УДК 32.019.51:323.28:323

**ГУЦАЛЮК М.В.,** *кандидат юридичних наук, доцент, с.н.с.,*
провідний науковий співробітник Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю при РНБО України.
ORCID: https://orcid.org/0000-0003-4496-5173.

# СТРАТЕГІЇ ПРОТИДІЇ СУЧАСНИМ КІБЕРЗАГРОЗАМ ТА ЗАБЕЗПЕЧЕННЯ КІБЕРСТІЙКОСТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ

***Анотація.*** *У статті розглянуто зростаючі загрози в кіберпросторі та їхній вплив на критичну інфраструктуру. З кожним роком кількість і складність кібератак збільшується, що спричиняє значні збитки для державних і приватних секторів. Основними викликами для кібербезпеки України залишаються гібридна агресія з боку РФ та внутрішні кіберзлочинці, діяльність яких стає дедалі більш організованою та складною. Аналізується сучасний стан кібербезпеки в Україні та пропонуються напрями вдосконалення чинного законодавства з урахуванням інтеграції України до європейського інформаційного простору. Вказано на необхідність розробки нових підходів до забезпечення кіберстійкості, зокрема через оперативне виявлення та розслідування кіберінцидентів.*

***Ключові слова:*** *кібербезпека, кіберзлочинність, кібератака, кіберінцидент, критична інфраструктура, кіберстійкість.*

***Summary.*** *The article examines the growing threats in cyberspace and their impact on critical infrastructure. Each year, the number and complexity of cyberattacks increase, causing significant damage to both the public and private sectors. The main challenges for Ukraine's cybersecurity remain the hybrid aggression from the Russian Federation and internal cybercriminals, whose activities are becoming increasingly organized and sophisticated. The paper analyses the current state of cybersecurity in Ukraine and proposes directions for improving existing legislation, considering Ukraine's integration into the European information space. The necessity of developing new approaches to ensuring cyber resilience is emphasized, particularly through the prompt detection and investigation of cyber incidents.*

***Keywords:*** *cybersecurity, cybercrime, cyberattack, cyber incident, critical infrastructure, cyber resilience.*

**Постановка проблеми.** З кожним роком кількість та складність кібератак у кіберпросторі постійно зростає. Вони можуть бути спрямовані на злам інформаційних систем з метою викрадення чутливої інформації, перешкоджання у роботі інформаційних систем або навіть порушення нормального функціонування критично важливих об'єктів.

Наприклад в США у 2023 році було зареєстровано 2365 кібератак, внаслідок яких постраждали 343.338.964 юридичних та фізичних осіб. При цьому кількість витоків даних зросла на 72 % у порівнянні з 2021 роком, що є історичним рекордом. Витік даних коштував в середньому 4,45 $ млн. [1].

В Україні за даними урядової команди реагування на комп'ютерні надзвичайні події CERT-UA Держспецзв'язку у 2023 році кількість кібератак зросла, порівняно з 2022 роком, на 15,9 % до 2543 інцидентів. 347 кібератак було зафіксовано на уряд та урядові організації, 276 – на місцеві органи влади, 175 – на організації у секторі безпеки та оборони, 127 – комерційні організації [2].

Масштаби збитків від кібератак можна оцінювати на прикладі кіберінциденту в інфраструктурі телекомунікаційного оператора "Київстар", коли приблизно 24 мільйонів користувачів, протягом декількох днів, починаючи з 12 грудня залишилися без зв'язку. Атака знищила "майже все", включаючи тисячі віртуальних серверів і ПК. У деяких регіонах перестали працювати банкомати, які використовували SIM-карти "Київстар" для Інтернету, а сирена повітряної тривоги, яку використовували під час ракетних обстрілів і атак безпілотників, не працювала належним чином. Це, ймовірно, перший приклад деструктивної кібератаки, яка "повністю знищила ядро телекомунікаційного оператора" [3].

Тому сучасні реалії технологічного розвитку та підвищеного ризику в кіберпросторі вимагають оперативно виявляти кіберінциденти та проводити відповідні розслідування для відновлення стабільної роботи інформаційних систем, посилення їх кібербезпеки та мінімізації збитків.

Проблемам кібербезпеки, у тому числі критичної інфраструктури приділялася значна увага як вітчизняними так і закордонним науковцями. Слід зазначити роботи таких науковців як Бурячок В.Л., Гнатюк С.О., Дубов Д.В., Марущак А.І., Ткачук Н.А., Шеломенцев В.П., Юдін О.К. та ін. Посилилась увага і до проблем протидії кіберзлочинності, зокрема в роботах таких науковців, як Ахтирська Н.М., Біленчук П.Д., Гавловський В.Д., Кравцова М.О., Яцишина М.А., Самойленко О.А. та багатьох інших. Водночас в зв'язку з динамічною зміною кіберзагроз, методів та способів здійснення кібератак, подальшою глобалізацією суспільства та інтенсифікацією використання інформаційних технологій постає необхідність пошуків нових підходів щодо забезпечення кібербезпеки в сучасних умовах.

**Метою статті** є аналіз сучасного стану кібербезпеки та кіберзлочинності в Україні та визначення напрямів вдосконалення чинного законодавства у даних сферах з врахуванням інтеграції України в європейський інформаційний простір та забезпечення кіберстійкості.

**Виклад основного матеріалу.** Основною загрозою кібербезпеці України в сучасних умовах залишається гібридна агресія рф у кіберпросторі. Дана кіберзагроза була зазначена у Стратегії кібербезпеки України і, нажаль, постійно посилюється після повномасштабного вторгнення рф. Напередодні та під час кінетичних атак кібернападу зазнали державний, енергетичний, медійний, фінансовий сектори, посилились спеціальні кампанії з дезінформації, значно поширилося розповсюдження фішингових електронних листів та діпфейків.

