МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ВАСИЛЯ СТУСА

**САВЧУК АЛІНА ВАЛЕНТИНІВНА**

Допускається до захисту:
в.о. завідувача кафедри
міжнародних
відносин і зовнішньої політики,
д-р економічних наук, доцент
_____ В. В. Лимар
«____»_____ 20__ р.

# КІБЕРБЕЗПЕКА В СИСТЕМІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

Спеціальність 291 Міжнародні відносини, суспільні комунікації та регіональні студії

**Кваліфікаційна (бакалаврська) робота**

Керівник:
Богінська І. В.,
кандидат історичних наук, доцент

Оцінка:_____/ _____/ _____

(бали за шкалою ЄКТС/за національною шкалою)

Голова ЕК:_____

(підпис)

Вінниця-2022

## АНОТАЦІЯ

**Савчук А. В. Кібербезпека в системі національної безпеки України.** Спеціальність 291 «Міжнародні відносини, суспільні комунікації та регіональні студії», спеціалізація «Міжнародні відносини», Донецький національний університет імені Василя Стуса, Вінниця, 2022.

У кваліфікаційній (бакалаврській) роботі досліджено становлення кібербезпеки України від початку її формування як окремої галузі безпеки. Показано процеси, що відбуваються в українському кіберпросторі в умовах російсько-української війни. Встановлено значення кібербезпеки в системі національної безпеки держави.

Ключові слова: кібербезпека, національна безпека, Україна, Російська Федерація, війна.



## ABSTRACT

**Savchuk A. Cybersecurity in the system of national security of Ukraine.** Specialty 291 "International Relations, Public Communications and Regional Studies". Vasyl` Stus Donetsk National University, Vinnytsia, 2022.

In the qualification (bachelor's) work researched the formation of cybersecurity of Ukraine from the beginning of its becoming as a separate security sector. Shown the processes, that take place in the Ukrainian cyberspace in the conditions of the Russian-Ukrainian war. Installed the importance of cybersecurity in the national security system of the state

Keywords: cybersecurity, national security, Ukraine, Russian Federation, war.

**ЗМІСТ**

# ВСТУП

Внаслідок швидкого розвитку технологічних можливостей людства майже всі сфери людського життя пов’язані з кіберпростором. Держави активно переорієнтовуються на використання інформаційно-комунікаційних технологій, створюючи нову інформаційну інфраструктуру. Вирішення проблем інформаційної безпеки сильно пов’язане з захистом національного інформаційного простору, підвищенням ролі інтелектуальної власності та розвитком інформаційно-комунікаційної системи для забезпечення державної інформаційної політики.

**Актуальність теми дослідження** обґрунтовується необхідністю суттєвого покращення становища України у кіберпросторі, яке допоки визначається як нестабільне і вразливе. Законодавство у цій галузі хоч і удосконалюється, проте все ще не здатне само по собі захистити український інформаційний простір належним чином. Кіберзлочини не є рідкісним явищем. З початком військової агресії Російської Федерації Україна почала все частіше відчувати на собі наслідки недосконалості системи національної кібербезпеки внаслідок кібератак на стратегічно-важливі об’єкти української інфраструктури. Хакерські групи, що підконтрольні владі Російської Федерації, постійно розробляють нові та ще більш небезпечні віруси і шкідливе програмне забезпечення, яке згодом тестується на території України.

Українська влада в свою чергу не може забезпечити попередження цих загроз своєчасно через відсутність чіткої системи інфраструктури кіберзахисту та конкретного плану дій у критичних ситуаціях. Таким чином, реагування на кіберзлочини відбувається уже після їх вчинення, замість запобігання. Зміцнення кібербезпеки України стає ще більш нагальною потребою з огляду на перехід України в режим безпаперового документообігу. За таких умов, ще більше стратегічно важливої інформації, персональних даних громадян знаходиться в цифровому просторі, а отже потребують захисту від їх ушкодження чи викрадення.

На сьогоднішній день кібербезпека присутня майже у всіх сферах життя людини та держави, тому будь-які недоліки в системі безпеки згодом призведуть до проблем у функціонуванні держави. Для процесу державотворення найнебезпечнішим є поширення конфіденційної інформації держструктур.

**Мета роботи -** з'ясувати характер змін у кіберпросторі та їх вплив на функціонування держави.

Відповідно до поставленої мети в дослідженні виконано такі **завдання:**

- окреслити особливості кіберпростору як предмету політичної науки;
- встановити сутність і роль кібербезпеки в політичному дискурсі;
- описати наявні механізми забезпечення кібербезпеки України;
- проаналізувати шлях формування та розвитку системи кіберзахисту України;
- дослідити кейси злочинної діяльності Російської Федерації в українському кіберпросторі в умовах війни;
- обґрунтувати необхідність міжнародної співпраці для ефективного захисту цифрового середовища.

**Об'єктом** дослідження є національна безпека України.

**Предметом** дослідження є процес удосконалення системи кібербезпеки України на фоні вторгнення Російської Федерації.

**Теоретична або практичне значення одержаних результатів -** робота дає поштовх до подальшого дослідження явища війни в кіберпросторі, трансформації інструментів боротьби в цифровому просторі, відношення кіберпотужностей до інформаційної війни, зміни впливу кіберзахисту на політичні процеси, спостереження за удосконаленням системи кіберзахисту України, аналізу її сильних та слабких сторін в результаті імплементації нових законодавчих документів.

**Апробація результатів дослідження –** Вісник студентського наукового товариства Донецького національного університету імені В. Стуса, Том 1 № 14 (2022) – «Кібератаки Російської Федерації: реакція міжнародної спільноти»; Вісник студентського наукового товариства Донецького національного університету імені В. Стуса, Том 2 № 13 (2021) – «Пріоритет держави у кіберпросторі: атака чи захист?»; VI Міжнародна науково-практична конференція студентів, аспірантів і молодих учених “Topical issues of humanities, technical and natural sciences” – “The notion of cyber war in international relations”.

**Структура кваліфікаційної (бакалаврської) роботи –** робота містить в собі 7 основних частин з відповідним наповненням: вступ, 3 основних розділи, кожен з яких має свої підрозділи, висновки, список використаних джерел та додатки.

Перший розділ присвячений теоретичним питанням, що стосуються значення кіберпростору і його вплив на політику та державотворчі процеси. Другий розділ в свою чергу містить опис процесу становлення системи українського кіберзахисту, проблеми в середовищі поточної політики та окреслені основні її недоліки. У третьому розділі розглядаються шляхи підтримки України міжнародними партнерами в обставинах повномасштабної війни та що власне спонукає їх до дій.

Висновки узагальнюють результати дослідження, а додатки відображають більшою мірою теоретичні аспекти та візуалізують статистичні дані.

Загальний обсяг роботи – 58 сторінок.

# РОЗДІЛ 1. КОНЦЕПТУАЛІЗАЦІЯ КІБЕРБЕЗПЕКИ У МІЖНАРОДНО-ПОЛІТИЧНІЙ СФЕРІ

## 1.1. Кіберпростір як предмет політичної науки

Інтернет – це величезна мережа, яка об’єднує комп’ютери по всьому світу. Ми живемо в епоху, коли всі залежні від нього. Технології розвиваються з кожним днем, а на ринку з’являється все більше новітніх винаходів, пов'язаних з машинами та комп'ютерами.

Кіберпростір є електронним засобом спілкування через Інтернет та обміну даними – саме таким чином це поняття розуміється для пересічної людини. Проте насправді визначення кіберпростору можна окреслити багатьма способами і науковці не можуть прийти до одностайної думки з приводу трактування. Найбільш загальним і простим способом він розглядається як взаємозалежна мережа інфраструктур інформаційних технологій, що включає Інтернет, телекомунікаційні мережі, комп'ютерні системи [25].

Політика у світі зараз стосується і технічних, а не чисто політичних питань. Останніми роками питання кіберпростору, включаючи кібербезпеку, свободу Інтернету та управління, швидко стали «політизованими» і стали природною глобальною суспільною проблемою. Натомість в рамках політики поняття кіберпростору включає набагато більше аспектів, де технічні особливості стають менш критичними. Тому, в рамках цієї роботи наступне визначення вбачається більш доречним - середовище, що виникає в результаті взаємодії людей, програмного забезпечення та послуг в Інтернеті за допомогою підключених до нього технологічних пристроїв і мереж, яке не існує ні в якій фізичній формі. Виходячи з подібного визначення, Д. Кюль, розглядаючи різні елементи кіберпотужностей, звертає увагу на наступні речі [55]:

• діяльність, з метою впливу в кіберпросторі включає Інтернет, а також радіо, телебачення, засоби зв'язку, такі як мобільні телефони, і програми для всіх;

• кібервійськова діяльність включає операції, орієнтовані на мережу, атаки та використання комп'ютерних мереж, операції геополітичного впливу та безпеку;

• кібербезпека включає не тільки технічні проблеми, такі як віруси та атаки з відмовою в обслуговуванні, а й проблеми людського походження — наприклад, недобросовісні наміри, обман чи звичайні помилки.

Можна концептуалізувати кіберпростір у термінах багатьох рівнів діяльності, але просте перше наближення зображує його як унікальний гібридний режим фізичних та віртуальних властивостей [56]. Рівень фізичної інфраструктури слідує економічним законам конкуруючих ресурсів і збільшення граничних витрат, і політичним законам суверенної юрисдикції та контролю. Віртуальний або інформаційний рівень має характеристики економічної мережі, що підвищують віддачу від масштабу, а також політичні практики, які ускладнюють юрисдикційний контроль [30]. Атаки з інформаційної сфери, де витрати є низькими, можуть бути запущені проти фізичної сфери, де ресурси мізерні та дорогі. Але навпаки, контроль над фізичним рівнем може мати як територіальний, так і екстериторіальний вплив на інформаційний рівень.

У другій половині 20-го століття найбільш динамічні економіки світу — зокрема США, Японія, Південна Корея, Тайвань та значна частина ЄС — розробили програму політики для створення конкурентоспроможних секторів ІКТ. Рання політика була зосереджена на просуванні, захисті та підтримці складної вітчизняної виробничої промисловості для телекомунікаційного мережевого обладнання та компонентів. Багато інших країн, включаючи Китай, а також країни, що розвиваються в Південній та Південно-Східній Азії, Східній Європі та Латинській Америці, намагалися наслідувати цій стратегії. Основними мотивами такої політики є:

1. Військове застосування ІКТ: зокрема до 1990-х років рівень обчислювальної техніки країни вважався тісно пов'язаним з її потенціалом для розробки зброї.

2. Національна комунікаційна безпека: прагнення захистити внутрішні комунікації від перехоплення або порушення з боку сторонніх осіб — останнє стає все більш актуальним із зростанням залежності життєво важливої інфраструктури від ІКТ та зростанням складності кібератак.

3. Економічне зростання: з часом вплив сильного сектору ІКТ на інші частини економіки стає все більш очевидним.

Як політично актуальна проблема, кібербезпека розвивається на перетині між швидким технологічним розвитком, політичним і стратегічним використанням цих інструментів державними та недержавними суб’єктами, а також різними спробами держави, суспільства та приватного сектору визначити відповідні обов'язки, правові межі та прийнятні правила поведінки для цього простору [49].

Важливими ознаками політизації кіберсвіту є включення кібербезпеки до порядку денного. Свобода Інтернету є зовнішньополітичною зброєю, яку Сполучені Штати активно пропагували в останні роки, а теорія Інтернету як суспільного надбання є важливою теоретичною основою для зміцнення цієї концепції міжнародних відносин. Оскільки проблеми з кібербезпекою посилилися, а політика США щодо свободи Інтернету була реалізована, ризики кіберпростору поступово стали серйозною перешкодою для взаємної довіри та нормального обміну між країнами.

Проблема кіберпростору є актуальною глобальною суспільною проблемою. Дослідження на такі теми, особливо теоретичний аналіз, все ще стрімко розвиваються, але досі присутня чимала прірва між теорією і практикою. Взявши за приклад мережеву безпеку, люди по-різному тлумачать конотацію поняття мережевої безпеки і часто використовують його як синоніми з такими термінами, як комп’ютерна безпека, безпека мережі та інформаційна безпека [84].

## 1.2. Кіберзагрози та кібербезпека: суб'єкти та об'єкти

Сьогодні не лише державні, а й недержавні суб'єкти мають більше технічної майстерності, мотивації та фінансових ресурсів, ніж будь-коли раніше, щоб здійснювати руйнівні атаки на критичну інфраструктуру країни. Через пандемію кожна держава, підприємство та організація стали значною мірою залежними від технологій. Компанії та державні органи підтримують свою присутність в Інтернеті через веб-сайти, сторінки в соціальних мережах та блоги. Порушення безпеки є найбільшою загрозою у всіх подібних сценаріях [73]. Будь-яка атака на критичну інфраструктуру в одному секторі країни може призвести до збоїв і в інших секторах, наприклад, атака на телекомунікації країни може порушити електронні платежі [38].

