МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ ТА ЗАХИСТОМ ІНФОРМАЦІЇ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: "АКТУАЛЬНІ ТЕНДЕНЦІЇ ТА МЕТОДИ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ НА МІЖНАРОДНОМУ РІВНІ"

на здобуття освітнього ступеня бакалавра
зі спеціальності 125 Кібербезпека
освітньої програми Управління інформаційною та кібернетичною безпекою

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Денис ЛЕЖЕНІН
(підпис) *Ім'я, ПРІЗВИЩЕ здобувача*

Виконав(ла): здобувач(ка) вищої освіти гр. УБД-42

Денис ЛЕЖЕНІН
Ім'я, ПРІЗВИЩЕ

Керівник: Тетяна МУЖАНОВА
к. держ. упр., доцент Ім'я, ПРІЗВИЩЕ

Рецензент:
Ім'я, ПРІЗВИЩЕ

Київ 2026

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут кібербезпеки та захисту інформації

Кафедра управління кібербезпекою та захистом інформації

Ступінь вищої освіти бакалавр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри УКБЗІ
_____ Світлана ЛЕГОМІНОВА
“____”_____2026 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Леженіну Денису Олексійовичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Актуальні тенденції та методи протидії кіберзлочинності на міжнародному рівні”,
керівник кваліфікаційної роботи Мужанова Тетяна Михайлівна, к.держ.упр., доцент,
(ПРІЗВИЩЕ, Ім’я,, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від “20“ лютого 2026 р. №51.

2. Строк подання кваліфікаційної роботи “12” травня 2026 р.

3. Вихідні дані до кваліфікаційної роботи: *кіберзлочинність, методи протидії кіберзлочинності, нормативно-правове й інституційне забезпечення протидії кіберзлочинності на міжнародному рівні, кібератрибуція.*

4. Перелік питань, які мають бути розроблені:

4.1. Дослідити теоретичні основи кіберзлочинності, зокрема її види і тенденції розвитку.

4.2. Проаналізувати напрями і методи протидії кіберзлочинності на міжнародному рівні.

4.3. З’ясувати світові тенденції і виклики подолання кіберзлочинності, розробити рекомендації щодо подолання кіберзлочинності на міжнародному рівні.

5. Перелік ілюстративного матеріалу: *презентація PowerPoint*

6. Дата видачі завдання “05“ березня 2026 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	18.03.2026	
2.	Збір та аналіз літератури.	30.03.2026	
3.	Дослідження теоретичних основ кіберзлочинності.	08.04.2026	
4.	Аналіз напрямів і методів протидії кіберзлочинності на міжнародному рівні.	15.04.2026	
5.	Встановлення світових тенденцій і викликів подолання кіберзлочинності, розробка рекомендацій.	22.04.2026	
6.	Формулювання висновків за результатами проведеного дослідження.	29.04.2026	
7.	Оформлення роботи.	06.05.2026	
8.	Оформлення презентації.	11.05.2026	
9.	Отримання рецензії на роботу.	10.06.2026	
10.	Захист в ЕК.	__.06.2026	

Здобувач вищої освіти _____ Денис ЛЕЖЕНІН
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Тетяна МУЖАНОВА
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня бакалавра

Направляється здобувач Леженін Д.О. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Актуальні тенденції та методи протидії кіберзлочинності на міжнародному рівні"

Кваліфікаційна робота і рецензія додаються.

Директор ННІКБЗІ _____ Євгенія ІВАНЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач ЛЕЖЕНІН Денис у кваліфікаційній роботі дослідив теоретичні основи кіберзлочинності; проаналізував напрями і методи протидії кіберзлочинності на міжнародному рівні; з'ясував світові тенденції і виклики подолання кіберзлочинності, розробив рекомендації щодо подолання кіберзлочинності на міжнародному рівні.

ЛЕЖЕНІН Денис показав розуміння проблеми дослідження та бачення основних теоретичних і практичних напрямів її вирішення, ефективно використав різні науково-дослідницькі методи для досягнення мети роботи, відповідально й організовано підійшов до виконання завдань дослідження. Результати кваліфікаційної роботи апробовані на конференції "Стратегії кіберстійкості: управління ризиками та безперервність бізнесу" 25 лютого 2026 року.

Все це дозволяє оцінити кваліфікаційну роботу здобувача ЛЕЖЕНІНА Дениса на позитивну оцінку та присвоїти йому кваліфікацію бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Керівник кваліфікаційної роботи _____ Тетяна МУЖАНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"____" _____ 2026 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Леженін Д.О. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедри
управління кібербезпекою та
захистом інформації _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну бакалаврську роботу

здобувача вищої освіти ЛЕЖЕНІНА Дениса
на тему “Актуальні тенденції та методи протидії кіберзлочинності на міжнародному рівні”

Актуальність. Результати статистики показують стійкі тенденції до розширення обсягів транскордонної кіберзлочинної діяльності з багатомільярдним обігом, яку реалізують як кримінальні групи з метою наживи, так і державні суб’єкти для досягнення власних геополітичних цілей. Зусилля окремих держав вирішити цю проблему не мають стійкого успіху, а підходи до подолання кіберзлочинності на глобальному рівні потребують удосконалення і налагодження ефективної співпраці за участі усіх зацікавлених сторін: міжнародних організацій, держав і бізнесу.

З огляду на зазначене дослідження актуальних тенденцій та методів протидії кіберзлочинності на міжнародному рівні є актуальним науковим завданням.

Позитивні сторони.

1. У роботі досліджено напрями і методи протидії кіберзлочинності на міжнародному рівні, зокрема особливості нормативно-правового та інституційного забезпечення, проаналізовано роль міжнародних організацій та команд реагування на кіберінциденти у подоланні кіберзлочинності.

2. Кваліфікаційна робота має послідовну структуру, оформлена згідно з вимогами. Виклад матеріалу здійснено за чітким планом, зроблено логічні висновки. Ключові положення роботи представлено у вигляді рисунків і таблиць.

3. Автор опрацював значну джерельну базу: понад 50 публікацій, в тому числі нормативно-правові акти, наукові статті, статистичні дані.

4. За результатами дослідження запропоновано рекомендації щодо комплексного подолання кіберзлочинності на міжнародному рівні.

Недоліки.

Доцільно було б приділити більше уваги розгляду Конвенції ООН проти кіберзлочинності 2024 року, а також питанням внеску міжнародних неурядових організацій і аналітичних центрів в організацію протидії кіберзлочинності.

Однак, вищезгадані зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує позитивної оцінки, а здобувач ЛЕЖЕНІН Денис заслуговує присвоєння кваліфікації бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Рецензент:

_____ _____

підпис Ім’я, ПРІЗВИЩЕ

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню актуальних тенденцій та методів протидії кіберзлочинності на міжнародному рівні. Робота складається зі вступу, трьох розділів, що містять 9 рисунків і 10 таблиць, висновків і списку використаних джерел із 57 найменувань. Загальний обсяг роботи становить 74 аркуші, з яких 6 аркушів займає список використаних джерел.

Метою роботи є дослідження актуальних тенденцій та методів протидії кіберзлочинності на міжнародному рівні.

Об'єктом дослідження є засади протидії кіберзлочинності на міжнародному рівні.

Предмет дослідження – актуальні тенденції та методи протидії кіберзлочинності на міжнародному рівні.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи аналізу та синтезу, порівняння, класифікації, моделювання та прогнозування, аналізу нормативно-правової бази та узагальнення кращих практик забезпечення кібербезпеки.

Як результат у роботі досліджено теоретичні основи кіберзлочинності, зокрема її види і тенденції розвитку; проаналізовано напрями і методи протидії кіберзлочинності на міжнародному рівні; з'ясовано світові тенденції і виклики подолання кіберзлочинності, розроблено рекомендації щодо подолання кіберзлочинності на міжнародному рівні.

Галузь застосування. Розроблені підходи можуть бути використані при плануванні та реалізації комплексу нормативно-правових та організаційних заходів щодо протидії кіберзлочинності як загальнодержавного масштабу, так і на рівні підприємств та організацій.

Ключові слова: КІБЕРЗЛОЧИННІСТЬ, МЕТОДИ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ, НОРМАТИВНО-ПРАВОВЕ Й ІНСТИТУЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ НА МІЖНАРОДНОМУ РІВНІ, КІБЕРАТРИБУЦІЯ.

ABSTRACT

The qualification work is devoted to the study of current trends and methods of combating cybercrime at the international level. The work consists of an introduction, three chapters containing 9 figures and 10 tables, conclusions and the list of references containing 57 items. The total volume of the work is 74 pages, of which 6 pages are occupied by the list of references.

The purpose of the study is to study current trends and methods of combating cybercrime at the international level.

The object the study is the principles of combating cybercrime at the international level.

The subject of the study is current trends and methods of combating cybercrime at the international level.

Research methods. In order to solve the mentioned higher scientific task, the methods of analysis and synthesis, comparison, classification, modeling and forecasting, analysis of the regulatory framework and generalization of best cybersecurity practices were used.

As a result, the work investigated the theoretical foundations of cybercrime, in particular its types and development trends; analyzed the directions and methods of combating cybercrime at the international level; clarified global trends and challenges in overcoming cybercrime, developed recommendations for overcoming cybercrime at the international level.

Field of application. The developed approaches can be used in planning and implementing a set of regulatory and organizational measures to combat cybercrime both on a national scale and at the level of enterprises and organizations.

Keywords: CYBERCRIME, METHODS OF COMBATING CYBERCRIME, REGULATORY AND INSTITUTIONAL SUPPORT FOR COMBATING CYBERCRIME AT THE INTERNATIONAL LEVEL, CYBERATTRIBUTION.

ЗМІСТ

ВСТУП

Актуальність теми. У нинішніх умовах постійного розвитку ІКТ кіберзлочинність є одним із найбільш небезпечних і динамічних видів сучасної зловмисної діяльності. Як свідчить статистика, щорічно обсяги кібератак зростають приблизно на 15% і коштують світові понад 10 трлн доларів. Крім цього, сучасній кіберзлочинності притаманні прихованість впливу, складність виявлення і транснаціональний характер.

Практика показує, що подолати кіберзлочинність на рівні окремої держави є недосяжним завданням. Натомість організація комплексних і узгоджених заходів у загальносвітовому масштабі дозволять пом'якшити і в перспективі вирішити проблему протиправної діяльності в цифровому просторі.

З огляду на зазначене дослідження актуальних тенденцій та методів протидії кіберзлочинності на міжнародному рівні є актуальним науковим завданням.

Мета роботи полягає у дослідженні актуальних тенденцій та методів протидії кіберзлочинності на міжнародному рівні.

Об'єкт дослідження – засади протидії кіберзлочинності на міжнародному рівні.

Предмет дослідження – актуальні тенденції та методи протидії кіберзлочинності на міжнародному рівні.

Для досягнення цієї мети в роботі необхідно виконати наступні **завдання**:

1. Дослідити теоретичні основи кіберзлочинності, зокрема її види і тенденції розвитку.

2. Проаналізувати напрями і методи протидії кіберзлочинності на міжнародному рівні.

3. З'ясувати світові тенденції і виклики подолання кіберзлочинності, розробити рекомендації щодо подолання кіберзлочинності на міжнародному рівні.

Методи дослідження. Для вирішення означеного вище наукового

завдання в роботі використані методи аналізу та синтезу, порівняння, класифікації, моделювання та прогнозування, аналізу нормативно-правової бази та узагальнення кращих практик забезпечення кібербезпеки.

Практичне значення одержаних результатів. Застосування напрацювань дослідження дасть змогу забезпечити комплексний підхід і здійснити обґрунтований вибір нормативно-правових та організаційних заходів щодо протидії кіберзлочинності як загальнодержавного масштабу, так і на рівні підприємств та організацій.

Апробація результатів кваліфікаційної роботи відбулася на Всеукраїнській науково-практичній конференції “Стратегії кіберстійкості: управління ризиками та безперервність бізнесу” 25 лютого 2026 року.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ КІБЕРЗЛОЧИННОСТІ

1.1 Поняття кіберзлочинності та її основні види

У світі постійного розвитку цифрових технологій і науки кіберзлочинність є одним із найбільш небезпечних і динамічних видів сучасної злочинної діяльності, що виникла та активно розвивається разом із розвитком інформаційних технологій і глобальної мережі інтернет. Вона охоплює широкий спектр протиправних дій, які здійснюються за допомогою комп'ютерних систем, мереж або спрямовані на них. Здебільшого зловмисники здійснюють кіберзлочини з метою отримання фінансової вигоди, однак деякі роблять це з інших причин, зокрема, з політичних переконань або через особисті образи.

Як свідчить статистика [1-4], у 2025 році кіберзлочинність коштувала світові понад 10 трлн доларів, щорічно зростаючи приблизно на 15% і маючи величезний обіг коштів, який дорівнює бюджету великої держави з потужною економікою.

Ключові тенденції 2025 року охоплюють: широке використання фішингу на основі штучного інтелекту (82,6% фішингових атак), розширення масштабів програм-вимагачів (у 44% випадків порушення безпеки даних із середнім розміром викупу приблизно 115 тис. доларів) і сплеск атак на ланцюги постачань (60% керівників вищої ланки вважають, що атаки на ланцюг постачань є найімовірнішою загрозою для їхнього бізнесу). Середні втрати внаслідок витоку даних досягли 4,88 млн доларів, при цьому 88% організацій стикнулися з такими атаками [3-4, 8-9].

Крім цього встановлено, що основними векторами атак кіберзлочинців станом на 2025 рік є впровадження шкідливих програм (54% організацій) і фішинг (44%). Експлуатація вразливостей ПЗ було основним вектором зараження, що становить 20% порушень, зі значним збільшенням атак на периферійні пристрої та VPN. Лише за 2024 рік зловмисниками було скомпрометовано понад 2,1 млрд облікових даних за допомогою шкідливого ПЗ.

Кількість витоків, пов'язаних із партнерами чи постачальниками, подвоїлася і становить близько 30%. Дослідження показали безпрецедентне зростання атак з використанням штучного інтелекту, кількість яких зросла на 47% у 2025 році [10-13].

Відповідно до визначення Інтерполу, кіберзлочинність – це злочини, що здійснюються за допомогою використання інформаційно-комунікаційних технологій або спрямовані проти комп’ютерних систем, даних і мереж [5].

Кіберзлочинність має декілька особливостей серед яких:

- транснаціональний характер;
- високий рівень латентності;
- складність виявлення, запобігання та розслідування;
- використання сучасних технологій та анонімність.

Кіберзлочини доцільно поділити на дві основні категорії:

1. Кіберзлочини, спрямовані на комп’ютерні системи.

2. Кіберзлочини, в яких комп’ютер є інструментом.

Розглянемо кожну категорію детальніше.

Кіберзлочини, спрямовані на комп’ютерні системи. Зазвичай до даної категорії належать правопорушення, метою яких є порушення роботи інформаційних систем, несанкціонований доступ до них або викрадення даних.

Основними підвидами к*іберзлочинів, спрямованих на ІКС, є:*

- Злам системи. Зловмисники незаконно отримують доступ до комп’ютера, сервера чи мережі, щоб викрасти дані або встановити шкідливе ПЗ.
- Шкідливе ПЗ. Зазвичай зловмисники ховають шкідливе ПЗ у файлах чи скиптах, щоб непомітно заразити пристрій особи й викрасти її дані.
- Програми-вимагачі. Програми, які завантажують на комп’ютер для шифрування файлів жертви з метою вимагання викупу в обмін на ключ дешифрування.
- DDoS атаки. Атаки спрямовані на завантаження мережі підробленим інтернет-трафіком, щоб зробити її недоступною для користувачів.

- Витік даних. Кіберзлочинці незаконно отримують доступ до системи або до мережі з метою викрадення конфіденційної інформації.

- Криптоджекінг. Використання певного типу шкідливого типу ПЗ, яке використовує ОС жертви для майнінгу криптовалюти.

Кіберзлочини, в яких ПК є засобом реалізації злочинної діяльності, охоплюють:

- Фішинг – це метод соціальної інженерії, який використовується хакерами для виманювання в жертв грошей або конфіденційної інформації шляхом створення фейкових ресурсів, які видають себе за надійні.

- Кіберпереслідування (або кіберцькування) – це злочинні дії, які передбачають переслідування або погрози в Інтернеті (наприклад, у соціальних мережах або електронною поштою).

- Кіберкрадіжка інтелектуальної власності (наприклад, патентів або авторських прав) і використання її для отримання фінансової вигоди.

- Кібервимагання – є формою шантажу і передбачає погрози з боку кіберзлочинців розкрити конфіденційну інформацію жертви або почати кібератаку в разі відмови виконати їхні вимоги.

- Фінансові кіберзлочини зазвичай охоплюють шахрайство в онлайн-банкінгу, шахрайство з кредитними картками й відмивання електронних грошей.

- Кібершпигунство – це дії, які передбачають використання різних незаконних ІТ-технологій для крадіжки державних таємниць.

- Кібертероризм передбачає здійснення кібератак з політичних або ідеологічних мотивів, які зазвичай мають на меті залякування або порушення суспільного порядку.

- Продаж або розповсюдження незаконного й забороненого контенту (наприклад, відеороликів, що демонструють акти тероризму або пропагують ненависть) [5].

Розглянуті класифікації кіберзлочинів показані на рис. 1.1.

