НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»

Факультет психології, політології та соціології
Кафедра політичних теорій

Магістерська робота

052 «Політологія»

на тему:

«Кібербезпека як елемент національної безпеки»

Виконала: здобувачка 2 курсу
галузь знань: 05 «Соціальні та поведінкові науки»
спеціальність 052 «Політологія»
Ткачук Катерина Сергіївна

Керівник: доцент, к.політ.н.,
доцент Пехник А.В
Рецензент: професор, д.політ.н.,
професор Мамонтова Е.В.

Одеса – 2022

ЗМІСТ

ВСТУП

Актуальність теми дослідження обумовлена принциповою важливістю сучасного стану кібербезпекової політики в світі. Розвиток інформаційних технологій обумовив виникнення принципово нової сфери людського життя – кіберпростору, що з кожним днем стає все більш важливою частиною повсякденного існування.

Безмежність кіберпростору, його залежність від складних інформаційних технологій та активного використання електронних пристроїв та сервісів, що охоплюють майже всі сфери суспільного життя, визначають нові можливості, але при цьому й створюють нові загрози інтересам, правам і життєдіяльності громадян, організацій та діяльності державних органів. Проведення кібератак проти інформаційних ресурсів зі сторони кіберзлочинців і кібертерористів, використання сучасних засобів кіберзброї в рамках конфліктів та кібервійн, роблять питання розвитку і забезпечення кібербезпеки країн актуальним як ніколи раніше. Слід зазначити принципову важливість даного дослідження також й на фоні Російського вторгнення в Україну та розвитку сучасних гібридних війн та конфліктів в світі.

Тема магістерської роботи є актуальною як в науковому, так і в практичному плані. Наукова, пізнавальна актуальність полягає в необхідності дослідження поняття «кібербезпеки», оскільки в сучасній науці не існує чітко окресленого підходу до його сутності та розуміння. Практична актуальність теми дослідження обумовлена виникненням принципово нових інформаційних засобів та методів використання інструментів кіберпростору, та особливостями їх реалізації та результатів, які характеризуються новими політичними та економічними викликами для сучасних розвинених країн.

Ступінь наукової розробленості проблеми. Дослідженнями у цій сфері займалися такі вчені як: В. Ліпкан, праці якого присвячені питанням національної, міжнародної та інформаційної безпеки України; І. Діордіца, який займався дослідженнями в сфері кібербезпеки та надав власне визначення поняття кібертероризму; Ю. Завгородня, яка проводила дослідження в сфері кібербезпеки та

кіберконфліктів; Д. Мінін який виділив підходи до визначення поняття кібербезпеки; а також З. Коваль; А. Пехник, В. Шеломенцев; О. Глазов, Л. Кормич, Е. Мамонтова, С. Кухаренко, О. Запорожець, Дж. Вайс, Р. Кларк та інші.

Мета магістерської роботи полягає у комплексному аналізі феномену «кібербезпеки» та визначені його ролі в сучасній системі національної безпеки. Досягнення мети обумовлено вирішенням наступних ***дослідницьких завдань***:

- проаналізувати феномен «національна безпека» та визначити особливості його формування;
- дослідити поняття «кібербезпеки» та актуалізувати його значення в контексті політологічного знання;
- визначити загальну характеристику та проаналізувати поняття «кіберзагроза» та «кібератака»;
- визначити та охарактеризувати сучасні види кібератак, їх прецеденти;
- дослідити та охарактеризувати кібертероризм та кібервійну, як загрози XXI століття;
- проаналізувати національну систему кібербезпеки, як частини національної безпеки України;
- дослідити та визначити рівень ескалації кіберзагроз національним інтересам України в умовах війни;
- проаналізувати та визначити особливості зарубіжного досвіду кібербезпекової політики в контексті політики національної безпеки.

Об'єктом дослідження є національна безпека.

Предметом дослідження кібербезпека як елемент національної безпеки.

Методи дослідження були визначені метою, завданнями та складністю наукового дослідження. Специфіка дослідження обумовила необхідність використання як загальнофілософських: аналіз, синтез, дедукція та індукція, так і спеціальних методів, а саме системний, структурно-функціональний, історичний. В

поданій роботі системний метод використовувався для визначення загальної характеристики понять «кібербезпека» та «національна безпека»; структурно-функціональний – для дослідження окремих елементів та сфер кібербезпеки; історичний метод для спостереження динаміки зміни важливості розвитку кібербезпеки в світі, формально-логічний використовується для аналізу термінів, їх класифікації, типологізації досліджуваних явищ пов'язаних з поняттям кібербезпеки.

Структура бакалаврської роботи. Магістерська робота складається зі вступу, трьох розділів, висновків, списку використаної літератури, додатків.

РОЗДІЛ І
ТЕОРЕТИЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ КІБЕРБЕЗПЕКИ ЯК СКЛАДОВОЇ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

1.1 Теоретичний аналіз феномену «національна безпека» та особливостей його формування

XXI століття – епоха інноваційних технологій, розвитку всіх сфер людської діяльності, науки та філософії, але не дивлячись на досвід отриманий з минулого, перед людством все ще постають старі небезпеки, та виникають нові. Новий час потребує нового переосмислення системи національної безпеки, яка є дуже важливою складовою функціонування кожної держави.

Практичне значення терміну «національна безпека» вперше визначилось в політичній культурі США. В 1904 році президент Теодор Рузвельт у своєму посланні Конгресу, визначив встановлення контролю США над територією Панамського каналу з 1904 року по 31 січня 1999 року, інтересами «національної безпеки» США. Вже в 1947 році США прийняли закон «Про національну безпеку» для утвердження внутрішньої та зовнішньої політики Сполучених Штатів Америки.

Теоретиками філософії політики, національна безпека визначається як сукупність внутрішніх та зовнішніх умов для забезпечення стабільної еволюції держави та суспільства, захист своїх кордонів від зовнішніх загроз. Встановлені основні ознаки національної та/або інших видів безпеки : безумовна можливість для проведення державою самостійної внутрішньої та зовнішньої політики та відсутність зовнішнього втручання в діяльність держави.

Сучасна світова політика є системою зовнішньополітичної діяльності держав, міжнародних організацій, політичних партій, рухів, груп інтересів та політичних лідерів. Ознаки світової політики включають в себе всі процеси та явища, які властиві системі міжнародних відносин, а основою світової політики є взаємодія між двома або

більше державами, у формі співробітництва, суперництва або інших формах, які виділяються сучасними науковцями.

Співробітництво держав проявляється в розширенні політичних зв'язків між ними на взаємовигідній основі або близькості геополітичних інтересів, взаємодоповненні політичних культур та систем, релігій та ідеологій, а також цивілізаційної чи етнічної близькості та інших факторів.

З другої половини XX століття під впливом інтернаціоналізації та глобалізації міжнародних відносин та загострення глобальних проблем система світової політики поступово розширювалась. Такі проблеми світової політики як : збереження балансу сил; забезпечення військової безпеки; урегулювання економічного співробітництва; фактори енергетичних, продовольчих, демографічних, та екологічних проблем людства, роблять питання національної безпеки набуває більшої важливості та актуальності.

Баланс сил в світовій політиці – це сукупність переваг та недоліків силових характеристик держав як суб'єктів міжнародної політики, у відношенні до поставлених ними цілями і завданнями, а також вживаними заходами в міждержавних взаємодіях.

На сьогоднішній день існують різні визначення та трактування поняття «національна безпека», так на думку В. Ліпкана національна безпека представляє собою сукупність офіційно прийнятих поглядів на цілі та державну стратегію в галузі забезпечення безпеки особистості, суспільства й держави від внутрішніх та зовнішніх загроз економічного, політичного, військового, соціального, екологічного, техногенного та іншого характеру з урахуванням наявних в державі можливостей та ресурсів [23] .

Національну безпеку також розуміють як певну здатність нації задовольняти власні потреби, необхідні для її самозбереження, самовідтворення, функціонування і самовдосконалення з мінімальним ризиком шкоди для базових цінностей її нинішнього стану.

Науковець О. Глазов вбачає в понятті «національна безпека», насамперед, захищеність життєво важливих інтересів особистості, суспільства й держави в різних сферах життєдіяльності від внутрішніх та зовнішніх загроз, що й забезпечує стійкий сталий розвиток країни [17].

Деякі вчені визначають безпеку як стан, за якого в державі відсутні загрози. Так наприклад, під національною безпекою розуміється «такий стан країни, при якому відсутні або усунені реальні зовнішні та внутрішні небезпеки її національним інтересам, а також національному характеру життя».

Таким чином, можна зазначити, що науковці по-різному характеризують дане поняття, але більшість сходяться в тому, що національна безпека – це безпека та захист суверенної держави, включаючи її громадян, економіку та інституції, що є обов'язком уряду держави [24]. Поняття «національна безпека» спочатку мало на увазі саме захист держави від військового нападу, проте зараз дане поняття в широкому розумінні включає в себе також і не військові сфери, такі як економічна безпека, енергетична безпека, екологічна безпека, продовольча безпека та інші.

Під системою забезпечення національної безпеки слід розуміти систему нормативно-правових, теоретико-методологічних, інформаційно-аналітичних, розвідувальних, організаційно-управлінських, кадрових, науково-технічних, контррозвідувальних, ресурсних та інших заходів, які спрямовані на забезпечення процесу управління небезпеками та загрозами, за якого різними державними та недержавними інституціями гарантується прогресивний розвиток національних інтересів, джерел духовного і внутрішнього добробуту народу, а також ефективне функціонування самої системи забезпечення національної безпеки.

В сучасній науковій спільноті виділяють як мінімум три основні теоретичні підходи до розуміння національної безпеки.

До представників першого підходу відносяться такі вчені як : Р. Коен, Д. Гадді, Дж. Джонсон, А. Волферс та інші. Їх увага акцентується саме на захисті цінностей суспільства, і тут виділяють політичну незалежність, економічний добробут,

розвиток, справедливість та інше. При цьому безпека виражається не тільки у захищеності національних цінностей, а й у її безперешкодному поширенні. Аналізуючи даний підхід, слід обов'язково звернути увагу на Стратегію національної безпеки США, адже саме вона дуже добре відображає головну думку даного підходу. У ній стверджується що «з метою захисту нашої нації та поваги до наших цінностей США прагнуть поширити свободу у всьому світі, очолюючи міжнародні зусилля зі знищення тиранії та підтримки ефективної демократії» [49]. Даний підхід не обійшли стороною, і такі всесвітньо відомі автори і науковці як С. Хантінгтон та Ф. Фукуяма. В своїй роботі «Кінець історії та остання людина», Ф. Фукуяма стверджує, що сучасні ліберальні демократії не становлять загрози одна одній, а тому війни між справді демократичними державами стають майже неможливими. На думку С. Хантінгтона, яку він виразив у своїй роботі «Зіткнення цивілізацій», лінії розлому між цивілізаціями і будуть тими самими лініями фронтів у майбутніх війнах. Підхід до забезпечення національної безпеки шляхом поширення власних цінностей, в тому числі і за допомогою збройних сил, містить деструктивний потенціал для виникнення майбутніх конфліктів між державами.

Представники другого підходу : В. Горбулін, І. Волощук, В. Ліпкан та інші, наголошують на взаємозв'язку інтересів та національних цінностей, а також необхідності врахування їх взаємообумовленості в системі дослідження проблем національної безпеки.

Щодо третього підходу, то його представники зосереджують увагу на дослідженні національної безпеки в контексті захисту національних інтересів. До них відносимо : М. Каплана, Г. Моргентау, А. Бетлера, О. Бодрука, С. Хоффмана та інших. Вчені також роблять акцент на розширенні змісту поняття «національної безпеки». Раніше забезпечення національної безпеки розглядалось виключно в контексті захисту інтересів держави, проте в сучасних дослідженнях увага зміщується вже на захист інтересів громадянина та суспільства. Даний підхід є досить суперечливим серед різних науковців, оскільки зосереджує увагу виключно на інтересах держави,

розвитку її військового і економічного потенціалу й підпорядкування цим цілям інтересів окремих особистостей. Проблема співвідношення інтересів особи, суспільства й держави в політиці національної безпеки досі є актуальною і не вирішеною. Слід зазначити, що саме держава відіграє головну роль в системі забезпечення національної безпеки, оскільки власне державні органи та посадові особи формують нормативно-правову базу у сфері забезпечення національної безпеки, а також приймають рішення щодо запобігання загрозам і їх нейтралізації. Варто також акцентувати увагу на тому, що застосування воєнної сфери та здійснення інших передбачених законом заходів примусового характеру щодо забезпечення національної безпеки є виключно монополією держави.

