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: “МЕТОДИ ПРОТИДІЇ КІБЕРАТАКАМ, ЯКІ СПОНСОРУЮТЬСЯ ДЕРЖАВАМИ”

на здобуття освітнього ступеня магістра
зі спеціальності 125 Кібербезпека та захист інформації
освітньо-професійної програми Управління інформаційною та кібернетичною безпекою

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

_____ Максим КОВРИГА

(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: Здобувач вищої освіти гр. УБДМ-61

Керівник: Тетяна МУЖАНОВА, к.держ.упр., доцент

Рецензент:

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут кібербезпеки та захисту інформації

Кафедра Управління кібербезпекою та захистом інформації
Ступінь вищої освіти магістр
Спеціальність 125 Кібербезпека та захист інформації
Освітньо-професійна програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри УКБЗІ
_____ Світлана ЛЕГОМІНОВА
"____" _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Студенту Ковризі Максиму Віталійовичу
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: "Методи протидії кібератакам, які спонсоруються державами"

керівник кваліфікаційної роботи Тетяна МУЖАНОВА, к.держ.упр., доцент
(Ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від "30" жовтня 2025 р. №467.

2. Строк подання кваліфікаційної роботи "___" грудня 2025 р.
3. Вихідні дані до кваліфікаційної роботи:.
4. Перелік питань, які потрібно розробити:
   1. Дослідити теоретичні аспекти кібероперацій, спонсорованих державами.
   2. Встановити основні риси і тенденції зловмисної діяльності держав у кіберпросторі.
   3. Проаналізувати напрями і методи протидії кібератакам за підтримки держав, запропонувати практичні рекомендації..
5. Перелік ілюстративного матеріалу: *презентація*
6. Дата видачі завдання "02" жовтня 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назви етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	10.10.2025	
2.	Збір та аналіз літератури.	23.10.2025	
3.	Дослідження теоретичних аспектів кібероперацій, спонсорованих державами.	27.10.2025	
4.	Визначення основних рис і тенденцій зловмисної діяльності держав у кіберпросторі	10.11.2025	
5.	Аналіз напрямів і методів протидії кібератакам за підтримки держав	15.11.2025	
6.	Формулювання висновків за результатами дослідження.	22.11.2025	
7.	Оформлення роботи.	04.12.2025	
8.	Оформлення презентації.	14.12.2025	
9.	Отримання рецензії на роботу.	18.12.2025	
10.	Захист в ЕК.	__.01.2026	

Здобувач вищої освіти _____ Максим КОВРИГА
(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 магістра

Направляється здобувач Коврига М.В. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека та захист інформації
(код, найменування спеціальності)
Освітньо-професійної програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: “Методи протидії кібератакам, які спонсоруються державами”
Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

Здобувач **КОВРИГА Максим** у кваліфікаційній роботі дослідив теоретичні аспекти кібероперацій, спонсорованих державами, визначив основні риси і тенденції зловмисної діяльності держав у кіберпросторі, проаналізував напрями та методи протидії кібератакам за підтримки держав і запропонував практичні рекомендації.

КОВРИГА Максим показав достатню теоретичну і практичну підготовку, оформив кваліфікаційну роботу відповідно до вимог. Виклад матеріалу здійснено згідно з планом, зроблено відповідні висновки. Ключові положення роботи представлено у вигляді зображень. Результати дослідження апробовані на конференції “Актуальні проблеми кібербезпеки” 29 жовтня 2025 року.

Все це дозволяє оцінити кваліфікаційну роботу здобувача **КОВРИГИ Максима** на оцінку “добре” та присвоїти йому кваліфікацію “Магістр з кібербезпеки та захисту інформації за освітньо-професійною програмою Управління інформаційною та кібернетичною безпекою”.

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

“____“_____2025 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Коврига М.В. 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 магістерську роботу

здобувача вищої освіти Ковриги Максима Віталійовича
на тему “Методи протидії кібератакам, які спонсоруються державами”

Актуальність. Як свідчать реалії, сучасне протиборство між державами поступово переходить з фізичного полю бою у цифровий простір. Кібератаки національних держав постійно зростають за кількістю, складністю, а також агресивністю впливу. Цілями таких кібератак стають не тільки урядові системи і установи, але і критична інфраструктура, бізнес і громадянське суспільство. Ускладнюють ситуацію такі чинники як прихованість підготовки і реалізації кібернападів, слабкі можливості виявлення і притягнення агресорів до відповідальності тощо. У таких умовах міжнародна спільнота, держави, бізнес стикаються з нагальною потребою об’єднання зусиль і формування стратегій запобігання і протидії кібератакам з боку агресивних національних держав.

З огляду на зазначене дослідження методів протидії кібератакам, які спонсоруються державами, є актуальним науковим завданням.

Позитивні сторони

1. У роботі досліджено види, тактики і методи кібератак, організованих державами, встановлено їх основні мотиви, детально проаналізовано статистику кібернападів у розрізі найбільш активних держав і окреслено актуальні тенденції у цій сфері. Проаналізовано методи протидії кіберзагрозам з боку держав, зокрема національні й міжнародні стратегії, технологічні й нормативно-правові заходи.

2. Кваліфікаційна робота оформлена відповідно до вимог. Виклад матеріалу здійснено відповідно до плану, зроблено логічні висновки. Ключові положення роботи представлено у вигляді рисунків. Автор опрацював значну джерельну базу: понад 60 публікацій та електронних джерел, в тому числі англомовних.

3. За результатами дослідження запропоновано рекомендації щодо методів протидії кіберзагрозам з боку держав у комплексному вимірі.

Недоліки

1. Доцільно було б приділити більше уваги вивченню і класифікації методів запобігання кібератакам, які спонсоруються державами, особливостям їх використання у вітчизняних реаліях.

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 Коврига Максим Віталійович заслуговує присвоєння кваліфікації “Магістр кібербезпеки за освітньо-професійною програмою “Управління інформаційною та кібернетичною безпекою”.

Рецензент:

_____
підпис

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 91 с.., 20 рис., 2 табл., 63 джерела.

Метою роботи є дослідження методів протидії кібератакам, які спонсоруються державами.

Об'єктом дослідження є злочинна діяльність держав у кіберпросторі.

Предмет дослідження – методи протидії кібератакам, які спонсоруються державами.

Методи дослідження. Для вирішення завдань дослідження використовувалися історичний, статистичний і прогностичний методи, методи аналізу та синтезу, порівняння, класифікації, моделювання, теорії інформаційного протиборства.

Короткий зміст роботи. Як результат у роботі досліджено теоретичні аспекти кібероперацій, спонсорованих державами, зокрема види, методи і тактики кібернападів; визначено основні риси і тенденції зловмисної діяльності держав у кіберпросторі; проаналізовано напрями та методи протидії кібератакам за підтримки держав, серед яких розробка національних стратегій, міжнародна співпраця, методи технологічного захисту, запропоновано практичні рекомендації.

Галузь застосування. Розроблені підходи можуть бути використані при плануванні та реалізації стратегій і заходів протидії кібератакам з боку держав на національному й корпоративному рівнях.

КЛЮЧОВІ СЛОВА : КІБЕРБЕЗПЕКА, ГЕОПОЛІТИЧНЕ ПРОТИБОРСТВО У КІБЕРПРОСТОРІ, КІБЕРАТАКИ, ЯКІ СПОНСОРУЮТЬСЯ ДЕРЖАВАМИ, МЕТОДИ ПРОТИДІЇ КІБЕРАТАКАМ З БОКУ ДЕРЖАВ.

ABSTRACT

The text part of the qualification paper for obtaining a master's degree: 89 pages, 12 figures, 2 tables, 63 sources.

The purpose of the work is to study the methods of countering state-sponsored cyberattacks.

Object of research is the criminal activity of national states in cyberspace.

Subjec*t *of research is methods of countering state-sponsored cyberattacks.

Research methods. For solving the research tasks, historical, statistical and prognostic methods, methods of analysis and synthesis, comparison, classification, modeling, theories of information warfare were used.

Summary of the paper. The author investigates the theoretical aspects of state-sponsored cyberoperations, in particular the types, methods and tactics of cyberattacks; identifies the main features and trends of malicious activity of states in cyberspace; analyzes the directions and methods of countering nation state cyberattacks, including the development of national strategies, international cooperation, methods of technological defense, and proposes relevant practical recommendations.

Field of research. The presented approaches can be used in planning and implementing strategies and measures to counter nation state cyberattacks at the national and corporate levels.

KEYWORDS: CYBERSECURITY, GEOPOLITICAL WARFARE IN CYBERSPACE, STATE-SPONSORED CYBERATTACKS, METHODS OF COUNTERING NATION STATE CYBERATTACKS.

ЗМІСТ

ВСТУП

Актуальність теми. Як свідчить статистика, у 2024 році 36% кібератак було організовано або здійснено державними суб'єктами, а їхня кількість, складність і наслідки деструктивного впливу постійно зростають. Незважаючи на те, що зловмисні кібероперації зазвичай є інструментами міждержавного протиборства, їх цілями стають не тільки системи національного значення і критична інфраструктура, але й бізнес і громадянське суспільство.

Держави-нападники часто співпрацюють з кіберзлочинними групами та ідеологічно налаштованими хакерами, використовують різноманітні засоби впливу, серед яких як технологічні (програми-вимагачі, ботнети), так і соціальні (дезінформація, соціальна інженерія). Водночас, зусилля окремих держав, бізнесу і міжнародної спільноти щодо виявлення і протидії кібернападам з боку зловмисних держав на сьогодні не є достатньо успішними і не дозволяють упевнено ідентифікувати агресорів і притягнути їх до відповідальності.

З огляду на зазначене дослідження методів протидії кібератакам, які спонсоруються державами, є актуальним науковим завданням.

Мета роботи полягає у дослідженні методів протидії кібератакам, які спонсоруються державами.

Об'єкт дослідження - злочинна діяльність держав у кіберпросторі.

Предмет дослідження – методи протидії кібератакам, які спонсоруються державами.

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

1. Дослідити теоретичні аспекти кібероперацій, спонсорованих державами.

2. Визначити основні риси і тенденції зловмисної діяльності держав у кіберпросторі.

3. Проаналізувати напрями та методи протидії кібератакам за підтримки держав і запропонувати практичні рекомендації.

Методи дослідження. Для вирішення завдань дослідження використовувалися історичний, статистичний і прогностичний методи, методи

аналізу та синтезу, порівняння, класифікації, моделювання, теорії інформаційного протиборства.

Наукова новизна одержаних результатів. У роботі досліджено специфіку сучасних кібератак, які організуються державами, а також статистику щодо їх кількості, видів і найбільш активних держав-агресорів, запропоновано рекомендації щодо протидії кібероперація м за підтримки держав на міжнародному, національному і корпоративному рівнях.

Практичне значення одержаних результатів. Застосування напрацювань дослідження буде доцільним для обґрунтованого вибору нормативно-правових, організаційних і програмно-технічних методів протидії кібератакам з боку держав на національному й корпоративному рівнях.

Апробація результатів кваліфікаційної роботи була здійснена на конференції “Актуальні проблеми кібербезпеки” 29 жовтня 2025 року.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ОСНОВИ КІБЕРОПЕРАЦІЙ, СПОНСОРОВАНИХ ДЕРЖАВАМИ

1.1 Кібероперації з ініціативи держав: історія виникнення та мета

Залежність підприємств, організацій і громадян від пристроїв та систем, підключених до Інтернету, зросла до такого рівня, який неможливо було передбачити навіть кілька десятків років тому. Аналогічно, системи національної безпеки, оборони, громадського порядку та інші критичні системи управління державою значною мірою залежать від стабільного та безпечного Інтернету, і, як наслідок, піддаються кібервтручанню й атакам.

Поряд із реалізацією багатьох міжнародних ініціатив із забезпечення безпечного і відкритого кіберпростору, немало держав вирішили відкрити нову зону конфлікту, нарощуючи темпи і масштаби кібератак, часто непередбачуваним чином. Доступність мережі для всіх гравців та відмінні цілі, для яких використовується Інтернет, є основною причиною, чому держави нерідко ставляться до наступальних кібероперацій інакше, ніж до традиційних наступальних операцій. Тим не менше, дії та реакції держав у кіберпросторі так само корелюють з метою операцій та їх наслідками [1].

Після повільного, понад 20-річного нарощування, військові кібероперації раптово стали гарячою темою у 2008 році. Неурядовий сектор почав реагувати на зростаючі кіберзагрози задовго до цього. Відправною точкою стало виявлення Міністерством оборони США (DoD), що його секретна комп'ютерна мережа була зламана і заражена шкідливим програмним забезпеченням.

Справа 2008 року, яку пізніше назвали «найсерйознішим порушенням секретних комп'ютерних систем американських військових», була результатом під'єднання зараженої флешки в ноутбук американських військових на базі на Близькому Сході. Потім шкідлива програма поширювалася через флеш-накопичувачі та інші знімні носії інформації, заразивши як несекретні, так і

засекречені системи. Зловмисне ПЗ, відоме як Agent.btz, проникало в системи, а потім сигналізувало або викликало встановлену інтернет-адресу, щоб повідомити про своє успішне проникнення. Коли в листопаді 2008 року з'явилися новини про атаку Agent.btz, його назвали «черв'яком, який з'їв Пентагон» і одночасно «поворотним моментом» і «важливим сигналом тривоги».

Як негайний наслідок усвідомлення того, що флеш-накопичувачі становлять значну вразливість, Міністерство оборони розпочало операцію «Buckshot Yankee» та заборонило знімні носії у своїх комп'ютерних системах. Крім цього, невдовзі відбулися значні організаційні зміни у структурі відомства: у 2010 році Міністерство оборони США об'єднало свої функції кібернаступу та оборони в єдине військове командування – Кіберкомандування США [2].

Слід відзначити, що після цього випадку багато інших держав усвідомили необхідність захисту від кібернападів. Водночас активізувалися дискусії з питань міжнародного права та дипломатії щодо кіберпростору: зріс інтерес до Групи урядових експертів ООН, яка займається питаннями кіберпростору; Центр передового досвіду НАТО з питань співпраці в кіберзахисті спільно із згаданою групою експертів з міжнародного права написали перший посібник з кіберправа (Талліннський посібник з міжнародного права, що застосовується до кібервійни); у новинах регулярно висвітлювалися питання агресивної діяльності в кіберпросторі.

У 2015 році група експертів ООН з питань кіберзахисту висунула перелік норм кіберповедінки, з якими погодилися держави-учасниці [3].

Так, перелік задекларував зобов’язання держав:

- підтримувати співпрацю у розвитку та застосуванні заходів для зростання стабільності і безпеки використання ІКТ та запобігання практикам їх деструктивного використання на шкоду міжнародному миру і безпеці;
- у разі інцидентів, пов'язаних з ІКТ, враховувати всю відповідну інформацію, включаючи ширший контекст події, проблеми атрибуції

(встановлення зловмисника) в середовищі ІКТ, а також характер і масштаби наслідків;

- співпрацювати для обміну інформацією, надавати взаємну допомогу, переслідувати за використання ІКТ у терористичних та злочинних цілях та впроваджувати інші заходи співпраці для боротьби з такими загрозами;
- повідомляти про вразливості ІКТ та обмінюватися відповідною інформацією про доступні засоби для їх усунення;
- здійснювати адекватні заходи для захисту своєї критичної інфраструктури від кібератак;
- сприяти просуванню, захисту й реалізації прав людини і громадянина в кіберпросторі, зокрема права на приватність у цифрову епоху, права на свободу вираження поглядів.

Водночас, у нормах зазначалося, що держави не повинні:

- свідомо дозволяти використовувати свою територію для «міжнародно протиправних» кіберактів;
- проводити або свідомо підтримувати кібердіяльність, яка навмисно пошкоджує критичну інфраструктуру;
- проводити або свідомо підтримувати діяльність, спрямовану на завдання шкоди групам реагування на надзвичайні ситуації інформаційних систем (CERT/CSIRTS);
- використовувати власні групи реагування на надзвичайні ситуації для зловмисної міжнародної діяльності.

Однак, у подальшому не вдалося досягти консенсусу між державами щодо застосовних норм, наслідком чого стало розширення кібероперацій у нові та креативні сфери, які особливо впливають на цивільне населення та часто проводяться поза контекстом збройного конфлікту. Таким чином, кібероперації і сьогодні знаходяться поза межами суворих обмежень, які міжнародне право накладає на діяльність держав під час збройних конфліктів.

З того часу масштаби і різноманіття кібероперацій, організованих або спонсорованих державами, зросли в рази.

Розглянемо детальніше основні характеристики кібератак за підтримки держав.

Кібератаки, що спонсоруються державами, виникають з різноманітних мотивів, що охоплюють шпигунство, саботаж, пропаганду, отримання економічної вигоди та стратегічної переваги. Зазвичай вони слугують ключовими компонентами ширших геополітичних стратегій держав, які прагнуть перехитрити суперників або досягти чітких національних цілей у стратегічному контексті. Ці мотиви лежать в основі складної мережі кібероперацій, кожна з яких розроблена для використання вразливостей та досягнення конкретних цілей. Незалежно від того, чи спрямовані вони на крадіжку конфіденційної інформації, порушення роботи критичної інфраструктури чи підрив можливостей супротивників, ці атаки є продуманими маневрами на світовій геополітичній арені. Більше того, багатогранний характер кіберагресії, що спонсорується державами, підкреслює накладання політичної, економічної та технологічної сфер, формуючи сучасний ландшафт міжнародних відносин.

Цікавою є концепція, представлена у праці [1], яка потенційною метою кібератак, ініційованих державами, у зростаючому порядку визначає:

1) розвідку і шпигунство;

2) маніпулювання даними і пошкодження віртуальних активів;

3) пошкодження матеріальних активів і фізичне знищення.

На рис. 1.1 показано приклади операцій, які були реалізовані для досягнення певної мети. Зокрема, з метою розвідки та шпигунства були реалізовані згадана вище операція Міністерства оборони США «Buckshot Yankee» (2010) у відповідь на успішну спробу несанкціонованого доступу до секретних урядових мереж і APT-атака на Управління персоналом Уряду США (2015), в результаті якої було скомпрометовано понад 22 млн записів державних службовців [4].

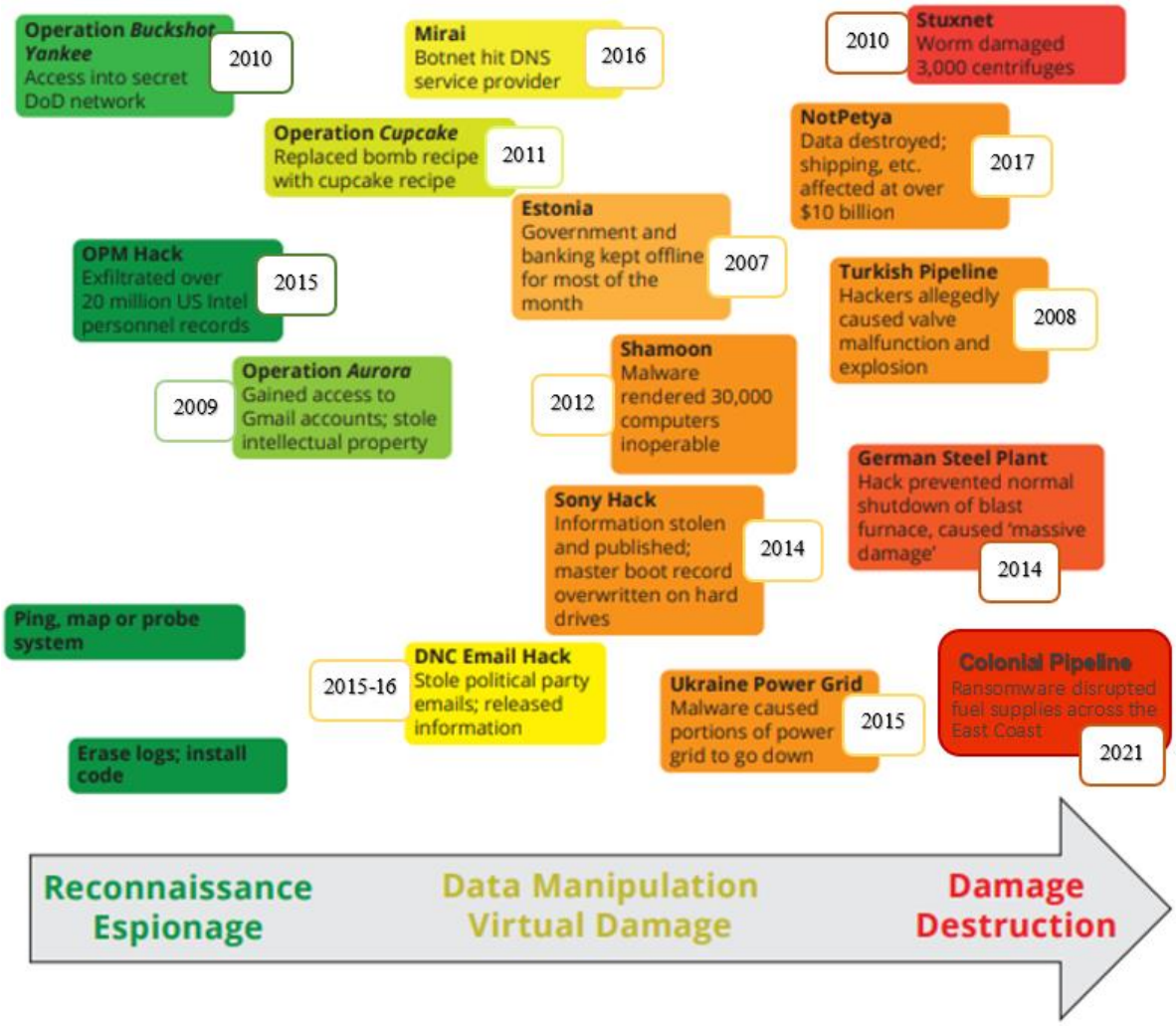

Рис. 1.1. Приклади кібератак, ініційованих державами з різною метою

Шкідливе програмне забезпечення Mirai інфікувало «розумні» пристрої, під'єднані до Інтернету, і створило з них мережу ботів, яка реалізувала, зокрема масштабну DDoS-атаку на постачальника послуг реєстрації доменів Dyn у 2016 році. [5]. Зразком атак з метою маніпулювання даними і пошкодження віртуальних активів є також атака у 2014 році на компанію Sony Pictures Entertainment, яка призвела не тільки до витоку неопублікованих фільмів і конфіденційних даних, але й висвітлив серйозні наслідки неадекватних заходів кібербезпеки [6].