Крім зовнішніх кіберзагроз в Україні залишається складною ситуація з кіберзлочинністю. Аналіз офіційної статистичної звітності Офісу Генерального прокурора України щодо облікованих кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку свідчить, що порівняно з 2022 роком кількість облікованих кримінальних правопорушень, передбачених статтями Розділу XVI КК України, збільшилася на 12,5 % (у 2022 році – 3415).

Варто відмітити, що кількість особливо тяжких кримінальних правопорушень збільшилася у 7 разів порівняно з 2022 роком (108 у 2022 році проти 756 у 2023 році), кримінальних проступків – у 1,7 рази (247 у 2022 році проти 431 у 2023 році), нетяжких кримінальних правопорушень – у 1,5 рази (905 у 2022 році проти 1400 у 2023 році).

Посилилась організованість кіберзлочинності. До суду у 2023 році скерували матеріали щодо 42 організованих злочинних груп, у тому числі семи злочинних організацій, що на 83 % перевищує аналогічний показник у 2022 році [4].

Окрім того, що Україна перебуває в стані кібервійни з рф, яка спонсорує діяльність кіберугрупувань, не зменшують свою активність і вітчизняні кіберзлочинці, які діють у складі міжнародних організованих злочинних угруповань. Їх злочинна діяльність спрямована як на українських користувачів Інтернету, так і на більш коштовні європейські та північноамериканські ринки.

Так, наприклад, наприкінці 2023 року оперативники Департаменту кіберполіції та слідчі Головного слідчого управління Нацполіції провели багаторівневу спецоперацію у складі об'єднаної слідчої групи JIT (The Joint Investigation Team) до якої також увійшли колеги з Європолу (установа правопорядку ЄС з протидії міжнародній організованій злочинності) та Євроюсту (агентство, що координує судові органи ЄС).

У результаті багатомісячної кропіткої роботи українські правоохоронці за сприяння колег з США, Норвегії, Нідерландів, Німеччині та Франції ідентифікували 32-річного лідера хакерського угруповання та його чотирьох найактивніших спільників. Для хакерських атак фігуранти використовували самостійно розроблене шкідливе програмне забезпечення, зокрема, кілька вірусів-шифрувальників.

За дешифрування інформації члени міжнародної хакерської групи вимагали мільйонні виплати у криптовалюті. Наприклад, за відновлення роботи серверів однієї з провідних хімічних компаній Нідерландів, зловмисники вимагали перерахувати 450 BTC (біткоінів) на підконтрольний криптогаманець, що в еквіваленті складає 48 мільйонів гривень. Встановлено, що за кілька років злочинної діяльності зловмисники зашифрували понад 1000 серверів світових підприємств та спричинили збитків на суму у понад 3 мільярди гривень в перерахунку на національну валюту [5].

У лютому 2024 року кіберфахівці Служби безпеки спільно з правоохоронними органами США, Великої Британії та Євросоюзу викрили міжнародне угруповання хакерів-вимагачів LockBit.

Серед організаторів та учасників угруповання були громадяни України та рф. Протягом майже 5 років зловмисники здійснили більше ніж 3000 кібератак проти фінансових установ та корпорацій західних країн, які надають оборонну допомогу Україні. Задокументовано, що тільки з однієї із американських компаній хакери вимагали понад 90 $ млн. США.

Повідомляється, що в США і семи країнах Євросоюзу вилучено понад 30 серверів, з яких зловмисники проводили кібератаки і на яких зберігали викрадені дані, а також заблоковано понад 200 криптовалютних рахунків злочинного угруповання [6].

У 27 – 29 травня 2024 року була проведена масштабна міжнародна операція Endgame, яка була ініційована й проведена Францією, Німеччиною та Нідерландами. Різними діями (арешти, допити підозрюваних, обшуки, вилучення й видалення серверів та доменів) операцію підтримали Вірменія, Болгарія, Литва, Португалія, Румунія, Швейцарія й Україна. Це найбільша в історії операція проти ботнетів, які відіграють важливу роль у розгортанні програм-вимагачів. Понад 100 Інтернет-серверів, які використовувалися для створення і розповсюдження шкідливих програм було від'єднано від мережі або заблоковано. Трьох із чотирьох злочинців заарештували в Україні.

В повідомленні Європолу зазначається, що шкідливе програмне забезпечення дозволяє кіберзлочинцям таємно під'єднуватися до комп'ютерів людей у шкідливих цілях. За даними слідчих, один із головних підозрюваних заробив не менше 69 € млн. у криптовалюті, здаючи в оренду об'єкти кримінальної інфраструктури для розміщення програм-вимагачів [7].

Показовим є той факт, що відповідно до світового індексу кіберзлочинності Україна займає 2 місце після рф, “випередивши” Китай, Північну Корею та Іран.

Світовий індекс кіберзлочинності (WCI) ранжує країни на основі їх внеску в глобальну кіберзлочинність (див Табл.). Ранжування встановили дослідники з Оксфордського університету та UNSW Canberra, які опросили 245 експертів з кіберзлочинності (отримавши 92 відповіді) з кожного регіону світу розглянути п’ять основних типів кіберзлочинності:

- технічна продукція/послуги;
- напади та вимагання;
- крадіжка даних/ідентифікації;
- шахрайство;
- виведення/відмивання грошей.