Сучасна наука про безпекознавство виділяє такі основні елементи національної безпеки : державна безпека; безпека особистості; громадська безпека; екологічна безпека; техногенна безпека; економічна безпека; енергетична безпека; інформаційна безпека; кібербезпека [24].

Громадяни, суспільство і держава є головними об’єктами національної безпеки, саме тому виділяють такі основні чинники впливу на національну безпеку:

- внутрішньополітична стабільність;
- готовність і здатність політичних сил реалізувати визначені цілі;
- економічні можливості держави;
- національне визначення та самобутність;
- національна згода та єдність;
- національна незалежність і суверенітет, територіальна цілісність держави;
- наявність загальної стратегії національного розвитку, «національної ідеї», загальновизнаної мети;
- розвиненість громадянського суспільства, рівень демократизму, сформованість і дієвість законодавчої бази правової держави, захищеність особи;
- розвиток національної самосвідомості й культури;

- стан збройних сил, їхню боєздатність і боєготовність.

Міністр оборони США 1977-1981 років, Г. Браун казав, що «національна безпека – це здатність зберегти фізичну цілісність і територію країни; підтримувати її економічні відносини з рештою світу на розумних умовах; зберегти її природу, інституції та управління від підриву ззовні, а також контролювати її кордони» [2].

Захист державного та суспільного ладу, забезпечення територіальної цілісності та суверенітету, забезпечення політичної та економічної незалежності нації, її здоров'я, охорона громадського порядку, боротьба із злочинністю та забезпечення техногенної безпеки є головними цілями та завданнями національної безпеки.

1.2 Концептуалізація поняття «кібербезпеки» в контексті політологічного знання

Сучасний розвиток інформаційних технологій поступово змінює світ. Звичне людське спілкування все більше переходить з реального життя в мережу Інтернет, доступ до майже всієї людської історії можна отримати просто на екрані смартфону, а взаємодія з більшістю державних служб з часом буде витрачати лише кілька кліків мишкою за комп'ютером.

Інформаційні технології стали невід'ємною складовою життя сучасного суспільства, а оскільки інформація є одним з найцінніших і важливіших ресурсів будь-якої сфери життя, інформаційна безпека стає найбільш важливим аспектом нашого життя, ведення бізнесу чи функціонування держави.

Інформаційна безпека включає в себе сукупність мір та засобів, спрямованих на усунення та запобігання несанкціонованого доступу, обробки, модифікації, форматування, аналізу, виправлення чи знищення даних.

Проблема захисту інформації від несанкціонованого доступу та небажаного впливу існує вже дуже давно, разом із розвитком людського суспільства, появою приватної власності, державного ладу, подальшим розширенням людської діяльності,

інформація набуває все більшого значення. Вона стає ціннішою, а контроль над нею надає можливість отримати певні привілеї.

Інформаційні технології та Інтернет значно спрощують людське життя, але чи дійсно все так райдужно як нам здається?

Разом із усіма перевагами сучасного цифрового світу, перехід на інформатизовані системи звичайних сфер людського життя та навіть органів державної влади, обумовив виникнення нових загроз національній та міжнародній безпеці. Жодна система не може існувати без інформаційних потоків, а порушення їх роботи або їх нехватка призводить до втрати ефективності та зниженню динаміки розвитку. Інформаційна сфера є рушійним фактором життя суспільства та активно впливає та стан політичної, економічної та військової сфер.

Доки одна людина використовує мережу Інтернет для замовлення піци на вечерю, інші намагаються отримати доступ до даних державної важливості, які можуть спричинити дуже страшні наслідки. От тут і виникає потреба у створенні спеціальних методів та засобів захисту даних, а поруч із відомими нам повітрям, суходолом, морем та космосом виникає нова сучасна арена – кіберпростір.

Вперше поняття «кіберпростір» було використано письменником В. Гібсоном. У 1982 році опублікувавши свою новелу «Пекучий хром», він ввів даний термін, трохи пізніше у 1984 році у творі «Некромант» він розкриває його вже більш детально. За словами автора, «кіберпростір – це синергетична ілюзія, яку щодня відчувають мільярди звичайних операторів у всьому світі. Це логічне представлення відомостей, збережених в пам'яті та на носіях комп'ютерів всього розумного людства».

Мітчелл Капор разом із Джоном Перрі Барлоу у 1990 році опублікували свій маніфест «Перетинаючи електронні кордони». В ньому вони далі розвинули сутність та зміст концепції кіберпростору, а також підкреслили його інтерактивну складову [44].

З кінця XX століття в зарубіжній та міжнародній літературі все частіше з'являється термін «кіберпростір». У 2013 році група експертів НАТО запропонувала

нове визначення кібепростору як середовища, яке сформовано з фізичних та нефізичних елементів і характеризується використанням комп'ютерів та електромагнітного спектра для зберігання, модифікації та обміну даними з використанням комп'ютерних мереж.

Захист інтересів держав та громадян в кіберпросторі стає новим життєво важливим завданням, що перетворює використання ІТ-мереж та технологій на питання безпеки й оборони. Оскільки потенційна небезпека загрожує системам державного та військового управління, економіки та промисловості це актуалізує дослідження такого нового поняття як «кібербезпека».

Прийнято вважати, що вперше цей термін виник у середині 1990-х років, адже з саме того часу уряд США почав активно досліджувати цю тему. Багато країн прийняли або почали розробку власної стратегії в сфері кібербезпеки. Не дивлячись на те, що було проведено досить багато форумів, конференцій, семінарів та опублікована велика кількість робіт, присвячених різним аспектам кібернетичної безпеки, серед вчених й досі відсутнє єдине визначення поняття «кібербезпеки».

На думку Б.А. Кормич, «кібербезпека – це захищеність встановлених законом правил, за якими відбуваються інформаційні процеси в державі, що забезпечують гарантовані Конституцією умови існування і розвитку людини, всього суспільства та держави» [9].

Кібербезпека – це такий стан систем, за якого нейтралізуються загрози щодо доступності, цілісності або конфіденційності даних, які циркулюють в цих інформаційних системах.

На думку Ю.В. Завгородньої, «під час характеристики кібербезпеки дуже часто використовують поняття кіберзахисту, і слід відзначити, що кіберзахист є складовою частиною кібербезпеки, але це не тотожні поняття, адже кібербезпека – це узагальнена термінологія, а кіберзахист – конкретна форма впливу в конкретному напрямку для реалізації кібербезпеки» [9, с. 36].

Виділяють також інше визначення, при якому під кібербезпекою слід розуміти «окремий випадок інформаційної безпеки, поява якого обумовлена використанням телекомунікаційних мереж або комп'ютерних систем» [4]. В більш розгорнутому значенні, це «такий стан захищеності важливих інтересів держави, суспільства і особистості в умовах використання комп'ютерних систем або телекомунікаційних мереж, при якому завдання їм шкоди мінімізується через: невчасність, неповноту або невірогідність інформації, що використовується; несанкціоноване поширення, використання і порушення цілісності, конфіденційності та доступності інформації; негативні наслідки функціонування інформаційних технологій». Об'єктом даного визначення є інформація, яка і є головним учасником інформаційних правовідносин, які відбуваються у кіберпросторі. Серед основних ознак інформації виділяють: селективність, субстанціональну несамостійність, системність, невичерпність, здатність до трансформування, масовість, універсальність та якість. З юридичної точки зору інформація є тиражованою, має фізичну невідчужуваність та властивість екземплярності. Вона може бути одночасно відома багатьом, а при існуванні на матеріальному носії – також і належати необмеженій кількості осіб.

Саме існування цих ознак і є першопричиною для виникнення кібербезпеки. Кібербезпека – це захист кіберсистем від неправильного користування, що може нанести шкоди, та від інших деструктивних дій.

Аналізуючи визначення, можна також окремо виділити дії, які порушують системи інформаційної безпеки:

- безпекові інциденти як наслідок непередбачених і ненавмисних подій, таких, як природні лиха, зброї в роботі апаратних засобів та програмного забезпечення, людські помилки;
- деструктивні атаки на мережі, зокрема атаки на доменні імена, сервери або перевантаження мережі штучними повідомленнями, атаки, спрямовані на порушення маршрутизації;
- неавторизований доступ до комп'ютера або комп'ютерних мереж;

- перехоплення електронної комунікації, копіювання або модифікація даних;
- підробка веб-сайтів;
- шкідливе (піратське) програмне забезпечення.

На мою думку, кібербезпеку також слід розуміти як захист інформаційних систем, які входять до складу кіберпростору, від дій та нападів; забезпечення цілісності, конфіденційності та доступності інформації, яка опрацьовується в цьому просторі, а також виявлення і протидія атакам і кіберінцидентам.

Структура інформаційної системи складається з окремих її частин – підсистем. Підсистема – це виділена певною ознакою частина системи. Таким чином будь-яка інформаційна система може бути представлена у вигляді сукупності підсистем, які забезпечують її інформаційне, програмне, технічне, організаційне та правове забезпечення.

Для повноти картини, окремо також виділяють саме поняття «кібернетична безпека», під ним мають на увазі «стан захищеності, певних життєво важливих інтересів людини та громадянина, суспільства та держави в кіберпросторі» [20]. В даному випадку, визначення терміну кібернетичної безпеки базується на визначенні поняття «кібернетичного простору», який визначається як «середовище, яке виникає в результаті функціонування на принципів та загальних правил інформаційних та телекомунікаційних систем». З цього визначення можна зробити висновок, що під середовищем розуміється сукупність інформаційних або автоматизованих, телекомунікаційних та інформаційно-телекомунікаційних систем.

Поруч із цим постає питання ідентифікації життєво важливих інтересів громадянина та людини, суспільства та держави, які виникають в цьому середовищі. Проте дане завдання стає дещо абсурдним, оскільки в такому середовищі відсутні якісь суспільні відносини між суб'єктами.

Слід зосередити увагу на тому, що через неповне або неправильне розуміння поняття кібербезпеки, та надання йому хибного визначення, втрачається або стає

неможливим ідентифікація цілей і стратегій, пов'язаних з його реалізацією, а також визначення предмету та об'єкту, які характеризують його діяльність.

Я вважаю, логічніше буде визначити, що кібербезпека – це сукупність методів та практик захисту від атак зловмисників, для збереження даних комп'ютерів, комп'ютерних мереж, серверів, мобільних пристроїв та електронних систем, або по іншому – збереження даних в кіберпросторі.

Завдяки такому визначенню ми розуміємо головну мету кібербезпеки: захист даних, та можемо визначити де саме буде розгортатися діяльність щодо її реалізації.

Ще одним важливим питанням є принципова різниця між поняттями «*кібербезпеки*» та «*інформаційної безпеки*». Досить часто ці поняття ототожнюються, або взагалі використовуються в якості синонімів. Проте в дійсності, ці терміни сильно відрізняються і не є взаємозамінними. В той час коли, кібербезпека розуміється як захист даних від атак в кіберпросторі, інформаційна безпека – є захистом даних від будь-яких форм загроз, незалежно від того, чи є вони цифровими або аналоговими.

Після вирішення проблеми із визначенням терміну «кібербезпека», зосередимо увагу на сфері інтересів даної діяльності. Практики кібербезпеки можуть застосовуватися в зовсім різних направленнях, від промислових підприємств до звичайних мобільних пристроїв середньостатистичних користувачів.

Безпека критичної інфраструктури - це заходи щодо захисту комп'ютерних мереж, об'єктів критичної інформаційної інфраструктури. До таких об'єктів відносять електричні мережі, транспортні мережі, автоматизовані системи управління та інформаційно-комунікаційні системи та інші системи, захист яких є життєво важливим для безпеки країни і спокійного життя її громадян.

Мережева безпека – захист базової мережевої інфраструктури від несанкціонованого доступу та неправильного використання, а також від крадіжки інформації. Технологія передбачає створення безпечної інфраструктури для пристроїв, додатків та користувачів.

Безпека додатків – заходи безпеки, які застосовуються на рівні додатків (комп'ютерних або мобільних програм) та направлені на попередження крадіжки, взлому даних або коду додатку. Методи включають в себе питання безпеки, які виникають під час розробки, проектування, реалізації та експлуатування додатку.

Хмарна безпека (від англ. *Cloud Security*) – взаємопов'язаний набір елементів управління та інструментів захисту систем хмарних обчислень від кіберзагроз. Заходи хмарної безпеки направлені на забезпечення безпеки даних, онлайн-інфраструктури, а також додатків та платформ. Хмарна безпека має ряд загальних концепцій з традиційною кібербезпекою, проте в цій сфері є також і власні передові методи та унікальні технології [20].

