МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Західноукраїнський національний університет
Навчально-науковий Інститут міжнародних відносин ім. Б. Д. Гаврилишина
Кафедра міжнародних економічних відносин

КАСТРАНЕЦЬ Вадим Володимирович

Реагування Європейського Союзу на глобальні ризики в сфері інформаційних технологій /The European Union's Response to Global Risks in the Field of Information Technology

спеціальність: 292 - Міжнародні економічні відносини
освітньо-професійна програма - Міжнародний маркетинг

Кваліфікаційна робота

Виконав студент групи
МЕВМАм-21
В. В. Кастранець

Науковий керівник:
д.філ.н., професор, Т. В. Чолач

Кваліфікаційну роботу допущено
до захисту:

" " 20 р.

Завідувач кафедри
_____ Р. Є. Зварич

ТЕРНОПІЛЬ - 2024

Вступ

Актуальність теми дослідження. В умовах, коли бізнес-середовище стає дедалі складнішим і менш передбачуваним, управління та оцінка бізнес-ризиків є критично важливими для стабільної роботи компанії. Ризик можна визначити як ймовірність того, що певні події або зміни, такі як економічні спади, природні катастрофи або зміни в законодавчій сфері, можуть негативно вплинути на діяльність підприємства. Іншими факторами ризику можуть бути зміни в ринковій конкуренції чи інші зовнішні обставини, що впливають на бізнес.

Технології аналізу, оцінки та управління ризиками є важливими інструментами для компаній, які допомагають знижувати ймовірність негативних наслідків при прийнятті управлінських рішень. Вони включають аналіз даних, моделювання та симуляцію ризиків, а також розробку відповідних стратегій для їх мінімізації. Використання аналітики даних дозволяє організаціям виявляти наявні тенденції та передбачати майбутні загрози, грунтуючись на аналізі попередніх періодів. Моделювання та симуляція ризиків допомагають оцінити ймовірність виникнення певних подій та їх можливі наслідки. Урахування ризиків є важливою складовою сучасного управління, що робить їх вивчення надзвичайно актуальним для організацій.

Аналіз останніх досліджень і публікацій. Теоретичне обґрунтування сутності ризиків та дослідження причин їх формування з метою ефективного управління підприємством були предметом уваги багатьох науковців, зокрема: В. В. Вітлінського, О. М. Крайніка, О. Луціва, В. М. Іщенка, Т. Л. Мостенської, Н. С. Скопенко, І. А. Нечаєвої та інших.

Незважаючи на обширні дослідження категорії «ризик» та факторів, що його спричиняють, особливу важливість набуває впровадження ефективної системи управління ризиками. Це стає невід'ємною частиною корпоративного управління, оскільки дозволяє своєчасно ідентифікувати потенційні загрози та мінімізувати ймовірність їх негативного впливу на діяльність організації.

Метою дослідження є узагальнення типів і методів дослідження глобадьних ризиків у сфері ІТ-технологій, систематизація процесів їх управління, а також обґрунтування заходів, спрямованих на їх попередження та уникнення Європейським Союзом.

Відповідно до мети сформульовані такі **завдання**:

- вивчити теоретичне та методологічне розуміння поняття глобальних ризиків в ІТ сфері;

- дослідити стратегії та політику Європейського Союзу щодо кібербезпеки;

- проаналізувати програми та ініціативи, які спрямовані на співпрацю з міжнародними партнерами у сфері інформаційних технологій;

- вивчити результати впровадження заходів ЄС у боротьбі з глобальними ризиками;

- з’ясувати успіхи та недоліки програм та стратегій ЄС у цьому напрямку;

- сформувати рекомендації для удосконалення політики та стратегій ЄС в галузі інформаційних технологій;

- оцінити напрямки розвитку міжнародного співробітництва у сфері кібербезпеки.

Об’єкт дослідження. Реагування Європейського Союзу на глобальні ризики в сфері інформаційних технологій.

Предметом дослідження є глобальні ризики в сфері інформаційних технологій.

Методи дослідження обрані з урахуванням потреби в комплексному підході до аналізу проблеми. Для цього застосовувалися аналітичні методи, історичний огляд, міждисциплінарний підхід та емпіричні дослідження, що дозволяють глибше зрозуміти та спрогнозувати глобальні ризики у сфері інформаційних технологій, а також оцінити стратегії реагування на них з боку Європейського Союзу.

Практичне значення отриманих результатів полягає в тому, що сформульовані узагальнення та висновки дослідження дозволяють точніше визначити основні загрози для інформаційних технологій на глобальному рівні. Систематизація використаних джерел, проведена в рамках роботи, може знайти застосування в науково-педагогічній діяльності, зокрема при розробці загальних та спеціалізованих курсів у вищих навчальних закладах, а також підготовці навчальних посібників та підручників з міжнародних економічних відносин.

Апробація роботи. Деякі тези дипломної роботи доповідалися на конференціях «Наукові орієнтири: теорія та практика досліджень» (Тернопіль, грудень 2023 р.) та «Інформаційна гігієна в соціальних мережах» (Тернопіль, квітень 2024 р.).

Структура дипломної роботи визначена метою та завданнями дослідження. Робота, загальний обсяг якої складає 56 сторінок, включає вступ, три основні розділи, висновки та список використаних джерел, що містить 50 найменувань.

Розділ 1. Теоретико-методологічні засади глобальних ризиків в сфері інформаційних технологій

1.1. Пояснення поняття глобальних ризиків

Ризик визначається «як процес перетворення потенційних загроз на реальні, а також виникнення небажаних наслідків, які можуть настати внаслідок різних дій» [12, с.34]. Він виникає через ймовірність появи несприятливих або непередбачених подій, що можуть призвести до негативних наслідків. Вони можуть мати різну природу та проявлятися в різних сферах життя, таких як бізнес, фінанси, безпека, природа тощо.

Ризики характеризуються двома основними аспектами:

- ймовірністю того, що певна подія відбудеться (у бізнесі ризик може полягати в можливості втрати прибутку через зміну ринкових умов або несподівані фінансові труднощі);
- масштабом наслідків цієї події, якщо вона все ж таки станеться.

Управління ризиками включає в себе ідентифікацію потенційних загроз, оцінку їх можливих наслідків і розробку стратегій для зниження або мінімізації цих ризиків.

Глобальні ризики - це потенційні загрози, які можуть вплинути на всю планету та її населення, маючи серйозні, далекосяжні наслідки для економіки, здоров'я, довкілля, безпеки або соціальних структур. Ці ризики зазвичай виходять за межі національних кордонів і вимагають міжнародного співробітництва для їхнього ефективного управління. Через це можна виділити економічні, технічні, природні, фінансові, правові ризики тощо. Глобальні ризики дозволяють бізнесу бути готовим до можливих наслідків і впроваджувати заходи для їх запобігання та зменшення негативного впливу.

Глобальні ризики часто переплітаються, і їхнє взаємне посилення може привести до ще більш серйозних наслідків. Оскільки ці загрози мають транснаціональний характер, ефективне їхнє управління вимагає співпраці на

міжнародному рівні, а також розробки механізмів раннього попередження та адаптації до змін.

Кожен з глобальних ризиків вимагає комплексного підходу до їх ідентифікації, аналізу та управління, щоб зменшити потенційні негативні наслідки. Варто зазначити, що фактори, що впливають на ризики, можуть варіюватися та залежати від конкретного виду діяльності і специфіки ринку. До них належать:

1. Економічна ситуація в країні та на міжнародних ринках, що передбачає підвищення економічної активності і сприяє розширенню бізнесу та зменшенню ризиків, тоді як в інших умовах можуть виникнути фінансові труднощі.

2. Конкуренція на ринку, рівень якої може суттєво впливати на ризики, з якими стикаються компанії.

3. Фінансова стійкість підприємства, де ризик може слугувати інструментом для регулювання ринкової ситуації та підтримки її стабільності.

4. Стратегічна невідповідність під час якої ризики можуть збільшуватися в разі обрання компанією неефективної стратегії.

5. «Політична ситуація, яка проявляється тоді, коли внутрішні політичні конфлікти, зміни в законодавстві та нестабільність урядових структур можуть призвести до змін в підприємницькому середовищі та вплинути на бізнес-ризики.

6. Залежність від постачальників або клієнтів, яка може підвищити вразливість компанії до ризиків» [50, с.35].

7. Зміни в технологічному середовищі, що проявляються через новітні технології, які можуть допомогти зменшити ризики, але також здатні змінити споживчі потреби та конкурентні умови. Тому важливо уважно слідкувати за технологічними трендами та враховувати їх у стратегії бізнесу.

Однак існують загальні чинники, які можуть впливати на ризики незалежно від його напрямку. «Оскільки повне уникнення ризиків є

неможливим, важливо активно вирішувати виникаючі проблеми та зменшувати їх наслідки. Процес ідентифікації ІТ-ризиків передбачає оцінку потенційних загроз безпеці, які можуть виникнути внаслідок впливу різних чинників. Існують різноманітні методології, що складаються з певної послідовності етапів: ідентифікація потенційних ІТ-ризиків, оцінка їх впливу, аналіз ймовірності виникнення, визначення пріоритетів, розробка плану управління ризиками та його реалізація. Завдяки виконанню цих етапів компанія отримує комплексну картину ІТ-ризиків, їх впливу на бізнес-процеси та можливості їх зменшення» [25, с. 67].

Зв'язок між ІТ-ризиками та бізнес-ризиками є актуальною темою для бізнес-середовища. Згідно з дослідженнями, збитки від кібератак у 2023 році «перевищили 1,5 трлн дол. США, що підкреслює важливість захисту інформації в бізнесі. ІТ-ризики можна визначити як потенційні загрози, пов'язані з використанням технологій та інформації в бізнес-процесах. Основною метою управління ІТ-ризиками є забезпечення стійкості бізнес-процесів підприємства до можливих випадків порушення їх нормального функціонування» [34, с. 28].

Для ефективного «управління ІТ-ризиками критично важливо мати необхідну експертизу та знання щодо технологій і стандартів безпеки. Наприклад, впровадження фреймворку NIST (Національний інститут стандартів і технологій) дозволяє організаціям розробити дієві політики та процедури безпеки, які зменшують ризики та забезпечують відновлення функціонування систем у разі інцидентів. У зв'язку з цими ризиками, забезпечення безпеки даних та розробка відповідних політик є надзвичайно важливими. Зокрема, згідно з звітом компанії Cisco, 61% підприємств у світі впровадили політику безпеки для технологій, що підвищує їх захищеність від ІТ-ризиків. Управління ІТ-ризиками є ключовим аспектом діяльності будь-якої організації, оскільки ефективне їх управління гарантує безпеку даних, знижує витрати на обслуговування ІТ-інфраструктури та підвищує продуктивність бізнес-процесів» [49, с.84].

Передові організації, що функціонують в умовах складного та змінного середовища, мають ряд спільних характеристик, які дозволяють їм досягати успіху навіть у непередбачуваних обставинах. Серед цих характеристик можна виокремити: гнучкість та адаптивність, інноваційність, конкурентні переваги, усвідомлення ризиків, ефективну командну роботу, орієнтацію на підтримку клієнтів та фокус на результат. Успіх компанії в умовах складності також визначається її здатністю управляти ризиками «та взаємодіяти із зацікавленими сторонами, такими як клієнти, постачальники та регуляторні органи. Аналіз ризиків є критично важливим етапом для будь-якої компанії, особливо для IT-компаній, які стикаються зі швидкими змінами в технологіях та вимогах споживачів» [10, с.16].

1.2. Аналіз основних загроз для інформаційних технологій на світовому рівні

Глобальні ризики в IT-сфері охоплюють різноманітні загрози, які можуть впливати на технологічні системи, бізнес-процеси та суспільство в цілому. Основні пояснення цього поняття можна поділити на кілька категорій.

