МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ ТА ЗАХИСТОМ ІНФОРМАЦІЇ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “ СИСТЕМА ПРАВОВОГО РЕГУЛЮВАННЯ ТА СТАНДАРТИЗАЦІЇ ЗАХОДІВ КІБЕРЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ”

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

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

_____ Дмітрій БОРИСЮК
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: Здобувач вищої освіти гр. УБД-41

Дмітрій БОРИСЮК
Ім’я, ПРІЗВИЩЕ

Керівник: Віталій САВЧЕНКО
Д.т.н., професор Ім’я, ПРІЗВИЩЕ

Рецензент: _____
Ім’я, ПРІЗВИЩЕ

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут кібербезпеки та захисту інформації

Кафедра управління кібербезпекою та захистом інформації
Ступінь вищої освіти бакалавр
Спеціальність 125 Кібербезпека
Освітня програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри УКБЗІ
_____ Світлана ЛЕГОМІНОВА
"____"_____2025 р.

ЗАВДАННЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

Дмітрію Юрійовичу Борисюку
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи " Система правового регулювання та стандартизації заходів кіберзахисту критичної інфраструктури ",
керівник кваліфікаційної роботи САВЧЕНКО Віталій, д.т.н., професор,
(ІПРІЗВИЩЕ, Ім'я,, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологійвід "24" лютого 2025 р. №56.

2. Строк подання кваліфікаційної роботи "12" травня 2025р.

3. Вихідні дані до кваліфікаційної роботи: теоретичні аспекти правового регулювання, міжнародні та національні стандарти, проблем та перспективи реалізації заходів кіберзахисту в критичній інфраструктурі .

4. Перелік питань, які мають бути розроблені:
   4.1. теоретичні аспекти правового регулювання кіберзахисту критичної інфраструктури.
   4.2. міжнародні та національні стандарти в галузі кіберзахисту критичної інфрастурктури.
   4.3. проблем та перспективи реалізації заходів кіберзахисту в критичній інфраструктурі.

5. Перелік ілюстративного матеріалу: *презентація PowerPoint*
6. Дата видачі завдання "5" березня 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	18.03.2025	
2.	Збір та аналіз літератури.	29.03.2025	
3.	Аналіз особливості управління інформаційною безпекою підприємства	08.04.2025	
4.	дослідження основних характеристик технологій формування системи правового регулювання та стандартизації заходів.	15.04.2025	
5.	Вивчення інструментів та методів систем правового регулювання та стандартизації заходів	22.04.2025	
6.	Формулювання висновків за результатами проведеного дослідження.	29.04.2025	
7.	Оформлення роботи.	06.05.2025	
8.	Оформлення презентації.	09.05.2025	
9.	Отримання рецензії на роботу.	12.06.2025	
10.	Захист в ДЕК.	__.06.2025	

Здобувач вищої освіти _____ Дмітірій БОРИСЮК
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Віталій САВЧЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

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

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

Направляється здобувач Борисюк Д. Ю. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: “ Система правового регулювання та стандартизації заходів кіберзахисту критичної інфраструктури ”
Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

Здобувач БОРИСЮК Дмітрій у кваліфікаційній роботі проаналізував особливості управління інформаційною безпекою підприємства, дослідив основні характеристики технологій формування системи правового регулювання та стандартизації заходів, вивчив інструменти та методи системи правового регулювання та стандартизації заходів, розробив практичні рекомендації за темою дослідження.

Дмітрій БОРИСЮК показав розуміння проблеми дослідження та бачення основних теоретичних і практичних напрямів, довів володіння методами наукового дослідження, проявив себе як організований, відповідальний виконавець.

Все це дозволяє оцінити кваліфікаційну роботу здобувача БОРИСЮКА Дмітрія на оцінку “відмінно” та присвоїти йому кваліфікацію бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Керівник кваліфікаційної роботи _____ Віталій САВЧЕНКО
(підпис) *(Ім’я,ПРІЗВИЩЕ)*

“____“_____2025 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Борисюк Д. Ю. допускається до захисту даної роботи в Екзаменаційній комісії.

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

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну бакалаврську роботу

здобувача вищої освіти БОРИСЮКА Дмітрія
на тему “ Система правового регулювання та стандартизації заходів кіберзахисту критичної інфраструктури ”

Актуальність. В Україні проблема кібербезпеки набула ще більшої актуальності після початку повномасштабної агресії з боку Російської Федерації. Кібератаки стали складовою воєнної стратегії противника, що загострило необхідність швидкого реагування, зміцнення кіберстійкості та реформування нормативно-правової бази у сфері кіберзахисту.

Особливої уваги потребує захист критичної інфраструктури – об’єктів, безперебійна робота яких є життєво важливою для функціонування держави, економіки, безпеки та здоров’я населення. Уразливість таких систем до кібератак може призвести до катастрофічних наслідків – від перебоїв у постачанні ресурсів до людських жертв і політичної дестабілізації.

Позитивні сторони.

1. У роботі охарактеризовано поняття критичної інфраструктури та її значення для національної безпеки; сформульовано основні принципи правового регулювання кіберзахисту; означено роль держави в забезпеченні кібербезпеки критичних об'єктів інфраструктури.
2. Кваліфікаційна робота оформлена відповідно до вимог. Виклад матеріалу здійснено відповідно до плану, зроблено логічні висновки. Ключові положення роботи представлено у вигляді рисунків..
3. Автор опрацював значну джерельну базу: близько 50 публікацій, в тому числі англомовних.
4. За результатами дослідження запропоновано рекомендації щодо правового регулювання та стандартизації заходів кіберзахисту критичної інфраструктури.

Недоліки.

Доцільно було б приділити більше уваги вивченню і класифікації програмних інструментів для оцінки та стандартизації заходів кіберзахисту критичної інфраструктури .

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

Висновок: Кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує оцінки “відмінно”, а здобувач БОРИСЮК Дмітрій заслуговує присвоєння кваліфікації бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Рецензент: _____ _____
підпис Ім’я, ПРІЗВИЩЕ

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню технологій формування обізнаності й навчання персоналу з інформаційної безпеки. Робота складається зі вступу, трьох розділів. Загальний обсяг роботи становить 80 аркушів, з яких 9 аркуші займають перелік умовних скорочень та список використаних джерел.

Метою роботи є дослідження системи правового регулювання та стандартизації заходів кіберзахисту критичної інфраструктури.

Об'єктом дослідження є суспільні відносини щодо кіберзахисту критичної інфраструктури.

Предмет дослідження - система правового регулювання та стандартизації заходів кіберзахисту критичної інфраструктури.

Методи дослідження. - основу дипломної роботи становить діалектичний метод як загальнонауковий метод пізнання соціально-правових явищ.

Системний метод використано для дослідження принципів правового регулювання кіберзахисту

***Галузь застосування*.** Розроблені підходи можуть бути використані при правовому регулюванні та стандартизації заходів кіберзахисту критичної інфраструктури.

Ключові слова: ІНФРАСТРУКТУРА, КРИТИЧНА ІНФРАСТРУКТУРА, СКЛАДОВІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ, КІБЕРЗАХИСТ, МІЖНАРОДНІ СТАНДАРТИ КІБЕРЗАХИСТУ, УГОДИ РЕАЛІЗАЦІЇ КІБЕРЗАЗХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ, ПРОБЛЕМИ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТУРКТУРИ.

ABSTRACT

The qualification thesis is dedicated to the study of technologies for raising awareness and training personnel in information security.
The thesis consists of an introduction and three chapters. The total volume is 80 pages, of which 9 pages are devoted to the list of abbreviations and the list of references.

The purpose of the study is to examine the system of legal regulation and standardization of cybersecurity measures for critical infrastructure.

The object of the research is the social relations concerning the cybersecurity of critical infrastructure.

The subject of the research is the system of legal regulation and standardization of cybersecurity measures for critical infrastructure.

Research methods: The foundation of the thesis is the dialectical method as a general scientific approach to understanding socio-legal phenomena.

The system method is used to explore the principles of legal regulation of cybersecurity.

Field of application: The developed approaches can be used in the legal regulation and standardization of cybersecurity measures for critical infrastructure.

Keywords: INFRASTRUCTURE, CRITICAL INFRASTRUCTURE, COMPONENTS OF CRITICAL INFRASTRUCTURE, CYBERSECURITY, INTERNATIONAL CYBERSECURITY STANDARDS, AGREEMENTS ON THE IMPLEMENTATION OF CRITICAL INFRASTRUCTURE CYBERSECURITY, PROBLEMS OF CRITICAL INFRASTRUCTURE PROTECTION.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ:

КІ – критична інфраструктура

ІБ – інформаційна безпека

ФРН – Федеративна Республіка Німеччина

ЄС – Європейський Союз

ІКТ – інформаційно-комунікаційні технології

КСЗІ – комплексна система захисту інформації

ВСТУП

Актуальність дослідження полягає в тому, що у сучасному світі, де цифрові технології пронизують усі сфери життя, питання кібербезпеки стає однією з ключових проблем національного та міжнародного рівня у зв'язку із стрімким поширенням кібератак та кіберзлочинів різного характеру. У сучасному світі кіберзахист – це не лише технічне завдання, а питання національної безпеки, де кожен має свою важливу роль.

В Україні проблема кібербезпеки набула ще більшої актуальності після початку повномасштабної агресії з боку Російської Федерації. Кібератаки стали складовою воєнної стратегії противника, що загострило необхідність швидкого реагування, зміцнення кіберстійкості та реформування нормативно-правової бази у сфері кіберзахисту.

Особливої уваги потребує захист критичної інфраструктури – об'єктів, безперебійна робота яких є життєво важливою для функціонування держави, економіки, безпеки та здоров'я населення. Це об'єкти енергетики, транспорту, водопостачання, охорони здоров'я, фінансової системи, зв'язку тощо. Уразливість таких систем до кібератак може призвести до катастрофічних наслідків – від перебоїв у постачанні ресурсів до людських жертв і політичної дестабілізації.

Окрім того, зважаючи на проєвропейський курс держави, слід докладати зусиль для покращення законодавчої бази, зокрема, у сфері кібербезпеки, враховуючи положення міжнародних правових норм. Доцільно підкреслити, що інтеграція досвіду та найкращих практик країн Євросоюзу й стандартів НАТО має бути ключовою метою.

В процесі вдосконалення системи законів важливо враховувати надзвичайну швидкість технологічного прогресу, що часто виводить порушників уперед державних службовців на кілька кроків у розробці

своїх дій. Отже, лише злагоджена робота відповідних відомств на всіх рівнях кібероборони забезпечуватиме її ефективність та досягнення пріоритетних завдань, поставлених перед державою.

У зв'язку з цим дослідження на тему систему правового регулювання та стандартизації кіберзахисту критичної інфраструктури набуває особливої актуальності.

Вивченню системи правового регулювання та стандартизації заходів кіберзахисту критичної інфраструктури присвятили свої наукові праці Ю.Березденький, С. Бірюков, К. Ганкевич, С. Гнатюк, С. Демедюк, О.Єрменчук та ін. Проблемам правового регулювання та стандартизації заходів кіберзахисту критичної інфраструктури присвячено розробки Б. Воровича, П.Горінова, Р.Драпушка, С.Демедюка, О. Полякова, П.Рогова, В. Роллера та ін., проте, сьогодні ряд питань залишаються дискусійними та потребують подальшого дослідження.

Мета роботи – дослідити систему правового регулювання та стандартизації заходів кіберзахисту критичної інфраструктури.

Для досягнення поставленої в даній роботі необхідно було вирішити низку ***завдань***, а саме:

- уточнити поняття критичної інфраструктури та визначити її значення для національної безпеки;

- охарактеризувати основні принципи правового регулювання кіберзахисту;

- з'ясувати роль держави в забезпеченні кібербезпеки критичних об'єктів інфраструктури;

- навести характеристику міжнародних стандартів та угод щодо кіберзахисту;

- дослідити національні правові акти, що регулюють кібербезпеку критичних інфраструктур в Україні;

- вивчити особливості співпраці державних органів та приватного сектору в забезпеченні кіберзахисту;

- здійснити аналіз правових проблем кіберзахисту в критичних галузях;

- розглянути особливості стандартизації процедур і технічних заходів кіберзахисту;

- вивчити перспективи розвитку кіберзахисту в Україні в контексті критичної інфраструктури;

- узагальнити матеріал та зробити висновки.

Об'єктом дослідження є суспільні відносини щодо кіберзахисту критичної інфраструктури.

Предметом дослідження є система правового регулювання та стандартизації заходів кіберзахисту критичної інфраструктури.

Методи дослідження:

- основу курсової роботи становить діалектичний метод як загальнонауковий метод пізнання соціально-правових явищ.

- системний метод використано для дослідження принципів правового регулювання кіберзахисту;

- формально-юридичний метод та метод системного аналізу використано для дослідження правового врегулювання кіберзахисту критичної інфраструктури України.

- завдяки порівняльно-правовому методу визначено рівень врегульованості щодо кіберзахисту критичної інфраструктури у законодавстві інших держав;

- конкретними методами дослідження були аналіз та синтез, що використовувалисть у роботі для дослідження проблем та перспектив реалізації заходів кіберзахисту в критичній інфраструктурі.

Інформаційною базою роботи є чинне законодавство України, навчальні посібники, монографії, періодична література, матеріали конференцій, а також Інтернет-ресурси.

Практичне значення одержаних результатів. Сформульовані в дипломній роботі положення та практичні рекомендації можуть бути використані в науково-теоретичних дослідженнях щодо правового регулювання та стандартизації заходів кіберзахисту критичної інфраструктури.

РОЗДІЛ 1
ТЕОРЕТИЧНІ АСПЕКТИ ПРАВОВОГО РЕГУЛЮВАННЯ КІБЕРЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

1.1 Поняття критичної інфраструктури та її значення для національної безпеки

Термін *«інфраструктура»* (*Infrastructure*) має латинське походження. Воно утворене від частки *infra*, що перекладається як «нижче» або «внизу», та слова *structura*, яке означає «будова», «конструкція» або «організована система». Таким чином, термін «інфраструктура» у буквальному сенсі означає «підтримуючу структуру» або «основу», яка лежить під чимось і забезпечує стабільне функціонування інших елементів або систем [8].

Р. Грищук зауважує, що на всіх історичних етапах формування та еволюції держави чи світового співтовариства в цілому постійно виникали виклики та можливі небезпеки для об'єктів – складових її інфраструктури, що зумовлювало пошук шляхів удосконалення її системи [10].