Табл. Світовий індекс кіберзлочинності (WCI).

| ***Ranking*** | ***Country*** | ***WCI Score*** | ***Ranking*** | ***Country*** | ***WCI Score*** |
|---|---|---|---|---|---|
| 1 | Russia | 58.39 | 11 | Iran | 4.78 |
| 2 | Ukraine | 36.44 | 12 | Belarus | 3.87 |
| 3 | China | 27.86 | 13 | Ghana | 3.58 |
| 4 | United States | 25.01 | 14 | South Africa | 2.58 |
| 5 | Nigeria | 21.28 | 15 | Moldova | 2.57 |
| 6 | Romania | 14.83 | 16 | Israel | 2.51 |
| 7 | North Korea | 10.61 | 17 | Poland | 2.22 |
| 8 | United Kingdom | 9.01 | 18 | Germany | 2.17 |
| 9 | Brazil | 8.93 | 19 | Netherlands | 1.92 |
| 10 | India | 6.13 | 20 | Latvia | 1.68 |

Це лише перший етап у великому дослідницькому проекті. Професор Федеріко Варезе, співавтор дослідження, сказав веб-сайту Оксфордського університету, що він та його колеги-дослідники “сподіваються розширити дослідження, щоб ми могли визначити, чи національні характеристики, такі як рівень освіти, проникнення Інтернету, ВВП чи рівні корупції пов’язані з кіберзлочинністю”.

Визначення цих факторів матиме вирішальне значення для запобігання кіберзлочинності в майбутньому. Хоча в деяких країнах чинники, що сприяють кіберзлочинності, можуть бути відносно очевидними, і їх важко позбутися (наприклад, росія славиться терпимістю та навіть заохочує кіберзлочинців), в інших країнах розуміння цих факторів може сприяти запобіжним діям [8].

Варто зазначити, що з початку повномасштабної агресії рф всі сили суб’єктів забезпечення кібербезпеки України були спрямовані на захист державних реєстрів та стабільного функціонування об’єктів критичної інфраструктури. І це вдалося здійснити, у тому числі завдяки міжнародній підтримці та належному стратегічному плануванню у попередні роки.

Зокрема у Стратегії кібербезпеки України, затвердженій Указом Президента України від 26.08.21 р. № 447/2021 були визначені нові виклики і кіберзагрози, а також підкреслена роль забезпечення кібербезпеки, як одного із пріоритетів у системі національної безпеки України.

В останні роки була суттєво вдосконалена та розширена система нормативно-правових актів, які регулюють питання забезпечення кібербезпеки, у тому числі на

об’єктах критичної інфраструктури та протидію кіберзлочинності. Зокрема, слід зазначити такі документи, як:

- Закон України “Про критичну інфраструктуру” від 16.11.21 р. № 1882-IX;
- Закон України “Про хмарні послуги” від 17.02.22 р. № 2075-IX;
- Закон України “Про внесення змін до Кримінального процесуального кодексу України” та Закону України “Про електронні комунікації” щодо підвищення ефективності досудового розслідування “за гарячими слідами” та протидії кібератакам від 15.03.22 р. № 2137-IX;
- Закон України “Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану” від 24.03.22 р. № 2149-IX;
- Постанова Кабінету Міністрів України від 19.06.19 р. № 518 “Про затвердження загальних вимог до кіберзахисту об’єктів критичної інфраструктури”;
- Постанова Кабінету Міністрів України від 04.04.23 р. № 299 “Деякі питання реагування суб’єктами забезпечення кібербезпеки на різні види подій у кіберпросторі”;
- Наказ Адміністрації Держспецзв’язку від 03.07.23 р. № 570 “Про затвердження Методичних рекомендацій щодо реагування суб’єктами забезпечення кібербезпеки на різні види подій у кіберпросторі” тощо.

Так Постановою Кабінету Міністрів України від 04.04.23 р. № 299 затверджено “Порядок реагування суб’єктами забезпечення кібербезпеки на різні види подій у кіберпросторі”.

Порядком реагування на кіберінциденти визначено їх критичність відповідно до 6 рівнів (0 – 5):

рівень 0, некритичний (білий);
рівень 1, низький (зелений);
рівень 2, середній (жовтий);
рівень 3, високий (помаранчевий);
рівень 4, критичний (червоний);
рівень 5, надзвичайний (чорний) [9].

Постановою Кабінету Міністрів України від 03.06.22 р. № 522 був затверджений “Порядок надання послуг Національного центру резервування державних інформаційних ресурсів”. Цей нормативно-правовий акт визначає механізм надання користувачам послуг Національного центру резервування державних інформаційних ресурсів, який функціонує у Держспецзв’язку. В додатку до Порядку надано перелік з майже 40 послуг, який надає даний Центр.

Посилено також і організаційне забезпечення у сфері кібербезпеки. Зокрема, координацію діяльності суб’єктів забезпечення кібербезпеки здійснює Національний координаційний центр кібербезпеки, при якому створена постійна Об’єднана група реагування на кіберінциденти/кібератаки.

В умовах правового режиму воєнного стану заходи реагування на кіберінциденти здійснюються з урахуванням заходів стримування та відсічі збройної агресії проти України, визначених для основних суб’єктів національної системи кібербезпеки директивами, бойовими наказами (розпорядженнями) Головнокомандувача Збройних Сил України.

Водночас виявлення кіберінцидентів та кіберзлочинів постійно ускладнюється, що пов’язано з низкою технічних, правових та організаційних перешкод. Наведемо основні проблеми, які можуть виникати під час виявлення кіберінцидентів:

1. Кіберзлочинці використовують різноманітні техніки і методи для досягнення своїх цілей, від простих фішингових атак до складних багатоступеневих вторгнень. Через це складно створити універсальні методи виявлення, оскільки загрози постійно розвиваються.

2. Складність ідентифікації джерела кіберзлочину внаслідок використання методів приховування злочинної діяльності, такі як шифрування, стеганографія, мережі Tor або VPN.

3. Відсутність видимих ознак кіберзлочину. Це ускладнює виявлення інцидентів, оскільки потрібен ретельний аналіз комп'ютерних даних та логів для виявлення аномалій.

4. Висока швидкість розвитку технологій. Технології розвиваються дуже швидко, що створює додаткові складнощі для захисників кібербезпеки. Нові методи та інструменти злочинців можуть з'явитися раніше, ніж організації встигають адаптуватися до них.