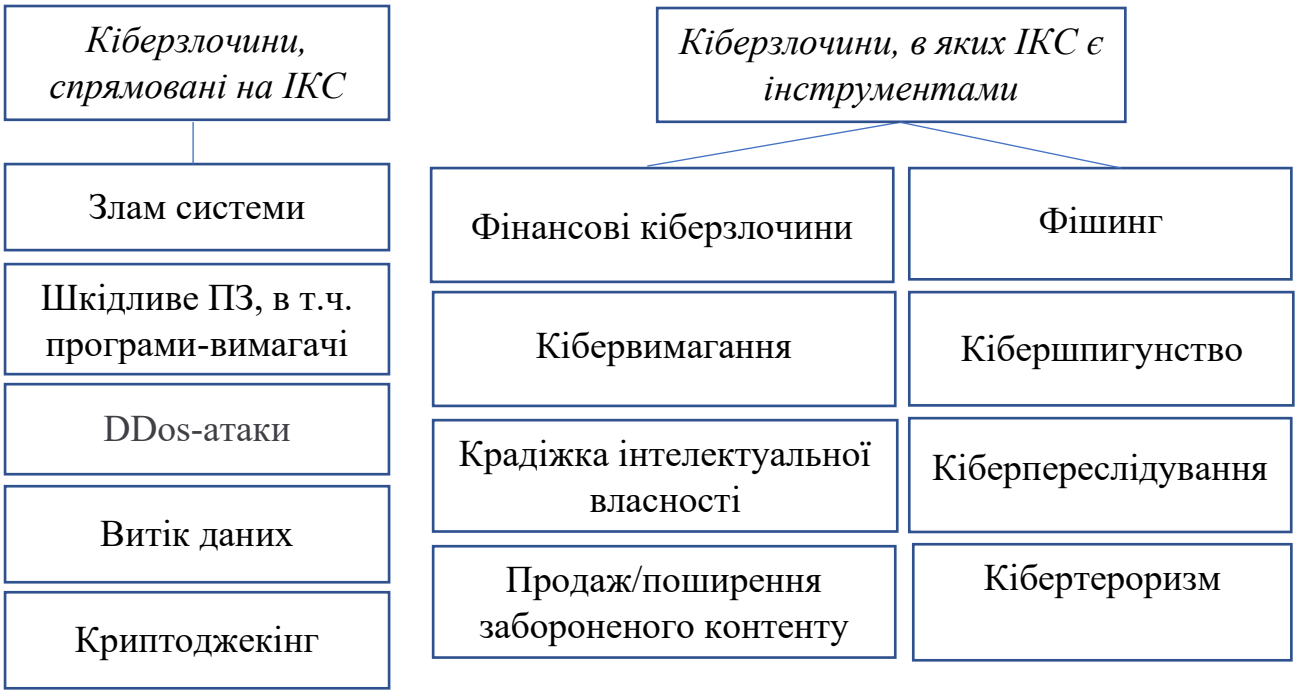

Рис. 1.1. Класифікації кіберзлочинів

Невід'ємну роль в аналізі та класифікації кіберзлочинів відіграють міжнародні організації, такі як Міжнародна організація кримінальної поліції Інтерпол**,** та органи ЄС: Європейське поліцейське управління Європол та Європейське агентство з кібербезпеки ENISA [5-7].

Як показало дослідження, Інтерпол зосереджується на боротьбі з високотехнологічними «чистими» кіберзлочинами (хакінг, шкідливе програмне забезпечення, програми-вимагачі) та «традиційними» кіберзлочинами в кіберпросторі, що охоплюють шахрайство, фішинг, сексуальне вимагання). Їхнім пріоритетом є руйнування глобальних злочинних мереж, задіяних у реалізації атак із програмами-вимагачами, компрометації ділової електронної пошти (BEC), цифрових афер і сексуальній експлуатації дітей.

Ключові типи кіберзлочинів, яким Інтерпол надає пріоритет, включають:

- програми-вимагачі та шкідливе ПЗ, тобто атаки з метою блокування доступу до ІКС або їх пошкодження з метою вимагання грошей;
- компрометація ділової електронної пошти (BEC) та фінансове шахрайство, що має на меті перенаправлення корпоративних платежів у власних інтересах зловмисників;

- фішинг та онлайн-шахрайство, зокрема масові кампанії з використанням підробних електронних листів або веб-сайтів для крадіжки облікових і персональних даних;
- цифрове вимагання на сексуальному ґрунті (Digital Sextortion), яке є підвидом шантажу з використанням сексуального контенту, знайденого в Інтернеті;
- викрадення даних (Infostealers) з браузера з їх подальшим замаскованим виводом через IP-адресу реального приватного пристрою неподалік місця проживання жертви;
- незаконні операції з криптовалютою, зокрема відмивання грошей і незаконний прибуток, який виводиться через цифрові гаманці;
- сексуальна експлуатація дітей онлайн, в тому числі онлайн-насильство [5, 10-11].

Європол у своїх звітах пропонує класифікувати кіберзлочини за напрямом діяльності, виділяючи такі категорії як: злочини проти інформаційних систем, онлайн-шахрайство, експлуатація персональних даних і діяльність організованих кіберзлочинних угрупувань [6].

ENISA застосовує класифікацію за технічною природою та методами реалізації кіберзлочину, виділяючи шкідливе ПЗ, фішинг, DDoS атаки, витоки даних та атаки на ланцюги постачання [7, 13].

Таким чином, класифікація кіберзлочинності базується на поєднанні двох різних підходів: функціонального та технічного, що дозволяє у повному обсязі охарактеризувати її суть, структуру та прояви.

Важливим аспектом дослідження кіберзлочинності є визначення мотивів діяльності кіберзлочинців. Більшість зловмисників керуються метою особистого збагачення за рахунок інших людей або реалізації політичних цілей.

Основним способом досягнення цих цілей є отримання незаконного доступу до конфіденційної інформації, викрадення фінансових ресурсів, а також встановлення контролю над комп’ютерними системами та мережами.

Попри це, у сучасних умовах спостерігається зростання кількості кібератак, спрямованих на здійснення інформаційного впливу, дестабілізації суспільства та порушення функціонування критичної інфраструктури.

Це демонструє ускладнення характеру кіберзлочинності та розширення спектру її цілей. Так, прикладом кіберактивності з політичними мотивами є кібервійна між Україною та росією, яка розпочалася у 2014 році, та активізувалася після повномасштабного вторгнення у 2022 році.

1.2 Основні тенденції розвитку кіберзлочинності у світі

У поточному сторіччі протиправна діяльність у цифровому середовищі перетворилась у глобальну загрозу, яка демонструє надзвичайну масштабність та динамізм. Процес розвитку суспільства супроводжується не лише кількісним зростанням інцидентів у сфері кіберпезпеки, а й якісним ускладненням інструментарію зловмисників. Кібератаки стають більш сфокусованими, а фінансові та репутаційні втрати, яких вони завдають світовій економіці, набувають критичних масштабів [2].

Важливою характеристикою кіберзлочинності є її глобальний характер. Рівень кіберзагроз, сильно залежить від рівня цифровізації країни, розвитку інформаційної інфраструктури, економічної стабільності та політичної ситуації. Найбільша кількість кібератак припадає як раз на економічно розвинені регіони, зокрема на країни Європи та Північну Америку. В той же час значна активність кіберзлочинів спостерігається також у країнах Азії, які є як і джерелом так і об’єктом атак [6,7] (Рис. 1.2).

Окремої уваги заслуговують країни які знаходяться у стані військового конфлікту. Зокрема Україна, яка є одним із ключових об’єктів кібератак у зв’язку із триваючою війною.

Узагальнення статистичних даних щодо географічного розподілу кіберзлочинності наведено в таблиці 1.1.

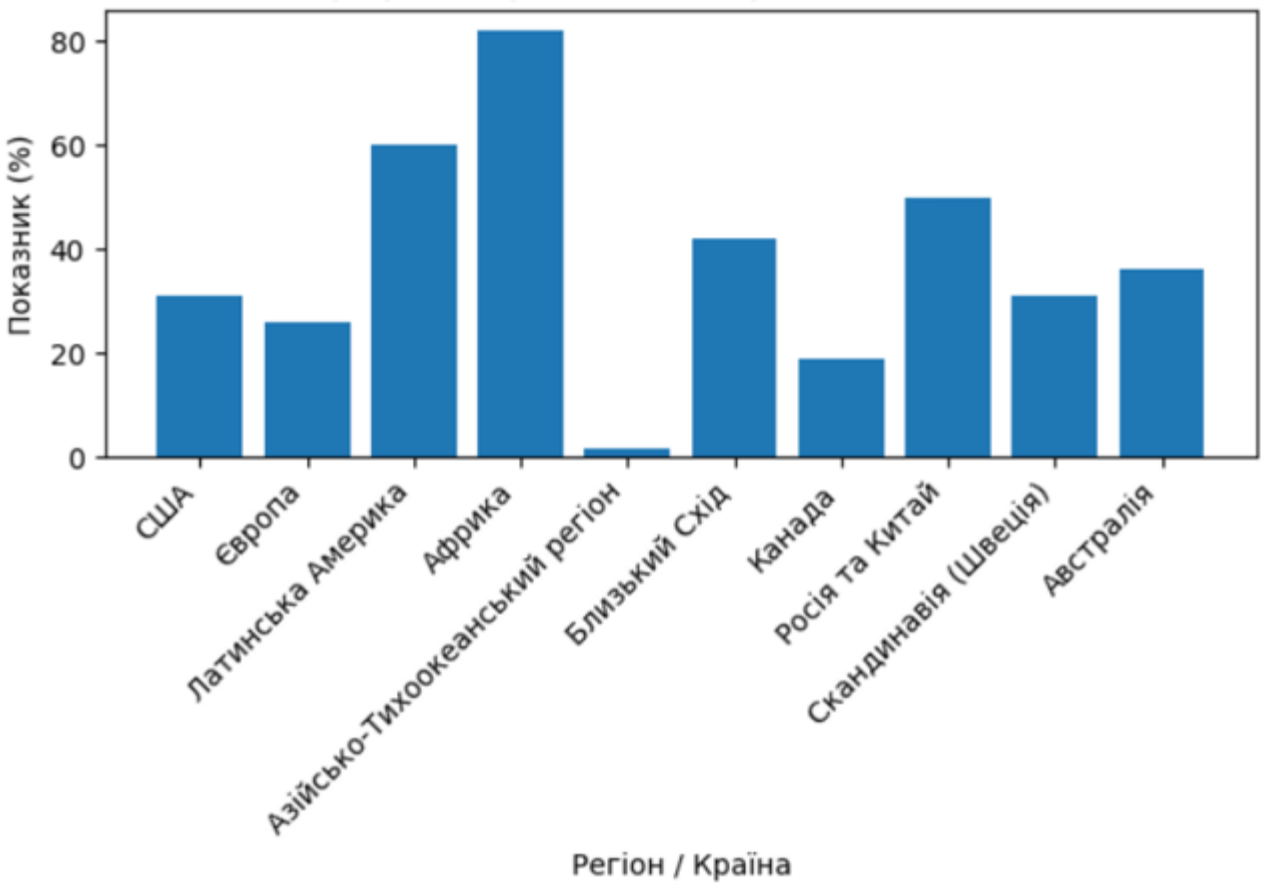

Рис. 1.2. Поширення кібератак в різних регіонах світу у 2025 році

За даними досліджень, у 2025 році понад 84% організацій світу зазнали принаймні однієї кібератаки протягом останнього року, що свідчить про глобальність цієї проблеми [3]. Згідно з прогнозами до 2031 року середній час між кібератаками буде складати близько 2 секунд [8,9].

Серед технічних тенденцій у лідерах залишаються фішинг та соціальна інженерія, на них припадає більша частина злочинних інцидентів, кожного дня реєструється понад 1 млн фішингових атак [13].

Для більш повного розуміння сучасних тенденцій розвитку кіберзлочинності, важливим є аналіз статистичних показників, які як правило формуються на основі звітності правоохоронних органів і аналітики міжнародних організацій [2-4].

Статистичні показники дозволяють оцінити не лише кількість кіберзлочинів, але й їх економічні наслідки, географічне поширення і основні інструменти які використовують кіберзлочинці.

Таблиця 1.1.

Статистика щодо географічного розподілу кіберзлочинності

Джерела даних	Географія	Вікно вимірювання	Статистика	Висновки
Скарги та збитки потерпілих (публічна звітність)	США	Календарний рік 2024	859 532 скарги; $16.6 млрд втрат; +33% втрат у порівнянні з минулим роком	Великі втрати від шахрайства; консервативна нижня межа (залежно від звітності).
Розслідувані інциденти безпеки та підтверджені порушення (файли справ + учасники)	По всьому світу	Набір даних для публікації 2025 року	Понад 22 тис інцидентів; 12,2 тис підтверджених порушень у 139 країнах	Широке, глобально поширене уявлення про порушення, які досягають дослідників/партнерів; сильний для шаблонів і векторів.
Відстежені фішингові атаки (унікальні фішингові сайти/атаки)	По всьому світу	1-й квартал Q1 2025 року	Понад 1 млн спостерігали фішингові атаки (найбільша квартальна сума з кінця 2023 року)	Масштаб фішингу як засобу масової злочинності; корисний для спрямування трендів і уособлення сектора.
Відстежені фішингові атаки (унікальні фішингові сайти/атаки)	По всьому світу	3-й квартал Q3 2025 року	Майже 900 тис відстежених фішингових атак; виявлення шахрайства на основі смс; +~35% (Q3 проти Q2)	Постійні високі обсяги фішингу + перехід каналу до смішингу/вішингу.

Продовження табл. 1.1.

Джерела даних	Географія	Вікно вимірювання	Статистика	Висновки
Набір інцидентів, орієнтованих на ЄС (відкриті джерела + дані держав-членів)	ЄС	01 липня 2024 – 30 червня 2025	Проаналізовано 4875 інцидентів; DDoS ~76, 7% типів інцидентів	Зважена за видимістю картина діяльності ЄС з порушеннями, особливо хактивістських DDoS; не перепис.
Відстеження нових жертв програм-вимагачів через екосистему вимагання (аналітика місця витоку)	По всьому світу	3-й квартал Q3 2025 року	1592 нових жертви у 85 активних групах здирництва; +25% у порівнянні з минулим роком	Структура економіки вимагання (фрагментація, розповсюдження), а не загальна кількість програм-вимагачів.
Організаційна поширеність (опитування організацій)	Велико-британія	Минулі 12 місяців під час опитування	43% підприємств і 30% благодійних організацій зазнали порушень/атак; високі показники для середніх /великих фірм	Масштаби порушень за розміром організації /сектором; чутливим до зрілості виявлення.
Національна звітність і попит на допомогу	Австралія	2024–25 фінансовий рік	84,7 тис повідомлень про кіберзлочини; понад 42,5 тис дзвінків на гарячу лінію; більше 1200 інцидентів відреаговано	Потужність тиску кіберзлочинності на національні системи реагування; корисність для планування потенціалу.

Аналіз наведених у таблиці даних свідчить про значні масштаби поширення кіберзлочинності у світі. Глобальні дослідження також підтверджують величезну кількість кіберінцидентів. Окрему увагу привертає значне поширення фішингових атак, кількість яких у 1-му кварталі 2025 року перевищила 1 млн випадків. Також важливою тенденцією є зростання кількості атак із використанням програм-вимагачів [13-15].

Таким чином, статичні дані підтверджують тенденцію до постійного зростання масштабів кіберзлочинності, її глобалізацію та ускладнення методів кібернападу.

Програми-вимагачі (ransomware) мають статус одних із найпоширеніших загроз. Згідно із статистикою, понад 70% світових атак пов’язані зі здирницькою діяльністю, при чому середні витрати на усунення наслідків атаки сягають більше ніж 4-5 млн доларів [3].

Ця переважна поширеність у порівнянні з іншими типами атак, такими як порушення мережі (18,83%0, вимагання даних (7,14%), викрадення даних (1,3%), атаки завантажувачів (0,65%), і DDoS-атаки (0,65%) [14-16], - демонструє, що цей метод став одним із найбільш поширеним у кіберзлочинців, які прагнуть монетизувати свою діяльність (Рис. 1.3).

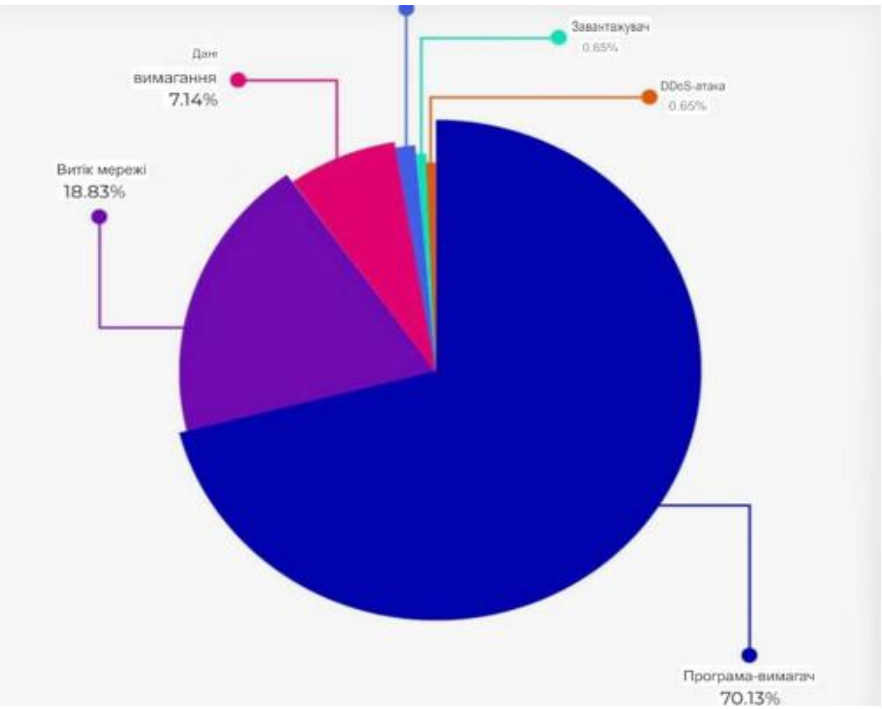

Рис. 1.3. Питома вага різних видів кіберзлочинів у 2025 році

Крім цього, спостерігається значне зростання кількості шкідливого програмного забезпечення й атак на пристрої Інтернету речей (IoT), де їх кількість збільшилась на понад 70% [11,12].