Система навчання користувачів – програма підвищення знань в сфері інформаційної безпеки та кібербезпеки, яка є важливою умовою при створенні надійної системи захисту будь-якої компанії або навіть держави. Дотримання правил «цифрової гігієни» допомагає посилити рівень безпеки, таким чином користувачі, які заздалегідь проінформовані про небезпеки, не стануть відкривати підозрілі електронні листи та відмовляться від використання ненадійних засобів переносу інформації.

Аварійне відновлення (планування) безперервності бізнесу – сукупність стратегій, політичних правил та процедур, які визначають яким чином організація має реагувати на потенційні загрози або непередбачувані стихійні лиха, для того щоб належним чином адаптуватися до них та мінімізувати негативні наслідки.

Операційна безпека – процес керування безпекою та ризиками, які попереджують потрапляння інформації в чужі руки. Початково принципами операційної безпеки користувалися військові, аби не допустити можливість потрапляння секретних даних до супротивника, проте в сучасності практики операційної безпеки широко використовуються для захисту бізнесу та держави від потенційних витоків даних [25].

В сучасному світі спостерігається стрімкий ріст числа кіберзагроз. ЗМІ щодня повідомляють про нові випадки викрадення інформації або взлому важливих сервісів

даних. Державні структури та бізнес намагаються вистояти проти цих атак, які спустошують банківські рахунки громадян, а тому надійний захист від загроз цифрового світу стає базовою необхідністю для кожного з нас. Стає очевидним важливість кібербезпеки в сфері національної безпеки кожної країни. Збереження даних пересічних громадян та критичних структур функціонування держави стає одним з найголовніших завдань сучасних урядів.

Протистояння в кіберпросторі є небезпечною складовою нової проблеми людства - гібридних війн. Для цього необхідне швидке та ефективне реагування на будь-які кіберзагрози, що неможливе без створення та інтегрування в систему державного управління чіткої системи методів та засобів реалізації кібербезпеки. Очевидною стає потреба створення національної системи кібербезпеки, та її нормативно-правового забезпечення на всіх державних рівнях.

РОЗДІЛ ІІ
КІБЕРЗАГРОЗИ НАЦІОНАЛЬНІЙ БЕЗПЕЦІ : ВИДИ ТА ЗАСОБИ ЇХ ПОПЕРЕДЖЕННЯ

2.1 Загальна характеристика та аналіз понять: «кіберзагроза» та «кібератака»

«Ми повинні навчитися домовлятися про нову географію, де кордони не мають значення, а відстані — безглузді, де ворог може завдати шкоди життєво важливим системам, від яких ми залежимо, не протистоячи нашій військовій силі.»

Саме такі слова в 1997 році президент США Білл Клінтон висловив щодо результатів дослідження спеціальної «Президентської комісії із захисту критичної інфраструктури США». Комісія визначила певні фізичні і кібернетичні вразливості, які існують в системі. Також, не дивлячись на те, що безпосередньої кризи, яка б загрожувала інфраструктурі країни, комісією виявлено не було, все одно мала місце стурбованість щодо потенційних небезпек, які несе за собою кіберпростір.

Швидке зростання населення, яке володіє комп'ютерною грамотністю, що передбачає потенційне збільшення кількості хакерів, а також властива вразливість загальних протоколів у комп'ютерних мережах, легка доступність хакерських «інструментів» (різних сайтів), і той факт, що ці основні інструменти хакерів (телефонні лінії, модеми, комп'ютери) є тими самими основними технологіями, які щоденно використовуються звичайним населенням, вказувало комісії на існування загроз та вразливостей.

Основними «цінностями в небезпеці» через кіберзагрози та вразливі місця є активи та репутація організацій, або навіть держав. Через критичну залежність, наслідки для цих активів можуть стати результатом більшої, каскадної події, що буде знаходитись поза контролем суб'єкта її господарювання.

Визначимо, що взагалі мається на увазі під поняттям кіберзагрози. Кіберзагроза – це будь-яка виявлена спроба, спрямована на доступ, викрадення, маніпулювання або порушення цілісності, конфіденційності , безпеки чи доступу до даних, програм чи державної системи без законних на це повноважень. Також, це потенційні кіберподії, які можуть спричинити небажані наслідки, що призводять до шкоди системі чи організації. Загрози можуть виникати ззовні або із середини, а також від окремих осіб, організацій або країн.

Кіберзагрози – це будь-що, що може поставити під загрозу безпеку або завдати шкоди інформаційним системам та пристроям, підключеним до мережі Інтернет (включно із апаратним забезпеченням, програмним забезпеченням і пов'язаною із цим інфраструктурою), даним на них і послугам, які вони надають, переважно за допомогою кіберзасобів [19].

Вони можуть бути навмисними або ненавмисними, таргетованими або нонтаргетними (безцільовими) , та можуть надходити з різних джерел, зокрема з іноземних держав, залучених у шпигунство та інформаційну війну, злочинців, хакерів, розробників вірусів, або навіть незадоволених співробітників чи підрядників, які працюють в організації.

Ненавмисні загрози можуть бути спричинені неуважними або ненавченими співробітниками, оновленням програмного забезпечення, процедурами технічного обслуговування та збоями обладнання, які випадково порушують роботу комп'ютерних систем або пошкоджують дані на них.

Навмисні загрози включають в себе, як *таргетні*, так і *нонтаргетні* атаки. Таргетна або ж цілеспрямована атака – це дія, під час якої група або окрема особа спеціально атакує систему критичної інфраструктури. Нонтаргетна атака виникає у випадку, коли мета атаки не є визначеною, наприклад, коли вірус або зловмисне програмне забезпечення випущено в мережу Інтернет, без якоїсь конкретної цілі [19].

Найбільш тривожною загрозою неодноразово визнається саме «*інсайдер*» - або хтось, із законним доступом до системи чи мережі. Інші зловмисники можуть

використовувати інсайдерів, чи то організована злочинна група чи терористична організація, підпорядковуючи добровільного інсайдера (наприклад, незадоволеного працівника компанії) або використовуючи спонтанного (випадкового) інсайдера.

Існує велика кількість джерел кіберзагроз, зокрема слід виділити:

Оператори бот-мереж – оператори використовують мережу або ботнет спеціально скомпрометованих дистанційно керованих систем для координації атак і розповсюдження фішингових схем, спаму та атак зловмисного програмного забезпечення. Послуги цих мереж іноді доступні на підпільних ринках.

Бізнес-конкуренти – компанії, що конкурують із цільовою компанією або ведуть із нею бізнес, можуть прагнути отримати певну конфіденційну інформацію, для покращення своєї конкурентної переваги в різних сферах, таких як ціноутворення, виробництво, розробка продукту та укладення контрактів.

Злочинні угрупування – групи людей, що намагаються атакувати системи з метою отримання грошової вигоди. Зокрема, організовані злочинні групи використовують спам, фішинг та шпигунське/зловмисне шпигунське забезпечення для крадіжки особистих даних і шахрайства і Інтернеті. Міжнародні корпоративні шпигуни та злочинні організації також становлять загрозу для США через їхню здатність здійснювати промислове шпигунство та великомасштабні грошові крадіжки, а також наймати та розвивати таланти хакерів.

Іноземні держави – іноземні розвідувальні служби використовують кіберінструменти як частину своєї діяльності зі збору інформації та шпигунства. Крім того, деякі країни активно працюють над розробкою доктрин, програм і можливостей інформаційної війни. Такі можливості дозволяють одній організації мати значний і серйозний вплив, порушуючи постачання, комунікації та економічну інфраструктуру, яка підтримує військову міць держав. Зростаюча кількість державних і недержавних супротивників все частіше націлюється на інформаційну інфраструктуру з метою експлуатації, потенційного підриву чи її знищення, включаючи сюди Інтернет,

телекомунікаційні мережі, комп'ютерні системи та вбудовані процесори та контролери в системах критичних галузей.

Хакери – особи, що проникають у мережі, окрім інших причин, для того щоб отримати задоволення від протиправної діяльності та похвалитись в хакерській спільноті, або отримати грошову вигоду. Колись отримання несанкціонованого доступу вимагало від хакера певних навичок в програмуванні, тепер же вони можуть завантажувати готові програми, сценарії та протоколи атаки з Інтернету, та просто запускати їх проти сайтів-жертв. Таким чином, засоби атаки з часом стали не тільки більш досконалими, а ще й легшими у використанні. Переважна більшість хакерів не мають необхідного досвіду для великої загрози безпеці різних комп'ютерних мереж або важливої інфраструктури. Проте кількість хакерів у всьому світі становить відносно високу загрозу ізольованого або короткочасного збою, що може спричинити серйозну шкоду деяким організаціям або навіть країнам.

Хактивісти – ті, хто здійснюють політично мотивовані атаки на загальнодоступні веб-сторінки чи сервери електронної пошти. Ці групи та особи перевантажують сервери та зламують веб-сайти, для того щоб надіслати політичне повідомлення.

Інсайдер – невдоволена особа, яка працює всередині організації, та є основним джерелом комп'ютерних злочинів. Інсайдерам може не знадобитися велика кількість знань про комп'ютерні системи, адже частіше за все вони є просто підрядниками, і передають реальному злочинцю необмежений доступ, для завдання шкоди системі або викрадення системних даних.

Міжнародні корпоративні шпигуни – які становлять загрозу через свою здатність здійснювати економічне та промислове шпигунство та масштабні грошові крадіжки, а також наймати та розвивати таланти хакерів.

Фішери – окремі особи або невеликі групи людей, які використовують схеми фішингу, намагаючись викрасти ідентифікаційні дані або інформацію з метою

отримання грошової вигоди. Фішери також можуть використовувати спам та шпигунське програмне забезпечення для досягнення своїх цілей [20].

Спамери – окремі особи чи організації, що розповсюджують інформацію за допомогою електронної пошти, задля продажу продуктів, здійснення фішингових схем, розповсюдження зловмисного програмного забезпечення або атаки на організації.

Творці зловмисного програмного забезпечення (шпигунських програм) – особи чи організації із зловмисними намірами, які здійснюють атаки на користувачів шляхом створення та розповсюдження шкідливих комп'ютерних програм. Деякі такі програми можуть нанести удару навіть державним структурам, або повністю стерти дані серверів.

Терористи (кібертерористи) – люди чи організації, що прагнуть вивести з ладу, знищити або використати критично важливу інфраструктуру задля заподіяння шкоди національній безпеці країн, спричинити масові жертви чи послабити економіку. З появою більш компетентного технічного покоління хакерів, зростає рівень кіберзагроз у всіх країнах світу.

Визначивши основні поняття пов'язані з кіберзагрозами, перейдемо до конкретних засобів їх реалізації.

Атака на комп'ютерні мережі або *кібератака* – це зловмисний комп'ютерний код або інші направлені дії, призначені для зміни, руйнування, заборони, погіршення або знищення інформації (що знаходиться в комп'ютерах та комп'ютерних мережах) або навіть самих комп'ютерів та мереж. Використання кібератак, можливо протягом тривалого періоду часу – для зміни, зриву, погіршення, або знищення інформаційних систем та мереж супротивника або інформації чи програми. Такий вплив на ворожі системи також може мати непрямий вплив на об'єкти, пов'язані з ними або залежні від них.

Кібератака – це будь-яка навмисна дія, яка впливає на бажаний доступ до даних чи систем, невід'ємних від операційних результатів даної організації. Не всі

кібервторгнення є атаками; насправді переважна більшість робить зовсім інше. Кібератаки можуть мати тимчасові або постійні наслідки; вони можуть руйнувати обладнання або лише порушувати роботу послуг; також вони можуть проводитися дистанційно або з закритим доступом (у тому числі інсайдерами). Крім того, значна увага приділяється кібератакам, спрямованим на дані та програмне забезпечення у роботі, уразливість ланцюга постачання викликає дедалі більше занепокоєння у світі, де критично важлива інфраструктура будується та підтримується через глобальний ланцюг постачання, що піддається змінам на різних етапах життєвого циклу системи.

2.2 Кібератаки: види та сучасні прецеденти

Через відсутність повного розуміння того як працює мережа Інтернет та програмне забезпечення телефонів чи комп'ютерів, люди часто недооцінюють шкоду, яку можуть завдати кібератаки.

Кібератаки можуть здійснюватися кількома способами, такими як люди, ланцюги поставок апаратного забезпечення, а також шкідливі програми, що передаються через мережу.

Гаррієт Пірсон та Джеймс Денвіл з Вашингтону, в 2017 році видавши свою статтю «Управління кіберризиками робочої сили в глобальному просторі : юридичний огляд» зазначили, що «55% усіх кібератак є результатом зловмисних або ненавмисних дій працівників» [45].