Як зазначає В. Бурячок, у процесі розвитку різних держав світу однією з головних загроз для їхнього соціального прогресу було визнано вторгнення іноземних військ, що зумовлювало пряму військову загрозу. В умовах такої небезпеки першочерговим прагненням будь-якого потенційного ворога-інтервента було знищення найвразливіших об’єктів, які забезпечували оптимальну життєдіяльність країни чи окремих її регіонів, постраждалих від військового нападу або збройної агресії [4].

Ще на початку VII століття до н.е. до п’яти найважливіших об'єктів у цьому контексті, які мають великий ризик бути знищеними ворогом були віднесені: людські ресурси із боку противника, його запаси, обози, склади та загони. Все це було окреслено у праці давньокитайського мислителф Сунь Цзи (славнозвісний трактат «Мистецтво війни») [4].

Окрім того, до числа важливих об’єктів, які могли бути ліквідовані або пошкоджені стороною протистояння збройного конфлікту на той час, були віднесені транспортна мережа та водопроводи, які були критично важливими для забезпечення життєдіяльності та благополуччя населення, країни, яка мала статус об'єкта збройного нападу. Основне завдання держави полягало у тому, щоб надійно захистити саме ці ключові об’єкти від руйнування чи знищення із боку ворога.

Згодом, в процесі історичного розвитку та еволюції людства, знищення чи захист інфраструктури критичних об'єктів держави став основним напрямком для досліджень в контексті розвитку й становлення військового мистецтва та діяльності спеціальних служб і силових правоохоронних органів усіх країн.

Як зазначають (Ю. Березделцький, М. Пальчик), поява дефініції «критична інфраструктура» та його поява бере початок ще з давніх часів (із часів греко-римської доби). Чи не вперше термін «інфраструктура» використав Сократ (V століття до н.е.). «Для існування людини, – підкреслював давньогрецький філософ, – необхідні захисні механізми, які надає суспільство: безпека, соціальний порядок і господарські ресурси» [2].

Проте, зміст та функції цього поняття могли бути реалізовані лише за умов діяльності органів державної влади через виконання нею своїх обов’язків задля забезпечення належного рівня добробуту її громадян. Основними з цих обов’язків було надання суспільного захисту населенню, що могла реалізувати виключно держава.

Поняття «критична інфраструктура», за визначенням (М. Борисов, А.Матанська), його виникнення у Франції спочатку співвідносилося із військовою сферою. Пізніше воно набуло поширення і в інших галузях (зокрема, у сфері будівництва), оскільки терміном «інфраструктура» позначали «те, що знаходиться під спорудами» [28].

О. Єрменчук вказує на те, що цей термін застосовували, як правило, у сфері будівництва залізничних шляхів, мостів і тунелів не тільки у Франції та Англії, але й у США. Саме на американському континенті воно набуло широкого поширення, і невдовзі його почали активно використовувати у всьому світі [15].

На думку С. Гнатюка, В. Лядовської, із часом значення поняття «інфраструктура» та «критична інфраструктура» а також перелік об'єктів, які вони охоплювали, безперервно змінювались згідно з трансформаціями у суспільстві, в умовах зростаючих потенційних загроз та воєнних конфліктів. Ці дефініції мали нерозривний зв'язок із провідними формами ведення бойових дій та зумовлювалися із діяльністю спеціальних державних служб. Зокрема, питання захисту критичної інфраструктури у період ХХ століття набуло особливої актуальності та значущості через так звані гібридні (неоголошені) війни [9].

Як зазначає Д. Федченко, в таких війнах агресор використовував унікальну комбінацію загроз, які були скеровані на тактично важливі та найбільш уразливі об'єкти такої агресії, представлені інфраструктурою та критичною інфраструтурою в умовах використання зброї, під час партизанських війн, при тероризмі тощо для досягнення певної політичної мети. «Гібридний» тип воєнних дій при цьому ставав дедалі актуальнішим [48].

Дослідник С. Демидюк вказав на те, що першими в Європі окреслили та почали оберігати безпеку національної критичної інфраструктури Федеративна Республіка Німеччина й Велика Британія (відповідно, з 1991 та 1999 років), адже саме тоді були сформовані Федеральне відомство інформаційної безпеки ФРН і Координаційний центр з безпеки національної інфраструктури Великої Британії. Федеральне відомство інформаційної безпеки ФРН скоро перейшло до структури МВС країни, й з 1998 року й по сьогодні воно залишається провідним федеральним

органом у питаннях інформаційної безпеки, зосереджуючись на захисті критично важливої інфраструктури [11].

Для захисту об’єктів своєї інфраструктури, за визначенням С. Гнатюка, В.Лядовської, було віднено дев’ять секторів критичної інфраструктури, об’єднаних такими галузями: енергетика (електропостачання, газопостачання, нафтовидобуток); водопостачання (комунальні та громадські водні ресурси); продовольство (харчова промисловість, торговельні мережі, забезпечення населення безпечною їжею); інформаційні технології та зв'язок; охорона здоров’я (медична допомога, медикаменти та вакцини, діагностика та лабораторні дослідження); фінанси та страхування (банки, біржі, страхові компанії, фінансові послуги); транспорт (авіація, морські перевезення, внутрішній водний транспорт, залізничні шляхи, автомобільні перевезення, логістика); державне управління (урядові структури, парламент, судова система, служби екстреної допомоги, включно з цивільним захистом); ЗМІ та культура (радіомовлення, телебачення, друковані та онлайн видання, культурна спадщина, архітектурні пам’ятки) [8].

Як зазначає В. Пядишев, враховуючи широке використання інформаційних технологій, до КІ відносили й інформаційну інфраструктуру. Спочатку воно містило у собі дев’ять, а згодом – тринадцять національних секторів КІ визначено у Великій Британії: хімічна промисловість, виробництво, оборона, цивільна ядерна сфера, екстрені служби, енергетика, фінанси, продовольство, уряд, охорона здоров’я, космос, вода та транспорт [42].

Дослідники (С. Вдовенко, Ю, Данюк, С. Фараон) зауважують, що у структурі національної інфраструктури Франції до КІ були віднесені 12 секторів: державне управління; збройні сили; система правосуддя; сільськогосподарська сфера; електронні комунікації; аудіовізуальні інформаційні технології; енергетика, космічна галузь та наукові

дослідження; фінансовий сектор; водопостачання; охорона здоров’я; транспортна система та промисловість [6].

За визначенням Н. Браліновського, в Іспанії критична інфраструктура охоплювала такі сфери: фінанси, електростанції та мережі, телекомунікації, охорона здоров'я, продовольство, водосховища, транспорт, аеропорти, морські й інші порти, національні пам'ятки, виробництво, зберігання й транспортування небезпечних вантажів (хімічних, біологічних або ядерних матеріалів) [51].

Як зазначає М. Федченко, на противагу іншим державам, у Данії замість терміна КІ використовують словосполучення «критичні суспільні функції». До них зараховують такі види діяльності, продукти й послуги, що гарантують стале функціонування суспільства й потребують підтримки та відновлення в разі аварій або катастроф. Згадані функції зосереджені передусім у таких галузях, як енергетика, транспорт, інформаційні технології, телекомунікації, хімічна промисловість тощо [48].

Окреслимо зміст та сутність різноманітних підходів науковців до дефініції «критична інфраструктура» та охарактеризуємо її значущість (роль) у питанні забезпечення національної безпеки. В сучасних реаліях термін «інфраструктура», за твердженням Ю. Березdецького, М. Пальчика використовується в різних контекстах та має декілька значень. Перш за все, під цим поняттям мається на увазі сукупність галузей економіки, які забезпечують виробничу діяльність і створюють необхідні умови для повсякденного функціонування суспільства [2].

Як зазначає вітчизняний дослідник Р. Грищук, інфраструктура також визначається як комплекс споруд, будівель, технічних систем та служб, що забезпечують функціонування секторів матеріального виробництва, а також сприяють підтримці життєдіяльності суспільства. У цьому контексті інфраструктуру прийнято поділяти на виробничу (наприклад, транспортні

мережі, канали, склади, порти, системи зв'язку) та соціальну (зокрема, лікарні, школи, театри, бібліотеки, стадіони) [10].

М. Ковалів під інфраструктурою розуміє сукупність галузей економіки, які мають допоміжний характер, зокрема транспорт, зв'язок, охорону здоров'я, освіту тощо [20].

Також інфраструктура розглядається як організована система взаємопов'язаних технічних та організаційних елементів або об'єктів, які формують основу для належного функціонування певної системи [18].

У дослідженнях (О. Скіцько, Р. Ширшова) ккритичну інфраструктуру схарактеризовано як комплекс структур, призначених для вирішення конкретного завдання або забезпечення цілісної роботи системи в цілому [47].

Загалом, під інфраструктурою розуміють також сукупність галузей народного господарства, що створюють загальні умови для економічної діяльності.

У науковій літературі (В. Заплатинський, Л. Хоферйтер) виокремлено такі види інфраструктур: виробничу; інноваційно-інвестиційну;освітню; глобальну інформаційну; інформаційно-комунікаційну; ГІС-інфраструктуру та інфраструктуру фондового ринку [17].

На думку зарубіжного дослідника А. Клімбурга, даний перелік не охоплює всього різноманіття видів інфраструктур, його можна доповнити наступними видами, а саме: військова інфраструктура, соціальна інфраструктура, інженерна інфраструктура, транспортна інфраструктура, ринкова інфраструктура, інфраструктура економіки, інформаційна інфраструктура, інноваційна інфраструктура тощо [51].

Таким чином, поняття інфраструктури включає сукупність об'єктів і систем, які обслуговують різні сфери (галузі) з метою їх належного функціонування.

Щодо терміну «критичний», то він має кілька значень:

- здатний до розумного та логічного мислення, заснованого на фактах та доказах;

- схильний до аналізу та виявлення слабких місць або недоліків;

- критичні умови або ситуації, що є складними, небезпечними або вимагають термінових дій [28].

При визначенні терміну «критична інфраструктура» важливо розглядати значення терміну «критичний» саме в контексті третього його тлумачення, яке стосується небезпеки та складних ситуацій.

«Критичний» – це той, що стосується кризи, знаходиться в стані кризової ситуації, переломний або небезпечний; це може означати винятково важкий, небезпечний або скрутний стан [9].

Отже, термін «критичний» в контексті інфраструктури слід трактувати як такий, що перебуває на межі рівноваги, після якої можуть виникнути серйозні загрози або негативні наслідки (криза). Інший варіант — це інфраструктура, яка перебуває в самому центрі кризи.

Здійснивши огляд літературних джерел, слід відмітити, що сьогодні наявні різні підходи щодо трактування поняття «критична інфраструктура» (табл. 1.1)

Таблиця 1.1

Основні наукові підходи щодо визначення поняття «критична інфраструктура»

Автор, джерело	Визначення поняття «критична інфраструктура»
Д. Бірюков, С. Кондратьєв	«…» - системи та ресурси, як фізичні, так і віртуальні, що виконують важливі функції та надають послуги, порушення роботи яких можуть призвести до найбільш серйозних негативних наслідків для життя суспільства, а також вплинути на соціально-економічний розвиток

	країн та національну безпеку [3, с. 108].
О. Скіцько, Р.Ширшов	«…» - це сукупність об'єктів, систем і мереж, порушення роботи яких може мати негативний вплив на різні аспекти соціально-економічного розвитку країни, а також загрожувати здоров'ю і безпеці населення [28].
О. Єрменчук	«…» - це система критично важливих матеріальних та нематеріальних об'єктів національної інфраструктури, включаючи їх власність та результати діяльності, що забезпечують її стабільне функціонування. Руйнація або пошкодження таких об'єктів, викликані наявними загрозами, можуть призвести до людських жертв і значних матеріальних збитків, що спричинить серйозні негативні наслідки для життєдіяльності суспільства, соціально-економічного розвитку країни та національної безпеки [8, с. 24].
В Заплатинський Л. Хофрейтер	«…» - це система важливих матеріальних і нематеріальних об’єктів національної інфраструктури, що включає підприємства та установи незалежно від форми власності, а також їхні ресурси та результати діяльності. Вона забезпечує стабільне функціонування таких стратегічних секторів, як енергетика, ядерна і хімічна промисловість, транспорт і зв'язок, фінансові установи, система інформаційних технологій та телекомунікацій, продовольча галузь, охорона здоров’я, комунальне господарство та інші. Ці об’єкти мають вирішальне значення для забезпечення національної безпеки та сталого розвитку економіки, і

	будь-які порушення їх роботи можуть спричинити серйозні наслідки для суспільства та держави в цілому [9, с. 2].

У розробках Д. Бірюкова, С.Кондратьєва критичну інфраструктуру України слід визначати як системи та ресурси, фізичні або віртуальні, що забезпечують функції та послуги, порушення яких призводять до серйозних негативних наслідків для життя суспільства та соціально-економічного розвитку, а також національної безпеки [3].

Дослідники (О. Скіцько, Р. Ширшов) надають більш широке визначення, підкреслюючи, що критична інфраструктура складається з сукупності об'єктів, систем і мереж, збій у роботі яких має негативний вплив на різні аспекти соціально-економічного розвитку країни і може призвести до погіршення стану здоров'я та безпеки населення [47].

Сучасний дослідник О. Єрменчук визначає критичну інфраструктуру як систему надзвичайно важливих матеріальних та нематеріальних об'єктів національної інфраструктури (також включаючи їх власність і результати діяльності), що забезпечують її стале функціонування. Руйнація чи пошкодження таких об'єктів можуть призвести до людських жертв, значних матеріальних збитків та серйозних негативних наслідків для життєдіяльності суспільства, соціально-економічного розвитку країни і національної безпеки [15].

Дослідники В. Заплатинський та Л. Хофрейтер формулюють своє визначення критичної інфраструктури як систему надзвичайно важливих матеріальних і нематеріальних об'єктів національної інфраструктури, що включають підприємства і установи незалежно від форми власності, їх власність і результати діяльності. Вони підкреслюють, що критична інфраструктура забезпечує стабільне функціонування таких галузей, як енергетика, ядерна і хімічна промисловість, транспорт і зв'язок, фінансові

установи, система інформаційних технологій і телекомунікацій, продовольча галузь, охорона здоров'я, а також галузь комунального господарства та інші [17].

Відповідно до Закону України «Про критичну інфраструктуру» (1882-IX від 16.11.2021) критична інфраструктура – це сукупність об’єктів критичної інфраструктури. Об’єкти критичної інфраструктури - об’єкти інфраструктури, системи, їх частини та їх сукупність, які є важливими для економіки, національної безпеки та оборони, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам [37].