Сумнозвісним є комп'ютерний черв'як Stuxnet, який став відомим завдяки своєму використанню для атаки на електромеханічне обладнання іранських ядерних об'єктів у 2010 році [7]. Масштабні наслідки мав також вірус NotPetya, який у 2017 році атакував щонайменше 2 тис. організацій, переважно

в Україні, і приніс серйозні наслідки для численних підприємств у всьому світі на суму понад 10 мільярдів доларів. Слід відзначити, що атака NotPetya приписується хакерській групі Sandworm у складі ГРУ РФ, а, отже, має геополітичне підґрунтя [8].

Наслідки кібератак, що спонсоруються державою

Кібератаки, що спонсоруються державою, мають глибокі наслідки, які відбиваються на багатьох сферах, від національної безпеки до глобальної економічної стабільності [9] (Рис. 1.2). Ці наслідки підкреслюють складний і багатогранний характер кіберпротиборства, формуючи сучасний ландшафт міжнародних відносин та кібербезпеки.

Рис. 1.2. Наслідки кібератак, що спонсоруються державами

Проблеми національної безпеки. Кібератаки, що спонсоруються державою, створюють значні загрози національній безпеці, оскільки вони спрямовані на критичну інфраструктуру, державні установи, системи безпеки й оборони. Проникнення в чутливі мережі може поставити під загрозу секретну інформацію, порушити роботу критичних послуг і підірвати цілісність оборонних потужностей, ставлячи під загрозу здатність держави захищатися від зовнішніх загроз.

Деструктивний вплив на економіку. Економічні наслідки кібератак, що спонсоруються державами, є далекосяжними, з потенційними наслідками, починаючи від фінансових втрат до ринкової нестабільності. Атаки, спрямовані на підприємства, фінансові установи й об’єкти інтелектуальної власності, можуть призвести до колосальних збитків, підірвати довіру споживачів і порушити глобальні ланцюги постачань, впливаючи на економіку як на місцевому, так і на міжнародному рівні.

Геополітична напруженість. Кібератаки, що спонсоруються державами, нерідко загострюють існуючу геополітичну напруженість і можуть спровокувати дипломатичні конфлікти між різними міжнародними суб’єктами, серед яких держави, міждержавні й міжнародні об’єднання, транснаціональні корпорації тощо. Кібершпигунські атаки, диверсійні операції та дезінформаційні кампанії можуть призвести до ескалації воєнних дій, напруження дипломатичних відносин та підриву довіри між урядами, що призведе до заходів у відповідь та подальшої дестабілізації в кіберпросторі.

Гонка озброєнь у кіберпросторі. Поширення кібератак за підтримки держав підживлює стрімку гонку озброєнь у кіберпросторі, оскільки останні прагнуть посилити свої наступальні й оборонні можливості. Така боротьба озброєнь характеризується розробкою та розгортанням передової кіберзброї, дослідженням нових векторів атак і мілітаризацією кіберпростору, що підвищує ризик ескалації та потенціал катастрофічних наслідків у майбутніх конфліктах.

Вплив на цивільне населення. Кібератаки, що проводяться державами або в їхніх інтересах, можуть мати прямий та опосередкований вплив на цивільне населення, починаючи від перебоїв у наданні життєво важливих послуг і закінчуючи порушеннями приватності особистого життя. Атаки, спрямовані на критично важливу інфраструктуру, таку як транспортні й електромережі, системи охорони здоров'я і реагування на надзвичайні ситуації, можуть поставити під загрозу суспільну безпеку і добробут населення, що вимагає надійних заходів кібербезпеки для їх захисту.

Порушення міжнародних норм і засад управління. Поширеність кібератак, що підтримуються державами, ставить під сумнів існуючі міжнародні норми та засади управління кіберпростором. Дебати навколо таких питань, як атрибуція, стримування та підзвітність, підкреслюють необхідність колективних дій і співпраці між державами для встановлення норм відповідальної поведінки в кіберпросторі та зменшення ризиків кіберконфліктів.

Загрози демократичним цінностям. Кібератаки, організовані в інтересах окремих держав, становлять загрозу для демократичних інститутів і процесів, підриваючи чесність виборів, поширюючи дезінформацію та сіючи недовіру до демократичних систем. Втручання у вибори, витоки даних та операції впливу, що проводяться ворожими суб'єктами, можуть підірвати суспільну довіру, демократичні норми й основи вільного та справедливого управління, створюючи серйозні виклики для демократичних суспільств у всьому світі.

Наслідки кібератак, що спонсоруються державами, є масштабними й багатогранними, охоплюючи національну безпеку, економічну стабільність, геополітичну динаміку, добробут цивільного населення, міжнародне управління та демократичну стійкість. Запобігання цим наслідкам вимагає узгоджених зусиль урядів, зацікавлених сторін приватного сектору, громадянського суспільства та міжнародної спільноти для підвищення кіберстійкості, зміцнення механізмів стримування та підтримки принципів миру, безпеки і стабільності в кіберпросторі.

1.2 Види кібероперацій, організованих державами

Як показало дослідження, види кібероперацій з ініціативи держав можна класифікувати за такими критеріями:

- природою нападу (отримання несанкціонованого доступу, шпигунство; порушення інформаційних процесів/функціонування кіберінфраструктури; пошкодження/виведення з ладу фізичної інфраструктури, людські жертви);

- метою деструктивного впливу - вплив на цивільне населення; загрози національній безпеці; пошкодження/руйнування критичної інфраструктури; вплив на процеси прийняття рішень [1] (Рис.1.3).

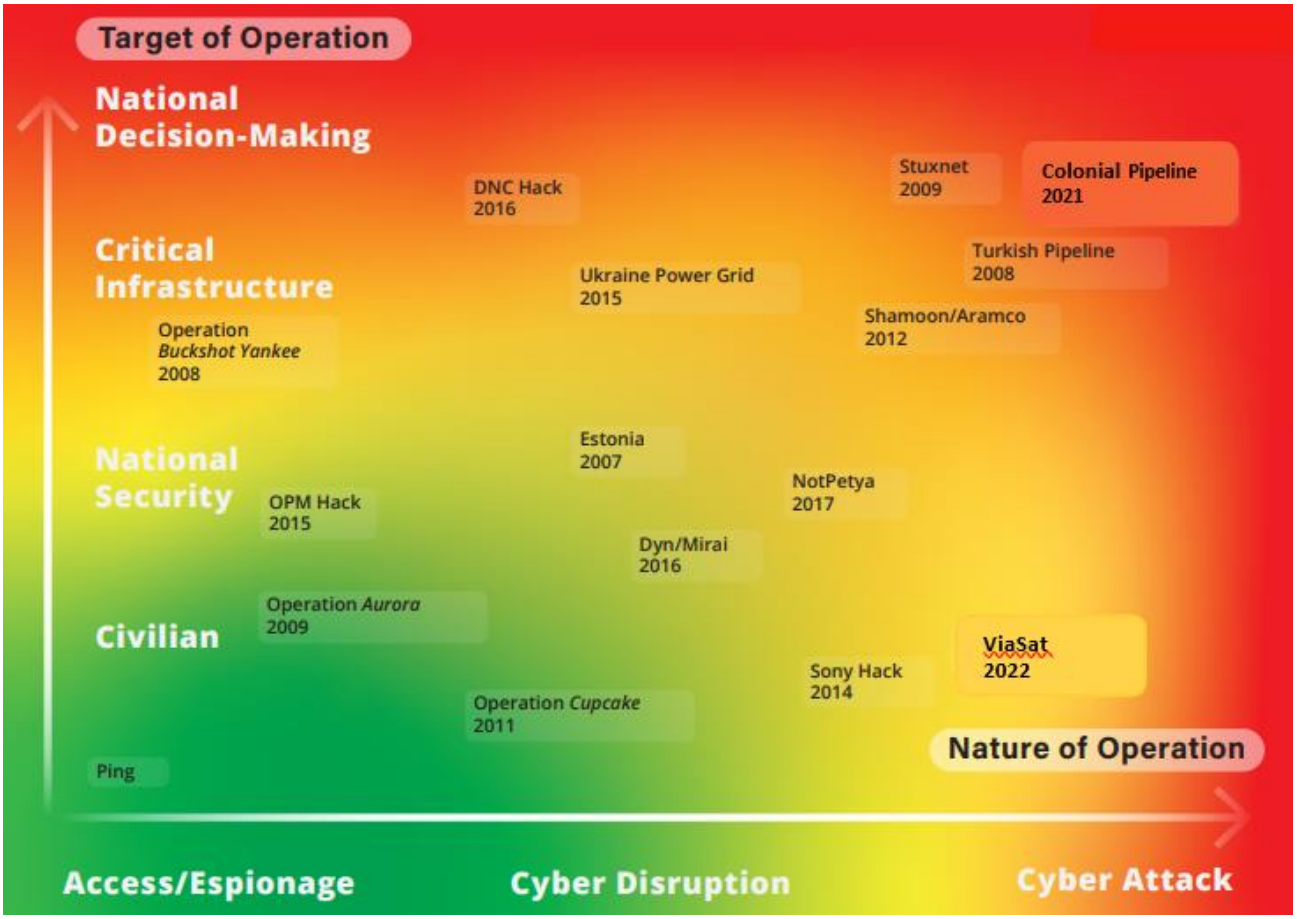

Рис. 1.3. Види кібероперацій за підтримки держав

Як бачимо на рисунку, кібероперації з найменшим впливом розташовані внизу ліворуч, а у верхньому правому кутку розташовані операції з масштабними наслідками проти цілей високої важливості.

Розглянемо основні види операцій детальніше.

Операції з метою отримання несанкціонованого доступу і шпигунства, які часто називають операціями для створення умов для подальших дій (enabling operations). Як відомо, отримання доступу до цільової системи, тобто проникнення в неї, є необхідною умовою для більшості видів зловмисної кібердіяльності, а сам доступ може бути використано як перший крок у

шпигунському нападі, інформаційній операції, виведенні з ладу IT-інфраструктури або повномасштабній кібератаці.

Часто операції несанкціонованого доступу є прихованими, маючи на меті отримання й утримання доступу протягом певного періоду часу без відома власника системи. Такі операції доступу рідко спрямовані на пошкодження або руйнування інформаційних активів. Однак, за певних обставин зловмисники можуть пошкодити або зруйнувати систему для полегшення подальшого доступу. Наприклад, захищена система зв'язку може бути виведена з ладу кіберзасобами з метою зловмисного використання іншої, більш уразливої системи зв'язку.

Операції з метою пошкодження або виведення з ладу інформаційно-комунікаційних систем охоплюють дії, які переривають процес передавання інформації або функціонування систем обробки інформації. До цієї категорії відносять більшість зловмисних кібероперацій, зокрема атаки типу «відмова в обслуговуванні (DDoS) і маніпулювання даними.

Доречним прикладом буде використання ботнетів, обчислювальна потужність яких використовується для виконання простих шкідливих завдань через Інтернет, таких як розсилка спаму або перевантаження веб-сайтів величезним обсягом запитів. Ключовим елементом успішного ботнету є отримання контролю над достатньою кількістю обчислювальної потужності для здійснення цілеспрямованого деструктивного впливу на системи-жертви.

Кібератаки, спрямовані на пошкодження, виведення з ладу або знищення фізичної інфраструктури, спричинення значних людських жертв. Найбільш очевидним прикладом таких атак є будь-який зловмисний промисловий інцидент, зокрема несправність обладнання або відмова системи безпеки. З огляду на те, що сучасні промислові об’єкти управляються складними автоматизованими системами і підключені до мереж, кібератака на АСУ може призвести до надлишкового тиску, перегріву, увімкнення або вимкнення системи або виконання будь-якої кількості функцій з негативними наслідками у фізичному вимірі.

Ймовірно, найвідомішою такою кібератакою є зараження складним шкідливим ПЗ Stuxnet промислових систем управління на іранському об’єкті зі збагачення урану в Натанзі у 2009 році. Вірус досяг цільової системи, заразив програмовані логічні контролери, підключені до центрифуг, які використовувалися для виробництва збагаченого урану, і врешті-решт фізично знищив понад тисячу таких центрифуг [10].

Відповідно до іншого подібного за критеріями підходу виділяють сім категорій кіберінцидентів [11], які у порядку зростання наслідків представлені на рис. 1.4.

Рис. 1.4. Види кіберінцидентів

Розглянемо детальніше кожну з категорій.

Розвідка/спроба проникнення. Розвідка кіберсистеми може складатися зі сканування портів або будь-якої подібної діяльності. Часто це автоматизований процес, метою якого є простий пошук вразливостей у системах-потенційних жертвах. Хакери, що фінансуються державою, найчастіше намагаються знайти вразливості в конкретних системах, що становлять інтерес.

Проникнення – це перший етап отримання несанкціонованого доступу до системи, на якому системні адміністратори можуть помітити порушників, які безуспішно намагаються проникнути в систему.

Проникнення та ескалація привілеїв. В узагальненому вигляді виділяють такі способи проникнення в систему без авторизації: шляхом експлуатації

людей, апаратного або програмного забезпечення. Якщо людина є інсайдером, якого експлуатують за допомогою методів соціальної інженерії, таких як фішинг, кінцевим результатом часто буде використання викрадених облікових даних для отримання незаконного доступу. Апаратні експлойти часто є наслідком проблем із ланцюгом постачань, які нерідко пов’язані з присутністю всередині організації, і зазвичай розвиваються протягом тривалого часу [11].

Початкове проникнення хакера в систему може забезпечити лише базовий доступ користувачів до мережі. Одним із перших кроків, які намагаються зробити зловмисники, є підвищення привілеїв кінцевого користувача, щоб він міг маніпулювати операційною системою та конфігурацією мережі, а також замести сліди, стираючи журнали мережевої активності. Метою є отримання прав системного адміністратора, оскільки цей рівень доступу дозволяє порушникам виконувати операції в усіх наступних категоріях.

Постійна присутність та шпигунство. Після того, як зловмисник отримав доступ до системи та підвищив свої привілеї, він прагне встановити тривалу присутність, включаючи повторне використання системи у випадку виявлення та усунення наслідків проникнення. Це може охоплювати встановлення шкідливих програм або створення додаткових облікових записів користувачів для атак «через чорний хід» (backdoor).

Шпигунство передбачає «копання» в системі для спостереження за налаштуваннями й роботою системи, а також інформацією, що там зберігається і обробляється. Це включатиме певний обмін пакетами даних, але не їх експорт у більших масштабах.

Організація витоку даних. Надсилання копій даних за межі системи може бути результатом шпигунської діяльності. Усі держави займаються шпигунством і загалом усвідомлюють, що їхні супротивники роблять те саме. У випадку кібершпигунства необмежену кількість копій даних можна створити і відправити мережею без негативного впливу на оригінал. Саме володіння

інформацією або знаннями є кінцевим результатом такого виду зловмисної кібердіяльності.

Маніпуляції з даними або їх знищення. Якщо зловмисник виходить за рамки копіювання інформації, а натомість використовує доступ до системи для маніпулювання, зміни або видалення даних, таку діяльність кваліфікують як більш загрозливу дія, яка вимагає серйозніших заходів реагування.

Віртуальне пошкодження системи або негативний вплив на її функціональність спрямоване на тимчасове неналежне функціонування системи, не завдаючи їй постійної шкоди. Це схоже на ситуацію, коли після завантаження користувачем нової програми або втрати інтернет-з'єднання комп'ютер «зависає», і необхідно його перезавантажити, щоб повернути до робочого стану. У випадку, якщо така ситуація спричинена навмисними діями, а не звичайним шумом в системі, вона підпадає під цю категорію [12].

Оскільки може бути важко сформулювати різницю між віртуальною та фізичною шкодою, серед експертів з міжнародного права існують певні суперечки з цього питання.

Дослідження показало, що об'єкти кібератак, які підтримуються державами, охоплюють такі загальні категорії (Рис. 1.5):

- цивільні системи;
- урядові системи;
- системи критичної інфраструктури, які можуть включати як урядові, так і цивільні компоненти;
- системи національної безпеки, зокрема класифіковані розвідувальні системи, а також військові системи, необхідні для національної оборони;
- системи ядерного командування, управління та зв'язку (NC3) [1].

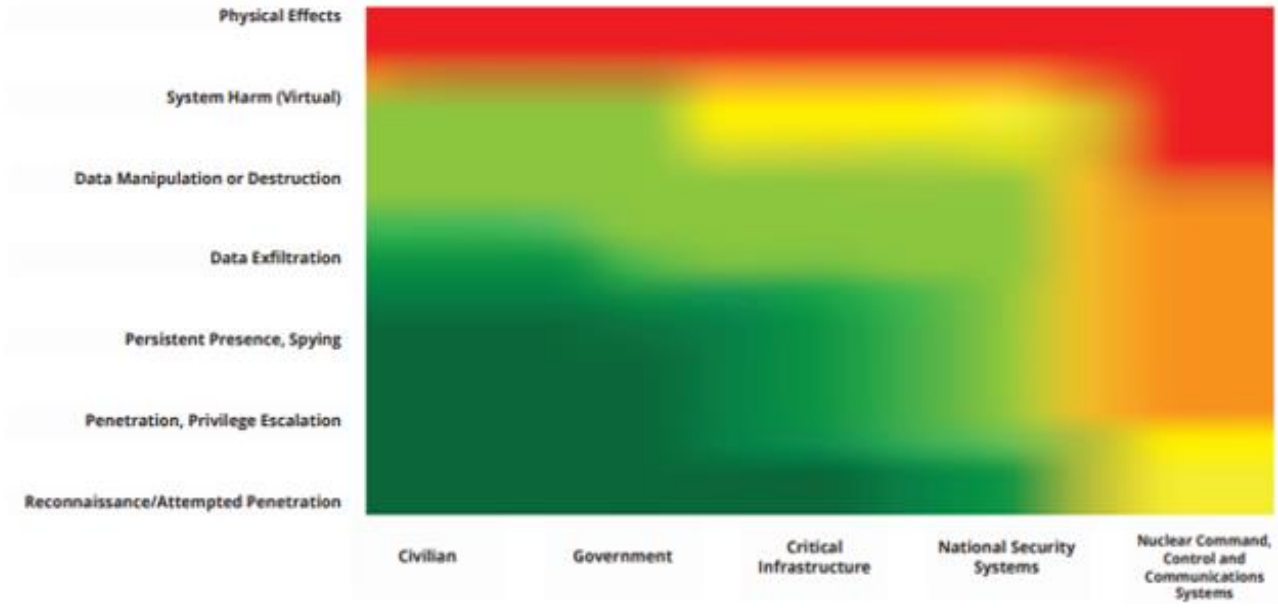

Рис. 1.5. Види об’єктів кібератак

Як бачимо, по вертикальній шкалі у порядку зростання розміщені категорії наслідків кібератак: розвідка загроз і пробне проникнення; проникнення в систему і ескалація привілеїв; постійна присутність і шпигування; розкриття даних; маніпулювання або знищення даних; пошкодження віртуальних систем; фізичний вплив.

1.3 Тактика та методи кібератак з боку держав

У кібератаках, що підтримуються державами, використовуються різноманітні тактики і методи для досягнення стратегічних цілей. Ці тактики часто адаптуються для використання вразливостей у цільових системах з уникненням виявлення і встановлення агента кібернападу.

Нижче представлені найбільш поширені тактики та методи, що використовуються в кібератаках за сприяння держав (Рис. 1.6) [9, 13-14].

Рис. 1.6. Тактики і методи кібератак за сприяння держав

Фішинг, цільовий фішинг. Кіберсуб'єкти, які підтримуються державами, часто використовують фішингові електронні листи, щоб обманом змусити користувачів натискати на шкідливі посилання або завантажувати вкладення, заражені шкідливими програмами. Фішинг з використанням спеціальних посилань спрямований на конкретних осіб або організації з використанням персоналізованої інформації для збільшення ймовірності успіху.