В останнє десятиліття прийнято виділяти такі типи та методи кібератак:

Атака на відмову в обслуговуванні (*DDoS-атаки*) – атаки спрямовані на вимкнення та неспроможність жертви працювати. За допомогою скоординованої атаки з великої кількості комп'ютерів, користувачі яких часто навіть і не помічають, що їх пристрій став одним з «зомбі» у армії хакера [32].

DDoS-атаки відбуваються у два етапи. По-перше, зловмисник захоплює велику кількість хост-комп'ютерів в мережі Інтернет та встановлює на них програму, яка

дозволить йому будь-коли віддалено контролювати ці пристрої. По-друге, пізніше хакер надсилає команду головним комп'ютерам одночасно розпочати атаку на цільову мережу (компанію, організацію, чи навіть державний орган).

Блюджекінг (від англ. *bluetooth hijacking*) – атака, що здійснюється на мобільні пристрої з підтримкою Блютуз (стільникові телефони, смартфони, комп'ютери). Зловмисник надсилає небажані повідомлення або файли користувачеві з підтримкою Блютуз. Фактичні повідомлення не завдають шкоди пристрою, але вони використовуються, для того щоб змусити користувача відповісти належним чином або додати новий контакт до адресної книги пристрою. Ця атака нагадує спам та фішинг, які здійснюються проти користувачів електронної пошти.

Ботнет, раніше я вже згадувала про цей вид кіберзагроз, але зараз хочу зосередити на ньому трохи більше уваги. Він представляє собою мережу скомпрометованих (або заражених) комп'ютерів, якими дистанційно керують зловмисники. Вони використовуються для розсилки величезної кількості спаму, а також координації поодиноких атак на відмову у обслуговуванні (або по іншому DDoS) чи сприяння фінансовому шахрайству чи махінаціям з особистими даними. Саме боти становлять серйозну небезпеку в онлайн-середовищі, а також знижують рівень довіри серед користувачів мереж. Слід зазначити, що першопочатково боти не несли негативних наслідків, адже вони використовувалися для забезпечення спілкування в Інтернеті в спеціальних чатах, які були популярні в 1990-2000 роках. Однак програмісти придумали їм зовсім інше призначення, і зараз слово «бот» асоціюється в більшості із чимось негативним. Ботнети стають основним інструментом сучасної кіберзлочинності, частково тому, що вони можуть бути розроблені для дуже ефективного руйнування цільових комп'ютерних систем. Їх часто називають «швейцарськими армійськими ножами», оскільки вони є дуже універсальними.

Ще окремо виділяють Інтернет-ботів, які зосереджені на різних сайтах та в соціальних мережах. Частіше за все це спеціально створені штучні аккаунти, або старі

взламані. Деякі сайти навіть спеціально продають бази даних покинутих аккаунтів, а тому побачити дописи під постами відомих блогерів від неіснуючих або давно загиблих людей, стає реальністю XXI століття.

Атака за допомогою *сніфферу* (програми нюхача) – програми, які перехоплюють маршрутизовані дані та перевіряють кожен пакет у пошуках певної інформації, такої як паролі, передані відкритим текстом. Сніфери відстежують мережевий трафік у дротових та бездротових мережах і перехоплюють пакети даних. Загалом ці програми можуть бути налаштовані на захоплення як всіх пакетів, або лише деяких з окремими обраними характеристиками.

Вразливість SQL-ін'єкцій - це спосіб виклику виконання певної команди бази даних на віддаленому сервері. Виконання такої команди може спричинити витік інформації, створити вектор для вандалізму, або забезпечити впровадження шкідливого програмного забезпечення, яке згодом буде активовано на пристрої жертви [1].

Логічна бомба – комп'ютерна програма, яка може виконувати певну корисну функцію, але при цьому містить прихований код, активація якого може знищувати дані, форматувати жорсткий диск або випадково вставляти файли-сміття у дані. Логічна бомба може потрапити в комп'ютер, коли користувач завантажує програми чи інший файл, який було видозмінено. Після активації або встановлення, логічна бомба завдає шкоди негайно. Серед програмістів дані атаки визначаються як форма саботажу.

Бєкдор (запасний вихід) – також його часто називають люком або золотим ключем доступу, це апаратний або програмний механізм, який забезпечує доступ до системи та її ресурсів за допомогою обходу заходів безпеки через спеціальний залишений розробниками запасний протокол. Бекдори задумувались як спеціальний інструмент для самих розробників, задля покращення своїх програм, проте після завершення розробки деякі з бєкдорів просто забували прибрати, і таким чином деякі програми можуть легко змінюватися зловмисниками [19].

Також слід приділити увагу найвідомішому тріо Інтернету – *вірусу, хробаку та трояну*.

Хробак (з англ. *Worm*) – незалежна програма, яка відтворюється шляхом копіювання однієї системи в іншу через мережу. Хробаки можуть виконувати шкідливі дії, наприклад споживати мережеві або локальні системні ресурси, що також є однією з причин DDoS-атак, а також зв'язувати всі обчислювальні ресурси в мережі та фактично вимикати її. Зазвичай хробак активується під час кожного запуску системи.

Появу хробаків відносять ще до часів перших комп'ютерів, а так звані «великі хробаки» як Melissa(1999), ILOVEYOU(2000), SoBig(2003) та Mydoom(2004), почали поширюватися в суспільстві за допомогою електронної пошти ще наприкінці 1990-х років. Ці програми могли подвоювати кількість комп'ютерів-жертв кожні одну-дві години, та досягали свого піку вже через 12-18 годин після запуску в мережу.

Вірус – самовідтворюваний шкідливий код, що приєднується до іншої програми чи компоненту системи та не залишає явних ознак своєї присутності. Він намагається поширюватися з комп'ютера на комп'ютер, проте на відміну від хробака, для поширення вірусу потрібна участь людини (зазвичай навіть неспеціально). Його можна передати за допомогою електронного листа, компакт-диску, USB-флешки, або файлу з хмари. Вони можуть містити звичайні повідомлення чи зображення, та просто споживати простір і пам'ять комп'ютера, або у більш серйозних випадках, знищувати файли і спричиняти цим пошкодження системи.

Trojan (троянський кінь) – програма, що приховує деструктивний код. Як правило, троянський кінь маскується під корисну програму, яку користувачі мають запустити. Він працює або виглядає, як і очікувалось, але також завдає прихованої шкоди. Троян дещо схожий на вірус, за винятком того, що він не розмножується. Такі програми можуть видаляти деякі файли під час кожного свого використання, доки з часом не призведуть до помилок в системі, або до її недієздатності.

Зростання кількості фінансових операцій в мережі Інтернет призвела до підвищення кількості інцидентів безпеки та появи нових типів шкідливого програмного забезпечення та атак. Сьогодні масових хробаків чи спалахів вірусів відбувається все менше і менше, а поява прихованого програмного забезпечення, такого як трояни та бекдори, зростає.

Говорячи про кіберзагрози, слід також згадати й про такі типи кібервпливів як : «порушення конфіденційності інформації», «порушення доступності інформації», «порушення цілісності інформації» та психологічний вплив.

Для того щоб показати, що все вище сказане не є чимось нереальним, розберемо деякі найвідоміші кібератаки останнього десятиліття.

Взлом Capital One : в 2019 році з банківської системи американської компанії Capital One було викрадено інформацію понад 100 мільйонів користувачів. В червні 2022 року за цією справою було засуджено Пейдж Томпсон, колишню робітницю компанії Amazon, яка використала свої знання про вразливість хмарних серверів і викрала особисту інформацію людей. Правопорушниця заявляла, що вона є етичним хакером, і хотіла лише вказати компанії на прогалини в їх системі безпеки, проте під час розслідування були знайдені докази, що заперечували її слова. Даний інцидент показує серйозність небезпеки, яка може йти від інсайдерів.

WannaCry – програма-вимагач 2017 року, яка використовувала вразливість різних версій операційної системи Windows. Проникаючи в комп'ютери, вірус зашифровував всі дані, а потім вимагав гроші за їх розблокування, але нажаль розблокувати їх було неможливо. Вперше його було виявлено в Іспанії, а згодом і в інших країнах. Найбільше збитків програма завдала Україні, Росії та Індії. Програма зупинила роботу банків, урядових організацій та навіть аеропортів. У Великобританії деякі лікарні не змогли провести термінові операції через відмову систем. І досі невідомо, хто був реальним творцем даного вірусу. Він встиг вразити близько 500 тис. комп'ютерів у 150 країнах світу і завдати збитків на суму у 1 млрд. доларів.

Petya/NotPetya/ExPetr – перша версія вірусу з'явилася ще у березні 2016 року, але серйозні кібератаки почалися вже в 2017. Так само, як і WannaCry, Petya та його новіші версії вражали комп'ютери на базі Microsoft Windows. Вони зашифровували дані, а точніше робили базу даних з усією інформацією з пристрою, блокували користувачу доступ до них, та вимагали викуп у біткоїнах. Найбільша проблема полягала в тому, що навіть коли жертви платили гроші, та вводили необхідні коди, замість відновлення роботи свого пристрою, вони отримували комп'ютер з повністю знищеними даними. При цьому вірус отримував повний контроль над інфраструктурою компанії, в якій знаходився заражений пристрій. Найбільше від цього вірусу постраждала Україна. Пізніше під час аналізу цього інциденту, було виявлено що зараження вірусом почалося саме звідси. Причиною стало автоматичне оновлення бухгалтерської програми MTdoc, якою на той час користувалось більшість компаній та держорганів України.

Вірус торкнувся компаній та держорганів Європи, США, Австралії, України, Індії, Китаю та Росії. Серед постраждалих - міжнародні корпорації Merck, Maersk, TNT Express, Saint-Gobain, Mondelez, Reckitt Benckiser. В Україні постраждали понад 300 компаній, включаючи «Запоріжжяобленерго», «Дніпроенерго», Київський метрополітен, українські мобільні оператори «Київстар», LifeCell та «Укртелеком», магазин «Ашан», Приватбанк та аеропорт Бориспіль. 10% пам'яті всіх комп'ютерів країни виявилося стерто. Загальна сума збитків від діяльності хакерів склала понад 10 млрд. доларів.

Президентські вибори в США 2016 року : в липні були атаковані сервери Національного комітету Демократичної партії США та Комітету Демократичної партії з виборів до конгресу. Хакери використовували шкідливе програмне забезпечення для віддаленого керування серверами та передачі файлів, а також стеження за всіма діями користувачів у цій мережі. Після кібератаки хакери повністю стерли сліди своєї активності. Їм вдалося отримати доступ до електронної пошти кандидата у президенти від демократів Хіларі Клінтон та її команди. У результаті 30

тис. електронних листів було опубліковано на сайті WikiLeaks, включаючи 7.5 тис. документів, надісланих Клінтон. Велика кількість документів були секретними і стосувалися терористичних атак на консульство США у Бенгазі в 2012 році. Інші містили персональні дані членів та спонсорів демократичної партії, включаючи номери їх кредитних карток. Історія з листуванням викликала розкол усередині демократів та сильно похитнула їх позиції напередодні виборів. Скандал негативно вплинув на рейтинги Клінтон та можливо і був однією з причин її поразки на президентських виборах.

2.3 Загрози XXI століття : кібертерроризм та кібервійна

«Наступним Перл-Харбором, з яким ми зіткнемося, цілком може бути кібератака»

Колишній Міністр оборони США Леон Панетта

За даними Global Digital Report 2022, 67% населення землі використовують мобільні телефони, а кількість унікальних користувачів сягає 5,31 мільярда на початок 2022 року. Разом із цим рівень доступу в Інтернет становить 62,5% або 4,95 мільярда [42]. А тепер уявіть, що кожен мобільний телефон є потенційним інструментом зловмисників для доступу до конфіденційних даних, інфраструктури чи державних органів.

Стає зрозумілим поява принципово нового рівня в сфері кібербезпеки, та виокремлення нових понять як «кібертероризм» та «кібервійна».

Існує багато визначень терміну *кібертероризм*. Так наприклад, експерт з безпеки США Дороті Е. Деннінг визначає кібертероризм як «політично вмотивовані хакерські операції, спрямовані на заподіяння серйозної шкоди, такої як втрата життя або великих економічних збитків».

Дослідницька Служба конгресу США визначає цей термін як «політично вмотивоване використання комп'ютерів як зброї або цілей субнаціональними групами чи таємними агентами, які мають намір вчинити насильство, щоб вплинути на спільноту чи змусити уряд змінити свою політику».