Ключовою характеристикою кіберпростору є те, що він є загальнодоступним ресурсом. На даний момент обмежень у його використанні немає. З цієї причини кіберпростір є ресурсом подвійного призначення. З одного боку, це платформа для економічного розвитку, розширення ринку та обміну ідеями та інформацією. З іншого боку, він також використовується в далеко не респектабельних цілях. Це засіб для терористичних організацій координувати свою діяльність і залучати нових послідовників. Приклад ІДІЛ є дуже яскравою демонстрацією цього. Кіберпростір використовується недемократичними режимами для збору інформації про зовнішній світ, технології та знання або як платформа для впливу або нападу на окремі компанії чи цілі країни. Тобто, гравці не змінились: з одного боку – сучасні демократії, з іншого - авторитарні режими та терористичні організації, лише протистояння перейшло з фізичного світу в цифровий [85].

Кібербезпека стає все нагальнішим питанням після майже 20 років активних досліджень, розробок та практичних кейсів. Має місце відчуття, що проблема погіршується, а не покращується. Щоб розібратись у цьому, потрібно вийти за межі суто технічного дослідження кібербезпеки. Це правда, що технічні аспекти не менш важливі; але якщо поглянути на

проблему ширше, навіть якщо буде вирішено технічні проблеми, кібербезпека залишиться важким питанням з трьох причин [33]:

*1. Це не просто технічна проблема.* Вона включає аспекти економіки, людської психології та інших дисциплін. Сюди можна приписати величезну кількість речей. Але «людський фактор» визнано найслабшою ланкою у створенні безпечного цифрового середовища та користування ним. Кожен стикався з тим, що молодше покоління значно вправніше користується ІКТ ніж люди старшого віку. Це також пояснює те, що молодь більш обізнана і частіше усвідомлює, що стала, наприклад, жертвою фішингу. Так, за результатами дослідження Стенфордського Університету 50% опитаних 18-30 років сказали, що вони робили помилки стосовно порушення правил особистої безпеки в кіберпросторі, проте лише 10% опитаних старше 51 року визнали цей факт [82].

*2. Законодавство, політика та практика щодо кібербезпеки ще не повністю розроблені.* Сьогодні багато людей використовують Інтернет для незаконних дій, таких як відмивання грошей та крадіжка особистих даних. Уряди створюють суворі закони для підвищення кібербезпеки з тією метою, щоб люди розумно використовували технології та уникали зловживання ними. Оскільки кіберпростір повністю відрізняється від фізичного світу, кібернетичні закони також відрізняються від традиційних [72].

Протягом останніх років було неодноразово закликано сформулювати закони і нормативні акти у відповідь на нові загрози міжнародній безпеці, які несуть інформаційні технології. Перший – це пропозиція прийняти в ООН договір, який має обов’язковий характер, два десятиліття тому. На жаль, враховуючи природу кіберзброї та прогрес розвитку технологій, така угода не підлягала верифікації, тому що могла швидко втратити актуальність. Натомість ООН створила Групу урядових експертів (GGE), яка у 2013 та 2015 роках розробила набір необов’язкових правил. У 2017 році група не змогла оприлюднити звіт, але її робота продовжилася в розширеному вигляді – Глобальна комісія зі стабільності в кіберпросторі. Вона визначає

стабільність мережі як стан, у якому люди та установи можуть бути впевнені, що вони мають можливість безпечно користуватися мережевими послугами, що зміни відбуваються відносно мирно, а конфлікти, що виникають, вирішуються без ескалації. Стабільність базується на існуючому міжнародному праві, яке також стосується кіберпростору [21].

Ці норми не обіцяють балансу в кіберпросторі, адже вони є лише початком, а шлях до врегулювання відносин на законодавчому рівні обіцяє бути тривалим. У довгостроковій перспективі принцип співробітництва між державами тут є основоположним, оскільки більшість питань, пов'язаних із діяльністю в інформаційному середовищі можуть бути вирішеними лише через співпрацю держав та міжнародних організацій [13].

*3.* П*равила кіберпростору відрізняються від правил фізичного світу.* Маються на увазі не соціальні «правила», а фізика та математика кіберпростору. Вузлова природа мережі означає, що такі поняття, як відстань, кордони та близькість, працюють по-різному, що має глибокі наслідки для безпеки. По-перше, при значному зменшенні відстані між вузлами (тобто окремими пристроями, наприклад, комп'ютерами) загрози можуть надходити буквально звідусіль і від будь-якого суб'єкта. По-друге, кордони в кіберпросторі не відповідають тим самим лініям, які існують в фізичному світі. Дехто розглядає кіберпростір як аналог некерованого беззаконного Дикого Заходу, але на практиці існує багато сфер приватного та державного управління.

Тому за однією з теорій, кіберпростір захищений від державного суверенітету. Цей простір не залежить від правил, які намагається нав'язати влада. Інформація більше не повністю контролюється державою, а люди взаємодіють через соціальні мережі в кіберпросторі [67]. У практичному військовому сенсі це означає, що існує великий потенціал впливу на появу та діяльність різних соціальних груп на території противника. Держава не має ні морального права, ні ефективних методів управління кіберпростором.

Противники цієї теорії стверджують, що кіберпростір не може бути захищеним від державної влади [52]. По-перше, кіберпростір потребує контролю. Деякі суб'єкти підтримують існування та функціонування кіберпростору. При цьому вони здійснюють роботу мережевого контролю на території, яка підпадає під вплив конкретних державних органів. По-друге, фінансові відносини у кіберпросторі вимагають державного управління, оскільки в іншому випадку ці відносини не регулюються законодавством, а їх учасники практично незахищені. По-третє, контент, який існує у кіберпросторі, впливає на реальний світ. Деякі відомості можуть суперечити державній політиці та закону. Наприклад, у справах про безкоштовне розповсюдження дитячої порнографії в кіберпросторі суди стверджували, що ці відносини мають регулюватися національним законодавством держави [32]. Нарешті, по-четверте, держави повинні мати контроль над кіберпростором в цілях національної безпеки.

## 1.3. Кібербезпека як ключова проблема національної безпеки

Глобалізація сектору інформаційно-комунікаційних технологій (ІКТ) протягом останніх 20 років постійно прискорюється, а конкуренція за лідерство в новітніх винаходах стає дедалі жорсткішою; і, в той же час, ці досягнення приносять із собою нові ускладнення щодо правил торгівлі та міркувань національної безпеки.

«Кібербезпека» — концепція, яка з’явилася на порядку денному після холодної війни у відповідь на суміш технологічних інновацій та мінливих геополітичних умов. Більшість комп’ютерних вчених прийняли технічний дискурс, який зосереджений на розробці хороших програм з обмеженою кількістю серйозних помилок і систем, в які важко проникнути стороннім зловмисникам. При переході від «комп’ютерної безпеки» до «кібербезпеки» цей технічний дискурс був пов’язаний з дискурсом сек’юритизації, розвинутим у спеціалізованій сфері національної безпеки. «Кібербезпеку» можна розглядати як «комп’ютерну безпеку» + «сек’юритизацію» [47].

Як кібербезпека пов’язана з політикою безпеки? По-перше, кібербезпека є відносно новим терміном для набору старих практик безпеки комп’ютерних мереж. По-друге, значення терміна змінюється з часом. Не так давно обмежене коло експертів обговорювало кібербезпеку насамперед як питання управління технічними ризиками в захисті критичної інформаційної інфраструктури. Зараз найвищі урядові кола розглядають кібербезпеку як ключову проблему національної безпеки. По-третє, паралельно з переходом все більшої кількості аспектів економіки, суспільства та політики в цифровий простір, питання кібербезпеки поширюються на додаткові сфери політики. Загалом, кібербезпека в той же час просувається вгору в політичному порядку денному і стає проблемною областю у безлічі додаткових сфер політики [25].

Кібертехнології керують глобальною економікою і їх можна використовувати для охоплення великої кількості населення певної країни, регіону чи навіть у всьому світі. При цьому кіберпростір можна використовувати для вчинення злочинів і перетворити його на зброю. Тому сучасний кіберсвіт впливає на національну безпеку, а це має безпосередній вплив на суспільні інтереси і, отже, привертає політичну увагу [39].

Загалом, чим розвиненіша країна, тим більша ймовірність того, що вона стане об’єктом кібератак. Багато в чому це пов’язано з кореляцією між економічним розвитком та залежністю від ІКТ. Чим більше залежить населення країни від Інтернету, тим більше можливостей для кібершахрайства; так само, чим більше держава покладається на Інтернет для функціонування уряду та основної фізичної інфраструктури, тим більше політичних цілей можуть мати зловмисники. Серед кіберзалежних країн легко розвивається гонка кіберозброєнь [66].

Держава, заснована на папері та бюрократії, вже відійшла в минуле. Сьогодні в багатьох європейських країнах більшість контактів і взаємодій з державними адміністраціями можна здійснювати онлайн. Використання для цього кіберпростору створює нові ризики та загрози. Їх нейтралізацію не

може здійснити окремий уряд або лише уряди. Ефективна відповідь вимагає скоординованих зусиль як державного, так і приватного секторів, встановлення спільних стандартів, платформ і політики для використання кіберпростору та захисту від атак.

Виходячи з різних національних підходів, кібербезпека розглядається як інструмент досягнення національних інтересів, оскільки більшість сучасних теорій зосереджені на матеріальній вигоді. Тим часом деякі країни розглядають кібербезпеку як інструмент впливу на світосприйняття противників. Цей стан будується на основі величезного руйнівного впливу кібератак. На відміну від двох основних підходів, інститути національної безпеки роблять акцент на ідеї, а не на матеріальній вигоді. Різниця між цими підходами до національної безпеки полягає в тому, як використовувати цей інструмент для досягнення цілей. Саме тому кібербезпека відіграє важливу й особливу роль у світовій політиці.

Тим не менш, правильна роль держави у питаннях кібербезпеки залишається політично оскарженою, оскільки кібербезпека — це не лише національна безпека. Питання полягає не в тому, чи є роль держави, а в тому, хто має брати на себе відповідальність у різних механізмах управління, які спрямовані на підвищення національної та міжнародної безпеки [26]. Очевидно, що держави самі по собі не можуть забезпечити підвищення кібербезпеки, не в останню чергу тому, що багато важливих мереж перебувають у приватних руках. Таким чином, політика кібербезпеки визначається національними та міжнародними процесами переговорів про межі відповідальності державних, економічних і суспільних суб'єктів, а також згоди чи розбіжності щодо засобів, які використовуються цими суб'єктами [27].

Розрізняють два різних впливи кібератак: прямий і непрямий. У непрямих атаках ціллю є не конкретна особа чи окремий комп'ютер. Метою будуть електромережі, ланцюги поставок, банківські системи, системи водопостачання, комунікації та транспорт. Тобто руйнується інфраструктура,

щоб обмежити постачання електрики, води, готівки. Натомість прямі атаки спрямовані на конкретних осіб. Під час війни цивільне населення, свідомо чи випадково, також може бути під прицілом. У кібервійні технічні методи дуже схожі, але наслідки можуть бути більш особистими. Наприклад, що робити, якщо всі дані на персональному комп'ютері вкрадено або стерто, особливо якщо це єдині копії фотографій або документів [59].

Очевидно, що сучасні виміри кібербезпеки виходять далеко за межі звичайного захисту IT-інфраструктури або захисту певних об'єктів у чутливих національних інфраструктур. Вони стосуються особливих економічних і політичних міркувань, оскільки сучасні суспільства базуються на знаннях та інформації, а також на дослідженнях і розробках і керуються ними. З цієї причини кіберзагрози не можна ігнорувати чи нехтувати ними. Позиція «це не може статися з нами» сьогодні не працює; кіберзагрози є глобальними, і жодна країна не застрахована від них, а також не може дати адекватну відповідь в ізоляції [41]. Очікується, що до 2025 року злочини в кіберпросторі будуть коштувати світовій економіці $10.5 трильйонів за рік, а це майже $20 мільйонів щохвилини [22].

Завдяки постійному розвитку кіберпростору побутує кілька проблем, що не зникають з плином часу, а навпаки потребують все більшої уваги, особливо говорячи про захист критичних для держави структур. Першою з них варто виділити, що хакери стають розумнішими [40]. Вони щодня знаходять нові способи доступу до даних. Тому необхідно визначати прогалини безпеки раніше, ніж це зроблять хакери. Оскільки навички хакерів стають все більш складними, для розробки та впровадження передових рішень безпеки потрібна все більша кількість спеціалістів з кібербезпеки. Таким чином, завжди існує потреба в кваліфікованих співробітниках, які б справлялися з новітніми розробками. Це, власне, теж має місце серед труднощів. Пошук добре підготовлених фахівців з кібербезпеки історично був проблемою для всіх галузей, але постійний перехід до більш

розподіленої робочої сили створює все більш критичну потребу в них, щоб допомогти підвищити безпеку корпоративних мереж [37].