Насамперед це технічні ризики, які пов’язані з відмовою обладнання, адже можливість виходу з ладу апаратних засобів, може призвести до простоїв. Також зустрічаються і помилки в програмному забезпеченні, що відбувається через недоліки в коді, які можуть викликати збої в системі. Сьогодні часто зустрічаються кібератаки – «це загрози, пов'язані з несанкціонованим доступом до інформаційних систем» [21, с.49]. Сюди можна також віднести втрату даних, яка зустрічається через різні причини, такі як збої в системі або людські помилки.

Людські ризики, що проявляються через несумісність команди проблемам в їх взаємодії, що може вплинути на продуктивність. Ці ризики можуть призвести до втрати ключових членів команди, фахівців, які мають важливі знання та навички. Зустрічається і недостатня кваліфікація персоналу, що проявляється у відсутності необхідних навичок у співробітників для виконання своїх обов’язків. Через людські ризики може зустрічатися і викрадення даних,

небезпека втрати інформації через дії недобросовісних осіб. Природні ризики включають повені під час яких вода, що затоплює території, може пошкодити обладнання та документи. Також зустрічаються і землетруси, стихійні лиха, які можуть завдати серйозної шкоди інфраструктурі, пожежі, під час яких вогонь, може знищити обладнання та дані, торнадо - потужні вітрові явища, які можуть завдати шкоди будівлям. Безпека даних також відноситься до ІТ ризиків. Вона може проявлятися у втраті конфіденційності даних небезпеці розкриття особистої інформації, неправомірному доступі до даних несанкціонованому використанні інформації. Сюди відноситься і витік інформації непередбачене поширення конфіденційних відомостей, віруси та шкідливе програмне забезпечення, програмні загрози, які можуть пошкодити системи та дані.

«Ризики, пов’язані зі змінами в законодавстві, які можуть викликати зміни в регуляторному середовищі, нормативні зміни, які можуть вплинути на бізнес-процеси» [11, с.16]. Потенційні штрафи або судові позови, які ведуть до фінансових витрат через невиконання законодавчих вимог. Несумісність з новими вимогами, що пов’язані з проблемами адаптації до нових юридичних стандартів. Сюди можна віднести і зміну політики конфіденційності, актуалізацію вимог щодо захисту даних.

Існують і ризики, пов’язані зі змінами в технологіях. Сюди можна віднести і застарілість технологій, невідповідність сучасним вимогам через використання застарілого обладнання чи програмного забезпечення, перехід до нових платформ, що супроводжувалися викликами, пов’язаними з переходом на нові технології. Зустрічається і нестабільність нових технологій, потенційні проблеми з новими рішеннями, що можуть бути ще не відпрацьованими. Конкуренція на ринку нових рішень також складає ризики, оскільки зростаюча конкуренція може знижувати позиції компанії на ринку.

Як вже зазначалося, всі ці ризики вимагають комплексного підходу до управління, що включає аналіз, оцінку та розробку стратегій для їх зменшення та адаптації до змінюваного середовища.

Розділ 2. Обговорення заходів Європейського Союзу з реагування на глобальні ризики

2.1. Стратегії та політика ЄС щодо кібербезпеки

«Європейський Союз, як регіональне інтеграційне об'єднання, є найуспішнішим та найамбіційнішим проєктом міждержавної співпраці. Його особливість полягає в прагматичному підході до питань, які мають важливе і спільне значення для його учасників. Саме в цьому контексті розробляються всі комунітарні стратегії та реалізуються політики в окремих секторах» [1, с.23]. Щодо концепцій інформаційної кібербезпеки, які відображають національні прагнення реалізації певних стратегій відповідно до моделей розвитку країн, ЄС не має чітко визначених стратегій. «Проте країни-члени ЄС однозначно підтримують демократичний розвиток кіберпростору та відносин у сфері інформаційних і комунікаційних технологій. Це, наприклад, виявляється в їхній підтримці американського проєкту резолюції Генеральної Асамблеї ООН «Заохочення відповідальної поведінки держав у кіберпросторі в контексті міжнародної безпеки» у 2018 році. Однак окремі країни мають свої власні уявлення про перспективи міждержавного узгодження питань кібернетичної та інформаційної безпеки» [47].

Рівень безпека цієї сфери в Європейському Союзі розглядається через призму кібербезпеки і стала актуальною лише нещодавно, в порівнянні з зазначеними раніше країнами, фактично після ухвалення документа про стратегію кібербезпеки ЄС у 2013 році. Відтоді політика ЄС у сфері кіберпростору активно розвивається. З 2013 року досягнуто значного прогресу в політиці кібербезпеки, яка зайняла центральне місце в пріоритетах Європейської комісії та стала важливою складовою «Стратегії єдиного цифрового ринку. Кібербезпека та боротьба з кіберзлочинністю стали одним із трьох основних напрямків Європейського порядку денного безпеки 2015 року, а в Глобальній стратегії ЄС 2016 року кібербезпека вже розглядається як горизонтальна політика Союзу, охоплюючи широкий спектр аспектів, від загальнодоступного

цифрового простору до діяльності ЄС. Глобальна стратегія представляє новий підхід до розуміння безпеки та загроз для громадян і самого Союзу, серед яких виділяються кіберзагрози поряд з гібридними загрозами, тероризмом, економічною нестабільністю, змінами клімату та енергетичними загрозами» [2]. «У питаннях безпеки вперше проголошено курс на стратегічну автономію, що означає необхідність пошуку шляхів протистояння цим загрозам силами самого Союзу. Можливо, до більш автономного підходу в розв'язанні проблем спонукали посилення загроз у кіберпросторі внаслідок розвитку інформаційно-комунікаційних технологій, а також непослідовність у зовнішній політиці головного партнера ЄС - США за президентства Дональда Трампа, а також вихід Великої Британії з ЄС. Ймовірно, ЄС буде шукати і використовувати відповідні можливості також на рівні зовнішньої політики» [40, с. 35].

«У сфері кібербезпеки Глобальна стратегія ЄС передбачає узгодження захисту комп'ютерних загроз із забезпеченням відкритого, вільного та безпечного кіберпростору. Це включає зміцнення технологічного потенціалу для зменшення загроз, підвищення стійкості критичної інфраструктури, мереж і послуг, а також протидію кіберзлочинності. Стратегія визначає кілька рівнів політики кібербезпеки: перший стосується відносин всередині ЄС, другий - взаємодії з третіми країнами та міжнародними організаціями, а третій - спільного бачення в цій сфері для узгодженої репрезентації на міжнародних майданчиках» [3, с.12].

У відносинах із міжнародними організаціями, такими як США та НАТО, головним пріоритетом є посилення співпраці. Основне повідомлення, закладене в стратегії, відображає західний (американський) підхід до забезпечення безпеки в кіберпросторі, що полягає в прагматичній меті стати «перспективним кібергравцем», «захищаючи свої ключові активи та цінності в цифровому середовищі. Це досягається шляхом просування вільного й безпечного глобального інтернету через прогресивний альянс між державами, міжнародними організаціями, промисловістю, громадянським суспільством і технічними експертами» [17].

Крім того, ЄС «шукатиме угоди про відповідальну поведінку держав у кіберпросторі на основі існуючого міжнародного права, підтримуючи багатостороннє цифрове управління та глобальні рамки співпраці в кібербезпеці, з повагою до вільного потоку інформації. Таким чином, можна стверджувати, що Європейський Союз виступає єдиним фронтом з іншими країнами Заходу в питаннях інформаційної кібербезпеки. Це проявляється, зокрема, в успішному розвитку концепції заохочення відповідальної поведінки держав у кіберпросторі, яка була представлена Сполученими Штатами у вигляді проєкту резолюції Генеральної Асамблеї ООН» [31, с.8].

«З початку розробки політики в сфері кібербезпеки Європейський Союз здебільшого орієнтувався на так звану м'яку безпеку. Це включало посилення зовнішнього виміру політики кібербезпеки, підвищення стійкості мереж і систем інформаційно-комунікаційних технологій до кіберзагроз, розробку можливостей та інструментів реагування на кібератаки, співпрацю в боротьбі з кіберзлочинністю, а також просування стандартів і цінностей у кіберпросторі. У 2016 році Директивою про безпеку мереж і інформаційних систем (NIS) було введено перші загальні правила безпеки інформаційних систем» [15]. «Директива NIS передбачає правові заходи для підвищення рівня кібербезпеки в ЄС, що включає підготовку країн-членів до реагування на інциденти з кібербезпеки за допомогою груп реагування на інциденти комп'ютерної безпеки (CSIRT) та відповідних національних органів NIS, підтримку стратегічного співробітництва й обміну інформацією щодо інцидентів і ризиків, а також сприяння розвитку кібербезпеки серед операторів критичної інфраструктури» [35, с.34].

«У цій сфері діють спеціалізовані структури, такі як Агентство ЄС з питань безпеки мережі та інформації (ENISA), Європейський центр кіберзлочинності (ЕС3) в рамках Європолу, Команда ЄС з питань комп'ютерного реагування на надзвичайні ситуації (CERT-EU) та Європейське оборонне агентство. Однак концепція стратегічної автономії, представлена в Глобальній стратегії ЄС, в найближчі роки вимагатиме певних заходів, які мають бути підтримані

відповідним фінансуванням. Практична реалізація цього нового підходу почалася з прийняттям у вересні 2017 року так званого пакета кібербезпеки, що передбачає низку заходів, які в подальшому координовано зміцнюватимуть структури й можливості ЄС у сфері кібербезпеки за активної співпраці держав-членів і різних зацікавлених структур ЄС» [45, с.45].

«Наприкінці 2020 року Європейська комісія разом із Високим Представником Союзу з закордонних справ і політики безпеки представили нову «Стратегію кібербезпеки для цифрового десятиліття». Ця стратегія має на меті зміцнити колективну стійкість ЄС до кіберзагроз і забезпечити надійність цифрових послуг та інструментів. Крім того, Комісія запропонувала дві нові ініціативи: оновлену Директиву NIS2, яка спрямована на досягнення високого загального рівня кібербезпеки в усьому Союзі, та нову Директиву щодо стійкості критичних організацій. Разом ці документи формують новий пакет кібербезпеки» [37, с.42].

Вторинне європейське законодавство було доповнене в цій сфері та стало логічним кроком, враховуючи виявлені недоліки попередніх нормативних актів і виклики, що виникли внаслідок пандемії Covid-19 та повномасштабної російсько-української війни. Стратегія окреслює кібербезпеку як багаторівневу проблему, для вирішення якої визначено кілька основних напрямків: «стійкість, технологічний суверенітет і лідерство; нарощування оперативного потенціалу для запобігання, стримування та реагування; а також просування глобального та відкритого кіберпростору.

Європейський Союз планує створити мережу Оперативних центрів безпеки по всій своїй території, які працюватимуть на основі штучного інтелекту, щоб сформувати європейський щит кібербезпеки» [9, с.37]. Крім того, передбачається розгортання надзвичайно безпечної інфраструктури квантового зв’язку для передачі конфіденційної інформації, а також упровадження ряду інших інструментів і заходів, зокрема зміцнення інструментів кібердипломатії, розробка плану «дій на випадок надзвичайних ситуацій для вирішення

екстремальних сценаріїв, що можуть вплинути на цілісність і доступність глобальної кореневої системи DNS, та встановлення стандартів безпеки. Варто зазначити, що ЄС реагує на зростання кіберзагроз, розгортаючи систему засобів і інструментів протидії, яка охоплює все більше сфер, пов'язаних із кіберпростором. Так, у резолюції, прийнятій 10 червня 2021 року, Європарламент закликає забезпечити захист пов'язаних продуктів і супутніх послуг, включаючи ланцюги поставок, з акцентом на їхню стійкість до кіберінцидентів» [48]. «Також наголошується на необхідності встановлення вимог кібербезпеки для програм, програмного забезпечення, вбудованого програмного забезпечення (яке контролює різні пристрої та машини, що не є комп'ютерами) та операційних систем (програмне забезпечення, яке виконує основні функції комп'ютера) до 2023 року. Реалізація таких вимог, ймовірно, матиме наслідки, схожі на обмеження присутності на ринку відповідних продуктів іноземного виробництва, як це вже було в США» [5].