Узагальнюючи викладене, основними тенденціями розвитку кіберзлочинності можна визначити;

1. *Зростання кількості та масштабу кібератак*, від яких потерпають дедалі більше користувачів і організацій по всьому світу стають жертвами атак.

2. *Ускладнення технологічної природи кібератак*. Через розвиток технологій зловмисники змушені застосовувати нові види шкідливого ПЗ і методи обходу систем захисту.

3. *Активне використання соціальної інженерії та фішингу*. Більшість інцидентів пов’язана із маніпуляцією свідомістю користувачів та обманом для отримання доступу до даних.

4. *Зростання ролі ШІ*. Інструменти штучного інтелекту щораз частіше використовуються кіберзлочинцями для генерації шкідливих повідомлень, обходу захисту та масштабування атак.

5. *Глобалізація та геополітична складова*. Кібератаки все частіше є складовою більш широкого геополітичного протистояння держав або внутрішньо-політичної боротьби. Типовим прикладом є кіберпротистояння як доповнення широкомасштабних військових дій в Україні.

6. *Збільшення обсягів збитків від кібератак*. Витрати організацій на усунення наслідків після інцидентів та компенсація постраждалим постійно зростають.

Таким чином, сучасна кіберзлочинність характеризується глобальністю, високим рівнем організованості та постійним розвитком, що зумовлює необхідність удосконалення підходів до її протидії.

1.3 Сучасні форми і методи кібератак, організованих злочинними суб'єктами

Сучасні кібератаки можна охарактеризувати високим рівнем складності, багаторівневістю й використанням комбінованих підходів. Кіберзлочинні угрупування зазвичай використовують не окремі методи, а сплановані сценарії атак, які можуть включати багато етапів, починаючи від отримання доступу до ПК чи системи до закріплення в ній та отримання прибутку [17,18].

Типова схема кібератаки передбачає такі етапи (Рис. 1.4).

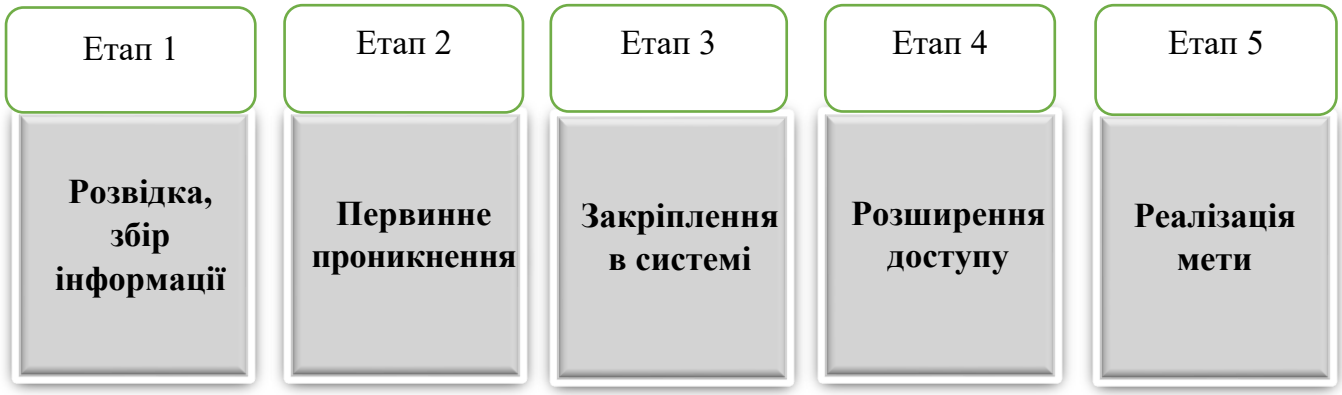

Рис. 1.4. Етапи кібератаки

Розглянемо детальніше зміст кожного із представлених етапів.

1. Розвідка та збір інформації

На цьому етапі зловмисники зазвичай виконують збір інформації про організацію, яка є ціллю атаки: її структуру, організаційні інформаційно-комунікаційні системи, персонал і потенційні вразливості. Як правило, засобами розвідки служать відкриті джерела (соціальні мережі, веб-сайти), а також інструменти сканування мережі (Nmap, Wireshark, Shodan, Nessus/Openvas).

2. Первинне проникнення

Як відзначалося вище, одним із найпоширеніших методів отримання первинного доступу до системи є фішинг і соціальна інженерія. Механізм даної атаки полягає у створенні фейкових електронних листів, веб-сайтів або повідомлень, які імітують офіційні ресурси. Користувач, який довіряє джерелу, переходить за посиланням і авторизується, тим самим надаючи зловмисникам доступ до внутрішніх систем організації. Через велику вразливість людського

чинника як ключової ланки системи безпеки, цей метод показує дуже високу ефективність.

3. Закріплення в системі

Отримавши доступ до системи, метою зловмисника стає забезпечення постійного доступу до неї. Основними методами для виконання цього завдання є:

- Встановлення бекдорів, тобто програм, які дозволять злочинцю управляти системою навіть після її перезавантаження. Типовими прикладами таких програм є Cobalt Strike – комерційний інструмент для управління бекдорами і виконання атак всередині мережі; NjRAT, DarkComet – популярне шкідливе ПЗ для забезпечення віддаленого доступу; Plug X – бекдор для Windows, для прихованого встановлення управління.

- Створення нових шкідливих акаунтів з метою залишатися в мережі. З цією метою використовують команди PowerShell для створення нових користувачів і підключення до Active Directory для створення адміністративних облікових засобів.

- Автозавантаження та модифікація системних конфігурацій. Шкідливі процеси додають до автозавантаження або змінюють ключі реєстру, щоб вони запускалися при старті ОС.

4. Розширення доступу

Зловмисники підвищують свої права в системі: від рівня доступу звичайного користувача до адміністратора системного рівня. Зазвичай для цього використовують такі інструменти як Mimikatz – це інструмент для викрадення паролів і хешів із пам’яті системи; Windows Exploit Suggester – програма, яка допомагає виявити вразливості для підвищення прав; експлуатація вразливостей типу Privilege Escalation Exploits, наприклад у Windows або Linux.

5. Реалізація атаки

Фінальний етап, на якому досягається основна мета зловмисників. У сучасному світі можна відзначити три найпопулярніші цілі кіберзлочинів, а саме:

- Кіберзлочини з фінансовою метою, зокрема використання даних для шахрайства або викупу.

- Кіберзлочини проти інформаційної цілісності та репутації, наприклад атаки спрямовані на знищення або модифікацію інформації.
- Кіберзлочини з політичними або ідеологічними мотивами, серед яких кібервійни, зрив функціонування критично важливої інфраструктури, демонстрація сили, тиск на державні або корпоративні суб'єкти [17,18].

Варто згадати також інший підхід до планування кібератаки - так званий ланцюг кібератаки (Cyber-Kill Chain) [19,20], який дозволяє зрозуміти, як хакер мислить, планує та виконує свої дії і, відповідно, сформувати уявлення про сфери, які слід оцінювати та пріоритезувати в стратегії кіберзахисту організації.

Cyber-Kill Chain також складається з п'яти кроків:

1. Дослідження та розвідка.
2. Озброєння.
3. Отримання доступу.
4. Експлуатація.
5. Викрадення інформації.

1. Дослідження та розвідка. Перший етап кібератаки – це коли хакер починає досліджувати свою ціль, щоб зібрати якомога більше інформації. Цей етап має на меті розуміння цілі, її місцезнаходження, типів інформації, яку вона зберігає, способів захисту цілі та способів здійснення атаки.

Хакери отримують дані про IP-адресу з загальнодоступних джерел і проводять сканування, щоб з'ясувати, яке обладнання та програмне забезпечення використовує цільова компанія. Вони перевіряють доменні імена, використовуючи онлайн-базу даних реєстрації, що підтримується Інтернет-корпорацією з присвоєння імен та номерів (ICANN).

Спроби злому будуть успішнішими, якщо хакери витратять більше часу на вивчення персоналу та IT-інфраструктури компанії. Розвідку поділяють на два типи: пасивну та активну розвідку.

Пасивна розвідка передбачає використання платформи з відкритим кодом для збору інформації про ціль без будь-якої безпосередньої взаємодії з нею. Здійснюючи пасивну розвідку щодо цілі, злочинець намагається зібрати корисну

інформацію, таку як системні дані, використовувані програми організації, імена та електронні адреси співробітників, дані соціальних мереж, публічні записи та, найголовніше, дані про домен. Типи корисної інформації, яку збирають хакери через відкриті джерела охоплюють: загальнодоступні записи (звіти, прес-релізи тощо); збір даних і адрес електронної пошти; інформацію із соціальних мереж; оголошення про вакансії; доменні імена (реєстрація домену, дані про IP-адреси).

Активна розвідка передбачає безпосередню взаємодію з цільовою організацією та її співробітниками чи системами для збору інформації. Активну розвідку складніше реалізувати, але зібрана з неї інформацію можна безпосередньо використати для використання слабких місць у будь-якій системі організації. Як правило, активна розвідка має форму сканування портів або мережі, і ці сканування виявляють та розкривають брандмауери, мережеву архітектуру, програми виявлення вторгнень або інші механізми безпеки, які використовуються для блокування входу, та їхні слабкі місця.

2. *Озброєння*. Завершення розвідувальних зусиль розпочне фазу озброєння. За допомогою інформації, зібраної на етапі розвідки, зловмисник розробить методи використання захисту цілі, отримуючи доступ до бажаної зловмисником інформації. Використання засобів нападу визначається навичками хакера та інформацією, зібраною на етапі розвідки. Наступним кроком для зловмисника є створення передумов для реалізації атаки шляхом написання фішингових електронних листів, створення та публікації фальшивих веб-сайтів, а також розробки або придбання шкідливого ПЗ. Зловмисник зазвичай починає атаку після достатнього дослідження та підготовки на наявність вразливостей програмного та/або апаратного забезпечення.

3. Отримання доступу. До мережі можуть підключатися різні точки. Співробітники, які натискають на вкладення у фішинговому електронному листі та завантажують шкідливу програму, є прикладами потенційних слабких місць. Інші вразливості можуть виникнути, коли працівників переконують розголошувати конфіденційну інформацію, таку як паролі для входу, або коли одна з систем організації неправильно налаштована або виправлена, що дозволяє

зловмиснику обійти засоби захисту. Можливо, зловмисник використав складний пошуковий запит, щоб знайти сторінку входу в загальнодоступній мережі, а потім використав дані, отримані із соцмереж та інструментів для злому паролів, щоб вгадати ім'я користувача та пароль. У результаті він стає частиною мережі організації-жертви.

4. Експлуатація. Дві мети зловмисника, який отримав доступ до системи, полягають у підвищенні своїх привілеїв та збереженні доступу. Підвищуючи привілеї для себе, хакер може внести зміни до системи, які зазвичай заборонені для звичайних користувачів або програм. Отримавши доступ до системи, хакери використовуватимуть різноманітні методи для підвищення своїх привілеїв, зокрема: використання дійсних облікових записів; маніпулювання токенами доступу; використання системи контролю облікових записів користувачів Windows.

Хакер намагатиметься продовжувати заглиблюватися в систему після отримання доступу до середовища, використовуючи різноманітні методи, такі як створення нових облікових записів користувачів, зміна налаштувань брандмауера, увімкнення віддаленого доступу до робочого столу або додавання бекдору за допомогою руткітів чи інших шкідливих файлів, завдяки можливості виконувати привілейовані команди.

5. Вихід. Після досягнення мети хакера він залишає систему або мережу, попередньо замітаючи свої сліди. З точки зору зловмисника, цей крок є дуже важливим, оскільки видалення програм, які використовувалися під час атаки, і створених папок, зміни, редагування, або видалення журналів аудиту, зменшить до мінімуму можливість встановлення зловмисника. Коли організація або особа виявляє атаку на свою систему або мережу, вони докладуть подальших зусиль для виявлення першопричин, організаторів і замовників атаки, залучаючи правоохоронні органи [19].

Слід відзначити, що у розширеному варіанті Cyber-Kill Chain передбачає інші фінальні стадії завершення атаки. Після перших чотирьох реалізують наступні етапи:

5. *Встановлення*. Після компрометації системи зловмисник встановлює шкідливі програми або бекдори для підтримки довгострокового доступу, що дозволяє повторний вхід навіть після виправлення початкової вразливості.

6. *Командування та управління (C2).* На цьому етапі зловмисники встановлюють канал зв'язку між власним командним сервером і зламаною машиною. Це дозволяє їм віддалено витягувати дані, переміщатися всередині системи-жертви й передавати команди, тобто здійснювати повний контроль, залишаючись максимально непомітним з невеликими шансами бути виявленим.

7. *Досягнення кінцевої мети.* На цьому етапі зловмисник досягає запланованої мети, яка може передбачати крадіжку даних, шифрування системи з метою вимагання викупу або пошкодження / перешкоджання її роботі [20].

Яскравим прикладом сучасної масштабної кібератаки, яка продемонструвала практичну реалізацію класичної схеми кібервимагання є Cyber-attack on Hydro 2019. Norsk Hydro – одна з провідних світових компаній у сфері виробництва алюмінію. З огляду на те, що компанія несе відповідальність за критично важливі виробничі процеси та глобальні логістичні ланцюги, напад на її інфраструктуру стала серйозним викликом систем кібербезпеки.

Особливістю кібератаки стало те, що зловмисники використовували шкідливе ПЗ LockerGoga, поєднуючи шифрування даних із соціальною інженерією, що призвело до інфікування понад 22 тис. ПК у більш ніж 40 країнах за лічені години. Атака була спрямована не лише на офісні системи, а й на критично важливі сервери виробництва, що призвело до зупинки виробничих ліній на понад два тижні.

Цікавим є те, що попри великий тиск, компанія відмовилася платити викуп і змогла самостійно відновити роботу за рахунок резервних копій, тип самим вона продемонструвала високу готовність до кібератак та ефективну стратегію протистояння таким інцидентам [21].

Для кращого розуміння унікальності атаки Norsk Hydro, порівняємо її ключові характеристики з іншими масштабними інцидентами кібервимагання (Таблиця 1.2).

Таблиця 1.2.

Порівняльна характеристика атаки Norsk Hydro з іншими масштабними атаками кібервимагання

	Nork Hydro	Інші типові інциденти	Примітки
Тип ПЗ	LockerGoga	WannaCry, NotPetya, Ryuk	LockerGoga фокусувався на промислових системах
Масштаб мережі	22 000 ПК у 170 локаціях	Зазвичай до 5-10000 тисяч ПК	Масштабне зараження всередині виробничої компанії
Кількість країн	40+	10-20	Світова географія поширення
Час простою виробництва	>2 тижні	1-7 днів	Прямий вплив на виробничі лінії
Фінансові витрати	$40-50 млн в перші тижні	$10-20млн	Високі витрати через паралізоване виробництво
Відповідь компанії	Відмова від викупу, використання резервних копій	Часто платять викуп	Демонструє успішну стратегію кіберстійкості

Висновки до розділу 1

У розділі 1 досліджено теоретичні основи кіберзлочинності, її сутність, види й сучасні тенденції розвитку. Встановлено, що кіберзлочинність є складним і багатогранним явищем, яке охоплює як атаки, спрямовані на інформаційні системи, так і злочини, в яких сучасні ІКТ є тільки інструментом їх здійснення.

Аналіз сучасних тенденцій продемонстрував, що кіберзлочинність має глобальний характер, стрімко зростає та еволюціонує разом із кіберпростором, а

її масштаби підтверджуються вражаючою статистикою щодо кількості інцидентів, фінансових втрат і географічного поширення. Важливу роль у розвитку кіберзлочинності відіграють такі фактори як поширення Інтернету, а також посилення залежності людини від ІКС та цифрових технологій.

Дослідження сучасних форм і методів кібератак показало, що кіберзлочинність набуває все більш організованого характеру, а реалізація злочинів відбувається за чітко структурованими етапами, серед яких: 1) розвідка та збір інформації; 2) первинне проникнення; 3) закріплення в системі; 4) розширення доступу; 5) реалізація атаки. Використання фішингу, соціальної інженерії, шкідливого ПЗ значно підвищує ефективність кібератак. Атака на компанію Norsk Hydro показала масштабність сучасних кіберінцидентів, їх глобальний вплив і колосальні економічні наслідки.

Виходячи із вище переліченого, кіберзлочинність у наш час можна охарактеризувати високим рівнем технологічності, динамічності та організованості, що зумовлює необхідність детального дослідження методів її протидії, вдосконалення систем кіберзахисту й розвитку міжнародної співпраці для подолання цієї проблеми.

РОЗДІЛ 2. НАПРЯМИ І МЕТОДИ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ НА МІЖНАРОДНОМУ РІВНІ

2.1 Нормативно-правове регулювання боротьби з кіберзлочинністю на глобальному рівні

Сучасна система протидії кіберзлочинності ґрунтується на комплексі міжнародних нормативно-правових актів, які, у свою чергу, формують основу для співпраці держав у сфері виявлення, розслідування та запобігання кіберзлочинам. З огляду на глобальний характер кіберзлочинності, ефективне протистояння цьому явищу неможливе в межах однієї держави і вимагає узгодження законодавства і створення спільних механізмів протидії на міжнародному рівні.

Одним із головних документів у сфері кібербезпеки міжнародного масштабу є Будапештська конвенція про кіберзлочинність (2001р.), яка стала першим правовим актом, що визначив основні категорії кіберзлочинів і механізми міжнародного співробітництва з метою їх подолання [22].

Структура Будапештської конвенції представлена на рис. 2.1.