Іншою постійною проблемою є застарілі та неефективні системи захисту. Оскільки кібератаки стають дедалі складнішими разом із технологіями, що швидко змінюються, ці застарілі та неефективні системи стають легкою мішенню. Ця швидка еволюція загроз кібербезпеці означає, що професіонали в цій галузі повинні бути в курсі останніх стратегій, оновлень та швидко оволодівати новими навичками, щоб залишатися конкурентоспроможними [24].

Хоча вчені все більш серйозно ставляться до впливу технологій на міжнародну безпеку, вони продовжують розходитися щодо рівня та природи загрози, а також відповідних політичних реакцій, які мають прийняти уряди та інші зацікавлені сторони. Найбільш помітно, що вчені дискутують, чи буде кібервійна чи ні. На тлі ескалації геополітичної та геоекономічної напруженості це одна з найбільших загроз, з якими сьогодні стикаються нації: від втручання у вибори до імовірної спроби крадіжки чутливих досліджень вакцини від COVID-19 до відключення електроенергії для майже чверті мільйона людей, спонсоровані державою кібератаки, що проникають у критичну інфраструктуру країн по всьому світу. Поступово ця наука та її орієнтація на державу доповнюються зростаючою програмою досліджень, що вивчають загрозу, яку представляють недержавні суб'єкти та поширення кіберпотужностей.

Держави також мають дуже різні погляди на кіберпростір та його належне використання, причому все більша кількість країн розвиває наступальні кіберспроможності. Прикладом цього є США та Росія, що обоє використовують кіберпростір для шпигунства з метою збору конфіденційної інформації. Проте, тим часом поки США здебільшого маніпулюють інформацією, Росія виправдовує свої кібероперації інформаційною війною [74]. Кібербезпека стала невід'ємною частиною національної оборони урядів, а також зовнішньої політики та доктрини безпеки, сприяючи розбудові

кібербезпеки як нової сфери ведення війни. На відміну від морського, повітряного та космічного, кіберсфера має три подібні характеристики з сухопутною війною, хоча й у ще більших вимірах: кількість гравців, легкість входу та можливість приховування. На суші домінування не є легко досяжним критерієм. Хоча деякі держави, як Сполучені Штати, Росія, Великобританія, Франція та Китай мають репутацію більших потужностей, ніж інші, немає сенсу говорити про домінування в кіберпросторі, як у морській чи повітряній силі [54]. Зусилля з розробки правил використання кіберпростору зосереджені на застосуванні існуючого міжнародного права, потенційних прогалинах, розробці норм, заходах зміцнення довіри та формулювання позицій стримування. Як коротко стверджує Джозеф Най [63], комплекс режимів кібербезпеки еволюціонував, охоплюючи численні регіональні та міжнародні інституції, які відіграють ключову роль у формуванні відповідної політики. Таким чином, зростає консенсус щодо того, що стійкість стає одним із основних стовпів загального режиму кібербезпеки, тоді як операція злому під час виборів у США пожвавила багаторічну дискусію про взаємозв'язок між інформаційними операціями та кібероперaціями [36].

Постійне, але помилкове припущення щодо кіберпростору полягає в тому, що злочин має перевагу над захистом. Багато експертів змальовують кіберпростір як «сферу вищої кваліфікації», де атаки відбуваються швидко і часто без попередження. Але багато політологів налаштовані скептично, особливо враховуючи час, ресурси та навички, яких може вимагати успішне кіберзлочинство, особливо на стратегічному рівні [83].

Кіберпростір відкриває широкі перспективи для окремих осіб, організацій та урядів. Але це вимагатиме рішучих кроків, щоб гарантувати, що реалізація його потенціалу не буде мати руйнівних наслідків. Крім того, необхідно розуміти, що це середовище, хоч воно й відмінне від фізичного, все одно створене людиною, тому стверджувати, що це лише технічні питання – помилково. Сама природа кібербезпеки та обговорення, які

відбувалися на даний момент, повинні зробити очевидним, що кібербезпека не може розглядатися виключно на національній основі. Кібернетика у багатьох її проявах є наслідком глобалізації, і це явище необхідно аналізувати та переглядати з урахуванням міжнародної структури та наслідків для міжнародного товариства. Фундаментальні проблеми є такими ж міжнародними, включаючи безпеку, управління, використання в геополітичному контексті та інші, і їх вирішення вимагатиме або, принаймні, буде посилено міжнародними діями [54].

## РОЗДІЛ 2. ПОЛІТИКО-ПРАВОВІ ТА ІНСТИТУЦІЙНІ ОСНОВИ КІБЕРБЕЗПЕКИ УКРАЇНИ

### 2.1. Кібератаки та їх роль у сучасній війні

Як відомо, російська агресія на Україну не обмежилася лише збройними протистояннями. Агресія в кіберпросторі була і раніше, але в 2014 році вона набрала відкритих форм. Перед початком відкритої російської агресії було здійснено низку шпигунських операцій, які мали на меті збір інформації з державних установ та приватних компаній. Це надавало можливість владі РФ будувати певну стратегію подальших дій, відповідно до планів української сторони.

Взагалі найбільшим джерелом хакерських атак протягом 2020-2021 років в світі стає саме Російська Федерація, яка здійснює більш ніж половину усіх злочинних дій – 58%. За нею КНДР, на яку припадає 23%  Україна займає друге місце серед тих, проти кого вони спрямовані. На Україну припадає 19% усіх світових кібератак. Для контрасту відсоток кібератак на Бельгію, Японію та Німеччину не перевищує 3%.  Попереду лише США [18]. Відповідно до звіту Microsoft, РФ наростила кіберпотужність за звітній період з 21% до 32%. Також було визначено основні галузі, що піддаються атакам. Найбільше зусиль хакерів припадає на сектор держуправління та дипломатії – 48%. До речі, саме на цю сферу зросла увага російських хакерів аж з 3% до 53%. 31% кібератак приймають на себе неурядові організації та аналітичні центри. З дуже великим відром в перелік цілей потрапляє освіта – 3% та медіа, охорона здоров’я, ІТ – 1%

Загалом 2021 рік важко назвати спокійним для України. Проте січень 2022 побив усі рекорди. (Дод. 1) Лише за один місяць було виявлено та нейтралізовано більше 120 атак [10], а це лише офіційна статистика.  За інформацією СБУ [7], більшість здійснених кібератак належали до 4 типів:

- Атаки на веб-додатки;
- Шкідливе програмне забезпечення
- З’єднання з командно-контрольними серверами

- Намагання отримати несанкціонований доступ

Треба зазначити, що далеко не всі кібератаки висвітлюються у ЗМІ, а лише ті, які стають публічними і відчутними для громадян [3]. Наприклад, такою стала атака в ніч з 13 на 14 січня, що була здійснена на сайти державних органів – Кабміну, МЗС, МОН. Також не працював додаток «Дія». Пізніше було зазначено, що витоку даних не сталося, не зважаючи, що на деяких ресурсах користувачі могли бачити погрозливе повідомлення [12]. Це повідомлення, до речі, мало меседж трьома мовами – українською, російською та польською, що розглядається як спосіб посіяти непорозуміння між Польщею та Україною, спробою перекинути відповідальність за кібератаку на Захід. Але польські ЗМІ вказують, що в польському фрагменті наявні граматичні помилки, тому підозри падають лише на РФ [9]. Але не лише Польща відреагувала на цей інцидент. Тоді керівництво Євросоюзу зробило заяву, що мобілізує свої сили для того, щоб допомогти Україні впоратись з кібератакою. Також підтримку виказали у МЗС Литви, Швеції та Польщі. Проте ніхто не насмілився стверджувати точно, хто стоїть за кібератакою.

У лютому ситуація повторилась: тоді була здійснена масштабна DDoS-атака, в наслідок якої постраждали не лише державні ресурси (Міноборони, Збройних Сил ), а й банки та низка ЗМІ [14]. Як стверджують держслужбовці, метою атаки було поширення паніки та дестабілізація ситуації в Україні. На той момент, система відреагувала швидко і проблему було незабаром усунуто за рахунок того, що низку сайтів вимкнули примусово аби локалізувати кібератаку і запобігти її поширенню.

Вартість такої кібератаки сягає мільйонів доларів, а вектори були організовані з різних країн. Дозволити собі таку суму могли лише держави чи їхні спецслужби, а не окремі хакери. Як стверджує керівник Департаменту кібербезпеки СБУ, лише Росія зацікавлена в подібних ударах по Україні [2].

Російська Федерація також заручилася підтримкою на поприщі кібероперацій. Так, уряд Великобританії підтвердив, що Національний центр кібербезпеки розслідує звинувачення, які стверджують, що понад 600 веб-сайтів, у тому

числі міністерство оборони України, були піддані тисячам спроб злому, координованих урядом Китаю. Хоча СБУ спростувала цю інформацію [61].

Протягом години після того, як президент Росії Володимир Путін перед світанком 24 лютого оголосив про введення військ в Україну, тисячі модемів у Центральній Європі втратили зв'язок із супутником. Люди в Італії, Німеччині та Польщі втратили інтернет. Viasat підтвердила цю подію, але не звинувачує Росію в цьому. Україну теж не оминуло, ця раптова втрата з'єднання для передачі даних вразила її розрізнені армійські бази. Але оскільки десятки військових модемів раптово перестали працювати, війська швидко перейшли до інших зашифрованих комунікацій. Це було саме тоді, коли почалася війна, але команди були підготовлені до цієї ситуації, щоб уникнути катастрофи будь-якою ціною [50].

З часу вторгнення Росії в Україні було щонайменше 150 кібератак. Їх вплив переважно психологічний, і експерти кажуть, що вони не вирішують війну [19]. Загалом, інтенсивність атак з початку бойових дій впала. Проте, це зовсім не стосується енергетичного блоку. Кількість кібератак на національну енергетичну компанію "Укренерго" зросла утричі з 24 лютого. За даними CERT-UA, енергетичний сектор України входить до однієї з головних цілей кіберзловмисників під час війни. Проте енергопостачання в Україні працює стабільно. Атаки в основному зосереджені на шпигунських операціях та дезінформації. Було щонайменше три атаки, які призвели до видалення даних у мережах, якими керує влада України. Але за весь час не було масових відключень електроенергії чи кібератак на критичну інфраструктуру.

Найбільша кількість кібератак припала на початок вторгнення – лютий-березень - напередодні приєднання України до ENTSO-E (європейська мережа системних операторів передачі електроенергії), адже основною метою було перешкодити цьому. Хоч вони не були успішними, проте, тривають і досі [8]. Щонайменше 115 000 облікових записів у Twitter і Facebook уже було виявлено для поширення фейкових новин про вторгнення [65].

У відповідь на російську загрозу були безпрецедентні зусилля приватних та державних установ – і навіть окремих осіб – для підтримки кіберстійкості України. Українські інженери, зокрема ті, що охороняють цивільну інфраструктуру від кібератак, змогли звернутися за допомогою до західних компаній, таких як Cisco, Microsoft та Google, яка зараз захищає щонайменше 150 українських фірм.

Зрозуміло, що відповідь на кібератаки та формування національної кіберстійкості ніколи не були – і ніколи не будуть – виключною відповідальністю урядів. Це вимагає підходу всього суспільства, заснованого на зусиллях міжнародного співробітництва. Вперше з моменту заснування команда ЄС швидкого кібернетичного реагування, яка має можливості виявляти різноманітні загрози та реагувати на них, очолювана Литвою, була розгорнута для захисту від кібератак, спрямованих на Україну.

Румунське національне агентство з кібербезпеки та компанія з кібербезпеки під назвою Bitdefender запустили державно-приватне партнерство, щоб надавати безоплатну технічну підтримку та розвідку про загрози уряду України, бізнесу та громадянам «доки це необхідно». НАТО, яка вже кілька років працює з Україною над підвищенням її кіберзахисту, підписала угоду за кілька тижнів до вторгнення, спрямовану на посилення кіберспівпраці з Україною. У той же час зусилля всередині України почали матеріалізуватися. У зв’язку з безпрецедентними зусиллями в розпал збройного конфлікту у відповідь на прохання міністра цифрової трансформації підтримати зусилля країни з кіберзахисту була зібрана ціла «ІТ-армія» волонтерів, деякі з яких діють навіть перебуваючи у бомбосховищах 46].

Цікавим щодо цифрових вимірів конфлікту в Україні є той факт, що події підтверджують багато з того, що вчені з кібербезпеки говорили роками про корисність кібер-інструментів для посилення інститутів державної влади. Як сказав експерт з кібербезпеки Джейсон Блессінг, російського «кібер-бліцкригу» не було, і навряд чи буде щось подібне, принаймні, згідно з переважаючим уявленням про кіберконфлікт. Це тому, що кібер-інструменти просто не є

хорошими засобами для контролю ескалації або впливу на полі бою. Стратегічної корисності для використання кібертактики в Україні для підтримки самого вторгнення просто не було. Кіберінструменти приносять лише тимчасові перемоги, тому не дуже підходять для прямого примусу. А через очікування Росією швидкої перемоги змусило її одразу відкинути складні кіберінструменти з переліку засобів боротьби за логікою «не ламайте те, що збираєтесь купити» [88].