Також, ФБР визначає кібертероризм як «навмисну, політично вмотивовану атаку на інформацію, комп'ютерні системи, програми та дані, що призводить до насильства проти некомбатантів з боку субнаціональних груп чи таємних агентів» [].

Власне визначення цього терміну має також Міжнародна спілка електрозв'язку, і визначає його як «незаконні атаки та погрози атаки на комп'ютери, мережі та інформацію, що зберігається, з метою залякування чи примусу щодо уряду або його народу для досягнення конкретних політичних чи соціальних цілей».

Виділяють також два окремі підходи щодо визначення даного терміну: з погляду наслідків та на основі намірів. Першим зазначається, що кібертероризм існує, коли комп'ютерні атаки призводять до настільки руйнівних наслідків, що викликають страх, який можна порівняти з традиційним терористичним актом, навіть якщо його здійснюють злочинці. Другий підхід акцентує увагу на тому, що кібертероризм існує, коли здійснюються незаконні або політично вмотивовані комп'ютерні атаки, щоб залякати чи примусити уряд та людей досягти політичних цілей або завдати шкоди населенню чи економічній сфері.

Деякі науковці також зазначають, що деякі фізичні атаки, які руйнують комп'ютеризовані вузли для критично важливої інфраструктури, такої як Інтернет, телекомунікації чи електромережі, також можуть сприяти кібертероризму або взагалі бути позначеними як акт кібертероризму.

Вже давно існують обґрунтовані докази того, що терористичні організації використовують кіберпростір для здійснення своєї діяльності. Ці угрупування користуються Інтернетом та всесвітньою мережею: для спілкування одне з одним; вербування членів; збору розвідданих; отримання грошей (законним і нелегальним

шляхом); організації і координування своєї діяльності; отримання незаконних паспортів, віз та поширення пропаганди.

Також слід навести кілька конкретних прикладів використання кіберпростору та Інтернет-мережі в діяльності різних терористичних організацій:

- деякі афганські терористи, такі як Усама бен Ладен, мають комп'ютери, комунікаційне обладнання та великі сервери для зберігання даних своїх операцій;
- близькосхідна терористична організація ХАМАС, використовує Інтернет-чати та електронну пошту для планування так координації операцій у Газі, на західному березі річки Йордан та в Лівані;
- Хізбалла, ще одне близькосхідне угрупування, керує кількома веб-сайтами в Інтернеті з метою пропаганди, для опису нападів на Ізраїль, а також одним для отримання новин та інформації;
- під час виборів в Індонезії, Шрі-Ланці та Мексиці, урядові комп'ютери були взламані терористичними групами;
- прихильники Ірландської республіканської армії злили в Інтернет конфіденційну інформацію про бази британської армії в Північній Ірландії, а також мають свій власний веб-сайт.

Даний феномен викликає і велику кількість критики серед різних спостерігачів та спеціалістів. Деякі науковці вважають, що термін «кібертероризм» є недоречним, оскільки широкомасштабна кібератака може просто викликати роздратування, але аж ніяк не жах, як бомба чи інша хімічна, біологічна, радіологічна чи ядерна зброя. Проте інші висловлюють думку, що наслідки широкомасштабної атаки на мережу будуть непередбачуваними та можуть спричинити достатні економічні зриви, страх і загибель цивільних, щоб кваліфікувати їх як тероризм.

В даному випадку, я підтримую важливість усвідомлення рівня небезпеки від кібератак. Сучасні компанії, організації та державні органи влади дуже сильно

залежать від стабільності роботи комп'ютерних мереж та інфраструктури комунікації, і майже неможливо реально оцінити наслідки масованої атаки на них.

Поруч із відомими нам поняттями як «локальний конфлікт», «військова агресія» та «війна», постає нова загроза XXI століття – «кібервійна».

Кібервійна (або з англ. *Cyberwarfare*) – будь-яка дія, спрямована на те, щоб змусити опонента виконати національну волю країни, вчинена проти програмного забезпечення, що контролює процеси в системі опонента. Включає в себе такі режими кібератак: кіберпроникнення, кіберманіпуляції, кібернапади та кіберрейди [12].

Також кібервійна передбачає проведення та підготовку спеціальних військових операцій відповідно до інформаційних принципів. Це означає «порушити, якщо навіть не знищити», інформаційні та комунікаційні системи, у широкому сенсі включають військову культуру, на яку супротивник покладається, щоб пізнати себе: «хто він, де, що може зробити, коли і чому він проводить ці дії, та яким загрозам має протистояти». Також такі дії потребують: отримання знань про супротивника, при цьому не надавши багато даних про себе; зміни балансу інформації та знань на свою користь, особливо якщо баланс сил не такий.

Кібервійна може включати: захист інформації та комп'ютерних мереж; стримування інформаційних атак і позбавлення супротивника можливості зробити те саме; наступальні операції проти супротивника або навіть домінування інформацією на полі бою; проникнення в комп'ютери та мережі; атаки на мережі за допомогою DDoS-атак; саботаж обладнання через кіберпростір; блокування датчиків і навіть маніпулювання надійними джерелами інформації, щоб контролювати мислення супротивника.

Під час визначення, чи є кібератака актом кібервійни, експерти оцінюють чотири ключові атрибути атаки:

Джерело: Чи була атака здійснена чи підтримана національною державою?

Наслідки: Чи завдав напад шкоди?

Мотивація: Чи був напад політично вмотивованим?

Рівень підготовки: Чи вимагала атака спеціальних методів, обладнання або складного планування?

Американські офіційні особи зазначають, що понад 20 країн проводять різного роду інформаційні операції, спрямовані проти Сполучених Штатів. ЦРУ засвідчило, що вороги включають кібервійну як нову частину своєї військової доктрини. Китай, Росія, Індія і Куба, за оцінкою ВМС США визначаються як країни, що визнали політику підготовки до кібервійни та які швидко розвивають свої можливості. Північна Корея, Лівія, Іран, Ірак і Сирія також мають певний потенціал, а Франція, Японія та Німеччина активно працюють у цій сфері [49].

Таким чином, поняття «кібертероризм» та «кібервійна» є невід'ємними складовими сучасного суспільства. Розвиток інформаційно-комунікаційних технологій дозволив кібератакам перейти на новий рівень, а шкода яку вони можуть нанести розцінюється в мільярдах доларів. Все це спричиняє нову тенденцію, за якою все більше і більше країн починають активно розвивати сферу кібербезпеки аби протистояти загрозам, або для того, щоб самим завдавати кібератак.

РОЗДІЛ ІІІ
ОСНОВНІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ ТА ДОСВІД ІНШИХ КРАЇН

3.1 Національна система кібербезпеки як складова частина національної безпеки України

Каталізатором змін у сфері кібербезпеки в нашій державі, безумовно, стала гібридна війна розв'язана РФ, в якій застосовується як класична зброя, так і нелетальна, в тому числі в кіберпросторі або через нього. Нові виклики та загрози національній безпеці України в кіберпросторі призвели до створення першої Стратегії кібербезпеки України, яка була впроваджена указом Президента від 15 березня 2016 року.

Перші спроби до створення нормативно-правового забезпечення кібербезпеки були зроблені ще набагато раніше в 2005 році, коли Україна ратифікувала «Конвенцію про кіберзлочинність» Ради Європи, проте саме Стратегія 2016 року стала повноцінним початком серйозного ставлення до проблем в кіберпросторі.

Сучасна українська система кібербезпеки ґрунтується на таких законодавчих документах, а саме:

- Стратегія кібербезпеки України (від 26 серпня 2021 року);
- Закон України «Про основні засади забезпечення кібербезпеки України» (2017 року, з останньою редакцією від 17 серпня 2022 року);
- Закон України «Про національну безпеку України» (2018 року, з останньою редакцією від 15 червня 2022 року).

Слід зазначити, що оскільки Стратегія кібербезпеки України 2021 року, була вже другою спробою українських законодавців в сфері кіберзахисту, в ній було зроблену певну роботу над помилками минулої стратегії, а також її зміст більше підходить до сучасних реалій в сфері розвитку кібепростору.

В стратегії зазначається принципова важливість розвитку законодавчого забезпечення в сфері захисту інформаційного простору та кіберпростору, також удосконалено нормативне забезпечення з питань кіберзахисту об'єктів критичної інфраструктури, ухвалено порядок її визначення та загальні вимоги до її кіберзахисту, чого не вистачало стратегії 2016 року [35].

Акцентовано увагу на тому, що для покращення кібербезпеки, створено спеціальні центри (підрозділи) в таких установах як: Державна служба спеціального зв'язку та захисту інформації України; Служба безпеки України; Національний банк України; Міністерство інфраструктури; Міністерство оборони та Збройні сили України; а при Раді національної безпеки і оборони, утворено новий робочий орган – Національний координаційний центр кібербезпеки, який має завдання забезпечення успішної координації діяльності суб'єктів сектору безпеки та оборони, які забезпечують кібербезпеку.

Ще одним важливим аспектом стратегії є активна співпраця України з іноземними партнерами, задля покращення сфери кіберзахисту, проведення кібернавчань за участю інших держав та міжнародних організацій, а також започаткування щорічного заходу – місяця кібербезпеки в Україні.

В стратегії 2021 року також міститься певна критика щодо діяльності влади у сфері кібербезпеки з 2016 по 2021 роки. Так тут зазначено, що реалізація минулої стратегії не перевищує 40%, а саме через проблеми у невизначенні чітких пріоритетів та напрямів забезпечення кібербезпеки в Україні, і незрозумілості кінцевої мети.

В новій стратегії зазначено, що основними загрозами кібербезпеці України є: гібридна агресія РФ проти України в кіберпросторі; кіберзлочинність; кібератаки організовані та спонсоровані урядами інших держав; кібертероризм. Також зазначено список передумов та чинників, які спричиняють окреслені загрози, а саме: висока технологічна залежність нашої держави від продукції інформаційно-комунікаційних технологій іноземних виробників та відсутність належної системи оцінки такої продукції вимогам безпеки; недосконалість нормативно-правової бази у сфері

кіберзахисту і повільне залучення положень європейського законодавства; низький рівень правової відповідальності за порушення закону в цій сфері; відсутність адекватної системи незалежного аудиту інформаційної безпеки та механізмів розкриття інформації; низький рівень підготовки фахівців в сфері кібербезпеки, а також неефективна діяльність щодо стимулювання роботи цих фахівців в державному секторі; відсутність системи цифрової грамотності громадян та культури безпекового поводження в кіберпросторі.

Необхідно зазначити, що в стратегії міститься багато актуальних думок щодо правильної реалізації та забезпечення розвитку кібербезпеки в Україні, проте дуже мала увага приділена саме способам, за допомогою яких ця діяльність буде виконана. Наявні лише абстрактні фрази щодо «фінансового, кадрового, технічного чи законодавчого забезпечення», проте відсутні реальні заходи, які допоможуть розвинути цю сферу.

В законі «Про основні засади забезпечення кібербезпеки України» визначені конкретні загрози, які можуть завдавати шкоди державі та її громадянам, названі об’єкти та суб’єкти, які мають забезпечувати розвиток системи кібербезпеки, а також зазначається важливість захисту об’єктів критичної інфраструктури держави [31].

Проблема, що стосується виділення конкретних об’єктів критичної інфраструктури залишається невирішеною, проте слід зазначити що 12 серпня 2022 року було видано постанову «Про затвердження Положення про організацію кіберзахисту в банківській системі України та внесення змін до Положення про визначення об'єктів критичної інфраструктури в банківській системі України» [29]. Створено реєстр об’єктів критичної інформаційної інфраструктури, а отже ми бачимо, що перші кроки задля вирішення цього питання дійсно відбуваються.

В законі акцентується увага на важливості функціонування національної системи кібербезпеки, а реалізація її діяльності забезпечується шляхом оперативного розвитку державної політики в цій сфері, відповідності стандартам ЄС та НАТО, створення термінологічної бази у сфері кібербезпеки та загальнообов’язкових вимог

інформаційної безпеки об'єктів критичної інфраструктури, залучення експертів під час навчання нових фахівців, проведення спеціальних навчань, створення та забезпечення системи технічного та криптографічного захисту інформації, впровадження універсальної системи індикаторів кіберзагроз, а також за допомогою взаємодії держави із приватним сектором.