Розгортання шкідливого програмного забезпечення. Кіберзлочинці, що спонсоруються державами, розробляють і розгортають різні типи шкідливих програм, включаючи віруси, черв'яків, троянів і програми-вимагачі, для проникнення в цільові системи, крадіжки даних або порушення операцій. Корисне навантаження шкідливого програмного забезпечення у таких випадках розробляється для уникнення виявлення антивірусним ПЗ і засобами безпеки.

Експлойти нульового дня. Суб'єкти, які діють в інтересах держав, прагнуть використати раніше невідомі вразливості, так звані вразливості нульового дня, у програмному або апаратному забезпеченні, щоб отримати несанкціонований доступ до систем або виконати шкідливий код. Нульові експлойти надають зловмисникам значну перевагу, оскільки постачальники ще не встигли їх виправити.

Розширені постійні загрози (APT). Довгострокові кіберкампанії, що проводяться державами для отримання та підтримки несанкціонованого доступу до цільових мереж, поєднують приховане проникнення, розвідку і постійний моніторинг для вилучення даних або саботажу систем протягом тривалого періоду.

Атаки на ланцюги постачання. Зловмисники, що підтримуються державами, все частіше націлюються на ланцюг постачання програмного забезпечення, щоб скомпрометувати довірених постачальників або дистриб'юторів програм. Впроваджуючи шкідливий код у легітимні оновлення або пакети програмного забезпечення, зловмисники можуть заразити широкий спектр систем та організацій нижче у ланцюжку постачання і споживачів кінцевих продуктів.

Атаки типу «водяна діра». Під час атак типу «водяна діра» зловмисники компрометують веб-сайти, які часто відвідують цільові особи або організації. Заразивши ці веб-сайти шкідливим програмним забезпеченням, зловмисники прагнуть використовувати браузери або пристрої відвідувачів, щоб отримати доступ до їхніх систем або облікових даних.

Розподілені атаки типу «відмова в обслуговуванні» (DDoS). Державні суб'єкти можуть запускати DDoS-атаки, щоб порушити доступність онлайн-сервісів або веб-сайтів противників. Затоплюючи цільові сервери або мережі великим обсягом трафіку, зловмисники перевантажують їхні ресурси та роблять їх недоступними для законних користувачів.

Інфраструктура командування та управління (Command and Control, C2). Виконавці кримінальних замовлень держав у кіберпросторі створюють

інфраструктуру командування та управління для дистанційного управління скомпрометованими системами, викрадання даних або доставки додаткових корисних навантажень. Сервери C2 використовують модель клієнт-сервер, де зловмисник контролює центральний сервер для керування кількома зараженими системами. Після того, як шкідливе ПЗ заражає пристрій, воно знову підключається до сервера C2, очікуючи команд. Ці повідомлення часто шифруються, щоб уникнути виявлення системами безпеки [15].

Операції під хибним прапором. Державні суб'єкти можуть використовувати операції під хибним прапором, щоб ввести в оману слідчих і приписати кібератаки іншим країнам, організаціям або хакерським групам. Імітуючи тактику, методи та процедури (TTP) інших злочинних суб’єктів, зловмисники можуть приховати справжнє походження та мотиви кібероперацій.

Інформаційні операції. Слід зазначити, що протиборство держав у кіберсередовищі часто виходить за рамки технічних атак і охоплює пропаганду, дезінформацію та психологічні операції, спрямовані на формування громадської думки, дестабілізацію супротивників або вплив на геополітичну ситуацію.

Криптоджекінг. Кримінальні суб’єкти за підтримки держав можуть займатися криптоджекінгом, несанкціонованим використанням обчислювальних ресурсів жертв для майнінгу криптовалют, таких як Bitcoin або Monero. Заражаючи комп'ютери або мережі шкідливим програмним забезпеченням для майнінгу криптовалют, зловмисники отримують прибуток, використовуючи обчислювальну потужність скомпрометованих систем.

Соціальна інженерія. Зловмисники, які діють в інтересах держав, часто використовують методи соціальної інженерії, щоб маніпулювати окремими особами або працівниками організацій, змушуючи їх розголошувати конфіденційну інформацію, таку як імена користувачів, паролі або облікові дані доступу. Зокрема зловмисники видають себе за авторитетних і надійних для жертви осіб, щоб завоювати її довіру і заволодіти цінними даними.

Внутрішні загрози. Державні кіберсуб'єкти можуть вербувати або співпрацювати з інсайдерами у цільових організаціях для сприяння кібератакам зсередини. Зазвичай зловмисники використовують інсайдерів, які мають доступ до конфіденційної інформації або критично важливих систем, для викрадання даних, саботажу операцій або сприяння досягненню цілей зловмисників.

Фізичні атаки. У деяких випадках кіберзлочини за підтримки держав, можуть охоплювати фізичні атаки на інфраструктуру або апаратні компоненти. Зокрема поширеним є вбудовування шкідливих апаратних вкладок у ланцюги постачання, втручання в роботу критично важливих елементів інфраструктури або проведення цілеспрямованих диверсійних операцій проти центрів обробки даних чи телекомунікаційних установ.

Викрадання облікових даних. Зловмисники, що підтримуються державами, використовують для проведення атак з метою отримання несанкціонованого доступу до цільових онлайн-акаунтів викрадені заздалегідь, отримані внаслідок витоків даних або придбані на незаконних ринках облікові дані користувачів. Автоматизуючи процес входу на кількох веб-сайтах або сервісах, хакери можуть ідентифікувати облікові записи з повторно використаними обліковими даними та скомпрометувати їх.

Атаки на побічні канали. Злочинці, що діють на замовлення держав, використовують побічні канали, такі як електромагнітне випромінювання або коливання споживання енергії, для реалізації кібератак з метою вилучення конфіденційної інформації з цільових систем. Атаки побічних каналів можуть обійти традиційні засоби кіберзахисту і витягти ключі шифрування, криптографічні алгоритми або інші конфіденційні дані.

Вішинг. Суб'єкти, що спонсоруються державою, можуть використовувати методи голосового фішингу, щоб обманювати людей по телефону і збирати конфіденційну інформацію або облікові дані доступу. Атаки з використанням вішингу часто передбачають видавання себе за довірених осіб, таких як представники банків або органів влади, щоб маніпулювати жертвами та змусити їх розкрити конфіденційну інформацію.

Новітні технології. Кібернапади, що спонсоруються державами, часто передбачають використання інноваційних технологій, таких як штучний інтелект (ШІ), машинне навчання або квантові обчислення. Ці потенційно руйнівні технології можуть бути використані для розробки передової кіберзброї або покращення існуючих можливостей атаки, створення нових уразливостей або посилення впливу кібератак на цільові системи і мережі.

Супутникове втручання. У певних випадках злочинці за підтримки держав можуть атакувати системи супутникового зв'язку, щоб порушити роботу телекомунікацій, GPS-навігації або військових операцій держав або міждержавних суб’єктів. Атаки із застосуванням супутникового втручання можуть спричинити перебої в роботі, погіршити ситуаційну обізнаність або поставити під загрозу критичну інфраструктуру, залежну від супутникових технологій.

Кібератаки на супутники на орбіті, які можуть бути запущені з інших супутників під керівництвом наземної станції, є відносно новими і спрямовані на датчики та виконавчі механізми, що забезпечують виконання місії супутників, і можуть призвести до кіберфізичних наслідків. Атаки на ці компоненти є складними, з огляду на те, що вони можуть вимагати близькості або прямої видимості цільового об'єкта, а також керування супутником-нападником з наземної станції з можливостями майже реального часу для передачі та обробки сигналу. Впровадження хмарних наземних станцій для керування супутниками забезпечило безпрецедентний доступ до цих послуг і, відповідно, розширило коло держав, компаній або навіть окремих осіб, які можуть завдати шкоди іншим супутникам на орбіті [16].

Інструменти кібершпигунства. Кібератаки, що реалізуються з ініціативи держав, в багатьох випадках передбачають розробку та розгортання спеціалізованих інструментів і систем кібершпигунства для проведення прихованих операцій зі збору розвідувальних даних. Ці інструменти можуть охоплювати спеціально створене шкідливе ПЗ, трояни віддаленого доступу

(RAT) або складні імплантати спостереження, призначені для уникнення виявлення і вилучення конфіденційної інформації з цільових мереж.

Основними завданнями кібершпигунства є крадіжка інтелектуальної власності (комерційних таємниць, патентів, креслень та/або запатентованих технологій); отримання політичної переваги через отримання доступу до конфіденційної інформації щодо переговорів, політики або внутрішніх стратегій держави-жертви; заволодіння інформацією у сфері оборони, зокрема щодо переміщення військ, оборонної стратегії або технології зброї [17].

Дослідження показало, що держави як суб'єкти протиборства у цифровому просторі використовують різноманіття вже відомих і широко розповсюджених методів кібернападу, демонструючи при цьому витонченість тактик, унікальність інноваційних рішень і комплексний підхід із залученням інших кібергравців, водночас прагнучи залишитися інкогніто для жертв агресії у кіберпросторі та світової спільноти.

Висновки до розділу 1

Дослідження показало, що кібератаки за підтримки держав виникають з різноманітних мотивів, що охоплюють шпигунство, саботаж, пропаганду, отримання економічної вигоди та стратегічної переваги. Зазвичай вони є ключовими компонентами ширших геополітичних стратегій держав, які прагнуть перевершити суперників або досягти стратегічно важливих цілей.

Потенційною метою кібератак, ініційованих державами, у зростаючому порядку визначають розвідку і шпигунство; маніпулювання даними і шкоду віртуальним активам; пошкодження матеріальних активів і фізичне знищення.

Встановлено, що кібератаки, які спонсоруються державою, мають глибокі наслідки, які зачіпають багато сфер і охоплюють загрози національній безпеці, деструктивний економічний вплив, загострення геополітичної напруженості, дипломатичні конфлікти між різними міжнародними суб'єктами, посилення гонки озброєнь та мілітаризацію кіберпростору, вплив на цивільне населення,

порушення міжнародних норм і засад управління цифровим середовищем, загрози демократичним цінностям.

Запобігання переліченим наслідкам вимагає узгоджених зусиль урядів, зацікавлених сторін приватного сектору, громадянського суспільства й міжнародної спільноти для підвищення кіберстійкості, зміцнення механізмів стримування і підтримки принципів миру, безпеки і стабільності в кіберпросторі.

Результати аналізу засвідчили, що види кібероперацій з ініціативи держав можна класифікувати за такими критеріями: природою нападу (отримання несанкціонованого доступу, шпигунство; порушення інформаційних процесів і функціонування кіберінфраструктури; пошкодження/виведення з ладу фізичної інфраструктури, людські жертви); метою деструктивного впливу (вплив на цивільне населення; загрози національній безпеці; пошкодження/руйнування критичної інфраструктури; вплив на процеси прийняття рішень).

З’ясовано, що об’єктами кібератак, які підтримуються державами, є: цивільні й урядові ІКТ; системи управління критичною інфраструктурою і національною безпекою, зокрема розвідувальні і військові системи; системи ядерного командування, управління та зв'язку (NC3).

У кібератаках за сприяння держав використовуються різноманітні тактики і методи, серед яких розгортання шкідливого ПЗ, експлойти нульового дня, APT- і DDoS-атаки, атаки на ланцюги постачання, інформаційні операції, атаки із залученням інсайдерів, методи соціальної інженерії і кібершпигунства, криптоджекінг, технології ШІ та МН, супутникове втручання тощо.

РОЗДІЛ 2
ОСНОВНІ РИСИ І ТЕНДЕНЦІЇ ЗЛОВМИСНОЇ ДІЯЛЬНОСТІ ДЕРЖАВ У КІБЕРПРОСТОРІ

2.1 Статистика кібероперацій за підтримки держав

Постійним відстеженням і детальним аналізом наявних і потенційних кіберзагроз, у тому числі тих, що виникають з боку державних суб'єктів, займаються урядові структури у багатьох державах, зокрема Агентство з кібербезпеки та безпеки інфраструктури (CISA) [18], Агентство національної безпеки (NSA) [19] у США, Європейське агентство з мережевої та інформаційної безпеки (ENISA) [20] та відповідні органи на рівні держав-членів ЄС, громадські й експертні організації (NIST, ISACA [21], OWASP [22]), а також авторитетні компанії в галузі кібербезпеки та захисту інформації (Microsoft [23], ESET [24], Gartner [25]).

Розглянемо статистичні дані щодо кількості та видів кібероперацій за підтримки держав або афілійованих ними суб’єктів. База даних Європейського репозиторію кіберінцидентів (EuRepoC) [26] в період з 2000 по 2025 роки зафіксувала загалом 4115 політично мотивованих кібератак у всьому світі, скоєних 921 відомим суб'єктом (актором або групою).

На рис. 2.1 показано види кіберінцидентів, серед яких неполітизовані атаки на політичні цілі (1793 випадки); атаки на об’єкти критичної інфраструктури (1376); атаки, реалізовані недержавними акторами з політичною метою (945); атаки, проведені групами, пов’язаними з державами (700). Решта категорій, серед яких атаки реалізовані національними державами; політизовані атаки на політичні цілі; політизовані атаки на неполітичні цілі, охоплюють 371 і менше випадків порушень. Слід відзначити, що один інцидент може поєднувати ознаки кількох видів атак.

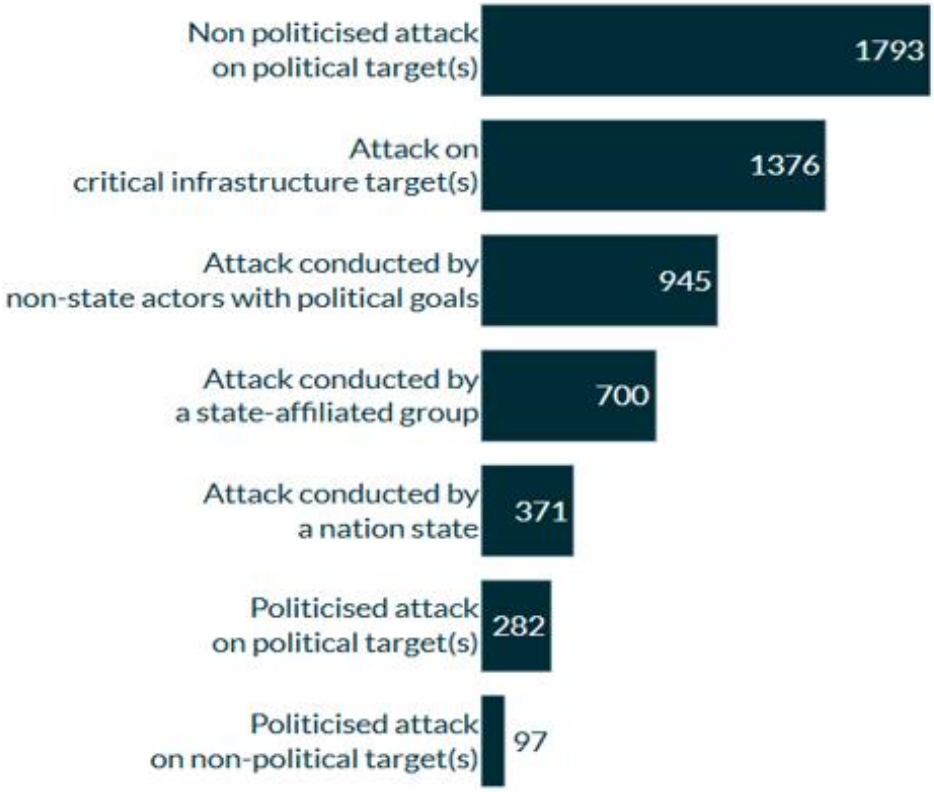

Рис. 2.1. Види політично орієнтованих кібератак згідно з EuRepoC

Глобальна платформа даних і бізнес-аналітики Statista провела дослідження даних EuRepoC за 2002-2023 роки і встановила, що майже 12% політично мотивованих кібератак, виявлених з початку ведення бази, були здійснені з Китаю, за ним іде Росія з майже аналогічною часткою (11,6%). Іран є відповідальним за 5,3% цих кібератак за досліджуваний період, а Північна Корея – за 4,7%. Важливо зазначити, що в більшості зловмисних дій цього типу (45%) впевнено ідентифікувати країну походження було не можливо [27] (Рис. 2.2).

Подібну статистику збирає відома компанія у сфері кібербезпеки Forescout. Аналіз бази даних кіберзловмисників Forescout показав, що у 2024 році 48% з понад 800 зловмисників, зафіксованих у базі, діють на користь певних держав, а це на 5% більше, ніж у попередньому році. Відзначено також, що за сприяння держав діють і хактивісти (7%).

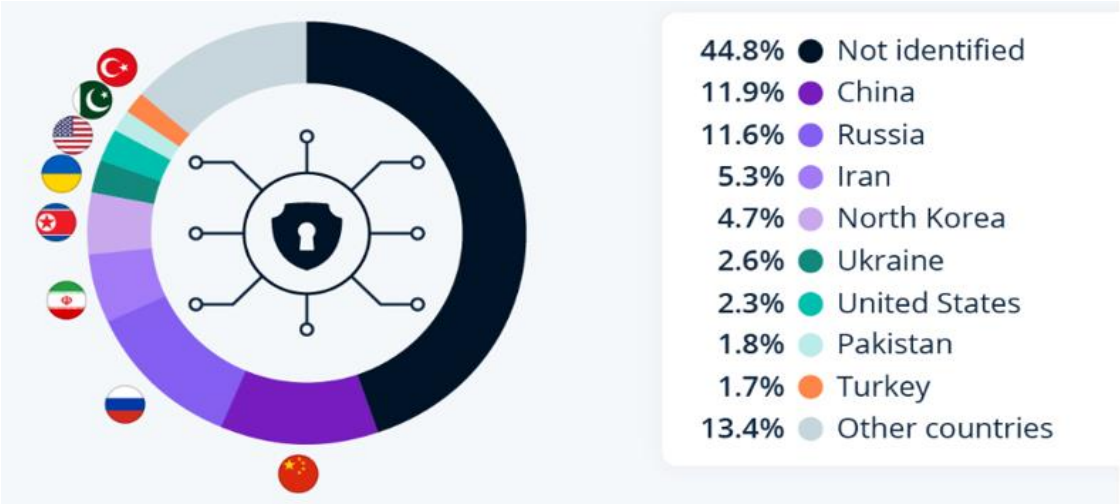

Рис. 2.2. Рейтинг держав, які реалізують кібератаки

Згідно з даними Forescout, більшість суб'єктів кібератак походять з Китаю (199), Росії (98) та Ірану (55). 43% нападів хакерських груп були реалізовані в інтересах зазначених держав. Встановлено, що основною ціллю для зловмисників є США, далі йдуть Німеччина та Індія. Уряд, фінансові послуги і телекомунікації найчастіше є мішенню для кібератак, причому найвищі показники мають напади на телекомунікаційні компанії [28].

Як відзначено вище, основними зловмисними гравцями у кіберпросторі є Китай, Росія, Іран і Північна Корея. На основі даних трекера кібероперацій Ради іноземних зв'язків США (Council on Foreign Relation) [29] встановлено показники кількості й видів кібероперацій зазначених держав (таблиця 2.1.).

Таблиця 2.1.

Кількість операцій, реалізовані державами-лідерами злочинної діяльності в кіберпросторі за 2005-2024 роки

	Держава	Кількість кібероперацій	Переважаючі види кібероперацій
1.	Китай	267	шпигунство, крадіжки конфіденційних даних, DDos-атаки, дезінформування
2.	РФ	193	шпигунство, компрометація даних, DDos-атаки, дезінформування
3.	Іран	110	шпигунство, компрометація даних, фінансові крадіжки, дезінформування
4.	Північна Корея	105	шпигунство, фінансові крадіжки

У звіті щодо цифрового захисту від Microsoft [30] висвітлено тенденції зловмисної кібердіяльності держав та їхніх агентів упродовж 2023-2024 років, серед яких:

Кіберактивність між державами була зосереджена навколо місць активних військових конфліктів або регіональної напруженості. Наприклад, 75% російських атак на держави були спрямовані на Україну або державу-члена НАТО.

Географічне охоплення кібероперацією Китаю залишалося стабільним протягом останніх кількох років: 72% кіберцілей КНР знаходилися в Північній Америці, на Тайвані та в інших країнах Південно-Східної Азії.

Активні кібергрупи, що базуються в Китаї (Raspberry Typhoon, Flax Typhoon та Granite Typhoon) інтенсивно атакували організації, пов'язані з IT, військовими та урядовими інтересами навколо Південно-Китайського моря.

50% кіберактивності Ірану з жовтня 2023 року по червень 2024 року було спрямоване проти Ізраїлю, що значно більше у порівнянні з попередніми періодами і було безпосереднім наслідком конфлікту між Ізраїлем та ХАМАС.

Іранські актори продовжували атакувати США та країни Перської затоки, включаючи ОАЕ і Бахрейн, частково через покращення їхніх зв'язків з Ізраїлем та побоювання Тегерану щодо їхнього сприяють воєнним зусиллям Ізраїлю.