5. Великий обсяг даних. Сучасні системи генерують величезний обсяг даних, включаючи логи, мережевий трафік, дані про користувачів тощо. Обробка та аналіз цього обсягу даних можуть бути надзвичайно складними, що ускладнює виявлення аномалій.

6. Брак кваліфікованих спеціалістів. У сфері кібербезпеки існує значний брак кваліфікованих фахівців, що створює додаткові труднощі для виявлення та реагування на кіберінциденти. Недостатня кількість спеціалістів може призвести до повільної реакції та невчасного виявлення інцидентів.

7. Вартість і ресурси. Виявлення кіберзлочинів вимагає значних ресурсів, таких як технології, обладнання, програмне забезпечення, а також кваліфікованих спеціалістів. Для багатьох організацій, особливо невеликих, ці витрати можуть бути надто високими.

Усі ці фактори разом ускладнюють завдання виявлення кіберінцидентів та кіберзлочинів. Успішне протистояння цим викликам потребує комплексного підходу, поєднання сучасних технологій, кваліфікованих спеціалістів і міжнародної співпраці.

Зупинимося окремо на технології, яку останніми роками використовують як кіберзлочинці так і кіберзахисники – це штучний інтелект (далі – ШІ). Якщо кіберзлочинці використовують ШІ для написання зловмисних кодів, то для кіберзахисників ця технологія стає важливим інструментом у виявленні та реагуванні на кіберінциденти. Перший у світі закон про штучний інтелект (Intelligence Act) був ухвалений 13 березня 2024 року Європейським Парламентом. Документ покликаний забезпечити безпеку і дотримання прав громадян [10].

Використання кіберзлочинцями ШІ призводить до експоненціального зростання кіберризиків завдяки можливості використання нових, дедалі складніших методологій атак хакерами або злочинними угрупованнями. ШІ дозволяє розробляти нові типи дедалі більш витончених алгоритмів для створення шкідливого коду, поширення більш адаптивного зловмисного програмного забезпечення, скорочення часу для запуску атак "0 дня", а також використання мультимедійних глибоких фейків, починаючи від шахрайства до кампаній дезінформації під час національних виборів.

Використання ШІ у системах кіберзахисту допоможе аналізувати величезні обсяги даних для виявлення аномалій, які можуть бути ознаками кіберзагроз. Аналіз даних відбувається в реальному часі, ідентифікуючи загрози та реагуючи на них набагато швидше, ніж людина. Це дозволяє виявляти складні атаки, які могли б залишитися непоміченими традиційними методами.

Крім того, поєднання різних типів даних, таких як мережевий трафік, журнали активності користувачів, вразливості програмного забезпечення та інші джерела, дозволяє ШІ створювати більш точні моделі для виявлення загроз. Це дає змогу виявляти складні атаки, які можуть використовувати різні вектори одночасно.

Також ШІ може використовуватися для автоматизації відповіді на інциденти. Це включає автоматичне ізолювання заражених систем, блокування підозрілих IP-адрес чи зміну конфігурацій для запобігання подальшому поширенню загрози.

Завдяки використанню ШІ можна зменшити навантаження на команди кібербезпеки, автоматизуючи рутинні завдання і дозволяючи експертам зосередитися на складніших проблемах та стратегічних питаннях.

Однією зі стратегічних цілей і невід'ємною частиною забезпечення кібербезпеки є протидія кіберзлочинності. Чинне місце у заходах протидії злочинному використанню інформаційних технологій належить розслідуванню кіберзлочинів. Вирішальне значення при розслідуванні кіберзлочинів має аналіз електронних доказів, збереження їх цілісності та належного зберігання для використання у кримінальному судочинстві. Водночас на сьогодні ці питання не повною мірою врегульовані чинним законодавством України. Зокрема поняття електронних (цифрових) доказів відсутнє в Кримінальному процесуальному кодексі України.

Поряд з цим існує низка як зарубіжних так і вітчизняних досліджень щодо використання електронних доказів у кримінальних провадженнях. Зокрема такі дослідження проводилися і у Міжвідомчому науково-дослідному центрі з проблем боротьби з організованою злочинністю при РНБО України.

При роботі з електронними доказами слід дотримуватися наступних принципів:

1. *Законність.* Працівники та підрозділів, що провадять розслідування і досліджують докази в електронній формі, зобов'язані дотримуватися чинного законодавства, загальних процесуальних та криміналістичних принципів.

2. *Цілісність даних*. Дії фахівця не повинні призводити до матеріальних змін даних, електронних пристроїв чи носіїв інформації, які можуть використовуватись як докази. Це включає в себе копіювання даних, фіксацію мережевого трафіку та заборону доступу до системи або даних, що розслідуються.

3. *Документування процесу*. Документують будь-які дії, виконувані стосовно електронних доказів, і зберігають ці документи на випадок перевірки, щоб незалежна третя сторона могла повторити ці дії та отримати аналогічний результат.

4. *Експертна підтримка*. Якщо передбачається, що при огляді (обшуку) можуть бути виявлені електронні докази, отримують підтримку фахівців (спеціалістів), забезпечивши, за можливості, їх присутність на місці події.

5. *Відповідна фахова підготовка*. Якщо при огляді (обшуку) відсутні фахівці з електронних доказів, першочергові дії на місці події здійснюють особи, які мають необхідні знання та навички для виявлення і збирання доказів.

6. *Розумна обережність*. Уникають будь-яких навмисних або ненавмисних дій, які можуть призвести до пошкодження потенційних доказів, представлених у цифровій формі [11].

Електронні докази можуть зберігатися не тільки на пристроях, які були атаковані, але й у постачальників (провайдерів), у тому числі і закордонних, а також власне на гаджетах, якими користувалися підозрювані у вчиненні кіберзлочинів – адже кіберзлочинці більше половини кіберзлочинів вчиняють з інших країн, користуючись відсутністю кордонів у кіберпросторі.