Термін «критична інфраструктура» зазвичай використовується урядами для позначення систем і ресурсів, що є необхідними для стабільного функціонування суспільства та економіки. До таких об'єктів часто відносяться важливі галузі, які забезпечують базові потреби та послуги для життя людей і розвитку країни. Зокрема, до критичної інфраструктури зазвичай включають:

- генерацію, передачу та розподіл електроенергії;
- видобуток, транспортування та розподіл газу, нафти та нафтопродуктів;
- системи комунікацій і телекомунікацій;
- водопостачання та санітарні послуги;
- виробництво та розподіл харчових продуктів;
- теплопостачання;
- охорону здоров'я;
- транспортні системи;
- фінансову систему та банківські установи;
- служби безпеки, включаючи правоохоронні органи і надзвичайні служби [32].

У більшості зарубіжних країн термін «критична інфраструктура» використовується для класифікації та систематизації об'єктів, що мають

важливе значення для забезпечення національної безпеки та економічної стабільності. Це поняття охоплює ресурси та системи, які є критичними для функціонування суспільства, і їх знищення чи серйозне порушення роботи може спричинити серйозні наслідки.

У США термін «критична інфраструктура» було визначено в рамках «USA Patriot Act», де вказано, що це фізичні або віртуальні системи та ресурси, які є настільки важливими для країни, що їхнє знищення чи пошкодження може мати паралізуючий вплив на безпеку, національну економічну безпеку, охорону здоров'я, або будь-яку їх комбінацію. Це означає, що ці об'єкти є основою для життєдіяльності країни, і їхнє пошкодження чи виведення з ладу може привести до серйозних кризових ситуацій, які впливають на безпеку та стабільність [30].

Згідно з Директивою Європейської комісії № 786 від 2006 року (European Programme for Critical Infrastructure Protection), європейська критична інфраструктура включає об'єкти національних критичних інфраструктур країн-членів Європейського Союзу, вплив яких у разі відмови, інциденту або зловмисного втручання поширюється не лише на країну, де знаходиться цей об'єкт, але й на принаймні одну іншу державу-члена ЄС. Це визначення підкреслює важливість інтернаціональної співпраці та забезпечення безпеки критичних об'єктів на всіх рівнях, оскільки інциденти з критичними інфраструктурами однієї держави можуть мати масштабні наслідки для сусідніх країн [58].

За слушним зауваженням С. Грищука, якщо, наприклад, в Ізраїлі експерти визначають інфраструктуру як критично важливу, якщо її порушення може викликати серйозні соціально-економічні потрясіння, здатні підривати соціальну стабільність країни. Такі порушення можуть викликати загрози національній безпеці, оскільки втрата функціонування ключових об'єктів може мати далекосяжні наслідки для економічної та соціальної структури держави. Визначення критичності інфраструктури в

Ізраїлі акцентує увагу на тісному зв'язку між стабільністю суспільства та функціонуванням основних систем, що забезпечують її життєдіяльність [10].

Отже, критична інфраструктура – це система надзвичайно важливих матеріальних і нематеріальних об’єктів національної інфраструктури, включаючи їх власність та результати діяльності, яка забезпечує стабільне функціонування важливих секторів економіки та суспільства.

Руйнування або пошкодження цих об'єктів, зокрема через наявні загрози, може спричинити значні людські жертви і матеріальні збитки, а також призвести до серйозних негативних наслідків для життєдіяльності суспільства, економічного розвитку країни та національної безпеки в цілому.

Критична інфраструктура має стратегічне значення для забезпечення стабільного функціонування економіки та національної безпеки. Вона включає об'єкти та системи, від яких залежить безпека держави і суспільства. У разі виведення з ладу, руйнування або знищення таких об'єктів можуть виникнути серйозні наслідки, зокрема загрози національній безпеці та обороні країни. Крім того, це може призвести до значних матеріальних і фінансових збитків, а також до непоправних людських жертв і втрат, що ставить під загрозу стабільність і розвиток країни.

1.2 Основні принципи правового регулювання кіберзахисту

Принципи є важливим елементом, який визначає напрямок і методи розвитку в різних сферах діяльності. Вони виступають як основоположні засадами, на яких ґрунтується подальша діяльність і процеси. Вони надають структуру і орієнтацію для організації соціальних явищ і систем.

Завдяки принципам можна побудувати ефективне і перспективне явище, а в разі необхідності – реформувати або змінити його, що допомагає уникати стагнації чи кризи [10].

У правовому регулюванні принципи виконують таку ж функцію. Вони є основою для формування законодавчих і правових норм, на яких згодом будуються правовідносини між суб'єктами.

Принципи правового регулювання забезпечують стабільність і цілісність правової системи, визначаючи основні орієнтири для ефективного і справедливого вирішення суспільних питань. Це не просто загальні ідеї, а конкретні засади, що спрямовують розвиток правового поля в країні та визначають справедливі механізми взаємодії людей у межах правових норм [27].

Із огляду на це, принципи правового регулювання є невід'ємною частиною правової системи, вони формують базу, на якій здійснюється правовий порядок і взаємодія в суспільстві. Вони забезпечують ефективність, стабільність і справедливість у правовому регулюванні всіх сфер суспільних відносин.

Основні принципи правового регулювання кіберзахисту визначенні у ст. 7 Закону України «Про основні засади забезпечення кібербезпеки України» [38].

Забезпечення кібербезпеки в Україні ґрунтується на наступних принципах:

- верховенство права, законність, повага до прав людини та основоположних свобод, а також їхній захист згідно з вимогами законодавства;

- захист національних інтересів України;

- відкритість, доступність, стабільність і захищеність кіберпростору, розвиток Інтернету та відповідальність за дії у кіберсфері;

- співпраця між державою та приватним сектором, а також активна взаємодія з громадянським суспільством у сфері кібербезпеки і кіберзахисту, зокрема через обмін інформацією про інциденти, спільну реалізацію наукових і дослідницьких проектів, навчання та підвищення кваліфікації кадрів;

- пропорційність і адекватність заходів кіберзахисту на основі реальних і потенційних ризиків, а також право держави на самозахист відповідно до міжнародного права у разі агресивних дій у кіберпросторі [38];

- пріоритетність запобіжних заходів;

- невідворотність покарання за кіберзлочини [38];

- пріоритетний розвиток і підтримка вітчизняного наукового, науково-технічного та виробничого потенціалу;

- міжнародне співробітництво для зміцнення довіри в галузі кібербезпеки, розробка спільних підходів до боротьби з кіберзагрозами, координація зусиль у розслідуванні і запобіганні кіберзлочинам, а також недопущення використання кіберпростору для терористичних, військових і протиправних цілей;

- забезпечення демократичного цивільного контролю за військовими формуваннями та правоохоронними органами, які здійснюють діяльність у сфері кібербезпеки відповідно до законів України [38].

Слід зазначити, що в науковій літературі виокремлюють і інші принципи правового регулювання кіберзахисту.

Із огляду на це, доцільно виокремлювати наступні принципи правового регулювання кіберзахисту:

1. Принцип верховенства права. Правове регулювання кіберзахисту має ґрунтуватися на дотриманні загальновизнаних норм права, що гарантують юридичну визначеність, передбачуваність та захист прав і свобод людини. Це означає, що всі заходи у сфері кібербезпеки мають

відповідати Конституції України, міжнародним договорам та законам, а також не допускати порушення прав громадян на приватність, свободу вираження думки та вільний доступ до інформації [16].

2. Принцип законності. Усі дії держави, її органів, посадових осіб та приватного сектору щодо захисту кіберпростору повинні здійснюватися виключно в межах повноважень, передбачених законом. Законність у сфері кіберзахисту – це гарантія того, що запобігання, виявлення та реагування на кіберінциденти не перетворюються на інструмент політичного чи економічного тиску, а здійснюються виключно з метою забезпечення національної безпеки [46].

3. Принцип пропорційності. Заходи з кіберзахисту повинні бути пропорційними загрозі, яку вони мають відвернути. Це означає, що втручання в інформаційну сферу, особисті дані чи діяльність суб'єктів господарювання повинне бути обґрунтованим, мінімально необхідним та виправданим з точки зору інтересів безпеки. Пропорційність – це баланс між захистом і свободою.

4. Принцип публічно-приватного партнерства. Оскільки значна частина інформаційної інфраструктури, включаючи елементи критичної інфраструктури, належить або управляється приватними структурами, ефективна кібербезпека можлива лише за умови тісної співпраці між державою та бізнесом. Правове регулювання повинне стимулювати такі партнерства, забезпечуючи при цьому взаємні обов'язки, стандарти звітності, обмін інформацією про кіберзагрози та спільну відповідальність [16].

5. Принцип конфіденційності та захисту персональних даних. Один із ключових принципів правового регулювання кіберзахисту полягає у дотриманні права на приватність і недоторканність особистої інформації.

6. Принцип комплексності. Кіберзахист має забезпечуватися на всіх рівнях: законодавчому, технічному, організаційному, кадровому,

міжнародному. Тому правове регулювання повинне охоплювати всі аспекти функціонування кіберпростору – від визначення повноважень суб'єктів до вимог до програмного забезпечення, політик безпеки та процедури реагування на інциденти [10].

7. Принцип адаптивності та технологічної нейтральності. Оскільки інформаційні технології швидко змінюються, правове регулювання не повинно залежати від конкретних технічних рішень. Закони мають бути технологічно нейтральними та адаптивними – передбачати загальні підходи, що легко застосовуються до нових загроз, технологій або бізнес-моделей. Це дозволяє зберігати актуальність правових норм навіть у динамічному середовищі [55].

8. Принцип міжнародної координації. Кіберзагрози не визнають кордонів, тому ефективне правове регулювання кіберзахисту повинне враховувати міжнародне право, договори, конвенції, а також співпрацю з міжнародними організаціями. Законодавство України має бути сумісним з ключовими міжнародними актами, зокрема з Будапештською конвенцією про кіберзлочинність [42].

9. Принцип відповідальності та невідворотності покарання. Правове регулювання повинне передбачати чітко визначені санкції за порушення вимог кібербезпеки, кіберзлочини, витоки інформації або недотримання політик захисту даних. Наявність юридичної відповідальності — адміністративної, кримінальної, цивільної — є важливим чинником профілактики порушень у сфері кіберзахисту.

10. Принцип відкритості та прозорості. Хоча сфера кібербезпеки потребує певної конфіденційності, базові положення, стандарти, правила, пов'язані з кіберзахистом, повинні бути відкритими для суспільства. Це забезпечує довіру, розуміння з боку громадськості та підвищує рівень цифрової культури населення [11].

Отже, до основних принципів (засад) правового регулювання кіберзахисту:

верховенства права (дотримання загально прийнятих норм, принципів та концепцій чинного законодавства);

принцип законності (реалізація діяльності органів, що забезпечують кібербезпеку, на законних засадах, в межах повноважень, які детермінує закон);

принцип пропорційності (заходи кіберзахисту повинні реалізуватися на засадах виправданості та доцільності, проводитися із особливою обережністю у питанні втручання у особисті дані, дані об'єкта господарювання тощо);

право конфіденційності (приватність і недоторканність при аналізі уповноваженими органами особистої інформації);

принцип комплексності (заходи кібербезпеки повинні проводитися на законодавчому, технічному, організаційному, кадровому, міжнародному рівнях); принцип відповідальності та невідворотності покарання (застосування санкційних заходів проти порушень у кіберсфері);

відкритість та прозорість (правила, стандарти, положення кібербезпеки повинні бути відкритими і прозорими – для забезпечення довіри із боку громадськості заходам із кібербезпеки).

Всі вище окреслені принципи дозволяють ефективно реагувати на кіберзагрози, захищати національну безпеку та права громадян у цифровому середовищі.

1.3 Роль держави в забезпеченні кібербезпеки критичних об'єктів інфраструктури

Держава відіграє ключову роль у забезпеченні кібербезпеки критичних об'єктів інфраструктури, оскільки їхнє функціонування має прямий вплив на національну безпеку, економіку та добробут громадян.

Розглянемо основні функції держави в даній сфері.

1. Нормативно-правове регулювання:

розробка законодавства, яке визначає правила захисту критичної інфраструктури від кіберзагроз;

ухвалення стандартів та вимог до кіберзахисту державних і приватних операторів критичних систем;

впровадження відповідальності за порушення норм кібербезпеки [11].

2. Інституційне забезпечення кібербезпеки:

створення та функціонування спеціалізованих органів, таких як національні центри кібербезпеки та кіберполіція;

координація діяльності між державними установами, приватним сектором та міжнародними партнерами [10];

3. Моніторинг та оцінка кіберзагроз:

оцінка загроз та ризиків для критичних об'єктів інфраструктури;

впровадження системи раннього попередження про можливі кібератаки;

організація державного контролю та аудитів безпеки операторів критичної інфраструктури [30].

4. Розвиток технологічних засобів кіберзахисту:

інвестування у створення сучасних засобів кібербезпеки, зокрема систем виявлення вторгнень, шифрування даних та резервного копіювання;

впровадження механізмів захисту державних інформаційних систем від атак [32].

5. Міжнародне співробітництво:

обмін інформацією про кіберзагрози з міжнародними партнерами та участь у міжнародних програмах з кібербезпеки;

співпраця з міжнародними організаціями у сфері протидії кіберзлочинності [10].

6. Освіта та підготовка кадрів:

розвиток системи навчання фахівців у сфері кібербезпеки, створення спеціалізованих освітніх програм;

проведення інформаційних кампаній для підвищення рівня цифрової грамотності громадян.

7. Фінансування заходів кібербезпеки:

виділення бюджетних коштів на реалізацію програм з кіберзахисту критичних об'єктів;

стимулювання розвитку інноваційних рішень у сфері кібербезпеки [8].

8. Реагування на кіберінциденти:

створення кризових центрів для оперативного реагування на кіберзагрози;

запровадження планів дій на випадок масштабних атак на критичну інфраструктуру.

Провідні країни Європи приділяють велику увагу щодо забезпечення кібербезпеки критичних об'єктів інфраструктури (таблиця 1.2.)

Таблиця 1.2.

Способи правового регулювання кіберзахисту країн ЄС та України: порівняльний аналіз; складено автором за [8; 9; 54]

№	Країна	Способи правового регулювання

		кіберзахисту
1.	Велика Британія, Південна Корея, Японія	Удосконалення чинного законодавства та його узгодженість із директивами
2.	Франція	Діє агентство із забезпечення безпеки інформаційних систем (ANSSI).
3.	Німеччина	Реалізує свої функції із питань кіберзахисту Федеральне відомство з безпеки інформаційних технологій (BSI)
4.	Ізраїль	Орієнтація діяльності державних органів із забезпечення кібербезпеки на ефективну розвідувальну діяльність, інтеграція кібезхахисту, військової сфери та розвідки.
5.	Китай	Централізована ефективна (передова) модель кіберзахисту, що передбачає чіткі та суворі заходи правового контролю із боку держави.
6.	Україна	Гібридна модель кіберзахисту (в умовах військової агресії РФ).

