ПРИВАТНЕ АКЦІОНЕРНЕ ТОВАРИСТВО
«ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«МІЖРЕГІОНАЛЬНА АКАДЕМІЯ УПРАВЛІННЯ ПЕРСОНАЛОМ»
Херсонський інститут

КУРСОВА РОБОТА

з дисципліни: Інформаційне право

на тему:

Кібербезпека як елемент національної безпеки

Виконала:
Студентка групи ІН19-9-22-Б1Пр (4,0ддс)
Фурт Олена
Керівник: к.ю.н., доцент Грінь А.А.

Оцінка:
Національна шкала _____
Кількість балів: _____ ECTS _____

Члени комісії _____ _____
(підпис) (прізвище та ініціали)
_____ _____
(підпис) (прізвище та ініціали)
_____ _____
(підпис) (прізвище та ініціали)

2026 рік

ЗМІСТ

ВСТУП

У сучасному світі стрімкий розвиток інформаційних технологій та цифровізація всіх сфер суспільного життя зумовлюють зростання значення кіберпростору як важливого середовища функціонування держави, економіки та суспільства. Разом із цим посилюються й загрози, пов’язані з використанням інформаційно-комунікаційних систем, що обумовлює необхідність формування ефективної системи кібербезпеки як складової національної безпеки.

Кібербезпека сьогодні розглядається як один із ключових елементів забезпечення стабільності держави, оскільки кіберзагрози можуть впливати на функціонування критичної інфраструктури, державних органів, фінансової системи та інформаційного простору. Кібератаки, витоки даних, інформаційні диверсії та інші форми кіберзлочинності здатні завдати значної шкоди як окремим суб’єктам, так і державі в цілому.

Особливої актуальності питання кібербезпеки набуває в умовах сучасних воєнних та гібридних конфліктів, де кіберпростір стає важливою ареною протистояння. Використання кібератак як інструменту впливу на державні процеси, дестабілізації суспільства та порушення функціонування стратегічно важливих систем свідчить про трансформацію характеру загроз національній безпеці.

В Україні проблема забезпечення кібербезпеки є особливо актуальною у зв’язку з тривалими безпековими викликами, що вимагають комплексного підходу до захисту інформаційних ресурсів та кіберінфраструктури. Важливим є не лише технічне забезпечення захисту, але й формування ефективної нормативно-правової бази, яка регулює діяльність у сфері кібербезпеки та визначає повноваження відповідних суб’єктів.

Крім того, актуальність дослідження зумовлена необхідністю гармонізації національного законодавства з міжнародними стандартами у сфері кібербезпеки, а також розвитком міжнародного співробітництва для протидії глобальним кіберзагрозам.

Таким чином, актуальність теми дослідження визначається зростанням ролі кібербезпеки у системі національної безпеки, необхідністю протидії сучасним кіберзагрозам, удосконаленням правового регулювання та забезпеченням ефективного функціонування держави в умовах цифровізації та глобалізації.

Метою курсової роботи є комплексне дослідження кібербезпеки як елемента національної безпеки, визначення її правової природи, аналіз нормативно-правового регулювання та виявлення актуальних проблем і напрямів вдосконалення системи забезпечення кібербезпеки.

Для досягнення поставленої мети визначено такі завдання:

– розкрити поняття кібербезпеки та її сутність;

– визначити місце кібербезпеки у системі національної безпеки;

– дослідити види та особливості сучасних кіберзагроз;

– проаналізувати вплив кіберзагроз на державу, суспільство та економіку;

– охарактеризувати принципи забезпечення кібербезпеки;

– визначити суб’єктів забезпечення кібербезпеки;

– проаналізувати національне законодавство України у сфері кібербезпеки;

– дослідити міжнародно-правові стандарти у цій сфері;

– розглянути організаційно-правові механізми забезпечення кібербезпеки;

– виявити актуальні проблеми забезпечення кібербезпеки;

– обґрунтувати напрями вдосконалення системи кібербезпеки в Україні.

Об’єктом дослідження є суспільні відносини, що виникають у процесі забезпечення кібербезпеки як складової національної безпеки.

Предметом дослідження є норми національного та міжнародного права, що регулюють сферу кібербезпеки, а також механізми їх реалізації та практичного застосування.

У процесі дослідження використано такі методи: діалектичний метод, формально-логічний метод, системно-структурний метод, порівняльно-правовий метод, історико-правовий метод, метод аналізу та синтезу, узагальнення.

Структура курсової роботи зумовлена метою та завданнями дослідження і складається зі вступу, трьох розділів, які поділяються на підрозділи, висновків та списку використаних джерел.

РОЗДІЛ 1. ТЕОРЕТИКО-ПРАВОВІ ОСНОВИ КІБЕРБЕЗПЕКИ ЯК ЕЛЕМЕНТА НАЦІОНАЛЬНОЇ БЕЗПЕКИ

1.1. Поняття кібербезпеки та її місце в системі національної безпеки

У сучасних умовах стрімкого розвитку інформаційно-комунікаційних технологій та цифровізації всіх сфер суспільного життя питання забезпечення кібербезпеки набуває особливої актуальності. Кіберпростір стає невід'ємною складовою функціонування держави, економіки та суспільства, що зумовлює необхідність формування чіткого розуміння сутності кібербезпеки як правової та наукової категорії.

У правовому аспекті поняття кібербезпеки закріплене в національному законодавстві України. Зокрема, відповідно до Закону України «Про основні засади забезпечення кібербезпеки України», кібербезпека визначається як захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечується сталий розвиток інформаційного суспільства, своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз у кіберпросторі [1]. Це визначення підкреслює комплексний характер кібербезпеки, яка охоплює як технічні, так і правові, організаційні та соціальні аспекти.