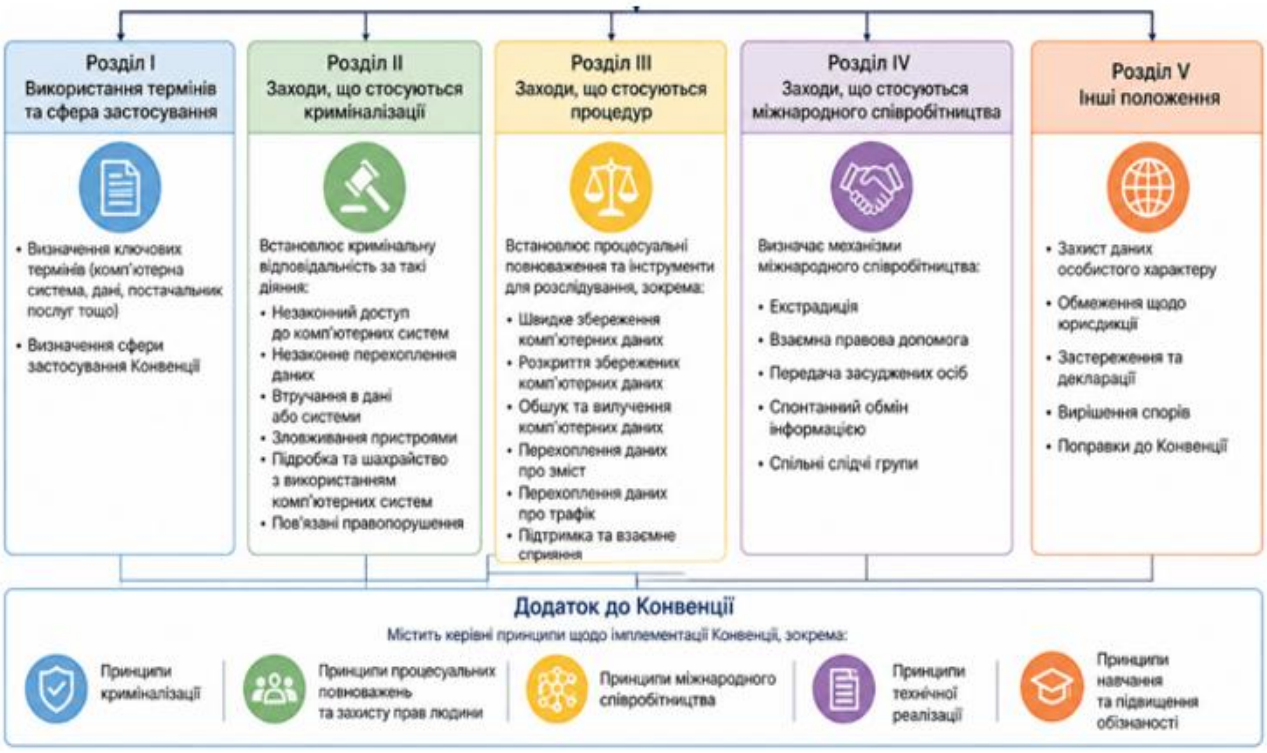

Рис. 2.1. Структура Будапештської конвенції про кіберзлочинність

Конвенція передбачає криміналізацію незаконного доступу до систем, перехоплення даних, втручання в системи та використання шкідливого ПЗ. Попри це станом на 2026 рік, правове поле вийшло за межі тільки кримінального переслідування і сьогодні охоплює питання технологічної стійкості та контроль використання штучного інтелекту.

Ключову роль у формуванні міжнародної політики кібербезпеки відіграє Організація об'єднаних націй (ООН), яка через Управління ООН з наркотиків і злочинності (UNODC) координує дослідження кіберзлочинності та сприяє розвитку міжнародних стандартів реагування на кібератаки [23].

Важливим етапом у діяльності ООН стало завершення роботи над Конвенцією щодо протидії використанню інформаційно-комунікаційних технологій у злочинних цілях 2024 року (UN Convention against Cybercrime) [24]. Цей документ став першою всеосяжною угодою під керівництвом ООН, спрямованим на створенні універсальної правової бази для боротьби з кіберзлочинністю, що доповнює регіональні угоди та розширює можливості екстрадиції та взаємної правової допомоги на світовому рівні.

Європейський союз, у свою чергу, формує власну нормативно правову базу через директиви та регламенти, серед яких ключовими є:

- Директива про мережеву та інформаційну безпеку (NIS Directive 2016) [22].
- Загальний регламент щодо захисту даних GDPR (2016) [25].
- Закон ЄС про кібербезпеку (Cybersecurity Act 2019) [26].
- Директива NIS2 (2022) [27].
- Закон про цифрову операційну стійкість DORA (2022) [28].
- Закон ЄС про ШІ (EU Artificial Intelligence Act 2024) [29].

Ці документи створені для підвищення рівня кіберстійкості критичної інфраструктури та захисту персональних даних.

У таблиці 2.1 наведено порівняння положень ключових міжнародних документів та актів ЄС з питань кібербезпеки і протидії кіберзлочинності.

Таблиця 2.1.

Порівняння нормативно-правових документів з кібербезпеки

Назва	Тип	Мета	Основні положення	Особливість
Будапештська конвенція про кіберзлочин-ність (2001)	Міжнародний договір	Гармонізація національних законів про кіберзлочини, покращення слідчих заходів і міжнародної співпраці.	Визначає злочини (незаконний доступ, перехоплення, втручання в дані) та зобов'язує держави взаємодіяти у розслідуваннях.	Перший і основний міжнародний інструмент, спрямований на кримінальне переслідування кіберзлочинців
Директива ЄС NIS-NIS2 (2016, 2022)	Директива ЄС (обов'язкова для членів ЄС, гармонізована в Україні).	Підвищення рівня кібербезпеки критичної інфраструк-тури	Розширення сфери застосування, суворіші вимоги до звітування про кіберінциденти, особиста відповідальність керівників за кіберпорушення.	Фокус на запобіганні та управлінні ризиками, а не лише на реагуванні на інциденти
Загальний регламент щодо захисту даних GDPR (2016)	Регламент ЄС (має пряму дію)	Захист персональних даних фізичних осіб у ЄС	Право на забуття, обов'язкове повідомлення про витоки даних протягом 72 годин	Екстериторіа-льність: діє для компаній по всьому світу, якщо вони обробляють дані громадян ЄС.

Продовження табл. 2.1.

Назва	Тип	Мета	Основні положення	Особливість
Закон про цифрову операційну стійкість DORA (2022)	Регламент ЄС	Забезпечення стійкості фінансового сектора до кіберзагроз.	Суворі вимоги до управління ризиками ІКТ, тестування стійкості й нагляду за сторонніми постачальниками послуг.	Вузько-галузевий, але дуже деталізований стандарт для фінансів.
Закон ЄС про кібербезпеку (2019)	Регламент ЄС	Створення системи сертифікації кібербезпеки та посилення ролі Агентства ЄС ENISA.	Запровадження єдиних сертифікатів для ІТ-продуктів та послуг, що гарантує їхню захищеність.	Довіра до цифрових продуктів на єдиному ринку.
Закон ЄС про ШІ (2024)	Регламент ЄС	Регулювання безпечного використання ШІ	Запобігання використанню ШІ для автоматизації кібератак та дезінформації	Перший у світі комплексний механізм контролю за алгоритмічними загрозами.
Конвенція ООН проти кіберзлочин-ності (2024)	Міжнародний договір	Створення універсальної правової бази	Перший документ під егідою ООН, що доповнює Будапештську конвенцію.	Глобальне охоплення, що виходить за межі окремих держав і регіональних союзів.

Слід окремо відзначити, що значну увагу в європейській практиці приділено проблемам безпеки новітніх технологій. Зокрема Закон ЄС про ШІ встановив жорсткі рамки для використання ШІ, що дозволило мінімізувати ризики його застосування для автоматизації кібератак і створення діпфейків [29]. Крім того, Закон про кіберстійкість запровадив обов'язкові вимоги до безпеки для всіх цифрових продуктів, що потрапляють на ринок ЄС, зобов'язуючи виробників забезпечувати підтримку безпеки протягом усього циклу життя продукту [30].

Технічне регулювання та стандартизація як інструмент дотримання міжнародних норм. Водночас, сьогодні ефективність міжнародних актів забезпечується не лише за допомогою законодавчих заборон, а й через систему економічного регулювання та обов'язкову сертифікацію. Головну роль у цьому процесі відіграє Агентство ЄС з кібербезпеки ENISA [7]. Згідно із Законом ЄС про кібербезпеку ENISA розробляє схеми сертифікацій, які стають обов'язковими для ІТ продуктів, що будуть використані в критичній інфраструктурі [26]. За допомогою цього створюється система де продукт не може бути допущений на ринок без підтвердження його стійкості до відомих вразливостей.

Паралельно з державним регулюванням діє система міжнародних стандартів ISO/IEC. Так, ISO/IEC 27001:2022 прийнято вважати «золотим стандартом» з управління інформаційною безпекою [31]. Документ інтегрує вимоги щодо захисту даних у хмарах та безпеки ланцюгів постачання, що дозволяє бізнесу відповідати вимогам Директиви NIS2 на практичному рівні.

Особливістю сучасного етапу є зміна техніко-правової парадигми на користь архітектури «нульової довіри». Ця модель, закріплена у міжнародних стандартах (зокрема NIST SP 800-207), базується на принципі «нікому не довіряй і завжди перевіряй» [32]. Впровадження Zero Trust дозволяє мінімізувати ризики внутрішніх загроз і горизонтального переміщення зловмисників у мережах.

Міжнародно-правові санкції як механізм примусу та атрибуції. Важливим елементом міжнародної протидії кіберзлочинцям нині є активне застосування

інструменту кібердипломатії ЄС (Cyber Diplomacy Toolbox). Оскільки традиційне кримінальне переслідування часто ускладнене через перебування зловмисника в країнах, які не видають злочинців, санкції стали інструментом прямого впливу [33]. Вони включають заморожування активів, візові обмеження та заборону на передачу технологій. Також важливу роль у цій сфері є співпраця з Міжнародною групою з протидії відмиванню брудних грошей FATF у сфері відстеження криптовалютних транзакцій, що дозволяє прибрати анонімність фінансових потоків хакерських угрупувань.

Україна активно гармонізує своє законодавство з нормами ЄС, зокрема у рамках адаптації вимог Директиви NIS2 та впровадження стандартів захисту персональних даних, що відповідають GDPR. Цей процес є частиною євроінтеграції та посилення національної системи кібербезпеки, що включає захист від гібридних загроз, що підтверджується звітами Держспецзв'язку [34].

Таким чином, діюче міжнародне регулювання характеризується переходом до концепції «Security by Design» (безпека за замовчуванням), відповідно до якої відповідальність за кіберзахист перекладається з кінцевого споживача на компанії-розробників технологій і керівників організацій, що закріплено у відповідних законодавчих нормах, зокрема NIS2. Для України імплементація цих норм є ключовим інструментом інтеграції до Єдиного цифрового ринку ЄС.

2.2 Роль міжнародних і регіональних організацій у подоланні кіберзлочинності (ООН, Інтерпол, Європол, ENISA)

Через активну глобалізацію кіберзлочинність набуває інтернаціонального характеру, що ускладнює її ефективне виявлення та розслідування в межах однієї держави. Саме тому головну роль у протидії кіберзагрозам відіграють міжнародні організації, що забезпечують координацію між країнами, обмін інформацією, розробку стандартів кібербезпеки та проведення спільних операцій. За оцінками міжнародних аналітичних досліджень, тільки у 2025 році загальні збитки від кіберзлочинності у світі перевищили 10 трлн доларів США,

а середній час між інцидентами скоротився до кількох секунд [13]. Зловмисники активно використовують глобальну інфраструктуру інтернету, розміщують свої сервери в різних юрисдикціях, застосовують засоби для анонімізації, такі як VPN, проксі-сервери та мережу Tor, а також здійснюють одночасні атаки на об’єкти в різних країнах.

Виходячи з даних міжнародних звітів [6,7], понад 80% організацій у світі щороку зазнають хоча б однієї кібератаки, при чому велика кількість інцидентів залишаються нерозкритими через складність атрибуції. Саме тому ключову роль у протидії кіберзагрозам відіграють міжнародні організації, що забезпечують координацію між державами, своєчасний обмін інформацією, розробку єдиних стандартів кібербезпеки і проведення спільних операцій з метою нейтралізації кіберзлочинних угрупувань.

До провідних міжнародних організацій у сфері боротьби із кіберзлочинністю належать ООН, зокрема Управління ООН з питань наркотиків і злочинів UNODC, Міжнародна організація кримінальної поліції Інтерпол, організація кримінальної поліції ЄС Європол, Агентство з кібербезпеки ЄС ENISA.

Кожна з цих організацій має чітку мету та власні інструменти впливу на процеси забезпечення кібербезпеки. Так, ООН виконує функції з координації та сприяння розвитку глобальних ініціатив з кібербезпеки. Інтерпол об’єднує правоохоронні органи понад 190 країн світу та координує десятки міжнародних організацій з протидії кіберзлочинам. Європол через підрозділ ЕС3 здійснює аналіз тисяч кіберінцидентів і формує рекомендації для країн ЕС.

Роль Організації Об’єднаних Націй у подоланні кіберзлочинності. Роль ООН полягає у формуванні та створенні політичного консенсусу і універсальних правових стандартів. Через Управління ООН з наркотиків і злочинності UNODC організація реалізує всеохоплюючу програму з протидії кіберзлочинності яка спрямована на [23]:

- Надання технічної допомоги країнам що активно розвиваються, для розбудови їхніх правових систем.

- Координацію роботи над Універсальною конвенцією ООН проти кіберзлочинності.
- Підтримку міжурядових експертних груп, що розробляють норми відповідальної поведінки держав у кіберпросторі.

Одним із ключових елементів діяльності ООН є робота Міжнародного союзу електрозв'язку (ITU). ITU виступає у ролі спеціалізованої установи, яка розробляє технічні стандарти, надає допомогу країнам для зміцнення їх кібербезпеки. Станом на сьогодні особливої уваги набув глобальний індекс кібербезпеки (GCI), який оцінює держави за п'ятьма критеріями: правові, технічні та організаційні заходи, розвиток потенціалу та міжнародна співпраця [35]. Це стимулює країни-члени ООН гармонізувати свої правові системи відповідно до світових вимог.

Розподіл рівнів кіберготовності країн за методикою ITU (ООН) показано у таблиці 2.2.

Таблиця 2.2.

Розподіл рівнів кіберготовності країн за методикою ITU у 2024-2026 рр.

Показник розбудови потенціалу	Середній світовий рівень (%)	Динаміка (2024-2026)	Основний фокус ООН
Юридичні заходи	82%	+12%	Гармонізація законів з Конвенцією ООН
Технічні заходи	68%	+18%	Створення національних груп CERT/CSIRT
Організаційні заходи	74%	+7%	Наявність діючих стратегій і дорожніх карт
Розвиток потенціалу	59%	+22%	Навчання фахівців, наукові гранти
Міжнародна співпраця	61%	+15%	Укладання двосторонніх договорів про екстрадицію

З наведених даних можна побачити, що найбільший приріст спостерігається у сфері розвитку потенціалу. Це є результатом реалізації Глобальної програми ООН з протидії кіберзлочинності, яка зосереджена на навчанні фахівців з цифрової криміналістики. Водночас технічні заходи потребують значних інвестицій, через різницю в розвитку ІКТ між країнами.

Діяльність Інтерполу у сфері протидії кіберзлочинності. Міжнародна організація кримінальної поліції є однією з головних міжнародних структур, що забезпечують координацію діяльності поліції різних країн світу у боротьбі з кіберзлочинністю. Інтерпол активно розвиває напрям кібербезпеки через створення підрозділів спеціального призначення та центрів аналізу загроз.

Основними функції Інтерполу є:

- Координація міжнародних розслідувань кіберзлочинів.
- Обмін оперативною інформацією між країнами.
- Проведення операцій проти кіберзлочинних угрупувань.
- Надання аналітичної та технічної інформації підтримки країнам [5].

Окреме значення має Глобальний комплекс інновацій Інтерполу у Сінгапурі, пріоритетами якого є:

- Оперативна підтримка: розсилка «Фіолетових сповіщень» про нові методи кіберзлочинів та інструменти хакерів.
- Публічно-приватне партнерство: спільні операції з технологічними гігантами, такими як Microsoft і Google, для виявлення та ліквідації ботнетів.
- Надання оперативного доступу до даних приватних компаній для визначення серверів управління кібертаками [36].

Схема взаємодії Інтерполу з національними правоохоронними органами показана на рис. 2.2.