Створено спеціальну урядову команду реагування на комп'ютерні надзвичайні події – CERT-UA [40]. Головними завданнями даної команди є: проведення аналізу даних про кіберінциденти, а також ведення їх державного реєстру; розміщення на своєму сайті спеціальних порад та рекомендацій щодо протидії сучасним видам кібератак та кіберзагроз; активна взаємодія з правоохоронними органами задля своєчасного інформування про можливі кібератаки; співробітництво із міжнародними та українськими командами з питань реагування на сучасні кіберзагрози; допомога та сприяння вирішення питань кіберзахисту та протидії кіберзагрозам для органів місцевого самоврядування, підприємств, установ, військових, а також громадян.

Відповідно до закону, окрема увага також приділяється саме державно-приватній взаємодії. Вона полягає у підвищенні цифрової грамотності громадян та створенні культури безпекового поводження у кіберпросторі, що включає в себе комплексні знання, навички та вміння, необхідні для забезпечення безпеки в кіберпросторі. Для цього державою буде забезпечена підтримка громадських проектів пов'язаних із підвищенням рівня обізнаності суспільства щодо кіберзагроз та кіберзахисту.

Відповідальність за вчинення злочинів в сфері кібербезпеки більше не несе якісь примарні та нереальні погрози, законом встановлюються реальні умови кримінальних правопорушень та наслідки за їх невиконання передбачені цивільним, адміністративним та кримінальним законодавством.

3.2 Ескалація кіберзагроз національним інтересам України в умовах війни

В 2022 році з повною впевненістю можна заявити, що разом із початком російської агресії проти України в 2014 році, почалась і російсько-українська кібервійна.

Не дивлячись на те, що кібератакам іноді не надається такої великої уваги як іншим військовим діям, це зовсім не означає, що вони є менш небезпечними чи важливими.

Початком війни на українському кіберфронті слід визнати масштабну DDoS-атаку спрямовану на Дарницьку ТЕЦ, яка відбулась в 2014 році. З того часу, різні підприємства та державні установи, зі змінною періодичністю почали зазнавати різних кібератак. Нажаль, на той час система кібербезпеки ще не була достатньо розвинена, для того щоб коректно систематизувати та протистояти кіберзагрозам.

Раніше згаданий у другому розділі вірус **Petya** теж слід відносити до однієї з атак Росії на Україну. Розслідування американських служб вказувало на те, що творцями даного вірусу були саме російські хакерські угрупування. Не можна виключати і можливість того, що велика розповсюдженість даного вірусу по всьому світу була лише одним з факторів прикриття його реальної цілі – України.

Друга масштабна хвиля кібератак на Україну почалася у січні 2022 року. Перша велика атака відбулася 14 січня, в результаті якої було виведено з ладу понад десяток державних сайтів, серед них: Міністерства закордонних справ, Кабінету міністрів та Ради безпеки і оборони та інші. Атаки полягали у тому, що хакери замінили дані веб-сайтів текстом, який нагадував суміш ломаної української, польської та російської мов, та виглядав як «бійтесь та чекайте гіршого» (*див. Додаток А*). Відновлення роботи сторінок зайняло лише кілька годин, а СБУ заявили що витоку даних не відбулось. Пізніше стало відомо про ще одну атаку, яка вразила Державну службу з надзвичайних ситуацій і Автотранспортне страхове бюро. 19 січня було виявлено сліди діяльності російської хакерської групи **Gamaredon**, яка активно займалася кібершпигунством в Україні ще з 2013 року, жертвами даної команди були не лише українські організації, а й цілі по всьому світу.

Українські державні установи зазначили в міжнародній спільності, що січневі атаки були далеко не першими випадками агресії Росії проти України в кіберпросторі, проте міжнародні представники не приділяли цьому великої уваги.

Вже 15 лютого 2022 року нова масштабна DDoS-атака вивела з ладу сайти Міністерства оборони, та двох найбільших банків України: ПриватБанку та Ощадбанку. Моніторинг показав, що атака посилювалась протягом усього дня, вплинувши також і на мобільні додатки та банкомати банків. Розслідування Уряду Великої Британії та Ради національної безпеки США, показало що атаку було здійснено Головним розвідувальним управлінням Росії, проте прес-секретар Кремля Дмитро Пєсков заперечив дане твердження.

23 лютого відбулась третя масштабна атака, що зламала кілька українських урядових, військових та банківських сайтів. Не дивлячись на те, що працездатність сайтів відновлювалась в дуже швидкому темпі, сайт СБУ був недоступним протягом досить тривалого періоду часу. Дослідницька група словацької компанії ESET (міжнародний розробник антивірусного програмного забезпечення) заявила, що зловмисну активність вірусу що вразив сайти 23 лютого, можна прослідити ще з грудня 2021 року, а отже можна зробити логічний висновок - дана атака була запланована заздалегідь.

Через три дні після вторгнення 24 лютого, кібератаки на державно-військовий сектор України збільшились майже вдвічі, в порівнянні з довоєнним періодом, а також було зафіксовано рекорд в 275 DDoS-атак на день, найпотужніші з яких перевищували 100000 Мб на секунду.

26 лютого Міністр цифрової трансформації України – Михайло Федоров, анонсував створення української ІТ-армії, до якої приєднались різні кіберфахівці, програмісти, копірайтери, дизайнери, маркетологи та багато інших спеціалістів. У перші дні ІТ-армія налічувала близько 175 тис. добровольців з усього світу: від білих хакерів та хактивістів до представників відомих технологічних компаній. До протидії російській агресії долучились і всесвітньо відомі хакери **Anonymous.**

Паралельно цьому українці на підпільних форумах закликали допомогти захистити український кіберпростір. Спеціальні інтернет канали діють і досі, а кількість учасників станом на жовтень 2022 року налічувала більше 300 тис. добровольців.

На думку зарубіжних експертів, створення Україною кіберармії таких масштабів є безпрецедентною. Раніше нікому не вдавалося завербувати до глобальної волонтерської організації стільки спеціалістів.

Слід відзначити скоординованість фізичних атак російських військових разом із кібератаками, так наприклад під час атаки на київську телевежу 1 березня, після обстрілу ракетами, що призвів до зупинки телевізійного мовлення, паралельно з цим відбувалась кібератака на концерн радіомовлення, радіозв'язку і телебачення.

Від початку війни, до атак на Україну приєдналися майже всі найвідоміші російські хакерські угрупування. Окрім хакерів російськомовного походження, за деякими, нажаль офіційно не підтвердженими даними, до атак на Україну залучились також і групи кіберзлочинців, серед яких виокремлюють угрупування Conti, CoomingProject та Killnet. Останнім приписують велику кількість атак на об'єкти критичної інфраструктури країн НАТО.

За даними урядового порталу CERT-UA, тільки за перший тиждень війни було здійснено 65 атак на об'єкти критичної інфраструктури України.

Кіберстратегія українських сил стала великою несподіванкою не тільки для російських нападників, а і для всього світу. Вперше з 2014 року, українська сторона починає проводити перші кібератаки у відповідь на російську агресію. У результаті атак, було зупинено роботу численних російських державних сайтів та банків, а також взято під повний контроль деякі телеканали, по яким спеціально транслювалися реальні відео з кадрами наслідків російського вторгнення. В деяких регіонах по російських телеканалах звучали українські пісні. Також в березні за допомогою волонтерів з усього світу, було знищено кілька ключових російських та білоруських сайтів, у тому числі і офіційний веб-сайт кремля.

В квітні було зареєстровано першу потужну російську атаку на українські електромережі, яку українцям вдалось відбити. А вже в серпні було здійснено атаку на сайт найбільшого постачальника електроенергії в Україні – компанію «Енергоатом». Для даної атаки було використано більше 7 млн бот-користувачів, які впродовж трьох годин постійно симулювали сотні мільйонів переглядів сторінки компанії.

Російська розвідка досить сильно недооцінила Україну не лише у військовій сфері, а й у сфері кібербезпеки. Після того, як наша країна зазнала сильних кібератак в 2014 та 2017 році, була зроблена досить велика робота над помилками та залучені значні інвестиції на розвиток цієї галузі.

3.3 Кібербезпекова політика в контексті політики національної безпеки : зарубіжний досвід

Останнє десятиліття показало, що розвиток національної системи кібербезпеки є необхідним для кожної сучасної країни, а захист конфіденційних даних громадян та інформації щодо діяльності підприємств та інфраструктури стають головними цілями урядів.

В 2022 році групою дослідників Гарвардського університету було опубліковано звіт під назвою «National Cyber Power Index 2022» [48]. Науковці визначили сім спеціальних критеріїв за якими оцінюються країни:

1. спостереження та моніторинг;
2. зміцнення та посилення національної системи кіберзахисту;
3. контроль та маніпулювання інформаційним середовищем;
4. збір даних зовнішньою розвідкою для національної безпеки;
5. комерційна вигода або посилення росту внутрішньої промисловості;
6. знищення або виведення з ладу інфраструктури та можливостей супротивника;

7. визначення міжнародних кібернорм та технічних стандартів.

Слід звернути увагу, що цей аналіз не є першою публікацією науковців, трохи раніше в 2020 році, вони вже робили подібне дослідження.

Станом на 2022 рік, рейтинг незмінно очолюють Сполучені Штати Америки, на другому місці - Китай, а третє місце займає Росія. Вчені зазначили, що в їх рейтингу все ж існує похибка, через складність із доступом до деякої інформації певних країн. Весь список рейтингу відображає сучасний топ-30 країн за рівнем кіберрозвитку.

Окремо увагу також слід приділити Україні, яка за період з 2020 року досягла фантастичних результатів, та посіла 12 місце рейтингу, у порівнянні з 29 місцем у 2020 році [47].

США. Очевидним є той факт, що через політичний статус та вплив Америки на сучасній політичній арені, кіберпростір цієї країни завжди знаходиться під загрозою, а дані державних структур є «ласим шматком» для розвідки будь-якої країни супротивника.

Перші активні кроки до розвитку системи кібербезпеки були зроблені в 2003 році, коли було розроблено «Національну стратегію захисту кіберпростору». В ній зазначалось, що «діяльність стратегії спрямована на захист складних і взаємопов'язаних інформаційних систем, які мають значення для сучасного інформаційного суспільства», а головним завданням визначено «запобігання кібернетичним нападам на критичну інфраструктуру».

В 2009 році було випущено «Огляд з кібербезпеки», ціллю якого було вироблення стратегічної основи кіберініціатив для Уряду США, також там зазначалась центральна роль Білого Дому в формуванні кібербезпекової політики. Цей документ окреслював і ключові завдання, які були спрямовані на посилення кібербезпеки в країні за допомогою підвищення готовності суспільства до протидії кіберзагрозам, а також посилення рівня кібербезпекової освіти в навчальних закладах. В тому ж 2009 при Білому Домі було створено відділ з кібербезпеки, в обов'язки якого

входить координація роботи урядових відомств, розслідування кіберзлочинів, і діяльність щодо розробки нових захисних технологій.

В 2011 році президентом США Б. Обамою була запропонована нова Стратегія кібербезпеки. В ній вперше ворожі атаки в кіберпросторі розглядаються як будь-які інші загрози, та передбачається право США на вживання заходів у відповідь на них, таким чином хакерські атаки фактично прирівнюються до оголошення війни.

У вересні 2018 року, нова Адміністрація на чолі з президентом Д. Трампом, презентувала своє бачення питання захисту кіберпростору в новій «Національній кіберстратегії США». Даний документ базувався на принципі «посилення федеральних мереж та критичної інфраструктури». Кіберстратегія змістовно складається з п'яти американських стовпів, де кожен з них корелюється із завданнями в сфері кіберзахисту:

- захищати батьківщину, захищаючи мережеві системи та їх дані;
- забезпечувати процвітання Америки, створюючи безпечну цифрову економіку та допомагаючи сильним внутрішнім інноваціям;
- зберігати мир та безпеку шляхом укріплення можливостей США співпрацюючи з союзними країнами та партнерами;
- стримувати, або за необхідності карати тих, хто використовує кіберзасоби в зловмисних цілях;
- розповсюджувати американський вплив за кордоном, для розширення спільного надійного та безпечного кіберпростору [49].

Безпека кіберпростору в США ґрунтується на принципах свободи в мережі Інтернет, а окрім забезпечення цієї свободи, одночасно необхідне і усвідомлення небезпеки, для того щоб запобігти випадкам коли ця свобода буде використовуватися для створення політичних загроз.

Китай. Країна, що посіла друге місце у рейтингу, проте випереджає США в деяких аспектах кібербезпеки.

Система кіберзахисту Китаю наразі складається з п’яти основних компонентів:

- «Закон про кібербезпеку» 2016 року;
- багаторівнева система захисту мережі;
- система захисту критичної інформаційної інфраструктури;
- захист важливих даних;
- захист персональної інформації.