Аналізуючи зазначене визначення, можна дійти висновку, що кібербезпека розглядається законодавцем не лише як стан захищеності інформаційних систем, але й як більш широка категорія, що включає забезпечення стабільного функціонування державних інституцій, економічних процесів та суспільних відносин у цифровому середовищі. Важливою складовою є також орієнтація на превентивний характер діяльності — виявлення та попередження загроз, що свідчить про стратегічний підхід до забезпечення кібербезпеки.

У науковій доктрині поняття кібербезпеки трактується дещо ширше і багатовимірніше. Науковці розглядають кібербезпеку як складну міждисциплінарну категорію, що поєднує елементи права, інформатики, управління та безпеки. Вона визначається як система правових, організаційних, технічних та інших заходів, спрямованих на захист інформаційних ресурсів, інформаційно-телекомунікаційних систем та інтересів суб'єктів у кіберпросторі від несанкціонованого доступу, впливу, руйнування чи інших загроз [1].

Окремі дослідники акцентують увагу на тому, що кібербезпека є не лише станом захищеності, але й процесом, який передбачає безперервне вдосконалення механізмів захисту у відповідь на динамічні кіберзагрози. У цьому контексті кібербезпека виступає як діяльність держави, приватного сектору та громадянського суспільства, спрямована на формування безпечного кіберпростору та мінімізацію ризиків, пов'язаних із використанням цифрових технологій.

Важливою рисою наукового підходу є також розуміння кібербезпеки як складової ширшого поняття інформаційної безпеки. Однак, на відміну від останньої, кібербезпека зосереджується переважно на захисті інформаційно-комунікаційної інфраструктури, цифрових систем і мереж, а також на протидії кіберзлочинності та кібертероризму. Це дозволяє розмежувати відповідні категорії та уточнити предмет правового регулювання.

Таким чином, узагальнюючи підходи, що сформувалися у праві та науковій доктрині, можна визначити кібербезпеку як комплексне явище, яке поєднує в собі стан захищеності, процес забезпечення безпеки та систему заходів, спрямованих на захист інтересів особи, суспільства і держави в кіберпросторі.

Її правове закріплення в Україні відповідає сучасним викликам та створює основу для подальшого розвитку ефективної системи кіберзахисту.

У сучасних умовах цифровізації суспільства кібербезпека набуває статусу однієї з ключових складових національної безпеки держави.

Стрімкий розвиток інформаційних технологій, зростання залежності державних інституцій, економіки та соціальної сфери від інформаційно-комунікаційних систем зумовлюють необхідність розгляду кібербезпеки як невід'ємного елементу загальної системи безпеки держави.

Відповідно до Закону України «Про національну безпеку України», національна безпека визначається як захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів від реальних і потенційних загроз [2].

У цьому контексті кібербезпека виступає як один із напрямів забезпечення національної безпеки, оскільки кіберзагрози можуть безпосередньо впливати на стабільність держави, функціонування її інституцій та життєдіяльність суспільства.

Слід зазначити, що сучасні загрози у кіберпросторі мають комплексний характер і можуть спричиняти значні наслідки для національної безпеки. Зокрема, кібератаки можуть бути спрямовані на об'єкти критичної інфраструктури, державні інформаційні ресурси, фінансову систему, енергетичний сектор, транспорт та інші важливі сфери. Це підтверджує, що кібербезпека безпосередньо пов'язана із забезпеченням таких складових національної безпеки, як економічна, інформаційна, воєнна та техногенна безпека.

У науковій літературі підкреслюється, що кібербезпека є інтегрованим елементом системи національної безпеки, який забезпечує функціонування держави в умовах цифрового середовища. Вона розглядається як складова

інформаційної безпеки, але водночас має власну специфіку, пов’язану з технічними аспектами функціонування кіберпростору та особливостями кіберзагроз [3, с. 112]. Такий підхід дозволяє визначити місце кібербезпеки в ієрархії безпекових категорій та окреслити її роль у забезпеченні загальної стабільності держави.

Особливого значення кібербезпека набуває в умовах сучасних гібридних загроз та збройної агресії, коли кіберпростір використовується як інструмент впливу на державу.

Кібероперації можуть бути спрямовані на дестабілізацію політичної ситуації, поширення дезінформації, порушення функціонування державних органів та критичної інфраструктури.

У таких умовах кібербезпека виступає не лише як технічний інструмент захисту, але і як важливий елемент оборонної політики держави.

Водночас ефективне забезпечення кібербезпеки потребує комплексного підходу, який включає правове регулювання, організаційні механізми, технічні засоби та міжнародне співробітництво.

Важливу роль відіграє також взаємодія держави з приватним сектором, оскільки значна частина кіберінфраструктури перебуває у приватній власності.

Це зумовлює необхідність формування єдиної системи кіберзахисту, що охоплює всі рівні функціонування держави та суспільства.

Таким чином, кібербезпека є невід’ємною складовою національної безпеки, яка забезпечує захист життєво важливих інтересів держави, суспільства та особи в умовах функціонування кіберпростору.

Її значення постійно зростає у зв’язку з розвитком цифрових технологій та появою нових кіберзагроз, що вимагає постійного вдосконалення механізмів правового та організаційного забезпечення кібербезпеки.

1.2. Кіберзагрози як фактор впливу на національну безпеку

У сучасних умовах цифрової трансформації суспільства кіберзагрози виступають одним із ключових чинників, що впливають на стан національної безпеки. Розвиток інформаційно-комунікаційних технологій, з одного боку, сприяє підвищенню ефективності функціонування держави та економіки, а з іншого — створює нові вразливості, які активно використовуються зловмисниками. У зв’язку з цим особливого значення набуває дослідження видів та характеристик сучасних кіберзагроз.

Під кіберзагрозами у науковій літературі розуміють потенційні або реальні дії, явища чи процеси у кіберпросторі, які можуть завдати шкоди інформаційним ресурсам, інформаційно-телекомунікаційним системам, а також інтересам особи, суспільства та держави [4, с. 87]. Вони характеризуються високим рівнем динамічності, складністю виявлення та значним масштабом можливих наслідків.