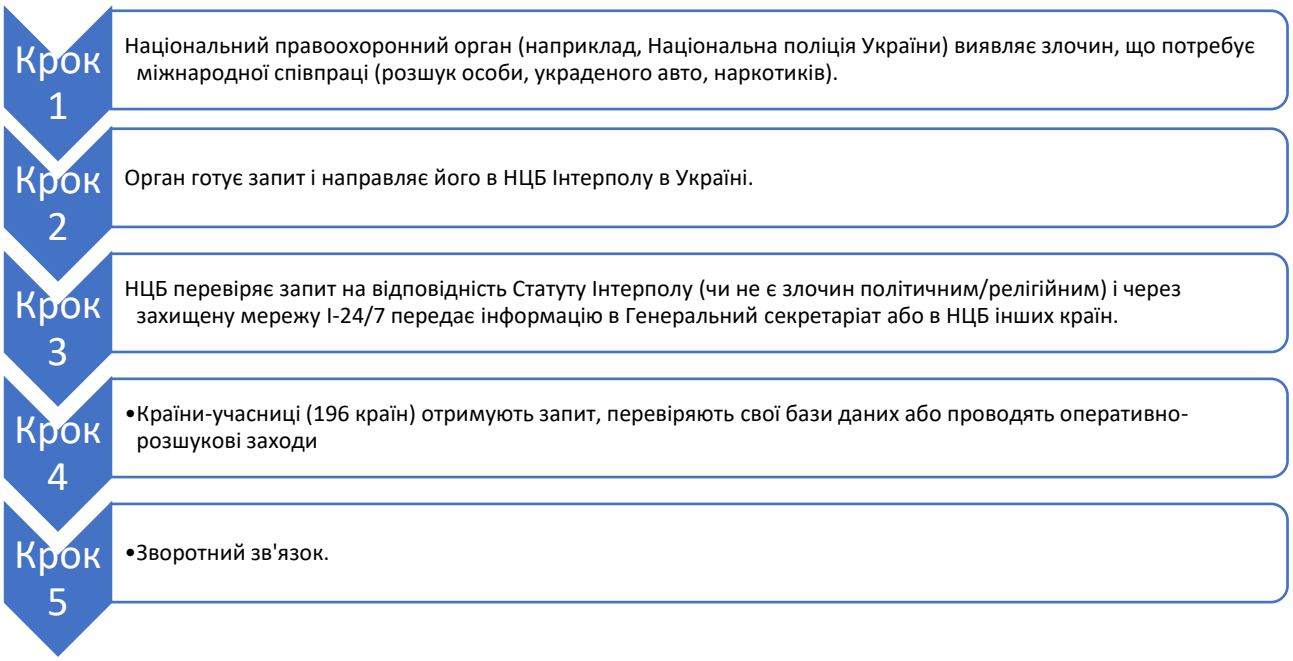

Рис. 2.2. Схема взаємодії Інтерполу з національними правоохоронними органами

Роль Європолу у забезпеченні кібербезпеки ЄС. На регіональному рівні найвищу ефективність демонструє Європейська організація кримінальної поліції, зокрема завдяки діяльності Європейського центру кіберзлочинності ЕСЗ та постійної міжнародної оперативної групи J-CAT [6,37].

Центр ЕСЗ став ключовим аналітичним хабом що забезпечує:

- Функціонування групи швидкого реагування, J-CAT (Joint Cybercrime Action Taskforce), де офіцери з різних країн світу спільно працюють над розслідуванням масштабних атак у реальному часі.
- Аналітичну підтримку, яка включає розробку щорічних звітів з оцінювання загроз організованої інтернет-злочинності (Internet Organized Crime Threat Assessment, IOCTA) [38], які є дорожньою картою для правоохоронців ЄС та інших країн.
- Координацію транскордонних операцій. Яскравим прикладом є операції з ліквідації інфраструктури вірусів вимагачів, де Європол забезпечує одночасні арешти серверів у десятках юрисдикцій.

Європол активно працює з правоохоронними органами країн ЄС, а також приватним сектором, серед яких ІТ-компанії, банки і провайдери цифрових послуг, завдяки цьому є можливість активно реагувати на нові кіберзагрози.

Крім того, Європол відіграє важливу роль у боротьбі з кіберзлочинністю в даркнеті, включаючи ліквідацію незаконних онлайн-маркетплейсів, які зазвичай використовуються для продажу наркотиків, викрадених даних і шкідливого ПЗ.

За останні роки було проведено багато операцій із закриттям таких платформ. Зокрема у межах операції Dark HunTor було ліквідовано понад 150 продавців незаконних товарів [9]. Іншим прикладом є закриття у 2022 році одного з найбільших ресурсів даркнету - маркету Hydra, який обслуговував сотні тисяч користувачів і генерував мільярдні обороти. У результаті спільної операції було вилучено серверну інфраструктуру платформи і значні обсяги криптовалюти на суму 23 млн євро [37].

Водночас, варто відзначити наявні відмінності в підходах міжнародної та європейської організацій кримінальної поліції, які наведені у таблиці 2.3.

Таблиця 2.3.

Відмінності у підходах Інтерполу та Європолу

Характеристика	Інтерпол	Європол
Географія	Весь світ: понад 194 країн	Країни ЄС та партнери
Основна роль	Обмін даними, розшук (Red Notices*)	Аналіз, координація операцій
Бази даних	Глобальні (ДНК, паспортів)	Оперативні Європейські
Арешти	Не проводять (тільки роблять запити)	Не проводять (координують)

***** Червоне повідомлення або «червона картка» - це офіційний міжнародний запит Інтерполу до правоохоронних органів усього світу про розшук і тимчасовий арешт особи з метою її подальшої екстрадиції (видачі) країні-ініціатору запиту.

Роль ENISA у формуванні стійкості до кіберзлочинів. На відміну від поліцейських структур, ENISA спрямовує свою діяльність на запобігання та

технічну експертизу у галузі протидії кіберзлочинності, зокрема виконуючи такі функції [39]:

- Сертифікація: розробка та нагляд за єдиними схемами сертифікації кібербезпеки для продуктів ІКТ у ЄС.
- Управління кризами: координація мережі груп реагування на інциденти кібербезпеки CSIRTs і проведення найбільших у світі кібернавчань Cyber Europe.
- Аналіз загроз: моніторинг ландшафту загроз і розробка рекомендацій щодо безпеки критичної інфраструктури (енергетика, транспорт, медицина).

ENISA не здійснює правоохоронної діяльності, однак її роль є критично важливою у формуванні політики безпеки та підвищенні рівня готовності до кіберінцидентів не тільки в рамках ЄС, але й у інших країнах Європи.

Короткий опис основних діючих ініціатив ENISA у сфері забезпечення кіберстійкості і протидії кіберзлочинам зокрема представлені у таблиці 2.4.

Таблиця 2.4.

Основні ініціативи ENISA у сфері забезпечення кіберстійкості у 2026 році

Напрям	Опис діяльності	Цільова аудиторія
Навчання Cyber Europe	Наймасштабніші симуляції атак на енергомережі та авіацію	Державні органи, оператори об’єктів критичної інфраструктури
Схеми EUCC	Сертифікація хмарних послуг та обладнання 5G/6G	Виробники ІКТ, провайдери зв'язку
Звіти ETL	Глибокий аналіз використання ШІ у кіберзлочинній діяльності	Аналітики безпеки, уряди країн ЄС та Європи, в т. ч. України

Сьогодні ENISA активно впроваджує оновлену модель кіберстійкості, що базується на принципі «Жодна система не може бути захищена на 100%», відповідно фокус змінюється на здатність системи функціонувати під час атаки та можливість швидкого відновлення.

Ця модель включає п’ять основних етапів, які ENISA інтегрує в національні стратегії країн-партнерів (у тому числі України):

1. Прогнозування: використання інструментів ШІ для аналізу великих масивів даних про нові вразливості та методи атак.

2. Стримування: застосування технічних стандартів сертифікації для того, щоб критичні системи були готові витримати початкову фазу атаки без повної зупинки.

3. Відновлення: розробка уніфікованих планів безперервності бізнесу та координація транскордонної допомоги через мережу команд CSIRT.

4. Адаптація: аналіз реалізованих атак для вдосконалення майбутніх механізмів протидії [40].

2.3 Технологічні методи виявлення та запобігання кіберзлочинам

В умовах стрімкого розвитку інформаційних технологій, еволюції програмного забезпечення та зростання атак «нульового дня», ефективна протидія кіберзлочинності неможлива без використання комплексних технологічних рішень. Зважаючи на постійне ускладнення методів атак, традиційні сигнатурні методи захисту втрачають свою ефективність, що зумовлює необхідність і невідкладність впровадження інтелектуальних систем виявлення, аналізу та реагування на кіберінциденти [11,15].

За даними міжнародних досліджень, понад 70% успішних кібератак пов’язані з недостатнім рівнем моніторингу та не своєчасним виявленням загроз. Станом на 2026 рік парадигма технологічного захисту трансформувалася від пасивного очікування атаки до проактивного виявлення (Threat Hunting) і впровадження архітектури нульової довіри, де головна роль відведена автоматизації та штучному інтелекту.

За аналітичними даними міжнародних досліджень [8,9,13]:

- Понад 80% атак мають багатоступеневий характер.
- Середній час виявлення інциденту становить від 10 до 20 днів, хоча раніше перевищував 200 днів.

- Використання сучасних систем кіберзахисту дозволяє скоротити час реагування на інцидент (Meen Time to Respond) більш ніж на 60%.

Це підтверджує що технологічні методи є ключовим фактором ефективного захисту від кіберзлочинів.

1. *Системи виявлення та запобігання вторгненням (IDS/IPS)* є базовим рівнем технічного захисту інформаційних систем і мереж [41]. Вони здійснюють безперервний аналіз мережевого трафіку та системних подій з метою виявлення аномалій і відомих сигнатур атак. Принципи роботи різних систем IDS/IPS можуть відрізнятися й охоплювати:

- Сигнатурний аналіз – порівняння вхідного трафіку з базою даних відомих сигнатур атак. Це показує високу ефективність проти масованих загроз, але абсолютно безсильно проти атак «нульового дня».
- Аномальний аналіз – створення профілю нормального трафіку та фіксація будь-яких відхилень від нього.
- Аналіз протоколів – перевірка відповідності стандартам.

Говорячи про конкретні показники, то можна відзначити, що IDS/IPS здатні виявляти до 70-80% відомих атак. Водночас, рівень хибнопозитивних спрацювань може сягати 10-30%, що потребує додаткової фільтрації. Як і у кожної системи технічного захисту, в IDS/IPS наявні обмеження, зокрема вони є неефективними проти нових атак і потребують постійного оновлення сигнатур загроз [41].

Сучасний мережевий захист перейшов до концепції розширеного виявлення і реагування на кіберзагрози (Extended Detection and Response, XDR). На відміну від класичних рішень, XDR поєднує дані не тільки від мережевих шлюзів, а й із хмарних контейнерів, зашифрованих каналів і пристроїв інтернету речей IoT [42]. Це дозволяє виявляти атаку, яка бере початок із фішингового листа, продовжується через злам хмарного сховища і закінчується спробою крадіжки даних через мережевий порт.

Виходячи із вище зазначеного можна сказати що, IDS/IPS це «перша лінія оборони», але вона недостатня та неповноцінна без інших систем.

2. *SIEM-системи (Security Information and Event Management).* Для управління великими масивами даних у сфері кібербезпеки використовують SIEM-системи. Їх роль в основному полягає у кореляції подій. Наприклад, один невдалий вхід в систему є лише подією, але 100 невдалих входів з різних IP-адрес протягом хвилини – це вже інцидент, який SIEM об'єднає та визначить як єдину Brute-force атаку, а не окремі інциденти.

Основними функціями SIEM-систем є:

- Централізований збір логів (сервери, мережі, додатки).
- Кореляція подій.
- Виявлення складних атак.
- Формування звітів і сповіщень [43].

Організації, що використовують SIEM-системи, як правило виявляють інциденти на 40-60% швидше. Також SIEM дозволяє виявляти атаки, які тривають тижнями без явних ознак. Сучасним стандартом є інтеграція SIEM із системами SOAR (Security Orchestration, Automation and Response) [44], які дозволяють створювати цифрові алгоритми автоматичного реагування.

Яскравим прикладом ефективності SIEM із систем SOAR є відбиття атаки програм-вимагачів на логістичну компанію «GlobalLogist» [14]. Атака було здійснена за допомогою методу соціальної інженерії, а саме вішингу, спрямованого на співробітника IT-підтримки. Розглянемо детальніше хід атаки і технологічну протидію.

На етапі початкового доступу зловмисники отримали доступ до облікового запису адміністратора: було зафіксовано вхід в систему у нетиповій географічній локації о 2:15 ночі. SIEM-система миттєво ідентифікувала це як аномалію, зіставивши вхід із графіком відпусток або відряджень працівника.

Потім зловмисники намагалися запустити сканування внутрішньої мережі для пошуку вразливих серверів баз даних. EDR-сенсори зафіксували запуск сканерів, а SIEM скорелювала цю активність із входом адміністратора.

Наступним кроком буда активація SOAR-плейбука «Ransomware Defense», який забезпечив ізоляцію: через визначений «критичний» рівень загрози,

система SOAR без підтвердження заблокувала скомпрометований обліковий запис у всьому домені; захист даних: SOAR ініціювала створення негайних «тіньових копій» критичних баз даних, щоб запобігти їх шифруванню; блокування комунікацій: на рівні корпоративного Firewall було автоматично заблоковано трафік до серверів CC2 зловмисників у реальному часі. Як результат атака була зупинена на етапі розвідки.

Використання такої інтегрованої моделі взаємодії SIEM і SOAR дозволило зменшити потенційні збитки з $4.5млн до $0 [8].

Системи EDR/MDR. Системи виявлення і реагування на рівні кінцевих точок (Endpoint detection and response, EDR) стали критично важливими через перехід більшості компаній на віддалену роботу та використання власних пристроїв [16]. Сучасне EDR-рішення виконує три основні функції:

- Постійний запис подій.
- Виявлення аномалій у реальному часі.
- Дистанційне реагування та ізоляція заражених пристроїв.
- Аналіз після атаки.

Нині стали популярні сервіси керованого виявлення та реагування (Managed Detection and Response, MDR), де EDR доповнюється цілодобовою підтримкою аналітичних груп. Для організацій, які не мають власного штату кібераналітиків, це стало особливо актуальним.

Використання штучного інтелекту. Використання штучного інтелекту та машинного навчання в галузі кібербезпеки перейшло з категорії інновацій у категорію необхідності [45].

Серед основних напрямів використання ШІ виділяють три основні:

- Прогнозування атак, який охоплює аналіз даркнету та форумів зловмисників для виявлення підготовки нових інструментів зламу.
- Зменшення кількості хибнопозитивних спрацювань, оскільки ШІ може фільтрувати тисячі фонових сповіщень, виділяючи лише небезпечні події.

- Розвиток генеративного ШІ, який допомагає аналітикам інтерпретувати складний код шкідливого ПЗ, перекладаючи його на зрозумілу «людську мову».

За оцінками аналітиків, використання ШІ підвищує ефективність виявлення атак на 30-40%. Попри наявність багатьох суттєвих переваг ШІ має низку недоліків, зокрема загроза «отруєння даних», коли зловмисник намагається навчити ШІ не помічати певні типи атак [45].

Розвідка кіберзагроз (Threat Intelligence) - це проактивний підхід до кіберзахисту, який базується на аналізі зовнішніх загроз і охоплює використання індикаторів компрометації, таких як хеш-суми файлів, IP-адреси серверів управління та зловмисні URL-адреси [11].

Розвідку загроз поділяють на такі види:

- Тактична, яка відповідає за методи кібератак.
- Технічна, яка відповідає за IP, домени, хеші.
- Операційна, що забезпечує аналіз загроз на рівні конкретної компанії.
- Стратегічна – комплексна і довготермінова, встановлює загальні тенденції розвитку кіберзагроз.

Порівняльна характеристика технологічних рішень кіберзахисту подана в таблиці 2.5.

Таблиця 2.5.

Порівняльна характеристика технологічних рішень кіберзахисту

Вид	Об’єкт захисту	Метод аналізу	Рівень автома-тизації	Переваги	Недоліки
IDS/IPS	Мережевий периметр, трафік	Сигнатур-ний та евристичний	6	Миттєве блокування відомих атак	Високий рівень хибних спрацювань
SIEM	Лог-файли, події безпеки	Кореляція подій у реальному часі	5	Централі-зований моніторинг всієї IT-інфрастр-ри	Складна конфігурація, потреба у великих обсягах сховища

Продовження табл. 2.5.

Вид	Об’єкт захисту	Метод аналізу	Рівень автоматизації	Переваги	Недоліки
EDR	ПК, сервери, хмари	Поведінковий аналіз	8	Виявлення складних загроз	Високе навантаження на ресурси кінцевих пристроїв
SOAR	Процес реагування на інцидент	Алгоритмічні «плейбуки»	10	Скорочення часу реагування	Ризик блокування процесів при помилці в алгоритмі
ШІ	Дані та моделі поведінки	Нейронні мережі, глибинне навчання	9	Самонавчання	Можливість «отруєння» даних
Розвідка загроз	Стратегія захисту	Аналіз зовнішніх баз загроз	4	Налаштування засобів захисту до початку атаки	Залежність від актуальності зовнішніх джерел даних

Всі вище зазначені технології об’єднуються в межах Центру операційної безпеки (SOC), який у сучасній конфігурації працює за моделлю безперервного моніторингу (Continuous Monitoring). Основні процеси SOC охоплюють:

- Збір даних шляхом агрегації логів з використанням SIEM/XDR.
- Аналіз, який передбачає верифікацію загроз за допомогою ШІ та розвідки загроз.
- Реагування з використання SOAR для нейтралізації атак.
- Цифрова криміналістика (Forensics) з метою встановлення причин інциденту [46].

Таким чином, проведений аналіз технологічних методів виявлення та запобігання кіберзагрозам, демонструє, що сучасна парадигма кібербезпеки

остаточно перейшла від пасивної оборони до проактивного інтелектуального реагування. Важливим елементом цього підходу є інтеграція й автоматизація, які забезпечують ефективність діючої системи захисту шляхом поєднання окремих інструментів (IDS, EDR, SIEM) на базі платформи SOAR.

Доведено, що використання алгоритмів ШІ, машинного навчання та нейромереж у системах поведінкового аналізу дозволяє виявляти аномалії, які неможливо ідентифікувати традиційними сигнатурними методами. Централізація процесів кіберзахисту забезпечується шляхом синергії технологій розвідки загроз і засобів автоматизованого реагування у рамках функціонування сучасних центрів моніторингу.

Таким чином, тільки комплексне поєднання новітніх технологічних рішень із чітко налаштованими процесами автоматизації та постійним моніторингом дозволяє забезпечити стійкість сучасної інформаційної інфраструктури до кіберзагроз будь-якого рівня складності.

