто реагування, а стратегічно вивіреної діяльності спеціалізованих структур — кіберпідрозділів.

Кіберпідрозділи є профільними підрозділами в межах силових та правоохоронних відомств (як-от кіберполіція, департаменти кібербезпеки СБУ, підрозділи в ЗСУ та Нацгвардії), які спеціалізуються на виявленні, розслідуванні й запобіганні злочинам у цифровому просторі. Їх функції включають технічний аналіз, цифрову експертизу, оперативно-розшукову діяльність у мережі та міжнародну співпрацю. Ці структури діють на стику права, ІТ-технологій і інформаційної аналітики.

Успішність кіберпідрозділів безпосередньо залежить від їхньої технічної спроможності. Мова йде не тільки про доступ до сучасного програмного забезпечення для цифрової експертизи чи трекінгу IP-адрес, але й про володіння методами криптоаналізу, протидії DDoS-атакам, виявлення прихованих серверів (darknet) та аналізу великих обсягів даних.

Постійне оновлення інструментарію — передумова гнучкості в умовах стрімкого технологічного розвитку.

Інформаційні злочини часто виходять за межі національної юрисдикції. Тому співпраця кіберпідрозділів із відповідними структурами інших країн, а також із міжнародними організаціями (INTERPOL, EUROPOL, ENISA тощо) є ключовою умовою для виявлення злочинних мереж. Йдеться не тільки про спільні операції, а й про обмін інформацією, участь у міжнародних платформах та аналітичних хабах.

Одна з головних внутрішніх проблем кіберпідрозділів — брак кваліфікованих фахівців, здатних працювати на перетині ІТ і кримінального процесу. Причини цього — низька конкурентна оплата, відтік кадрів у приватний сектор та складність правозастосування в умовах цифрових доказів. Вирішення кадрової проблеми передбачає формування нової освітньої моделі, адаптованої до викликів кібербезпеки.

Чинне кримінальне законодавство України ще не в повній мірі враховує специфіку інформаційних правопорушень. Часто виникають труднощі з юридичною кваліфікацією кіберзлочинів або процедурою збирання цифрових доказів, які можуть не визнаватися судом. Потрібна комплексна модернізація правової бази з урахуванням міжнародного досвіду у сфері боротьби з кіберзлочинністю.

У багатьох випадках жертвами інформаційних злочинів стають комерційні структури, зокрема банки, ІТ-компанії, телекомунікаційні оператори. Ефективність кіберпідрозділів значно підвищується завдяки тісній співпраці з приватним сектором, який володіє технологіями, експертизою і швидкістю реагування. Важливо розвивати механізми публічно-приватного партнерства у сфері кіберзахисту.

У сучасній війні, зокрема в умовах збройної агресії проти України, інформаційні злочини мають чітко виражений гібридний характер. Кіберпідрозділи все частіше залучаються не лише до боротьби з

кіберзлочинністю, а й до протидії інформаційно-психологічним операціям, хакерським атакам на об’єкти критичної інфраструктури та кібершпигунству. Це розширює їх функціонал і вимагає нового рівня інтеграції з сектором безпеки і оборони.

Боротьба з інформаційними злочинами не обмежується лише реагуванням на вже скоєні правопорушення. Один із ключових напрямів діяльності кіберпідрозділів — це превенція. Йдеться про виявлення загроз ще на ранніх етапах: моніторинг потенційно небезпечних ресурсів, аналіз підозрілої активності в мережі, виявлення вразливостей у державних інформаційних системах. Ефективна профілактика дозволяє знизити рівень загроз ще до того, як вони набудуть реальної форми злочину.

В умовах геополітичного протистояння, коли держави використовують кіберпростір як арену впливу, кіберпідрозділи стають інструментом забезпечення цифрового суверенітету. Вони захищають не лише інфраструктуру чи дані, а й право держави самостійно визначати інформаційну політику та забезпечувати недоторканність свого кіберпростору. У цьому контексті діяльність кіберпідрозділів набуває стратегічного виміру.

Для кіберпідрозділів важливо не лише реагувати на загрози, але й бути в курсі новітніх тенденцій у сфері інформаційної безпеки. У цьому сенсі активна взаємодія з університетами, аналітичними центрами, технічними лабораторіями та академічною спільнотою стає джерелом нових рішень. Зокрема, спільні дослідницькі проєкти, хакатони, пілотні моделі цифрового захисту — усе це сприяє посиленню кіберстійкості держави.

Важливо, щоб боротьба з кіберзлочинністю не порушувала базові права громадян, зокрема право на приватність. Тому діяльність кіберпідрозділів повинна бути не лише ефективною, але й правовою: із дотриманням стандартів захисту персональної інформації. Особливо це

стосується обробки цифрових доказів, моніторингу онлайн-активності та доступу до серверів. Будь-яке втручання повинно бути законним, необхідним і пропорційним.

Окрім суто технічної боротьби з хакерськими атаками, кіберпідрозділи все частіше залучаються до протидії інформаційним кампаніям, спрямованим на дестабілізацію ситуації всередині країни. Це охоплює моніторинг соціальних мереж, виявлення "ботоферм", аналіз поширення фейкових повідомлень, координацію дій з центрами стратегічних комунікацій. У цьому аспекті кіберпідрозділи виконують і функцію інформаційного щита.

Інформаційні злочини часто мають транскордонний характер: сервери можуть розташовуватись в одній країні, виконавець — в іншій, а потерпілий — у третій. Це створює складності для національних кіберпідрозділів, які стикаються з обмеженнями юрисдикції. Питання видачі зловмисників, доступу до інформації з іноземних хостингів або визнання цифрових доказів між юрисдикціями — досі залишаються дискусійними.

Діяльність у кіберпросторі завжди пов’язана з балансом між безпекою та правами людини. Коли кіберпідрозділи отримують широкі повноваження для спостереження чи моніторингу, виникають етичні ризики: чи може держава переглядати приватне листування в соцмережах задля "глобальної безпеки"? Відповідь на це питання залежить не лише від закону, але й від ціннісної основи, на якій будується суспільство.

Список використаних джерел

1. Конституція України: Закон України від 28 червня 1996 р. № 254к/96-ВР // Відомості Верховної Ради України. 1996. № 30. Ст. 141.

2. Кримінальний кодекс України: Закон України від 5 квітня 2001 р. № 2341-III // Відомості Верховної Ради України. 2001. № 25–26. Ст. 131.

3. Кримінальний процесуальний кодекс України: Закон України від 13 квітня 2012 р. № 4651-VI // Відомості Верховної Ради України. 2013. № 9–10. Ст. 88.

4. Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 р. № 2163-VIII. Відомості Верховної Ради України. 2017. № 45. Ст. 403.

5. Національна стратегія кібербезпеки України, затверджена Указом Президента України від 14 травня 2021 р. № 187/2021 [Електронний ресурс]. Режим доступу: https://www.president.gov.ua/documents/1872021-38961

6. Білорус О. В. Кіберпідрозділи в системі протидії інформаційним загрозам: організаційно-правовий аспект. Право і безпека. 2022. № 3. С. 46–52.

7. Клименко А. І. Особливості розслідування кіберзлочинів в умовах цифрової трансформації .Юридична наука. 2021. № 7(143). С. 33–39.