Великобританія, Південна Корея та Японія ретельно відслідковують ситуацію й роблять важливі кроки щодо захисту суспільства від кіберагресій.

Країни Європейського Союзу підходять до кібербезпеки критичної інфраструктури через гармонізацію національного законодавства з європейськими директивами.

Кожна країна-член зобов'язана створити національний центр кібербезпеки, розробити стратегію та налагодити обмін інформацією з ЄС. Наприклад, у Франції діє ANSSI – Агентство національної безпеки інформаційних систем, а в Німеччині – Федеральне відомство з безпеки інформаційних технологій (BSI) [9].

Ізраїль є одним із найактивніших гравців у сфері кібербезпеки. Основна особливість підходу цієї держави – орієнтація на національну безпеку, глибока інтеграція кіберсфер у військову та розвідувальну діяльність.

Координацію захисту критичної інфраструктури здійснює Національне управління з кібербезпеки (INCD), підпорядковане безпосередньо уряду та Службі безпеки. Особливістю є те, що Ізраїль застосовує превентивні, іноді навіть наступальні кіберзаходи [54].

Китай застосовує максимально централізовану модель кіберзахисту, засновану на суворому контролі з боку держави.

Україна, з огляду на постійні кіберзагрози з боку Росії, розвиває гібридну модель кіберзахисту критичної інфраструктури. З одного боку, формується нормативна база, що відповідає європейським стандартам (наприклад, Закон «Про критичну інфраструктуру»), з іншого [держава змушена діяти в умовах воєнного стану, залучаючи як урядові структури, так і волонтерів, приватні компанії, IT-спільноти [37].

Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України», суб'єктами забезпечення кібербезпеки є міністерства та інші центральні органи виконавчої влади, органи місцевого самоврядування, місцеві державні адміністрації, правоохоронні, розвідувальні та контррозвідувальні органи, суб'єкти оперативно-

розшукової діяльності, Збройні сили України, інші військові формування, утворені відповідно до закону, Національний банк України, підприємства, організації та установи, зараховані до об’єктів критичної інфраструктури, Служба безпеки України, Національна поліція України, Міністерство оборони України, Державна служба спеціального зв’язку та захисту України [38].

Ці організації відіграють важливу роль у забезпеченні кібербезпеки, здійснюючи виявлення, запобігання та розслідування кіберзлочинів. Вони відповідають за захист критичних об'єктів та інформаційних ресурсів країни, а також за розробку і реалізацію стратегій і заходів з кіберзахисту. Окрім цього, вони активно взаємодіють з міжнародними партнерами у сфері кібербезпеки і працюють над підвищенням кіберсвідомості серед громадян та підприємств [11].

Ще одним важливим суб’єктом забезпечення кібербезпеки є Рада національної безпеки. Її роль визначає законодавство, зокрема стаття 4 Закону України “Про Раду національної безпеки і оборони України” [33].

Згідно з цим положенням, Рада національної безпеки і оборони України має відповідальність за розробку та розгляд питань, що стосуються безпеки стратегічних національних інтересів, включаючи напрямки забезпечення кібербезпеки, оскільки це є невід'ємною частиною національної безпеки України [33].

Рада також здійснює низку заходів у сфері інформаційної безпеки, що включають захист інформаційної інфраструктури, в той час як кібербезпека в рамках цієї стратегії передбачає вжиття заходів для захисту від цифрових атак у кіберпросторі. Вона проводить стратегічну оцінку стану та перспектив забезпечення кібербезпеки, грунтуючись на аналізі інформації, отриманої від суб'єктів, відповідальних за кібербезпеку, щодо загального стану кібербезпеки в країні. Це свідчить про важливість

координаційної функції Ради в контексті забезпечення кібербезпеки України.

Таким чином, держава відіграє визначальну роль у забезпеченні кібербезпеки критичних об'єктів інфраструктури шляхом створення нормативної, технічної та організаційної основи для захисту від кібератак.

Основною метою кіберзахисту на сучасному етапі розвитку нашої держави (особливо, у реаліях війни, через збільшення кібератак із боку країни-агресорки), є посилення кіберзахисту, захист прав і свобод громадян, державних інтересів.

Висновки до розділу 1

Отже, за результатами розділу зроблено наступні висновки:

критична інфраструктура – це сукупність надзвичайно важливих матеріальних і нематеріальних об’єктів, а також їхніх ресурсів і результатів діяльності, які забезпечують безперервне функціонування ключових секторів економіки та соціального життя держави;

забезпечення кібербезпеки в Україні спирається на комплекс принципів, що охоплюють правові, організаційні, технічні та міжнародні аспекти. Вони спрямовані на захист прав людини, національних інтересів, розвиток партнерства між державою, бізнесом і громадянським суспільством, ефективне реагування на кіберзагрози та зміцнення міжнародної співпраці, що у сукупності забезпечує стійкість держави до викликів у кіберпросторі;

забезпечення кібербезпеки критичних об'єктів інфраструктури є однією з пріоритетних функцій держави, адже стабільна робота цих об'єктів безпосередньо впливає на національну безпеку, економічну стабільність та рівень добробуту населення. До провідних функцій

держави у забезпеченні заходів кіберзахисту критичної інфраструктури належать:

1. Нормативно-правове врегулювання:

розробка законодавчої бази, що визначає правила захисту критичної інфраструктури від кіберзагроз;

затвердження стандартів та вимог до кіберзахисту державних та приватних операторів критичних систем;

запровадження відповідальності за невиконання норм кібербезпеки.

2. Інституційне забезпечення кібербезпеки:

створення та функціонування спеціалізованих державних органів, як-от національні центри кібербезпеки та кіберполіція;

координація взаємодії державних органів, приватного сектора та міжнародних партнерів;

3. Моніторинг та оцінювання кіберзагроз:

оцінка загроз та ризиків для об'єктів критичної інфраструктури;

впровадження систем раннього оповіщення про ймовірні кібератаки.

4. Розвиток технологічних засобів кіберзахисту:

інвестування у розробку сучасних засобів кібербезпеки, зокрема, систем виявлення вторгнень, шифрування даних та резервного копіювання;

впровадження механізмів захисту державних інформаційних систем від кібернападів.

5. Міжнародна співпраця:

обмін інформацією про кіберзагрози з міжнародними партнерами та участь у міжнародних програмах з кібербезпеки;

співпраця з міжнародними організаціями у сфері протидії кіберзлочинності.

6. Освіта та підготовка кадрів:

розбудова системи навчання фахівців у сфері кібербезпеки, створення спеціалізованих освітніх програм;

проведення інформаційних кампаній для підвищення рівня цифрової грамотності серед населення.

7. Фінансування заходів кібербезпеки:

виділення бюджетних коштів на реалізацію програм з кіберзахисту критичних об'єктів;

стимулювання розробки інноваційних рішень у сфері кібербезпеки.

8. Реагування на кіберінциденти:

створення кризових центрів для оперативного реагування на кіберзагрози;

впровадження планів дій на випадок масштабних атак на критичну інфраструктуру.

РОЗДІЛ 2
МІЖНАРОДНІ ТА НАЦІОНАЛЬНІ СТАНДАРТИ В ГАЛУЗІ КІБЕРЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

2.1 Міжнародні стандарти та угоди щодо кіберзахисту

Впровадження в Україні європейських стандартів та угод є вкрай важливим кроком, особливо у світлі зростаючих загроз в кіберпросторі та кібератак з боку РФ.

Співпраця України з міжнародними партнерами та підписання нових угод і домовленостей у сфері кібербезпеки зобов'язують країну дотримуватись їхніх норм і стандартів. Це стане важливим кроком для виведення України на рівень держав з високим рівнем кібербезпеки на міжнародній арені.

Міжнародні стандарти кіберзахисту – це нормативні документи, які визначають вимоги до безпеки інформаційних систем та даних. Вони допомагають організаціям забезпечувати захист корпоративної інформації та виконувати вимоги законодавства щодо інформаційної безпеки [32] (таблиця 2.1.)

Таблиця 2.1

Міжнародні стандарти та угоди щодо забезпечення кіберзахисту; складено автором за [11; 47]

№	Назва	Характеристика та функції
1.	ISO/IEC 27001	Міжнародний стандарт. Передбачає окреслення змісту дій задля удосконалення механізмів управління кібербезпекою.

		Окреслює процедуру, методологію та інструкції у питанні управління національною кібербезпекою.
2.	Cybersecurity Framework NIST	Розроблений Німеччиною. Містить дієві та ефективні світові практики – задля ефективного управління кібербезпекою країни в умовах постійних кіберзагроз.
3.	PCI DSS (Payment Card Industry Data Security Standard)	Стандарт міжнародного зразка. Спрямований на збереження безпеки даних користувачів пластикових карток.
3.	Загальний регламент про захист даних (General Data Protection Regulation, GDPR)	Стандарт ЄС. Стосується правил та умов захисту персональних даних користувачів українських карток, які знаходяться за кордоном.
4.	Регламент Європейського Парламенту і Ради (ЄС) 2019/881 від 17 квітня 2019 року.	Стандарт ЄС. Стосується правил та умов, а також процедури забезпечення заходів кібербезпеки.
Міжнародні угоди		
1.	Будапештська конвенція («Convention on Cybercrime, Council of Europe», 2005).	Нормативно-правовий акт міжнародного спрямування Спрямований на протидію

		кіберзлочинності, визначає кримінальну відповідальність за правопорушення в інтернет-мережі. Дає можливість країнам обмінюватися інформацією щодо кібездочинів.
2.	Директива NIS2 (Network and Information Security Directive 2) , набула чинності 2023 р., замінивши Директиву 2016 р.	Спрямована на посилення заходів безпеки у країнах ЄС. Встановлює єдині стандарти кібербезпеки для всіх країн-учасниць ЄС.

Розглянемо детальніше найвідоміших стандарти в питанні системи управління кібербезпекою.

ISO/IEC 27001 — міжнародний стандарт, який встановлює вимоги до створення, впровадження, підтримки та постійного вдосконалення системи управління інформаційною безпекою (ISMS). Стандарт визначає СУІБ як сукупність політик, процедур, методів, інструкцій і пов’язаних ресурсів, які організація використовує для захисту своїх інформаційних активів [27].

Система управління інформаційною безпекою є системним підходом до встановлення, впровадження, експлуатації, моніторингу, перегляду, підтримки та покращення безпеки інформації, орієнтуючись на досягнення бізнес-цілей. Вона ґрунтується на оцінці ризиків та рівнях прийнятності ризиків організації для ефективного управління ними [47].

Cybersecurity Framework NIST – стандарт розроблений Національним інститутом стандартів і технологій США (NIST), пропонує гнучкий підхід до управління ризиками в галузі кібербезпеки. Цей фреймворк містить набір рекомендацій, кращих практик і стандартів, які організації можуть застосовувати для оцінки та поліпшення свого стану кібербезпеки [46].

Основою фреймворку є п'ять функцій:

ідентифікація – виявлення та розуміння кіберзагроз і вразливостей для активів організації;

захист – впровадження заходів для забезпечення захисту інформаційних систем, запобігання кібератакам та мінімізації впливу;

виявлення – розпізнавання кіберзагроз і атак у реальному часі за допомогою моніторингу та інструментів для виявлення аномалій;

реагування — розробка та виконання планів і стратегій реагування на кіберінциденти для мінімізації їхнього впливу;

відновлення – відновлення функціонування систем і послуг після інциденту, забезпечення безперервності діяльності [15].

PCI DSS (Payment Card Industry Data Security Standard) – стандарт безпеки даних індустрії платіжних карток, розроблений для забезпечення того, щоб компанії, які обробляють, зберігають або передають інформацію про кредитні картки, підтримували безпечне середовище. Він визначає набір вимог до управління безпекою, політик, процедур, архітектури мережі, розробки програмного забезпечення та інших критичних заходів безпеки [30].

Ще один важливий стандарт, який широко застосовується в Україні, – це Загальний регламент про захист даних (General Data Protection Regulation, GDPR) Європейського Союзу. Він визначає правила щодо захисту персональних даних на території країн-членів ЄС. Регламент є обов’язковим для компаній, що обробляють персональні дані громадян та резидентів ЄС, незалежно від їхнього місцезнаходження. Таким чином, GDPR є обов’язковим і для українських компаній, які обробляють дані осіб, що знаходяться в ЄС [30].

Регулювання ЄС у сфері кібербезпеки: Регламент Європейського Парламенту і Ради (ЄС) 2019/881 від 17 квітня 2019 року, що стосується «Агентства Європейського Союзу з питань мережевої та інформаційної

безпеки (ENISA) та сертифікації кібербезпеки інформаційно-комунікаційних технологій» [7].

ENISA – Агентство Європейського Союзу з кібербезпеки. ENISA, як агенція Європейського Союзу, працює над досягненням високого рівня загальної кібербезпеки на території Європи. Засноване в 2004 році.

Агентство було посилене Актом про кібербезпеку ЄС. ENISA підтримує кіберполітику ЄС, збільшує надійність продуктів, послуг та процесів інформаційно-комунікаційних технологій (ІКТ) за допомогою сертифікаційних схем з кібербезпеки. Агентство активно взаємодіє з державами-членами та інституціями ЄС, допомагаючи Європі підготуватися до майбутніх кіберзагроз [27].

Завдяки обміну досвідом, нарощуванню потенціалу та поширенню інформації, Агентство співпрацює з ключовими зацікавленими сторонами задля укріплення довіри до мережевої економіки та підвищення стійкості інфраструктури Союзу.

З огляду на потребу гарантувати злагоджену роботу внутрішнього ринку, водночас прагнучи досягти високого рівня кібербезпеки, стійкості до кіберзагроз та довіри в межах Євросоюзу, цей Регламент визначає (відповідно до ст. 1, де визначено його загальні положення):

- цілі, задачі та організаційні аспекти діяльності ENISA (Агенції Європейського Союзу з питань безпеки мереж та інформації), відповідно до пункту а);

- основні засади для розробки європейських схем сертифікації кібербезпеки з метою забезпечення належного рівня кіберзахисту для ІКТ-продуктів, ІКТ-послуг та ІКТ-процесів у Союзі, а також для уникнення роздрібненості внутрішнього ринку стосовно схем сертифікації кібербезпеки в межах Євросоюзу (за пунктом б) [27].

Засади, що викладені у пункті (б) першого абзацу, діють без будь-яких обмежень щодо конкретних положень інших актів права Союзу, які стосуються добровільної або обов’язкової сертифікації.