Висновки до розділу 2

У розділі 2 узагальнено сучасні напрями та методи протидії на міжнародному та національному рівнях, а також сформовано основні наукові та практичні висновки.

У сфері нормативно правового-регулювання з’ясовано, що сучасна світова практика перейшла від пасивного покарання за скоєні правопорушення до проактивної стратегії забезпечення цифрової стійкості інфраструктури. На міжнародному рівні діють нормативні акти різного спрямування: глобальні рамкові стандарти та конвенції з протидії комп’ютерній злочинності (зокрема акти під егідою ООН та Ради Європи), галузеві регламенти цифрової стійкості фінансового сектора, а також сучасні директиви ЄС з управління кіберризикам (такі як NIS2).

Встановлено, що новітнє законодавство впроваджує концепцію «Security by Design», яка юридично перекладає відповідальність за безпеку цифрових

продуктів на їхніх розробників, що є критично важливим для стабільності глобального інформаційного простору.

Аналіз інституційного аспекту протидії кіберзагрозам довів, що подолання транскордонної кіберзлочинності неможливе в межах однієї країни. Провідні міжнародні інституції (Інтерпол, Європол та Агентство ЄС з кібербезпеки ENISA) роблять свій внесок через координацію спільних транскордонних груп розслідування, аналітичний моніторинг ландшафту загроз, сертифікацію систем захисту та побудову каналів безпечного обміну даними про індикатори компрометації в режимі реального часу. Саме така інтегрована система дозволяє ефективно виявляти, блокувати та ліквідовувати складні анонімні злочинні інфраструктури у тіньовому сегменті мережі даркнет.

Дослідження технологічних методів протидії кіберпорушенням підтвердило фундаментальну зміну парадигми кіберзахисту від пасивного моніторингу периметра та локальної фіксації інцидентів до системного розширеного виявлення і повністю автоматизованого реагування. Сучасна архітектура безпеки базується на глибокій інтеграції систем збору логів SIEM, концепції розширеного аналізу кінцевих точок і хмарних середовищ XDR і платформ оркестрації та автоматизації захисту (SOAR). Ключовим фактором ефективності цього процесу є широке впровадження ШІ та машинного навчання, що дозволяє виявляти аномалії на ранніх стадіях атаки й мінімізувати можливі фінансові збитки до нульового рівня без залучення людини.

Загалом з’ясовано, що ефективність національної системи кібербезпеки України напряму залежить від темпів гармонізації вітчизняного законодавства із актуальними технічними стандартами та правовими регламентами ЄС, що є обов’язковою умовою для успішної інтеграції країни до Єдиного цифрового ринку ЄС в умовах сучасного воєнного стану та протидії гібридним агресіям.

РОЗДІЛ 3 СВІТОВІ ТЕНДЕНЦІЇ І ВИКЛИКИ ПОДОЛАННЯ КІБЕРЗЛОЧИННОСТІ

3.1 Роль команд реагування на події кібербезпеки (CERT, CSIRT) у транскордонній протидії кіберзлочинності

Транскордонний характер сучасних кібератак, здатність зловмисників миттєво змінювати цифрову інфраструктуру та використовувати юрисдикційні відмінності між державами роблять ізольований захист національних кіберпросторів неефективним. Сьогодні ключовим елементом системи колективної відсічі кіберзлочинності стала мережа команд реагування на комп'ютерні надзвичайні події (Computer Emergency Response Team, CERT) і груп реагування на інцидент комп'ютерної безпеки (Computer Security Incident Response Team, CSIRT).

Ці структури виступають у ролі «цифрової швидкої допомоги», забезпечуючи оперативний технічний захист, локалізацію кіберінцидентів і ліквідацію їхніх наслідків на національному, галузевому та корпоративному рівнях [47].

Історія створення перших команд реагування була відповіддю на загрози монолітного шкідливого ПЗ (зокрема, хробака Morpiса у 1988 році), проте еволюція ландшафту загроз, автоматизація атак за допомогою ШІ та масове поширення програм-вимагачів змусили CERT/CSIRT перейти від локального управління інцидентами до проактивної міжнародної координації.

CERT є спеціалізованою групу експертів, основною метою якої є виявлення, аналіз та реагування на кіберінциденти, а також розробка рекомендацій щодо запобігання подібним атакам у майбутньому. CSIRT є більш широким поняттям та включає організації або команди, які забезпечують комплексне реагування на події кібербезпеки, поєднуючи технічні, юридичні та управлінські аспекти. Їх діяльність охоплює:

- Виявлення, тріаж (первинна оцінка критичності) й аналіз кіберінцидентів.
- Обмін інформацією про загрози.
- Координацію дій між організаціями.
- Розробку рекомендацій із захисту інформаційних систем.
- Проведення навчань та симуляцію кібератак.
- Взаємодію з міжнародними структурами та правоохоронними органами [47].

Попри схожість функцій CERT та CSIRT між ними існують певні відмінності що зумовлені правовим статусом та історичними особливостями розвитку. Для більш наочного розуміння специфіки їхньої діяльності доцільно провести порівняльний аналіз, представлений у таблиці 3.1.

Таблиця 3.1.

Порівняльна характеристика CERT та CSIRT

Характеристика	CERT	CSIRT
Основне призначення	Реагування на інциденти	Комплексне управління інцидентами
Сфера діяльності	Переважно технічна	Технічна та організаційна
Географія діяльності	Національна або галузева	Національна, міжнародна, корпоративна
Додаткові функції	Аналіз загроз	Координація навчання, взаємодія
Основні користувачі	Державні установи	Державні та приватні установи
Нормативне закріплення	Закріплено переважно в нормативних документах NIST	Є офіційним терміном європейського законодавства (Директиви NIS2, ENISA)

Міжнародна співпраця між CERT та CSIRT відбувається через спеціалізовані мережі взаємодії, які забезпечують постійний обмін інформацією про загрози та координацію дій у реальному часі. Основні напрями міжнародної співпраці охоплюють:

Оперативний обмін даними про загрози (Threat Intelligence Sharing). Одним із ключових механізмів взаємодії є обмін індикаторами компрометації (IoC), які являють собою цифрові сліди діяльності зловмисників: IP-адреси серверів управління, доменні імена, хеш-значення шкідливих файлів, сигнатури програм-вимагачів та інші технічні параметри. Важливим інструментом такого обміну є система MISP (Malware Information Sharing Platform), яка дозволяє автоматично передавати інформацію між командами реагування інших держав [48]. Наприклад CERT-UA може оперативно передавати інформацію про нову загрозу партнерам у країнах ЄС та США, що дозволяє блокувати шкідливу активність на рівні локальних SIEM-систем та IPS ще до початку поширення атаки.

Спільне розслідування кіберінцидентів. Команди CERT та CSIRT здійснюють технічний аналіз кіберінцидентів, виконують реверс-інжиніринг шкідливого ПЗ, досліджують журнали подій та формують технічні звіти. Отримані результати передаються міжнародним правоохоронним організаціям, зокрема Інтерполу та Європолу, для проведення міжнародних операцій із ліквідації інфраструктури кіберзлочинців. Яскравим прикладом такої взаємодії стала операція «Operation Magnus» у результаті якої урядові команди реагування спільно із правоохоронцями США та країн ЄС повністю ліквідували інфостілерів Redline та Amadey. Аналогічно, завдяки координації CERT і спецслужб, раніше було нейтралізовано найбільші ботнет-мережі Qakbot та Emotet.

Стандартизація та підвищення рівня кіберготовності. Важливим напрямом діяльності є формування єдиних стандартів реагування на кіберінциденти. Методологічною основою такої стандартизації виступають міжнародні стандарти серії ISO/IEC 27035 та розроблені інститутом стандартів і технологій США настанови NIST SP 800-61 [49,50]. Під егідою Міжнародного

союзу електрозв'язку (ITU) здійснюється оцінка готовності держав у межах Глобального індексу кібербезпеки одним із ключових технічних показників якого виступає саме ефективність функціонування національних CERT.

Для кращого розуміння архітектури міжнародної взаємодії команд реагування доцільно представити її у вигляді структурної схеми на рисунку 3.1.

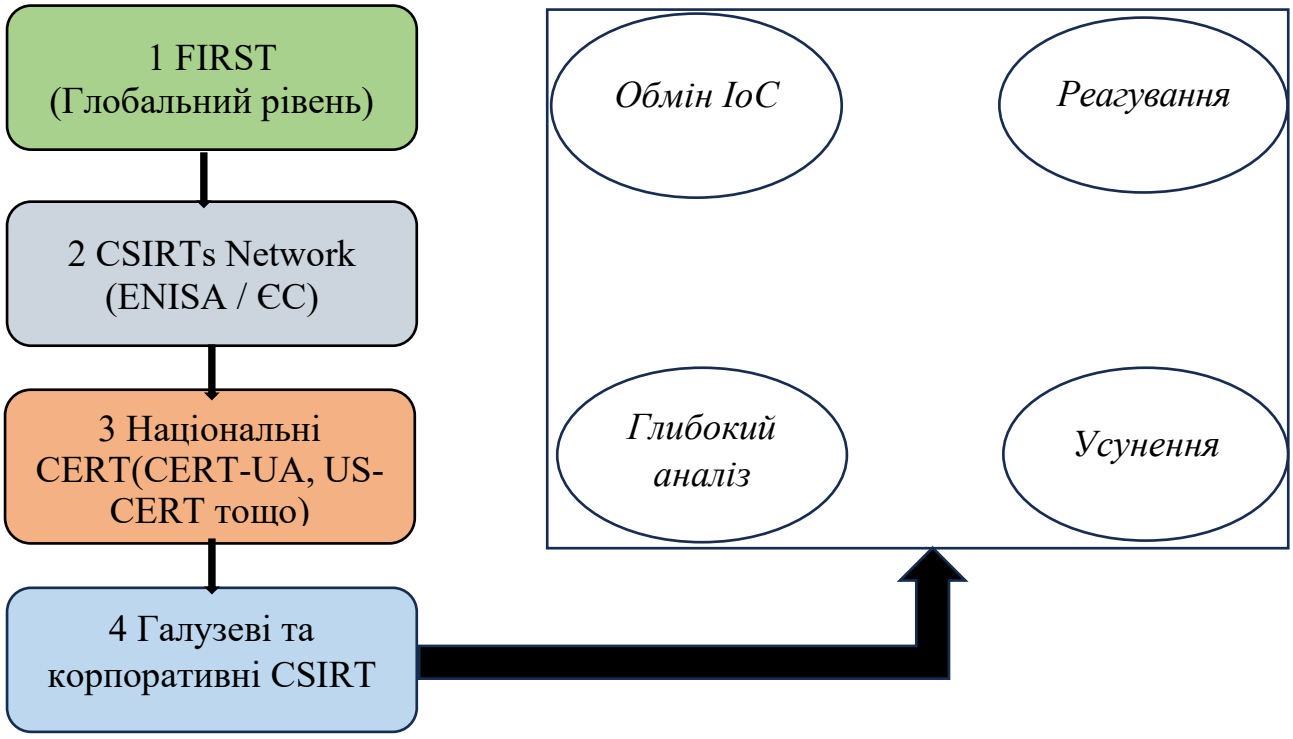

Рис. 3.1. Архітектура міжнародної взаємодії та життєвий цикл обробки інцидентів команд CERT/CSIRT

Аналіз представленої на рис. 3.1 архітектури дозволяє диференціювати міжнародну взаємодію на чотири базові рівні:

1. *Глобальний координаційний рівень - Форум FIRST,* який об'єднує понад 500 команд зі всього світу. Його діяльність спрямована на формування глобальних технічних стандартів(наприклад систем оцінювання вразливостей CVSS), визначення політик безпеки та верифікація критичних вразливостей нульового дня.

2. *Регіональний рівень – мережа команд CSIRT (ENISA),* який забезпечує координацію дій у межах ЄС і забезпечує транскордонну стійкість країн-членів ЄС відповідно до вимог Директиви NIS2 та проведення навчань Cyber Europe.

3. *Національний рівень - галузеві та корпоративні CSIRT.* Цей рівень представлений такими структурами як CERT-UA (Україна), US-CERT (США), які здійснюють безпосередній захист об’єктів критичної інфраструктури, моніторинг національного сегменту мережі інтернет та виявлення APT-атак, що фінансуються іншими державами.

4. *Операційний рівень - галузеві та корпоративні CSIRT,* охоплює внутрішні центри моніторингу безпеки SOC і профільні команди. На цьому рівні забезпечується впровадження практичного захисту підприємств, автоматизація реагування SOAR та обмін даними в межах вимог регламенту DORA.

Особливу роль у цій міжнародній архітектурі сьогодні відіграє саме Україна. Зокрема починаючи з 2022 року CERT-UA у співпраці з міжнародними партнерами протидіє координованим військовим операціям РФ. Основними цілями підконтрольних ГРУ та ФСБ хакерських угрупувань (Sandworm, Gamaredon APT28) є об’єкти критичної інфраструктури України. Завдяки унікальному практичному досвіду команди CERT-UA у відбитті масштабних кібератак на енергетичний та державні сектори, українські фахівці не лише отримують допомогу від західних партнерів, а й виступають головними надавачами аналітичних даних для світової спільноти, допомагаючи адаптувати глобальні системи захисту до нових типів загроз [51].

Незважаючи на високу ефективність, сьогодні функціонування цієї системи ускладнюється геополітичними суперечностями між окремими державами, правовими обмеженнями щодо транскордонної передачі технічних логів через закони про захист персональних даних (наприклад GDPR), а також необхідністю повної автоматизації аналізу через критичне зростання швидкості хакерських атак.

Таким чином, міжнародне співробітництво CERT та CSIRT є фундаментом практичної протидії кіберзлочинності. Інтеграція національних команд у глобальні мережі дозволяє світовому співтовариству оперативно локалізувати загрози, мінімізувати фінансові втрати і забезпечувати стабільність глобального цифрового простору.

3.2 Глобальні проблеми і виклики забезпечення кібератрибуції

У сучасному цифровому середовищі та умовах гібридних протистоянь важливим елементом міжнародної протидії кіберзлочинності є визначення джерела та виконавця кібератаки. Процес встановлення суб'єкта, відповідального за здійснення кібератаки, називається кібератрибуцією (Cyber Attribution). Цей процес передбачає комплекс технічних, організаційних, правових та політичних заходів, спрямованих на ідентифікацію осіб, груп або держав, які стоять за кіберінцидентом. Якщо технічна локалізація інциденту силами CERT/CSIRT дозволяє мінімізувати безпосередні збитки, то саме юридично та технічно обґрунтована атрибуція є базою для притягнення винних до відповідальності на міжнародному рівні, запровадження санкцій або реалізації права на колективну самооборону [52].

Проблема кібератрибуції в останні роки набула особливої актуальності у зв'язку із значним збільшенням кількості складних багаторівневих кібератак, які використовують приховану інфраструктуру, технології анонімізації та автоматизовані засоби маскування. Якщо традиційні злочини зазвичай мають чітко визначене місце скоєння, фізичні докази та конкретного виконавця, то у кіберпросторі процес встановлення джерела атаки є значно складнішим. Кіберзлочинці можуть використовувати сервери різних країн, мережі VPN, проксі-сервери, ботнети, інфраструктуру хмарних сервісів або мережу TOR для приховування власного місцезнаходження. Внаслідок цього навіть після виявлення IP-адреси джерела атаки вона не гарантує встановлення реального виконавця злочину [53].

За даними міжнародних досліджень [3,4], середній час виявлення та аналізу складних атак APT у 2025-2026 роках може перевищувати 250-300 днів, що суттєво ускладнюється проявами ретроспективного стирання логів і перешкоджає швидкому збору цифрових доказів й проведенню міжнародних розслідування. Для кращого розуміння складності кібератрибуції доцільно

виділити основні фактори які впливають на процес встановлення джерела атаки, класифікувати їх за технічними, правовими та геополітичними ознаками.

Анонімність кіберпростору та архітектура «хибних прапорів». Однією з головних особливостей цифрового середовища є високий рівень анонімності користувачів. Головною технічною перешкодою є засаднича архітектура мережі інтернет, яка розроблялася без урахування жорстких вимог до автентифікації відправника даних. Кіберзлочинці активно використовують :

- VPN-сервіси та проксі сервери у «сірих» юрисдикціях.
- Децентралізовану мережу TOR.
- Інфраструктуру глобальних ботнетів (включаючи скомпроментовані IoT пристрої).
- Зламані облікові записи й інфраструктуру третіх (легітимних) осіб.

У результаті реальне місцезнаходження злочинця може суттєво відрізнятися від місця, де було зафіксовано атаку. Наприклад, кібератака може фактично здійснюватися з однієї країни, тоді як журнали показують десятки інших держав, через які проходив трафік.

Особливу загрозу для міжнародної стабільності становить операції під хибним прапором (False Flag Operations). Складні APT-угрупування навмисно впроваджують у свій шкідливий код артефакти, які властиві хакерам з інших країн: використання чужих мовних розкладок або часових поясів під час компіляції файлів, запозичення специфічних методів шифрування або імітацію тактик, технік та процедур (TTPs) за класифікацією матриці MITRE ATT&CK, що належать іншим суб’єктам [54]. Внаслідок цього цифрова криміналістика стикається з проблемою ідентифікації: технічні сліди можуть вказувати на одну державу , тоді як реальний зловмисник перебуває в іншій.

Використання багаторівневої інфраструктури. Сучасні кіберзлочинні угрупування рідко використовують прямі канали зв’язку. Найчастіше застосовуються багаторівневі ланцюги перенаправлення трафіку, побудовані для унеможливлення зворотного трасування. Типову схему приховування джерела кібератаки представлено на рисунку 3.2.