Існує безліч здогадок, якими намагаються пояснити, чому кібероперації залишаються маргінальними в конфлікті. По-перше, українська сторона добре попрацювала над зміцненням цифрового простору та механізмами його захисту, частково за допомогою союзників. Існують також притаманні кібератакам обмеження: у повній кінетичній війні ракети пропонують швидший і ефективніший засіб досягнення стратегічних цілей, ніж рядки коду [87]. По-друге, на заваді стали масові сутички кібер-«партизанів» з обох сторін. Можливо, росіяни продовжують функціонувати в українських мережах для власних цілей, у тому числі для допомоги в зборі розвідувальних даних.

Росія також, схоже, інвестує більше ресурсів у скоординовані кампанії з дезінформації, ніж у відкриті хакерські операції. Експерти з дезінформації повідомили, що Росія веде скоординовану кампанію з просування неправдивих наративів про вторгнення в Україну, включаючи підроблені відео та дезінформацію. Російські чиновники заблокували доступ до соціальних мереж у країні, щоб запобігти поширенню інформації, яка не відповідає її розповіді [64].

Росія й раніше не використовувала надто руйнівні кібероперації у збройних конфліктах. Під час свого короткого конфлікту з Грузією в 2008 році вона використала лише DDOS-атаки і поширювала дезінформацію. Але це насправді не кваліфікується «важкою зброєю» у кіберпросторі. Тим не менш, ці операції цілком могли перешкоджати здатності Грузії відреагувати після початку збройного конфлікту. Операції, проведені Росією проти України під

час її окупації Криму в 2014 році, були подібними за амбіціями, масштабом та ефектом до операцій проти Грузії.

Все-таки, багато хто вважає, що не надто активна діяльність Росії на цифровій арені під час війни, швидше за все, відображає її неякісне планування та відсутність результативності на землі та в повітрі. Пильні спостерігачі були збентежені недостатньою підготовкою російської армії, відсутністю ефективних загальновійськових операцій, поганим матеріально-технічним забезпеченням та обслуговуванням, а також неможливістю належного шифрування комунікацій. Тому ворог прорахувався не лише на реальному полі бою, а й у віртуальному просторі [68].

Від 24 лютого експерти виявили три основні типи кібертактик, які наразі застосовувалися у російсько-українському конфлікті: операції стирання, DDoS-атаки та атаки зі знищенням. Усі три, по суті, роблять те саме: вони заважають людям отримати доступ до інформації, але різними способами. В середньому частота здійснення будь-яких злочинних дій в кіберпросторі проти України складає 1 раз на 2-3 дні, проте іноді по декілька на день [81].

Операції стирання видаляють інформацію в мережі, заважаючи людям у цій мережі отримати доступ до власних даних. Вони мають потенційно тривалий руйнівний ефект. Торстен Хольц сказав, що використання подібних операцій у цій війні свідчить про те, що Росія готувала деякі зі своїх кібератак місяцями. Це означає, що ці атаки міцно вкорінені у військовій стратегії Росії [57]. Шульце, який вважає прогрес Росії менш організованим, заперечує цю оцінку. Але справа в тому, що напади все ще відбуваються.

DDoS-атаки знищують веб-сайти. Це означає, що люди ззовні не можуть отримати доступ до інформації чи порад, наприклад, на урядовому веб-сайті під час надзвичайної ситуації. Ця форма атаки передбачає перевантаження системи через надмірну кількість «запитів» — людей, які намагаються отримати доступ до веб-сайту — за короткий проміжок часу. Якщо ця кількість запитів перевищує максимальну кількість, яку може обробити система, система взагалі перестає відповідати. Тому для зовнішнього світу він закривається.

Атаки зі знищенням видаляють інформацію на веб-сайті або змінюють інформацію, яка там з'являється — це основна тактика дезінформації, яка може ввести в оману широку громадськість, щоб вона думала, що підроблена інформація є надійною. І ця фейкова інформація може швидко поширюватися. Це одна з найстаріших військових тактик, коли учасники війни надають мирному населенню неправдиву інформацію. Його вплив значною мірою психологічний, але дуже ефективний.

Інші види кібервійни є більш відкритими та офіційними. Компанія Meta, яка володіє соціальною мережею Facebook, заблокувала деякі російські ЗМІ на своїх платформах. У контр-маневрі Росія обмежила доступ до Facebook.

Проте, говорячи про наявність чи відсутність окремого явища кібервійни у війні Росії проти України, треба сказати, що наявні події не є кібервійною в чистому вигляді, хоч чимало дослідників вважає інакше. У даному випадку кібеоперації і атаки все таки є лише допоміжним засобом, метою якого є дестабілізація ситуації в Україні, отримання стратегічної інформації, фактором залякування та шантажу як українського уряду, так і західних держав. На підтвердження цього треба звернутися до російського дискурсу інформаційної війни. Вона включає в себе кібервійну, яку зазвичай розглядають як технічний захист від технічних атак у війні, але лише як одну з багатьох стратегій [78]. Таким чином, це не є головною їх зброєю і кібервійну в чистому вигляду РФ не може продемонструвати. До того ж, у цій війні надалася перевага традиційним засобам.

Цікаво, що Москва може навіть нервувати через ескалаційний ефект російських кіберзлочинних груп, судячи з її арешту перед нинішнім конфліктом деяких із її найвідоміших кіберзлочинців. Міжнародне право чітко стверджує, що держава, яка закриває очі на дуже шкідливу кіберзлочинну діяльність, яка виходить з її території, сама вчиняє «міжнародно протиправні дії» і, отже, нестиме законну відповідальність за пропорційні контрзаходи [86].

Говорячи про російське вторгнення в Україну, неможливо не згадати сплеск хакерів-добровольців, або хактивістів, які борються на цифровій лінії

фронту з Москвою. Такі групи, як Anonymous, Squad303 і Cyber Partisan здійснюють кібератаки проти російських цілей. Найбільше відзначився колектив хактивістів Anonymous, який оголосив кібервійну президенту РФ. До їх «здобутків» належать злом російської телемережі, яку вважають найбільш креативною і важкою для здійснення. Крім цього, Anonymous стверджує, що вони також видалили російські веб-сайти для зміни вмісту, що відображається, та викрали і оприлюднили державні дані. Загалом, вони використовували DDoS-атаки, що є не надто складними у виконанні та тривалості дії. [80]

Поки що атаки викликали лише несерйозні порушення та збентеження, але кібер-експерти все більше стурбовані вибухом хактивізму після вторгнення. Вони стурбовані тим, що хакер може випадково зламати комп'ютерну мережу лікарні або перервати критичні комунікаційні канали. Anonymous, які з'явилися на початку 2000-х років, історично висловлювалися про захист свободи слова та конфіденційності, а їхні дії у кіберпросторі, хоча й були досить простими, але мали потенціал бути «дуже руйнівними».

Навіть якщо РФ погодиться на перемир'я, спроби кібератак та дезінформації стануть одним із небагатьох доступних для неї шляхів завдати шкоди Україні в сірій зоні за межею прямого зіткнення. Загнана в кут Москва, ймовірно, вдасться до кібератак знову, вбачаючи їх як ідеальний вектор для обходу ізоляції, шпигунства та зриву західних оборонних планів, крадіжки технологій та інтелектуальної власності. Атаки на українську телекомунікаційну компанію «Укртелеком» посилили побоювання, що зупинка військової кампанії Росії може змусити її звернутися до кібероперацій як до іншого засобу досягнення своїх цілей.

## 2.2. Стратегії кібербезпеки України (2016 р., 2021 р.)

В українському законодавстві до проблеми кібербезпеки як окремої галузі національної безпеки держави звернулись відносно недавно. Саме раптова, неочікувана потреба захищати цифровий простір від зайвого втручання стала причиною наявних проблем, адже не було приділено достатньо часу для розробки або опрацювання чіткої стратегії розвитку.

Таким чином, перша Стратегія кібербезпеки України з'явилась лише у 2016 році і постійно доопрацьовувалась. Проблема першої Стратегії полягала в нечіткості формулювання пріоритетів, тобто не було повною мірою усвідомлено кінцеву мету. Це унеможливлювало ефективну реалізацію заходів. Крім того, Плани заходів реалізації стратегії кібербезпеки створені лише на 2017 та 2018 роки, а їх виконання здійснено лише на 40%, то ж не дивно, що питання ефективної системи кібербезпеки України досі стоїть так гостро [1].

Частково дотичним до сфери кібербезпеки є інформаційна безпека. Інформаційна безпека спрямована на те, щоб захищати дані в будь-якій формі та є дещо ширшим поняттям, ніж кібербезпека (Дод. 2), але у цій галузі законодавство було теж досить загальне з розрахунком на період 2007 – 2015 роки. Конкретно до проблеми кіберзахисту до 2016 року українська влада не зверталася, тому система українського кіберзахисту будувалася фактично з нуля і поки що не можна сказати, що вона добре сформована.

Особливістю української системи кібербезпеки є те, що постійна потреба протистояти кіберзагрозам розвинула в Україні гарну систему оборони, боротьби проти кіберзлочинів та відповіді на них. Але це формує наступну проблему – реагування після фактичного здійснення атаки, натомість, відповідно до показників Національного індексу кібербезпеки, кризовий менеджмент та розвідницька діяльність довгий час не задіювалась взагалі [62]. (Дод. 3)

Такий нерівномірний розвиток кібербезпеки спричинений неточними формулюваннями пріоритетів та цілей у Стратегії, а також застарілим технічним обладнанням, що не передбачає виконання подібних операцій.

Для визначення ефективності діяльності наявної системи українського кіберзахисту можна звернутись до Глобального індексу кібербезпеки та Національного індексу кібербезпеки (Дод. 4).

Щодо показників Глобального індексу кібербезпеки з 2014 р. Україна не стоїть на місці. Якщо в 2014 р. [42] вона трималася на 70 місці у світовому рейтингу, маючи показник 0,353, то в 2017 р. [43] році цей показник збільшився майже вдвічі, досягнувши показника 0,501, і віддав Україні 59 місце в світі. У 2018 р. [44] показник ще збільшився - 0.661 (max. 1) і це відповідає 54 позиції в рейтингу. На жаль, за 2019 рік дані відсутні у зв'язку зі зміною процедури оцінювання в Міжнародному союзі електрозв'язку. Але в 2020 [45] році дані України значно погіршились - 65.93 (max. 100) і це 78 місце з 182 держав, на якому вона залишається донині. Пандемія Covid-19 фактично стала випробуванням на міцність для кібербезпеки не лише України, коли усі сфери життя перейшли в онлайн формат. Таким чином, показники Глобального індексу кібербезпеки демонструють, що в критичний момент задекларовані урядом підходи до розбудови кібербезпеки виявились не надто ефективними.

Звертаючись до Національного індексу кібербезпеки то тут показники більш стабільні і кращі. Треба зауважити, що ці дані оновлюються декілька разів на рік, тому позиції різні. В 2019 році позиція України коливалась від 24 до 28 позиції, у 2020 – позиція змінювалась від 25 до 29 сходинки, у 2021 році – поки що показник стабільний – 22 місце в рейтингу з 160 держав. Станом на 2022 рік Україна спустилась на 24 місце з зрозумілих причин, хоча могло бути й гірше [62].

Згідно з останніми дослідженнями, відсоток комп'ютерів, які зазнали хоча б однієї локалізованої атаки, в першому кварталі 2020 року складав – 21,01%, в другому кварталі – 21,3%, в третьому – 17,1% [62].

Як відомо, кіберзлочинці намагаються скористатися пандемією COVID-19. Таким чином, Україна знову стала їх ціллю і за період Вересень 2020 – Жовтень 2021 було виявлено понад 118 тисяч шкідливих файлів, і з такою кількістю Україна займає 12 місце в світі [31]. За таких умов вкрай важливим є

обов'язкове використання комплексу програмних і апаратних засобів, які б дозволили забезпечити прийнятний рівень захищеності інфраструктури, а саме: ефективне надійне антивірусне програмне забезпечення, системи запобігання вторгнень, модулі контролю пристроїв і доступу до інтернету, системи шифрування даних, керування роботою мобільних пристроїв, засоби для захисту поштових серверів і систем колективної роботи тощо.

Легко зрозуміти, чому Україна є привабливою мішенню для тестування інструментів кібервійни. Держава має таку ж інфраструктуру, як і в Західній Європі та Північній Америці. Але на відміну від Сполучених Штатів, Великобританії та Європейського Союзу (ЄС), Україна має більш обмежені ресурси для контратак, незважаючи на те, що присутня підтримка у зміцненні кіберзахисту від США та ЄС. І хоча Росія є очевидним підозрюваним, цілком можливо, що інші країни, такі як Іран, Північна Корея чи Китай, також випробовують свою кіберзброю в Україні. Тому це є менше ризиків бути притягнутим до відповідальності [59].