У березні 2021 року Комісія опублікувала документ під назвою «Цифровий компас: європейський шлях до Цифрового десятиліття», в якому окреслила своє бачення цифрової трансформації Європи до 2030 року. У цьому комюніке було визначено концепцію цифрового суверенітету ЄС, що передбачає амбітні плани для впровадження цифрової політики, спрямованої на мінімізацію вразливостей і зменшення залежностей. Основною метою цієї політики є стимулювання інвестицій, щоб забезпечити лідерство Європейського Союзу в умовах відкритого та взаємопов'язаного глобального середовища.

Серед визначених цілей - прискорений розвиток цифрової економіки та суспільства, а також створення набору «цифрових принципів, що охоплюють доступ до інтернет-послуг, безпечне й надійне онлайн-середовище, цифрові медичні та державні послуги, орієнтовані на людину. Ці принципи доповнюватимуть існуючі права, які вже захищають і розширюють можливості європейців в інтернеті, зокрема захист особистих даних, конфіденційність, свободу вираження поглядів, можливості ведення бізнесу в онлайні та захист інтелектуальної власності» [39, с. 57].

Європейська стратегія може здатися схожою на китайську модель, що базується на активному державному втручанні у напрямки розвитку економіки та суспільства. Однак ключова відмінність полягає в тому, що європейська політика орієнтована не стільки на централізоване управління, скільки на ефективний перерозподіл стимулів без явних геополітичних амбіцій. Концепція «цифрового суверенітету» ЄС полягає в прагненні до технологічної самостійності, що досягається через значні інвестиції у європейські науково-дослідні проекти та ініціативи у сфері інформаційних і комунікаційних технологій, а також телекомунікацій.

Європейський Союз продовжує орієнтуватися «на західну (американську) концепцію розвитку кіберпростору і його безпеки. Відповідно до нової стратегії, ЄС активізує співпрацю з міжнародними партнерами для зміцнення глобального порядку, заснованого на правилах, сприяння міжнародній безпеці та стабільності в кіберпросторі, а також захисту прав людини та основних свобод в інтернеті. У цьому контексті ЄС прагне просувати міжнародні норми та стандарти, які відображають його основні цінності, співпрацюючи з партнерами в ООН та на інших відповідних форумах» [7].

Суттєвою рисою європейської стратегії є активне просування західної моделі розвитку кіберпростору, одночасно з розробкою власних підходів до ключових аспектів міжнародної співпраці. ЄС не лише сприяє інтеграції західних принципів, а й формулює власні позиції щодо важливих глобальних питань взаємодії в цифровому середовищі. Наприклад, позиція ЄС по відношенню кіберстримування наразі формується і, згідно зі стратегією кібербезпеки 2020 року, має сприяти відповідальній поведінці держав у кіберпросторі та співробітництву, надаючи конкретні рекомендації щодо протидії кібератакам, які мають значний вплив, зокрема на критичну інфраструктуру та демократичні інститути.

Також аналізуються перспективи введення додаткових обмежень через механізми кібердипломатії, а також застосування горизонтальних санкцій як відповіді на кібератаки.

Стратегії ЄС направлена на подальше зміцнення інструментів кібернетичної дипломатії, що охоплює різноманітні дипломатичні практики, пов'язані з управлінням кіберпростором. Це включає регулярне функціонування цих інструментів, інтеграцію їх у структури ЄС, які повязані з кризами, а «також забезпечення синергії у зусиллях протидії гібридним загрозам, дезінформації та зовнішньому втручанню в рамках Спільної рамки протидії гібридним загрозам» [28].

«Зовнішній вимір нової стратегії кібербезпеки ЄС базується на прагматичному підході, який передбачає продовження співпраці з міжнародними партнерами для просування політичної моделі, що ґрунтується на верховенстві права, правах людини, основних свободах і демократичних цінностях. Це сприятиме соціальному, економічному та політичному розвитку» [19? c/56].

2.2. Аналіз програм та ініціатив, які спрямовані на співпрацю з міжнародними партнерами у сфері інформаційних технологій

Оцінка ефективності співпраці з структурними фондами Європейського Союзу є критично важливим етапом, який дозволяє зрозуміти, як ефективно використовуються фінансові ресурси для розвитку європейських регіонів. Цей процес не лише оцінює результати інвестицій ЄС у регіональний розвиток та соціальну єдність, а й допомагає сформулювати рекомендації для майбутніх дій.

Початковий етап включає визначення цілей і завдань проектів або програм, які фінансуються структурними фондами ЄС. Важливо враховувати потреби громадян, їхні очікування та пріоритети, а не лише встановлювати цілі.

Далі формулюються критерії та показники, які допоможуть оцінити досягнення цих цілей. Це вимагає об'єктивності та ретельного відбору показників, що найкраще відображають реальний стан справ.

Наступним кроком є збір і аналіз даних, а також оцінка результатів співпраці зі структурними фондами ЄС, враховуючи як якісні, так і кількісні показники для визначення успіху досягнення поставлених цілей.

Завершальним етапом є формулювання висновків і рекомендацій на основі проведеного аналізу. Ці рекомендації є важливими для подальшого вдосконалення співпраці та підвищення її впливу на розвиток регіонів і поліпшення якості життя населення.

Створення єдиного цифрового ринку в Європейському Союзі є одним із ключових завдань, визначених у стратегії "Європа 2020", яка була ухвалена в 2010 році. Хоча концепція почала формуватися раніше, справжній поштовх для її реалізації отримано в 2015 році після підписання Угоди про асоціацію. Тоді ЄС активно розпочав роботи над цим ринком, розробивши стратегію, спрямовану на «поліпшення доступу до цифрових товарів і послуг, розвиток цифрових мереж та економіки, заснованої на новітніх технологіях» [26].

Огляд Стратегії Єдиного цифрового ринку, проведений у травні 2017 року Європейською Комісією, виявив багато важливих результатів. У цьому документі було проаналізовано прогрес у виконанні стратегії з 2015 року та визначено подальші кроки. ЄС приділяє значну увагу політичним сферам, важливим для ефективного управління цифровими технологіями, таким як кібербезпека, цифрова грамотність, розвиток цифрових послуг та інфраструктури, а також покращення державного управління через електронні сервіси, охорону здоров’я та соціальну допомогу.

У 2020 році понад половина світового населення, близько 4,66 мільярда людей, мала доступ до Інтернету. За даними Євростату, цього ж року більше 80% населення ЄС користувалися Інтернетом щодня. Урядові витрати на цифрові технології в ЄС зросли на 14% у 2022 році порівняно з попереднім роком.

Світовий ринок цифрових технологій у 2023 році оцінювався у понад 11,5 трильйона доларів США, а до 2025 року прогнозується, що обсяги даних у світі зростуть до 175 зетабайтів, що вдвічі перевищить показники 2020 року.

Ці напрямки були включені до Програми "Цифрова Європа" на 2021-2027 роки, для якої ЄС планує виділити 9,2 мільярди євро. Кошти будуть спрямовані на підтримку проектів і програм, що розвивають цифровий ринок, підвищують цифрову грамотність, забезпечують кібербезпеку та сприяють інноваціям у сфері цифрових технологій. Очікується, що ці заходи стимулюватимуть подальший розвиток цифрової економіки та відкриють нові можливості для європейських громадян і підприємств.

Аналіз програм та ініціатив, які спрямовані на співпрацю з міжнародними партнерами у сфері інформаційних технологій, може охоплювати широкий спектр аспектів. Ось кілька ключових напрямків, які можна розглянути:

1. Міжнародні програми та ініціативи в сфері ІТ.

Цей напрямок включає програми співпраці з такими міжнародними організаціями, як ООН, ЄС, Світовий банк, ІТ-асоціації, такі як IEEE чи ICANN. «Одним із пріоритетів визначено активізацію участі у міжнародних стандартизаційних процесах і лідерство в них. Це обумовлено технологічними та економічними вигодами для тих, хто очолює розробку і затвердження стандартів. Окрім того, міжнародна стандартизація дедалі частіше використовується третіми країнами для просування своїх політичних і ідеологічних програм, що часто суперечить цінностям ЄС. Наприклад, технологічні розробки Китаю в таких сферах, як штучний інтелект, квантові обчислення, використовуються для обмеження свободи слова та громадянських прав» [13].

Нова кіберстратегія акцентує увагу на продовженні співпраці з міжнародними партнерами з метою просування концепції відкритого, безпечного та стабільного глобального кіберпростору, що дотримується міжнародного права, включаючи Статут ООН, а також добровільних норм і

принципів відповідальної поведінки держав у кіберсфері. Цей підхід узгоджується з консенсусним звітом Робочої групи відкритого складу, опублікованим у 2021 році.

«З посиленням багатосторонніх дебатів щодо міжнародної безпеки в кіберпросторі, зокрема після появи конкуруючих проєктів резолюцій Генеральної асамблеї ООН у 2018 році від росії та США, виникла необхідність для Європейського Союзу та його держав-членів зайняти більш активну позицію на міжнародних форумах, таких як ООН. ЄС має сильні можливості для просування, координації та закріплення позицій держав-членів у цих дебатах, а також, як зазначено в Стратегії кібербезпеки 2020 року, повинен виробити спільну позицію щодо застосування міжнародного права в кіберпросторі» [34].

«У цьому контексті особливо слід відзначити проактивну позицію окремих держав-членів та самого ЄС. У жовтні 2020 року Франція разом із Єгиптом та 40 іншими країнами (серед яких Аргентина, Колумбія, Еквадор, Габон, Грузія, Японія, Марокко, Норвегія, Сальвадор, Сінгапур, Республіка Корея, Республіка Молдова, Республіка Північна Македонія, Сполучене Королівство, а також сам ЄС і його держави-члени) представила програму дій для просування відповідальної поведінки держав у кіберпросторі. В умовах багаторічної конкуренції між російсько-китайським і західним підходами до інформаційної безпеки це виглядало як спроба подолати роздвоєність дискусій із кіберпитань в ООН, зокрема в рамках групи урядових експертів та робочої групи відкритого складу» [22, с. 89].

Ця ініціатива була представлена не у формі проекту резолюції, а у вигляді записки, яка була опублікована в рамках Робочої групи з міжнародної безпеки (РГВС). Франція стала основним ініціатором цього кроку, отримавши підтримку від ЄС, його членів та ряду інших країн, які підтримують західний підхід до кібербезпеки. Замість того щоб продовжувати окремі дискусії між ГУЕ та РГВС, ці країни висловили пропозицію створити постійний форум, який об’єднає обговорення питань використання інформаційно-комунікаційних технологій у

контексті міжнародної безпеки. Як модель для такого форуму вони запропонували використовувати формат програм дій, подібний до тієї, що спрямована на запобігання незаконному обігу стрілецької зброї та легких озброєнь.

«Заснований цими сторонами «Постійний форум ООН для розгляду питання використання ІКТ державами в контексті міжнародної безпеки» передбачає, що програма дій (ПД) буде діяти «в єдиному, довгостроковому, інклюзивному та орієнтованому на прогрес форматі». Умови функціонування цього форуму можуть бути обговорені поточними групами урядових експертів (ГУЕ) та робочою групою відкритого складу (РГВС), а впровадження та подальші заходи можуть бути схвалені Генеральною асамблеєю ООН» [33, с.71].

Згідно з запропонованою ініціативою, ПД має визначити «структуру та політичні зобов'язання», які базуватимуться на вже існуючих міжнародних стандартах, включаючи рекомендації, норми та принципи, які були узгоджені, зокрема, у звіті ГУЕ ООН 2015 року. В рамках цього процесу передбачається проведення регулярних щорічних робочих зустрічей, що спрямовані на реалізацію зазначених рамок. ПД повинно сприяти зміцненню співпраці, ініціювати консультації з іншими зацікавленими сторонами, а також залучати регіональні організації та установи ООН, включаючи інші важливі учасники процесу.