Однією з найбільш поширених класифікацій кіберзагроз є їх поділ залежно від способу реалізації та об’єкта впливу. Зокрема, виділяють шкідливе програмне забезпечення (malware), яке включає віруси, троянські програми, шпигунське програмне забезпечення та програми-вимагачі (ransomware). Такі загрози спрямовані на несанкціонований доступ до інформації, її знищення або блокування з метою отримання фінансової вигоди чи дестабілізації роботи систем.

Окрему групу становлять мережеві атаки, серед яких найбільш поширеними є атаки типу «відмова в обслуговуванні» (DDoS). Їх метою є перевантаження серверів або мережевих ресурсів, що призводить до тимчасової або повної недоступності інформаційних сервісів. Такі атаки часто

використовуються як інструмент впливу на державні органи, банківські установи та об’єкти критичної інфраструктури.

Значну небезпеку становлять також фішингові атаки та соціальна інженерія, які спрямовані на отримання конфіденційної інформації шляхом маніпулювання користувачами. Зловмисники використовують підроблені електронні листи, вебсайти або повідомлення, що імітують офіційні джерела, з метою викрадення паролів, банківських даних чи іншої важливої інформації. Особливістю таких загроз є те, що вони базуються не лише на технічних, але й на психологічних механізмах впливу.

Крім того, сучасні кіберзагрози включають кіберрозвідку та кібершпигунство, які здійснюються як окремими групами, так і державами. Їх метою є отримання стратегічно важливої інформації, що може використовуватися у політичній, економічній чи військовій сферах. Такі загрози є особливо небезпечними для державної безпеки, оскільки вони часто мають прихований характер і можуть тривалий час залишатися непоміченими.

Серед новітніх кіберзагроз також варто виділити атаки на об’єкти критичної інфраструктури, включаючи енергетичні системи, транспорт, зв’язок та медичні установи. Використання цифрових технологій у цих сферах підвищує їх ефективність, але водночас робить їх вразливими до кібератак, наслідки яких можуть мати катастрофічний характер для функціонування держави.

Характерною рисою сучасних кіберзагроз є їх комплексність та транснаціональний характер. Кіберпростір не має чітких географічних меж, що ускладнює ідентифікацію джерел загроз та притягнення винних осіб до відповідальності. Крім того, кіберзагрози постійно еволюціонують, адаптуючись до нових умов та технологій, що вимагає безперервного вдосконалення системи кіберзахисту.

Таким чином, сучасні кіберзагрози є багатогранним явищем, що охоплює широкий спектр дій — від технічних атак до психологічного впливу на користувачів. Їх різноманітність та складність обумовлюють необхідність системного підходу до їх виявлення, аналізу та нейтралізації, що є важливою передумовою забезпечення національної безпеки держави.

У сучасних умовах цифровізації кіберзагрози мають суттєвий і багатовимірний вплив на ключові сфери життєдіяльності держави, суспільства та економіки. Зростання залежності від інформаційно-комунікаційних технологій призводить до того, що будь-які порушення у кіберпросторі можуть мати значні негативні наслідки як на національному, так і на глобальному рівнях.

Вплив кіберзагроз на державу проявляється передусім у порушенні стабільності функціонування органів державної влади та систем управління. Кібератаки можуть бути спрямовані на державні реєстри, інформаційні ресурси, системи електронного урядування, що призводить до втрати або спотворення даних, зниження довіри до державних інституцій та ускладнення процесу прийняття управлінських рішень. Крім того, кіберзагрози можуть використовуватися як інструмент політичного впливу, зокрема шляхом втручання у виборчі процеси або поширення дезінформації [5, с. 142].

Особливої актуальності проблема кіберзагроз набуває у сфері національної безпеки та оборони. Кібероперації можуть бути складовою гібридної війни, спрямованої на дестабілізацію внутрішньої ситуації в державі, підрив її обороноздатності та ослаблення міжнародних позицій. У цьому контексті кіберпростір стає новим полем протиборства, де здійснюються атаки на військові системи, об’єкти критичної інфраструктури та стратегічні комунікації.

Вплив кіберзагроз на суспільство проявляється у порушенні прав і свобод громадян, зокрема права на приватність, захист персональних даних та інформаційну безпеку. Викрадення персональної інформації, фінансових даних, а також використання цих даних у шахрайських схемах створює серйозні ризики для громадян. Крім того, поширення фейкової інформації, маніпуляцій та інформаційних кампаній у мережі Інтернет може впливати на суспільну свідомість, формувати викривлене сприйняття реальності та сприяти соціальній напруженості.

Окремої уваги заслуговує вплив кіберзагроз на економіку. Сучасні підприємства значною мірою залежать від цифрових технологій, що робить їх вразливими до кібератак. Внаслідок атак можуть виникати фінансові збитки, пов’язані з простоєм виробництва, втратою комерційної інформації, витоком конфіденційних даних або необхідністю відновлення систем. Особливо небезпечними є атаки на банківський сектор, платіжні системи та електронну комерцію, оскільки вони можуть підірвати фінансову стабільність та довіру до економічних інститутів.

Крім прямих економічних втрат, кіберзагрози мають і непрямі наслідки, зокрема зниження інвестиційної привабливості держави, погіршення ділового клімату та уповільнення інноваційного розвитку. Інвестори, як правило, враховують рівень кіберзахисту країни при прийнятті рішень щодо вкладення коштів, що свідчить про тісний взаємозв’язок між кібербезпекою та економічною стабільністю.

Таким чином, кіберзагрози мають комплексний вплив на державу, суспільство та економіку, створюючи серйозні виклики для забезпечення національної безпеки. Їхній масштаб та наслідки зумовлюють необхідність розробки ефективних механізмів протидії, що включають удосконалення законодавства, розвиток технічних засобів захисту, підвищення рівня

обізнаності населення та активізацію міжнародного співробітництва у сфері кібербезпеки.