Цей Регламент не звужує сферу повноважень країн-членів у питаннях, пов’язаних із громадською безпекою, обороною, національною безпекою, а також діяльністю держави у сфері кримінального права.

Статею 2 Регламенту здійснено аналіз означень та термінів, що детермінують кібербезпеку критичної інфраструктури, зокрема:

1.«Кібербезпека» охоплює заходи, що мають на меті захист мережевих і інформаційних систем, а також користувачів цих систем та інших осіб, які зазнають негативного впливу кіберзагроз.

«Мережева та інформаційна система» охоплює: мережу електронного зв'язку, як це визначено у пункті (a) статті 2 Директиви 2002/21/ЄС; будь-який пристрій або сукупність взаємопов'язаних чи суміжних пристроїв, де один або більше пристроїв, згідно з програмою, автоматично обробляють цифрові дані; або цифрові дані, які зберігаються, обробляються, витягуються або передаються за допомогою елементів, згаданих у пунктах (a) та (b), задля їх експлуатації, використання, захисту та технічного обслуговування;

3.«Національна стратегія безпеки мережевих та інформаційних систем» означає загальну структуру, яка визначає стратегічні цілі та пріоритети безпеки мережевих та інформаційних систем на рівні держави.

4.«Оператор основних послуг» визначається як оператор основних послуг, згідно з пунктом (4) статті 4 Директиви (ЄС) 2016/1148.

5.«Надавач цифрових послуг» означає будь-яку юридичну особу, що забезпечує цифрові послуги.

Щодо міжнародних угод, то на міжнародному рівні слід виділити Будапештську конвенцію та Директиву мережевої та інформаційної безпеки (NIS) [27].

У 2005 році Україна ратифікувала Будапештську конвенцію – єдиний міжнародний юридично обов’язковий документ, що регулює кібербезпеку. Вона встановлює спільну кримінальну політику для боротьби з кіберзлочинністю, вимагаючи прийняття відповідного національного законодавства та сприяння міжнародній співпраці [50].

Проте не всі її положення були інтегровані в національне законодавство, і для повної реалізації необхідно буде внести значні зміни до Кримінально-процесуального кодексу [41].

У 2016 році Європейський Парламент ухвалив першу частину єдиного законодавства ЄС щодо кібербезпеки – Директиву NIS. Оскільки Україна не є частиною ЄС, ця директива не є обов'язковою, проте вона служить орієнтиром для належної практики. Декілька її положень були добровільно імплементовані в українське законодавство, однак деякі залишаються без уваги. Проте, у 2023 цей документ було замінено на більш удосконалену версію – Директиву NIS2 (Network and Information Security Directive 2). Директива NIS2 (Network and Information Security Directive 2) – це оновлений нормативний акт Європейського Союзу, що набув чинності 16 січня 2023 року, після затвердження 14 грудня 2022 року. Вона замінила попередню Директиву NIS 2016 року та спрямована на посилення захисту кіберпростору в державах-членах ЄС. Основною метою NIS2 є забезпечення високого рівня захисту мережевих та інформаційних систем в країнах ЄС [14].

Цілі та завдання Директиви NIS2 – це:

1.Розширення сфери застосування: Директива NIS2 стосується ширшого кола галузей та організацій, включно з енергетикою, транспортом, охороною здоров’я, фінансовими послугами, цифровою інфраструктурою та іншими критично важливими секторами;

2.Уніфікація вимог безпеки: Запровадження єдиних стандартів кібербезпеки для всіх держав-членів ЄС сприяє гармонізації підходів до захисту інформаційних систем;

3. Підвищення відповідальності: Встановлення суворіших вимог до управління ризиками та звітування про інциденти кібербезпеки для організацій, що підпадають під дію директиви [14].

Україна зобов'язалась узгодити своє законодавство з Директивою NIS2 в рамках Ukraine Facility – фінансової допомоги від ЄС на відбудову та реформування країни.

Крім того, імплементація Директиви NIS2 є важливим етапом інтеграції України у цифровий ринок ЄС, що є ключовим кроком на шляху до членства України в ЄС [14]

Відповідно до цього практики ЄС у сфері кібербезпеки успішно адаптовано до європейських норм [**Ошибка! Источник ссылки не найден.**].

Отже, до важливих нормативно-правових актів, що детермінують особливості правового регулювання та стандартизації кіберзахисту критичної інфраструктури в Україні відносимо:

1. ISO/IEC 27001 – це стандарт міжнародного спрямування, котрий визначає необхідні параметри для розробки, розгортання, підтримки та безперервного вдосконалення системи управління інформаційною безпекою (СУІБ).

2. Регламент Європейського Парламенту та Ради (ЄС) 2019/881 від 17 квітня 2019 року "Щодо Агенції Європейського Союзу…», що стосуються різноманітних аспектів мережевої та інформаційної безпеки (ENISA) та передбачають сертифікацію кібербезпеки інформаційно-комунікаційних технологій.

3. Cybersecurity Framework NIST – стандарт-фреймворк, що містить ряд рекомендацій, найкращих практик та загальноприйнятих норм, які організації мають можливість використовувати задля оцінки й поліпшення

свого рівня кіберзахищеності. Він передбачає гнучке реагування на управління ризиками в сфері кібербезпеки.

4. PCI DSS (Payment Card Industry Data Security Standard) – стандарт безпеки даних у індустрії платіжних карт, котрий встановлює ряд вимог до управління безпекою, політикам, процедурам, архітектурі мережі, розробки програмного забезпечення та інших критичних заходів з безпеки.

5. На міжнародному рівні, до чинних стандартів, що регламентують управління державною безпекою, відносимо Будапештську конвенцію та Директиву щодо мережевої та інформаційної безпеки, яку Україна ратифікувала у 2005 році. Директива NIS, що детермінує заходи кібербезпеки, ухвалена 2016 Європарламентом, концепції якої передбачали ряд недосконалостей у питанні кіберзахисту та кібербезпеки, тому ці основні положення було розглянуто й вдосконалено через затвердження Директиви NIS2, що набула чинності із 2023. Це зумовило посилення заходів кібербезпеки інформаційних та мережевих систем.

2.2 Національні правові акти, що регулюють кібербезпеку критичних інфраструктур в Україні

Згідно з ст. 17 Конституції України, забезпечення інформаційної безпеки є однією з ключових функцій держави, яка є справою всього Українського народу [21].

Законодавство України у сфері кібербезпеки встановлює ефективні механізми реагування на кіберзагрози та кіберінциденти, закріплені у нормативно-правових актах, що становлять основу правового забезпечення кібербезпеки.

Розглянемо детальніше основні нормативно-правові акти, що регулюють кібербезпеку критичних інфраструктур в Україні.

Закон України «Про основні засади забезпечення кібербезпеки України» встановлює правові та організаційні основи захисту життєво важливих інтересів людини, громадянина, суспільства та держави в кіберпросторі, визначає основні цілі, напрями та принципи державної політики в сфері кібербезпеки, а також регулює повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, встановлюючи засади координації їх діяльності з забезпечення кібербезпеки [38].

Аналіз закону показує, що він створює загальні рамки для регулювання кібербезпеки, але не містить детальних вимог щодо захисту інформації та комунікацій.

Закон України «Про критичну інфраструктуру» встановлює правові та організаційні основи для створення та функціонування національної системи захисту критичної інфраструктури та є частиною законодавства у сфері національної безпеки [37].

Закон визначає критерії віднесення об’єктів до критичної інфраструктури з урахуванням їх важливості для національної безпеки, економіки та соціальної сфери. Енергетика, транспорт, інформаційно-комунікаційні технології, банківська справа та фінанси, охорона здоров’я, водопостачання та водовідведення, питне водопостачання, цивільний захист, хімічна промисловість, космічна діяльність, електронні комунікації, поштовий зв’язок та паливно-енергетичний комплекс [37].

Законом також визначено обов’язки розвідувальних органів щодо забезпечення кібербезпеки, включаючи проведення оцінки ризиків, здійснення заходів кіберзахисту, реагування на кіберінциденти та інформування компетентних органів про кіберінциденти. Передбачається створення Національної системи захисту розвідувальних органів, яка включає розвідувальні органи, державні установи та інші організації [37].

Отже, закон встановлює конкретні вимоги до захисту інформаційної інфраструктури та відіграє важливу роль у регулюванні кібербезпеки інформаційної інфраструктури.

Стратегія кібербезпеки України (Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України». Стратегія є важливим документом стратегічного планування, який визначає загальний напрям розвитку системи кібербезпеки України [33].

Указ Президента України; Стратегія від 26.08.2021 № 447/2021 визначають пріоритетні напрями державної політики у сфері кібербезпеки, в тому числі у сфері захисту інформаційно-комунікаційних технологій.

Постанови Кабінету Міністрів України: розвивають положення закону та визначають конкретні механізми реалізації державної політики у сфері кібербезпеки інформаційно-комунікаційної інфраструктури (Про затвердження плану заходів на 2023-2024 роки з реалізації Стратегії кібербезпеки України : Розпорядження Кабінету Міністрів України; План, Заходи від 19.12.2023) [10].

Наприклад: Постанова Кабінету Міністрів України від 19 червня 2019 року № 512 «Про затвердження Порядку формування переліку об’єктів критичної інфраструктури» (Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури : Постанова Кабінету Міністрів України; Вимоги, Перелік від 19.06.2019) [36].

Отже, аналіз чинного законодавства України свідчить про наявність базової правової бази. Водночас були виявлені прогалини та суперечності, які потребують вирішення.

Серед них виділяємо такі, як: відсутність чіткого диференційованого підходу до різних типів організацій критичної інфраструктури, а також необхідність посилення міжвідомчої координації та обміну інформацією щодо кіберінцидентів. Вивчення міжнародного досвіду може допомогти

визначити найкращі практики та сфери для вдосконалення українського законодавства. Диференціювати підхід до регулювання кібербезпеки відповідно до критичності об’єкта.

2.3 Співпраця державних органів та приватного сектору в забезпеченні кіберзахисту

Для України питання розбудови ефективного кіберзахисту у сфері критичної інфраструтури актуальне і нині, адже державно-приватна взаємодія проголошувалась одним з наріжних принципів забезпечення кібербезпеки країни, починаючи із затвердження Закону «Про основні засади забезпечення кібербезпеки» (2017 р). [38].

Чинна Стратегія кібербезпеки України (2021 р.) передбачає низку заходів для розбудови ДПП, переважна більшість із них не реалізована або ж не набула ознак системної діяльності. Динамічне, але епізодичне партнерство між приватним і державним секторами, що склалося після початку повномасштабного вторгнення у 2022 р., так і не оформилося в повноцінні інституційні форми, зокрема через нездатність жодної зі сторін такого партнерства чітко окреслити його цілі та організаційну структуру [26].

Запозичення досвіду міжнародних партнерів України в тій чи іншій формі може бути адаптованим в Україні. Український ринок кібербезпеки, зокрема, все ще обмежений з точки зору наявних ресурсів (фінансових та кадрових), що додатково ускладнюється воєнно-політичною ситуацією (рис. 2.1).

Рис. 2.1. Аналіз досвіду країн ЄС у питанні взаємодії державних органів та приватного сектору в забезпеченні кіберзахисту; складено автором за [50]

Створення хабів для стартапів та інновацій у сфері кібербезпеки (на зразок Cyber Ireland), що залучатиме як приватний сектор, так і освітні установи, здатне дати поштовх для розробки нових технологічних рішень у цій області.

Адаптація британської моделі «Industry 100» може слугувати основою для знаходження рішення щодо залучення кіберволонтерів до кібербезпекових заходів у державному секторі, що, своєю чергою, сприятиме співпраці державних органів та фахівців приватного сектора, та частково вирішить кадрову проблему у багатьох державних структурах.

Водночас досвід Латвії та Нідерландів може бути корисним для створення секторальних неурядових систем обміну інформацією про

кіберінциденти, що підвищить готовність підприємств відповідних секторів до реагування на кіберзагрози.

Із огляду на врахування досвіду європейських країн у питанні, жоден суб'єкт, чи то держава, чи приватна компанія, не здатен самостійно протистояти сучасним кіберзагрозам, які часто мають складний і транснаціональний характер. Тому актуальним є створення сталого механізму взаємодії між усіма учасниками цифрового середовища [50].

Державні органи, зокрема ті, що відповідають за інформаційну безпеку, володіють правовими та адміністративними інструментами для забезпечення захисту критичної інфраструктури, координації дій у випадку надзвичайних ситуацій, формування національної стратегії кібербезпеки.

Водночас саме приватні компанії: банки, телекомунікаційні оператори, постачальники програмного забезпечення першими зіштовхуються з реальними кіберзагрозами, виявляють вразливості та мають практичні знання про специфіку атак. Тому об'єднання зусиль дозволяє не лише своєчасно виявляти потенційні загрози, але й оперативно реагувати на них [59].

Одним із прикладів такої взаємодії є створення центрів реагування на кіберінциденти, які функціонують на базі державних структур (наприклад, CERT-UA в Україні) та активно взаємодіють із представниками приватного сектору [59].

Компанії передають інформацію про інциденти, з якими зіштовхуються, що дозволяє органам влади аналізувати ситуацію в режимі реального часу та попереджати інші установи про можливі атаки. У свою чергу, держава забезпечує нормативно-правову підтримку, надає рекомендації щодо посилення захисту та організовує спільні навчання та тренінги.

Важливим напрямом є також участь бізнесу у формуванні державної політики кібербезпеки.

Через галузеві асоціації, професійні об’єднання або напряму - через консультації з урядом - приватний сектор може впливати на розробку регуляторних актів, що відповідають сучасним технологічним викликам.

Також варто відзначити важливість публічно-приватного партнерства у сфері інвестицій у нові технології захисту, розробку інноваційних продуктів, підготовку кадрів та впровадження спільних дослідницьких програм.

Особливо показовою є роль бізнесу в умовах воєнного стану в Україні. З початком повномасштабного вторгнення Росії приватні IT-компанії, такі як SoftServe, Ajax Systems, EPAM та інші, не лише підтримали уряд технічно, а й стали активними учасниками національної кібероборони. Вони допомагали в розгортанні систем кіберзахисту, створенні рішень для резервного зберігання даних, організації кіберрезервів тощо. Така мобілізація ресурсів свідчить про високий рівень готовності приватного сектору долучатися до спільного захисту цифрового простору країни [31].

Таким чином, в умовах стрімкого зростання цифровізації та збільшення кількості кіберзагроз, співпраця між державними органами та приватним сектором стає ключовим фактором для забезпечення ефективного кіберзахисту.

Ефективне забезпечення кіберзахисту можливе лише за умови системної, постійної та довірливої співпраці між державою та бізнесом. Вона повинна базуватись на обміні інформацією, координації дій, спільній відповідальності та прагненні до постійного вдосконалення системи кібербезпеки.