Стратегія кібербезпеки від 26 серпня 2021 року значно конкретніше окреслює цілі та завдання, розмежовує наявні загрози українській кібербезпеці на глобальному та національному рівнях [5]. Передбачити ефективність Стратегії 2021 року важко, адже майже завжди теорія відрізняється від практики.

Окремої уваги заслуговує План реалізації Стратегії, що введений в дію від 1 лютого 2022 року. Потрібно відзначити, що в новому Плані значною мірою відрізняється підхід. По-перше, керівництво вирішило прописувати завдання не щороку, як це було з Стратегією 2016 року, а одразу продумати дії на весь період - 2021-2025 роки. Очевидно, це було зроблено таким чином, щоб реалізація стратегії не випускалась з поля зору, як це сталося з Планами реалізації 2019-2020. По-друге, у плані 2022 року поставлені чіткі цілі, до яких прописані конкретні кроки, відповідальні органи та строки виконання. Цікавою особливістю є те, що вказані терміни розробки деяких кроків, а їх реалізація позначена як "постійно". По-третє, до переліку включено заходи, що

стосуються не лише технічного забезпечення кібербезпеки, а й громадян держави у вигляді інформаційної роз'яснювальної кампанії. Тут же, є спроба розподілити завдання між органами за їх компетенцією. Так, наприклад, до інформаційної кампанії залучено Міністерство освіти. У розбудові системи кібербезпеки автори рівняються на США та держави-члени Європейського Союзу. Проте, як і в попередніх планах, знову присутні загальні фрази на кшталт "ефективні механізми", "вітчизняні рішення", а якими вони повинні бути – невідомо. Але такі випадки поодинокі.

Окремим вагомим пунктом виділено міжнародне співробітництво у сфері кібербезпеки. Виконання завдань у цьому розділі покладено суто на Міністерство закордонних справ. Діяльність спрямована на різні аспекти: обмін інформацією щодо кіберінцидентів, спільна відповідь на кібератаки і подолання кризових ситуацій у кібербезпеці, проведення спільних навчань, залучення України до розробки правової бази, проведення спільних кібероперацій та розслідування міжнародних кіберзлочинів тощо [15].

## 2.3. Інституційна основа забезпечення кібербезпеки

За декілька років прискіпливої уваги до проблематики кіберпростору, починаючи з 2016 р., в Україні з’явилась досить розгалужена система органів, що відповідають за забезпечення кібербезпеки, але фактично кожен з них має одну й ту саму мету - виявлення та запобігання загрозам. Але основним недоліком є те, що до реалізації заходів з розвитку кібербезпеки залучені лише суб’єкти сектору безпеки та оборони. Цивільні міністерства і відомства залучені мінімально, тобто цілі, що пов’язані з науковим розвитком галузі кібербезпеки та підвищенням цифрової грамотності громадян покладені на відомства, що не мають відповідних компетенцій.

Таким чином, основним суб’єктом забезпечення кібербезпеки визначено Президента України, який визначає пріоритети до Стратегії та напрями її

забезпечення. Рада національної безпеки і оборони України здійснює координацію органів, що безпосередньо причетні до заходів забезпечення кібербезпеки, контролює їхню діяльність, співпрацює з Президентом для уточнень положень законодавчих документів. На Кабінет Міністрів України покладено формування політики з забезпечення прав і свобод громадян в кіберпросторі, боротьбу з кіберзлочинністю, забезпечення національних інтересів держави [6]. Також до переліку суб'єктів відноситься Міністерство оборони України, Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, Національна поліція України, Національний банк України, розвідувальні органи [17].

Національний координаційний центр кібербезпеки при РНБО вважається головним суб'єктом забезпечення кібербезпеки. Не дивлячись на те, що поява в Україні НКЦК була зумовлена саме необхідністю вирішення питання ефективної координації всіх суб'єктів, які діють в сфері кібер-захисту, злагодженість в діях усіх структур все ще відсутня. Причиною цьому є недостатня комунікація між органами та відсутність оперативної передачі інформації щодо виявлених кіберзагроз.

В цілому наявні структури все ж дають позитивні результати. Наприклад, Ситуаційний центр забезпечення кібербезпеки, що функціонує при Службі безпеки України, на даний момент займається створенням децентралізованої системи кібербезпеки - відкриваються регіональні центри забезпечення кібербезпеки СБУ. Поки що їх 3 – в Сумах, Дніпрі та найновіший в Одесі. Крім того, відповідно до звітів СБУ [16] у першому півріччі 2021 року кіберфахівці Служби безпеки України локалізували 1000 потенційних загроз інформаційній безпеці нашої держави, а також було заблоковано масштабну кібератаку підконтрольного ФСБ РФ хакерського угруповання «Armageddon». Відповідно до опублікованого звіту компанії Microsoft [60].

Варто відзначити роль НАТО у розбудові українського кіберзахисту. Україна здійснює свою діяльність з метою консолідації зусиль для пришвидшення впровадження стандартів НАТО у сфері приєднання до

колективної системи забезпечення кіберзахисту. Але цей процес все ж є досить повільним, що свідчить про недосконалість існуючої системи протидії загрозам у кіберпросторі та зовнішнім кібератакам у сучасних умовах. Одним з головних програм з розвитку кібербезпеки України був Трастовий фонд Україна – НАТО, який спрямовувався на підтримку України у розвитку її оборонних можливостей у галузі кібернетичної безпеки, пропонуючи обладнання, програмне забезпечення, технічну допомогу, консультативні послуги та проведення навчальних тренінгів. Також за підтримки НАТО був створений центр реагування на інциденти у кіберпросторі – CERT-UA.

Україна намагається дотримуватись сучасних тенденцій, працює над вдосконаленням законодавчої бази та залучає активно технології в державотворчі процеси. Аналіз діяльності України в сфері кібербезпеки дозволяє зробити такі висновки: цифровий простір України все ще не достатньо захищений і потерпає від атак інших країн. Якщо держава не може захистити свої стратегічно важливі об’єкти, в поле ще більшої небезпеки потрапляють громадяни. Не дивлячись на те, що систему механізмів оборони інформації активно трансформують та розширюють, діяльність на попереднє виявлення та нейтралізацію загроз ще не розвинена. У міжнародному просторі становище України також все ще нестабільне, а в умовах кризи і посиленні ударів ззовні система виявилась не такою стійкою, як це здавалось. Загалом, українська кібербезпека не є найгіршим прикладом, але простору для вдосконалення ще багато. За період від створення фундаменту системи в 2016 році до створення значних змін в сторону покращення не прослідковується.

## РОЗДІЛ 3. МІЖНАРОДНЕ СПІВРОБІТНИЦТВО У ГАЛУЗІ КІБЕРБЕЗПЕКИ В УМОВАХ РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ

### 3.1. Обґрунтування можливості спільних зусиль у забезпеченні кібербезпеки

Технологічний прогрес і глобальний взаємозв'язок прискорюють системні ризики безпеки. Оскільки з'являються нові кіберризики, з'являється потреба в єдиній глобальній реакції. Оскільки уряди, суспільства та підприємства все більше покладаються на технології для управління послугами, продуктами та процесами, Всесвітній економічний форум розглядає нові технології як інструменти для відповідального ведення нас у цифрове майбутнє. Для кіберспільноти важливо об'єднатися навколо спільних цінностей. Тому заохочення відповідального обміну інформацією, підвищеної пильності і співпраці повинні бути на першому місці [65].

Експерти уважно стежать за обома країнами, побоюючись, що нестабільна криза за участю однієї з провідних світових хакерських супердержав може призвести до величезного конфлікту в онлайні, який може не порівнятися з фізичними битвами.

Причиною того, що міжнародна спільнота підтримує Україну і в технологічній боротьбі є ризик того, що будь-які кіберінструменти, які Росія використовує, не залишаться в межах однієї держави. Такий випадок вже мав місце декілька років тому, а саме мається на увазі вірус NotPetya 2017 року, коли зловмисне програмне забезпечення, спрямоване на певну мету, «випускається на волю», а потім починає жити власним життям. Тож і інші держави можуть стати жертвою російського шкідливого програмного забезпечення, яке вийшло за межі наміченої мети [70].

Експерти з різних країн стверджують, що такі заходи, як надання розвідувальних даних про загрози або допомога в навчанні експертів для реагування на інциденти, можуть допомогти Україні захиститися від майбутніх атак [3].

Динамічний характер збройного конфлікту вносить рівень невизначеності. У міру розвитку війни суб'єкти, зацікавлені в конфлікті, будуть діяти відповідно до все більш нагальних вимог, щоб заповнити критичні прогалини в розвідці та досягти конкретних тактичні цілі. Те, як кібероператори вирішують відповідати цим вимогам, може становити значний ризик для глобальної кібербезпеки. Таке нестабільне середовище може стимулювати використання можливостей, які дозволять учасникам отримати гарантований доступ до мереж або маніпулювати аспектами інформаційних систем для досягнення стратегічних цілей. Уже відомі кібернетичні можливості, такі як, атаки на критичну інфраструктуру, атаки на ланцюги поставок та інші нові методи, майже напевно будуть продемонстровані в середньостроковій перспективі. Є ризик того, що утвориться дії між суб'єктами кіберпростору перейдуть в гру «кішки-мишки», створюючи довгий ланцюг інцидентів [75].

Завдяки санкціям, які Сполучені Штати та союзники НАТО накладають на російські організації, швидка ескалація атак програм-вимагачів у різних галузях, ймовірно, повернеться з агресією та підвищеним рівнем витонченості. Аналітики прогнозують швидке та стійке зростання кібератак на внутрішньому та міжнародному рівні. Жертви майбутніх атак програм-вимагачів можуть зіткнутися з ще однією проблемою через потенційну можливість агресора «подвоїти» свої цілі. Це стосується тих випадків, коли злочинці отримують викуп від жертви, розшифровують частину скомпрометованих активів, а потім вимагають ще один платіж для продовження. На додаток до зростання числа програм-вимагачів у всіх галузях, організації критичної інфраструктури особливо повинні бути готові до кібератак і гарантувати, що їхня технологічна інфраструктура захищена, відстежується та готова швидко та ефективно реагувати, щоб мінімізувати шкоду. Нарешті, аналітики попереджають про масові DDoS-атаки, які мають значне повернення проти компаній по всьому світу. Відомо, що зловмисники протягом багатьох тижнів пошкоджують цілі мережі, роблячи Інтернет-послуги непрацездатними, доки потік мережевих

пакетів не вщухне. Повернення цих векторів атаки є неминучим і буде відданим безжальним суб'єктам загрози, чиї союзи розпадаються з ворогом [79].

Джо Байден завчасно попереджав Росію, що США «готові відповісти» на будь-які атаки на критичну інфраструктуру, а інші роками попереджали про «Кібер Перл-Харбор»: єдиного катастрофічного злому, який нарешті пробудить світ до справжньої загрози кібератак [69]. Насправді шкода від кібератак походить від низки подрібнених зломів, які часто приховані від громадськості і не завжди призводять до негайної відчутної шкоди.

Хоч ще і не було серйозних атак, це не означає, що їх не буде в майбутньому або що зараз не буде інших. За її словами, для розгортання багатьох таємних операцій, особливо широкомасштабних, потрібен час. У випадку злому Solarwinds, наприклад, масове порушення Росією американських організацій, розпочате в березні 2020 року, не було виявлено до грудня 2020 року.

### 3.2. Суб'єкти міжнародної допомоги України у галузі кібербезпеки

Військова допомога західних партнерів на разі дуже важлива. Але ЄС та НАТО одночасно розуміють, що підтримка у питаннях протидії кіберзагрозам та підвищення кіберстійкості України є не менш необхідною. Саме тому представники США, Європейського Союзу та НАТО обговорюють потенційні форми допомоги Україні у сфері кібербезпеки, оскільки розмови про економічні санкції проти Росії посилюються.

Насправді, велика кількість держав надала і продовжує надавати допомогу Україні для захисту кіберпростору. Наприклад, литовські чиновники, що запропонували відправити підрозділ ЄС під назвою Cyber Rapid Response Team, який очолює балтійська країна, для реагування на масштабні кібератаки в Україні. Підрозділ було створено у 2019 році і включає кібераналітиків з Литви, Естонії, Хорватії, Румунії, Нідерландів та Польщі [20]. Прес-секретар Європейської комісії, виконавчого органу ЄС, сказав, що цей орган підтримує

зв’язок з українською владою і готовий збільшити підтримку у разі потреби. Д. Кулеба також попросив у ЄС додаткове технічне обладнання та програмне забезпечення для посилення інфраструктури кібербезпеки. [29]

НАТО заявило, що надасть Україні доступ до своєї платформи для обміну інформацією про шкідливе програмне забезпечення, інструмент, який був вирішальним для розуміння основних кіберзагроз, включаючи NotPetya. Чиновники з країн ЄС обговорили розширення існуючих ініціатив з кібербезпеки, які блок фінансує в Україні. Деякі чиновники закликали надати додаткову негайну допомогу, наприклад, відправити в країну технічних експертів з кібербезпеки [77].