Закон про кібербезпеку набув чинності 1 червня 2017 року, та був введений з метою встановлення єдиного нормативного режиму для кібербезпеки та захисту даних в Китаї. В забезпеченні реалізації закону бере участь багато державних установ, зокрема: Адміністрація кіберпростору Китаю та її місцеві офіси; Міністерство громадської безпеки; Міністерство промисловості та інформаційних технологій та місцеві телекомунікаційні бюро; Міністерство науки і технологій; Національне енергетичне управління та Комісія з регулювання банківської та страхової діяльності Китаю. Оператори китайських мобільних та Інтернет мереж зобов’язані дотримуватись правил багаторівневої систему захисту, а всі компанії, які працюють із конфіденційними даними громадян мають відповідати державним стандартам кіберзахисту та використовувати шифрування.

Після виходу в 2021 році «Закону про захист персональної інформації», в світі з’явився новий термін під назвою «велика китайська кіберстіна». Закон привернув увагу майже всього світу, і спровокував неабияку реакцію зі сторони світової спільноти через його екстериторіальний характер. Згідно із його положеннями, будь-яка іноземна компанія яка веде свою діяльність в Китаї та працює з конфіденційною інформацією, має підтвердити, що рівень кіберзахисту даних відповідає вимогам китайського уряду, а китайським компаніям забороняється збереження даних громадян Китаю на серверах в інших країнах. Також компанії повинні постійно надавати звіти, щодо дотримання вимог захисту персональної інформації, а за

порушення цих правил настає відповідальність від штрафів до конфіскації, або повної заборони та припинення діяльності компанії в країні.

Естонія. Не дивлячись на те, що ця маленька країна зайняла лише 25 місце в загальному рейтингу, вона все ж варта уваги.

Естонія була однією з перших країн, яка серйозно сприйняла важливість розвитку системи кіберзахисту задля збереження даних і безпеки об'єктів інфраструктури. Історія розвитку кібербезпеки в цій країні почалась в 2007 році, і була пов'язана з дуже цікавими обставинами. Ще в 1947 році радянською владою в столиці країни було поставлено статую бронзового солдата під назвою «Пам'ятник визволителям Талліна». Оскільки для багатьох естонців радянські солдати сприймалися лише як окупанти, а не визволителі, урядом Естоніїї було вирішено перенести статую на військове кладовище на околиці міста. Російські ЗМІ наповнилися неправдивими заявами про те, що уряд Естонії знищує статую та військові могили, що викликало протести серед російськомовного населення міста. 26 квітня заворушення охопили столицю, а через кілька днів на країну була здійснена масова кібератака, яка тривала тижнями та вивела з ладу естонські банки, державні органи та ЗМІ. Хто стояв за цими нападами невідомо, проте є фактом, що вони відбувались з російських ір-адрес.

Дані події навіть були названі «Першою веб-війною», і сильно вплинули на усвідомлення суспільством вразливості цифрової інфраструктури. В тому ж 2007 році, виникає Ліга кіберзахисту Естонії – волонтерський підрозділ кіберзахисту, який допомагав уряду протистояти кіберзагрозам. З допомогою провідних ІТ-експертів, Естонія побудувала свою надійну систему кібербезпеки.

Маючи впевненість у захисті даних своїх громадян, країна активно розвиває взаємодію уряду з громадськістю цифровим способом, від голосування та сплати податків до створення компаній та підтвердження особистості.

Така успішна діяльність реалізується шляхом системи резервного копіювання даних. Навіть якщо, якась частина системи з даними зазнає кібератаки, завжди є інша яка забезпечить безперервну роботу всієї системи [43].

ВИСНОВКИ

Аналіз кібербезпеки як елементу національної безпеки надали автору можливість дійти таких висновків:

Під національною безпекою пропонується розуміти систему нормативно-правових, теоретико-методичних, розвідувальних та організаційно-управлінських заходів, спрямованих на забезпечення безпеки та захисту суверенної держави, включаючи її громадян, національні інтереси, джерела духовного добробуту народу, інститути та економіку. Сучасна сфера безпекознавства зосереджує свою увагу на таких галузях: державна безпека, громадська безпека, екологічна безпека, інформаційна безпека, економічна безпека та кібербезпека.

В умовах стрімкого розвитку цифрового простору, інформаційні технології стали невід'ємною частиною людського життя. Разом із цим виникає таке нове поняття як кіберпростір, яке визначають як середовище, сформоване з фізичних та не фізичних елементів, яке характеризується використанням комп'ютерів та обміном даних за допомогою інформаційних мереж. Не дивлячись на всі переваги використання комп'ютерних мереж, вони обумовили виникнення нових загроз національній та міжнародній безпеці. Кіберпростір займає місце нової сучасної військової арени, поруч із повітрям, морем та суходолом. Саме тут виникає потреба у створенні спеціальних засобів захисту даних в цій сфері, що і є головною ціллю кібербезпеки. Кібербезпека – це сукупність методів та практик захисту від атак зловмисників, для збереження даних комп'ютерних мереж, серверів та електронних систем.

Небезпеки які виникають в кіберпросторі несуть вже не тільки якісь примарні загрози для країн, а їх основними цілями є активи та репутація організацій та держав. Кіберзагрози визнаються як реальна шкода, що може спричинити негативні наслідки, а також систематизуються та досліджуються різними науковцями. Загрози можуть бути таргетними або нонтаргетними та носити навмисний чи ненавмисний характер.

Серед джерел кіберзагроз виокремлюють: бот-мережі, злочинні угрупування, іноземні держави, хакерів, хактивістів, фішерів, спамерів, інсайдерів та кібертерористів.

Кібератаки, або будь-які навмисні дії, які впливають на доступ до даних чи систем, стають серйозними проблемами для сучасного суспільства.

Встановлено, що кібератаки можуть бути здійснені різними способами: за допомогою людей, шкідливих програм чи апаратного забезпечення. Серед основних типів кібератак є: DDoS-атаки або атаки на відмову в обслуговуванні; блюджекінг; ботнет; атаки за допомогою сніфферів; логічні бомби; бєкдори; а також найвідоміші – вірус, хробак та троян. Деякі такі зловмисні програми можуть наносити шкоди на мільярди доларів, змінювати політичну ситуацію в країні або навіть ставати загрозою для життя людей.

Активне збільшення використання мобільних телефонів та комп'ютерів в житті людей, діяльності підприємств та функціонуванні держави, посилює ріст потенційних загроз і зумовлюють появу принципово нового рівня в сфері кібербезпеки та виокремлення таких понять як кібертероризм та кібервійна. Політично вмотивовані хакерські операції, спрямовані на заподіяння серйозної шкоди економічній сфері чи життю громадян визначаються як кібертероризм. В роботі зазначається, що на думку деяких науковців термін «кібертероризм» є недоречним, оскільки широкомасштабні кібератаки можуть викликати лише роздратування, але ніяк не жах, як наприклад, хімічна чи ядерна бомба. Однак необхідно відмітити, що сучасні кібератаки на об'єкти критичної інфраструктури можуть спричинити дуже руйнівні наслідки для економіки держав та навіть призвести до загибелі її громадян. Поруч із поняттям «військова агресія» чи конфлікту, виникає такий новий феномен як «кібервійна», яка включає в себе: кіберпроникнення, кіберманіпуляції, кібернапади та кіберрейди. Під кібервійною розуміють будь-яку дію, спрямовану на те, щоб змусити свого опонента виконати національну волю країни, вчинену проти програмного забезпечення, що контролює процеси в комп'ютерній мережі опонента. Визначені чотири спеціальні

атрибути, за допомогою яких визначається чи була кібератака актом кібервійни, а саме: джерело, наслідки, мотивація та рівень підготовки.

Аналіз нормативно-правової системи України в сфері кібербезпеки, показав що не дивлячись на те, що даний процес активно було розпочато лише 7 років тому, наша держава безумовно зробила великі кроки в створенні стратегії та систематизації знань щодо кіберзахисту. Діяльність спеціально створених підрозділів та урядової команди реагування на комп'ютерні надзвичайні події – CERT-UA, реально покращили ситуацію в кіберпросторі нашої країни у порівнянні з 2015 чи 2017 роком.

Велику роль у розвитку системи кібербезпеки України зіграла агресія РФ, яка почалася з 2014 року. З того часу, наша країна систематично зазнавала кібератак на різні підприємства, урядові сайти та комп'ютерні мережі. Із покращенням системи захисту кіберпростору, час на відновлення роботи після кібератак зменшувався, а іноді і зовсім не потребувався, оскільки захист прекрасно з усім справлявся. Масштабне російське вторгнення в Україну 24 лютого, показало що російська розвідка досить сильно недооцінила нашу державу не лише у військовій сфері, а й у сфері кібербезпеки. Українцям вдалося створити кіберармію безпрецедентних масштабів, та успішно протидіяти російським кібератакам та навіть проводити власні у відповідь.

Розвиток національної системи кібербезпеки є необхідним для кожної сучасної країни, а захист конфіденційних даних громадян та інформації щодо діяльності підприємств та інфраструктури є головними пріоритетами урядів держав. Активною діяльністю по розробці нормативно-правових актів у сфері кібербезпеки займається Європейський Союз, НАТО та більшість сучасних міжнародних організацій.

Безумовно сучасними лідерами в сфері кіберзахисту є США та Китай. Задля успішної реалізації діяльності в цій сфері країни виділяють величезні кошти з бюджетів, проводять активне міжнародне співробітництво в сфері кібербезпеки та постійно актуалізують нормативно-правове забезпечення задля успішного реагування на кіберзагрози.

Питання кібербезпеки стає одним з головних у міжнародній спільноті. Країни та міжнародні організації більше не можуть ігнорувати кіберпростір і загрози, які він може принести. Розвиток національної системи кібербезпеки є необхідною частиною реалізації системи національної безпеки країн.

Україна активно покращує своє законодавство в сфері кіберзахисту, для швидкого реагування та усунення загроз, що можуть бути нанесені нашій комп'ютерній мережі та інфраструктурі. Останні два роки показали, що наша держава вже встигла досягти великих успіхів в цій сфері, а усвідомлення важливості захисту даних громадян, спонукає нас і до подальшого її розвитку.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Васильєв Б. Г. SQL-ін'єкція та її небезпека. *Кібербезпека в сучасному світі : матеріали II Всеукраїнської науково-практичної конференції (м. Одеса, 20 листопада 2020 р.) / за ред. О. В. Дикого ; уклад.: Н. І. Логінова, В. Д. Бойко, М. О. Флюнт. – Одеса : Видавничий дім «Гельветика», 2020.* С. 143-147. URL : http://dspace.onua.edu.ua/bitstream/handle/11300/

2. Глазов О. Національна безпека: сутність, ознаки, концепція та геополітичні чинники. *Наукові праці [Чорноморського державного університету імені Петра Могили]. Сер. «Політологія». 2011. Т. 155. Вип. 143. С. 42–46.* URL : http://nbuv.gov.ua/UJRN/Npchdupol_2011_155_143_10.