Висновки до розділу 2

Отже, за результатами розділу зроблено наступні висновки:

дотримання міжнародних стандартів та участь у міжнародних угодах у сфері кібербезпеки є ключовими чинниками для інтеграції України у світовий простір кіберзахисту. Це не лише сприяє підвищенню рівня інформаційної безпеки в державі, а й дозволяє адаптувати найкращі світові практики, зміцнювати міжнародне співробітництво та посилювати спроможність країни протистояти сучасним кіберзагрозам;

в Україні сформовано основи національного законодавства у сфері кібербезпеки критичної інфраструктури, які забезпечують правове регулювання, розмежування повноважень органів влади та визначення стратегічних напрямів державної політики. Відсутність чіткого розмежування у підходах до різних видів організацій критичної інфраструктури, а також потреба в покращенні міжвідомчої взаємодії та обміну інформацією стосовно кіберінцидентів. Дослідження міжнародного досвіду може допомогти виявити оптимальні практики та напрямки для вдосконалення українського законодавства на принципах диференційованого підходу;

співпраця між державними органами та приватним сектором є критично важливою для ефективного забезпечення кібербезпеки в умовах сучасних викликів. Поєднання регуляторних можливостей держави та технічної обізнаності бізнесу створює основу для швидкого реагування на кіберзагрози, виявлення вразливостей і вдосконалення системи захисту.

Досвід України, особливо в умовах воєнного стану, демонструє важливість публічно-приватного партнерства, що охоплює обмін інформацією, координацію зусиль та спільну відповідальність. Така взаємодія повинна постійно розвиватися, аби відповідати динаміці цифрових загроз та зміцнювати національну кібербезпеку.

Особливо яскраво проявилася роль бізнесу в контексті війни в Україні. З перших днів широкомасштабного вторгнення Росії приватні IT-компанії, серед яких SoftServe, Ajax Systems, EPAM та інші, продемонстрували не лише технічну підтримку уряду, але й активну участь в укріпленні національної кібероборони. Вони брали участь в розгортанні систем кіберзахисту, розробці рішень для збереження резервних копій інформації, організації кіберрезервів та інших важливих завданнях. Ця консолідація ресурсів підкреслює готовність приватного сектора долучатися до забезпечення спільної безпеки цифрового простору країни.

Зважаючи на європейський напрямок розвитку держави, існує нагальна потреба вдосконалювати правову базу, особливо у сфері кібербезпеки, беручи до уваги приписи міжнародних нормативно-правових документів. Необхідно визнати першочерговість інтеграції досвіду та передових практик країн Євросоюзу та стандартів Північноатлантичного альянсу.

Більше того, процес удосконалення системи законодавства повинен враховувати стрімкий розвиток технологій, що стає причиною випередження злочинцями державних органів у вдосконаленні своєї діяльності.

Надзвичайно важливо акцентувати увагу на ключовій ролі публічно-приватного партнерства в фінансуванні передових технологій безпеки, створення новаторських продуктів, професійному розвитку спеціалістів та реалізації спільних наукових проектів.

Відтак, лише узгоджені зусилля відповідних структур на всіх рівнях кібероборони забезпечать її дієвість та досягнення поставлених перед країною задач в умовах складної ситуації протидії збройній агресії російської федерації проти України.

РОЗДІЛ 3
ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ РЕАЛІЗАЦІЇ ЗАХОДІВ КІБЕРЗАХИСТУ В КРИТИЧНІЙ ІНФРАСТРУКТУРІ

3.1 Правові проблеми кіберзахисту в критичних галузях

Недосконаліть системи чинного регулювання у сфері кібербезпеки значною мірою зумовлена відсутністю цілісної правової бази, а також наявністю численних прогалин і нечітких положень у законодавстві. Серед основних проблем можна виокремити такі:

Необхідність узгодження національного законодавства з міжнародними зобов'язаннями. В українському законодавстві відсутні визначення таких термінів, як «користувач послуг», «дані про рух інформації» та «електронні докази», а також не врегульовані питання щодо «термінового збереження комп'ютерних даних», «термінового збереження та часткового розкриття даних про рух інформації». Це ускладнює реалізацію положень Будапештської конвенції та обмежує можливості міжнародної співпраці у протидії кіберзлочинності [8]

Непослідовність термінології. Закон про кібербезпеку вводить низку нових термінів, однак деякі з них не відповідають поняттям, вживаним в інших нормативно-правових актах. Потрібно провести аналіз чинного законодавства для його гармонізації з новими положеннями. Крім того, деякі терміни сформульовані надто складно й потребують додаткового пояснення.

Відсутність чіткої нормативної бази щодо критичної інфраструктури. В Україні досі не створено єдину національну систему захисту критичної інфраструктури, а чинні регуляторні норми є фрагментарними та неузгодженими [10].

Брак нормативного регулювання аудитів інформаційної безпеки об’єктів критичної інфраструктури. Закон про кібербезпеку передбачає ухвалення урядом правил проведення таких аудитів, які мають базуватись на міжнародних стандартах ЄС і НАТО. Ці правила повинні розроблятися за участю профільних державних органів, наукових установ, незалежних аудиторів, експертів та громадських організацій [49].

Дублювання повноважень. До основних органів, що відповідають за кібербезпеку в Україні, належать Міноборони, ДССЗЗІ, СБУ, Нацполіція, НБУ та розвідувальні служби [9].

Окрім того, існує правова невизначеність щодо повноважень і обов’язків держустанов у сфері захисту критичної інфраструктури (КІ), а також щодо прав та обов’язків її власників і управлінців.

Наприклад, СБУ та МВС мають схожі повноваження щодо експертиз у справах, пов’язаних із кібербезпекою, однак не визначено критерії розподілу цих функцій. Хоча Закон про кібербезпеку закріплює за СБУ компетенцію в галузі кіберінцидентів, інші нормативні акти цього не відображають. Відповідні правоохоронні повноваження, як зазначено в Будапештській конвенції, не мають чіткого закріплення в КПК України, що ускладнює взаємодію органів, впливає на захист конфіденційності та підриває принципи верховенства права [49].

Відсутність чітких вимог до операторів критичної інфраструктури та цифрових провайдерів. Директива NIS зобов’язує країни встановлювати вимоги щодо безпеки та інформування операторів важливих послуг і цифрових провайдерів.

Обмежене бюджетне фінансування, що ускладнює залучення фахівців. Уряд обмежений у можливості виплачувати конкурентоспроможні зарплати спеціалістам з ІТ та кібербезпеки. У доповіді MITRE наголошується на проблемі низького рівня оплати праці в державному секторі порівняно з приватним. Це визнається стримувальним

чинником багатьма українськими стейкхолдерами. Чинні правові норми обмежують можливості урядових установ утримувати кваліфікованих фахівців, тому їх слід переглянути. Низький рівень оплати також підвищує ризик інсайдерських загроз і створює додаткову вразливість у системі кібербезпеки [18].

Отже, система правового регулювання кібербезпеки в Україні має суттєві недоліки: від відсутності узгодженості з міжнародними стандартами та нечіткої термінології до дублювання повноважень органів і браку нормативної бази щодо критичної інфраструктури.

Крім того, відсутність фінансових стимулів для залучення кваліфікованих фахівців поглиблює вразливість держави до кіберзагроз.

Для підвищення ефективності кіберзахисту необхідне комплексне оновлення та удосконалення чинного законодавства, посилення міжвідомчої координації та створення умов для залучення професійних кадрів.

3.2 Стандартизація процедур і технічних заходів кіберзахисту

Питання стандартизації у сфері кібербезпеки та захисту інформації є предметом постійних дискусій між вітчизняною професійною спільнотою і профільними державними органами.

Наразі в Україні як єдиний (крім банківського сектору) державний стандарт технічного захисту інформації діє серія нормативних документів, центральним з яких є НД ТЗІ 2.5–004–99 «Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу». Стандарт розроблений на основі так званих Канадських критеріїв безпеки комп’ютерних систем (Canadian Trusted Computer Product Evaluation Criteria (CTCPEC)), а також з урахуванням прийнятих в 2005 р.

міжнародних «Загальних критеріїв» (Common Criteria for Information Technology Security Evaluation (ISO 15408)).

На відміну від найпоширенішої у світі серії ISO/IEC27000, яка сфокусована на менеджменті інформаційної безпеки, критерієм захищеності інформації в НД ТЗІ 2.5–004–99 є відповідність архітектури та параметрів програмно-апаратних засобів об'єкта чіткому регламенту – комплексній системі захисту інформації (КСЗІ).

З точки зору фахівців, сама ідея, внутрішня структура і модель впровадження КСЗІ здебільшого не відповідає вимогам сучасного кіберзахисту, особливо в недержавному секторі.

Зазвичай експерти вказують на такі її недоліки, як:

недостатня гнучкість. Концепція КСЗІ вимагає ретельного документування архітектури та всіх налаштувань системи захисту інформації, а при внесенні будь-яких змін – складного й бюрократизованого процесу переатестації (до кількох місяців). Досить очевидно, що така статична модель захисту мало корелює з динамікою та розмаїттям бізнес-процесів, та й взагалі є не зовсім неадекватною викликам сучасного кіберпростору [55];

громіздкість. Підходи НДТЗІ, що вимагають створення великої кількості документації, є занадто громіздкими для приватного бізнесу;

обмежені можливості масштабування. КСЗІ/НДТЗІ не підходять для великих організацій/підприємств, приміром для заводів, де можуть використовуватися великі розподілені системи спостереження та керування промисловими процесами (наприклад, SCADA/АСК ТП);

застаріла концепція захисту/захищеності. Модель КСЗІ/НДТЗІ орієнтована на захист інформації в інформаційно-комунікаційній (комп'ютерній) системі як такій, без урахування конкретних безпекових потреб об'єкта кіберзахисту загалом [49].

Як свідчить міжнародний досвід, у сучасних умовах значно більший ефект дає проактивний, так званий ризик-орієнтований підхід, який передбачає моніторинг, імовірнісний аналіз та оцінювання ризиків (за шкалою – від прийнятних до неприпустимих) суб'єкта господарювання у певній екосистемі з метою дотримання кібербезпеки шляхом управління цими ризиками [2].

Нині у світі існує ціла низка відкритих для використання міжнародних стандартів кібербезпеки, але насамперед варто згадати про два їх різновиди, оскільки саме вони:

задають нині у світі певну концептуально-технологічну рамку і широко застосовуються в багатьох країнах;

до того ж, у них враховані найсучасніші тренди розвитку і відсутні вади, властиві українському НД ТЗІ 2.5–004–99 [49].

По-перше, це серія міжнародних стандартів ISO/IEC27000, розроблена Міжнародною організацією з стандартизації (ISO) спільно з Міжнародною електротехнічною комісією (IEC), яка постійно доповнюється новими документами. Серія, по суті, являє собою модель (фреймворк) для розробки, впровадження, функціонування, моніторингу, аналізу, підтримки та поліпшення системи менеджменту інформаційної безпеки як на загальному рівні (27001), так і в окремих секторах та галузях, – таких як фінанси, транспорт, енергетика, охорона здоров'я, оператори зв'язку, хмарні обчислення, інфраструктурні проекти, аудит і сертифікація тощо [11].

Впровадження системи управління інформаційною безпекою (СУІБ) відповідно до ISO/IEC27000 дозволяє оптимізувати процес захисту інформаційних ресурсів і управління ризиками для цих ресурсів. У нашій країні статус державного стандарту отримала перша версія ISO/IEC27001 (найновішою є ISO/IEC27001:2013), проте де-факто імплементований він лише в банківській сфері – у вигляді вимог СОУ Н НБУ 65.1 СУІБ 1.0:

2010 (згідно із Законом «Про основні засади забезпечення кібербезпеки України» Національний банк України є одним з суб'єктів національної системи кібербезпеки). Практичне застосування ISO/IEC27001 в інших галузях української економіки та бізнесу поки залишається відкритим через нормативно-правову неврегульованість [7].

Одним із найбільш авторитетних і відомих у світі є також National Institute of Standarts and Technology Cybersecurity Framework (NIST CSF) – розроблений американським Інститутом стандартів і технологій для організацій приватного сектору США комплекс методологій та рекомендацій щодо зниження IT-ризиків, запобігання, моніторингу і реагування на кібератаки. Фреймворк є відкритим, призначений виключно для добровільного використання і достатньо «гнучкий» для адаптації в різних умовах/краї нах, що зумовило його поширеність у світі. Уперше NIST CSF був випущений у 2014 р., в поточному році винесений на обговорення проект (draft version) версії 1.1. [49].

Отже, узагальнюючи все вище зазначене, варто відзначити, що нормальною світовою практикою є розробка і застосування у разі необхідності альтернативних або призначених для тих чи інших секторів недержавного сектору стандартів та фреймворків з кібербезпеки.

Серед іншого, це дозволяє уникати надмірної регуляторної монополізації, недоброчесної конкуренції й корупції, що нині особливо актуальне для України. Наприклад, хоча близько 70 % приватних організацій у США сьогодні віддають перевагу NIST Cybersecurity Framework, в американському енергетичному секторі діють стандарти NERC CIP, розроблені Північно американською корпорацією із забезпечення надійності електросистем (North American Electric Reliability Corporation), яка, до речі, є неприбутковою недержавною організа цією.

3.3 Перспективи розвитку кіберзахисту в Україні в контексті критичної інфраструктури

У сучасному світі кіберзахист критичної інфраструктури набуває особливого значення, адже від його надійності залежить не лише безперебійна робота економіки, а й національна безпека держави. В Україні це питання стало особливо актуальним після початку війни у 2014 році, а з 2022 року – набуло ще більшої ваги через активне використання кібератак як інструменту гібридної війни. Енергетика, транспорт, телекомунікації, водопостачання, охорона здоров'я, банківська система – усі ці сфери критичної інфраструктури стають потенційними цілями для кіберзлочинців і держав-агресорів. Саме тому розбудова ефективної системи кіберзахисту критичних об'єктів є одним із ключових завдань України на найближчі роки.

З огляду на виклики сьогодення, перспективи розвитку кіберзахисту в Україні визначаються кількома ключовими напрямами:

1. Вдосконалення нормативно-правового поля.

Україна зробила суттєві кроки у сфері кіберзахисту, зокрема ухваливши Закон України «Про основні засади забезпечення кібербезпеки України» [25]. Водночас нормативна база потребує подальшої деталізації: необхідно чітко визначити перелік об'єктів критичної інфраструктури, розробити єдині стандарти кіберзахисту, узгодити вимоги до інформаційної безпеки в різних секторах економіки. Важливу роль відіграє також гармонізація законодавства з європейськими та міжнародними нормами – зокрема, з Директивою NIS2 ЄС [14].