«Запропоновано проводити регулярні конференції кожні п'ять років, на яких держави можуть ухвалити рішення про розробку додаткових норм. У Стратегії кібербезпеки ЄС 2020 року, яка з'явилася майже одночасно з ініціативою щодо ПД, проголошено про просування консенсусної пропозиції відповідно до цієї програми дій. ЄС підтверджує підтримку ініціатив, базуючись на доробках ГУЕ 2015, 2013 та 2010 років, схвалених Генеральною асамблеєю ООН. Також ЄС підтримує створення платформи для співпраці та обміну кращими практиками в рамках ООН і пропонує механізм для практичного впровадження норм відповідальної поведінки держав» [22].

Позиція Євросоюзу щодо кібербезпеки, зокрема ініціатива «Постійного форуму ООН», чітко демонструє відданість західному підходу, спрямованому на захист прав людини та основних свобод в інтернеті. Відсутність підтримки з боку росії та Китаю, які просувають концепції міжнародної інформаційної безпеки та кіберсуверенітету, підкреслює цю відповідність.

Цікаво, що США також не підтримали цю ініціативу, що може вказувати на можливі політичні маневри, оскільки французько-єгипетський проєкт по суті нагадує американську ініціативу, спрямовану на заохочення відповідальної поведінки держав у кіберпросторі. Однак, під час досягнення консенсусу в РГВС у березні 2021 року, ймовірно, підтримка з боку ЄС і ініціативи ПД суттєво вплинули на результат, що дало перевагу західній концепції безпеки.

Відповідно до західного підходу, ЄС акцентує увагу на стратегічних цілях протидії «цензурі, масовому стеженню, порушенню конфіденційності даних і репресіям, що підкреслює його роль як лідера у сфері захисту прав людини та основних свобод в інтернеті» [17, с.12]. Це свідчить про прагнення створити відкритий та безпечний кіберпростір, що відповідає демократичним цінностям.

2. Ініціативи у сфері цифрової трансформації

ЄС активно працює над цифровою трансформація в державному управлінні. Сюди входять і програми, спрямовані на модернізацію державних послуг через цифровізацію, е-урядування, використання великих даних і штучного інтелекту для покращення державних процесів.

Ініціативи через цифрове включення, спрямовані на забезпечення доступу до технологій та Інтернету для різних соціальних груп, особливо в країнах, що розвиваються. Це може включати програми, які допомагають розширити цифрову грамотність серед населення. Євросоюз активно працює над зміцненням міжнародного законодавства та стандартів цифрової трансформації, що включає дотримання «Статуту ООН і Загальної декларації прав людини. У рамках цього зусилля було прийнято План дій із прав людини та демократії на

2020–2024 роки, а також Настанови з прав людини щодо свободи вираження поглядів в інтернеті та офлайн, що залишаються актуальними» [23].

Щодо цифрової трансформації, позиція ЄС збігається з американською і протилежна російській. ЄС підтримує Будапештську конвенцію про модернізацію державних послуг через цифровізацію та сприяє третім країнам, які бажають приєднатися до неї. Важливою метою є доопрацювання Другого додаткового протоколу до конвенції, що має на меті покращення міжнародної співпраці.

Водночас, ЄС вважає, що перешкоджання поширенню цифрових технологій може загострити розбіжності та завадити національним реформам і міжнародному співробітництву. Таким чином, ЄС прагне дотримуватися вже існуючих рамок і сприяти їхньому розвитку, замість впровадження нових, що можуть ускладнити ситуацію.

Стратегія цифрової трансформації ЄС передбачає створення Порядку денного її розбудови, який акцентує увагу на систематичних зусиллях з покращення цифрових трансформацій в третіх країнах. Вона має на меті зміцнення стійкості критичних цифрових послуг, захист «інформаційної інфраструктури, підтримку реформ кримінального правосуддя в галузі кіберзлочинності, боротьбу з терористичним використанням інтернету» [47, с.12], а також розвиток навичок і компетенцій у сфері цифрових трансформацій.

У цьому контексті ЄС акцентує на цивільних аспектах Спільної політики безпеки та оборони, інтегруючи заходи з поширення цифрових технологій для підвищення стійкості третіх країн. На відміну від Китаю, який надає підтримку на основі політичних союзів, ЄС фокусується на країнах-сусідах та країнах, що розвиваються, визначаючи чіткі пріоритети для своєї підтримки в розбудові цифрового потенціалу. Це підкреслює прагнення ЄС до стабільності та безпеки в регіоні, створюючи умови для більш ефективної міжнародної співпраці в сфері цифрових технологій.

3. Кібербезпека та захист даних.

Для того аби розвивати зовнішній кіберпотенціал ЄС створює мережу EU CyberNet. Ця ініціатива має на меті зміцнення глобальної реалізації, координації та узгодженості проектів ЄС у сфері кібербезпеки. Мережа забезпечить технічну допомогу третім країнам, враховуючи потреби, які стали очевидними після масштабних атак зловмисного програмного забезпечення в 2017 році.

«Запущена у 2019 році, EU CyberNet планує досягти чотирьох основних результатів протягом чотирьох років:

1. Створення мережі експертів і зацікавлених сторін у сфері кібербезпеки.
2. Розробка технічної платформи для підтримки кібернетичного потенціалу.
3. Забезпечення навчання та допомоги для країн-партнерів.
4. Перетворення на центр знань ЄС у сфері кібербезпеки, сприяючи обміну досвідом та інформацією» [38].

Ця мережа не лише покращить кібербезпеку в регіоні, але й зміцнить позиції ЄС як лідера у глобальному кіберпросторі, підтримуючи демократичні цінності та права людини.

В першу чергу для самої ЄС у розбудові кіберпотенціалу є держави на Західних Балканах, сусідні держави та партнери з швидким цифровим розвитком. У рамках EU CyberNet також активно розвивається співпраця з африканськими країнами та Латинською Америкою, де ЄС підтримує законодавчі ініціативи й політики, узгоджені з європейськими стандартами.

Прикладом може бути той факт, що у 2021 році в Домініканській Республіці було проведено перші національні тренування з кібербезпеки, що отримали назву «Кіберполум’я». Крім того, в цей же період стартував процес створення регіонального центру кіберкомпетентності, який покликаний об'єднати країни Латинської Америки та Карибського басейну для розвитку спільних можливостей у сфері кібербезпеки.

У контексті інформаційної кібербезпеки важливе «значення має те, що країни ЄС, які є одночасно членами НАТО, приймають позицію щодо застосування міжнародного права в кіберпросторі, зафіксовану в «Талліннському посібнику» (The Tallinn Manual on the International Law Applicable to Cyber Warfare). Цей документ, розроблений за участю Центру передового досвіду кіберзахисту НАТО» [16], є спробою визначити застосовність чинних норм міжнародного права до нових викликів кібербезпеки, враховуючи брак загальновизнаних стандартів.

У «Таллінському посібнику» сформульовано чіткі позиції щодо суверенітету в кіберпросторі та його правового регулювання, що узгоджується із західною концепцією кібербезпеки. Цей документ є важливим індикатором європейського підходу до безпеки, оскільки він акцентує на необхідності дотримання міжнародного права.

4. Інвестиції в IT-інфраструктуру та стартапи

ЄС постійно підтримує стартапи та інвестиції в IT-сектор. Сюди входять програми, які залучають міжнародних інвесторів до підтримки українських технологічних стартапів або навпаки - українські інвестиції в IT-сектори інших країн.

Важливим є і міжнародне партнерство в сфері розробки нових технологій, що включає в себе інвестиційні програми та партнерства для спільної розробки та комерціалізації нових технологій (наприклад, в сфері блокчейну, штучного інтелекту, Інтернету речей).

Європейський Союз приділяє значну увагу співпраці з різними регіональними організаціями, зокрема Африканським Союзом, АСЕАН, Організацією американських держав та ОБСЄ. Основною метою є формування неформальної мережі ЄС в галузі інвестиційної дипломатії, яка буде сприяти популяризації європейської моделі IT-інфраструктури, покращенню обміну інформацією та координації зусиль серед партнерів у цьому напрямку.

Основним принципом міжнародної співпраці Європейського Союзу в галузі кібербезпеки є підтримка моделі управління інтернетом, в якій беруть участь численні зацікавлені сторони. ЄС наголошує, що жодна окрема організація, уряд чи міжнародна структура не повинні отримувати монопольний контроль над Інтернетом. Замість цього важливо забезпечити колективне управління та ефективну співпрацю між усіма учасниками цього процесу.

Співпраця між ЄС і НАТО має велике значення, особливо в контексті ІТ-інфраструктури. У липні 2016 року в Варшаві було підписано Спільну декларацію, яка покликана надати новий імпульс стратегічному партнерству між цими двома організаціями. Декларація підкреслює важливість спільних зусиль міжнародного партнерства в сфері розробки нових технологій.

«На основі цієї декларації ЄС і НАТО розробили спільний набір пропозицій для імплементації, який був схвалений Радами ЄС та НАТО в грудні 2016 року. У сфері розробки нових технологій оголошено про розширення координації, що включає місії, навчання та сумісність» [31].

Основні напрямки співпраці включають:

1. Підвищення здатності у розробці нових технологій. Це передбачає зміцнення стійкості, спільну роботу над аналізом загроз та своєчасний обмін інформацією.
2. Співпраця в сфері розробки нових технологій для стратегічних комунікацій. Включає реагування на інформаційні загрози та дезінформацію.

Таким чином, співпраця між ЄС і НАТО в сфері ІТ-інфраструктури є ключовим елементом для забезпечення стабільності та безпеки в Європі.

5. Освітні та дослідницькі ініціативи

Сюди відноситься робота ЄС з міжнародних навчальних програм та обмінів. Це програми обміну студентами та молодими фахівцями в галузі ІТ, що сприяють розвитку навичок і знань, важливих для сучасного ІТ-сектора.

Важливими тут є спільні дослідження та наукові ініціативи, що сприяють міжнародній співпраці в науково-дослідницьких проєктах, пов'язаних з інформаційними технологіями, такими як дослідження в галузі штучного інтелекту, машинного навчання, нанотехнологій.

Крім того, тісна співпраця ЄС зі Сполученими Штатами Америки також відіграє ключову роль у формуванні спільних освітніх та дослідницьких програм. ЄС і США поділяють думку про те, що міжнародне співробітництво є центральним елементом у цій сфері. Основною ознакою їхнього спільного підходу є підтримка принципу свободи та демократичних засад.

Таким чином, європейський підхід до освітніх та дослідницьких ініціатив, заснований на співпраці з НАТО та США, формує єдиний фронт, що грунтується на принципах міжнародного права та демократичних цінностях.

6. Інфраструктурні ініціативи в ІТ-сфері

Європейський Союз завжди виступав за створення спільних ІТ-хабів та технологічних парків. Це включало партнерство між країнами, що створює інноваційні простори для розвитку ІТ-бізнесу. Це можуть бути спільні інкубатори, акселератори, технопарки.

Важливою складовою у роботі ЄС в цьому питанні є розвиток цифрової інфраструктури, яка включає спільні ініціативи щодо створення високошвидкісного Інтернету, 5G зв'язку тощо.

ЄС та США також координують свої дії в практичних напрямках, включаючи співпрацю «між спеціалізованими інституціями. Обидві сторони поділяють спільні принципи управління інтернетом, такі як відкритість, свобода та сумісність, а також забезпечення прав і свобод людини» [41, с.69]. Вони визнають необхідність багатостороннього 5G зв'язку, який є децентралізованим і демократичним у прийнятті рішень.

7. Регулювання та стандартизація в ІТ-сфері

Сюди входить міжнародна співпраця ЄС у сфері ІТ-стандартів. Всі програми, які фінансуться Європейським Союзом спрямовані на гармонізацію національних ІТ-стандартів з міжнародними, що дозволяє забезпечити сумісність систем, сервісів та продуктів.

Важливим тут є правові ініціативи, які направлені на співпрацю в межах міжнародних угод і нормативних актів, що регулюють використання цифрових технологій, електронної комерції, захисту авторських прав у цифровому середовищі.