Відзначено розширення масштабів використання програм-вимагачів державними гравцями, а також скорочення часових рамок реалізації таких атак. Час від спостереження до порушення роботи у 2025 році становив лише 14 хв., а шифрування зупинялося через 1 хв. і 8 секунд після його початку. Найпоширенішими методами початкового доступу для розгортання програм-вимагачів продовжують залишатися методи соціальної інженерії, такі як фішинг електронної пошти та голосовий фішинг .

Розширюються обсяги використання кіберзлочинної інфраструктури, такої як ботнети, державними суб'єктами, які раніше покладалися на власні можливості [31].

Встановлено збільшення активності операцій національних держав з помітним розширенням спрямованості на сектори зв'язку, досліджень і академічні кола. Це розширення в першу чергу зосереджено на використанні кібершпигунства проти традиційних цілей на додаток до розвідувальних операцій. Решта галузей, такі як роздрібна торгівля, виробництво, транспорт, зв’язок, фінанси, охорона здоров’я, оборона і енергетика стають цілями кібернападів у 3-7% випадків. Кібератаки на різні галузі розглядаються також як елемент попередньої підготовки до майбутніх конфліктів або потенційних фізичних руйнувань у поточних конфліктах.

Очікується, що геополітичний вплив надалі відіграватиме важливішу роль у формуванні поведінки кіберзловмисників, а кібероперації ймовірно будуть дедалі більше зосереджуватися на критично важливих виробничих галузях, пов'язаних з національною інфраструктурою або стратегічними ланцюгами постачань.

Встановлено, що очевидною є тенденція збільшення кількості державних акторів, що, на думку експертів, відображає зростання кількості та складності геополітичних конфліктів.

На користь зростання значення геополітичної боротьби у кіберпросторі свідчать результати опитування Global_Cybersecurity_Outlook 2025, відповідно до якого майже 60% респондентів відзначили вплив геополітичної напруженості на їхні корпоративні кіберстратегії. Більше того, триваючі міждержавні конфлікти у 2024 році продовжували впливати на регіони, які не були залучені до них безпосередньо: 18% організацій коригували торговельну або операційну політику, 17% повністю припинили бізнес або операції в певних регіонах, а 16% організацій повідомили про зміни постачальників [32].

Підсумовуючи висновки експертів з кібербезпеки, слід наголосити, що кібербезпека має бути пріоритетом, вбудованим в структуру організаційної стратегії та регулярно розглядатися як частина управління ризиками; налагодження глобальної співпраці між галузевими партнерами та навіть конкурентами є необхідною передумовою для координації та співпраці у справі

захисту від спільних противників у кіберпросторі; традиційних форм захисту периметру більше не достатньо, отже кіберстійкість має бути впроваджена в системи, ланцюги поставок, процеси та управління на всіх рівнях; з огляду на те, що нові типи загроз виникатимуть дедалі частіше, залишатися поінформованими й підготовленими є критично важливим для забезпечення ефективного запобігання і протидії кіберзагрозам, в тому числі з боку державних суб'єктів.

2.2 Тенденції розвитку злочинної кіберактивності держав

Дослідження засвідчило, що національні держави, вороже налаштовані до Заходу, включаючи Китай, РФ, Іран та Північну Корею, протягом останніх років здійснювали значну злочинну кіберактивність. Їхні атаки традиційно використовувалися для шпигунства, крадіжки конфіденційних даних урядів суперників та організацій критичної інфраструктури з метою отримання геополітичних переваг.

Однак, із посиленням глобальних конфліктів і геополітичної напруженості, національні держави також продемонстрували готовність брати участь у руйнівних кібератаках, спрямованих на завдання шкоди критично важливим службам держав-суперників.

Порівняно з кінетичними атаками, кіберактивність має перевагу в тому, що забезпечує «правдоподібне заперечення» національними державами їхніх злочинних дій. Це пояснюється тим, що важко виявити і довести причетність до зловмисної кіберактивності конкретних осіб або організацій.

Дослідження Infosecurity дозволило виділити такі основні тенденції розвитку кібератак за підтримки національних держав протягом останніх років [33] (Рис. 2.3).

Конвергенція з фінансово мотивованою кіберзлочинністю. Межі між суб'єктами національних держав та фінансово мотивованими кіберзлочинцями стають дедалі більш розмитими. Сучасні держави все частіше стають просто

клієнтами, які купують у злочинних груп протизаконні послуги. Придбання шкідливого програмного забезпечення, облікових даних або інших ключових ресурсів з незаконних форумів може бути дешевшим для держав, ніж їх розробка власними силами, а також забезпечує певну можливість інтегруватися у фінансово мотивовані операції та привертати менше уваги [28].

Рис. 2.3. Тенденції зловмисної кібердіяльності держав

Використання кіберзлочинних угруповань має на меті, зокрема, збір розвідувальних даних, проведення операцій з метою отримання фінансової вигоди і використання інструментів, яким віддають перевагу ці фінансово мотивовані групи (викрадачі інформації та системи командування й управління).

Прикладами такої співпраці є передача РФ деяких зі своїх операцій з кібершпигунства, зокрема проти України, на аутсорсинг злочинним групам; використання атак програм-вимагачів Іраном для отримання фінансової вигоди від деяких своїх наступальних кібероперацій; проведення Північною Кореєю операцій з використанням програм-вимагачів, як для збору розвідувальних даних, так і для монетизації свого доступу.

Ця координація між фінансово мотивованою кіберзлочинністю і діяльністю, що спонсорується державами, також дозволила кіберзлочинним групам отримати доступ до нових інструментів і методів [29].

Згідно зі звітом Microsoft [30] національні держави активізували співпрацю з кіберзлочинцями для досягнення своїх політичних та військових

цілей. Це охоплює аутсорсинг Росією деяких своїх операцій з кібершпигунства злочинним угрупованням, зокрема, для атак на Україну.

Експерти Microsoft також наголосили на доказах того, що національні державні угруповання все частіше використовують інструменти, які надають перевагу фінансово мотивованим кіберзлочинцям, для проведення своїх операцій, такі як викрадачі інформації та системи командування та управління.

Ще один новий зв'язок між діяльністю національних держав і кіберзлочинністю пов'язаний з методами атак, що застосовуються державними суб'єктами. Дослідники з SentinelLabs та Recorded Future [34] зазначили, що пов'язані з державою китайські групи APT використовують під час операцій програми-вимагачі, які зазвичай є прерогативою фінансово мотивованих суб'єктів. Це покликано збити зі сліду дослідників з кібербезпеки та приховати їхній справжній намір кібершпигунства.

Крім того, північнокорейські державні суб'єкти часто використовували методи кіберзлочинності, такі як програми-вимагачі та криптохаки, з метою отримання коштів для режиму Корейської Народно-Демократичної Республіки (КНДР).

Перехід до деструктивних атак. Кіберсуб'єкти національних держав традиційно зосереджувалися на операціях зі збору розвідувальних даних, проте спостерігається перехід до деструктивних атак, які спрямовані на порушення роботи критично важливих служб. Ця тенденція збіглася зі зростанням геополітичних конфліктів та напруженості, таких як війна між Росією та Україною та регіональна суперечка Китаю з Тайванем.

Росія використовувала кібератаки, щоб спробувати порушити роботу критично важливої інфраструктури в Україні поряд з традиційними війнами. Це включає спроби зупинити енергетичні та водопостачання в країні. Росія також здійснила деструктивні атаки на території за межами України. У вересні 2024 року США, Велика Британія та сім інших урядів звинуватили російських військових у здійсненні диверсійних кібератак на критично важливу інфраструктуру в країнах-членах НАТО в Європі та Північній Америці.

США та їхні союзники також висловили стурбованість тим, що китайські державні суб'єкти розмістилися в критично важливих секторах, включаючи зв'язок, енергетику, транспорт та водопостачання, щоб здійснити деструктивні атаки на численні сектори критично важливої інфраструктури у разі військового конфлікту. Крім того, Іран звинувачують у спробах порушити роботу критично важливих служб у таких країнах, як США та Ізраїль, після початку війни між Ізраїлем та ХАМАС у жовтні 2023 року [35].

Значна концентрація атак на національні держави. Ще однією тенденцією, що виникає внаслідок нещодавніх глобальних конфліктів і регіональної напруженості, є значна концентрація атак національних держав у географічних районах, що викликають у них найбільше занепокоєння.

Звіт Microsoft [30] показав, що 75% російських атак на національні держави в період з липня 2023 року по червень 2024 року були спрямовані на Україну або державу-члена НАТО. Експерти також наголосили, як Іран посилив свою увагу до Ізраїлю після спалаху конфлікту в Газі, що становило 50% його активності з жовтня 2023 року по червень 2024 року.

Основною ціллю атак Китаю були Північна Америка, Тайвань та інші країни Південно-Східної Азії, що становило 72% його кіберактивності, згідно з тим самим звітом. Крім того, у січні 2025 року Бюро національної безпеки Тайваню повідомило, що тайванські урядові мережі зазнали вдвічі більшої кількості щоденних атак у 2024 році порівняно з 2023 роком, більшість з яких були пов'язані з хакерами, яких підтримувала китайська держава [36]. Отже, китайська кіберактивність на Тайвані, схоже, посилюється на тлі зростання напруженості навколо самоврядного статусу острівної території.

Атаки на ланцюги постачань, спрямовані на багато організацій. Останніми роками спостерігалися численні випадки, коли суб'єкти національних держав націлювалися на постачальників програмного забезпечення та інших складників, щоб скомпрометувати кількох жертв. Такі атаки використовувалися переважно для шпигунських цілей.

Першим гучним інцидентом такого характеру став злом SolarWinds у 2020 році, коли російські суб'єкти додали шкідливий код до оновлення SolarWinds Orion, щоб скомпрометувати клієнтську базу компанії. Серед організацій, на які потрапив інцидент, були урядові відомства США та постачальники кібербезпеки.

Відтоді атаки на ланцюги поставок програмного забезпечення стали поширеною тактикою, що використовується групами національних держав, зокрема Китаєм. Так, у 2023 році китайська шпигунська група Storm-0558 скомпрометувала облікові записи Microsoft 365 численних організацій, включаючи урядові відомства США, що дозволило їй отримати доступ до тисяч електронних листів урядовців.

Microsoft виявила, що Storm-0558 підробив токени автентифікації, використовуючи отриманий ключ шифрування Microsoft. Коли цей ключ було поєднано з іншою вразливістю системи автентифікації Microsoft, це дозволило Storm-0558 отримати повний доступ майже до будь-якого облікового запису Exchange Online у будь-якій точці світу.

Наприкінці 2024 року було виявлено дві інші великі атаки китайського шпигунства на ланцюги поставок. У листопаді Salt Typhoon скомпрометував основних провайдерів зв’язку в США, дозволивши зловмисникам отримати доступ до записів дзвінків, незашифрованих повідомлень і аудіо-повідомлень від цільових осіб, включаючи державних чиновників.

Наприкінці грудня Міністерство фінансів США повідомило, що китайські хакери отримали доступ до деяких його комп'ютерів після компрометації стороннього постачальника кібербезпеки BeyondTrust. За словами представників агентства Bloomberg, серед скомпрометованих пристроїв був комп'ютер міністра фінансів США Джанет Єллен [37].

Використання ШІ для покращення кібероперацій. Зловмисники, які діють за підтримки та в інтересах таких держав як Росія, Китай, Північна Корея та Іран, використовують ШІ та інші передові технології для підтримки своїх операцій.

Дослідники з Microsoft та OpenAI спостерігали, як державні структури досліджують поточні можливості й засоби контролю безпеки ШІ, використовуючи їх для допомоги в таких сферах, як виконання базових завдань кодування та перекладів для кампаній соціальної інженерії.

ШІ також став важливою частиною кампаній впливу та дезінформації державних структур, спрямованих на дезінтеграцію суспільства й маніпулювання громадською думкою в інших країнах [28].

У звіті Центру аналізу загроз (MTAC) Microsoft було підкреслено, як спостерігалося, як пов'язані з Комуністичною партією Китаю (КПК) суб'єкти публікували контент, зокрема зображення та відео за участю людей, створений ШІ, у соціальних мережах для посилення суперечливих внутрішніх питань у різних країнах, включаючи США.

Напередодні президентських виборів у США 2024 року урядові установи попереджали, що держави-конкуренти використовують такі технології, як генеративний ШІ та діпфейки, для просування своїх наративів в Інтернеті.

Атаки національних держав стали серйозною проблемою для організацій, особливо в урядовому секторі та секторі критичної інфраструктури. Актори національних держав розширили свої операції та тактику в останні роки, що зробило їх більш небезпечними. Це охоплює співпрацю з фінансово мотивованими кіберзлочинцями, зростаючий інтерес до проведення деструктивних атак та використання складних інструментів ШІ.

Загроза з боку хакерів, що підтримуються державами, перейшла від виключно крадіжки даних до можливості порушення роботи критично важливих послуг.

2.3 Огляд держав, які є основними організаторами кібератак

Аналіз публікацій з теми дослідження показав, що основними несанкціонованими «гравцями» у кіберпросторі є низка держав.

Китай. Галузеві дослідження показують, що групи, що базуються в Китаї, досі зосереджувалися на шпигунстві, крадіжці інтелектуальної власності та стеженні; найчастіше вони спрямовують свої зусилля проти урядів і секторів охорони здоров'я, технологій та телекомунікацій (Рис. 2.4). Офіс Директора Національної розвідки (ODNI) заявив, що КНР майже напевно здатний на кібератаки, які порушать роботу критичної інфраструктури США, і що він проводить кібероперації для протидії передбачуваним загрозам Комуністичній партії Каю, таким як злом облікових записів і онлайн-ресурсів журналістів.

Рис. 2.4. Напрями кіберзлочинної діяльності Китаю

Китай результативно використовує хакерські операції і дезінформаційні кампанії в соціальних мережах для підриву довіри до державних інституцій та управлінських рішень у державах конкурентах, зокрема США. У рамках таких кампаній передбачається зокрема розміщення так званих «підроблених новин» у відомих соцмережах, зловмисне руйнування банківських систем і державних урядових структур, відповідальних за базове забезпечення громадської життєдіяльності, автоматичні порушення інфраструктури й прихований контроль над цільовими мас-медіа [38].

Прокитайська злочинна група UNC5174 використовує онлайн-образ хактивіста "Uteus", який стверджує, що пов'язаний з Міністерством державної безпеки Китаю, працює брокером доступу та можливим підрядником, який здійснює вторгнення з метою отримання прибутку. UNC5174 використав численні вразливості як зброю невдовзі після їх публічного оголошення,

намагаючись скомпрометувати численні пристрої, перш ніж їх можна було виправити. Наприклад, у лютому 2024 року було помічено, що UNC5174 використовував CVE-2024-1709 у ConnectWise ScreenConnect для компрометації сотень установ, переважно у США та Канаді, а у квітні 2024 року GTIG підтвердила, що UNC5174 використав CVE-2024-3400 як зброю, намагаючись використати пристрої GlobalProtect мережі Palo Alto Network (PAN). В обох випадках було виявлено кілька кластерів China-nexus, які використовували експлойти, що підкреслює, як UNC5174 може сприяти розвитку додаткових операторів [39].

Окремо слід відзначити системний деструктивний кібервплив КНР, спрямований проти Тайваню. Науковці виділяють такі види атак: дезінформування населення Тайваню з метою залякування і формування зневіри у можливостях уряду захиститися від загроз боку Китаю; пропагування ідеї «єдиного Китаю» серед громадян Тайваню; дискредитація Тайваню в очах міжнародної спільноти; кібершпигунство, яке охоплює несанкціоноване заволодіння конфіденційною інформацією з метою отримання економічної вигоди, переваг у політичній чи військовій сфері [40].

Підсумовуючи, слід відзначити, що кіберможливості Китаю сьогодні є складними та високоінституціоналізованими. Зловмисна кібердіяльність КНР є скоординованою екосистемою, яка охоплює рівні підрядників, державний нагляд і передові інструменти. Наявні кіберзасоби дозволяють Китаю утримувати лідерство у кібершпигунстві проти урядових і приватних структур, викраденні об’єктів інтелектуальної власності, дезінформуванні та стеженні за громадськими активістами, які критикують Китай [41].

Російська Федерація. Росія, яка здебільшого використовує кібероперації проти держав для збору розвідувальних даних, а Microsoft стверджує, що групи, що базуються в Росії, все частіше націлюються на уряди CrowdStrike. Управління директора національної розвідки США (ODNI) повідомило, що Росія також намагається зламати системи організацій і журналістів, які

розслідують діяльність російського уряду. Руйнівні кібератаки, зокрема проти України та енергетичної промисловості США, приписуються Росії.

Російська держава все частіше використовує шкідливе програмне забезпечення та інструменти, отримані зі злочинних ринків (Рис. 2.5)

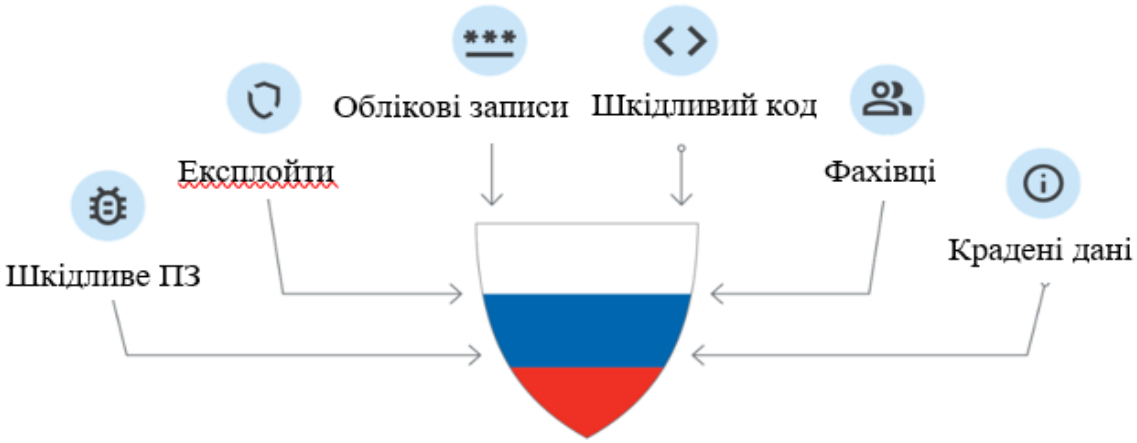

Рис. 2.5. Ресурси, які РФ отримує з даркнету

Google оцінює, що обмеженість ресурсів та операційні вимоги сприяли зростанню використання російськими групами кібершпигунства безкоштовних або загальнодоступних шкідливих програм та інструментів, включаючи ті, що зазвичай використовуються злочинцями для проведення своїх операцій. Після повномасштабного вторгнення Росії в Україну GTIG спостерігала, як групи, підозрювані у зв'язку з російськими військовими розвідувальними службами, застосовують такий підхід "низького рівня власного капіталу" до управління своїм арсеналом шкідливих програм, утиліт та інфраструктури.

Інструменти, придбані у фінансово мотивованих суб'єктів, є більш поширеними та дешевшими, ніж ті, що розроблені урядом. Це означає, що якщо операцію з використанням цього шкідливого програмного забезпечення буде виявлено, витрати на розробку нового інструменту не нестиме розвідувальне агентство; крім того, використання таких інструментів може ускладнити зусилля з атрибуції. Примітно, що численні кластери загроз, пов'язані з російською військовою розвідкою, використовували руйнівне шкідливе програмне забезпечення, адаптоване з існуючих варіантів програм-вимагачів, для атаки на українські організації.

Російські розвідувальні служби дедалі частіше використовують вже існуючі або нові зв'язки з кіберзлочинними групами для досягнення національних цілей та розширення збору розвідувальних даних. Вони зробили це, зокрема, з початку повномасштабного вторгнення Росії в Україну. GTIG вважає, що це поєднання нових зусиль російської держави та продовження поточних зусиль щодо інших фінансово мотивованих, російських суб'єктів загроз, які мали зв'язки з російськими розвідувальними службами до вторгнення. Принаймні в деяких випадках нинішні та колишні члени російських кіберзлочинних груп здійснювали діяльність із вторгнення, ймовірно, на підтримку державних цілей [42].

Як показало дослідження, основною ціллю російських кібератак упродовж останніх років була Україна як до повномасштабного вторгнення, так і після його початку. За період з 2005 по 2024 рік РФ здійснила 65 масштабних кібероперацій, спрямованих проти українського уряду, міністерств, силових відомств, органів місцевого самоврядування, підприємств енергетики, телекомунікацій, мобільного зв’язку, логістики, громадського транспорту, банківських установ, громадян України, організацій, які підтримували Україну, іноземних посольств, засобів масової інформації тощо [29]. Кібератаки насамперед мали на меті переривання або виведення з ладу критичних сервісів, збої в роботі офіційних джерел інформації, викрадення або знищення конфіденційних даних, поширення дезінформації, дискредитацію влади і залякування населення.

Іран. На думку експертів уряду Великої Британії, будучи менш агресивним й досвідченим, ніж вище згадані потужні держави, Іран використовує цифрові вторгнення для досягнення своїх цілей, зокрема шляхом крадіжки та саботажу.

Наприклад, у травні 2024 року GTIG виявила підозрювану іранську групу UNC5203, яка використовувала вищезгаданий бекдор RADTHIEF в операції з використанням тем, пов'язаних з ізраїльською ядерною дослідницькою галуззю.