2. Посилення інституційної спроможності державних органів.

Державна служба спеціального зв'язку та захисту інформації України (ДССЗЗІ) і Національний координаційний центр кібербезпеки при РНБО є ключовими суб'єктами в системі захисту критичної інфраструктури. У майбутньому необхідно розширювати їхні технічні можливості, створювати регіональні центри реагування на інциденти (CERT-UA), підвищувати ефективність міжвідомчої взаємодії. Важливо також забезпечити стабільне фінансування й кадрове оновлення цих структур [22].

3. Впровадження сучасних технологій.

Сучасні рішення у сфері кібербезпеки базуються на використанні штучного інтелекту, машинного навчання, автоматизованих систем моніторингу, засобів багатофакторної автентифікації, криптографічного захисту. В Україні лише починається впровадження таких технологій, проте саме вони дозволяють перейти від реактивного до проактивного підходу в управлінні кіберризиками. Інвестиції у відповідні технології та підтримка інноваційних стартапів у сфері безпеки можуть значно посилити національну кіберстійкість [53].

4. Розвиток людського капіталу.

Жодна система кіберзахисту не буде ефективною без кваліфікованих фахівців. Україна потребує комплексної державної програми з підготовки, перепідготовки та підвищення кваліфікації спеціалістів з кібербезпеки.

Також важливо впроваджувати курси цифрової грамотності на рівні середньої та вищої освіти, адже людський фактор – одна з основних причин успішності кіберзагроз. Потрібно розвивати культуру інформаційної безпеки серед працівників державного сектору та компаній, що обслуговують критичну інфраструктуру [17].

5. Міжнародне співробітництво.

Україна активно співпрацює з НАТО, Європейським Союзом, США, Ізраїлем, Канадою та іншими країнами у сфері кіберзахисту. Ця співпраця

передбачає не лише обмін інформацією, а й участь у спільних навчаннях, технічну допомогу, інтеграцію у глобальні системи реагування на інциденти. У майбутньому важливо посилити участь України у міжнародних структурах, таких як EU CyberNet, НАТО Cooperative Cyber Defence Centre of Excellence (CCDCOE) тощо [60].

6. Публічно-приватне партнерство.

Багато об'єктів критичної інфраструктури перебувають у приватній власності, тому співпраця між державою і бізнесом є необхідною умовою ефективного захисту [5].

Особливо яскраво проявляється роль бізнесу в контексті війни в Україні. З перших днів широкомасштабного вторгнення Росії приватні IT-компанії, серед яких SoftServe, Ajax Systems, EPAM та інші, продемонстрували не лише технічну підтримку уряду, але й активну участь в укріпленні національної кібероборони. Вони брали участь в розгортанні систем кіберзахисту, розробці рішень для збереження резервних копій інформації, організації кіберрезервів та інших важливих завданнях. Така консолідація ресурсів підкреслює готовність приватного сектора долучатися до забезпечення спільної безпеки цифрового простору країни.

Ефективне втілення визначених дій буде підсилено рядом заходів з боку держави, зокрема:

заснування у структурі Міністерства оборони України кібервійськ та їх забезпечення відповідними фінансовими, кадровими та технічними ресурсами з метою стримування збройної агресії в кіберпросторі та забезпечення відсічі агресору;

впровадження дієвих механізмів взаємодії основних учасників національної системи кібербезпеки та сил оборони в частині спільного вирішення завдань кібероборони [8];

розробка та реалізація плану кібероборони як складової оборонного плану України;

проведення щонайменше двічі на рік спільних тематичних навчань з відповідними підрозділами країн – членів НАТО для досягнення оперативної сумісності;

створення MIL.CERT-UA в інтересах Міністерства оборони України та Збройних Сил України, налагодивши постійну співпрацю з європейською військовою CERT-мережею [19];

забезпечення оцінки спроможностей суб'єктів сектору безпеки і оборони в частині спільного виконання задач кібероборони, зокрема під час оборонних оглядів, оглядів національної системи кібербезпеки, оглядів стану кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури;

впровадження у системі військово-патріотичного виховання та системі територіальної оборони навчальних програм підготовки та проведення практичних навчань у сфері кібербезпеки [19].

Основні напрямки удосконалення системи правового регулювання та стандартизації заходів кібербезпеки нашої країни мають такий вигляд (рис 3.1.)

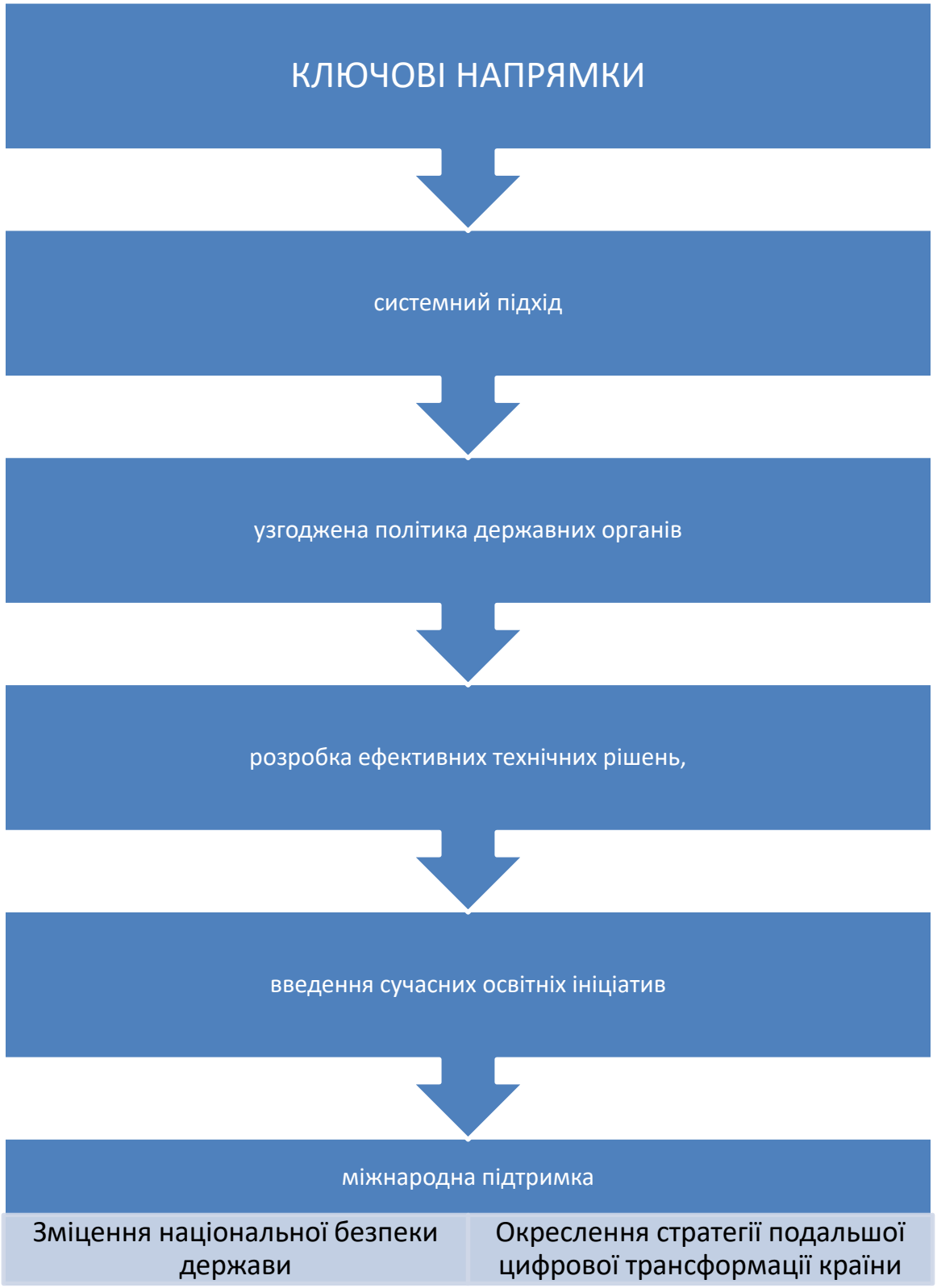

Рис. 3.1. Пріоритетні напрямки розвитку кіберзахисту в Україні в контексті критичної інфраструктури

Таким чином, розвиток кіберзахисту в Україні в контексті критичної інфраструктури – це багатогранне завдання, яке вимагає системного підходу, узгодженої політики, технічних рішень, освітніх ініціатив та міжнародної підтримки. Успішна реалізація зазначених напрямів дозволить не лише зміцнити національну безпеку, а й створить фундамент для подальшої цифрової трансформації держави.

Пріоритетні напрями кібероборони України можуть бути реалізовані через такі заходи, що стосуються:

гарантування безпеки кіберпростору задля збереження державного суверенітету та прогресу суспільства;

мають безпосередній зв'язок із забезпеченням захисту прав, свобод та законних інтересів українських громадян у віртуальному середовищі;

передбачають інтеграцію до європейського та євроатлантичного простору кібербезпеки.

Отож перспективи розвитку кіберзахисту в Україні в контексті критичної інфраструктури є широкими, але потребують системного підходу, координації на всіх рівнях, інвестицій у технології та людський капітал.

Висновки до розділу 3

Отже, за результатами даного розділу зроблено наступні висновки:

система правового регулювання кібербезпеки в Україні має суттєві недоліки - від відсутності узгодженості з міжнародними стандартами та нечіткої термінології до дублювання повноважень органів і браку нормативної бази щодо критичної інфраструктури. Крім того, відсутність фінансових стимулів для залучення кваліфікованих фахівців поглиблює вразливість держави до кіберзагроз. Для підвищення ефективності кіберзахисту необхідне комплексне оновлення законодавства, посилення

міжвідомчої координації та створення умов для залучення професійних кадрів;

система стандартизації кіберзахисту в Україні базується на застарілих підходах, що не відповідають сучасним вимогам динамічного кіберпростору. Вітчизняні стандарти (зокрема, КСЗІ/НД ТЗІ 2.5–004–99) мають низку недоліків: негнучкість, громіздкість, складність масштабування та орієнтація на застарілі концепції. Натомість у світі домінують ризик-орієнтовані підходи, втілені в міжнародних стандартах ISO/IEC 27000 та NIST CSF, які є більш гнучкими, практичними й адаптованими до потреб різних секторів.

Україна нині потребує перегляду національних підходів до стандартизації та гармонізації їх із міжнародними практиками, аби ефективно реагувати на сучасні кіберзагрози.

розвиток кіберзахисту критичної інфраструктури в Україні є стратегічним завданням, що набуло особливої актуальності в умовах війни та зростаючої кіберзагрози.

Основні перспективи полягають у вдосконаленні законодавчої бази, посиленні інституційної спроможності державних органів, впровадженні сучасних технологій, розвитку фахового потенціалу, міжнародній співпраці та публічно-приватному партнерстві.

Ефективна реалізація цих напрямів забезпечить стійкість ключових секторів економіки до кіберзагроз та підвищить рівень національної безпеки.

ВИСНОВКИ

Отже, відповідно до мети дослідження та поставлених завдань в роботі зроблено ряд висновків.

1. Уточнено поняття критична інфраструктура, під якою запропоновано розуміти систему надзвичайно важливих матеріальних і нематеріальних об’єктів національної інфраструктури, включаючи їх власність та результати діяльності, яка забезпечує стабільне функціонування важливих секторів економіки та суспільства. Досвід сучасних розвинених країн показує, що захист критичної інфраструктури є одним з основних напрямів їх державної політики у сфері забезпечення національної безпеки. Це логічно, оскільки КІ є невід'ємною частиною національної інфраструктури будь-якої країни та відіграє надзвичайно важливу роль основи функціонування та розвитку держави, її економіки й суспільного життя.

2. В ході дослідження зроблено висновок, що національна система кібербезпеки ґрунтується на цілісному підході, що включає правові, організаційні, технічні та міжнародні компоненти. Вона спрямована на захист прав громадян, національних інтересів, розбудову взаємодії між державою, бізнесом і громадянським суспільством, а також на своєчасне реагування на кіберзагрози та розвиток міжнародного співробітництва, що в сукупності формує кіберстійкість держави.

3. Встановлено, що охорона кібербезпеки об’єктів критичної інфраструктури є ключовою функцією держави, оскільки їх стабільне функціонування напряму впливає на рівень безпеки країни, економічну стабільність і добробут громадян.

4. В роботі обґрунтовано, що дотримання міжнародних стандартів і активна участь у глобальних ініціативах з кібербезпеки виступають

необхідною умовою інтеграції України у міжнародний кіберпростір. Це сприяє як впровадженню найкращих світових практик, так і підвищенню рівня захисту інформаційного середовища країни.

5. В Україні сформовано основи національного законодавства у сфері кібербезпеки критичної інфраструктури, які забезпечують правове регулювання, розмежування повноважень органів влади та визначення стратегічних напрямів державної політики.

6. Встановлено, що ефективний кіберзахист неможливий без тісної співпраці державного сектору з приватним. Поєднання регуляторних інструментів держави та експертних знань бізнесу дозволяє оперативно виявляти та реагувати на загрози, вдосконалювати системи безпеки, а також формувати культуру кіберзахисту. Практика останніх років, зокрема під час війни, підтверджує значущість публічно-приватного партнерства як основи для посилення національної кібербезпеки.

7. Існуюче законодавче регулювання у сфері кібербезпеки має суттєві прогалини: від недосконалості термінології та дублювання функцій органів до невідповідності міжнародним стандартам і відсутності стимулів для залучення фахівців.

8. Система стандартизації кіберзахисту в Україні базується на застарілих нормах, які не відповідають сучасним умовам цифрового середовища. Існуючі національні стандарти є громіздкими, негнучкими та важкими в реалізації, на відміну від міжнародних підходів на базі ризик-менеджменту (ISO/IEC 27000, NIST CSF). Необхідно провести реформу стандартів із врахуванням актуальних потреб секторів критичної інфраструктури та гармонізувати їх із міжнародними практиками.

9. Розвиток системи кіберзахисту критичної інфраструктури є стратегічною метою України, особливо в умовах воєнного часу та зростання кібератак. Основні напрями майбутнього розвитку повинні включати модернізацію законодавства, посилення можливостей державних

інституцій, впровадження новітніх технологій, формування професійного кадрового резерву, активізацію міжнародної співпраці та поглиблення взаємодії з приватним сектором. Державі слід створити стимули для інвестування бізнесом у кібербезпеку, а також – механізми обміну інформацією про загрози, рекомендації щодо захисту, спільні протоколи реагування. Крім того, бізнес може стати джерелом інноваційних рішень для національного кіберзахисту. Комплексне втілення цих заходів забезпечить стійкість держави до кіберзагроз та зміцнить її загальну безпеку.