Тому, як зазначено в Конвенції про кіберзлочинність, ратифікованою Україною у 2005 році, ефективна боротьба з кіберзлочинністю вимагає більшого, швидкого і ефективно функціонуючого міжнародного співробітництва у кримінальних питаннях. Конвенцією зокрема передбачено, що кожна сторона вживає законодавчі та інші заходи та застосовує повноваження і процедури для збору доказів у електронній формі

стосовно кримінального правопорушення. Також кожна Сторона призначає орган для здійснення контактів цілодобово впродовж тижня з метою надання негайної допомоги для розслідування або переслідування стосовно кримінальних правопорушень, пов'язаних з комп'ютерними системами і даними, або з метою збирання доказів у електронній формі. Такий контактний пункт 24/7 тривалий час вже функціонує в Департаменті кіберполіції НП України. Також активний обмін інформацією з зарубіжними партнерами проводиться шляхом використання Мережевого додатку безпечного обміну інформацією (Secure Information Exchange Network Application – SIENA) Європолу.

Водночас ще не імплементовані в чинне законодавство такі статті Конвенції, як: ст. 16 – "Термінове збереження комп'ютерних даних, які зберігаються" та ст. 17 – "Термінове збереження і часткове розкриття даних про рух інформації".

У зв'язку з необхідністю посилення ефективності взаємодії як між державами так і з приватним сектором, якому належить переважна частина інформаційної інфраструктури, у травні 2022 року в Римі було започатковано підписання Другого додаткового протоколу до Конвенції про кіберзлочинність. Даний документ надає такі механізми для розкриття електронних доказів, як пряма співпраця з постачальниками електронних послуг і реєстраторами в різних країнах, ефективні засоби отримання інформації про абонентів і даних про трафік, негайне співробітництво в надзвичайних ситуаціях або спільні розслідування тощо. Протокол був підписаний і Україною, проте ще не ратифікований Верховною Радою України.

Сьогодні, крім кіберзлочинів, електронні докази активно використовуються для розслідування традиційних злочинів. У ЄС більше половини всіх кримінальних розслідувань сьогодні включають транскордонні запити на доступ до електронних доказів, таких як текстові повідомлення, електронні листи або програми обміну повідомленнями. Саме тому Комісія ЄС запропонувала кілька дій, щоб спростити та пришвидшити для поліції та судових органів доступ до електронних доказів, необхідних їм у розслідуваннях та засудження злочинців, у тому числі терористів.

Зокрема у липні 2023 року був розроблений Регламент щодо європейських ордерів на пред'явлення та європейських ордерів на збереження електронних доказів у кримінальному провадженні [12].

Регламент передбачає:

- створення європейського наказу про пред'явлення документів: це дозволить судовому органу в одній державі-члені отримати електронні докази (такі як електронні листи, текстові повідомлення або повідомлення в програмах, а також інформацію для ідентифікації злочинця як перший крок) безпосередньо від постачальника послуг або його законного представника в іншій державі-члені, який буде зобов'язаний відповісти протягом 10 днів, а в екстрених випадках – протягом 8 годин (порівняно з до 120 днями для існуючого європейського наказу про розслідування або в середньому 10 місяцями для процедури взаємної правової допомоги);
- створення європейського наказу про збереження: це дозволить судовому органу в одній державі-члені вимагати, щоб постачальник послуг або його законний представник в іншій державі-члені зберіг певні дані з огляду на наступний запит на отримання цих даних через взаємну правову допомогу, європейський Ордер на розслідування або європейський ордер на виробництво;
- сильні гарантії: нові правила гарантують надійний захист фундаментальних прав, включаючи гарантії права на захист персональних даних. Особи, дані яких запитуються, отримають різні гарантії та право на засоби правового захисту. Органи влади держави-

члена, де зареєстрований або представлений постачальник послуг, будуть задіяні в певних випадках через механізм сповіщення та можуть припинити виробництво даних на основі списку з чотирьох підстав. Передбачено спеціальну процедуру залучення судді чи суду, якщо постачальник послуг є суб'єктом колізійного права;

- створення децентралізованої IT-системи, за допомогою якої весь зв'язок між органами влади та постачальниками послуг може відбуватися безпечним і надійним способом, забезпечуючи автентифікацію всіх учасників.
- зобов'язання постачальників послуг призначити установу або призначити законного представника в Союзі: щоб гарантувати, що всі постачальники, які пропонують послуги в Союзі, підпадають під однакові зобов'язання, навіть якщо їх штаб-квартира знаходиться в третій країні, вони повинні призначити створювати або призначати законного представника в Союзі для отримання, дотримання та забезпечення виконання рішень і наказів.
- забезпечення юридичної визначеності для підприємств і постачальників послуг: тоді як сьогодні правоохоронні органи часто залежать від доброї волі постачальників послуг щодо надання їм необхідних доказів, у майбутньому застосування однакових правил доступу до всіх постачальників послуг покращить правову визначеність і чіткість.

Нові правила набули чинності 17 серпня 2023 року та застосовуватимуться з 17 серпня 2026 року [13].

У зв'язку з важливістю розслідування кіберінцидентів на об'єктах критичної інфраструктури у Департаменті кіберполіції НП України створено окреме управління захисту критичної інфраструктури.

Слід звернути увагу на те, що діяльність кіберугрупувань рф спрямована не тільки на українські інформаційні системи, але і на інформаційну інфраструктуру багатьох інших демократичних країн. Глава Європейського агентства з кібербезпеки (ENISA) Юхан Лепассаар заявив, що кількість деструктивних кібератак у ЄС, до багатьох із яких причетні підтримувані росією групи, подвоїлася за останні місяці. Хакерські атаки, зокрема, націлені на сервіси, пов'язані з виборами. Він також додав, що це частина російської агресивної війни, яку вони ведуть фізично проти України, але також і в цифровій формі по всій Європі [14].