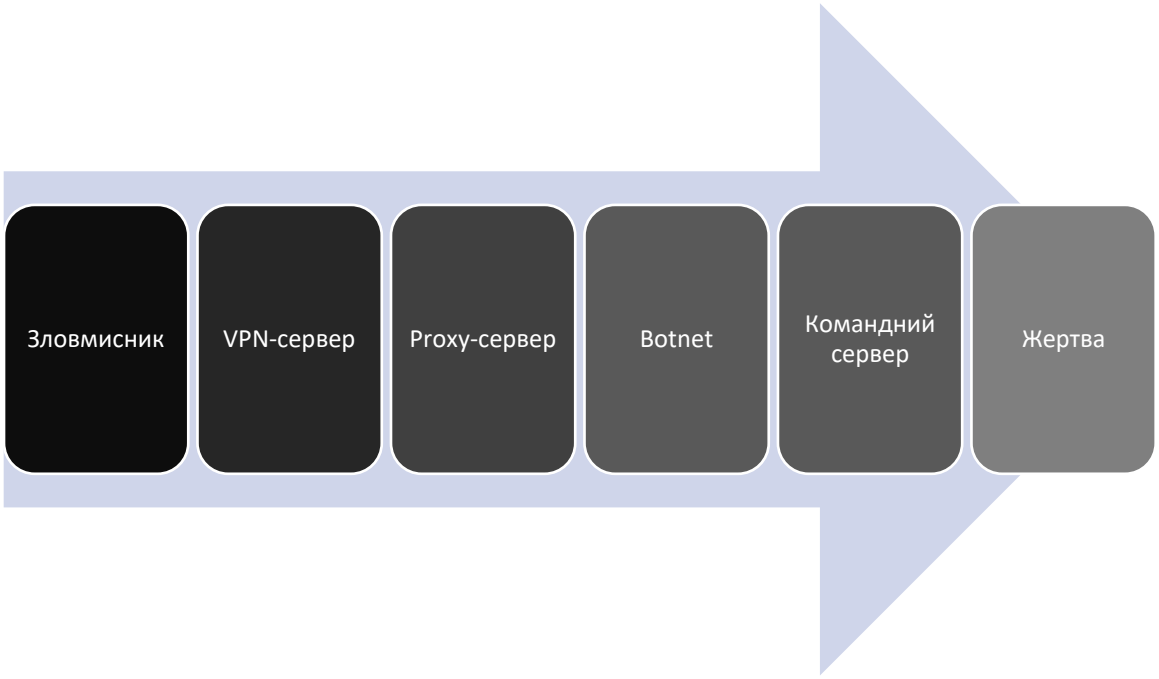

Рис. 3.2. Типова схема приховування джерела кібератаки

Юрисдикційні та правові обмеження. Кіберзлочини часто охоплюють територію декількох держав одночасно. Внаслідок цього виникає проблема визначення держави, яка має право проводити розслідування, порядку отримання цифрових доказів, механізмів міжнародного обміну інформацією та процедури екстрадиції підозрюваних осіб.

Суттєвою проблемою залишається правова фрагментація. Будапештська конвенція не охоплює у повному обсязі транскордонні кібератаки, що фінансуються урядами, а новий проєкт Конвенції ООН містить політичні колізії. Крім того, дії, які в одній державі вважаються тяжким кіберзлочином, а в іншій можуть бути недостатньо врегульовані законодавством. Передача логів між корпоративними SOC різних країн часто обмежується вимогами щодо захисту персональних даних (наприклад, регламентом GDPR в ЄС), що значно уповільнює міжнародне розслідування [53].

Геополітичні фактори та політизація рішень. Під час розслідування атак, пов’язаних із державними або напівдержавними структурами, процес атрибуції виходить за межі технічного аналізу. Низка авторитарних держав (зокрема РФ, КНДР, Іран) свідомо надають безпечний притулок (Safe Haven) внутрішнім кіберкримінальним угрупованням, якщо їхня деструктивна діяльність

спрямована проти політичних опонентів. Деякі країни відмовляються надавати інформацію, ігнорують запити Інтерполу, не визнають результати розслідувань , приховують діяльність кіберугрупувань та використовують кібероперації як інструмент політичного тиску.

Саме тому у міжнародній практиці чітко розділяють три типи атрибуцій:

- Технічна атрибуція: здійснюється компаніями з кібербезпеки (CrowdStrike, Mandiant) та державними CERT. Вона визначає лише цифровий профіль (наприклад, діяльність групи SandWorm або APT28).
- Юридична атрибуція: Висунення офіційних звинувачень або видача ордерів на арешт конкретних хакерів судовими органами.
- Політична атрибуція: Публічна заява керівництва держави або коаліції країн (НАТО, ЄС) про відповідальність конкретної країни, що часто базується на аналізі геополітичної вигоди [52].

Практичні кейси міжнародної атрибуції та досвід України

Одним із найбільш відомих прикладів складної атрибуції стала атка із використання шкідливого програмного забезпечення NotPetya у 2017 році. Первинно шкідлива програма маскувалася під програму-вимагача, однак подальший аналіз показав її суто деструктивний характер. Атака призвела до збитків понад 10 млрд доларів у світовому масштабі та уразила організації у десятках країнах світу [55]. Іншим прикладом є атака SolarWinds, під час якої складна компрометація ланцюга постачання дозволила зловмисникам непомітно отримати доступ до систем урядових установ та великих компаній США та ЄС.

Україна сьогодні є унікальним майданчиком дослідження проблем кібератрибуції. Національні структури (CERT-UA, СБУ) у щоденному режимі стикаються із атаками підконтрольних ГРУ та ФСБ хакерських угруповань, які маскуються під діяльність хакерів-активістів. Під час атаки на українську енергетику шкідливе ПЗ класу wiper часто запускалося одночасно з масованими ракетними ударами. Саме ця кінетично-цифрова синхронізація, поряд із глибоким аналізом коду партнерами Microsoft та Cisco, дозволила здійснити

точну політичну та юридичну атрибуцію всупереч інфраструктурі маскування ворога.

Основні проблеми кібератрибуції систематизовано в таблиці 3.2.

Таблиця 3.2.

Основні міжнародні проблеми забезпечення кібератрибуції

Проблема	Характеристика	Наслідки
Анонімність	Використання VPN, TOR, проксі-серверів	Ускладнення встановлення реального першоджерела атаки
Ботнети	Використання мереж заражених пристроїв IoT	Приховування реального географічного місцезнаходження
Правові відмінності	Різне кримінальне законодавство держав, вимоги GDPR	Складність та затягування транскордонного розслідування
Політичні фактори	Міждержавні суперечності, надання «притулку» хакерам	Блокування та уповільнення офіційного обміну інформацією
Технічна складність	Велика кількість та модифікація цифрових доказів	Суттєве збільшення часу проведення атрибуції APT

Таким чином, процес кібератрибуції є одним із найскладніших елементів міжнародної протидії кіберзлочинності. Незважаючи на розвиток засобів цифровою криміналістики, механізмів міжнародного співробітництва та систем кіберрозвідки , анонімність кіберпростору, правові розбіжності між державами та політичні фактори суттєво ускладнюють встановлення реальних злочинців.

3.3 Перспективи і рекомендації щодо подолання кіберзлочинності на міжнародному рівні

Стрімкий розвиток цифрових технологій, глобалізація інформаційного простору та активне впровадження штучного інтелекту формують новий етап

еволюції кіберзлочинності. Нині міжнародна спільнота стикається не лише зі зростанням кількості кібератак, але й зі значним ускладненням їхньої структури, автоматизацію процесів злочинної діяльності та використанням кіберпростору як інструменту геополітичного впливу. Сучасні кіберзагрози вже не обмежуються фінансовими злочинами або окремими інцидентами витоку даних. Значна частина масштабних атак спрямована на об'єкти критичної інфраструктури держав, енергетичний сектор, банківську систему, транспортні мережі та державні інформаційні ресурси. У зв'язку із цим проблема кіберзлочинності набуває глобального характеру та потребує комплексної міжнародної відповіді.

Важливою тенденцією останніх років стало використання штучного інтелекту не лише для захисту інформаційних систем, але й для автоматизації кібератак. Сучасні системи генеративного ШІ дозволяють кіберзлочинцям створювати високо реалістичні фішингові повідомлення, автоматизувати підбір автентифікаційних даних, здійснювати миттєвий аналіз вразливостей нульового дня та динамічно генерувати поліморфний шкідливий програмний код. За оцінками міжнародних аналітичних центрів [4], у 2025-2026 роках понад 80% фішингових компаній уже частково або повністю використовували інструменти ШІ для обходу традиційних засобів захисту.

У таких умовах ключовим завданням стає формування глобальної системи колективної кібербезпеки, яка базується на міжнародному співробітництві, уніфікації правових форм та інтеграції сучасних технологій проактивного захисту. На основі проведеного дослідження сформовано комплексні рекомендації за п'ятьма стратегічними напрямками:

Розширення міжнародного обміну кіберрозвідувальними даними. Одним із найефективніших механізмів сучасної протидії кіберзагрозам є оперативний обмін інформацією про інциденти, індикатори компрометації, шкідливі домени, IP-адреси серверів керування та нові методі атак між державними та міжнародними організаціями. Сьогодні значного поширення набувають автоматизовані платформи обміну розвідувальними даними: відкриті системи

типу MISP, стандартизовані протоколи взаємодії STIX/TAXII, інтегровані транскордонні рішення класів XDR та SOAR, а також мережі взаємодії команд CERT/CSIRT під егідою FIRST. Загальну концепцію цієї взаємодії представлено на рисунку 3.3.

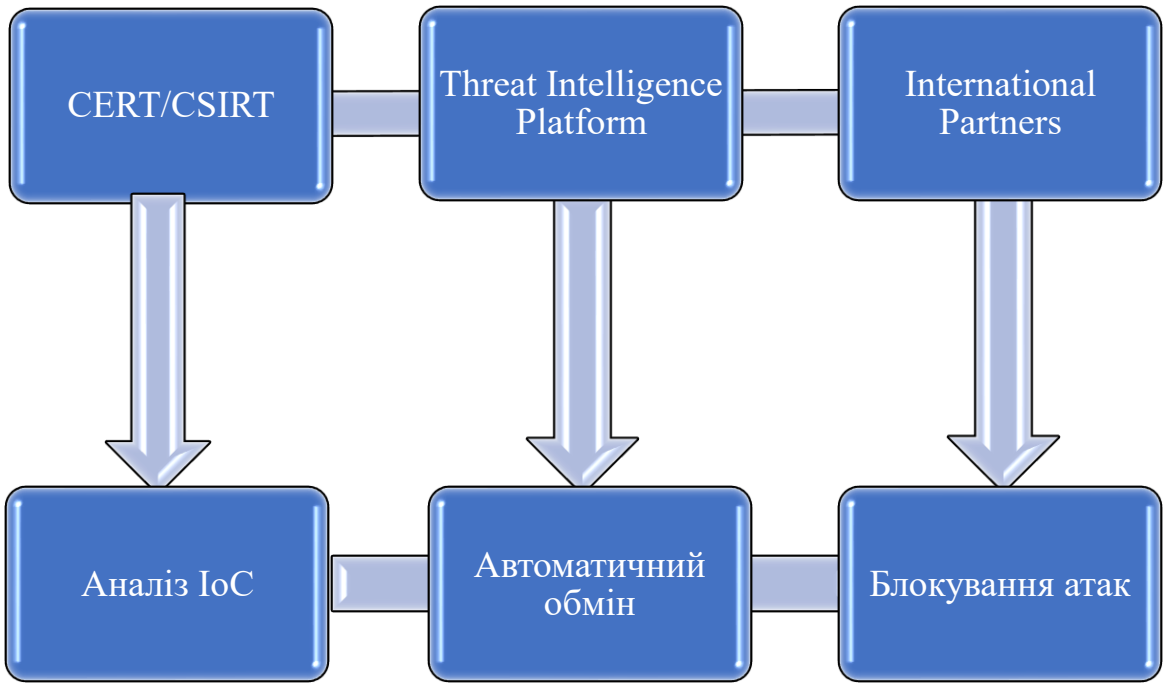

Рис. 3.3. Модель міжнародного обміну даними кіберрозвідки

Практичні рекомендації щодо реалізації напряму:

- Створення Глобального реєстру індикаторів компрометації IoC. Рекомендується під егідою Міжнародного союзу електрозв'язку або форуму FIRST розгорнути єдину децентралізовану хмарну платформу даних розвідки загроз для миттєвого міждержавного обміну технічними даними про атаки.

- Автоматизація обміну «без людського фактору». Державним CERT та приватним провайдерам критичних послуг рекомендовано повністю перейти на API-інтеграцію протоколів STIX2.1/TAXII, що дозволить блокувати шкідливу інфраструктуру по всьому світу за мілісекунди після першого виявлення.

Уніфікація міжнародного законодавства в галузі кібербезпеки. Правова фрагментація та різниця у національному законодавстві держав суттєво ускладнює проведення міжнародних розслідувань, транскордонний обмін цифровими доказами, екстрадицію кіберзлочинців і реалізацію спільних правоохоронних операцій під егідою Інтерполу чи Європолу. Важливим кроком

є саме вдосконалення вже існуючих механізмів Будапештської конвенції та адаптація засад нової Універсальної конвенції ООН про кіберзлочинність.

Практичні рекомендації щодо реалізації напряму:

- Впровадження спрощеного правового режиму для транскордонного збору доказів. Рекомендується розробити та підписати Додатковий протокол Будапештської конвенції, який дозволить відповідним структурам у реальному часі за згодою провайдера отримувати доступ до технічних логів серверів анонімізації в обхід тривалих бюрократичних процедур міжнародної правової допомоги.

- Юридична стандартизація «цифрової криміналістики». Необхідно уніфікувати на міжнародному рівні правила збору, фіксації та верифікації електронних доказів (відповідно до стандартів ISO/IEC27037) для забезпечення їхньої беззаперечної легітимності в судах будь-якої юрисдикції.

Використання ШІ й автоматизація систем захисту. Через стрімке зростання кількості кіберзагроз традиційні методи вже не забезпечують необхідної швидкості аналізу трафіку. У зв’язку із цим міжнародна спільнота активно впроваджує системи автоматизованого захисту на основі ШІ та концепції нульової довіри. Сучасні системи кібербезпеки дозволяють автоматично аналізувати гігабайти мережевого трафіку в реальному часі; виявляти аномальну поведінку користувачів та процесів в середині периметра; прогнозувати потенційні вектори атак на основі ретроспективного аналізу; автоматизувати розгортання сценаріїв реагування без участі людини; блокувати шкідливу активність у режимі реального часу.

Практичні рекомендації щодо реалізації напряму:

- Впровадження когнітивних SOAR систем на основі ШІ. Рекомендується зобов’язати операторів критичних інформаційних систем інтегрувати рішення з автоматизованого пошуку загроз, які здатні самостійно ізолювати компрометовані сегменти мережі без очікування дій з боку SOC.

- Масштабування стандарту Zero Trust. Рекомендується розширити впровадження стандарту NIST SP 800-207 [56] з корпоративного рівня на рівень

міждержавної інформаційної взаємодії (між урядовими базами даних і транскордонними фінансовими шлюзами). Принцип «ніколи не довіряй, завжди перевіряй» має діяти на всіх рівнях доступу.

Результати аналізу сучасних технологій у протидії кібератакам і рекомендації щодо їх застосування наведено в таблиці 3.3.

Таблиця 3.3.

Перспективні технології та практичні рекомендації з їх впровадження

Технологія	Основне призначення	Очікуваний ефект на міжнародному рівні	Рекомендований захід для впровадження
Штучний інтелект	Автоматичне виявлення загроз та аномалій	Скорочення часу виявлення атак на 40-50%	Інтеграція ML-моделей аналізу поведінки користувачів (UEBA) в урядові SOC
SOAR	Автоматизація та оркестрація реагування	Мінімізація людського фактору, миттєве виконання захисних сценаріїв	Створення уніфікованих плейбуків для типових інцидентів
XDR	Централізований наскрізний моніторинг	Виявлення прихованих APT – атак на рівні різних середовищ	Обов’язкове розгортання агентів XDR на кінцевих точках критичної інфрастр-ри
Zero Trust	Жорсткий безперервний контроль доступу	Радикальне зменшення ризику компрометації внутрішніх мереж	Впровадження MFA та мікросегментації мереж
Threat Intelligence Platform	Автоматизований обмін даними кіберрозвідки	Чітка координація та синхронізація міжнародного захисту	Під’єднання вітчизняних CERT до глобальних децентралізованих хабів обміну IoC

Ці технології та заходи формують основу сучасної міжнародної системи кіберзахисту та визначають перспективні напрями розвитку глобальної кібербезпеки.

Посилення захисту критичної інфраструктури. Об’єкти енергетики, фінансового сектору, транспорту та державного управління дедалі частіше стають мішенню кібератак державного рівня та транснаціональних програм-вимагачів. На міжнародному рівні орієнтиром є нормативи ЄС, такі як Директива NIS2, регламент DORA та Закон України «Про основні засади забезпечення кібербезпеки» [57].

Практичні рекомендації щодо реалізації напряму:

- Гармонізація українського законодавства з NIS2 та DORA. Необхідно посилити персональну юридичну та фінансову відповідальність топ-менеджменту підприємств за недотримання базових вимог кібергігієни, шляхом внесення змін до Закону України «Про основні засади забезпечення кібербезпеки України».
- Впровадження обов’язкового аудиту ланцюгів постачання. Організаціям критичної інфраструктури необхідно заборонити використання ПЗ та обладнання, що не мають сертифікатів відповідності Акту про кіберстійкість ЄС, щоб унеможливити ризики закладок від APT-угруповань.