Команда Google Threat Intelligence Group (GTIG) спостерігала, як іранські групи використовують програми-вимагачі для зламу систем і отримання прибутку. Так, протягом останніх кількох років іранські шпигунські групи проводили операції з використанням програм-вимагачів та руйнівні операції зі злому та витоку інформації. Хоча значна частина цієї діяльності, ймовірно, в першу чергу зумовлена руйнівними намірами, деякі суб'єкти, що працюють від імені іранського уряду, також можуть шукати способи монетизації викрадених даних для особистої вигоди, а погіршення економічного клімату в Ірані може служити поштовхом для цієї діяльності.

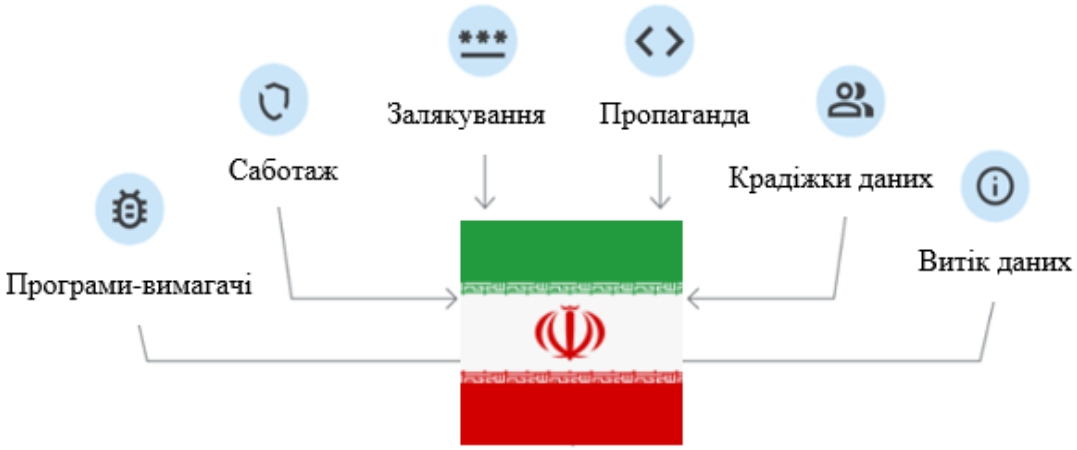

Рис. 2.6. Цілі кіберзлочинної діяльності Ірану

У кількох інцидентах особи, які здійснювали кібератаки від імені іранського уряду, також були ідентифіковані як такі, що здійснювали фінансово мотивовані вторгнення. Наприклад, у 2020 році Міністерство юстиції США підтвердило проведення кібератак двома громадяни Ірану кібератак, спрямованих на дані, що стосуються національної безпеки, розвідки зовнішньої політики, невійськової ядерної інформації, аерокосмічних даних, інформації про правозахисників, фінансової інформації жертв та особистої інформації, а також інтелектуальної власності. У деяких випадках вторгнення здійснювалися за наказом іранського уряду, тоді як в інших випадках відповідачі продавали зламані дані для отримання фінансової вигоди [35].

Слід відзначити діяльність Ірану у кіберпросторі, спрямовану на Ізраїль, основною формою якої були операції впливу в соцмережах. Метою цих операцій було поширення дезінформації і антиізраїльської пропаганди, залякування населення, дискредитація уряду. Так, у 2023 році під час чергового загострення відносин між Ізраїлем і рухом ХАМАС операції впливу мали на меті залякати ізраїльтян, поширювати критику військових операцій та поводження з полоненими з боку ізраїльського уряду, що мало врешті дестабілізувати Ізраїль.

Особливо гнучкими й ефективними були операції Ірану на початку конфлікту, коли Іран почав застосовувати тактику використання так званих онлайн-персон, які виступали в якості джерел деструктивної критики і пропаганди. Прикладом операція впливу, організована іранською державною групою Storm-1364, яка за допомогою онлайн-персони під назвою "Tears of War", що видавала себе за ізраїльських активістів, поширювала негативну інформацію проти уряду серед ізраїльської аудиторії в різних соцмережах і на платформах обміну повідомленнями.

Протягом першого тижня війни ідентифіковано 9 іранських груп, які активно діяли проти Ізраїлю, з часом їх кількість зросла до 14-ти. З часом вони почали використовувати нові методи, які раніше не спостерігалися серед іранських джерел загроз, зокрема застосовувався штучний інтелект як основний компонент їхніх повідомлень [43].

Крім цього, Іран спрямовував кібератаки та операції впливу проти політичних союзників і економічних партнерів Ізраїлю, щоб підірвати підтримку його військових операцій.

Північна Корея. Північна Корея, яка на сьогодні є світовим лідером за викраденням криптовалютних ресурсів, продовжує надавати пріоритет цій кримінальній діяльності, здійснюючи атаки на ланцюги поставок програмного забезпечення та націлюючись на своїх передбачуваних супротивників у сфері національної безпеки. Ймовірно, що КНДР планує таким чином генерувати дохід, головним чином для своєї програми озброєння, а також збирати розвідувальні дані про США, Південну Корею та Японію.

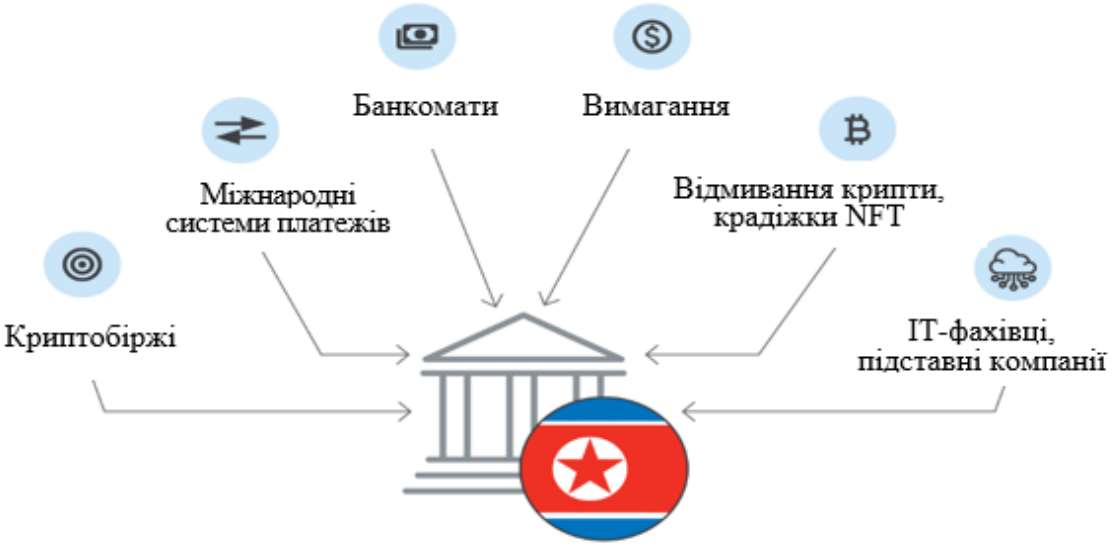

Рис. 2.7. Цілі атак КНДР

За оцінками ООН, північнокорейські кіберсуб'єкти з 2017 року вкрали понад 3 мільярди доларів криптовалюти. Тільки у 2023 році було здійснено пограбування на загальну суму від 600 до 1 мільярда доларів [44].

Північна Корея все частіше використовує кібератаки для фішингу й ураження ланцюгів постачання програмного забезпечення, а також спроб підірвати тристоронній альянс між США, Японією та Південною Кореєю.

Примітно, що Microsoft та OpenAI спостерігали, як північнокорейський кіберактор Emerald Sleet, використовує інструменти на базі моделей ШІ та великих мовних моделей (LLM), щоб зробити свої операції більш ефективними та результативними [45].

2.4 Роль злочинних груп у здійсненні кібератак за підтримки держав

Держави можуть проводити кібероперації через свої служби безпеки та іноземні розвідувальні служби або через недержавних посередників, таких як приватні підрядники. Кіберзлочинні групи можуть бути державними або пов'язаними з державою і здійснювати кібероперації від імені урядів, часто для розвідувальних або стратегічних цілей, а також можуть брати участь у фінансово мотивованих атаках.

Такі угруповання називають ще APT-групами, тобто такими які реалізують складні просунуті атаки APT. Отже, вони є високоорганізованими структурами, які займаються довгостроковим шпигунством, викраденням даних і саботажем. У своїх операціях вони використовують передові тактики, методи та процедури (TTP) для атак на уряди, критичну інфраструктуру та великі корпорації. Їхня здатність залишатися непоміченими протягом місяців або навіть років робить їх однією з найнебезпечніших загроз кібербезпеці.

Розглянемо найвідоміші злочинні кіберугруповання детальніше (Рис. 2.8).

Рис. 2.8. Логотипи кіберзлочинних груп, спонсорованих державами

Китай

Salt Typhoon - китайська державна група, яка активно працює з 2020 року та пов’язана з Міністерством державної безпеки Китаю. Група зосереджується на проникненні в критичні комунікаційні мережі та викраденні конфіденційних даних. З 2024 року її діяльність активізувалася, зосередившись переважно на секторі телекомунікацій.

APT31, також відома як ZIRCONIUM або Judgment Panda, - спонсорована КНР злочинна група, яка займається кібершпигунством і збором розвідувальних даних в національних інтересах Китаю. Група відома своїми складними фішинговими кампаніями, розгортанням шкідливого ПЗ і використанням вразливостей «нульового дня» для атак на уряди, бізнес і політичні структури по всьому світу.

APT41 є численною групою, яка здійснює як державне шпигунство в інтересах Китаю, так і фінансово мотивовану кіберзлочинну діяльність, зокрема запуск програм-вимагачів і крадіжки фінансової гуманітарної допомоги у зв'язку з COVID-19.

APT10 (Stone Panda) - китайська державна група, що займається кібершпигунством і викраденням інтелектуальної власності, спрямована проти технологічної та виробничої галузей держав-конкурентів КНР [39].

РФ

APT29, також відома як Cozy Bear, - російська кібершпигунська APT-група, пов'язана зі Службою зовнішньої розвідки РФ. Група, яка діє з 2008 року, відома своїми атаками на уряди, дипломатичні установи та критично важливі галузі промисловості по всій території Сполучених Штатів та Європи. Значне збільшення ролі APT29 відбулося на початку 2024 року у зв’язку з її участю в масштабній шпигунській кампанії, спрямованій проти державних і військових установ, а також промислових підприємств України.

Star Blizzard, раніше відома як Seaborgium і Callisto Group, є державною антитерористичною групою, яку пов'язують із ФСБ РФ. Група активно працює з 2019 року, проводячи довгострокові шпигунські кампанії проти країн НАТО,

аналітичних центрів, оборонних структур, академічних кіл, неурядових організацій і урядових організацій. Група відома своїми цілеспрямованими фішинговими атаками з використанням соцінженерії, фальшивих доменів, імперсонації електронної пошти.

Voodoo Bear/Sandworm - кібергрупа, яка, ймовірно, діє під керівництвом російського ГРУ, принаймні саме вона взяла на себе відповідальність за атаки на критичну інфраструктуру деяких держав, включаючи українську енергосистему, й атаку NotPetya.

Gamaredon - пов'язана з РФ група хакерів, яка діє щонайменше з 2013 року, спеціалізується на здійсненні кібератак на органи державної влади та об’єкти критичної інформаційної інфраструктури України. Злочинці використовують спеціально розроблене шкідливе ПЗ, методи фішингу і проникнення через відомі вразливості чи скомпрометовані облікові записи [46].

Іран

APT42 є іранською державною групою, що зосереджена на зборі інформації та спостереженні, часто спрямована проти осіб та організацій, що становлять стратегічний інтерес для уряду Ірану, включаючи урядовців і журналістів, які критикують режим. Група також послідовно націлюється на західні аналітичні центри, дослідників, журналістів, чинних західних урядовців, колишніх іранських урядовців та іранську діаспору за кордоном. Операції групи, спрямовані на побудову довіри та взаєморозуміння зі своїми потенційними жертвами, отримання доступу до їхніх особистих та корпоративних електронних адрес, мобільних пристроїв.

APT39 – іранська кіберзлочинна група, чия діяльність зосереджена переважно на Близькому Сході. APT39 надає пріоритет телекомунікаційному сектору, додатково націлюючись на туризм та IT-фірми, що його підтримують, а також на високотехнологічні галузі. Група реалізує переважно операції з моніторингу та стеження за особами або компаніями, збирає їхні дані або дані клієнтів відповідно до національних пріоритетів або створює формує нові

вектори для сприяння майбутнім кампаніям. Крім цього APT39 не відмовляється збирати геополітичні дані в інтересах держави Ірану.

Північна Корея

Lazarus, спонсорована північнокорейською державою група, яку приписують Генеральному бюро розвідки Північної Кореї. На відміну від багатьох APT, зосереджених на зборі розвідувальних даних, Lazarus надає пріоритет фінансовій вигоді, здійснюючи масштабні кіберпограбування, кампанії з використанням програм-вимагачів і крадіжки криптовалют. Група активно працює принаймні з 2009 року і здійснює операції, що відповідають стратегічним і фінансовим цілям країни.

Kimsuky, також відома як APT43, - це північнокорейська кібершпигунська група, яка діє з 2013 року. Група в першу чергу націлена на Південну Корею, США й Європу, зосереджуючись на зборі розвідувальних даних, зокрема в політичному та військовому секторах [47].

Крім безпосередньої підтримки з боку певної держави і проведення кібероперацій в державних інтересах, у деяких випадках уряди можуть просто закривати очі на певну злочинну або шпигунську діяльність, якщо вона відповідає їхнім стратегічним інтересам.

Зазвичай, операції, що підтримуються державою, збігаються з геополітичним конфліктом, можуть постійно бути спрямовані на стратегічні активи (при цьому операції продовжуються, незважаючи на відсутність успіху), і можуть бути особливо складними та ресурсномісткими. Водночас держави також використовують прості методи, зокрема «фішингові» електронні листи, які змушують одержувачів ділитися конфіденційною інформацією.

Висновки до розділу 2

Дослідження показало, що у період 2000-2025 рр. було зафіксовано 4115 політично мотивованих кібератак у всьому світі, скоєних понад 900 відомими суб'єктами. Лідерство у здійсненні кібератак утримують Китай (майже 12%

політично мотивованих кібератак), Росія з майже аналогічною часткою (11,6%), Іран (5,3%) і Північна Корея (4,7%). Основними цілями для зловмисників є США, Німеччина та Індія. Уряд, дослідницькі й академічні кола, фінансові установи і телекомунікації найчастіше є мішенню для кібератак.

Встановлено, що кіберактивність держав була зосереджена навколо місць активних військових конфліктів або регіональної напруженості; переважали кібератаки на країни, які розміщені у зоні геополітичного впливу держав-агресорів; зросли масштаби використання програм-вимагачів і ботнетів. Кіберзусилля національних акторів охоплювали насамперед кібершпигунство й розвідку, крадіжки конфіденційних даних та ураження об’єктів критичної інфраструктури.

Основними тенденціями розвитку злочинної кіберактивності держав є конвергенція з фінансово мотивованою кіберзлочинністю; перехід від традиційних розвідувальних операцій до деструктивних кібератак; концентрація кібератак національних держав у регіонах, які становлять для них геополітичний інтерес; зростання обсягу кібератак на ланцюги постачань; використання ШІ й інших передових технологій для покращення кібероперацій.

Аналіз засвідчив, що основні напрями кібердіяльності Китаю охоплюють шпигунство, викрадення інтелектуальної власності і стеження. Найчастіше КНР спрямовує свої зусилля проти урядів і секторів охорони здоров'я, технологій і зв’язку. Китай активно використовує хакерство і дезінформаційні кампанії в соціальних мережах для підриву довіри до держав-конкурентів, зокрема США і Тайваню. Зловмисна кібердіяльність КНР є скоординованою екосистемою, яка охоплює рівні підрядників, державний нагляд і передові інструменти.

Встановлено, що РФ здебільшого використовує кібероперації проти держав для збору розвідувальних даних часто з використанням шкідливих програм та інструментів, придбаних на злочинних ринках. Основною ціллю російських кібератак упродовж останніх років була Україна, а кібератаки насамперед мали на меті переривання або виведення з ладу критичних сервісів, збої в роботі офіційних джерел інформації, викрадення або знищення

конфіденційних даних, поширення дезінформації, дискредитацію влади і залякування населення.

Будучи менш агресивним і досвідченим, ніж згадані потужні держави, Іран протягом останніх років проводив операції з використанням програм-вимагачів і руйнівні операції зі злому та витоку інформації. Крім того, деякі кібератаки від імені іранського уряду були ідентифіковані як випадки фінансово мотивованих вторгнень. Окрема слід відзначити дезінформаційні та пропагандистські операції впливу Ірану у соцмережах, спрямовані на Ізраїль і його союзників.

Дослідження показало, що, КНДР яка сьогодні є світовим лідером у викраденні криптовалюти, продовжує надавати пріоритет цій кримінальній діяльності. Північна Корея усе частіше використовує кібератаки для фішингу й ураження ланцюгів постачання ПЗ, а також спроб підірвати партнерство між США, Японією та Південною Кореєю. Ймовірно, КНДР планує таким чином генерувати дохід, головним чином для своєї програми озброєння, а також збирати розвідувальні дані про держави-конкурентів.

З’ясовано, що держави можуть проводити кібероперації через свої служби безпеки та іноземні розвідувальні служби або шляхом залучення кіберзлочинних груп, які є високоорганізованими структурами і займаються довгостроковим шпигунством, викраденням даних і саботажем, переважно з метою отримання фінансової вигоди. Варто наголосити, що APT-груп використовують передові технології нападу і здатні залишатися непоміченими упродовж довгих періодів часу, що робить їх однією з найнебезпечніших загроз кібербезпеці.

РОЗДІЛ 3
НАПРЯМИ І МЕТОДИ ПРОТИДІЇ КІБЕРАТАКАМ ЗА ПІДТРИМКИ ДЕРЖАВ

3.1 Стратегії національної протидії операціям держав у кіберпросторі

Стратегії кібербезпеки для захисту від кібератак з боку держав-противників мають відображати багатогранний підхід до кібербезпеки, який враховує як соціально-політичні реалії країни, геополітичну ситуацію і технологічні виклики. Ефективні стратегії повинні поєднувати надійну національну політику, міжнародну співпрацю, технологічні інновації та державно-приватне партнерство. Розглянемо ключові стратегії кібербезпеки, які країни можуть прийняти для запобігання й протидії кіберзагрозам, ініційованих державами [42, 48, 49, 50] (Рис. 3.1).

Рис. 3.1. Стратегії захисту від кібератак з боку держав

Національна стратегія і політика кібербезпеки. Потужна й надійна система кібербезпеки на національному рівні є основою захисту від кіберзагроз. Першопочатковим завданням кожної з держав у запобіганні і протидії кібератакам держав-агресорів є розробка національної стратегії і плану дій у

галузі кібербезпеки, які дозволять запобігти вторгненням і атакам у кіберпросторі шляхом розширення можливостей, визначення відповідальності та розробки ефективних заходів реагування як для державного, так і для приватного секторів.

Держава має розробити комплексну політику кібербезпеки, яка стосується запобігання, виявлення, реагування та відновлення після кібератак. Ця політика регламентує питання захисту критичної інфраструктури, зокрема встановлення суворих стандартів безпеки для критично важливих секторів, таких як енергетика, охорона здоров'я, транспорт та фінанси; захищеності даних: забезпечення дотримання правил, які вимагають зберігання та обробки конфіденційних даних у межах національних кордонів для зменшення впливу зовнішніх загроз [48].

Крім цього політика кібербезпеки визначає засади проведення національних кампаній з підвищення обізнаності про кібербезпеку, навчання громадян, бізнесу та державних службовців правилам безпечної поведінки, реагування на події безпеки тощо, а також регламентує розвиток кіберпотенціалу шляхом інвестування в навчання, дослідження та розвиток робочої сили з кібербезпеки для створення потужного кадрового резерву, здатного протистояти новим кіберзагрозам.

Правові та регуляторні заходи. Міцна правова база, яка забезпечує підзвітність і створює основу для переслідування кіберзлочинців, має бути розроблена на основі передового міжнародного досвіду і містити:

• національне законодавство, яке забезпечує виконання норм, що криміналізують кібердіяльність, таку як хакерство, крадіжка даних, використання програм-вимагачів, криптоджекінг тощо.

• нормативні акти, які регулюють технологічні засади кібербезпеки, зокрема встановлюють зобов’язання щодо обов'язкового дотримання стандартів безпеки та притягнення компаній до відповідальності за порушення.

• закони про захист прав споживачів, зокрема щодо захисту від крадіжки особистих даних, шахрайства та інших кіберзлочинів [51].

Покращення кіберстійкості та здатності національних держав захищатися від широкого спектру загроз. Розширення зусиль щодо захисту критичної інфраструктури і мереж з метою забезпечення рівних гарантій стійкості та захисту для підтримки національних місій та економічної стабільності є одним із стратегічних завдань. Стан економіки, безпека та надійність критичної інфраструктури, які можуть вплинути на здатність держав ефективно функціонувати в кризових ситуаціях, стають дедалі важливішими чинниками безпеки та якості життя.