1.3. Принципи та основи забезпечення кібербезпеки

Забезпечення кібербезпеки як важливої складової національної безпеки ґрунтується на системі загальних принципів, які визначають основні підходи, напрями та механізми формування ефективної державної політики у цій сфері. Принципи кібербезпеки виступають фундаментом для розробки нормативно-правових актів, організації діяльності уповноважених суб'єктів та впровадження практичних заходів захисту кіберпростору.

У науковій літературі принципи забезпечення кібербезпеки розглядаються як сукупність базових ідей та засад, які відображають закономірності функціонування системи кіберзахисту та визначають її спрямованість на захист інтересів особи, суспільства і держави [6, с. 59]. Вони мають комплексний характер і охоплюють правові, організаційні, технічні та соціальні аспекти забезпечення безпеки.

Одним із ключових принципів є принцип законності, який передбачає, що діяльність у сфері кібербезпеки повинна здійснюватися виключно на підставі та в межах чинного законодавства. Це означає, що всі заходи з виявлення, попередження та нейтралізації кіберзагроз мають відповідати правовим нормам, а також забезпечувати дотримання прав і свобод людини. Реалізація цього принципу сприяє підвищенню довіри до державних інституцій та ефективності їх діяльності.

Важливе значення має принцип комплексності, який передбачає поєднання різних заходів — правових, організаційних, технічних та інформаційних — для досягнення належного рівня кібербезпеки. Кіберзагрози

є багатогранними, тому протидія їм потребує системного підходу, що включає як запобігання, так і реагування на інциденти.

Принцип превентивності (попередження) полягає у необхідності своєчасного виявлення потенційних загроз та вжиття заходів для їх недопущення. Це означає, що основна увага має приділятися не лише ліквідації наслідків кібератак, але й запобіганню їх виникненню шляхом моніторингу кіберпростору, аналізу ризиків та впровадження сучасних засобів захисту.

Окремо слід виділити принцип координації та взаємодії, який передбачає узгоджену діяльність усіх суб'єктів забезпечення кібербезпеки. Ефективна протидія кіберзагрозам можлива лише за умови тісної співпраці між державними органами, приватним сектором, науковими установами та міжнародними партнерами. Це дозволяє забезпечити обмін інформацією, досвідом та ресурсами, необхідними для боротьби з кіберзагрозами.

Не менш важливим є принцип відповідальності, який передбачає притягнення до відповідальності осіб, винних у порушенні вимог кібербезпеки. Наявність ефективних механізмів юридичної відповідальності сприяє запобіганню правопорушенням у кіберпросторі та забезпечує дотримання встановлених норм і правил.

Також варто зазначити принцип адаптивності, який полягає у здатності системи кібербезпеки швидко реагувати на зміни у середовищі кіберзагроз. З огляду на динамічний характер розвитку інформаційних технологій, система кіберзахисту повинна постійно вдосконалюватися та оновлюватися відповідно до нових викликів.

Таким чином, загальні принципи забезпечення кібербезпеки формують основу для ефективного функціонування системи кіберзахисту. Вони визначають ключові напрями діяльності у цій сфері, сприяють узгодженості

дій різних суб’єктів та забезпечують належний рівень захисту інтересів особи, суспільства і держави у кіберпросторі.

Ефективне забезпечення кібербезпеки неможливе без чіткого визначення кола суб’єктів, які беруть участь у формуванні та реалізації державної політики у цій сфері. Система суб’єктів забезпечення кібербезпеки в Україні є багаторівневою та включає органи державної влади, правоохоронні органи, спеціальні служби, суб’єктів господарювання, а також громадян і громадські організації.

У науковій літературі суб’єкти забезпечення кібербезпеки визначаються як сукупність органів, установ, організацій та осіб, на яких покладено повноваження щодо здійснення заходів, спрямованих на захист кіберпростору, інформаційних ресурсів та інтересів держави, суспільства і особи [7, с. 134]. Такий підхід підкреслює комплексний характер системи кібербезпеки та необхідність взаємодії між різними її елементами.

Центральне місце у системі суб’єктів забезпечення кібербезпеки посідають органи державної влади. Зокрема, визначальну роль відіграє Президент України, який здійснює загальне керівництво у сфері національної безпеки, а також Рада національної безпеки і оборони України, яка координує та контролює діяльність органів виконавчої влади у сфері кібербезпеки. Важливим суб’єктом є також Кабінет Міністрів України, який забезпечує реалізацію державної політики та організацію виконання відповідних заходів.

До ключових суб’єктів належать і спеціалізовані органи, що безпосередньо здійснюють діяльність у сфері кібербезпеки. Серед них варто виділити Службу безпеки України, яка здійснює контррозвідувальну діяльність у кіберпросторі та протидіє кібертероризму, а також Державну службу спеціального зв’язку та захисту інформації України, яка відповідає за функціонування систем захисту інформації, кіберзахист державних

інформаційних ресурсів та реагування на кіберінциденти. Важливу роль відіграє і Національна поліція України, зокрема підрозділи кіберполіції, які займаються розслідуванням кіберзлочинів.

Окрім державних органів, значну роль у забезпеченні кібербезпеки відіграють суб'єкти господарювання, особливо ті, що є власниками або операторами об'єктів критичної інфраструктури. Вони зобов'язані впроваджувати заходи кіберзахисту, забезпечувати безпеку своїх інформаційних систем та взаємодіяти з державними органами у разі виникнення кіберінцидентів.

Важливим елементом системи кібербезпеки є також громадяни та громадські організації. Вони виступають як користувачі інформаційних систем і водночас як потенційні об'єкти кіберзагроз. Рівень їх обізнаності у сфері кібербезпеки, дотримання правил інформаційної гігієни та активна участь у формуванні безпечного інформаційного середовища суттєво впливають на загальний стан кібербезпеки в державі.