Першим спільним проєктом, який здійснювався в інтересах ЄС та США була боротьба із захистом авторських прав у цифровому середовищі. Обидві сторони підтримують Будапештську конвенцію, ухвалену Радою Європи у 2001 році, на рівні ООН, координуючи свої зусилля для просування цього стандарту на міжнародній арені. Конвенцію ратифікували багато країн, які навіть не були членами Ради Європи, це стосується Сполучених Штатів, які тільки носять статус окремого спостерігача в цій організації.

Щодо інституційної співпраці між ЄС та США реалізується через Робочу групу з питань захисту авторських прав у цифровому середовищі та електронної комерції, засновану у 2010 році. Сторони спільно організовують програми співпраці, навчання та заходи для захисту авторських прав у цифровому середовищі, залучаючи також приватний сектор.

Одним із прикладів такої співпраці стало започаткування «Глобального альянсу захисту авторських прав у цифровому середовищі та електронної комерції». Цей альянс має на меті посилити зусилля країн у боротьбі із захистом авторських прав в онлайн-просторі. У 2016 році альянс об’єднався з американсько-британським WePROTECT, що дозволило йому стати одним із найбільших у сфері координації зусиль у цьому напрямку, об’єднуючи 98 країн, численні компанії та міжнародні організації.

8. Співпраця в сфері екологічних ІТ-ініціатив

ЄС виступає за екологічно чисті технології в ІТ. На це направлені міжнародні програми, спрямовані на розробку та впровадження екологічно сталих ІТ-рішень, зокрема для енергоефективних дата-центрів, використання відновлювальних джерел енергії в ІТ-секторах.

Важливий результат стосувався щодо розвитку співпраці на рівні євроатлантичної у галузі екологічних ІТ-ініціатив. Це був Екодіалог між ЄС та США, який розпочався в грудні 2014 року. Цей діалог зосереджений на координації зовнішньої політики сторін у питаннях екологічних технологій та стратегічних аспектах глобальної екобезпеки. Серед основних цілей — встановлення норм поведінки в екопросторі, зміцнення довіри між державами та застосування існуючих норм міжнародного права до екопростору.

Ключовою характеристикою «американсько-європейського підходу до екологічних ІТ-ініціатив є активне залучення приватного сектору, наукових установ і громадянського суспільства до управління цим простором. У цьому контексті ЄС та США започаткували Трансатлантичну ініціативу з дослідження екополітики. Ця ініціатива об'єднує академічні, промислові та експертні центри з метою вирішення ключових проблем екополітики та підвищення потенціалу досліджень у цій сфері» [23].

Таке залучення різних стейкхолдерів сприяє формуванню «комплексного підходу до екобезпеки, що включає в себе як технічні, так і політичні аспекти» [5], а також забезпечує більш ефективну реакцію на виклики в екопросторі.

Всі ці напрямки міжнародного співробітництва ЄС у сфері інформаційних технологій допомагають розвитку національних економік, покращенню інфраструктури та зміцненню безпеки.

Розділ 3. Оцінка дієвості заходів ЄС у боротьбі з глобальними ризиками

3.1. Вивчення результатів впровадження заходів ЄС у сфері інформаційних технологій

У попепредньому розділі ми аналізували програми та ініціативи, які спрямовані на співпрацю ЄС з міжнародними партнерами у сфері інформаційних технологій. У цьому розділі ми спробуємо проаналізувати їх успіхи та недоліки. Вивчення результатів впровадження заходів ЄС у сфері інформаційних технологій є важливим аспектом для оцінки ефективності політик та ініціатив Європейського Союзу, спрямованих на розвиток цифрової економіки, технологій та інфраструктури в межах ЄС. Так, Європейський Союз протягом останніх років активно впроваджує свою Цифрову стратегію (Digital Compass), яка ставить конкретні цілі до 2030 року щодо цифрового розвитку. Вивчення результатів цієї стратегії можна подати через такі аспекти:

1. Покриття високошвидкісним Інтернетом є один із основних результатів цієї стратегії - це забезпечення доступу до високошвидкісного Інтернету для всіх громадян ЄС. Оцінка результатів включає розширення покриття фіксованим та мобільним Інтернетом у віддалених і сільських районах, а також розгортання 5G.

2. Розвиток цифрової грамотності, який проявляється в аналізі рівня цифрової грамотності серед населення ЄС та кількість людей, які використовують Інтернет для різноманітних послуг, включаючи освіту, працю та здоров'я. Сюди також можна включити програми по зменшенню цифрового розриву серед різних соціальних груп.

3. Вкладання інвестицій в цифрову інфраструктуру, що полягає у вивченні фінансування та інвестицій у цифрову інфраструктуру, зокрема в дата-центри, хмарні технології та інші інноваційні рішення.

Ще однією програмою ЄС є Horizon Europe для ІТ та інновацій, яка є головною програмою ЄС для фінансування наукових досліджень та інновацій. У сфері ІТ вона охоплює такі ключові області:

1. Інновації в сфері штучного інтелекту (ШІ). Програма сприяє розвитку нових технологій ШІ, аналізуючи, як інноваційні проєкти фінансувались і як вони покращують цифрові послуги та індустрії.

2. Розвиток технологій майбутнього, який повязаний з вивченням фінансованих досліджень у таких областях, як квантові обчислення, Інтернет речей (IoT), блокчейн, кібербезпека тощо.

3. Підтримка стартапів та малих і середніх підприємств (МСП). Суть її полягає у тому, як програма підтримує стартапи, що працюють у сфері IT, та чи забезпечує вона їх необхідними ресурсами для розвитку.

Важливим напрямком є вивчення результатів політики ЄС у сфері кібербезпеки, зокрема в рамках Європейської стратегії кібербезпеки та Нового регламенту про кібербезпеку (Cybersecurity Act). Про цю програму ми також вже вели мову вище. Її результатами є:

1. Покращення стійкості інфраструктури. Вивчення того, як були впроваджені програми для захисту критичної інфраструктури (енергетика, транспорт, фінанси) від кіберзагроз.

2. Європейський центр реагування на інциденти (EU CERT), який повязаний з оцінкою результатів діяльності цього центру щодо швидкості та ефективності реагування на кіберзагрози.

3. Розвиток співпраці між країнами ЄС це полягає в оцінці того, наскільки ефективно країни-члени ЄС співпрацюють у питаннях кібербезпеки та чи забезпечена узгодженість стандартів безпеки.

4. Підвищення рівня кіберосвіти та професіоналів, що полягає у вивченні ефективності освітніх програм для підготовки фахівців з кібербезпеки, а також популяризація кібербезпеки серед бізнесу та громадян.

Ще одним із завдань ЄС є забезпечення «доступу до цифрових технологій для всіх верств населення, включаючи віддалені регіони» [27], малозабезпечені сім'ї та людей з обмеженими можливостями. Ця програма включає:

1. Програми цифрової інклюзії, які проявляються в аналізі результатів таких ініціатив, як доступ до цифрових послуг для людей старшого віку, інвалідів або тих, хто проживає в сільських районах.

2. Забезпечення рівного доступу до технологій. Вивчення ефективності заходів щодо ліквідації цифрового розриву між країнами та різними соціальними групами. ЄС також активно сприяє розвитку електронного урядування (e-Government) через впровадження цифрових рішень в публічному секторі. Це включає:

1. Директиви ЄС щодо електронної ідентифікації (eIDAS). Вивчення того, як розвиваються електронні ідентифікаційні системи для громадян та бізнесу, їх вплив на забезпечення безпеки та зручності цифрових послуг.

2. Інтеграція цифрових послуг. Як ЄС допомагає державам-членам інтегрувати цифрові послуги в систему національного управління, що дозволяє громадянам та підприємствам отримувати електронні послуги більш ефективно.

Вивчення результатів застосування Загального регламенту захисту даних (GDPR) є важливим елементом політики ЄС. Ось кілька аспектів для аналізу:

1. Вплив на бізнес і компанії. Оцінка того, як GDPR змінив підходи до обробки персональних даних, забезпечення конфіденційності та безпеки.

2. Ефективність застосування GDPR. Аналіз того, як регламент сприяє підвищенню захисту даних громадян ЄС, скільки було накладено штрафів та як компанії адаптуються до нових вимог. Щодо аналізу фінансових результатів та інвестицій, то ЄС також спрямовує значні кошти на підтримку інновацій та цифрових технологій через програми, такі як Європейський фонд стратегічних інвестицій (EFSI), Програма цифрової Європи (Digital Europe Programme). Оцінка результатів може включати:

1. Кількість успішних проєктів і стартапів. Скільки проєктів було профінансовано в рамках програм і які їхні економічні результати.

2. Фінансування в інфраструктуру та дослідження. Як ці кошти сприяли розвитку новітніх технологічних досягнень, таких, наприклад, 5G, штучний інтелект, блокчейн та інші. ЄС здійснює оцінку результатів щодо сталого розвитку та екологічності. Це полягає у вивченні того, як цифрові технології та інновації ЄС сприяють досягненню цілей сталого розвитку, зокрема через «зелений перехід» (green transition). Це може включати:

1. Енергоефективність та цифрові технології. Як ІТ-ініціативи ЄС сприяють зменшенню викидів вуглецю, використанню відновлювальних джерел енергії в дата-центрах та ІТ-інфраструктурі.

Таким чином, вивчення результатів впровадження заходів ЄС у сфері інформаційних технологій дозволяє оцінити ефективність політик ЄС в розвитку цифрової економіки, кібербезпеки, інклюзивності та інновацій. Оцінка цих результатів допомагає визначити подальші кроки для покращення цифрової інфраструктури, сприяння інноваціям, розвитку бізнесу та посилення безпеки в Європейському Союзі.

3.2. Ідентифікація успіхів та недоліків програм та стратегій ЄС у цьому напрямку

Ідентифікація успіхів і недоліків програм та стратегій ЄС у сфері інформаційних технологій (ІТ) - це важливий етап для оцінки їх ефективності та визначення шляхів для подальшого розвитку. ЄС має широкий спектр стратегій і програм, спрямованих на розвиток цифрової економіки, кібербезпеки, інклюзивності та інновацій. Ось як можна структуровано розглянути успіхи та недоліки цих ініціатив:

1. Цифрова стратегія ЄС (Digital Compass).

Успіхи:

1. Покриття високошвидкісним Інтернетом. Одна з основних цілей стратегії - забезпечити високошвидкісний Інтернет для всіх громадян ЄС до 2030

року. Багато країн-членів досягли значного прогресу в розширенні доступу до широкосмугових послуг у віддалених і сільських районах.

2. Інвестиції в цифрову інфраструктуру. Програма також допомогла реалізувати інвестиції в новітню цифрову інфраструктуру, включаючи 5G та дата-центри.

3. Цифрова грамотність: Збільшення фінансування на програми підвищення цифрової грамотності серед різних соціальних груп, особливо «для літніх людей та людей з обмеженими можливостями» [4].

Недоліки:

1. Цифровий розрив. Хоча прогрес є, все ж існує значний цифровий розрив між різними регіонами ЄС. Сільські й віддалені райони все ще часто мають обмежений доступ до високошвидкісного Інтернету, що перешкоджає рівному доступу до цифрових послуг.

2. Затримки у впровадженні 5G. Низка держав-членів стикається з труднощами у розгортанні інфраструктури 5G через регуляторні проблеми та технічні труднощі.

3. Низька цифрова грамотність серед певних груп населення. Не всі соціальні групи мають однакові можливості для підвищення цифрової грамотності, що створює додаткові бар'єри для цифрової інклюзії.

2. Програма Horizon Europe.

Успіхи:

1. Підтримка інновацій. Horizon Europe став потужним інструментом для підтримки наукових досліджень і технологічних інновацій, зокрема в таких сферах, як штучний інтелект, блокчейн, квантові технології.

2. Стимулювання розвитку стартапів і МСП. Програма допомогла підтримати інноваційні стартапи і малий та середній бізнес у секторі інформаційних технологій.