Сьогодні головний пріоритет має надаватися урядовій інформаційній інфраструктурі та мережам, які будуть захищені від кібератак за допомогою оцінок безпеки, а також впровадження міжнародних і регіональних правил безпеки. Мета полягає у виявленні та розпізнаванні порушень критичних функцій та реагуванні таким чином, щоб мінімізувати їх негативні наслідки.

Забезпечення стійкості насамперед національних ІКТ забезпечує безперервність операцій під час і після кіберінцидентів. Для досягнення цієї мети необхідно використовувати зокрема системи резервного копіювання, завдяки яким буде забезпечено збереження даних для критично важливої інфраструктури і мінімізовано простої під час атак; розробити плани відновлення після кіберінцидентів, зокрема протоколи для швидкого відновлення систем і даних після порушення; забезпечити децентралізацію мереж для зменшення залежності від окремих точок відмови і підвищення стійкості системи.

Створення ефективної моделі партнерства між урядом і приватним сектором. Стратегічним напрямком забезпечення кібербезпеки є посилення активної співпраці між усіма зацікавленими сторонами з метою досягнення спільної обізнаності про ситуацію та ефективного захисту від кіберзагроз. Для спрощення визначення критичних ІТ-інфраструктури і систем необхідно створити стандартний набір критеріїв, а також систему ретельного оцінювання ризиків та вразливостей. Заохочення обміну знаннями та регулювання, а також

співпраця між органами влади та бізнес-спільнотою сприятимуть розвитку кібербезпеки.

З огляду на стрімке зростання сектору ІКТ, забезпечення безпечного обчислювального середовища стає одним із головних пріоритетів будь-якої держави. Уразливість кіберпростору до різноманітних подій може стати причиною низки економічних, політичних і соціальних змін, негативно вплинути на сфери охорони здоров'я, безпеки та національної безпеки. Втрата і крадіжка інформації можуть суттєво вплинути на репутацію, довіру та авторитет держави.

Водночас, держава і приватний сектор можуть пом'якшити ситуацію у кіберпросторі шляхом раннього виявлення, обміну знаннями, розслідування, а також добре організованого реагування й усунення наслідків. Захист ІКТ, а також забезпечення конфіденційності, справедливості й доступності інформації є основними характеристиками безпечного кіберпростору.

Держава має забезпечити обмін розвідувальними даними про загрози в режимі реального часу між урядом і бізнесом; розробити й реалізувати спільні плани реагування на інциденти як інструменти координації стратегій реагування різних кіберакторів для вирішення масштабних кіберінцидентів; стимулювати приватні компанії дотримуватися вимог кібербезпеки, зокрема шляхом надання податкових пільг, грантів або інших переваг для їхнього заохочення інвестувати в надійні заходи кібербезпеки [51, 52].

Міжнародна співпраця. Враховуючи глобальний характер кіберпростору, міжнародна співпраця є важливою для боротьби з транскордонними кіберзагрозами з боку держав-супротивників і встановлення норм поведінки держав. Такі стратегії мають охоплювати:

- двосторонні та багатосторонні угоди між державами для сприяння відповідальній поведінці в кіберпросторі та встановлення протоколів для обміну інформацією та реагування на інциденти;
- глобальні стандарти кібербезпеки у співпраці з такими організаціями, як ООН, ОБСЄ і Міжнародний союз електрозв'язку (МСЕ), які забезпечують

дотримання міжнародних норм і стандартів кібербезпеки усіма партнерами і заохочують долучатися держави-конкурентів;

- договори про взаємну правову допомогу (Mutual Legal Assistance Treaties, MLAT), які покликані сприяти транскордонним розслідуванням та переслідуванню кіберзлочинців;
- заходи зміцнення довіри (Confidence-Building Measures, CBM), щоб забезпечити прозорість і довіру шляхом регулярного спілкування та обміну інформацією між країнами [51].

Розглянемо основні сфери міжнародної співпраці детальніше (Рис. 3.2).

Рис. 3.2. Напрями міжнародної співпраці у протидії державам-кіберагресорам

Обмін розвідувальними даними передбачає взаємне надання інформації про кібероперації противників, нові загрози, схеми атак і потенційні вразливості. Держави-партнери мають підтримувати безпечні канали для обміну інформацією та проводити спільний аналіз загроз, обмінюватися технічними показниками, сигнатурами шкідливих програм і даними про атрибуцію, щоб створити всебічне розуміння ландшафту кіберзагроз.

Обов’язковим елементом співпраці є *захист критичної інфраструктури* шляхом встановлення протоколів для захисту енергетичних мереж, фінансових мереж, транспортних систем та інфраструктури охорони здоров'я, спільного проведення оцінки вразливостей, розробки стратегій стійкості та координації планів реагування на інциденти. Доцільно обмінюватися передовим досвідом

щодо безпеки інфраструктури й активно співпрацювати у сфері безпеки ланцюгів постачання.

Співпраця у сфері протидії кіберзлочинності, яка сьогодні дуже часто використовується державами для реалізації кібератак, зазвичай охоплює обмін слідчими ресурсами, можливостями криміналістики та інформацією про злочинну діяльність, координацію зусиль щодо боротьби з атаками програм-вимагачів, фінансовим шахрайством та витоками даних. Спільні слідчі групи за участю представників країн-партнерів займаються транскордонними кіберінцидентами, а спрощені процеси сприятимуть швидкому обміну інформацією про нові загрози та злочинні методи. Важливим елементом співпраці є розробка і впровадження колективного підходу до визначення винних та відповідальності.

Спільне встановлення (атрибуція) держав-винуватців кібератак з їх подальшим притягненням до відповідальності передбачає відстеження й ідентифікацію держав та їхніх агентів, винних у кібератаках, і може мати стримуючий вплив на агресорів, особливо якщо воно пов'язане із заходами щодо притягнення до відповідальності, такими як санкції, обвинувальні акти та інші заходи реторсії (правомірні примусові дії держави у відповідь на недружній акт іншої держави).

Нарощування потенціалу можна забезпечити шляхом реалізації спільних програм, які покращують можливості усіх країн у сфері кібербезпеки. До них належать спільні навчання з кіберзахисту, обмін персоналом та спільні навчальні програми. Обмін технічним досвідом відбувається в таких сферах, як аналіз шкідливих програм, реагування на інциденти та мережевий захист. Країни також співпрацюють у науково-дослідницьких проектах з метою розробки і впровадження нових технологій кібербезпеки.

Кібердипломатія відіграє життєво важливу роль у сприянні миру та стабільності в кіберпросторі, одночасно захищаючи від Інтернет-загроз, які походять від конкуруючих держав. Обов’язковими елементами кібердипломатії є відстоювання кібернорм шляхом активної участі у міжнародних форумах для

формування норм відповідальної поведінки держав у кіберпросторі; запобігання кіберконфліктам через підтримання постійного діалогу зацікавлених сторін і створення каналів для деескалації під час криз; налагодження механізмів атрибуції і притягнення винних держав до відповідальності за рахунок посилення співпраці з міжнародними і приватними партнерами.

Міжнародна співпраця може здійснюватися, зокрема, на міжнародних форумах, таких як ООН, ОБСЄ, для сприяння відповідальній поведінці держав у кіберпросторі поза межами двосторонніх відносин, і повинна бути поступальною і безперервною. На таких заходах держави мають виступати за спільні стандарти безпеки, координувати позиції щодо управління кіберпростором і підтримувати регіональні зусилля з нарощування потенціалу [48, 53, 54].

Важливою темою для міжнародних дискусій є використання у кібербезпеці нових технологій, таких як штучний інтелект (ШІ), квантові обчислення, мережі 5G/6G та Інтернет речей, а також урахування нових загроз і технологічних розробок у практиці кібербезпеки.

Технологічні інновації. Технологічний прогрес може значно покращити здатність держави захищати свій цифровий простір від кіберзагроз, у тому числі з боку агресивних держав. Стратегії впровадження технологічних інновацій як передумова успішного кіберзахисту передбачають зокрема використання таких передових технологій як:

- штучний інтелект і машинне навчання (застосування інструментів на базі ШІ для виявлення загроз, прогнозної аналітики й автоматизованих систем реагування);
- квантово-стійке шифрування - інвестування в квантово-безпечні криптографічні методи закладає основи підготовки до майбутніх загроз, що виникають внаслідок розвитку квантових обчислень;
- блокчейн-технології, які забезпечать безпечне зберігання даних, перевірку особистих даних і відстеження транзакцій;

- стандарти безпеки Інтернету речей – мають гарантувати розробку і впровадження надійних протоколів безпеки для захисту пристроїв IoT від кіберзагроз.

Обізнаність і навчання з кібербезпеки. Регулярне проведення інформаційних кампаній і навчань, в тому числі симуляцій з кібербезпеки допомагає країнам і організаціям виявляти вразливості, покращувати координацію й готуватися до реальних кібератак. Такі навчання мають охоплювати настільні симуляції (Tabletop Simulations), які передбачають обговорення на основі сценаріїв для перевірки прийняття рішень та координації між зацікавленими сторонами; симуляції атак (Red Teaming), тобто моделювання атак для перевірки ефективності кіберзахисту; транскордонні навчання у співпраці з іншими країнами для моделювання і реагування на транснаціональні кіберзагрози [51].

Сприяння розвитку культури кібербезпеки на всіх рівнях суспільства допомагає зменшити вплив людських помилок, які залишаються частою причиною кіберінцидентів. Основними кроками в цьому напрямку є формування обізнаності, навчання й освіта, зокрема включення навчальних курсів із кібербезпеки до шкільних програм і впровадження програм професійної підготовки; формування корпоративної відповідальності, тобто заохочення організацій прийняти менталітет «безпека понад усе» у своїй діяльності; залучення громадян до справи забезпечення спільної кібербезпеки, зокрема через розширення їхніх можливостей розпізнавати і повідомляти про кіберзагрози [55].

3.2 Методи технологічного захисту від кібератак з боку держав

Кібератаки за підтримки держав стали серйозною проблемою для установ і організацій, особливо в урядовому секторі та секторі критичної інфраструктури. За останні роки національні держави розширили свої деструктивні кібероперації й постійно удосконалюють тактику, що робить їх щораз більш небезпечними.

Держави-кіберагресори тісно співпрацюють з фінансово мотивованими хакерами, проявляють зростаючий інтерес до проведення деструктивних атак і використання інструментів штучного інтелекту. Як свідчить статистика, у 2024 році 36% кібератак було організовано або здійснено державними суб'єктами, що може бути пов'язано з активними регіональними і глобальними конфліктами, а також із застосуванням кібератак для підтримки різних сторін конфліктів [56].

З огляду на обсяги і складність кібератак, що спонсоруються державами, а також їх серйозні наслідки для національної безпеки держав-мішеней основним завданням є забезпечення належного і всеохоплюючого захисту державних установ і організацій, об'єктів критичної інфраструктури, бізнес-суб'єктів тощо.

Огляд досліджень щодо протидії кібератакам за підтримки держав дозволив виділити ключові стратегії захисту, які поєднують зусилля як у галузі кібербезпеки, так і в правовому полі окремих держав, міждержавних об'єднань і міжнародного масштабу [57-59] (Рис. 3.3).

Рис. 3.3. Основні стратегії протидії кібератакам за підтримки держав

Для ефективного захисту від кібератак, що спонсоруються державами, необхідно проводити проактивну оцінку ризиків, на основі якої визначати пріоритетні заходи безпеки. Використовуючи можливості розвідки загроз, зокрема платформи обміну розвідувальними даними і обміну передовими практиками «полювання» на загрози, можна отримати уявлення про тактику, методи та процедури (TTP) організаторів кібернападів, а також зрозуміти їх поведінку й адаптувати оборонні стратегії для зменшення конкретних ризиків.

Основою ефективного кіберзахисту від кібератак, що спонсоруються державами, слугують надійні практики кібергігієни. Організації повинні регулярно впроваджувати оновлення програмного забезпечення, сегментацію мережі, засоби контролю доступу та безпечні конфігурації, щоб мінімізувати поверхню атаки й мінімізувати вразливості. Навчання персоналу навичкам виявлення і протидії методам соціальної інженерії має вирішальне значення для зниження ризику людських помилок та зміцнення загальної кіберстійкості.

Впровадження архітектури поглибленого захисту, яка передбачає розгортання кількох рівнів забезпечення безпеки (фаєрволи, системи виявлення і запобігання вторгненням IDS/IPS, засоби антивірусного захисту, виявлення та реагування на загрози кінцевим точкам EDR, системи управління інформацією та подіями безпеки SIEM тощо), сприяє виявленню кіберзагроз і зменшенню їхніх негативних впливів на різних етапах життєвого циклу атаки.

Сегментація мережі є важливою для обмеження горизонтального руху зловмисника і стримування впливу потенційних порушень внаслідок кібератак, що спонсоруються державами. Сегментуючи мережі та забезпечуючи дотримання принципу найменших привілеїв, можна зменшити площу атаки й мінімізувати потенціал несанкціонованого доступу до критично важливих систем і конфіденційних даних.

Розробка і регулярне тестування планів реагування на інциденти є важливим для надання ефективної відповіді на кібератаки, ініційовані державами. Важливо встановити чіткі ролі й обов'язки, протоколи зв'язку та процедури ескалації, щоб забезпечити скоординоване та своєчасне реагування

на кіберінциденти. Готуючись до різних сценаріїв, можна значно підвищити стійкість до кібератак.

Технології безперервного моніторингу і виявлення загроз, такі як системи IDS, EDR і платформи аналітики безпеки, мають вирішальне значення для виявлення ознак компрометації або зловмисної діяльності. Відстеження мережевого трафіку, активності кінцевих точок і поведінки користувачів у режимі реального часу дозволяє виявляти й реагувати на кіберзагрози за підтримки держав, перш ніж вони переростуть у серйозні інциденти безпеки.

Посилення безпеки ланцюга поставок є важливим для зменшення ризиків кібератак з ініціативи держав, спрямованих на сторонніх постачальників і підрядників. Організації повинні перевіряти й контролювати партнерів і сторонні організації щодо їхньої діяльності у сфері кібербезпеки та наявності вразливостей, впроваджувати заходи для перевірки цілісності й автентичності програмних та апаратних компонентів, а також встановлювати вимоги щодо дотримання вимог безпеки та готовності до реагування на інциденти в угодах.

Сьогодні в умовах глобального характеру кіберпростору безпрецедентно важливою є міжнародна співпраця та обмін інформацією за участі державних установ, підприємств, міжнародних організацій. Постійне партнерство в галузі кібербезпеки сприяє підвищенню ситуаційної обізнаності про загрози і координації зусиль щодо реагування на кібернапади, організовані державами. На міжнародному рівні основними напрямами протидії державам-кіберагресорам є розробка міжнародних норм щодо взаємодії в кіберпросторі для сприяння відповідальній поведінці та стримування ворожих дій; дипломатичні зусилля для протидії кіберагресії, зниження напруженості та зміцнення довіри [59].

Розроблення чіткої політики кіберстримування та інформування про її положення всіх залучених сторін є важливим чинником перешкоджання зловмисній діяльності держав у кіберпросторі. Водночас, особливого значення набуває організація ефективних процесів атрибуції, тобто встановлення суб’єкта, який стоїть за кібератакою, та судово-медичного аналізу.

Забезпечення стійкості критичної інфраструктури та бізнес-операцій є важливим для пом'якшення впливу кібератак з боку держав і забезпечення безперервності операцій. Організації повинні розробляти надійні плани забезпечення безперервності бізнесу та відновлення після аварій, впроваджувати резервні системи і копії, механізми відновлення після збоїв, а також проводити регулярні навчання для перевірки готовності реагувати на кіберінциденти.

Готуючись до різних сценаріїв та пом'якшуючи потенційні збої, можна мінімізувати вплив кібератак, що спонсоруються державами, на свою діяльність і репутацію, тим самим підтримуючи безперервність бізнесу та зберігаючи довіру клієнтів перед обличчям динамічних кіберзагроз.

Отже, з огляду на масштабність і складність кібератак, що спонсоруються державами, захист від них вимагає комплексного та багаторівневого підходу, який поєднує технічні, організаційні, стратегічні заходи і є важливою передумовою посилення кіберстійкості установ, підприємств та організацій, захисту критичної інфраструктури і в підсумку - зменшення ризиків для кібербезпеки держави.

3.3 Кібератрибуція як засіб встановлення держав-винуватців кібератак

Як зазначалося раніше, кібератрибуція – це процес відстеження та ідентифікації винуватця кібератаки. Звернення до відповідальної держави з проханням про пояснення та припинення атаки є можливим першим кроком, хоча деякі держави відмовляються взаємодіяти з цих питань. Однак, атрибуція для дипломатичних цілей буде ефективнішою, якщо вона супроводжуватиметься переконливими доказами підтримуватиметься багатьма країнами. Атрибуція може здійснюватися як у приватному, так і в державному вимірі.

Крім цього, кібератрибуція має технічний, політичний та юридичний виміри. Технічна атрибуція полягає у визначенні джерела зловмисної операції

шляхом дослідження тактики, методів та процедур атаки на основі технічних доказів, таких як IP-адреси, веб-сайти, журнали активності, шкідливе ПЗ тощо.

Політична атрибуція полягає у приписуванні відповідальності за зловмисну кібероперацію державі, державній організації або групі, що спонсорується державою, шляхом оцінки технічних доказів, розвідувальної інформації та шляхом прийняття ширших політичних суджень. Юридична атрибуція полягає у визначенні держави як ініціатора кібератаки на основі юридичних критеріїв атрибуції, що містяться в законодавстві.

Технічна атрибуція здійснюється приватними охоронними компаніями, а також державами, часто у співпраці з приватним сектором. Політична атрибуція в основному здійснюється державами індивідуально або колективно. Після такого приписування винним держави можуть вжити заходів проти винної держави, організації чи особи. Водночас, держави не часто використовують атрибуцію, оскільки вона може додати ще один шар до існуючого конфлікту або сама стати об'єктом конфлікту [60].

Кібератрибуція вважається важливою для багатьох країн, і труднощі з атрибуцією кібератак часто перебільшуються. Вимога політичних лідерів щодо високої точності атрибуції може становити значний тягар і ускладнювати реагування на дії зловмисних кіберсуб'єктів. Хоча атрибуція в кіберпросторі є складною через здатність опонентів використовувати анонімність, яку вона надає, поєднання методів може забезпечити точну атрибуцію.

Створення системи визначення винних. Визначення винних – це не лише питання технічних можливостей (хоча брак можливостей може бути перешкодою). Для міжнародних відносин важливіше політичне визначення винних, тобто прийняття і оприлюднення рішення уряду про встановлення відповідальності за певний акт. Рішення щодо визначення винних є переважно політичними та вимагають міцної основи в розвідці й аналізі інформації; багато країн вважають за краще уникати публічного визначення винних, а нинішній рівень обміну інформацією між державами є недостатнім для підтримки колективного підходу. Створення системи технічного та фактичного

визначення винних у поєднанні з політичним рішенням про дії було б одним із способів привернути увагу до політичних вимог до дій.

Держави можуть використовувати норми Групи урядових експертів ООН 2015 року як систему дій. Зменшення кількості, масштабів та ризику зловмисних кібератак вимагатиме механізмів співпраці та спільного розуміння визначення винних, пропорційності та управління будь-яким ризиком від реагування.

Експерти ООН відзначили, що в разі інцидентів з ІКТ держави повинні враховувати всю відповідну інформацію, включаючи ширший контекст події, проблеми атрибуції в середовищі ІКТ, а також характер і масштаби наслідків. Також наголошено, що атрибуція є складним завданням, і перед встановленням джерела інциденту ІКТ слід враховувати широкий спектр чинників. Таким чином, перш публічно оголошувати винних у кібератаках, слід переконатися у повній обізнаності про обставини порушення і пам’ятати про високий рівень відповідальності у випадку хибних звинувачень [52].

Визначення достовірної атрибуції. Використання правового прецеденту ускладнює і заплутує обговорення кібератрибуції. Кібератрибуція знаходиться у сфері компетенції суверенних держав, а не судів, де стандарти доказів є різними і часто несумісними. Найголовніше, що атрибуція державами не передбачає ідентифікації винної особи з певним рівнем сумніву, а визнає тільки однозначне і безперечне визначення держави, відповідальної за дію, або з території якої виникла дія.

Визначення відповідальної держави є центральним елементом прийняття рішень у кібератрибуції. Приписування кібернападів ґрунтується на відповідальності, узгодженій усіма державами-членами ООН, дотримуватися свого зобов'язання гарантувати, що з їхньої території не відбуватимуться зловмисні дії, співпрацювати з державою-жертвою, коли її просять про допомогу, та забезпечувати вжиття заходів проти зловмисника. Якщо цей зловмисник не може або не бажає вживати заходів, держава-жертва має право

вжити заходів самостійно (відповідно до міжнародного права), як колективно, так і індивідуально.