Слід підкреслити, що ефективність діяльності суб'єктів забезпечення кібербезпеки значною мірою залежить від рівня їх взаємодії та координації. У сучасних умовах кіберзагрози мають транснаціональний характер, що зумовлює необхідність міжнародного співробітництва та обміну інформацією між державами.

Таким чином, система суб'єктів забезпечення кібербезпеки є складною та багаторівневою, що включає як державні органи, так і приватний сектор та громадянське суспільство. Їх узгоджена діяльність є необхідною умовою ефективного функціонування системи кіберзахисту та забезпечення національної безпеки України.

РОЗДІЛ 2. НОРМАТИВНО-ПРАВОВЕ РЕГУЛЮВАННЯ КІБЕРБЕЗПЕКИ

2.1. Національне законодавство України у сфері кібербезпеки

На сучасному етапі розвитку інформаційного суспільства питання нормативно-правового регулювання кібербезпеки в Україні набуває особливої актуальності. Формування ефективної системи кіберзахисту неможливе без належної законодавчої бази, яка визначає правові засади діяльності суб'єктів, механізми реагування на кіберзагрози та забезпечення захисту національних інтересів у кіберпросторі.

Система національного законодавства у сфері кібербезпеки України є комплексною та включає нормативно-правові акти різного рівня — від Конституції України до спеціалізованих законів та підзаконних актів. Конституція України закріплює основоположні принципи захисту прав і свобод людини, зокрема право на інформацію, недоторканність приватного життя та захист персональних даних, що становить базу для формування правового регулювання у сфері кібербезпеки [8, с. 45].

Одним із ключових нормативно-правових актів у цій сфері є Закон України «Про інформацію», який визначає основні принципи інформаційних відносин, права та обов'язки суб'єктів, а також гарантії захисту інформації. Цей закон створює правову основу для регулювання процесів обігу інформації та встановлює вимоги щодо її захисту від неправомірного доступу, що є важливою складовою кібербезпеки [9].

Важливе місце у системі законодавства займає також Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», який регламентує порядок забезпечення захисту інформації в автоматизованих системах, визначає вимоги до створення комплексних систем захисту

інформації та встановлює відповідальність за порушення у цій сфері. Цей нормативно-правовий акт має прикладне значення, оскільки визначає технічні та організаційні засади захисту інформаційних ресурсів.

Крім того, важливу роль відіграють нормативні акти, що регулюють діяльність у сфері електронних комунікацій, цифрових послуг та захисту персональних даних. Зокрема, законодавство у сфері захисту персональних даних спрямоване на забезпечення прав громадян на приватність та контроль над власною інформацією, що є невід'ємною складовою кібербезпеки.

Система нормативно-правового регулювання кібербезпеки в Україні також включає підзаконні акти, стратегії та концепції, які визначають напрями державної політики у цій сфері. Вони спрямовані на розвиток національної системи кібербезпеки, удосконалення механізмів реагування на кіберінциденти та підвищення рівня захищеності об'єктів критичної інфраструктури.

Водночас слід зазначити, що національне законодавство у сфері кібербезпеки перебуває у стані постійного розвитку та адаптації до сучасних викликів. Зростання кількості кіберзагроз, поява нових технологій та інтеграція України у міжнародний інформаційний простір вимагають постійного оновлення правових норм та гармонізації їх із міжнародними стандартами.

Таким чином, національне законодавство України у сфері кібербезпеки є складною та багаторівневою системою, яка забезпечує правове регулювання відносин у кіберпросторі, визначає повноваження суб'єктів та створює умови для ефективного захисту інформаційних ресурсів і національних інтересів держави.

2.2. Міжнародно-правові стандарти та досвід забезпечення кібербезпеки

У сучасному глобалізованому світі кібербезпека набуває міжнародного характеру, оскільки кіберпростір не має чітких державних кордонів, а кіберзагрози можуть виникати та реалізовуватися з будь-якої точки світу.

У зв’язку з цим важливого значення набуває формування міжнародно-правових стандартів у сфері кібербезпеки та вивчення досвіду інших держав щодо протидії кіберзагрозам.

Одним із ключових міжнародно-правових актів у сфері кібербезпеки є Конвенція Ради Європи про кіберзлочинність (Будапештська конвенція), яка визначає основні підходи до криміналізації кіберзлочинів, встановлює механізми міжнародного співробітництва та гармонізації національного законодавства [10].

Цей документ став першим універсальним міжнародним договором, спрямованим на боротьбу з кіберзлочинністю, і є основою для формування національних правових систем у цій сфері, у тому числі й в Україні.

Важливу роль у формуванні міжнародних стандартів кібербезпеки відіграють також документи Європейського Союзу. Зокрема, Директива ЄС щодо безпеки мережевих та інформаційних систем (NIS Directive) встановлює вимоги до держав-членів щодо забезпечення належного рівня кіберзахисту, зобов’язує операторів критичної інфраструктури впроваджувати заходи безпеки та повідомляти про кіберінциденти [11].

Цей документ є важливим орієнтиром для України в процесі гармонізації законодавства з європейськими стандартами.

У науковій літературі підкреслюється, що міжнародне співробітництво у сфері кібербезпеки є необхідною умовою ефективної протидії кіберзагрозам.

Це зумовлено тим, що кіберзлочини часто мають транснаціональний характер і потребують координації дій правоохоронних органів різних держав, обміну інформацією та спільного розслідування [12, с. 176].

Крім того, міжнародні організації, такі як ООН, НАТО та ЄС, активно розробляють рекомендації, стратегії та стандарти, спрямовані на зміцнення глобальної кібербезпеки.

Аналіз міжнародного досвіду свідчить, що провідні держави світу приділяють значну увагу розвитку національних систем кібербезпеки, створенню спеціалізованих органів, впровадженню сучасних технологій захисту та підвищенню рівня кіберграмотності населення.