Не можна оминути і допомогу США:  Штати вже надали Україні допомогу у розмірі кількох мільйонів доларів на захист від хакерів. Конгресмени від Демократичної партії звертались до президента США Джо Байдена з проханням посилити захист Україні від хакерських атак РФ. Вони висловили стурбованість тим, що Росія може розпочати подальші кібератаки проти Україні, тим самим перевіряючи рішучість НАТО. Конгресмени пропонують зміцнити співпрацю з Україною новоствореного Бюро з кібербезпеки при Держдепі [11].

Крім того, кіберкомандування США відіграло ключову роль у захисті мереж та критичної інфраструктури в США та за кордоном напередодні та під час атаки Росії на Україну. Зокрема, кіберкомандування надавало дистанційну аналітичну підтримку та проводило заходи із захисту мережі [34].

Наприкінці 2021 року США надіслало в Україну групу фахівців із кіберзахисту, щоб допомогти захистити українську інфраструктуру від атак РФ. Деякі з них були солдатами з кіберкомандування армії США. Інші були цивільними підрядниками та деякі співробітники американських компаній, які допомагають захистити критично важливу інфраструктуру від кібератак, які російські агентства завдавали Україні роками. США допомагали Україні зміцнювати кіберзахист протягом багатьох років, майже від самого початку конфлікту з РФ у 2014 [76].

Не менш вагомим фактором стає глобальний волонтерський рух і формування ІТ-армії на боці України. Винаходи хакерів-добровольців варіюються від програмних інструментів, які дозволяють власникам смартфонів і комп'ютерів будь-де брати участь у розподілених атаках з відмовою в обслуговуванні на офіційні російські веб-сайти, до ботів на платформі обміну повідомленнями Telegram, які блокують дезінформацію, дозволяють людям повідомляти про розташування російських військ і пропонують інструкції. зі складання «коктейлів Молотова» та елементарної першої допомоги.

Ефективність кібер-волонтерів важко оцінити. Веб-сайти російських урядів неодноразово, хоча й ненадовго, були виведені з мережі через DDoS-атаки, але, як правило, протистояли їм за допомогою контрзаходів [23]. Є ризик того, що діяльність хакерів-волонтерів, хоч і на боці України, може мати серйозні наслідки, адже, по-перше, їхні дії ніким не контролюються, по-друге, люди можуть втратити контроль над небезпечним програмним забезпеченням.

### 3.3. Форми міжнародного співробітництва у галузі кібербезпеки

Війна в Україні представляє чи не найгостріший кіберризик, з яким коли-небудь стикалися американські та західні партнери. Сполучені Штати зацікавлені в технологічній допомозі Україні, оскільки їх основний інтерес полягає в підриві військових зусиль Росії [53]. Однак це може створити значний відсоток із непередбачуваними негативними наслідками, розмиваючи правові норми, які уряд США прагне заохочувати, і ускладнюючи для Сполучених Штатів притягнення інших держав до відповідальності за подібні дії в майбутньому.

Міністр закордонних справ Дмитро Кулеба напередодні повномасштабного вторгнення РФ на територію України надіслав листа до Європейського Союзу щодо конкретних кроків на зміцнення кібербезпеки [4]. Міжнародне співтовариство не повинно терпіти зловживання Росією використанням кіберпростору для підриву національної безпеки, суверенітету

та територіальної цілісності України, намагаючись підірвати основні послуги, бізнес і довіру суспільства» [35].

На тлі зростання кількості кібератак уряди посилюють боротьбу: президент Джо Байден видав указ, у якому говориться, що цифрові активи потрібно розвивати відповідально. Цей указ зосереджується на боротьбі з кіберзлочинністю та запобіганні кіберзлочинності, тому організація зобов'язує розкривати, якщо їхні мережі були скомпрометовані. Це має сприяти більшій прозорості та співпраці [48]. Побоювання полягає в тому, що якщо кібератаки триватимуть і посиляться, а досягнувши точки, коли центри обробки даних не впораються з тиском і або сповільняться в роботі, або повністю зруйнуються. Тому уряд України оголосив, що має екстрений план переміщення центрів обробки даних в інші країни [71].

Поряд з цим, партнери з державного та приватного секторів долучились до зміцнення своїх кіберсистем. USAID надає підтримку кібербезпеці через програму, яка діє з 2020 року. Ця ініціатива допомогла Україні зміцнити її кіберзахист та усунути слабкі місця. Але залишається відкритим питання, наскільки далеко Сполучені Штати можуть зайти у підтримці України, не будучи більш безпосередньо залученими до війни.

Західні уряди не єдині, хто ділиться з українцями своєю допомогою. Приватний сектор, включаючи технологічні компанії, такі як Google, Amazon і Microsoft, також співпрацюють з українським урядом, щоб допомогти йому протистояти кібератакам і відверто заявили про свою роль у захисті цифрової інфраструктури. За кілька годин до російського вторгнення Microsoft заявила, що виявила нову шкідливу програму — відому як FoxBlade — яка намагалася порушити цифрову інфраструктуру України. Компанія заявила, що поділилася інформацією з українським урядом і змогла нейтралізувати загрозу протягом трьох годин [51].

Румунські компанії з кібербезпеки Bitdefender і Vectra AI заявили, що пропонуватимуть Україні підтримку у вигляді технологічних продуктів і послуг. Румунська компанія Bitdefender, засновники якої виросли під час

жорстокого радянського маріонеткового режиму Ніколае Чаушеску, об’єдналася з Румунським національним управлінням кібербезпеки (DNSC), щоб запропонувати свій досвід, розвідку загроз і технології, тоді як DNSC, румунський еквівалент британському Національному центру кібербезпеки (NCSC) надаватиме технічні консультації, розвідку загроз та технології кібербезпеки будь-якому українському бізнесу, державному органу чи приватним громадянам до тих пір, поки їм це може знадобитися.

Надати підтримку країні після великої кібератаки складно, оскільки стороння допомога може перешкодити вітчизняним експертам, які найкраще знають свої технологічні системи. Але не менш важливим є фокус майбутньої співпраці – міжнародна кіберпідтримка була б найефективнішою, якщо б вони покращували служби безпеки та досвід України протягом тривалого періоду, а не реагували на конкретну атаку з боку Росії. Особливістю ситуації в українському кіберпросторі під час війни є те, що цей випадок є дуже важливим для вивчення для світової технічної спільноти, щоб забезпечити прогрес у розвитку кібербезпеки [58].

## ВИСНОВКИ

Україна намагається реагувати на сучасних тенденцій розвитку світу, працює над вдосконаленням законодавчої бази та залучає активно інформаційно-комунікаційні технології в державотворчі процеси. Проте, цифровий простір України все ще не достатньо захищений і потерпає від атак інших країн. Російська Федерація все ще залишається основним джерелом кіберзагроз, що вражають не лише Україну, а й значну кількість інших держав. Таке становище вітчизняного кіберпростору створює додаткові ризики в умовах російської агресії проти України. Збільшення кількості кібератак з боку РФ та їх наслідки створюють загрози не лише для функціонування інститутів державної влади, але є небезпечними для громадян. Трансформація механізмів оборони інформації залишається актуальною для України для того аби вчасно виявляти загрози та нейтралізувати їх. В умовах кризи і посиленні ударів ззовні це стало ще більш очевидним. У міжнародному просторі становище України також потребує значних покращень, в тому числі з точки зору іміджу.

Ефективний кіберзахист – це результат довготривалого процесу, який вимагає постійних стратегічних інвестицій, а не роботи в останню хвилину. Загалом, українська кібербезпека не є найгіршим прикладом, але простору для вдосконалення ще багато. За період від створення фундаменту системи в 2016 році дотепер розвиток системи кібербезпеки України був повільним, в тому числі через недоопрацьовану законодавчу базу, але досвід протистояння на цифровому фронті чималий. А з оновленням Стратегії можна сподіватись на прискорення процесу.

Всупереч поширеним очікуванням, використання кіберзброї у війні Росії з Україною поки що було обмеженим. Проте, цілями зловмисників стають не лише державні установи. Вагомою мішенню, за даними CERT-UA, стають також громадяни. Так, хакери намагаються отримати доступ до облікових записів Telegram або отримати дані, надсилаючи на електронні скриньки громадян фішингові листи.

Безумовно війна Росії проти України, з одного боку, сповільнить розвиток кіберсистеми, з іншого боку – фахівці отримають великий досвід у протидії кіберзлочинам завдяки підтримці міжнародних партнерів. До того ж, наслідки війни значно позначяться й на глобальній кіберспільноті з огляду на цінності та у поглядах на відповідальність за скоєні дії.

Особливістю кіберпростору є те, що щоб захистити установу або уряд, знадобиться багато ресурсів. Щоб атакувати систему, потрібен лише один-двоє кваліфікованих осіб, а коли таких людей велика кількість, агресивні дії несуть великий ризик. До того ж, є ймовірність втратити контроль над заподіяною шкодою і тоді під удар потрапляє не лише запланована ціль.

Хоч високорозвинена держава не може дозволити собі відступати від цифрових технологій або уникати їх використання через кіберзагрози, треба пам’ятати, що активна діяльність у кіберпросторі поза межами власних кордонів має свої наслідки. Глобальна геополітична напруженість зростає, а життя у XXI столітті активно спрямовується у цифровий простір. Оскільки зростає всеосяжна економічна інтеграція держав, то наслідки технологічних ушкоджень можуть бути негативними далеко не для однієї держави. З моральної та етичної точки зору, будь-яка кібератака тягне за собою втручання, викрадення або пошкодження часто приватної та конфіденційної інформації користувачів та чутливої інформації для державних служб. Тому обмеження доступності інформації та основоположної її інфраструктури, наприклад, у формі зупинки мережі, в наслідок направлених кібератак, порушує широкий спектр прав: необґрунтоване обмеження доступу до інформації і можливостей людей висловлюватись та мирно спілкуватися, користуватися цілим рядом економічних, соціальних та культурних благ. У свою чергу, для держави-замовника кібератаки подібні дії можуть призвести до зниження рівня довіри міжнародної спільноти, та утвердженню репутації, як актора, що дестабілізує міжнародне безпекове середовище. Звідси правові та етичні аспекти кібербезпеки не менш важливі ніж технічні.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ


1. Гаценко А., Садомська Б. Нова стратегія кібербезпеки: як Україна захищатиметься в кіберпросторі? Adastra. 14.02.2022. URL: https://adastra.org.ua/blog/nova-strategiya-kiberbezpeki-yak-ukrayina-zahishatimetsya-v-kiberprostori?fbclid=IwAR3GZdsJPY6rggiqE8Ms-eFARNbyAi-2uAU6CHkKnA8f2GKAZ9fAtE9qBWA
2. Гордійчук Д. Кібератака за мільйони доларів: за нападом може стояти РФ. Економічна правда. 16.02.2022. URL: https://www.epravda.com.ua/news/2022/02/16/682428/
3. Дерев'янко О. Яка міжнародна підтримка у сфері кібербезпеки потрібна Україні? Delo.ua. 14.02.2022. URL: https://delo.ua/opinions/yaka-miznarodna-pidtrimka-u-sferi-kiberbezpeki-yaknaisvidse-potribna-ukrayini-392745/
4. Дмитро Кулеба: Україна отримає комплексну пропозицію ЄС задля системного зміцнення кібербезпеки. Представництво України при Європейському Союзі. 21.02.2022. URL: https://ukraine-eu.mfa.gov.ua/news/dmitro-kuleba-ukrayina-otrimaye-kompleksnu-propoziciyu-yes-zadlya-sistemnogo-zmicnennya-kiberbezpeki
5. Дубов Д. В. Формуючи нову стратегію кібербезпеки України: чи можемо уникнути помилок першої спроби стратегування? Національний інститут стратегічних досліджень. 27.01.2021. URL: https://niss.gov.ua/sites/default/files/2021-01/tezy-dubov-2.pdf
6. Закон України "Про основні засади забезпечення кібербезпеки України" від 14.04.2016 № 2126а. Верховна Рада України. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=55657
7. Захист інформаційного та кіберпростору. Служба безпеки України. 02.2022. URL: https://ssu.gov.ua/zabezpechennia-informatsiinoi-bezpeky
8. Інтенсивність кібератак на Укренерго після вторгнення рф зросла утричі. УкрІнформ. 06.04.2022. URL: https://www.ukrinform.ua/rubric-

economy/3450550-pisla-vtorgnenna-rf-intensivnist-kiberatak-na-ukrenergo-zrosla-utrici.html