Достовірне приписування та пропорційність у будь-якій відповіді, що ґрунтується на цьому приписуванні, є важливими складовими державної прийнятної відповіді на зловмисні кібердіяння. Фактори, які держави повинні враховувати при приписуванні атаки і використанні приписування як інструменту для підвищення відповідальності та стабільності в кіберпросторі, охоплюють прецедент (наприклад, попередні атаки); технічні показники і наявність найкращих практик, таких як ведення обліку перед інцидентом; ціль (злочинці навряд чи будуть переслідувати військові цілі); ймовірний намір; наслідки (які дані були викрадені, які послуги були порушені); зовнішні джерела інформації (наприклад, союзники чи приватний сектор); підтримка розвідувальних даних з людських або технічних джерел [52] (Рис. 3.4).

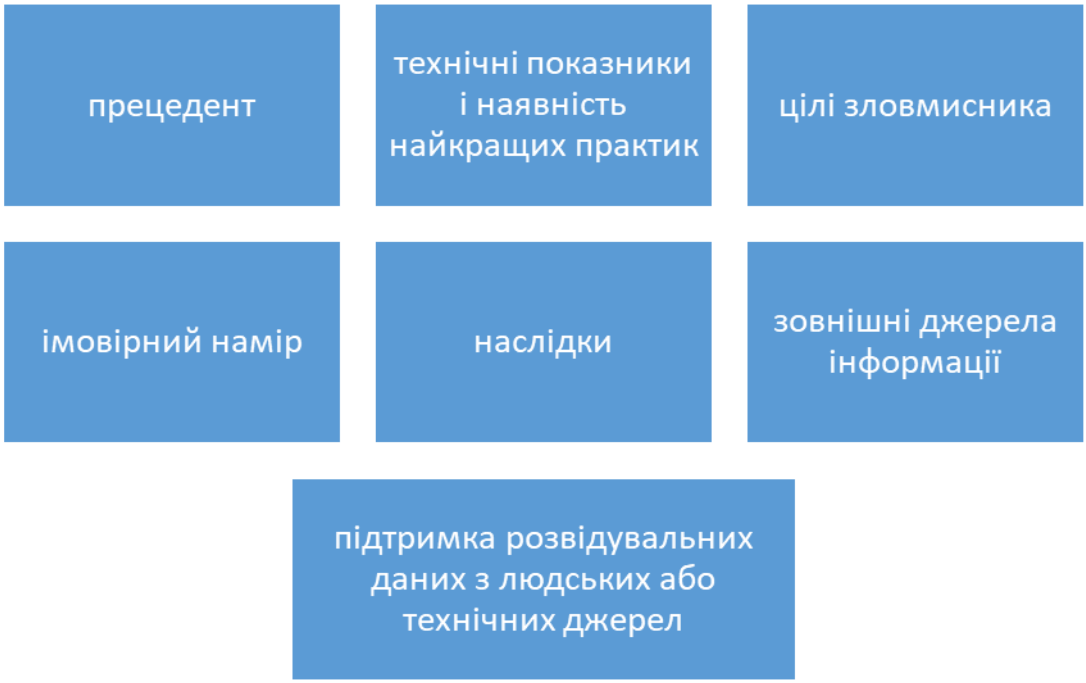

Рис. 3.4. Чинники кібератрибуції

Держави можуть використовувати регіональні, двосторонні та багатосторонні платформи, щоб обмінюватися передовим досвідом та інформацією щодо визначення винних у різних типах загроз та інцидентів у сфері ІКТ. Скоординоване визначення винних у зловмисній діяльності вимагатиме кращого обміну інформацією між партнерами та, можливо, нових

механізмів обміну та гармонізації підходів, зокрема впровадження стандартів доказової бази та механізмів обміну інформацією для координації будь-якого колективного визначення винних.

Визначення винних у контексті підзвітності не є переважно технічним, а скоріше політичним і вимагає міцної бази розвідувальних даних для політичних рішень. Однак, як зазначено вище, поточний рівень обміну інформацією між державами є недостатнім. Створення системи технічної та фактичної атрибуції в поєднанні з політичним рішенням було б корисним. Інші фактори допомагають визначити ступінь ретельності, необхідної для визначення винних, наприклад, чи пов'язане визначення винних з відповідними діями, чи висновки спроб визначення винних залишаться внутрішніми чи будуть оприлюднені.

Немає потреби ідентифікувати особу, відповідальну за зловмисні кібердіяння. Необхідно лише визначити, з чиєї території виникла атака. Звичайно, кращим варіантом було б ідентифікувати відповідальних осіб, але це може ускладнити завдання та не є необхідним для політичного приписування. Фундаментальним моментом є відповідальність держави за кібердії, здійснені з їхньої території.

Водночас, дискусійними залишаються випадки проведення операцій «під фальшивим прапором». На думку експертів, мало які операції під фальшивим прапором можуть витримати перевірку. І хоча для громадськості було б більш прийнятним ідентифікувати конкретного винуватця, це не є необхідним, оскільки він є тільки виконавцем. Основна відповідальність лежить на державі-замовнику кібератаки.

Також багато дебатів ведеться щодо необхідності достатніх доказів, щоб переконати громадськість. Бажання мати високий ступінь упевненості у приписуванні кіберзлочину перед ужиттям заходів пов’язане з побоюваннями щодо потенційного ризику ескалації та бажанням уникнути непередбачуваних наслідків. Це також може спричинити непотрібні затримки. Слід відзначити, що за 30-річну історію кібератак не було жодного випадку ескалації. Крім цього, інструменти кібердипломатії можуть сприяти керованості таких ризиків [60].

Проблеми спільного визначення відповідальності. Існує кілька суттєвих проблем у проведенні спільного визначення відповідальності за кібератаки [61] (Рис. 3.5), перша з яких технічна невідповідність, тобто наявність у різних держав різних технічних можливостей, інструментів і методологій визначення відповідальності. З огляду на це, їхні системи та підходи можуть не завжди бездоганно узгоджуватися, що потенційно може призвести до прогалин або невідповідностей в аналізі визначення відповідальності.

Рис. 3.5. Проблеми спільного визначення відповідальності за кібератаки

Структури класифікації та обміну інформацією можуть впливати на співпрацю. Кожна країна має власні системи класифікації національної безпеки та обмеження на обмін конфіденційною розвідувальною інформацією. Це може обмежувати глибину та швидкість обміну інформацією, необхідною для комплексного визначення відповідальності. Іноді через проблеми з класифікацією держави не можуть повноцінно обмінюватися критичними технічними показниками або джерелами розвідувальної інформації.

Різні правові структури впливають на те, як можна збирати та використовувати докази. Держави функціонують за різними правовими системами з різними стандартами щодо цифрових доказів, захисту конфіденційності та вимог допустимості, що ускладнює зусилля щодо побудови юридично обґрунтованих справ про визначення відповідальності, які б мали право на існування в юрисдикціях різних держав.

Політичні міркування іноді створюють різні пріоритети. Хоча держави-партнери поділяють занепокоєння щодо кібероперацій, вони можуть мати різні

дипломатично чутливі питання щодо приписування атак іншим державним суб'єктам, а також різний рівень готовності приписувати атаки публічно.

Ризики операційної безпеки зростають зі спільним приписуванням. Координація між двома країнами за своєю суттю збільшує кількість залучених людей і систем, створюючи більше потенційних точок компрометації. Це може ускладнити підтримку операційної безпеки під час розслідувань конфіденційної атрибуції. Залучені держави можуть мати різні терміни та пороги того, коли вони почуваються достатньо впевнено, щоб робити заяви про атрибуцію. Один партнер може віддати перевагу швидшому публічному приписуванню, тоді як інший захоче отримати більше переконливих доказів, перш ніж робити заяви.

3.4 Кіберситуаційна обізнаність у боротьбі з кіберопераціями

Спільний підхід до кіберситуаційної обізнаності у процесі запобігання і протидії кібератакам з боку держав вимагатиме від усіх учасників розробки процесів і узгоджених стандартів координації комунікації в реальному часі, прийняття більш своєчасних і обґрунтованих рішень, а також вжиття проактивних заходів для захисту цифрових активів та інфраструктури від кіберзагроз.

Як показало дослідження, для забезпечення кіберситуаційної обізнаності необхідно володіти інформацією різних видів, зібраної в результаті комплексу послідовних і безперервних заходів (Рис. 3.6).

Рис. 3.6. Джерела даних для забезпечення кіберситуаційної обізнаності

По суті, кіберситуаційна обізнаність поєднує три фундаментальні виміри: отримання знань про те, що відбувається в цифровому середовищі; розуміння та здатність пояснити, чому ці події відбуваються; оцінку того, який вплив ці події можуть мати на національну безпеку, економічну стабільність і громадську безпеку [62].

Цей процес вимагає складних методологій збору даних, передових аналітичних рамок і добре організованих систем управління інформацією. Найголовніше, що для встановлення кіберситуаційної обізнаності між країнами-партнерами має бути досягнута згода щодо протоколів обміну інформацією, процедур розподілу завдань і засад визначення пріоритетів, використовуючи існуючу систему спільних зусиль.

Інфраструктура збору даних і розвідки. Формування ефективної кіберситуаційної обізнаності спочатку вимагає створення можливостей для збору та обміну сукупними даними з різних джерел, зокрема урядових мереж, секторів критичної інфраструктури (наприклад, енергетики, фінансів, охорони здоров'я, транспорту й водопостачання), приватних компаній, академічних установ і розвідки з відкритих джерел. Дані слід обробляти для виявлення зловмисних дій, а також розуміння тактики і методів різних зловмисників, зокрема держав і кіберзлочинних груп та ідеологічно мотивованих хактивістів, які нерідко виступають у ролі виконавців урядових замовлень на кібернапади.

У контексті формування інфраструктури збору даних для кіберситуаційної обізнаності вартим уваги прикладом є діяльність Європейського агентства з кібербезпеки ENISA, яке забезпечує інформаційний обмін між мережею груп CSIRT, Європейською мережею організацій щодо кіберкризової взаємодії (EU-CyCLONe), Міжінституційною робочою групою з кіберкриз і співпрацює з багатьма іншими службами, серед яких Служба кібербезпеки для суб'єктів Союзу (CERT-EU), Європейський центр боротьби з кіберзлочинністю (EC3) при Європолі тощо.

У сфері ситуаційної обізнаності ENISA також керує Програмою кіберпартнерства та використанням обміну інформацією з постачальниками

засобів безпеки та організаціями з кібербезпеки, що не входять до ЄС. Для забезпечення своєчасної та точної кіберситуаційної обізнаності не лише для ENISA, але й для інших організацій та держав-членів, ENISA розробила та керує відкритою системою кіберситуаційної обізнаності OpenCSAM) на базі ШІ, яка обробляє щоденні обсяги даних та надає узагальнену і актуальну інформацію щодо кіберзагроз [63].

Інструменти штучного інтелекту. Інструменти ШІ можуть покращити кіберситуаційну обізнаність, обробляючи та аналізуючи величезні обсяги даних, пов'язаних з безпекою, зі швидкістю та масштабами, що перевищують людські можливості. Це дозволить державам отримати більш повне розуміння свого стану безпеки та розвитку ландшафту загроз, а також спільно розробити алгоритми для виявлення закономірностей та аномалій у мережевому трафіку і поведінці користувачів, які можуть свідчити про зловмисну діяльність, з більшою точністю та швидкістю, ніж традиційні системи на основі правил.

ШІ також може автоматизувати частини процесу реагування на інциденти і покращити сканування вразливостей з їх пріоритезацією. Ефективне впровадження ШІ для цілей кіберситуаційної обізнаності вимагає поєднання спеціалізованих інструментів, що підтримуються кваліфікованими аналітиками безпеки, які можуть інтерпретувати дані ШІ для вжиття належних заходів.

Проактивний захист і прогнозування. Окрім простого реагування на безпосередні загрози, комплексна кіберситуаційна обізнаність охоплює аналіз тенденцій і закономірностей для прогнозування майбутніх кібератак і нових загроз, і має здійснюватися спільно усіма залученими країнами. Прогнозування є важливим для проактивного кіберзахисту, оскільки дозволяє вживати превентивні заходи, а не суто реактивних відповідей. Основа ефективної ситуаційної обізнаності спирається на надійні механізми обміну розвідданими та інформацією про кіберзагрози своєчасно, безпечно та дієво.

Спільні аналітичні стандарти. Створюючи інтегрований підхід до ситуаційної обізнаності, держави, які співпрацюють для протидії кіберзагрозам з боку інших держав, отримають суттєву користь від спільних аналітичних

критеріїв, розроблених для виявлення закономірностей, зв'язків і потенційних інцидентів у їхніх цифрових екосистемах. Ці аналітичні рамки можна інтегрувати з іншими джерелами розвідувальної інформації про загрози, щоб створити більш повне розуміння ландшафту загроз, з яким вони стикаються.

Згенерована інформація має містити як стратегічні зведення високого рівня для керівників вищої ланки, так і більш детальну, технічно зорієнтовану звітність для оперативних аналітиків. Для сприяння такій співпраці державам потрібно буде значно розширити існуючі канали зв'язку та розробити стандартизовані процеси обміну конфіденційною інформацією з кібербезпеки.

У разі відсутності необхідно створити національні інституції, які б забезпечували ситуаційну обізнаність технічній і нетехнічній аудиторії, надаючи своєчасну інформацію про загрози та проблеми кібербезпеки, а також загальні теми безпеки. Форми надання такої інформації можуть охоплювати, але не обмежуватися технічними сповіщеннями, рекомендаціями і звітами систем управління, щотижневими бюлетенями про вразливості й порадами щодо найкращих практик кібергігієни [62].

Будь-які узгоджені стандарти колективної роботи повинні встановлювати чіткі рекомендації щодо своєчасності, повноти та точності спільної інформації. У багатьох випадках обмін даними в режимі реального або майже реального часу є критично важливим для ефективного реагування на швидкозмінні кіберзагрози. Усі спільні дані повинні бути послідовно відформатовані та структуровані, щоб забезпечити ефективний міжвідомчий аналіз та спільні оборонні операції. Спільні зусилля повинні включати спільні стандарти щодо належного рівня деталізації, що підлягає обміну, балансуючи потребу в дієвій розвідці з законними занепокоєннями щодо захисту джерел та методів.

Ці стандарти та протоколи є критично важливими темами, які мають бути спільно розроблені та узгоджені органами кібербезпеки залучених до співпраці країн. Створення спільних стандартів для колективної кібербезпеки має враховувати своєчасність, щоб забезпечити швидкі захисні дії. Такі стандарти мають визначати конкретні часові рамки для обміну різними категоріями даних

про загрози, включаючи негайне повідомлення (протягом кількох хвилин) про критичні вразливості нульового дня й активні атаки на критичну інфраструктуру, а також 24-годинні вікна для менш термінової, але все ще значущої інформації про загрози.

Ця структура має включати протоколи, які автоматично прискорюють обмін інформацією під час кризових ситуацій, таких як широкомасштабні атаки. Крім того, країни-учасники повинні додатково інвестувати в сумісні канали безпечного зв'язку й автоматизовані системи обміну, які передають зашифровані дані у стандартизованих форматах з мінімальним втручанням людини, тим самим зменшуючи затримку між виявленням загрози та захисною реакцією.

Спільні стандарти також встановлюють мінімальні вимоги до даних для різних типів розвідки кіберзагроз, щоб дати повну картину спільної інформації. Ці вимоги повинні визначати, які технічні показники (наприклад, IP-адреси, сигнатури шкідливих програм та інфраструктура командування та управління) і контекстуальна інформація (моделі таргетування, методи противника і потенційний вплив) відносяться до різних категорій звітів про загрози.

Стандарти також мають уточнювати очікування щодо включення необроблених даних порівняно з аналітичними висновками, а також визначати обставини, за яких певні деталі можуть бути приховані через проблеми класифікації або захисту джерела. Для забезпечення належного впровадження країни-партнери повинні створити спільні механізми перегляду для періодичної оцінки повноти спільної розвідки та виявлення систематичних прогалин або зон для покращення практики обміну інформацією.

Крім того, для забезпечення точності звітності спільні стандарти мають розробити і впровадити суворі протоколи перевірки для спільного використання розвідувальних даних про кіберзагрози. Ці протоколи можуть охоплювати рейтинги достовірності для різних типів інформації, чіткі вимоги до джерел (з використанням спільного формату для посилань) і процедури для розмежування підтверджених фактів та аналітичних суджень, отриманих на основі цих фактів.

Країни-партнери повинні створити спільні технічні робочі групи для перевірки важливих технічних висновків, перш ніж вони розпочнуть серйозні захисні дії, зберігаючи при цьому можливість швидко обмінюватися чутливими до часу розвідувальними даними з відповідними застереженнями. Крім того, стандарти мають включати механізми зворотного зв'язку, які дозволять одержувачам повідомляти про практичність і точність наданих розвідувальних даних, створюючи цикл постійного вдосконалення. Цей акцент на точності має бути збалансований з вимогами до своєчасності через встановлені процедури обміну попередніми даними з чіткими маркерами невизначеності, а потім більш ретельно перевірені оновлення, коли з'являються додаткові підтвердження.

Стратегічне значення кіберситуаційної обізнаності. У сучасному взаємопов'язаному цифровому просторі будь-які країни фактично мають спільний кордон у кіберпросторі, що робить покращений обмін розвідувальними даними не лише корисним, але й необхідним для взаємної оборони. Створюючи комплексну систему для кіберситуаційної обізнаності, усі зацікавлені країни можуть покращити свою колективну здатність виявляти, аналізувати і реагувати на складні кіберзагрози з боку конкуруючих держав, націлені на їхні спільні стратегічні інтереси і критичну інфраструктуру.

Окрім протидії конкретним загрозам, співпраця у сфері кіберситуаційної обізнаності передбачає обмін широким спектром інформації та передовим досвідом щодо управління кіберкризами, забезпечення стійкості критичної інфраструктури та розробки політики, пов'язаної з новими технологіями. Незважаючи на існування таких проблем, як різне сприйняття загроз і труднощі у спільному впровадженні активного кіберзахисту, співпраця між різними країнами та формування спільної обізнаності у галузі кібербезпеки має бути спрямована на глибшу інтеграцію шляхом проактивного реагування.

Узагальнені рекомендації щодо протидії кібероперaціям за підтримки національних держав представлені у таблиці 3.1.

Таблиця 3.1.

Рекомендації щодо протидії кібероперацiям за підтримки національних держав

Міжнародний рівень	**Національний рівень**	**Корпоративний рівень**
Удосконалення міжнародної нормативно-правової бази кібербезпеки, стандартів безпеки	Розробка і впровадження національних стратегій і політик кібербезпеки з урахуванням кіберзагроз з боку держав	Розробка і впровадження корпоративних стратегій і політик кібербезпеки
Забезпечення обміну розвідданими з подальшими діями щодо запобігання і протидії кіберзлочинам	Формування нормативно-правової бази в галузі кібербезпеки, зокрема щодо підзвітності й переслідування кіберзлочинців	Участь у приватно-державному партнерстві в галузі кібербезпеки і протидії державним атакам зокрема
Спільна атрибуція держав-винуватців кібератак з їх подальшим притягненням до відповідальності	Підвищення кіберстійкості об'єктів критичної інфраструктури і національних/урядових мереж	Формування кіберобізнаності і культури кібербезпеки на корпоративному рівні
Реалізація міжнародних програм у галузі кібербезпеки і протидії кіберзлочинності	Посилення державно-приватного партнерства, зокрема в напрямку досягнення спільної кіберобізнаності й ефективного кіберзахисту	Забезпечення ефективного поглибленого кіберзахисту компанії як чинника запобігання кібератакам, спонсорованим державами, в тому числі реалізація нормативних, організаційних, програмно-технічних і етичних заходів
Кібердипломатія, зокрема з метою формування міжнародних норм відповідальної поведінки держав у кіберпросторі	Участь у міжнародній співпраці в галузі кібербезпеки і протидії кіберзлочинності, в тому числі спонсорованої державами	
Розробка стратегій впровадження технологічних інновацій з урахуванням вимог кіберзахисту	Розробка і впровадження стратегій поглибленого технологічного захисту для об'єктів критичної інфраструктури і національних мереж	
Просування ідей кіберобізнаності і розвитку культури кібербезпеки на глобальному рівні	Участь у спільній діяльності держав щодо відстеження та ідентифікації винуватця кібератаки (кібератрибуції)	
	Просування ідей кіберобізнаності і розвитку культури кібербезпеки на національному рівні	

Висновки до розділу 3

Дослідження показало, що стратегії кібербезпеки для захисту від кібератак з боку держав-противників мають відображати багатогранний підхід до кібербезпеки, який враховує як соціально-політичні реалії країни, геополітичну ситуацію і технологічні виклики. Ефективні стратегії мають поєднувати надійну національну стратегію і політику кібербезпеки; міцну нормативно-правову базу; заходи з посилення кіберстійкості; ефективне державно-приватне партнерство; багатовекторну міжнародну співпрацю для протидії транскордонним кіберзагрозам, тому числі обмін розвідувальними даними, боротьба з кіберзлочинністю, встановлення держав-винуватців кібератак, зусилля з кібердипломатії; застосування технологічних інновацій (ШІ, МН, квантові обчислення, блокчейн-технології); формування обізнаності й навчання з кібербезпеки; сприяння розвитку культури кібербезпеки.