Під час виступу на міжнародній конференції CYBERSEC FORUM "Об'єднані в кіберсилі" 17 – 18 травня 2022 року в Катовіце заступник голови Держспецзв'язку Олександр Потій запропонував розробити Концепцію кіберстримування. Розробка такої програми має бути аналогічною програмі ядерного стримування, – наголосив заступник очільника Держспецзв'язку. Серед ключових критеріїв такої концепції:

- Формування державами відповідних кіберспроможностей та здатності проводити активні кібероперації проти агресора.
- Ефективна атрибуція: коли агресор точно знає, що його ідентифікують.
- Невідворотність покарання за кіберзлочини. Для фізичних осіб – кримінальне переслідування. Для юридичних осіб і держав – застосування санкцій.
- Розроблення та впровадження системи превентивних заходів проти створення, придбання й поширення кіберзброї та засобів для проведення кібератак.
- Урядовий контроль розроблення кіберзброї та проведення активних кібероперацій.
- Запровадження кіберзахисту на всіх рівнях: від міжнародного – до дрібної компанії.

•Запровадження єдиних правил відповідальної поведінки у кіберпросторі, які є обов'язковими для всіх країн [15].

Водночас інші, патріотично налаштовані хакери допомагають спецслужбам України отримувати цінну інформацію з ресурсів рф, проводити інформаційні операції, приводити до збоїв у роботі різноманітних важливих об'єктів ворога.

Українська хакерська група "Блекджек", пов'язана з головним розвідувальним агентством країни, викрала плани будівництва понад 500 російських військових об'єктів. Блекджеку вдалося отримати понад 1,2 терабайта секретних даних.

Ці дані містять карти понад 500 російських військових баз по всій території Росії та в регіонах України, які окупував путін. Це і військові штаби російської армії, і засоби протиповітряної оборони, і арсенали озброєння.

У ГУР додали, що в рамках кібероперації "Блекджек" було видалено всі викрадені дані з семи російських серверів. Українське інформаційне агентство "Інтерфакс" повідомило, що хакери також вивели з ладу 150 комп'ютерів [16].

Нажаль, на сьогодні, нормативне регулювання кібервійни не відсутнє. Зокрема, наприклад, є дискусійним питання про втручання в діяльність цивільних об'єктів супротивника. І де межа між кібервійськовою та кримінальною діяльністю.

Також, на нашу думку, слід активно розбудовувати вітчизняні кібервійська, які могли б більш чітко виконувати відповідні спеціальні операції у кіберпросторі.

Одним з нових механізмів захисту інтересів у кіберпросторі є кібердипломатія. Президент України Володимир Зеленський пропонує Верховній Раді додати Міністерству закордонних справ функцію кібердипломатії. Про це йдеться у проєкті закону № 10370, зареєстрованому у Верховній Раді України 22 грудня 2023 року.

У законопроєкті зазначається, що кібердипломатія – комплекс дій та стратегій, спрямованих на просування та захист національних інтересів і реалізацію зовнішньополітичних цілей України в кіберпросторі, а також підтримання дипломатичних зносин з іноземними державами, їх об'єднаннями та міжнародними організаціями з відповідних питань [17].

У липні 2023 року на засіданні Національного координаційного центру кібербезпеки учасники засідання обговорили питання щодо розбудови кібердипломатії, стану виконання Стратегії кібербезпеки України та підвищення ефективності щорічного планування реалізації її завдань, а також про додаткові заходи кібербезпеки систем управління технологічними процесами на об'єктах критичної інфраструктури. Учасники засідання підтримали пропозицію заступника Секретаря РНБО України щодо необхідності формування підходів до реалізації заходів у сфері кібердипломатії Міністерством закордонних справ України, а комунікації з міжнародними партнерами – за участю НКЦК та основних суб'єктів національної системи кібербезпеки для забезпечення узгодженої позиції. У цьому контексті обговорено питання щодо створення міжвідомчої робочої групи та відповідної цифрової платформи.

Євросоюз вдається до кібердипломатії, щоб у рамках міжнародної співпраці захищати свій кіберпростір. У 2017 році ЄС запустив відповідний інструментарій, наприклад санкції за зловмисну кібердіяльність. Дипломатична відповідь ЄС на зловмисну кібердіяльність повністю використовуватиме заходи в рамках Спільної зовнішньої політики та політики безпеки, включаючи, якщо необхідно, обмежувальні заходи. Спільна відповідь ЄС на зловмисну кібердіяльність буде пропорційною обсягу, масштабу, тривалості, інтенсивності, складності, витонченості та впливу кіберактивності [18].

Пізніше на підтримку кібердипломатії був запущений проект EU Cyber Direct – ініціатива кібердипломатії ЄС, що фінансується ЄС і зосереджена на підтримці політики, дослідженнях, охопленні та розбудові потенціалу у сфері кібердипломатії.

EU Cyber Direct фокусується на чотирьох ключових темах:

- запобігання конфліктам і просування відповідальної поведінки в кіберпросторі через міжнародне право, норми та заходи зміцнення довіри (CBMs);
- кіберстійкість і захист критичної інфраструктури;
- кіберзлочинність і кримінальне правосуддя в кіберпросторі;
- нові та перспективні технології з потенційним руйнівним ефектом.

EU Cyber Direct реалізується спільно Інститутом досліджень безпеки ЄС (координатор) у співпраці з Інститутом безпеки та глобальних справ Лейденського університету [19].

На міжнародному рівні, у тому числі в рамках ООН сьогодні проводяться консультації щодо розробки всеосяжної міжнародної конвенції про протидію використанню інформаційно-комунікаційних технологій у злочинних цілях.