9. Кібератака на держструктури України: що сталося та хто може стояти за нападом. Слово і діло. 14.01.2022. URL: https://www.slovoidilo.ua/2022/01/14/stattja/bezpeka/kiberataka-derzhstruktury-ukrayiny-stalosya-ta-xto-mozhe-stoyaty-napadom
10. Кібератаки на держоргани України: скільки інцидентів було заблоковано. Слово і діло. 15.02.2022. URL: https://www.slovoidilo.ua/2022/02/15/infografika/bezpeka/kiberataky-derzhorhany-ukrayiny-skilky-incydentiv-bulo-zablokovano
11. Конгресмени просять Байдена посилити кіберзахист України. Українська Правда. 06.04.2022. URL: https://www.pravda.com.ua/news/2022/04/6/7337485/
12. Луценко Є. В Україні вночі сталася кібератака на сайти міністерств і Кабміну. В СБУ кажуть, що витоку даних не було (ОНОВЛЕНО). Громадське. 14.01.2022. URL: https://hromadske.ua/posts/v-ukrayini-vnochi-stalasya-kiberataka-na-sajti-ministerstv-i-kabminu-voni-dosi-ne-pracyuyut
13. Най Дж. Вісім правил кібербезпеки. Що придумали в ООН. НВ. 5.12.2019. URL: https://nv.ua/ukr/opinion/vosem-pravil-kiberbezopasnosti-chto-pridumali-v-oon-50057635.html
14. Нова масштабна кібератака: ключові урядові сайти знову "лягли". BBC News Україна. 23.02.2022. URL: https://www.bbc.com/ukrainian/news-60497679
15. План реалізації Стратегії кібербезпеки України від 03.02.2022. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/n0087525-21#n3
16. Результати СБУ за І півріччя 2021 року. СБУ. URL: https://ssu.gov.ua/rezultaty-sbu-za-i-pivrichchia-2021-roku
17. Указ Президента України №96/2016 Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію

кібербезпеки України". URL: https://www.president.gov.ua/documents/962016-19836

18. Хакерські атаки: які країни найчастіше зазнають нападів і чим це небезпечно. Слово і Діло. 08.11.2021. URL: https://www.slovoidilo.ua/2021/11/08/video/suspilstvo/xakerski-ataky-yaki-krayiny-najchastishe-zaznayut-napadiv-chym-ce-nebezpechno
19. Abbany Z. Ukraine: Cyberwar creates chaos, 'it won't win the war'. Made for Minds. 03.03.2022. URL: https://www.dw.com/en/ukraine-cyberwar-creates-chaos-it-wont-win-the-war/a-60999197
20. Abukevicius M. Post. Twitter. 22.02.2022. URL: https://twitter.com/AbukeviciusM/status/1496061646946586625?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1496061646946586625%7Ctwgr%5E%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fwww.eurointegration.com.ua%2Fnews%2F2022%2F02%2F22%2F7134436%2F
21. Advancing Cyberstability. Final report. Global Commission on the stability of cyberspace. 11.2019. URL: https://cyberstability.org/norms/#toggle-id-1
22. Ang C. The Most Significant Cyber Attacks from 2006-2020, by Country. Visual Capitalist. 04.2021. URL: https://www.visualcapitalist.com/cyber-attacks-worldwide-2006-2020/
23. Bajak F. Ukraine volunteer ‘hacker’ corps fights Russia with cyberattacks, intel and infowar. The Times of Israel. 05.03.2022. URL: https://www.timesofisrael.com/ukraine-volunteer-hacker-corps-fights-russia-with-cyberattacks-intel-and-infowar/
24. Burnham K. Cybersecurity Trends Emerging in 2022. Northeastern University. 14.05.2021. URL: https://www.northeastern.edu/graduate/blog/trends-in-cybersecurity/
25. Cavelty D. M. Cyber security meets security politics: Complex technology, fragmented politics, and networked science. Contemporary Security Policy. Vol. 41, 2020 - Issue 1: Special issue: Cyber Security Politics. Pp. 5-32. URL: https://www.tandfonline.com/doi/full/10.1080/13523260.2019.1678855

26. Cavelty D. M., Egloff, F. J. The Politics of Cybersecurity: Balancing Different Roles of the State. St Antony's International Review, 15(1). 2019. P. 37–57. URL: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Dunn_Cavelty_Egloff_2019%20STAIR%20Issue%2015.1.pdf
27. Cavelty D. M., Wenger A. Cyber Security Politics: Socio-Technological Transformations and Political Fragmentation. Center for Security Studies, Swiss Federal Institute of Technology (ETH), Zurich. 2022. 287 p. URL: https://library.oapen.org/bitstream/id/20a53302-dee5-4834-9d98-8f9c07f0a602/9781000567113.pdf
28. CERT-UA. Новини. URL: https://cert.gov.ua/articles
29. Cerulus L. EU to mobilize cyber team to help Ukraine fight Russian cyberattacks. Politico. 21.02.2022. URL: https://www.politico.eu/article/ukraine-russia-eu-cyber-attack-security-help/
30. Cooper J. R. New Approaches to Cyber-Deterrence: initial thoughts on a new framework. Issue. 29.12.2009. 161 p. URL: https://issuu.com/bugmenot2/docs/new_approaches_to_cyber_deterrence./88
31. COVID-19 Related Malicious File Detections. McAfee. URL: https://www.mcafee.com/enterprise/en-gb/lp/covid-19-dashboard.html#overview
32. Cyber Conflict Around the Globe. Information Security Institute. Johns Hopkins University. URL: https://cyberheatmap.isi.jhu.edu
33. Daniel M. Why Is Cybersecurity So Hard? Harvard Business Review. 22.05.2017. URL: https://hbr.org/2017/05/why-is-cybersecurity-so-hard
34. Demarest C. US Cyber Command reinforces Ukraine and allies amid Russian onslaught. Defense News. 07.04.2022. URL: https://www.defensenews.com/cyber/2022/04/07/us-cyber-command-reinforces-ukraine-and-allies-amid-russian-onslaught/
35. Dziedzic S. Australia promises cyber support to Ukraine as Russian forces array along its borders. ABC News. 21.02.2022. URL:

https://www.abc.net.au/news/2022-02-21/ukraine-australia-cyberattack-russia-war-cybersecurity/100846870

36. Ebert H., Maurer T. The impact of cybersecurity on international relations. Oxford University Press. 12.02.2017. URL: https://blog.oup.com/2017/02/impact-cyber-security-international-relations/
37. Eleven Emerging Cybersecurity Trends in 2021. Panda. 12.04.2021. URL: https://www.pandasecurity.com/en/mediacenter/tips/cybersecurity-trends/
38. Fadia A., Nayfeh M., Noble J. Follow the leaders: How governments can combat intensifying cybersecurity risks. McKinsey & Company. 16.09.2020. URL: https://www.mckinsey.com/industries/public-and-social-sector/our-insights/follow-the-leaders-how-governments-can-combat-intensifying-cybersecurity-risks
39. Farrell H. The political science of cybersecurity I – why people fight so hard over cybersecurity. The Washington Post. 23.01.2014. URL: https://www.washingtonpost.com/news/monkey-cage/wp/2014/01/23/the-political-science-of-cybersecurity-i-why-people-fight-so-hard-over-cybersecurity/
40. Four reasons cybersecurity field rapidly growing. Tulane University. 2020. URL: https://sopa.tulane.edu/blog/four-reasons-cybersecurity-field-rapidly-growing
41. Garkov K. Cyber Security: Between Technical Issues and Political Priorities. International center for Defence and Security. 15.09.2017. URL: https://icds.ee/en/cyber-security-between-technical-issues-and-political-priorities/
42. Global Cybersecurity Index 2014. International Telecommunication Union Publications. 15 p. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/WP-GCI-101.pdf
43. Global Cybersecurity Index 2017. International Telecommunication Union Publications. 78 p. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf

44. Global Cybersecurity Index 2018. International Telecommunication Union Publications. 92 p. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf
45. Global Cybersecurity Index 2020. International Telecommunication Union Publications. 172 p. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf
46. Hakmeh J., Naylor E. How the tech community has rallied to Ukraine's cyber-defence. The Guardian. 07.03.2022. URL: https://www.theguardian.com/commentisfree/2022/mar/07/tech-community-rallied-ukraine-cyber-defence-eu-nato
47. Hansen L., Nissenbaum H. Digital Disaster, Cyber Security, and the Copenhagen School. International Studies Quarterly №53, 2009. Pp. 1155–1175. URL: https://nissenbaum.tech.cornell.edu/papers/Digital%20Disaster.pdf
48. How the cyber world can support Ukraine. The European Sting. 21.03.2022. URL: https://europeansting.com/2022/03/21/how-the-cyber-world-can-support-ukraine/
49. Huet N. Ukraine war: What part is hackers' collective Anonymous playing in the war effort against Russia? EuroNews. 28.02.2022. URL: https://www.euronews.com/next/2022/02/28/ukraine-war-what-part-is-hackers-collective-anonymous-playing-in-the-war-effort-against-ru
50. Inside Ukraine's online defence: the battle against Moscow's cyber attacks. Financial Times. 21.03.2022. URL: https://www.ft.com/content/20544951-2c98-4d47-842d-b34a246a564f
51. Kagubare I. US, EU cyber investments in Ukraine pay off amid war. The Hill. 13.03.2022. URL: https://thehill.com/policy/technology/597921-us-eu-cyber-investments-in-ukraine-pay-off-amid-war/
52. Kegley C. W., Raymond G. A. Realism in the Age of Cyber Warfare. Carnegie Council for Ethics in International Affairs. 26.04.2021. URL: https://www.ethicsandinternationalaffairs.org/2021/realism-in-the-age-of-cyber-warfare/

53. Kolbe P., Zabierek L., Morrow M. The Cybersecurity Risks of an Escalating Russia-Ukraine Conflict. Harvard Business Review. 24.02.2022. URL: https://hbr.org/2022/02/the-cybersecurity-risks-of-an-escalating-russia-ukraine-conflict
54. Kramer F. D.,Cyberpower and National Security: Policy Recommendations for a Strategic Framework. National Defense University Press. 01.04.2009. 18 p. URL: https://ndupress.ndu.edu/Publications/Article/1216674/cyberpower-and-national-security/
55. Kuehl. D. T. From Cyberspace to Cyberpower: Defining the Problem. 2020. 17 p. URL: https://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSP-Exports/Cyberpower/Cyberpower-I-Chap-02.pdf?ver=2017-06-16-115052-210
56. Libicki M. C. Cyberdeterrence and Cyberwar. Strategic Studies Quarterly. Vol. 5, No. 1. Air University Press. pp. 148-150. URL: https://www.jstor.org/stable/26270515?seq=1
57. Liedekerke A., Laudrain A. Russia's Cyber War: What's Next and What the European Union Should Do. Council on Foreign Relations. URL: https://www.cfr.org/blog/russias-cyber-war-whats-next-and-what-european-union-should-do
58. Lonergan E. D. Cyber Proxies in the Ukraine Conflict: Implications for International Norms. Council for Foreign Relations. 21.03.2022. URL: https://www.cfr.org/blog/cyber-proxies-ukraine-conflict-implications-international-norms
59. Madnick S. What Russia's Ongoing Cyberattacks in Ukraine Suggest About the Future of Cyber Warfare. Harvard Business Review. 07.03.2022. URL: https://hbr.org/2022/03/what-russias-ongoing-cyberattacks-in-ukraine-suggest-about-the-future-of-cyber-warfare?registration=success
60. Microsoft Digital Defense Report. October, 2021. 134 p. URL: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi
61. Milmo D. China accused of cyber-attacks on Ukraine before Russian invasion. The Guardian. 02.04.2022. URL:

https://www.theguardian.com/technology/2022/apr/01/china-accused-of-launching-cyber-attacks-on-ukraine-before-russian-invasion

62. National cyber security index. Ukraine. URL: https://ncsi.ega.ee/country/ua/
63. Nye J. S. Jr. Cyber Power. Harvard Kennedy School. 05.2010. 30 p. URL: https://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf
64. Paul K. 'Catastrophic' cyberwar between Ukraine and Russia hasn't happened (yet), experts say. The Guardian. 09.03.2022. URL: https://www.theguardian.com/technology/2022/mar/09/catastrophic-cyber-war-ukraine-russia-hasnt-happened-yet-experts-say
65. Pipikaite A., Bester L. How the cyber world can support Ukraine. World Economic Forum. 19.03.2022. URL: https://www.weforum.org/agenda/2022/03/how-the-cyber-world-can-support-ukraine/
66. Politics, cyber-security, trade and the future of ICT supply chains. The Economist. Intelligence Unit Limited. 02.2014. 66 p. URL: https://shorturl.ae/zbqfb
67. Richards J. Cyber Warfare. Oxford Bibliographies. 09.10.2019. URL: https://www.oxfordbibliographies.com/view/document/obo-9780199743292/obo-9780199743292-0076.xml.
68. Rid T. Why You Haven't Heard About the Secret Cyberwar in Ukraine. The New York Times. 18.03.2022. URL: https://www.nytimes.com/2022/03/18/opinion/cyberwar-ukraine-russia.html
69. Rivero N. Stop waiting for a "cyber Pearl Harbor". Quartz. 10.08.2021. URL: https://qz.com/2044945/the-threat-of-a-cyber-pearl-harbor-is-a-red-herring/
70. Sanger D. E., Barnes J. E., Conger K. As Tanks Rolled Into Ukraine, So Did Malware. Then Microsoft Entered the War. The New York Times. 28.02.2022. URL: https://www.nytimes.com/2022/02/28/us/politics/ukraine-russia-microsoft.html