Для ефективного захисту від кібератак, що спонсоруються державами, необхідно проводити комплекс заходів технологічного захисту, який охоплює проактивну оцінку ризиків і розвідку кіберзагроз; впровадження надійних практик кібергігієни і архітектури поглибленого захисту; сегментацію мережі і безперервний моніторинг і виявлення загроз; розробка і регулярне тестування планів реагування на інциденти, посилення безпеки ланцюга поставок; міжнародне технологічне партнерство та обмін інформацією тощо.

Встановлено, що важливим чинником протидії кібероперація м за підтримки національних держав є кібератрибуція – процес відстеження та ідентифікації винуватця кібератаки з метою його подальшого притягнення до відповідальності. Водночас, незважаючи на постійні зусилля з боку держав і міжнародної спільноти, проведення спільного визначення відповідальності за кібератаки стикається з низкою проблем, серед яких невідповідність технічних можливостей і нормативної бази, різниця в політичних позиціях держав, зростання ризиків операційної безпеки внаслідок спільних дій з атрибуції.

Процесі запобігання і протидії кібератакам з боку держав-конкурентів вимагають спільного міждержавного підходу до формування кіберситуаційної обізнаності щодо агресивних дій у кіберпросторі, зокрема розробки узгоджених стандартів координації комунікації в режимі реального часу, прийняття більш своєчасних та обґрунтованих рішень, а також вжиття проактивних заходів для захисту цифрових активів та інфраструктури від кіберзагроз.

Як показало дослідження, для забезпечення кіберситуаційної обізнаності необхідно забезпечити збір інформації про те, що відбувається в цифровому середовищі; розуміння та здатність пояснити, чому ці події відбуваються; оцінку того, який вплив ці події можуть мати на національну безпеку, економічну стабільність і громадську безпеку. Створюючи комплексну систему кіберситуаційної обізнаності, усі зацікавлені країни можуть покращити свою колективну здатність виявляти, аналізувати та реагувати на складні кіберзагрози з боку конкуруючих державних суб’єктів, націлені на їхні спільні стратегічні інтереси і системи критичної інфраструктури.

ВИСНОВКИ

Дослідження показало, що кібератаки за підтримки держав виникли і реалізуються зараз з метою здійснення розвідки і шпигунства, саботажу, маніпулювання даними і завдання шкоди віртуальним і матеріальним активам, пропаганди, отримання економічної вигоди і стратегічної переваги. Зазвичай вони є ключовими компонентами ширших геополітичних стратегій держав, які прагнуть перевершити суперників або досягти стратегічно важливих цілей.

Встановлено, що кібератаки, які спонсоруються державою, мають глибокі наслідки, які зачіпають багато сфер і охоплюють загрози національній безпеці, деструктивний економічний вплив, загострення геополітичної напруженості, дипломатичні конфлікти між різними міжнародними суб’єктами, посилення гонки озброєнь та мілітаризацію кіберпростору, вплив на цивільне населення, порушення міжнародних норм і засад управління цифровим середовищем, загрози демократичним цінностям.

Результати аналізу засвідчили, що види кібероперацій з ініціативи держав можна класифікувати за такими критеріями: природою нападу (отримання несанкціонованого доступу, шпигунство; порушення інформаційних процесів і функціонування кіберінфраструктури; пошкодження/виведення з ладу фізичної інфраструктури, людські жертви); метою деструктивного впливу (вплив на цивільне населення; загрози національній безпеці; пошкодження/руйнування критичної інфраструктури; вплив на процеси прийняття рішень).

З’ясовано, що об’єктами кібератак, які підтримуються державами, є: цивільні й урядові ІКТ; системи управління критичною інфраструктурою і національною безпекою, зокрема розвідувальні і військові системи; системи ядерного командування, управління та зв'язку (NC3).

У кібератаках за сприяння держав використовуються різноманітні тактики і методи, серед яких розгортання шкідливого ПЗ, експлойти нульового дня, APT- і DDoS-атаки, атаки на ланцюги постачання, інформаційні операції,

атаки із залученням інсайдерів, методи соціальної інженерії і кібершпигунства, криптоджекінг, технології ШІ та МН, супутникове втручання тощо.

Дослідження показало, що у період 2000-2025 рр. було зафіксовано 4115 політично мотивованих кібератак у всьому світі, скоєних понад 900 відомими суб'єктами. Лідерство у здійсненні кібератак утримують Китай (майже 12% політично мотивованих кібератак), Росія з майже аналогічною часткою (11,6%), Іран (5,3%) і Північна Корея (4,7%). Основними цілями для зловмисників є США, Німеччина та Індія. Уряд, дослідницькі й академічні кола, фінансові установи і телекомунікації найчастіше є мішенню для кібератак.

Встановлено, що кіберактивність держав була зосереджена навколо місць активних військових конфліктів або регіональної напруженості; переважали кібератаки на країни, які розміщені у зоні геополітичного впливу держав-агресорів; зросли масштаби використання програм-вимагачів і ботнетів. Кіберзусилля національних акторів охоплювали насамперед кібершпигунство й розвідку, крадіжки даних і ураження об’єктів критичної інфраструктури.

Основними тенденціями розвитку злочинної кіберактивності держав є конвергенція з фінансово мотивованою кіберзлочинністю; перехід від традиційних розвідувальних операцій до деструктивних кібератак; концентрація кібератак національних держав у регіонах, які становлять для них геополітичний інтерес; зростання обсягу кібератак на ланцюги постачань; використання ШІ й інших передових технологій для покращення кібероперацій.

Аналіз засвідчив, що основні напрями кібердіяльності Китаю охоплюють шпигунство, викрадення інтелектуальної власності і стеження, які спрямовані проти урядів і секторів охорони здоров'я, технологій і зв’язку. Китай активно використовує хакерство і дезінформаційні кампанії в соціальних мережах.

Встановлено, що РФ здебільшого використовує кібероперації проти держав для збору розвідувальних даних часто з використанням шкідливих програм та інструментів, придбаних на злочинних ринках. Основною ціллю російських кібератак упродовж останніх років була Україна, а кібератаки насамперед мали на меті переривання або виведення з ладу критичних сервісів,

збої в роботі офіційних джерел інформації, викрадення або знищення даних, поширення дезінформації, дискредитацію влади і залякування населення.

Іран проводить операції з використанням програм-вимагачів і руйнівні операції зі злому та витоку інформації. Крім того, деякі кібератаки від імені іранського уряду були ідентифіковані як випадки фінансово мотивованих вторгнень. Окрема слід відзначити дезінформаційні та пропагандистські операції впливу Ірану у соцмережах, спрямовані на Ізраїль і його союзників.

Дослідження показало, що, КНДР сьогодні є світовим лідером у викраденні криптовалюти. Північна Корея усе частіше використовує кібератаки для фішингу й ураження ланцюгів постачання ПЗ, а також спроб підірвати партнерство між США, Японією та Південною Кореєю.

З’ясовано, що держави можуть проводити кібероперації через свої служби безпеки та іноземні розвідувальні служби або шляхом залучення кіберзлочинних груп, які є високоорганізованими структурами і займаються довгостроковим шпигунством, викраденням даних і саботажем, переважно з метою отримання фінансової вигоди.

Встановлено, що стратегії кібербезпеки для захисту від кібератак з боку держав-противників мають поєднувати надійну національну стратегію і політику кібербезпеки; міцну нормативно-правову базу; заходи з посилення кіберстійкості; ефективне державно-приватне партнерство; багатовекторну міжнародну співпрацю для протидії транскордонним кіберзагрозам, тому числі обмін розвідувальними даними, боротьба з кіберзлочинністю, встановлення держав-винуватців кібератак, зусилля з кібердипломатії; застосування технологічних інновацій; формування обізнаності й навчання з кібербезпеки; сприяння розвитку культури кібербезпеки.

Для ефективного захисту від кібератак, що спонсоруються державами, необхідно проводити комплекс заходів технологічного захисту, який охоплює проактивну оцінку ризиків і розвідку кіберзагроз; впровадження надійних практик кібергігієни і архітектури поглибленого захисту; сегментацію мережі і безперервний моніторинг і виявлення загроз; розробка і регулярне тестування

планів реагування на інциденти, посилення безпеки ланцюга поставок; міжнародне технологічне партнерство та обмін інформацією тощо.

Встановлено, що важливими чинниками протидії кібероперація м за підтримки національних держав є кібератрибуція – процес відстеження та ідентифікації винуватця кібератаки з метою його подальшого притягнення до відповідальності, і формування кіберситуаційної обізнаності через збір інформації про те, що відбувається в цифровому середовищі; розуміння та здатність пояснити, чому ці події відбуваються; оцінку того, який вплив ці події можуть мати на національну безпеку, економічну стабільність і безпеку.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Gary D Brown. State Cyberspace Operations Proposing a Cyber Response Framework. *Royal United Services Institute for Defense and Security Studies.* 2020. URL: https://static.rusi.org/rusi_pub_184_op_strategic_military_operations_final_web_version.pdf

2. Looking back: Operation Buckshot Yankee & agent.btz. *Netsurion*. URL: https://www.netsurion.com/articles/looking-back-operation-buckshot-yankee-agent-btz

3. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. *United Nations. General Assembly*. 22 July 2015. URL: https://docs.un.org/en/A/70/174

4. Brendan I. Koerner. Inside the Cyberattack That Shocked the US Government. Oct 23, 2016. *Wired*. URL: https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/

5. What is the Mirai Botnet? *Cloudflare*. URL: https://www.cloudflare.com/learning/ddos/glossary/mirai-botnet.

6. Jerry Sanchez. The Sony Pictures Breach: A Deep Dive into a Landmark Cyber Attack. October 15, 2025. *Frameworksecurity*. URL: https://frameworksecurity.com/post/the-sony-pictures-breach-a-deep-dive-into-a-landmark-cyber-attack

7. What is Stuxnet? *Malwarebytes*. URL: https://www.malwarebytes.com/stuxnet

8. Andrii Bezverkhyi. Petya.A / NotPetya is an AI-powered cyber weapon, TTPs lead to Sandworm APT group. *Socprime*. URL: https://socprime.com/blog/petya-a-notpetya-is-an-ai-powered-cyber-weapon-ttps-lead-to-sandworm-apt-group/

9. State-Backed Cyber Attacks: Insights and Solutions. *Searchinform*. URL: https://searchinform.com/articles/cybersecurity/cyber-threats/cyber-attacks/state-sponsored-cyber-attacks/

10. Elizabeth Mohn. Stuxnet. *EBSCO Knowledge Advantage*. 2023. URL: https://www.ebsco.com/research-starters/computer-science/stuxnet

11. Christopher A Nissen et al. Deliver Uncompromised: A Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War. *Mitre*, 2018. URL: https://www.dni.gov/files/NCSC/documents/supplychain/20190327-Deliver-uncompromised.pdf

12. Michael Mcguire. Nation states, cyberconflict and the web of profit. University of Surrey. 2021. URL: https://threatresearch.ext.hp.com/wp-content/uploads/2021/04/hp-bps-web-of-profit-report_APR_2021.pdf

13. Agata Małecka. Non-State Actors in Nation-State Cyber Operations *Rocznik Bezpieczeństwa Międzynarodowego*. 2024, vol. 18, nr 1. URL: https://bibliotekanauki.pl/articles/55995775.pdf

14. Jerry M. Couretas. Nation-State Cyber Operations. *Cyber Operations: A Case Study Approach*, Wiley, 2024, pp.61-73, doi: 10.1002/9781119712121.ch4.

15. What are C2 Frameworks? The Foundation of Cyberattacks. Nov 4, 2024. URL: https://hunt.io/glossary/c2-frameworks-explained

16. Falco, Gregory. When Satellites Attack: Satellite-to-Satellite Cyber Attack, Defense and Resilience. November 16-18, 2020, Virtual Event. URL: https://www.researchgate.net/publication/340335070_When_Satellites_Attack_Satellite-to-Satellite_Cyber_Attack_Defense_and_Resilience

17. What is Cyber Espionage? Types & Examples. *Sentinelone*. URL: https://www.sentinelone.com/cybersecurity-101/threat-intelligence/cyber-espionage/

18. Cyber Threats and Advisories. *CISA*. URL: https://www.cisa.gov/topics/cyber-threats-and-advisories

19. NSA Cybersecurity Advisories & Guidance. NSA. URL: ttps://www.nsa.gov/Press-Room/Cybersecurity-Advisories-Guidance/

20. Cyber Threats. *ENISA*. URL: https://www.enisa.europa.eu/topics/cyber-threats

21. State of Cybersecurity 2025 report. *ISACA*. URL: https://www.isaca.org/resources/reports/state-of-cybersecurity-2025

22. OWASP Top Ten 2025. *OWASP*. URL: https://owasp.org/www-project-top-ten/

23. Microsoft Threat Analysis Center. *Microsoft*. URL: https://www.microsoft.com/en-us/corporate-responsibility/customer-security-trust/microsoft-threat-analysis-cente

24. ESET Threat Report H1 2025. *ESET*. URL: https://www.eset.com/ee-ru/business/threat-report/

25. Cybersecurity Threats: How to Prioritize, Manage and Reduce Them. *Gartner*. URL: https://www.gartner.com/en/cybersecurity/topics/cybersecurity-

26. Repository of Cyber Incidents (EuRepoC). URL: https://www.swp-berlin.org/en/swp/about-us/organization/swp-projects/european-repository-on-cyber-incidents-eurepoc/

27. Anna Fleck. Who's Behind Cyber Attacks? Feb 23, 2024. *Statista*. URL: https://www.statista.com/chart/31805/countries-responsible-for-the-largest-share-of-cyber-incidents/

28. Anna Ribeiro. Hacktivists, state-sponsored groups step up cyberattacks targeting manufacturing operations and OT systems. *Industrialcyber*. June 02, 2025. URL: https://industrialcyber.co/manufacturing/hacktivists-state-sponsored-groups-step-up-cyberattacks-targeting-manufacturing-operations-and-ot-systems/

29. Cyber Operations Tracker. *Council on Foreign Relation USA*. URL: https://www.cfr.org/cyber-operations/#OurMethodology

30. Digital Defense Report 2024. *Microsoft*. URL: https://www.microsoft.com/en-us/security/security-insider/threat-landscape/microsoft-digital-defense-report-2024

31. Digital Defense Report 2025. *Microsoft*. URL: https://www.microsoft.com/en-us/corporate-responsibility/cybersecurity/microsoft-digital-defense-report-2025/

32. Global Cybersecurity Outlook 2025. Insight Report. January 2025. *World Economic Forum*. URL: https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf

33. James Coker. Top 5 Nation State Cyber-Attack Trends. 05 Feb 2025. *Infosecurity Europe*. URL: https://www.infosecurityeurope.com/en-gb/blog/threat-vectors/top-nation-state-cyber-attack.html

34. Aleksandar Milenkoski, Julian-Ferdinand Vögele. Cyberespionage groups attacking critical infrastructure with ransomware. June 2024. *SentinelLabs*. URL: https://assets.sentinelone.com/sentinellabs/chamelgang-friends-en

35. Jerry M. Couretas. Nation-State Cyber Operations. Cyber Operations: A Case Study Approach. *Wiley Data and Cybersecurity*. 2024. P. 61-73. URL: https://ieeexplore.ieee.org/document/10501976/metrics#metrics

36. Yimou Lee. Chinese cyberattacks on Taiwan government averaged 2.4 mln a day in 2024. January 6, 2025. *Reuters*. URL: https://www.reuters.com/technology/cybersecurity/chinese-cyberattacks-taiwan-government-averaged-24-mln-day-2024-report-says-2025-01-06/

37. Corrin Jones. Explaining the 2024 US Treasury Hack: What Happened? *Red River*. March 4, 2025. URL: https://redriver.com/cybersecurity/us-treasury-hacked

38. Копійка М. «Гостра сила» в стратегії інформаційної безпеки Китаю. *Міжнародні відносини, суспільні комунікації та регіональні студії*. Розділ II. Суспільні комунікації. 1(7), 2020 С.68-80.

39. Cybercrime: A Multifaceted National Security Threat. February 12, 2025. *Google Threat Intelligence Group.* URL: https://cloud.google.com/blog/topics/threat-intelligence/cybercrime-multifaceted-national-security-threat

40. Фещуков Г.В. Кібертероризм з боку держав на прикладі дій Китайської Народної Республіки (КНР) проти Китайської Республіки (Тайвань). Міжнародно-правовий аналіз таких дій. *Юридичний науковий електронний журнал.* 2023. 11. С. 682-684. URL: http://www.lsej.org.ua/11_2023/166.pdf

41. Dakota Cary. China's Covert Capabilities. Silk Spun From Hafnium. July 30, 2025. Sentinel Labs. URL: https://www.sentinelone.com/labs/chinas-covert-capabilities-silk-spun-from-hafnium/

42. Filip Talac. How State-Sponsored Cyber Attacks Are Reshaping National Security in 2025. 28 Feb, 2025. *QFI Risk Solutions.* URL: https://qfirisksolutions.com/media/blog/how-state-sponsored-cyber-attacks-are-reshaping-national-security-in-2025/

43. Використання Іраном кібероперацій впливу для підтримки ХАМАС. *Security Insider. Microsoft.* 2024. URL: https://surl.li/uswgti

44. Note by the President of the Security Council. United Nations. S/2024/215. 7 March 2024. URL: https://documents.un.org/doc/undoc/gen/n24/032/68/pdf/n2403268.pdf

45. States' use of cyber operations. Postnote Nr 684 October 2022. URL: https://www.icheme.org/media/19137/postnote-684-states-use-of-cyber-operations.pdf

46. ESET Research investigates the Gamaredon APT group cyberespionage aimed at high-profile targets in Ukraine and NATO countries. *ESET Research*. September 26, 2024. URL: https://surl.li/awdyer

47. Advanced persistent threats (APTs). *Google Cloud*. URL: https://cloud.google.com/security/resources/insights/apt-groups

48. Tanvir Hassan, Zoha, Sifat-Nur-Billah. The Implications of State-sponsored Cyber Attacks in South Asian Countries. *International Journal of Chaotic Computing (IJCC)*. Volume 8. Issue 1. 2022. P. 204-208. URL: https://surl.li/ivtlzh

49. Azubuike, Callistus. Cyber Security and International Conflicts: An Analysis of State-Sponsored Cyber Attacks. 2023. 9. P.101-114. URL: https://surl.li/mcvuoz

50. State sponsored cyber warfare. *Identity Management Institute. Center for Identity Governance.* URL: https://identitymanagementinstitute.org/state-sponsored-cyber-warfare/

51. Krishna Yadav. Cybersecurity and National Sovereignty: Challenges in the Digital Age. *International Journal of Social Science Research (IJSSR).* Volume 1, Issue 1. 2024. P. 1-14. URL: https://www.ijssr.com/wp-content/uploads/journal/published_paper/volume-1/issue-1/IJSSR25204.pdf

52. Julia Brock, James Andrew Lewis. Mutual Defense in Cyberspace: Joint Action on Attribution. *Center for Strategic & International Studies.* September 17, 2025. URL: https://www.csis.org/analysis/mutual-defense-cyberspace-joint-action-attribution

53. Global Cybersecurity Index 2024. *ITU Publications*. URL: https://www.itu.int/epublications/publication/global-cybersecurity-index-2024

54. Тєтєвін М.С. Досвід України в галузі міжнародного співробітництва в галузі кібербезпеки. *Науковий вісник Ужгородського Нац. Університету*. 2024. Серія ПРАВО. Випуск 82: частина 3. С. 263-266. https://visnyk-juris-uzhnu.com/wp-content/uploads/2024/05/43-2.pdf

55. Martti Lehto. National Cyberspace and Cyber Operations. *The Defence Horizon Journal*. December 2, 2024. URL: https://tdhj.org/blog/post/cyberspace-cyber-operations/

56. 2025 Threat Landscape Report. *Cognyte.* 2025. URL: https://engage.cognyte.com/s/c8036aeb/?page=2

57. State-Backed Cyber Attacks: Insights and Solutions. *Searchinform* URL: https://searchinform.com/articles/cybersecurity/cyber-threats/cyber-attacks/state-sponsored-cyber-attacks/

58. Defending Against State-Sponsored Cyberattacks in 2025. *ISA Global Security Alliance*. 2025. URL: https://gca.isa.org/blog/defending-against-state-sponsored-cyberattacks-in-2025.

59. Decoding State-Sponsored Cyber Attacks. How Nation-States Wage War in the Digital Age. *Configr Technologies*. 2024. URL: https://configr.medium.com/decoding-state-sponsored-cyber-attacks-2f23f64ee439

60. Nicholas Tsagourias Cyber Attribution Agencies: A Sceptical View. *Questions of International Law*. Jul 31, 2024. URL: https://www.qil-qdi.org/cyber-attribution-agencies-a-sceptical-view/

61. Hal Berghel. On the Problem of (Cyber) Attribution. *IEEE Computer Society*. 2017. URL: http://www.berghel.net/col-edit/out-of-band/mar-17/oob_3-17.pdf

62. Julia Brock, James Andrew Lewis. Criteria for Cyber Security Awareness. *Center for Strategic & International Studies.* May 22, 2025. URL: https://www.csis.org/analysis/criteria-cyber-situational-awareness

63. Situational Awareness. *ENISA*. URL: https://www.enisa.europa.eu/topics/cyber-threats/situational-awareness