Підготовка фахівців та розвиток міжнародних кібернавчань. Кадровий дефіцит, який у 2025-2026 роках перевищив 4 млн осіб у світі [11], створює системні вразливості у захисті державного та приватного секторів. Цю проблему неможливо вирішити локально потрібні скоординовані міжнародні кроки.

Практичні рекомендації щодо реалізації напряму:

- Створення кіберполігонів та регулярні навчання. Розширення участі України у міжнародних кібернавчаннях типу Cyber Europe (під егідою ENISA) та Shields (під егідою Об'єднаного центру передових технологій з кібероборони НАТО) для відпрацювання взаємодії між державними та приватними командами реагування.

- Інституціоналізація унікального досвіду України. Створення під егідою РНБО України та Міністерства цифрової трансформації України «Міжнародного центру дослідження гібридних кіберзагроз». Це дозволить експортувати унікальний досвід України у відбитті кібератак у режимі реального часу, залучаючи іноземні інвестиції та гранти для розвитку вітчизняної системи освіти з кібербезпеки.

Виходячи із вище зазначеного, перспективи міжнародної протидії кіберзлочинності безпосередньо пов'язані із переходом від пасивного захисту до проактивних колективних дій. Жодна держава сьогодні не здатна самостійно протидіяти глобальним загрозам. Реалізація запропонованих рекомендацій – від автоматизації обміну даними до правової уніфікації та створення спільних центрів аналізу загроз – дозволить світовій спільноті випередити злочинні угруповання та забезпечити надійну і довготривалу кіберстійкість.

Висновки до розділу 3

Аналіз міжнародних аспектів протидії кіберзлочинності, проведений у розділі 3, дозволяє зробити висновки, що сучасний кіберпростір остаточно набув глобального і транскордонного характеру, а кіберзагрози перетворилися на один із основних факторів дестабілізації державної, економічної та інформаційної безпеки. Сучасна кіберзлочинність уже не обмежується окремими фінансовими махінаціями або локальними атаками на корпоративні мережі. Переважна кількість кібератак мають системний характер, націлені на критичну інфраструктуру, державні інформаційні ресурси, енергетичний сектор, фінансові установи й об'єкти військового управління. Це свідчить про поступову трансформацію кіберпростору на окремий домен геополітичного протистояння.

У рамках дослідження встановлено, що ключовим елементом міжнародної системи протидії кіберзлочинності є мережа команд CERT/CSIRT, які забезпечують своєчасний обмін розвідувальними даними, координацію дій під час ліквідації інцидентів і взаємодію між державними, галузевими і бізнес-

структурами. Саме міжнародна інтеграція національних команд CERT у глобальні мережі груп кіберреагування дозволяє забезпечувати швидке виявлення атак, мінімізувати наслідки компрометації та формувати колективну кіберстійкість держав. Водночас, ефективність такої взаємодії безпосередньо залежить від рівня автоматизації обміну даними, стандартизації процедур реагування та готовності держав до відкритої технічної кооперації.

Окрему увагу приділено проблемам забезпечення кібератрибуції. Встановлено, що процес визначення реального джерела кібератаки є одним із найскладніших елементів міжнародного переслідування кіберзлочинців через анонімність мережі Інтернет, використання VPN, TOR, ботнетів і багаторівневої інфраструктури приховування слідів. Ситуація додатково ускладнюється застосуванням операцій під «хибним прапором». Внаслідок цього технічна атрибуція не завжди може бути достатньою підставою для політичних або юридичних рішень.

На основі проведеного аналізу визначено, що перспективи ефективної протидії кіберзлочинності безпосередньо пов’язані з розвитком міжнародної співпраці, автоматизацією обміну розвідувальними даними, впровадженням систем ШІ, технологій SOAR, XDR і архітектури Zero Trust. Важливими напрямами залишаються уніфікація міжнародного законодавства, посилення захисту критичної інфраструктури і проведення інтернаціональних кібернавчань.

Особливе місце у сучасній міжнародній системі кібербезпеки займає Україна, яка в умовах постійних кібератак отримала унікальний практичний досвід захисту критичної інфраструктури та взаємодії з міжнародними партнерами. Досвід CER-UA та українських фахівців сьогодні є важливим джерелом практичних рішень для світової кібербезпеки.

Таким чином, ефективна протидія кіберзлочинності можлива лише за умови комплексної міжнародної взаємодії, технологічної інтеграції та розвитку колективної кіберстійкості держав. Лише поєднання правових, технічних та організаційних механізмів дозволить забезпечити стабільність глобального цифрового простору та мінімізувати наслідки сучасних кіберзагроз.

ВИСНОВКИ

Досліджено теоретико-методологічні основи кіберзлочинності та визначено її сутність як транснаціонального, динамічного та високотехнологічного явища. Встановлено, що сучасна класифікація кіберзлочинів базується на синергії функціонального та технічного підходів, що дозволяє чітко розмежовувати інциденти, де комп'ютерні системи є безпосередньо ціллю атаки (хакінг, DDoS, шкідливе ПЗ), і злочини де ІКТ є лише інструментом реалізації протиправної діяльності.

Проаналізовано глобальні статистичні показники та ключові тенденції розвитку кіберпростору станом на 2025-2026 роки. Виявлено критичне масштабування ландшафту загроз: сумарні збитки світової економіки перевищили 10 трлн доларів, а понад 84% організацій у світі зазнали щонайменше однієї атаки за останній рік. Провідними векторами кримінальної монетизації залишаються програми-вимагачі(ransomware), на які припадає понад 70% світових інцидентів, масові компанії фішингу та експлуатації вразливостей периферійних пристроїв і VPN-шлюзів.

Обґрунтовано визначальний вплив технологій ШІ на еволюцію сучасних кіберзагроз. Встановлено, що активне використання зловмисниками генеративного ШІ (генерація автоматизованого поліморфного коду, проведення ШІ-фішингових атак) призвело до скорочення середнього часу між інцидентами і нівелювання ефективності традиційних, статичних систем сигнатурного захисту.

Визначено ключову роль міжнародних мереж CERT/CSIRT у системі колективної протидії кіберзлочинності. Досліджено рівні транскордонної взаємодії (FIRST, ENISA) та доведено, що інтеграція національних команд у глобальні хаби дозволяє локалізувати загрози на ранніх стадіях завдяки автоматизованому обміну індикаторами компрометації через платформу типу MISP.

Систематизовано проблеми забезпечення кібератрибуції на міжнародному рівні. Встановлено, що використання зловмисниками багаторівневої інфраструктури (TOR, VPN у «сірих юрисдикціях») та операцій під «хибним прапором» збільшує час розслідування APT-атак ДО 250-300 днів, а обмеження регламенту GDPR та політичні суперечності блокують транскордонне переслідування хакерів.

Визначено унікальний статус України як головного постачальника аналітичних даних у сфері протидії гібридним загрозам. Досвід синергії CERT-UA та СБУ з партнерами довів, що синхронізація воєнних дій із цифровими ударами ворога дозволяє проводити точну кібератрибуцію.

Доведено, що успішна стратегія кіберстійкості організацій в умовах атак ransomware полягає у категоричній відмові від виплати викупу, побудові ізольованого резервного копіювання та готовності до автономного функціонування у кризовому режимі.

Обґрунтовано необхідність переходу до проактивного захисту на основі концепції нульової довіри. Впровадження інтелектуальних систем класів XDR та SOAR дозволяє автоматизувати аналіз трафіку, мінімізувати людський фактор і скоротити час блокування загрози на 40-50%.

Сформовано комплексні рекомендації щодо гармонізації законодавства України з Директивою ЄС, автоматизації обміну даними через протокол STIX/NAXII та створення Міжнародного дослідження гібридних кіберзагроз під егідою РНБО України.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Official Cybercrime Report 2016: Damage Cost Estimations. *Cybersecurity Ventures*. 2016. URL: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

2. Official Cybercrime Report 2025: Global Threat Landscape and Economic Impact. *Cybersecurity Ventures*. 2025. URL: https://cybersecurityventures.com/official-cybercrime-report-2025/

3. Top 50 Cybersecurity Statistics for 2025: Threats, Trends and Challenges. *BlueFire RedTeam & DeepStrike Analytics*. 2025. URL: https://bluefire-redteam.com/top-50-cybersecurity-statistics-for-2025/

4. Phishing Statistics 2025: The Alarming Rise in AI-Powered Attacks. *ZenSec Research*. 2025. URL: https://zensec.co.uk/blog/2025-phishing-statistics-the-alarming-rise-in-attacks/

5. Cybercrime: Our Response to Global Threats. *INTERPOL International Police Cooperation Directorate*. 2024. URL: https://www.interpol.int/Crimes/Cybercrime/Cybercrime-our-response

6. European Cybercrime Centre (EC3) Operational Reports. *Europol Portal*. 2025. URL: https://www.europol.europa.eu/

7. Cyber Threat Landscape and Security Certification Reports. *European Union Agency for Cybersecurity (ENISA)*. 2025. URL: https://www.enisa.europa.eu/

8. Cost of a Data Breach Report. *IBM Security Research*. 2024. URL: https://www.ibm.com/reports/data-breach

9. Data Breach Investigations Report (DBIR). *Verizon Business Resources*. 2024. URL: https://www.verizon.com/business/resources/reports/dbir/

10. Digital Threat Intelligence and Security Insights. *Microsoft Security Blog*. 2025. URL: https://www.microsoft.com/security/blog/

11. Global Threat Report: The Evolution of Adversaries. *CrowdStrike Intelligence*. 2025. URL: https://www.crowdstrike.com/global-threat-report/

12. Resource Center: Cyber Threats, Malware Analysis and Vulnerabilities. *Kaspersky Lab*. 2024. URL: https://www.kaspersky.com/resource-center/threats

13. Global Cyber Attack Trends and Malware Research. *Check Point Research (CPR)*. 2025. URL: https://research.checkpoint.com/

14. The State of Ransomware: Tactical and Financial Impacts. *Sophos Technical Papers*. 2024. URL: https://www.sophos.com/en-us/medialibrary/pdfs/technical-papers/sophos-state-of-ransomware

15. Unit 42 Cyber Threat Intelligence Insights. *Palo Alto Networks Research*. 2025. URL: https://unit42.paloaltonetworks.com/

16. Mandiant M-Trends: Cyber Security Reports and Case Studies. *Google Cloud Mandiant Resources*. 2024. URL: https://www.mandiant.com/resources/reports

17. The Stages of a Cyber Attack: Anatomy of Modern Breaches. *EBuilder Security Articles*. 2023. URL: https://ebuildersecurity.com/articles/the-stages-of-a-cyber-attack/

18. Threat Detection and Response: What is a Cyber Kill Chain? *Fidelis Security 101*. 2024. URL: https://fidelissecurity.com/cybersecurity-101/threat-detection-response/what-is-a-cyber-kill-chain/

19. Advanced Analysis of Attack Lifecycles. *EBuilder Security Technical Insights*. 2024. URL: https://ebuildersecurity.com/articles/the-stages-of-a-cyber-attack/

20. Understanding Cyber Kill Chain Frameworks for Enterprise Defense. *Fidelis Security Threat Research*. 2025. URL: https://fidelissecurity.com/cybersecurity-101/threat-detection-response/what-is-a-cyber-kill-chain/

21. B. Jeffries; S. Saravia; C. Carter; Z. Ankuda. Cyber Risk to Mission Case Study: Norsk Hydro – DTIC. *The MITRE Corporation*. 2022. URL: https://apps.dtic.mil/sti/trecms/pdf/AD1183007.pdf

22. Budapest Convention on Cybercrime. *Council of Europe Legislation*. 2001. URL: https://www.coe.int/en/web/cybercrime/the-budapest-convention

23. UNODC Global Programme on Cybercrime Technical Materials. United Nations Office on Drugs and Crime. 2025. URL: https://www.unodc.org/unodc/en/cybercrime/global-programme-on-cybercrime.html

24. United Nations Draft Convention against Cybercrime. UNODC Ad Hoc Committee Report. 2024. PP. 1–45. URL: https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home

25. Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation - GDPR). Official Journal of the European Union. 2016. L 119. PP. 1–88. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj

26. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance). URL: https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng

27. Directive (EU) 2022/2555 of the European Parliament and of the Council (NIS 2 Directive). Official Journal of the European Union. 2022. L 333. PP. 80–152. URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj

28. Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA). Official Journal of the European Union. 2022. L 333. PP. 1–79. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R2554

29. Regulation (EU) 2024/1689 of the European Parliament and of the Council (EU AI Act). Official Journal of the European Union. 2024. L 1689. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689

30. Proposal for a Cyber Resilience Act (CRA). European Commission Legislation. 2024. URL: https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

31. ISO/IEC 27001 Information Security Management Systems Standard Overview. International Organization for Standardization. 2022. URL: https://www.iso.org/standard/27001

32. NIST Special Publication 800-207: Zero Trust Architecture. National Institute of Standards and Technology. 2020. PP. 1–50. DOI: 10.6028/NIST.SP.800-207 URL: https://csrc.nist.gov/publications/detail/sp/800-207/final

33. The Cyber Diplomacy Toolbox. URL: https://www.cyber-diplomacy-toolbox.com/

34. Аналітичний звіт про кіберзагрози для критичної інформаційної інфраструктури України. Державна служба спеціального зв'язку та захисту інформації України (Держспецзв'язку). 2025. URL: https://cip.gov.ua/ua/statics/analitichni-materiali-derzhspeczv-yazku

35. Global Cybersecurity Index (GCI) Report. International Telecommunication Union (ITU). 2024. PP. 1–85. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

36. Interpol Innovation Centre. Towards agile and trusted policing. *Interpol*. URL: https://www.interpol.int/How-we-work/Innovation/INTERPOL-Innovation-Centre

37. Joint Cybercrime Action Taskforce (J-CAT). Fighting cybercrime worldwide. *Europol.* URL: https://www.europol.europa.eu/how-we-work/services-support/operational-coordination-support/joint-cybercrime-action-taskforce

38. Internet Organised Crime Threat Assessment (IOCTA). *Europol Cybercrime Centre (EC3).* 2025. URL: https://www.europol.europa.eu/publications-events/main-reports/iocta

39. ENISA. Our vision: A Trusted and Cyber Secure Europe. *ENISA*. URL: https://www.enisa.europa.eu/about-enisa/what-we-do

40. Driving Change, Building Resilience: ENISA's revised Strategy and Structure March 27, 2025. *ENISA*. URL: https://www.enisa.europa.eu/news/driving-change-building-resilience-enisas-revised-strategy-and-structure

41. M. Raza. Intrusion Detection Systems (IDS): Definition, Types, Purpose September 03, 2024 Splunk. URL: https://www.splunk.com/en_us/blog/learn/ids-intrusion-detection-systems.html

42. What is XDR (Extended Detection and Response)? August 20, 2025. *SentinelOne*. URL: https://www.sentinelone.com/cybersecurity-101/xdr/what-is-extended-detection-response-xdr/

43. Security Information and Event Management (SIEM) Technology Assessment. Gartner IT Glossary. 2025. URL: https://www.gartner.com/en/information-technology/glossary/siem

44. Security Orchestration, Automation, and Response (SOAR) Architecture Guide. Palo Alto Networks Cyberpedia. 2025. URL: https://www.paloaltonetworks.com/cyberpedia/what-is-soar

45. Cisco Cybersecurity Readiness Index: Resilience in the Age of AI. Cisco Systems Report. 2026. URL: https://www.cisco.com/c/en/us/products/security/cybersecurity-readiness-index.html

46. What Is a Security Operations Center (SOC)? *SearchInform*. URL: https://searchinform.com/articles/cybersecurity/measures/security-operations-center-soc/

47. K. Poireault. Cybersecurity Structures 101: What Are CERTs and CSIRTs. 21 Nov 2025. *Infosecurity Europe*. URL: https://www.infosecurityeurope.com/en-gb/blog/guides-checklists/cybersecurity-structures-101-cert-csirt.html

48. Платформа MISP, що це, як підключатися та які переваги. Роз'яснення CERT-UA. *Державна служба спеціального зв'язку та захисту інформації України*. URL: https://cip.gov.ua/ua/faqs/roz-yasnennya-cert-ua-platforma-misp-sho-ce-yak-pidklyuchatisya-ta-yaki-perevagi

49. ISO/IEC 27035-1:2023Information technology — Information security incident managementPart 1: Principles and process. *ISO*. URL: https://pecb.com/en/education-and-certification-for-individuals/iso-iec-27035

50. A. Nelson, S. Rekhi, M. Souppaya, K. Scarfone. NIST SP 800-61r3. Incident Response Recommendations and Considerations for Cybersecurity Risk Management. A CSF 2.0 Community Profile. *NIST*. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf

51. CERT-UA. Computer Emergency Response Team of Ukraine. URL: https://cert.gov.ua/

52. A. Kaushik. Attribution in Cyberspace : Beyond the “Whodunnit”. *Globsec*. URL: https://www.globsec.org/what-we-do/publications/attribution-cyberspace-beyond-whodunnit

53. N. Prasad, A. Diro, M. Warren, M. Fernando. A survey of cyber threat attribution: Challenges, techniques, and future directions. *Computers & Security*. 2025. Volume 157. URL: https://www.sciencedirect.com/science/article/pii/S0167404825002950

54. L. Danielson. What is a False Flag Attack in cybersecurity? *Huntress*. URL: https://www.huntress.com/cybersecurity-101/topic/what-is-false-flag-in-cybersecurity

55. NotPetya. Cyber Operations Home. *Council on Foreign Relations*. URL: https://www.cfr.org/cyber-operations/notpetya

56. NIST Special Publication 800-207. Zero Trust Architecture. August 2020. *NIST*. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207-draft2.pdf

57. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. Відомості Верховної Ради України. 2017. № 45. С. 403. (зі змінами 2024-2025 рр.). URL: https://zakon.rada.gov.ua/laws/show/2163-19