Зокрема Резолюція 74/247 Генеральної Асамблеї ООН (27 грудня 2019 р.) заснувала спеціальний міжурядовий комітет відкритого складу експертів і представників усіх регіонів для розробки зазначеної всеосяжної міжнародної конвенції.

Як це не абсурдно, але перший проект Конвенції подала країна, яка сама найбільше використовує ІКТ в злочинних цілях – рф.

Запропонована Конвенція має кілька амбітних цілей:

a. вона просить кожну державу-учасницю вжити таких законодавчих та інших заходів, які необхідні для визнання правопорушенням згідно з її внутрішнім законодавством про кіберзлочинність;

b. визначає нові процедури правового співробітництва щодо кіберзлочинності;

c. засновує міжнародну технічну комісію з боротьби зі злочинністю у сфері ІКТ для надання допомоги державам у перегляді виконання Конвенції.

Основною відмінністю даного проекту Конвенції від існуючої європейської Конвенції з кіберзлочинності є те, що в ній пропонується принцип суверенітету. Це відображено в преамбулі, де зазначено, “що кожна держава має суверенітет і здійснює юрисдикцію над своєю територією щодо інформаційного простору відповідно до свого національного законодавства”. Тобто Конвенція забороняє транскордонні операції, які здійснюються комп’ютерними мережами держав без схвалення їхніх органів влади. В той же час Будапештська конвенція 2001 року дозволяє транскордонні кібероперації.

На сьогодні експерти з кібербезпеки країн ЄС та США виступають за відкритий і безпечний кіберпростір, який зберігає вільний потік інформації в усьому світі, тоді як інша група на чолі з Росією і Китаєм прагне встановити режим управління, який би забезпечив більший державний контроль над кіберпростором. Враховуючи зазначене, а також високий рівень амбіцій запропонованої Конвенції та відповідні фінансові потреби (головним чином через створення Міжнародної технічної комісії), ймовірно, що шлях до формування Конвенції буде довгим і важким [20].

Іншим важливим документом на рівні ООН є Глобальний цифровий договір, який має бути узгоджений на Саміті майбутнього у вересні 2024 року через технологічне напрямок із залученням усіх зацікавлених сторін: урядів, системи ООН, приватного сектору (включно з технологічними компаніями), громадянського суспільства, низового рівня організації, наукових кіл та окремих осіб, включно з молоддю.

Очікується, що Глобальний цифровий договір “викладе спільні принципи відкритого, вільного та безпечного цифрового майбутнього для всіх”. Він може охопити,

зокрема цифрове підключення, уникнення фрагментації Інтернету, надання людям варіантів щодо використання їхніх даних, застосування прав людини в Інтернеті та просування надійного Інтернету шляхом запровадження критеріїв відповідальності за дискримінацію та дезінформацію [21].

На європейському рівні у червні 2021 року відбувся перший раунд Кібердіалогу Україна – Європейський Союз, на якому наша держава та ЄС підтвердили свою відданість глобальному, відкритому, стабільному та безпечному кіберпростору, який повністю відповідає принципам верховенства права.

Під час зустрічі сторони також порушили питання цифрової трансформації та діяльності з розбудови спроможностей, які сприяють кіберстійкості та боротьбі з кіберзлочинністю в Україні та світі. Сторони підкреслили важливість кібербезпеки як необхідного елемента забезпечення довіри до зусиль з цифрової трансформації та продемонстрували відданість активізації підтримки в цій сфері [22].

У грудні 2023 року був запущений Талліннський механізм, покликаний підтримати та покращити кіберзахист України, зокрема в довгостроковій перспективі. Учасниками коаліції даного механізму стануть Естонія, Канада, Данія, Франція, Німеччина, Нідерланди, Польща, Швеція, Великобританія та США. Європейський Союз та НАТО матимуть статус спостерігачів.

Раніше кібердопомога Україні надавалася за потреби. Тепер союзники працюватимуть над нею системно та скоординовано [23].

Також важливу роль відіграє ІТ-коаліція – спеціальна група держав у межах Контактної групи з питань оборони України (“формат Рамштайн”) під керівництвом Естонії та Люксембургу, яка зосереджена на наданні підтримки Міністерству оборони та Збройним силам України у сфері ІТ, зв’язку й кібербезпеки.

У межах ІТ-коаліції вже вдалося зібрати фінансових та матеріальних внесків більш як на 36 € млн. Внески в розмірі понад 23 € млн. ще очікуються [24].

**Висновки.**

Виявлення, припинення та розслідування кіберінцидентів є фундаментальними для забезпечення безпеки, стабільності та добробуту в сучасному суспільстві. Вони дозволяють протистояти загрозам, що виникають у цифровому світі, та захищати критично важливі інтереси як окремих осіб, так і суспільства в цілому. Виявлення і припинення кіберінцидентів на державному рівні допомагає запобігти катастрофічним наслідкам для країни.

Розслідування кіберінцидентів дозволяє виявити і притягнути до відповідальності кіберзлочинців. Це не лише забезпечує справедливість для постраждалих, але й служить потужним засобом стримування для потенційних кіберзлочинців, які, на жаль, навіть в умовах воєнного стану не залишають злочинну діяльність.

В Україні проведена значна робота по унормуванню нормативно-правової бази у сфері забезпечення кібербезпеки. Водночас залишається невирішеною низка проблем, до яких слід віднести неврегульованість на законодавчому рівні електронних доказів, які є ключовими при розслідуванні кіберінцидентів та неповну імплементацію положень Конвенції про кіберзлочинність, зокрема щодо збереження електронних доказів.

Окрему увагу слід приділити імплементації європейського законодавства у сфері кібербезпеки, зокрема NIS2, що дозволить ефективно протидіяти кіберзагрозам.