3. Глазов О.В. Національна безпека: сутність, ознаки, концепція та геополітичні чинники. *Політологія. Наукові праці. 2011. Вип. 143, Т. 155. С. 42–46.*

4. Дзяна Г, Дзяний Н. Реалізація національної політики у сфері кібербезпеки. *Ефективність державного управління. 2016. №3(48). Ч. 1. С. 123-130*

5. Діордіца І. В. Система забезпечення кібербезпеки: сутність та призначення URL : http://goal-int.org/sistema-zabezpechennya-kiberbezpeki-sutnist-ta-priznachennya/

6. Діордіца І. В. Сучасний кібертероризм: аспекти правового регулювання URL : http://goal-int.org/suchasnij-kiberterorizm-aspekti-pravovogo-regulyuvannya/

7. Діордіца І. В. Поняття та зміст кіберзагроз на сучасному етапі URL : http://goal-int.org/ponyattya-ta-zmist-kiberzagroz-na-suchasnomu-etapi/

8. Завгородня Ю. В. Баланс сил політичних суб'єктів в кіберконфліктах. *Європейський вибір України, розвиток науки та національна безпека в реаліях масштабної військової агресії та глобальних викликів XXI століття» (до 25-річчя Національного університету «Одеська юридична академія» та 175-річчя Одеської школи права) : у 2 т. : матеріали Міжнар.наук.-практ. конф. (м. Одеса, 17 червня 2022 р.) / за загальною редакцією С. В. Ківалова. – Одеса : Видавничий дім «Гельветика», 2022.* – Т. 1. – С. 201-203. URL : https://hdl.handle.net/11300/19152

9. Завгородня Ю. В. Кібербезпека як інноваційний захист у політичному просторі України. *Вісник НТУУ «КПІ» Політологія. Соціологія. Право. – Київ, 2021. - Випуск 4 (52). – С. 33-38.* URL: http://visnyk-psp.kpi.ua/article/view/248130/245405

10. Завгородня Ю. В. Кіберконфлікти як елемент політичних технологій в інформаційному просторі. *Актуальні проблеми філософії та соціології : Науково-практичний журнал / Голов. ред. С. Г. Секундант, відпов. ред. Д. В. Яковлев ; Міністерство освіти і науки України ; Національний університет "Одеська юридична академія". - Одеса, 2021. - Вип. 32. - С. 144-148. URL : https://hdl.handle.net/11300/17068*

11. Запорожець О. Ю. Кібервійна: концептуальний вимір. *Актуальні проблеми міжнародних відносин. Вип. 121. частина І / ред. В. В. Копійка. — К. : Ін-т МВ КНУ ім. Т. Г. Шевченка, 2014. — 232 с.*

12. *Кібербезпека в сучасному світі: актуальні виклики : матеріали ІІ Всеукр. наук.-практ. конф. (м. Одеса, 20 листоп. 2020 р.) / за ред. О. В. Дикого ; укад.: Н. І. Логінова, В. Д. Бойко, М. О. Флюнт. – Одеса : Гельветика, 2020. – 244 с.* URL : https://hdl.handle.net/11300/19641

13. Климчук О. О., Ткачук Н. А. Роль і місце спецслужб та правоохоронних органів провідних країн світу в національних системах кібербезпеки. *Інформаційна безпека людини, суспільства, держави. — 2015. — № 3. — С. 75-83.*

14. Коваль З. В. Динаміка світової управлінської реакції на кіберзагрози: уроки для України. *Демократичне врядування. — 2014. — Вип. 14.* URL : http://nbuv.gov.ua/UJRN/DeVr_2014_14_5.

15. Козьміних А. В. Кібербезпека та кібератаки в умовах гібридної війни. *Європейський вибір України, розвиток науки та національна безпека в реаліях масштабної військової агресії та глобальних викликів XXI століття» (до 25-річчя Національного університету «Одеська юридична академія» та 175-річчя Одеської школи права) : у 2 т. : матеріали Міжнар.наук.-практ. конф. (м. Одеса, 17 червня*

2022 р.) / за загальною редакцією С. В. Ківалова. – Одеса : Видавничий дім «Гельветика», 2022. – Т. 1. – С. 204-205. URL : https://hdl.handle.net/11300/19153

16. Концепція розвитку сектору безпеки і оборони України від 14.03.2016 р. URL : http://zakon3.rada.gov.ua/laws/show/92/2016.

17. Кормич Л. І. Національна безпека в глобалізаційних умовах : навчально-методичний посібник для студентів вищих навчальних закладів / Л. І. Кормич, Т. М. Краснопольська. – Одеса : Фенікс, 2020. – 76 с. URL: https://hdl.handle.net/11300/14889

18. Косогов О. М. Пріоритетні напрямки державної політики щодо забезпечення безпеки національного кіберпростору. *Збірник наукових праць Харківського університету Повітряних Сил. — 2014. — Вип. 3. — С. 127-130.*

19. Кухаренко С. В. Сучасні типи кіберзагроз. *Кібербезпека в сучасному світі : матеріали II Всеукраїнської науково-практичної конференції (м. Одеса, 20 листопада 2020 р.) / за ред. О. В. Дикого ; уклад.: Н. І. Логінова, В. Д. Бойко, М. О. Флюнт. – Одеса : Видавничий дім «Гельветика», 2020. - С. 115-120.* URL: http://dspace.onua.edu.ua/bitstream/handle/11300/19831/

20. Куцаєв В. В., Живило Є. О., Срібний С. П., Черниш Ю.О. Розширення термінології сучасного кіберпростору. URL: mino.esrae.ru/pdf/2014/3Sm/1387.doc.

21. Лахно В. А. Побудова адаптивної системи розпізнавання кіберзагроз на основі нечіткої кластерізації ознак. *Восточно-Европейский журнал передовых технологий. — 2016. — № 2(9). — С. 18-25.*

22. Лисецький Ю.М., Семенюк Ю.В., Павленко Д.Г. Аналіз чинників, що впливають на систему забезпечення національної безпеки України в умовах гібридної війни. *Вісник воєнної розвідки. 2020. № 60. С. 99–103.*

23. Ліпкан В. А. Інформаційна безпека України в умовах євроінтеграції : [навчальний посібник] / *В. А. Ліпкан, Ю. Є. Максименко, В. М. Желіховський. — К. : КНТ, 2006. — 280 с.*

24. Ліпкан В. А., Ліпкан О. С. Національна і міжнародна безпека у визначеннях та поняттях. *Вид. 2- доп. і перероб.— К.: Текст, 2008. — 400 с.*

25. Мінін Д. С. Підходи до визначення поняття «кібербезпека». URL : http://istfak.org.ua/tendentsii-rozvytku-suchasnoi-systemy-mizhnarodnykh-vidnosyn-ta-svitovoho-politychnoho-protsesu/185-heopolitychna-dumka-ta-heostratehichni-protsesy-v-khkhi-st/971-pidkhody-do-vyznachennya-ponyattya-kiberbezpeka.

26. Петров В. В Щодо формування національної системи кібербезпеки України. *Стратегічні пріоритети. — Київ: НІСД, 2013. — № 4(29). — С.127-130*

27. Пехник А. В., Завгородня Ю. В. Сучасні загрози кібертехнологій у політичному процесі. *Актуальні проблеми політики.* 2021. Вип. 68. С. 76-82. URL : https://hdl.handle.net/11300/16276

28. Положення про Національний координаційний центр кібербезпеки від 07.06.2016 р. URL: http://zakon2.rada.gov.ua/laws/show/242/2016 (дата звернення: 20.10.2022)

29. Про затвердження Положення про організацію кіберзахисту в банківській системі України : Проект постанови. URL: https://bank.gov.ua/ua/ news/all/kiberzahist-bankivskoyi-sistemi-ukrayini-maye-posilitisya-12738 (дата звернення: 20.10.2022)

30. Про національну безпеку : Закон України від 21 червня 2018 року № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 20.10.2022)

31. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовтня 2017 року № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 20.10.2022)

32. Ревацкий А. А. DOS / DDOS-атака. *Кібербезпека в сучасному світі : матеріали II Всеукраїнської науково-практичної конференції (м. Одеса, 20 листопада 2020 р.) / за ред. О. В. Дикого ; уклад.: Н. І. Логінова, В. Д. Бойко, М. О. Флюнт. – Одеса : Видавничий дім «Гельветика», 2020. - С. 186-190.* URL : https://hdl.handle.net/11300/19977

33. Словник термінів з кібербезпеки / *за заг. ред. О. Копана, Є. Скулиша. — К. : ВБ «Аванпост-Прим», 2012. — 214 с.*

34. Стратегія кібербезпеки України від 15.03.2016 р. URL : http://zakon3.rada.gov.ua/laws/show/96/2016. (дата звернення: 20.10.2022)

35. Стратегія кібербезпеки України : Безпечний кіберпростір – запорука успішного розвитку країни : Затверджено Указом президента України від 26 серпня 2021 року № 447/2021. URL: https://www.president.gov.ua/documents/4472021-40013 (дата звернення: 20.10.2022)

36. Стратегія кібербезпеки України : Затверджено Указом Президента України від 15 березня 2016 р. № 96/2016. URL: https://www.president.gov.ua/documents/962016-19836 (дата звернення: 20.10.2022)

37. Ткачук К.С. Роль кібербезпеки в системі національної безпеки. *Сучасні політичні процеси: глобальний та національний виміри: матер. міжнар. наук.-практ. інтернет-конф., 29 квітня 2022 р. – Одеса. – С. 79-81.* URL : https://doi.org/10.32837/11300/17452

38. Шеломенцев В. П. Сутність організаційного забезпечення системи кібернетичної безпеки України та напрями його удосконалення. *Боротьба з організованою злочинністю і корупцією (теорія і практика). — Київ: Міжвідом. наук.-дослід. центр з проблеми боротьби з організ. злочинністю, 2012. — № 2 (28). — С.299-309.*

39. 2009 Cyberspace Policy Review URL: https://www.cisa.gov/publication/2009-cyberspace-policy-review

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

41. Weiss J. Control System Cyber Vulnerabilities and Potential Mitigation of Risk for Utilities. Juniper Networks, Inc. 2009.

42. Digital 2022: Global Overview Report / Simon Kemp 2022. URL: https://datareportal.com/reports/digital-2022-global-overview-report

43. e-Estonia Programme For Cyber Security. URL: https://e-estonia.com/programme/cyber-security/

44. Kapor M., Barlow J.P. Across the Electronic Frontier / Washington 1990. URL: https://web.archive.org/web/20131004172703/http://w2.eff.org/Misc/Publications/John_Perry_Barlow/HTML/eff.html

45. Pearson H., Denvil J. Managing Workforce Cyber Risk in a Global Landscape / Washington 2017. URL: https://www.hoganlovells.com/~/media/hogan-lovells/pdf/2017/2017_10_5_pac_alert_managing_workforce_cyber_risk.pdf?la=en

46. Melykh O., Korbut A. Entertainment media in the context of hybrid war in the post-Soviet countries: the case of Ukraine. *Economic Annals-XXI. 2020. Vol. 182(3–4). P. 25-33.* URL: http://ea21journal.world/index.php/ea-v182-03/

47. Voo J., Hemani I., Jones S., DeSombre W., Cassidy D., Schwarzenbach A. National Cyber Power Index 2020 / *Belfer Center Report 2022.* URL: https://www.belfercenter.org/sites/default/files/2020-09/NCPI_2020.pdf

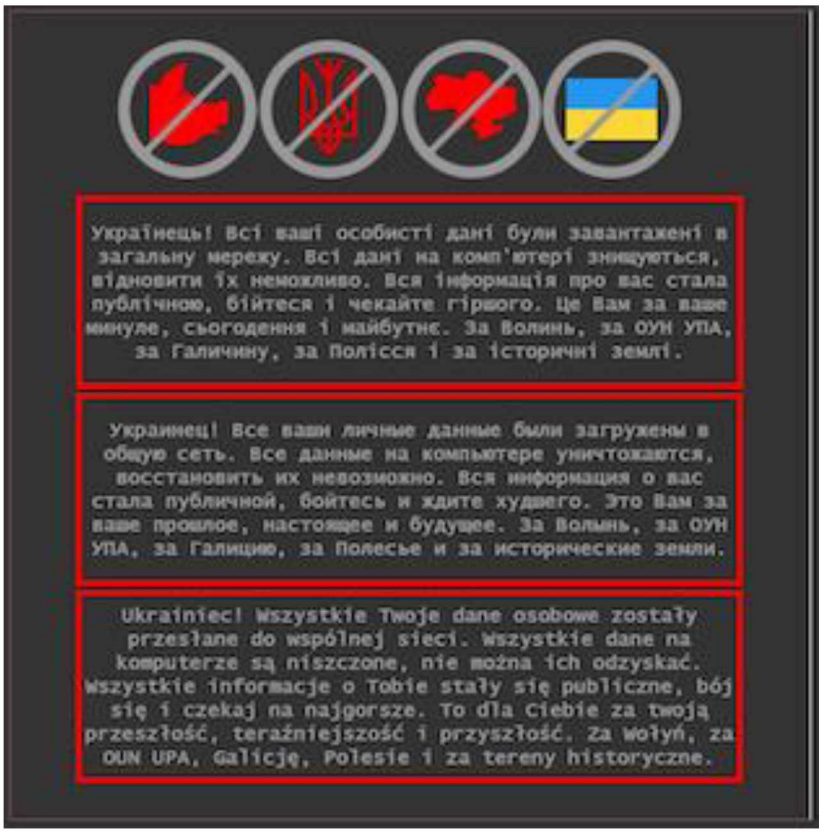
48. Voo J., Hemani I., Cassidy D. National Cyber Power Index 2022 / *Belfer Center Report 2022.* URL : https://www.belfercenter.org/sites/default/files/files/publication/CyberProject_National%20Cyber%20Power%20Index%202022_v3_220922.pdf

49. National Cyber Strategy of the United States of America 2018. URL : https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

50. NATO Cyber Defence URL : https://www.nato.int/cps/en/natohq/topics_78170.htm

ДОДАТКИ

Додаток А «DDoS-атака Січень 2022»



Джерело: Міністерство закордонних справ України

URL : https://web.archive.org/web/20220114032142/https://mfa.gov.ua/