3. Розвиток високих технологій. Були досягнуті значні результати в дослідженнях і розробках в галузі ШІ, а також в галузі екологічно чистих технологій.

Недоліки:

1. Складність доступу для малих компаній. Незважаючи на наявність механізмів підтримки стартапів, іноді малим та середнім підприємствам важко пройти через бюрократичні бар'єри та отримати фінансування.

2. Конкуренція за ресурси. Велика конкуренція за фінансування, що може обмежувати можливості для деяких інноваційних проектів, особливо для тих, які працюють в менш популярних технологічних галузях.

3. Європейська стратегія кібербезпеки.

Успіхи:

1. Створення ENISA та Європейського центру реагування на кіберзагрози. ЄС зміг значно посилити координацію в галузі кібербезпеки через створення Європейського агентства з кібербезпеки (ENISA) та підтримку мережі CERT.

2. Єдиний підхід до кіберзахисту. Європейський акт про кібербезпеку (Cybersecurity Act) закріпив основні принципи щодо сертифікації продуктів і послуг за стандартами безпеки на рівні ЄС, що сприяє підвищенню довіри до цифрових технологій.

3. Покращення захисту критичної інфраструктури. Зміцнення кіберстійкості «в таких важливих секторах, як енергетика, фінанси, охорона здоров'я, транспорт» [43].

Недоліки:

1. Недостатня готовність до гібридних атак. Враховуючи розвиток нових типів кіберзагроз (гібридні атаки, кібервійни), ЄС ще не повністю готовий до реагування на такі складні сценарії.

2. Неоднаковий рівень кібербезпеки між державами-членами. Країни ЄС мають різний рівень розвитку кіберзахисту, і цей розрив все ще є проблемою для ефективної координації на європейському рівні.

3. Проблеми з підтримкою малих підприємств: Малі підприємства часто не мають достатніх ресурсів для впровадження стандартів кібербезпеки, навіть коли ці стандарти вже розроблені на європейському рівні.

4. Цифрове урядування та е-уряди.

Успіхи:

1. Розвиток електронної ідентифікації (eID). ЄС зміг розробити загальні стандарти для електронної ідентифікації та електронного підпису, що спрощує доступ до державних послуг у країнах-членах.

2. Інтеграція цифрових послуг. ЄС активно працює над інтеграцією цифрових послуг через платформи, які дозволяють громадянам і бізнесу взаємодіяти з урядами онлайн (наприклад, через платформу EU Digital Services).

Недоліки:

1. Регуляторні бар'єри для транснаціональних послуг. Різні національні підходи до цифрових послуг та електронної ідентифікації все ще створюють бар'єри для надання єдиних послуг на рівні ЄС.

2. Цифровий розрив між державами-членами. В окремих країнах спостерігається значний розрив у доступі до цифрових державних послуг, що негативно впливає на ефективність політики цифрового урядування на рівні ЄС.

5. Програма «Цифрова Європа».

Успіхи:

1. Розвиток цифрових інфраструктур. Здійснено значні інвестиції у розвиток цифрових технологій, таких як хмарні обчислення, штучний інтелект, великий дані, квантові обчислення.

2. Підтримка інноваційних стартапів і МСП. Програма активно підтримує малий і середній бізнес у впровадженні новітніх технологій, допомагаючи їм адаптуватися до цифрової трансформації.

Недоліки:

1. Обмежена ефективність в деяких регіонах. Деякі менш розвинені регіони не отримують достатньої підтримки від цієї програми через конкуренцію за фінансування та обмеження в ресурсах.

2. Високий рівень конкуренції за кошти: Як і у випадку з Horizon Europe, стартапи та малі підприємства стикаються з високою конкуренцією за обмежене фінансування.

6. Вплив на екологічність і сталий розвиток.

Успіхи:

1. Інвестиції в зелені технології. ЄС активно сприяє впровадженню екологічно чистих технологій у сфері ІТ, таких як енергоефективні дата-центри та технології, що знижують викиди вуглецю.

Недоліки:

1. Необхідність більшої інтеграції екологічних стандартів у ІТ. Хоча програми ЄС підтримують сталий розвиток, необхідно більш активно інтегрувати екологічні стандарти в усі цифрові ініціативи для досягнення реальних результатів у зниженні впливу на навколишнє середовище.

Розділ 4. Рекомендації щодо подальшого посилення заходів у сфері кібербезпеки

4.1. Формулювання рекомендацій для удосконалення політики та стратегій ЄС в галузі інформаційних технологій

Формулювання рекомендацій для удосконалення політики та стратегій ЄС в галузі інформаційних технологій є важливою частиною оцінки поточної ситуації та пошуку шляхів для підвищення ефективності цифрової трансформації Європейського Союзу. У цьому контексті можна розглядати такі напрямки:

1. Зменшення цифрового розриву між регіонами та країнами-членами.

Рекомендації:

1. Збільшити інвестиції в розвиток цифрової інфраструктури в менш розвинутих регіонах ЄС. Це може включати більше фінансування для підключення сільських і віддалених територій до високошвидкісного Інтернету, а також 5G.

2. Спрощення доступу до програм фінансування для МСП, особливо в країнах, що відстають у цифровій трансформації. Важливо створити прозорі і прості механізми для отримання підтримки з боку ЄС.

2. Покращення цифрової грамотності серед населення, зокрема в сільських і віддалених районах. Це можна здійснити через програми навчання та підвищення кваліфікації для людей старшого віку, малозабезпечених верств населення і осіб з обмеженими можливостями.

2. Підтримка інновацій і стартапів у галузі ІТ.

Рекомендації:

1. Розширення доступу до фінансування для стартапів і технологічних компаній. Збільшити кількість програм, орієнтованих на підтримку інновацій у

сфері ІТ, особливо для стартапів, які працюють в передових технологіях (штучний інтелект, квантові обчислення, блокчейн тощо).

2. Впровадження механізмів менторства та співпраці між великими корпораціями та стартапами. Це дозволить стартапам отримати доступ до ресурсів, технологій та ринків великих компаній, а також спростить процеси інновацій та комерціалізації.

3. Забезпечення прозорості та спрощення регуляторних вимог для стартапів. Малі компанії часто стикаються з великими бюрократичними бар'єрами при виході на нові ринки або впровадженні нових технологій, тому важливо спростити цей процес на європейському рівні.

3. Посилення кібербезпеки та захисту даних.

Рекомендації:

1. Посилення співпраці між державами-членами у сфері кібербезпеки. ЄС повинен працювати над створенням єдиного, інтегрованого підходу до кіберзахисту, де обмін інформацією та координація між національними агентствами будуть ефективними і швидкими.

2. Розширення навчальних програм з кібербезпеки для громадян, малих бізнесів та державних організацій. Це дозволить підвищити рівень обізнаності і мінімізувати людський фактор як загрозу для кібербезпеки.

3. Покращення механізмів реагування на кіберінциденти. Важливо забезпечити швидку і ефективну реакцію на загрози з боку інфраструктури кібербезпеки ЄС, включаючи створення і розвиток європейських платформ для обміну інформацією про загрози.

4. Удосконалення цифрового урядування та електронних послуг.

Рекомендації:

1. Інтеграція єдиних стандартів для електронних послуг у всіх країнах-членах ЄС. Єдиний підхід до цифрових послуг дозволить спростити процеси для

громадян і бізнесу, забезпечуючи зручний і безпечний доступ до державних послуг у всьому Європейському Союзі.

2. Удосконалення механізмів електронної ідентифікації та цифрового підпису. Це дозволить громадянам і компаніям безпечно і зручно взаємодіяти з органами влади через Інтернет, без необхідності фізичної присутності.

3. Розширення електронних послуг для громадян та бізнесу. ЄС повинен сприяти розвитку цифрових платформ для надання послуг, таких як обслуговування бізнесу, медичні послуги, освіта, зниження податкових бар'єрів, надання соціальних послуг тощо.

5. Забезпечення екологічної сталості цифрових технологій.

Рекомендації:

1. Розвиток енергоефективних технологій для цифрових інфраструктур. ЄС має інвестувати в екологічно чисті технології для дата-центрів, серверних і комунікаційних інфраструктур, щоб зменшити енергоспоживання в IT-сфері.

2. Підтримка «зеленої» цифрової трансформації бізнесів. ЄС може створити стимули для компаній, що впроваджують екологічно чисті IT-рішення, наприклад, через податкові пільги або гранти на зелені інновації.

3. Розробка стандартів для екологічних IT-продуктів. Введення європейських стандартів щодо енергоефективності та стійкості продукції допоможе зменшити екологічний слід від технологій і сприятиме розвитку зелених ініціатив.

6. Створення спільного цифрового ринку.

Рекомендації:

1. Ліквідація бар'єрів для вільного обміну цифровими товарами та послугами між країнами ЄС. Важливо розробити політики, що сприятимуть інтеграції національних ринків цифрових послуг у єдиний цифровий ринок.

2. Створення єдиної платформи для електронної торгівлі та цифрових платіжних систем. Це дозволить забезпечити зручний доступ до цифрових товарів та послуг, створюючи рівні умови для всіх учасників ринку, зокрема для малих підприємств і стартапів.

3. Підтримка транснаціональних інвестицій у цифрові інфраструктури. Сприяння розвитку транснаціональних проектів у галузі IT, таких як спільні хмарні платформи або технології для кібербезпеки.

7. Залучення громадян до цифрової трансформації.

Рекомендації:

1. Поширення освіти і тренінгів для громадян на всіх рівнях. ЄС може створювати програми навчання, які покривають усі рівні цифрової грамотності - від базових навичок до просунутих курсів для професіоналів.

2. Створення платформ для цифрових ініціатив громадян. За допомогою цих платформ громадяни можуть пропонувати свої ідеї для цифрових інновацій або брати участь у програмах, що сприяють розвитку цифрових технологій у ЄС.

4.2. Оцінка потенційних напрямків розвитку міжнародного співробітництва у сфері кібербезпеки

Оцінка потенційних напрямків розвитку міжнародного співробітництва у сфері кібербезпеки є важливою для виявлення ефективних стратегій, які можуть допомогти країнам у боротьбі з кіберзагрозами. Враховуючи постійно зростаючий обсяг кіберзагроз, які виходять за національні межі, необхідність у міжнародній співпраці стає все більш очевидною. Ось основні напрямки, за якими можна здійснювати розвиток співпраці:

1. Глобальна координація у сфері кібербезпеки.

Потенційні напрямки:

1. Створення міжнародних коаліцій та платформ для обміну інформацією про кіберзагрози. Наприклад, платформи обміну даними між країнами про нові

кіберзагрози та уразливості можуть допомогти забезпечити швидке реагування на нові атаки. Співпраця на рівні міжнародних організацій (ООН, ЄС, НАТО, G7 тощо) дозволяє обмінюватися даними про кіберзагрози та розробляти спільні підходи до їх усунення.

2. Створення міжнародних стандартів і норм кібербезпеки. Наприклад, організація ООН вже почала розробляти принципи міжнародного права для кіберпростору, і такі ініціативи можуть стати основою для майбутнього співробітництва в цій сфері.

На сьогоднішній день, Європейський Союз та США мають спільні зусилля в обміні даними щодо кіберзагроз через Інформаційний обмін про загрози (ITIL) і програму реагування на інциденти у кіберпросторі (CERT).

Варто також відмітити, що і в цьому напрямку існують проблеми, а саме, різні країни мають різні підходи до кібербезпеки, і встановлення глобальних стандартів є складним через різницю в законодавстві, технічних вимогах і політичних інтересах.

2. Розвиток міжнародних інструментів і механізмів реагування на кіберінциденти.

Потенційні напрямки:

1. Міжнародні центри реагування на кіберінциденти (CERT, CSIRT) можуть бути інтегровані в глобальні системи для спільного реагування на атаки. Взаємодія таких центрів на міжнародному рівні дозволяє швидко усувати загрози, мінімізувати їх наслідки і підвищувати рівень захисту на глобальному рівні.