71. Scroxton A. Cyber companies step up support for Ukraine. TechTarget. 02.03.2022. URL: https://www.computerweekly.com/news/252514063/Cyber-companies-step-up-support-for-Ukraine
72. Secure Cyberspace: How is Cyberspace Different from the Physical World? Wisdom Plexus. 2021. URL: https://wisdomplexus.com/blogs/secure-cyberspace/#:~:text=Since%20Cyberspace%20is%20completely%20different,treated%20as%20a%20cyberspace%20violation
73. Seven Essential Features of Cyber Security One Should Know. Jaro education. 2019. URL: https://www.jaroeducation.com/blog/7-essential-features-of-cyber-security-one-should-know/
74. Shad M. Cyber Threat in Interstate Relations: Case of US-Russia Cyber Tensions. Policy Perspectives: The Journal of the Institute of Policy Studies. 2018. Pp. 41 - 55. URL: https://www.scienceopen.com/hosted-document?doi=10.13169/polipers.15.2.0041
75. Special Report: Ukraine. Microsoft. 27.04.2022. URL: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd
76. Srivastava M., Murgia M., Murphy H. The secret US mission to bolster Ukraine's cyber defences ahead of Russia's invasion. Financial Times. 09.03.2022. URL: https://www.ft.com/content/1fb2f592-4806-42fd-a6d5-735578651471
77. Stupp C. U.S., European Allies Offer Ukraine Cyberdefense. WSJ pro Cybersecurity. 01.02.2022. URL: https://www.wsj.com/articles/u-s-european-allies-offer-ukraine-cyberdefense-11643744602#top
78. Tashev B., Purcell M., McLaughlin B. Russia's Information Warfare: Exploring the Cognitive Dimension. Marine Corps University Journal, Vol. 10, № 2. 2019. P. 129-147. URL: https://www.usmcu.edu/Portals/218/MCUJ_Fall2019_10_2_web.pdf
79. Theisen T. The Cybersecurity Ripple Effects of the Russia-Ukraine Conflict. JDSupra. 23.03.2022. URL: https://www.jdsupra.com/legalnews/the-cybersecurity-ripple-effects-of-the-1117292/Tsakanyan V. The role of

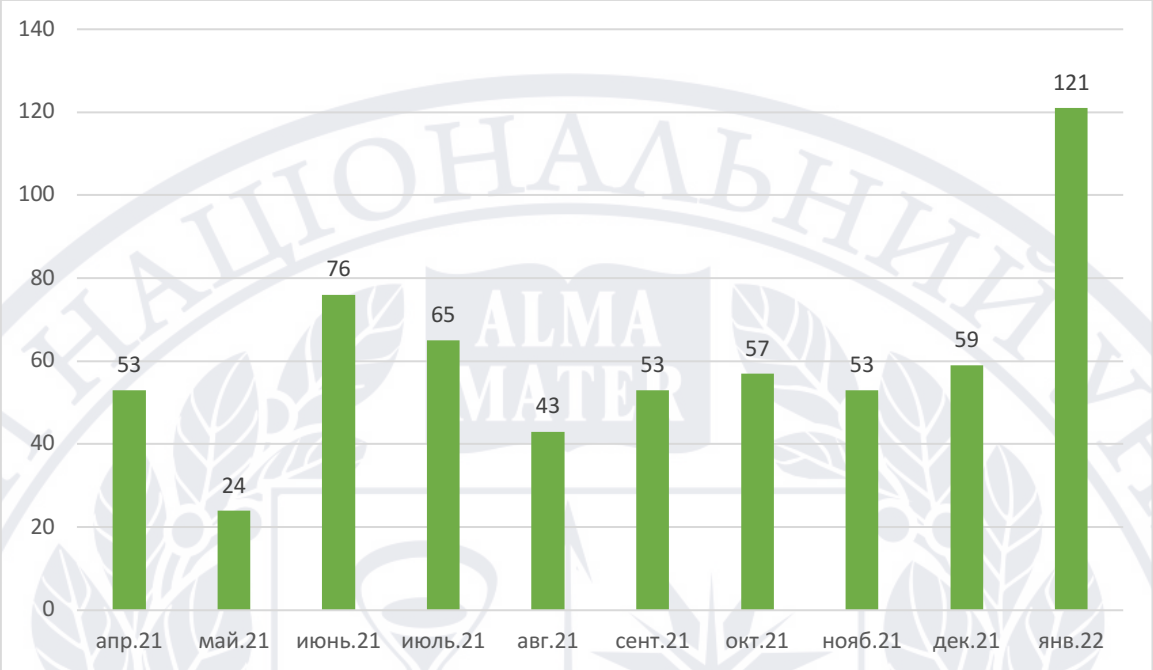
cybersecurity in world politics. Research Gate. 12.2017. 9 p. URL: https://www.researchgate.net/publication/316949336_The_role_of_cybersecurity_in_world_politics

80. Tidy J. Anonymous: How hackers are trying to undermine Putin. BBC News. 20.03.2022. URL: https://www.bbc.com/news/technology-60784526
81. Ukraine: Timeline of Cyberattacks on critical infrastructure and civilian objects. CyberPeace Institute. 27.04.2022. URL: https://cyberpeaceinstitute.org/ukraine-timeline-of-cyberattacks?utm_source=google&utm_medium=cpc&utm_campaign=ukraine&utm_term=kinetics&utm_content=1&gclid=Cj0KCQjwpImTBhCmARIsAKr58cw74TXYBaumNv0F5NlOuIutt4iM55rgd8Y0wL7CHiFbw_kEw_udc_EaAg71EALw_wcB
82. Understand the mistakes that compromise your company's cybersecurity. Psychology of human error. Tessian. 2022. 24 p. URL: https://f.hubspotusercontent20.net/hubfs/1670277/%5BCollateral%5D%20Tessian-Research-Reports/%5BTessian%20Research%5D%20Psychology%20of%20Human%20Error%202022.pdf?utm_referrer=https%3A%2F%2Fwww.tessian.com%2F
83. Valeriano B., Lonergan E. What Ukraine Shows about Cyber Defense and Partnerships. CATO Institute. 17.03.2022. URL: https://www.cato.org/commentary/what-ukraine-shows-about-cyber-defense-partnerships
84. Valori G. E. Cyberspace and world politics. ModernDiplomacy. 13.08.2021. URL: https://moderndiplomacy.eu/2021/08/13/cyberspace-and-world-politics/
85. Vallor S., Rewak W. An Introduction to Cybersecurity Ethics. 2019. 65 p. P. 7-13. URL: https://www.scu.edu/media/ethics-center/technology-ethics/IntroToCybersecurityEthics.pdfWelle D. Ukraine: Cyberwar creates chaos, 'it won't win the war'. Taiwan News. 03.03.2022. URL: https://www.taiwannews.com.tw/en/news/4461548

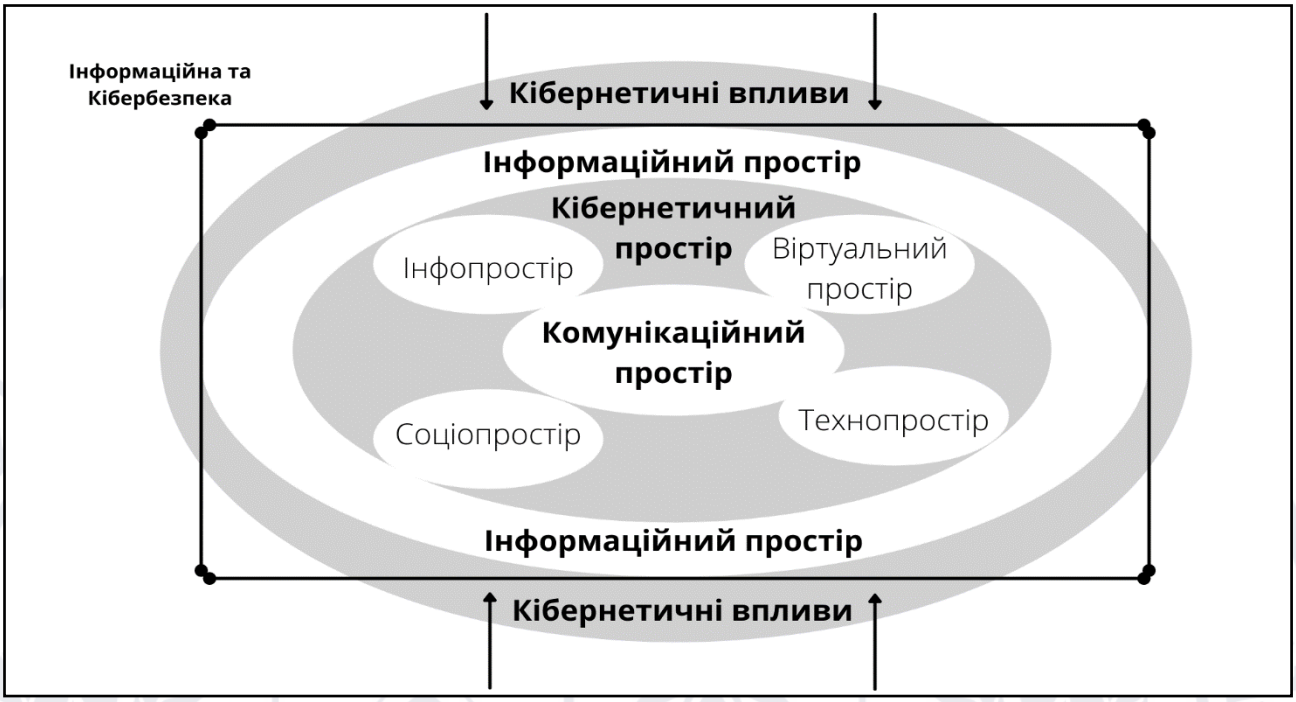
86. Willett M. Russia–Ukraine: Pressing the right button at the right time. International Institute for Strategic Studies. 10.03.2022. URL: https://www.iiss.org/blogs/analysis/2022/03/russia-ukraine-pressing-the-right-button-at-the-right-time
87. Welle D. Ukraine: Cyberwar creates chaos, 'it won't win the war'. Taiwan News. 03.03.2022. URL: https://www.taiwannews.com.tw/en/news/4461548
88. Whyte C. Learning the Right Cybersecurity Lessons From Putin. Foreign Policy Magazine. 24.03.2022. URL: https://foreignpolicy.com/2022/03/24/russia-war-cybersecurity-digital-threat/

# ДОДАТКИ

**Додаток 1.** Кількість кібератак на держоргани України.



**Додаток 2.** Взаємозв'язок інформаційного та кіберпростору.



**Додаток 3.** Динаміка показників кризового менеджменту та управління інцидентами.

**Додаток 4.** Порівняльна таблиця Глобального індексу сил кібербезпеки та Національного індексу кібербезпеки.

| | **Глобальний індекс сил кібербезпеки (The Global Cybersecurity Index)** | **Національний індекс кібербезпеки (National Cybersecurity Index)** |
|---|---|---|
| **Об'єкт вимірювання** | Виконання зобов'язань центральної влади щодо кібербезпеки | Готовність країн запобігати кіберзагрозам та управляти кіберінцидентами |
| **Мета** | Розробка міжнародної системи кібербезпеки та національної політики в галузі кібербезпеки | Надання інформації про сучасні національні системи кібербезпеки, розробку національних систем та політик кібербезпеки |
| **Завдання** | • Допомога країнам визначити напрямки вдосконалення<br>• Визначення та просування кращих практик кіберзахисту<br>Сприяння розвитку світової культури кібербезпеки | • Підвищення обізнаності щодо рівня розвитку сучасних національних систем кібербезпеки<br>• Порівняння власного рівня розвитку системи кібербезпеки з іншими країнами<br>Поширення інформації про найкращі практики |
| **Кількість індикаторів** | 25 індикаторів – 50 питань | 46 індикаторів |
| **Основні категорії оцінювання** | • Правові заходи<br>• Технічні заходи<br>• Організаційні заходи<br>• Спроможності для розвитку кібербезпеки<br>Співпраця | • Загальні показники кібербезпеки (розробка політики кібербезпеки, аналіз кіберзагроз та обмін інформацією, освіта та професійний розвиток, внесок у глобальну кібербезпеку)<br>• Базові показники кібербезпеки (захист цифрових послуг, захист основних послуг, електронна ідентифікація та послуги довіри, захист |

| | | |
|---|---|---|
| | | персональних даних)<br>Показники управління аваріями та кризовими ситуаціями (реагування на кіберінциденти, управління кіберкризисами, боротьба з кіберзлочинністю, військові кібер операції) |