Слід нарощувати темпи підготовки нових кіберфахівців, та продовжувати практику перепідготовки та тренінгу існуючих штатних одиниць в підрозділах кібербезпеки, особливо на об’єктах критичної інфраструктури. Практичне навчання слід проводити в спеціалізованих центрах, наприклад, на базі Інституту спеціального зв’язку та захисту

інформації Національного технічного університету України “Київський політехнічний інститут імені Ігоря Сікорського”.

У зв’язку з кадровими та фінансовими обмеженнями слід посилити використання штучного інтелекту та інших новітніх технологій у системах кіберзахисту.

Зважаючи на те, що, що система резервного копіювання є критично важливою для забезпечення стійкості до атак типу ransomware, слід посилити можливості Національного центру резервування державних інформаційних ресурсів.

Необхідно постійно посилювати міжнародну співпрацю по такими напрямами як обмін інформацією про кіберінциденти, обмін інформацією про кіберзлочини, участь у роботі міжнародних спільних слідчих групах, кібердипломатія.

## Використана література

1. Cybersecurity Stats: Facts And Figures You Should Know. URL: https://www.forbes.com/advisor/education/it-and-tech/cybersecurity-statistics

2. Урядова команда CERT-UA в 2023 році опрацювала 2543 кіберінциденти. URL: https://cip.gov.ua/ua/news/uryadova-komanda-cert-ua-v-2023-roci-opracyuvala-2543-kiberincidenti

3. Exclusive: Russian hackers were inside Ukraine telecoms giant for months. URL: https://www.reuters.com/world/europe/russian-hackers-were-inside-ukraine-telecoms-giant-months-cyber-spy-chief-2024-01-04

4. URL: https://new.gp.gov.ua/ua/posts/statistika

5. Понад 3 мільярди гривень збитків: кіберполіція та слідчі Нацполу викрили хакерів, які атакували провідні світові компанії. URL: https://cyberpolice.gov.ua/news/ponad--milyardy-gryven-zbytkiv-kiberpolicziya-ta-slidchi-naczpolu-vykryly-xakeriv-yaki-atakuvaly-providni-svitovi-kompaniyi-1780

6. СБУ спільно з правоохоронцями США, Великої Британії та ЄС викрила міжнародне угруповання хакерів-вимагачів. URL: https://t.me/SBUkr/11241

7. Largest ever operation against botnets hits dropper malware ecosystem. URL: https://www.europol.europa.eu/media-press/newsroom/news/largest-ever-operation-against-botnets-hits-dropper-malware- ecosystem

8. The World Cybercrime Index: What is it and why is it important? URL: https://www.tripwire.com/state-of-security/world-cybercrime-index-what-it-and-why-it-important#:~:text=The%20World%20Cybercrime%20Index%20(WCI,the%20researchers%20develop%20these%20rankings%3F

9. Деякі питання реагування суб’єктами забезпечення кібербезпеки на різні види подій у кіберпросторі: Постанова Кабінету Міністрів України від 04.04.23 р. № 299. URL: https://zakon.rada. gov.ua/laws/show/299-2023-%D0%BF#Text

10. EU AI Act: first regulation on artificial intelligence. URL: https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

11. Використання електронних (цифрових) доказів у кримінальних провадженнях: метод. реком. / М.В. Гуцалюк, В.Д. Гавловський, В.Г. Хахановський та ін. ; за заг. ред. О.В. Корнейка. Вид. 2-ге, доп. Київ: Вид-во Нац. акад. внутр. справ , 2020. 104 с.

12. REGULATION (EU) 2023/1543 OF THE EUROPEAN PARLIAMENT and of the COUNCIL of 12 July 2023. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJL_2023191. 01.0118.01.ENG

13. E-evidence – cross-border access to electronic evidence. URL: https://commission.europa.eu/law/cross-border-cases/judicial-cooperation/types-judicial-cooperation/e-evidence-cross-border - access-elect ronic-evidence_en

14. Europe’s cybersecurity chief says disruptive attacks have doubled in 2024, sees Russia behind many. URL: https://apnews.com/article/europe-election-cybersecurity-russia-ukraine-5b0cca725d17a028dd 458df77a60440c

15. Розроблення концепції кіберстримування має спиратися на досвід програми ядерного стримування. – (Держспецзв'язку). URL: https://www.kmu.gov.ua/news/rozroblennya-koncepciyi-kiber strimuvannya-maye-spiratisya-na-dosvid-programi-yadernogo-strimuvannya-derzhspeczvyazku

16. Хакери українського "блекджеку" зірвали джекпот у Росії. URL: https://www. newsweek. com/ukraine-blackjack-hackers-russia-defense-military-sites-1862139

17. Україні пропонують кібердипломатію. URL: https://zn.ua/ukr/UKRAINE/ukrajini-pro ponujut-kiberdiplomatiju.html

18. Cyber attacks: EU ready to respond with a range of measures, including sanctions. URL: https://www.consilium.europa.eu/en/press/press-releases/2017/06/19/cyber-diplomacy-toolbox

19. EU Cyber Diplomacy Initiative. URL: https://eucyberdirect.eu

20. Convention on countering the use of information and communications technologies for criminal purposes. URL: https://ccdcoe.org/library/publications/proposal-of-united-nations-convention-on-countering-the-use-of-information-and-communications-technologies-for-criminal-purposes-comme nt-on-the-first-draft-text-of-the-convention

21. Global Digital Compact. URL: https://www.un.org/techenvoy/ru/global-digital-compact

22. Україна та ЄС започаткували Кібердіалог. URL: https://mfa.gov.ua/news/ukrayina-ta-yes-zapochatkuvali-kiberdialog

23. Україну захищатиме Таллінський механізм: що це таке. URL: https://vechirniy.kyiv.ua/ news/92637/

24. Україні передали обладнання на 900 тисяч Євро в межах ІТ-коаліції. URL: https://ua. korrespondent.net/ukraine/4683833-ukraini-peredaly-obladnannia-na-900-tysiach-yevro-v-mezhakh-it-koa litsii

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~