2. Підтримка міжнародних механізмів для допомоги в разі кібернападів на критичні інфраструктури. Це включає спільні заходи з реагування на інциденти, обмін досвідом та практичними знаннями, а також надання допомоги при ліквідації наслідків атак.

Прикладом тут може бути той факт, що у 2019 році ЄС розробив механізм взаємодопомоги для своїх країн-членів у разі великих кіберінцидентів через програму EU Cybersecurity Response Framework.

Проблеми в цьому напрямку є те, що різні рівні розвитку інфраструктури та ресурсів у країнах можуть обмежувати ефективність спільних механізмів, особливо для країн, що мають обмежені фінансові можливості.

3. Міжнародне співробітництво в боротьбі з кіберзлочинністю.

Потенційні напрямки:

1. Спільні зусилля у боротьбі з кіберзлочинністю, зокрема, через Інтерпол і Європол. Розвиток міжнародного співробітництва між правоохоронними органами та організаціями, які займаються боротьбою з кіберзлочинністю, дозволяє ефективно розслідувати і затримувати кіберзлочинців на міжнародному рівні.

2. Покращення співпраці в обміні доказами та розслідуваннях кіберзлочинів через національні та міжнародні юридичні інструменти, зокрема через Будапештську конвенцію або подібні угоди, що забезпечують правовий механізм для розслідування кіберзлочинів.

Прикладом може тут бути програма Global Forum on Cyber Expertise (GFCE), яка сприяє розвитку міжнародних ініціатив для підвищення глобальної здатності до боротьби з кіберзлочинністю.

І тут також існують проблеми, в результаті яких може відбутися порушення суверенітету і розбіжності в законодавчих підходах, які можуть ускладнювати екстрадицію кіберзлочинців і співпрацю між країнами.

4. Посилення ролі приватного сектору у міжнародній співпраці.

Потенційні напрямки:

1. Партнерство між державними і приватними організаціями для розробки спільних заходів з кібербезпеки. Приватний сектор, включаючи великі

технологічні компанії, може надавати цінну інформацію про кіберзагрози, допомагати у створенні програм для запобігання атак і розвитку інструментів кібербезпеки.

2. Підвищення участі компаній у міжнародних ініціативах з підвищення кіберстійкості. Міжнародні організації можуть сприяти розробці стандартів кібербезпеки, які б включали рекомендації та стандарти для технологічних компаній.

Наприклад, спільна ініціатива між США та приватними технологічними компаніями (наприклад, Google, Microsoft) по кібербезпеці для критичних інфраструктур дозволяє обмінюватися даними та реагувати на інциденти в реальному часі.

І тут є проблеми повязані із складнощами в досягненні консенсусу щодо стандартів безпеки між приватними компаніями, особливо коли мова йде про комерційну таємницю або захист інтелектуальної власності.

5. Розвиток технологічного партнерства та обміну досвідом.

Потенційні напрямки:

1. Спільні науково-дослідні ініціативи з розробки новітніх технологій у сфері кібербезпеки, таких як системи для виявлення аномалій, антивірусні рішення, технології криптографії, захист інфраструктур. Такі дослідження можуть проводитися на основі міжнародних кооперацій між університетами, лабораторіями та державними агентствами.

2. Обмін досвідом і кращими практиками між країнами через проведення міжнародних конференцій, симпозіумів та навчальних курсів, що дозволяє державам вдосконалювати свої стратегії і підвищувати рівень підготовленості до кіберзагроз.

Наприклад, Міжнародна ініціатива Global Forum on Cybersecurity Education сприяє обміну знаннями та кращими практиками між країнами, зокрема в навчанні кадрів для кібербезпеки.

Проблемами тут є те, що різні рівні розвитку технологій у країнах можуть призвести до нерівномірного доступу до новітніх рішень та інструментів.

6. Забезпечення сталого розвитку кібербезпеки в рамках міжнародних правових норм.

Потенційні напрямки:

1. Розробка міжнародних правових норм для кіберпростору, що стосуються захисту критичної інфраструктури, захисту прав людини та боротьби з кіберзлочинністю. Сюди можуть входити ініціативи на рівні ООН або міжурядових організацій, спрямовані на створення глобальних угод щодо кібербезпеки.

2. Підтримка правових механізмів, що дозволяють забезпечити міжнародне співробітництво в боротьбі з кіберзлочинністю, зокрема через спільні правові рамки і процедури екстрадиції кіберзлочинців.

Прикладом може бути Будапештська конвенція, яка є важливим міжнародним правовим документом, який встановлює правила співпраці між країнами для боротьби з кіберзлочинністю.

Проблемами тут є те, що існують різні підходи до прав людини та суверенітету. Країни можуть мати різні погляди на те, як кіберпростір має регулюватися в межах національних законів, що може призвести до конфліктів між державами з приводу таких питань, як захист приватності, право на свободу слова, чи можливість доступу до даних за кордоном.

Також ще одна проблема полягає у тому, що відсутні універсальні стандарти кібербезпеки. Хоча вже є багато ініціатив, таких як Будапештська конвенція або інші міжнародні угоди, однак кожна країна має власні критерії щодо кіберзлочинності та кібербезпеки, що ускладнює міжнародне співробітництво в правовому полі.

Як рекомендація, варто розвивати міжнародне законодавство з урахуванням нового типу глобальних загроз і адаптацію до швидко змінюваних технологій.

Також потрібно поширювати практики взаємного визнання судових рішень і допомоги в розслідуваннях кіберзлочинів на міжнародному рівні.

7. Розвиток партнерства між країнами і міжнародними організаціями для спільної оборони від кіберзагроз.

Потенційні напрямки:

1. Спільні ініціативи з оборони від кіберзагроз через організації, такі як НАТО та ЄС, які можуть проводити спільні навчання і обміну кращими практиками в сфері кібероборони. Наприклад, НАТО активно проводить операції з кібербезпеки та спеціалізовані навчання для своїх країн-членів, що можуть бути відкриті для партнерів, таких як Японія чи Австралія.

2. Захист критичної інфраструктури в рамках глобальної співпраці, де міжнародні організації, такі як Міжнародний союз електрозв'язку (ITU), можуть виступати в ролі посередників у створенні стандартів для захисту критичних систем. У такому контексті важливо не тільки обмінюватися даними, а й стандартизувати методи захисту, щоб забезпечити узгодженість між країнами.

Це можуть бути, спільні операції з кібероборони між країнами-членами НАТО та партнерами, наприклад, Швеція чи Фінляндія, можуть посилити колективну безпеку і забезпечити швидку реакцію на загрози.

Але і тут існують проблеми. Спільні навчання і операції вимагають значних ресурсів і координації між державами, що іноді ускладнюється через різницю в технічному рівні розвитку або політичних інтересах.

8. Розвиток кіберстратегії для держав, що розвиваються.

Потенційні напрямки:

1. Забезпечення розвитку кібербезпеки в країнах, що розвиваються. Міжнародні організації, такі як ООН або Всесвітній економічний форум (WEF), можуть надавати технічну допомогу та створювати стратегії для підвищення рівня кібербезпеки в країнах, що розвиваються. Це може включати навчання фахівців, розробку інфраструктури та допомогу в розробці законодавства для боротьби з кіберзлочинністю.

2. Обмін знаннями та технологіями. Розвинені країни можуть ділитися досвідом та технологіями з країнами, що тільки починають розвивати свої кіберстратегії, що дозволить побудувати більш міцні та захищені кіберструктури.

Нариклад, ініціативи ITU Global Cybersecurity Agenda (GCA), яка надає технічну допомогу країнам, що розвиваються, в рамках створення та реалізації національних стратегій кібербезпеки.

Проблемами тут є недостатня інфраструктура та обмежені фінансові ресурси, які можуть бути серйозними бар'єрами для ефективної реалізації цих програм. Крім того, у деяких країнах відсутні базові закони щодо кібербезпеки, що ускладнює їх інтеграцію в міжнародні ініціативи.

9. Етичні та правові аспекти кібербезпеки на міжнародному рівні.

Потенційні напрямки:

1. Етика в кібербезпеці. У рамках міжнародного співробітництва важливо звертати увагу на етичні стандарти, пов'язані з кібербезпекою. Це може включати питання приватності даних, збереження конфіденційності, використання шпигунських технологій, а також етичне поводження з даними користувачів та національними інтересами.

2. Міжнародні правові норми для кібернападів. Оскільки кібернапади можуть мати значні геополітичні наслідки, важливо розробляти міжнародні угоди, які б визначали, що є допустимим у кіберпросторі і які заходи можуть бути застосовані у разі порушення міжнародних норм.

Прикладом може бути те, що ООН та інші міжнародні організації, як, наприклад, Рада Європи, працюють над розробкою стандартів і правових рамок для відповідальних і етичних дій у кіберпросторі.

Проблемами є те, що враховуючи різницю в політичних системах і правових культурах, розробка універсальних етичних стандартів у кібербезпеці є складним завданням.

10. Прогнозування майбутніх викликів і тенденцій у кібербезпеці на міжнародному рівні.

Потенційні напрямки:

1. Прогнозування нових кіберзагроз. Оскільки технології швидко розвиваються, важливо прогнозувати майбутні кіберзагрози, які можуть виникнути унаслідок появи нових технологій, таких як квантові обчислення, штучний інтелект чи Інтернет речей (IoT). Міжнародні організації мають активно працювати над вивченням нових технологій і розробляти стратегії захисту.

2. Інвестування в дослідження та розвиток (R&D) нових кіберзахисних технологій. Підтримка міжнародного співробітництва в розробці нових технологій і систем кіберзахисту допоможе забезпечити майбутній захист від кіберзагроз. Це може включати штучний інтелект для виявлення аномалій, розробку нових стандартів безпеки та інші інновації.

Нариклад, ініціативи, як European Cybersecurity Research & Innovation (EU), сприяють інвестуванню в дослідження новітніх технологій для захисту від кіберзагроз.

І тут існують проблеми. Вони повязані з тим, що враховуючи швидкість розвитку технологій, важко прогнозувати і підготуватися до всіх можливих загроз, що потребує постійного оновлення підходів до кібербезпеки.

Висновки

Міжнародне співробітництво в сфері кібербезпеки стикається з низкою серйозних проблем, які потребують комплексного підходу для їх вирішення. Однією з головних проблем є відсутність єдиного міжнародного стандарту у сфері кібербезпеки, що ускладнює координацію дій між країнами. Різні підходи до регулювання кіберпростору, прав людини, захисту даних і законодавчих ініціатив, а також відмінності в технічних вимогах, значно обмежують ефективність міжнародного співробітництва. Різниця у рівнях розвитку кіберінфраструктури також створює бар'єри для рівноправного участі країн у глобальних ініціативах.

Крім того, недостатній рівень технічної підготовленості в деяких країнах, особливо в тих, що розвиваються, ставить під загрозу глобальну кіберстійкість. Обмежені фінансові ресурси та брак спеціалістів у деяких країнах можуть значно ускладнити впровадження ефективних заходів безпеки. Також важливим викликом є забезпечення етики і прав людини в рамках міжнародного кіберспівробітництва, де різні країни мають різні підходи до захисту приватності, свободи слова і суверенітету.

З огляду на ці проблеми, для подальшого посилення міжнародного співробітництва та розвитку кібербезпеки необхідно ухвалити ряд ключових заходів:

Створення єдиних міжнародних стандартів і норм кібербезпеки. Це дозволить забезпечити узгодженість між країнами, полегшить обмін інформацією та координацію дій у разі кіберзагроз. Такі стандарти повинні охоплювати як технічні вимоги до захисту даних і інфраструктур, так і правові норми, що регулюють міжнародне співробітництво.

Розвиток правових рамок для боротьби з кіберзлочинністю. Міжнародні угоди, на кшталт Будапештської конвенції, мають бути вдосконалені і адаптовані до нових кіберзагроз. Це дозволить забезпечити ефективну боротьбу з кіберзлочинністю та виявлення правопорушників на міжнародному рівні.