Проведене дослідження не вичерпує глибини, проте, є підставою для подальших розвідок,що стосуються аналізу системи правового регулювання та стандартизації заходів кіберзахисту критичної інфраструктури.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Алексеєва О. А. Правове забезпечення кібербезпеки об’єктів критичної інфраструктури. Інформація і право. 2023. № 4 (47). С. 168–176. URL: https://doi.org/10.37750/2616-6798.2023.4(47).291633.

2. Березdецький Ю., Пальчик М. Окремі аспекти забезпечення кібербезпеки об’єктів критичної інфраструктури: досвід України. Інформаційна безпека людини, суспільства, держави. 2019. № 3(27). С. 49-56.

3. Бірюков Д.С., Кондратов С.І. Стратегія захисту критичної інфраструктури в системі національної безпеки держави. Стратегічні пріоритети. 2012. Вип. 3. С. 107 – 113.

4. Бурячок В.Л. Інформаційна та кібербезпека: соціотехнічний аспект / В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа. К.: ДУТ, 2015. 288 с.

5. Бодунова О.М. Кримінологічні засади запобігання злочинності у сфері інформаційних технологій: дисертація на здобуття наукового ступеня доктора юридичних наук за спеціальністю 12.00.08 «Кримінальне право та кримінологія; кримінально-виконавче право». Ірпінь, Державний податковий університет, 2024. 433 с.

6. Вдовенко С., Даник Ю., Фараон С. Дефініційні проблеми термінології у сфері кібербезпеки і кібероборони та шляхи їх вирішення. *CS&CS, Issue 1(13)* 2019. p. 17-29.

7. Ганкевич К.Б., Левчук В.Д., Корольов С.С. Особливості становлення правових засад існування об’єктів критичної інфраструктури України в системі Міністерства оборони України. Юридичний науковий електронний журнал. 2021. № 11. С. 79-82.

8. Горінов П.В., Драпушко Р.Г. Сучасні виклики адміністративно-правових засад кібербезпеки України в умовах воєнного стану. Юридичний науковий журнал. 2023. № 1. С. 267-270.

9. Гнатюк С.О., Лядовська В.М. Критерії визначення елементів критичної інфраструктури держави. 2013. URL: http://nauka.zinet.info/23/ gnatyuk.php.

10. Грищук Р.В. Основи кібернетичної безпеки/ Р.В. Грищук, Ю.Г. Даник. Житомир: ЖНАЕУ, 2016. 616 с

11. Демедюк С. В. Окремі питання адміністративно-правового та організаційного забезпечення кібербезпеки. *Південноукраїнський правничий часопис.* 2015. № 2. С. 144–147.

12. Демедюк С.В. Державно-приватне партнерство – важлива складова національної кібербезпеки в умовах війни. Діяльність Ради національної безпеки і оборони України та її Апарату, 2024. URL: https://www.rnbo.gov.ua/ua/Diialnist/7036.html?PRINT

13. Дудикевич В.Б. Основи інформаційної безпеки / В.Б. Дудкевич, В.О. Хорошко, Ю.Є. Яремчук. Вінниця: ВНТУ, 2018. 316 с.

14. Директива ЄС NIS2: що це таке, для яких потреб розроблена та для чого Україна її імплементує. URL: https://cip.gov.ua/ua/news/direktiva-yes-nis2-sho-ce-take-dlya-yakikh-potreb-rozroblena-ta-dlya-chogo-ukrayina-yiyi-implementuye

15. Єрменчук О.П. Основні підходи до організації захисту критичної інфраструктури в країнах Європи: досвід для України: монограф. Дніпро : Дніпроп. держ. ун-т внутр. справ, 2018. 180 с.

16. Єрема М., Борисенко А., Боротьба з кіберзлочинністю в умовах дії воєнного стану: Закон 2149-IX. Офіційний сайт «LIGAЗакон». URL: https://jurliga.ligazakon.net/ analitycs/210562_ borotba-z-kberzlochinnstyu-v-umovakh-d-vonnogo-stanu-zakon-2149-ix.

17. Заплатинський В., Хофрейтер Л. 2008. Критична інфраструктура та критична соціальна інфраструктура. Тези доповідей 8-ї міжвузівської науково-методичної конференції Безпека людини в сучасних умовах 4-5 грудня 2018 р. Харків: Національний технічний університет "Харківський політехнічний інститут". 2018. С. 4.

18. Іваненко О.І. Підхід до національної оцінки ризиків для критичної інфраструктури. Вісник ХНТУ. 2020. № 2(73). С. 9-22.

19. Ківалова Н.О. Правові проблеми захисту критичних об’єктів інфраструктури стратегічного значення в Україні. Право. Людина. Довкілля. 2019. № 3. С.124-131.

20. Ковалів М. Правове забезпечення кібербезпеки критичної інформаційної інфраструктури України. Traektoriâ Nauki = Pathof Science. 2021. Vol. 7. № 4. P. 2011-2018.

21. Конституція України. Закон від 28.06.1996 № 254к/96-ВР URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text

22. Когут Ю.І. Кібервійна та безпека об’єктів критичної інфраструктури: практичний посібник ; за ред. А.С. Довгополого. Київ: Консалтингова компанія “СІДКОН”, 2021. 332 с.

23. Комісія УСПП з питань науки та ІТ зробила переклад Директиви NIS2. I-UA.tv. 2023. URL: https:// i-ua.tv/tech/82418-komisiia-uspp-z-pytan-nauky-ta-it-zrobyla-pereklad-dyrektyvy-nis2.

24. Кримінальний кодекс України: Закон України від 05 квіт. 2001 р. № 2341-III / База даних «Законодавство України» / ВР України. URL: http://zakon4.rada.gov.ua/laws/show/2341-14.

25. Кучерина С.Є, Олейніков Д.О. Сучасний стан кримінально-правової охорони об’єктів критичної інфраструктури. Інформація і право. № 1(36)/2021. С. 90-98.

26. Лук'янчук Р.В. Міжнародне співробітництво у сфері забезпечення кібернетичної безпеки: державні пріоритети. Вісник Національної академії державного управління при Президентові України. Серія : Державне управління. 2015. № 4. С. 50-56.

27. Міжнародні стандарти у сфері інформаційної /кібербезпеки. URL: https://e-tk.lntu.edu.ua/pluginfile.php/24722/mod_resource/content/1/%D1%82%D0%B5%D0%BC%D0%B06.pdf

28. Матанська, А. О., Борисов, М.Ю. Шостий технологічний уклад в сучасній світовій економіці: зміст і початок. Добробут націй в умовах європейської інтеграції : зб. наук. праць 10-ї міжнар. наук.-практ. конф. – Одеса: Одес. нац. ун-т ім. І. І. Мечникова, 2020.

29. Моделі кіберкластерів у державно-приватному партнерстві: міжнародний досвід для України. URL: https://niss.gov.ua/news/komentari-ekspertiv/modeli-kiberklasteriv-u-derzhavno-pryvatnomu-partnerstvi-mizhnarodnyy

30. Підюков П.П., Калиновський О.В. Система державного захисту критичної інфраструктури України: генеза, сучасний стан і перспективи оптимізування в умовах подальшого забезпечення національної безпеки країни. URL:/Users/User/Downloads/592-%D0%A2%D0%B5%D0%BA%D1%81%D1%82%20%D1%81%D1%82%D0%B0%D1%82%D1%82%D1%96-1138-1-10-20211107.pdf

31. Поляков О. М. Активізація міжнародної співпраці у сфері забезпечення кібербезпеки: шляхи удосконалення в реаліях сьогодення. Інформація і право. 2021. № 2 (37). С. 129–138.

32. Поняття про критичну інфраструктуру. 2014. URL: http://mailswm.com/ponyattya-pro-kritichnuinfrastrukturu.

33. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ

Президента України від 26 сер. 2021 р. № 447/2021. URL : https://zakon.rada.gov.ua/laws/ show/447/2021#Text

34. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури : Постанова Кабінету Міністрів України; Вимоги, Перелік від 19.06.2019 № 518. База даних «Законодавство України». Верховна Рада України. 2025. URL: https://zakon.rada.gov.ua/go/518-2019-%D0%BF.

35. Про затвердження плану заходів на 2023-2024 роки з реалізації Стратегії кібербезпеки України : Розпорядження Кабінету Міністрів України; План, Заходи від 19.12.2023 № 1163-р. База даних «Законодавство України». Верховна Рада України. 2025. URL: https://zakon.rada.gov.ua/go/1163-2023-%D1%80.

36. Про затвердження Порядку ведення Реєстру об'єктів критичної інфраструктури від 28 квітня 2023 р. № 415 Київ. База даних «Законодавство України». Верховна Рада України. 2025. URL: https://zakon.rada.gov.ua/go/415-2023-%D0%BF

37. Про критичну інфраструктуру : Закон України від 16.11.2021 № 1882-IX. База даних «Законодавство України». Верховна Рада України. 2025. URL: https://zakon.rada.gov.ua/go/1882-20.

38. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163VIII. База даних «Законодавство України». Верховна Рада України. 2025. URL: https://zakon.rada.gov.ua/ go/2163-19.

39. Про ратифікацію Конвенції про кіберзлочинність : Закон України від 07 вер. 2005 р. № 2824-IV. URL : https://zakon.rada.gov.ua/laws/ show/2824-15#Text.

40. Про оборону України : Закон України від 06 груд. 1991 р. № 1932-XII. URL : https://zakon.rada.gov.ua/laws/ show/1932-12#Text.

41. Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації: Рішення РНБО від 29 грудня 2016 року. Офіційний сайт

Верховної Ради України. URL: https://zakon.rada. gov.ua/laws/show/n0015525-16#Text.

42. Пядишев В. Г. Кібербезпека критичних інфраструктур: закордонний досвід та українські реалії. Південноукраїнський правничий часопис. 2022. № 4. Ч. 3. С. 229–234. URL: http://www.sulj. oduvs.od.ua/ archive/2022/4/part_3/38.pdf.

43. Пінчук О.П.,. Литвинова С.Г., Буров О.Ю. "Синтетичне навчальне середовище – крок до нової освіти", Інформаційні технології та засоби навчання , 4(60), 28-45, ISSN 2076-8184. [Електронний ресурс]. Доступно: https://journal.iitta.gov.ua/index.php/itlt/article/view/1831, 2017.

44. Регламент Європейського Парламенту і Ради (ЄС) 2019/881 від 17 квітня 2019 року «Про Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA) та про сертифікацію кібербезпеки інформаційно-комунікаційних технологій. URL: https://zakon.rada.gov.ua/go/984_024-19

45. Рогов П. Д. Воровић Б. О., Ткаченко В. А. Шляхи Забезпечення кібернетичної безпеки об’єктів критичної інформаційної інфраструктури держави у воєнній сфері. Збірник наукових праць Центру воєнностратегічних досліджень Національного університету оборони України імені Івана Черняховського. 2017. № 1. С. 64–72. URL: http:// nbuv.gov.ua/UJRN/Znpcvsd_2017 _1_13

46. Роллер В.М. Правове регулювання здійснення кібероборони. Право і суспільство. 2018. № 5. Ч. 2. С. 137-141.

47. Скіцько О. І., Ширшов Р. А. Нормативно-правове забезпечення кібербезпеки об’єктів критичної інфраструктури. *Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична.* 2024. № 2. С. 73–79. DOI: https://doi.org/10.32782/2311-8040/2024-2-11.

48. Федченко Д.І. Система забезпечення кібербезпеки: проблеми формування та ефективної діяльності. Молодий вчений. 2017. Випуск 5 (57). С. 653–658.

49. Чибиряк М.С. & Федоровська Н.В. Проблемні питання та шляхи вдосконалення законодавства України у сфері забезпечення кібербезпеки. 2017. URL: http://dspace.oduvs.edu.ua/ bitstream/123456789/491/1/ilovepdf_ com-57-58%5B1%5D.pdf 21. ДІТМ МНТУ став партнером CRDF GLOBAL (2021). URL: http://www.ditm.com.ua/crdf-global.

50. Янковський О. Україні потрібна нова кіберстратегія. Українська правда. 2019. URL: https:// www.pravda. com.ua/rus/columns/2019/09/14/7226291/ 20.

51. Brailovskyi N. Evaluation of the Level of Cyber Security of Information / Brailovskyi N., Khoroshko V., Khokhlacheva Y., Ayasrah Ahmad. Scientific and Practical Cyber Security Journal (SPCSJ), vol3, #3, 2019. pp. 18-24.

52. Burov, "Virtual Life and Activity: New Challenges for Human Factors/Ergonomics", in Symp. Beyond Time and Space STO-MP-HFM-231, STO NATO, 2014, pp. 8-1…8-8. (in English).

53. Global Cybersecurity Index 2017 [Електронний ресурс]. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STRGCI.01–2017-PDF-E.pdf

54. Klimburg A. “National cyber security framework manual”. NATO CCD COE Publications (December 2012), [online]. Available: http://belfercenter.hks.harvard.edu/files/hathaway-klimburg-natomanualch-1.pdf, 2012. (in English).

55. Madeline Carr. Public–private partnerships in national cyber-security strategies [Електронний ресурс]. URL: https://www.chathamhouse.org/sites/files/chathamhouse/publications/ia/INTA92_1_03_Carr.pdf

56. Moore T. Introducing the Economics of Cybersecurity: Principles and Policy Options. Deterring Cyberattacks: Informing Strategies and Developing Options for U. S. Policy [Електронний ресурс]. URL: https://www.nap.edu/read/12997/chapter/3

57. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 ("USA Patriot Act"), Pub. L. No. 107-56, 115 Stat. 272

58. European Programme for Critical Infrastructure Protection (EPCIP). URL: https://ec.europa.eu/home-affairs/e-library/glos sary/european-programme-critical_en ; Council Directive 2008/114/E Cof 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. URL: https://eur-lex.europa.eu/legal-con
tent/EN/TXT/?uri=uriserv%3AOJ.L_.2008.345.01.0075.01.ENG

59. Hoffman F. Onnot-so-newwarfare: Political Warfare Vsvshybridthreats. 2014. URL: https://warontherocks.com/2014/07/on-notso-new-warfare-political-warfare-vs-hybrid-threats

60. Yan Z., Robertson T., Yan R., “Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment?”, ISSN: 2076-8184. Інформаційні технології і засоби навчання, 2019, Том 70, №2. 331 Computers in Human Behavior, ISSN: 0747-5632, Vol: 84, Page: 375-382, 2018. (in English).