Наприклад, країни Європейського Союзу активно впроваджують підхід, заснований на ризик-орієнтованому управлінні кібербезпекою, що дозволяє ефективно розподіляти ресурси та мінімізувати потенційні загрози.

Водночас важливим аспектом міжнародного досвіду є розвиток публічно-приватного партнерства у сфері кібербезпеки.

У багатьох країнах приватний сектор відіграє ключову роль у забезпеченні захисту інформаційної інфраструктури, що зумовлює необхідність налагодження ефективної взаємодії між державними органами та бізнесом.

Таким чином, міжнародно-правові стандарти та досвід забезпечення кібербезпеки мають важливе значення для формування ефективної національної системи кіберзахисту.

Їх впровадження сприяє гармонізації законодавства, підвищенню рівня захищеності інформаційних систем та забезпеченню належного рівня взаємодії між державами у боротьбі з кіберзагрозами.

2.3. Організаційно-правові механізми забезпечення кібербезпеки в Україні

Забезпечення кібербезпеки в Україні здійснюється через діяльність системи державних органів, на які покладено функції формування та реалізації державної політики, координації, контролю, а також безпосереднього реагування на кіберзагрози. Ефективність функціонування цієї системи значною мірою залежить від чіткого розподілу повноважень між суб'єктами, їх взаємодії та узгодженості дій.

У науковій літературі діяльність державних органів у сфері кібербезпеки визначається як сукупність організаційно-правових, технічних та управлінських заходів, спрямованих на забезпечення захисту інформаційних ресурсів, кіберпростору та національних інтересів держави від кіберзагроз [13, с. 98]. Такий підхід підкреслює системний характер державної діяльності у цій сфері.

Ключову роль у координації діяльності державних органів відіграє Рада національної безпеки і оборони України, яка визначає стратегічні напрями державної політики у сфері кібербезпеки, координує та контролює діяльність органів виконавчої влади. Саме через механізми РНБО забезпечується узгодженість дій різних суб'єктів та оперативне реагування на актуальні кіберзагрози.

Важливим суб'єктом є також Кабінет Міністрів України, який забезпечує реалізацію державної політики у сфері кібербезпеки, розробляє нормативно-правові акти, організовує діяльність центральних органів виконавчої влади та забезпечує фінансування відповідних заходів. Через систему міністерств і відомств Кабінет Міністрів формує практичні механізми реалізації державної політики у цій сфері.

Особливе місце серед державних органів займає Державна служба спеціального зв’язку та захисту інформації України, яка є спеціально уповноваженим органом у сфері кіберзахисту. Вона здійснює організацію захисту державних інформаційних ресурсів, координує діяльність щодо реагування на кіберінциденти, забезпечує функціонування національної системи кіберзахисту та впроваджує стандарти інформаційної безпеки.

Служба безпеки України відіграє важливу роль у протидії кіберзагрозам, що мають ознаки загроз державній безпеці. Вона здійснює контррозвідувальну діяльність у кіберпросторі, виявляє та припиняє діяльність кібертерористичних та кібердиверсійних груп, а також забезпечує захист державних інформаційних ресурсів від зовнішніх посягань.

Не менш важливим є внесок Національної поліції України, зокрема підрозділів кіберполіції, які здійснюють розслідування кіберзлочинів, виявляють правопорушення у сфері використання інформаційних технологій, а також взаємодіють із міжнародними правоохоронними органами з метою боротьби з транснаціональною кіберзлочинністю.

Крім того, у сфері кібербезпеки функціонують й інші державні органи, зокрема міністерства, відомства та регуляторні органи, які в межах своїх повноважень забезпечують реалізацію заходів кіберзахисту у відповідних галузях. Їх діяльність спрямована на забезпечення безпеки інформаційних систем, захист персональних даних, а також розвиток цифрової інфраструктури.

Слід зазначити, що ефективність діяльності державних органів у сфері кібербезпеки значною мірою залежить від рівня їх координації та взаємодії. У сучасних умовах кіберзагрози мають складний і динамічний характер, що вимагає оперативного обміну інформацією, спільного планування та реалізації заходів реагування.

Таким чином, діяльність державних органів у сфері кібербезпеки є комплексною системою заходів, спрямованих на забезпечення захисту кіберпростору та національних інтересів України. Її ефективність визначається рівнем організації, координації та здатністю адаптуватися до нових викликів у сфері кібербезпеки.

У сучасних умовах розвитку цифрової економіки ефективне забезпечення кібербезпеки неможливе без налагодженої взаємодії між державою та приватним сектором. Це зумовлено тим, що значна частина об’єктів інформаційної інфраструктури, включаючи телекомунікаційні мережі, фінансові системи, енергетичні ресурси та інші елементи критичної інфраструктури, перебуває у власності або під управлінням приватних компаній. Відповідно, рівень їх захищеності безпосередньо впливає на загальний стан кібербезпеки держави.

У науковій літературі взаємодія держави та приватного сектору у сфері кібербезпеки розглядається як форма публічно-приватного партнерства, що передбачає об’єднання ресурсів, інформації та зусиль для запобігання, виявлення та нейтралізації кіберзагроз [14, с. 121]. Такий підхід дозволяє підвищити ефективність заходів кіберзахисту, оскільки приватний сектор володіє значними технічними можливостями, інноваційними рішеннями та практичним досвідом у сфері інформаційної безпеки.

Однією з основних форм взаємодії є обмін інформацією про кіберінциденти, загрози та вразливості. Державні органи, зокрема спеціалізовані служби кіберзахисту, отримують від приватних компаній дані про виявлені атаки, що дозволяє оперативно реагувати на загрози та запобігати їх поширенню. У свою чергу, держава надає рекомендації, методичну допомогу та інформацію про актуальні кіберризики.