Підтримка і посилення ініціатив з розвитку кіберінфраструктури в країнах, що розвиваються. Міжнародні організації повинні надавати технічну допомогу та інвестиції для створення національних кіберстратегій, підготовки кадрів і розвитку інфраструктури в країнах з обмеженими ресурсами. Це дозволить забезпечити більш рівномірний рівень захисту кіберпростору на глобальному рівні.

Усвідомлення етичних і правових аспектів кібербезпеки. Важливо продовжувати роботу над розробкою етичних стандартів і принципів, які б враховували права людини та суверенітет країн у сфері кібербезпеки. Це включає питання захисту даних, забезпечення приватності користувачів та обмеження використання шпигунських технологій.

Активізація співпраці між державами, приватними компаніями та міжнародними організаціями. Приватний сектор, зокрема великі технологічні компанії, мають значний потенціал для забезпечення кібербезпеки, тому важливо сприяти тісній співпраці між державними органами та приватними компаніями для обміну інформацією про загрози і розробки нових захисних технологій.

Інвестування в дослідження та інновації в сфері кібербезпеки. Міжнародне співробітництво у галузі наукових досліджень допоможе розробити новітні технології для захисту кіберпростору. Прогнози щодо майбутніх кіберзагроз і нових технологій, таких як штучний інтелект або квантові обчислення, повинні стати основою для розвитку нових засобів захисту.

Регулярні навчання і симуляції кіберінцидентів на міжнародному рівні. Проведення спільних навчань та симуляцій допоможе країнам удосконалити свої стратегії реагування на кіберзагрози, а також покращити взаємодію між різними державами та міжнародними організаціями у разі кризових ситуацій.

Покращення координації реагування на кіберзагрози через міжнародні платформи обміну даними. Створення глобальних платформ для обміну інформацією про кіберзагрози дозволить забезпечити оперативну реакцію на

загрози і мінімізувати їх наслідки. Важливо створювати відкриті канали для обміну інформацією між державами, а також між державами і приватними компаніями.

У підсумку, для зміцнення глобальної кіберстійкості необхідно розвивати більш тісну співпрацю між країнами, міжнародними організаціями та приватним сектором. Розробка універсальних стандартів безпеки, ефективне правове співробітництво, інвестиції в розвиток технологій і підтримка країн, що розвиваються, є ключовими кроками для підвищення глобальної кібербезпеки в умовах нових викликів і загроз.

Список використаних джерел

1. Бойко О. Чим сьогодні занепокоєні аудитори різних країн світу: міжнародний досвід, на який варто звернути увагу. Вісник МСФЗ. 2021. № 8. https://msfz.ligazakon.ua/ua/magazine_article/FZ001292.

2. Данченко О. Б., Занора В. О. Проектний менеджмент: управління ризиками та змінами в процесах прийняття управлінських рішень: монографія. Черкаси, 2019. 278 с.

3. Демошенко Г. Цифрова трансформація муніципального управління: напрямки розвитку. Аспекти публічного управління. 2023. Т.8. №1. С. 36-38.

4. Дорош Н. І. Оцінювання ризиків при проведенні аудиту. Науковий вісник Національної академії статистики, обліку та аудиту. 2022. № 4. С. 40-47.

5. ДСТУ ISO 31000:2023 Менеджмент ризиків. Принципи та настанови (Risk management – Guidelines). URL: https://www.iso.org/ru/standard/65694.html.

6. Європейський Союз у XXI столітті: функціонування та розвиток: монографія / за заг.ред. В. С. Загорського, О. Я. Красівського. Львів: ЛРІДУ НАДУ, 2023. 632 с.

7. Європейський Союз: навч. посіб. / кер. авт. кол. Н. П. Карпчук, Н. І. Романюк та ін. Київ: ФОП Маслаков, 2020. 600 с.

8. Зварич Р.Є., Зварич І. Я. Імплементація плану дій ЄС у сфері циркулярної економіки. Науковий вісник Ужгородського національного університету: серія: Міжнародні економічні відносини та світове господарство. 2019. Вип. 25. Ч. 1. С. 93-98.

9. Ілляшенко С. М. Економічний ризик: Навчальний посібник. 2-ге вид., доп. перероб. К.: Центр навчальної літератури, 2024. 220 с.

10. Квітка С., Новіченко Н., Гусаревич Н., Піскоха Н., Бардах О., Демошенко Г. Перспективні напрямки цифрової трансформації публічного управління. Аспекти публічного управління. 2024. Т. 8. № 4, С. 129-146.

11. Кілієвич О. І. Економічне врядування. Публічне управління: термінолог. словник / за заг. ред. В. С. Куйбіди, М. М. Білинської, О. М. Петроє. Київ: НАДУ, 2021. С. 43.

12. Конкурентні стратегії безпеки розвитку України у глобальному середовищі: монографія / ДУ «Інститут регіональних досліджень імені М. І. Долішнього НАН України»; за заг. ред. А. І. Мокія. Львів, 2019. 872 с.

13. Косоруков А. А. Технології штучного інтелекту в сучасному державному управлінні. Соціодинаміка. 2023. № 5. С. 43-58

14. Кризові явища в єврозоні та їх вплив на політичні трансформації в ЄС: аналітична записка URL: https://niss.gov.ua/doslidzhennya/mizhnarodni-vidnosini/krizovi-yavischa-v-evrozonita-ikh-vpliv-na-politichni.

15. Маурер А. Д. Цифрові технології у виборах: питання, висновки та перспективи. Видавництво Ради Європи. 2023. URL: https://rm.coe.int/ardita-driza-maurer-digital-technologiesregulations-fin/16809e7f8f.

16. Міжнародні стандарти професійної практики внутрішнього аудиту (стандарти) (International Standards for the Professional Practice of Internal Auditing (Standards)). URL: http://iia-ua.org/wpcontent/uploads/2023/08/IPPF-Standards-2017-Ukrainian.pdf.

17. Нечаєва І. А., Дьордій Є. А. Управління ризиками підприємства в секторі іт-послуг як інструмент підвищення його конкурентоспроможності. Ефективна економіка. 2018. № 12. С. 45 -62

18. Олексюк Лілія. Кращі практики управління кібербезпекою. Оглядовий звіт. К: Комітет з питань цифрової трансформації. https://doi.org/10.1111/abac.12178.

19. Паламарчук С. А., Шемендюк О. В., Ляшенко Г. Т., Ткач В. О. Забезпечення захисту кіберпростору в провідних країнах світу. Збірник наукових праць ВІТІ. 2024. № 1. С. 58–64.

20. Перспективи розвитку політики ЄС: глобальні та регіональні виміри: монографія / колектив авторів; за заг. редакцією О. І. Брусиловської, І. М. Коваля. Одеса: ОНУ ім. І. І. Мечникова, 2019. 200 с.

21. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

22. Рудік Н. М. Економічне врядування в ЄС: розбудова в контексті сучасних викликів. Державне управління та місцеве самоврядування: зб. наук. пр. Дніпро: ДРІДУ НАДУ, 2020. Вип. 4 (47). С. 49–57.

23. Семенова С. М. Емерджентність у застосуванні системного підходу до управління підприємством. The International scientific and practical conference. A new view on the economy – the trend of innovative development. 2024. Kiev. Budapest. Vienna. Scientific.-inf. publ. center based on The Association of students and pedagogues «The Economist» Budapest: 2024. P. 35-38.

24. Семенова С. М. Ключові тенденції в управлінні ризиками провідних компаній ЄС за оцінками внутрішніх аудиторів. Ефективна економіка. 2020. № 9.

25. Семенченко А., Дрешпак В. Електронне урядування та електронна демократія. Київ. 2023. 60 с.

26. Тимків Я. Теорія і практика сучасної європейської політики безпеки: приклад Польщі: навчальний посібник. Львів: Видавництво Львівської політехніки, 2021. 224 с. URL: https://ena.lpnu.ua/bitstream/ntb/11535/1/Yaropolk%20Tymkiv%20Security%20Study%20ukr

27. 2030 Digital Compass: the European way for the Digital Decade. URL: https://ec.europa.eu/info/sites/default/files/communication-digital-compass-2030

28. A Digital Agenda for Europe. URL: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri

29. Clark L. Innovation in a Time of Crisis. Harvard Business Publishing. URL: https://www.harvardbusiness.org/innovation-in-a-time-of-crisis/

30. Dixit A. Governance Institutions and Economic Activity. URL: https:// www.princeton.edu/~dixitak/home/PresAd_F1

31. EUROPE 2020. A European strategy for smart, sustainable and inclusive growth. URL: https://ec.europa.eu/eu2020/pdf/

32. Europe's Digital Decade: Commission sets the course towards a digitally empowered Europe by 2030. URL: https://ec.europa.eu/commission/presscorner/ detail/en/ip_21_983

33. Global operational risk review. How war is fuelling geopolitical uncertainty. Economist Intelligence Unit (EIU), 2024. URL: https://www.eiu.com/n/campaigns/ operational-risk-review

34. Głodziński E., Marciniak S. Organisational Innovations in Crisis Management of ProjectBased Enterprises. Economics and Busines. Vol. 28. 2023. P. 26–32. URL: https://www.researchgate.net/publication/301571519_Organisational_ Innovations_in_Crisis_Management_of_Project-Based_Enterprises

35. Kolodziej P. Operational Risk, Compliance Risk & Auditing. January 2019.

36. Markopoulou D., Papakonstantinou V. P. de Hert. The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation. Computer Law & Security Review. 2023. Vol. 35. Issue 6. https://doi.org/10.1016/j.cls

37. Martinis M., Houghton K. The Business Risk Audit Approach and Audit Production Efficiency. December 2019. Abacus (A Journal of Accounting, Finance and Business Studies). № 55(4). P. 734-782.

38. National Security Strategy of the Republic of Poland. Warsaw, 2023. URL: https://www.files.ethz.ch/isn/156796/Poland-2007-eng.pdf

39. National Security Strategy of the Republic of Poland. Warsaw, 2024. URL: https://www.bbn.gov.pl/ftp/dokumenty/National_Security_Strategy_of_the_Republic_of_Poland

40. Osborne S., Brown L. Innovation in the public sector: a systematic review and future research agenda. Publc administration. Vol. 94. Is. 1. 2024. URL: https:// onlinelibrary. wiley.com/doi/10.1111/padm.12209

41. Putra F. Perspective 1: Crisis Management in Public Administration. Planning Forum UT. URL: https://sites.utexas.edu/planningforum/perspective-1-crisis-management-in-publicadministration/

42. Risk in Focus 2022: Hot topics for internal auditors. ECIIA, European Confederation of Institutes of Internal Auditing. The Corporate Governance House, Brussels, Belgium, September 2022. URL: https://www.eciia.eu/wp-content/uploads/2022/09/Risk-in-Focus

43. Risk in Focus 2023: Hot topics for internal auditors. Chartered Institute of Internal Auditing. URL: https://global.theiia.org/knowledge/Public%20Documents/Risk-in-Focus-Hot-Topics

44. Risk in Focus 2024: Hot topics for internal auditors. ECIIA, Chartered Institute of Internal Auditing, September 2024. URL: http://iap.work/wp-content/uploads/2024/12/risk-in-focus

45. Rocha J., Zavale G. Innovation and Change in Public Administration. Open Journal of Social Sciences. Vol. 9. Is. 6. 2021. P. 285–297. URL: https://www. scirp.org/ journal/paperinformation.aspx?paperid=110105

46. Shaping Europe's digital future. URL: https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digitalfuture

47. Single Supervisory Mechanism. URL: https://www.bankingsupervision. europa.eu/ about/ thessm/html/index.en.html

48. The official portal for Europeandata. URL: data.europa.eu.

49. Treaty on Stability. Coordination and Governance in the Economic and Monetary Union. URL: http://european-council.europa.eu/media/639235/st00tscg26

50. Vries H., Bekkers V. J. J. M., Tummers L. Innovation in the Public Sector: A Systematic Review and Future Research Agenda. ResearchGate: Electronic Journal. 2023. URL:https://www.researchgate.net/publication/315455642_Innovation_in_the_Public_Sector_A_Systematic_Review_and_Future_Research_Agenda