Важливим напрямом співпраці є також спільна розробка та впровадження стандартів кібербезпеки. Держава встановлює нормативні вимоги до захисту інформаційних систем, а приватний сектор забезпечує їх практичну реалізацію. Це сприяє уніфікації підходів до кіберзахисту та підвищенню рівня безпеки інформаційної інфраструктури.

Крім того, взаємодія держави та бізнесу проявляється у проведенні спільних навчань, тренінгів та симуляцій кіберінцидентів. Такі заходи дозволяють підвищити рівень готовності до реагування на кіберзагрози, удосконалити координацію дій та відпрацювати механізми взаємодії в умовах кризових ситуацій.Особливого значення набуває участь приватного сектору у забезпеченні кібербезпеки об’єктів критичної інфраструктури.

Власники та оператори таких об’єктів зобов’язані впроваджувати комплексні системи захисту, проводити оцінку ризиків та забезпечувати безперервність функціонування своїх систем. У цьому контексті держава виконує регуляторну та координаційну функцію, встановлюючи вимоги та контролюючи їх дотримання.

Водночас існують і певні проблеми у взаємодії держави та приватного сектору. Серед них можна виділити недостатній рівень довіри, обмежений обмін інформацією, відсутність єдиних стандартів та недостатню правову визначеність механізмів співпраці. Це зумовлює необхідність удосконалення нормативно-правової бази та розвитку інституційних механізмів публічно-приватного партнерства у сфері кібербезпеки.

Таким чином, взаємодія держави та приватного сектору є ключовим елементом системи забезпечення кібербезпеки. Її ефективність визначає здатність держави протидіяти сучасним кіберзагрозам, забезпечувати стабільність функціонування критичної інфраструктури та захищати національні інтереси в умовах цифрового середовища.

РОЗДІЛ 3. ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ РОЗВИТКУ КІБЕРБЕЗПЕКИ В УКРАЇНІ

3.1. Актуальні проблеми забезпечення кібербезпеки в умовах сучасних загроз

У сучасних умовах розвитку інформаційного суспільства та зростання кількості кіберзагроз питання забезпечення кібербезпеки в Україні набуває особливої актуальності. Незважаючи на формування нормативно-правової бази та створення відповідних інституцій, у цій сфері залишається низка суттєвих проблем, які потребують комплексного вирішення. До основних із них належать технологічні виклики, недосконаліть правового регулювання, а також проблеми кадрового та інституційного забезпечення.

Однією з ключових проблем у сфері кібербезпеки є зростання технологічних викликів, що супроводжують розвиток цифрових технологій. Сучасні інформаційні системи стають дедалі складнішими, що водночас підвищує їх функціональні можливості та створює нові вразливості. Використання застарілого програмного забезпечення, недостатній рівень захисту мереж, а також відсутність належного моніторингу кіберінцидентів сприяють підвищенню ризику успішних кібератак [15, с. 78].

Особливу небезпеку становить вразливість об’єктів критичної інфраструктури, які активно інтегрують цифрові технології. Атаки на енергетичні системи, транспорт або банківський сектор можуть мати масштабні наслідки для держави. Крім того, швидкий розвиток таких технологій, як штучний інтелект, Інтернет речей (IoT) та хмарні сервіси, створює нові ризики, які потребують адекватного реагування з боку держави.

Незважаючи на наявність законодавчої бази у сфері кібербезпеки, вона залишається недостатньо системною та адаптованою до сучасних викликів. Однією з проблем є фрагментарність правового регулювання, що проявляється

у наявності численних нормативно-правових актів, які не завжди узгоджені між собою [16, с. 102].

Крім того, законодавство часто не встигає за стрімким розвитком технологій, що призводить до виникнення правових прогалин. Наприклад, недостатньо врегульованими залишаються питання відповідальності за окремі види кіберзлочинів, захисту критичної інформаційної інфраструктури, а також механізмів реагування на кіберінциденти. Це ускладнює ефективну діяльність правоохоронних органів та інших суб’єктів кібербезпеки.

Важливою проблемою є також недостатній рівень гармонізації національного законодавства з міжнародними стандартами, що ускладнює міжнародне співробітництво у сфері кібербезпеки та боротьби з кіберзлочинністю.

Не менш важливим викликом є недостатній рівень кадрового забезпечення у сфері кібербезпеки. В Україні спостерігається дефіцит кваліфікованих фахівців, здатних ефективно протидіяти сучасним кіберзагрозам. Це пов’язано як із недостатнім рівнем підготовки спеціалістів, так і з відтоком кадрів до приватного сектору або за кордон, де умови праці є більш привабливими [17, с. 64].

Інституційні проблеми також негативно впливають на ефективність забезпечення кібербезпеки. Зокрема, спостерігається недостатня координація між державними органами, дублювання повноважень та відсутність єдиного центру управління кібербезпекою. Це ускладнює оперативне реагування на кіберзагрози та знижує ефективність державної політики у цій сфері.

Крім того, обмеженість фінансових ресурсів та недостатній рівень технічного забезпечення державних органів стримують розвиток національної системи кібербезпеки. В умовах постійного зростання кількості та складності кіберзагроз це створює додаткові ризики для національної безпеки.

Таким чином, актуальні проблеми забезпечення кібербезпеки в Україні мають комплексний характер і охоплюють технологічні, правові та організаційні аспекти. Їх вирішення потребує системного підходу, спрямованого на вдосконалення законодавства, розвиток кадрового потенціалу та підвищення ефективності функціонування інституцій у сфері кібербезпеки.

3.2. Кібербезпека в умовах війни та гібридних загроз

В умовах сучасних воєнних конфліктів, зокрема повномасштабної агресії проти України, кібербезпека набуває критичного значення як складова національної безпеки. Сучасна війна дедалі більше виходить за межі традиційних бойових дій, охоплюючи інформаційний та кіберпростір. Саме тому кіберзагрози стають важливим інструментом ведення гібридної війни, спрямованої на дестабілізацію держави, підрив її обороноздатності та вплив на суспільну свідомість.

У сучасній науковій та політичній доктрині гібридна війна розглядається як поєднання військових, інформаційних, економічних та кібернетичних засобів впливу. Кібератаки є одним із ключових інструментів такої війни, оскільки дозволяють здійснювати вплив на державу без прямого застосування військової сили. Вони можуть бути спрямовані на державні інформаційні ресурси, системи управління, фінансові установи, засоби масової інформації та інші об’єкти.

Особливістю кібератак у контексті гібридної війни є їх цілеспрямований та системний характер. Вони часто координуються на державному рівні та поєднуються з іншими формами впливу, такими як інформаційні кампанії чи економічний тиск. Наприклад, масовані атаки на урядові сайти або банківські

системи можуть супроводжуватися поширенням панічних настроїв серед населення через соціальні мережі.

Кібератаки дозволяють досягати значного ефекту при відносно невеликих витратах, що робить їх привабливими для держав-агресорів. Вони можуть призводити до порушення функціонування державних інституцій, втрати контролю над інформаційними системами, витоку конфіденційної інформації та дестабілізації економіки [18, с. 91].

Особливо небезпечними є атаки на об’єкти критичної інфраструктури, які можуть спричинити перебої у постачанні електроенергії, води, зв’язку або транспортних послуг. У контексті війни такі атаки можуть мати катастрофічні наслідки та значно ускладнювати функціонування держави.

Критична інформаційна інфраструктура є одним із ключових об’єктів кіберзахисту в умовах війни. До неї належать інформаційні системи та мережі, які забезпечують функціонування життєво важливих сфер, таких як енергетика, транспорт, охорона здоров’я, фінанси, оборона та державне управління.

У воєнний період ці об’єкти стають першочерговими цілями для кібератак, оскільки їх виведення з ладу може призвести до серйозних наслідків для держави та населення. Саме тому захист критичної інфраструктури набуває стратегічного значення та потребує комплексного підходу.

Основними напрямами забезпечення захисту є впровадження сучасних технічних засобів кіберзахисту, проведення регулярного аудиту безпеки, створення резервних систем та каналів зв’язку, а також розробка планів реагування на кіберінциденти. Важливим є також підвищення рівня підготовки персоналу, який відповідає за експлуатацію таких систем.

У науковій літературі підкреслюється, що ефективний захист критичної інфраструктури можливий лише за умови тісної взаємодії між державними

органами та приватним сектором, оскільки значна частина таких об’єктів перебуває у приватній власності [19, с. 143]. Це зумовлює необхідність створення єдиної системи координації та обміну інформацією про кіберзагрози.

Крім того, важливу роль відіграє міжнародне співробітництво, зокрема обмін досвідом, участь у спільних кібернавчаннях та використання міжнародних стандартів у сфері кіберзахисту. В умовах війни це дозволяє підвищити ефективність протидії кіберзагрозам та забезпечити стійкість державної інфраструктури.

Однією з важливих складових гібридної війни є інформаційно-психологічні операції, які активно реалізуються через кіберпростір. Сучасні цифрові технології, соціальні мережі та онлайн-платформи створюють широкі можливості для впливу на свідомість населення, формування громадської думки та поширення дезінформації.

Інформаційно-психологічні операції спрямовані на досягнення стратегічних цілей шляхом маніпуляції інформацією. Вони можуть включати поширення фейкових новин, пропаганду, дискредитацію державних органів, підрив довіри до влади, а також створення панічних настроїв у суспільстві. У цьому контексті кіберпростір виступає як основне середовище реалізації таких операцій.

Особливістю таких впливів є їх прихований характер та складність ідентифікації джерела. Часто вони здійснюються через анонімні акаунти, бот-мережі або підконтрольні інформаційні ресурси. Це ускладнює протидію та потребує використання спеціалізованих методів аналізу інформаційного простору.

Науковці зазначають, що інформаційно-психологічні операції можуть мати не менш серйозні наслідки, ніж традиційні військові дії, оскільки вони

впливають на моральний стан населення, рівень довіри до державних інституцій та соціальну стабільність [20, с. 67]. У поєднанні з кібератаками такі операції створюють потужний інструмент дестабілізації держави.

Протидія інформаційно-психологічним загрозам потребує комплексного підходу, який включає розвиток стратегічних комунікацій, підвищення рівня медіаграмотності населення, вдосконалення законодавства у сфері інформаційної безпеки та створення ефективних механізмів виявлення та блокування дезінформації.

Таким чином, у сучасних умовах війни кібербезпека стає невід'ємною складовою національної безпеки, а кіберпростір — одним із ключових полів протиборства. Поєднання кібератак, впливу на критичну інфраструктуру та інформаційно-психологічних операцій формує комплекс загроз, що потребують системного та багаторівневого реагування з боку держави.

3.3. Напрями вдосконалення системи кібербезпеки в Україні

Сучасний стан розвитку кіберпростору, зростання кількості кіберінцидентів, посилення воєнних і гібридних загроз, а також швидка цифровізація публічного управління, економіки та соціальної сфери зумовлюють необхідність подальшого вдосконалення системи кібербезпеки в Україні. Якщо на попередніх етапах основна увага зосереджувалася переважно на формуванні базових правових та інституційних засад кіберзахисту, то нині першочергового значення набуває питання підвищення ефективності всієї національної системи кібербезпеки. Йдеться вже не лише про реагування на окремі загрози, а про побудову цілісної, стійкої та адаптивної системи, здатної функціонувати в умовах тривалого воєнного навантаження, технологічних змін і постійної трансформації характеру загроз [21].

Удосконалення системи кібербезпеки України повинно відбуватися у кількох взаємопов’язаних напрямах. По-перше, необхідним є оновлення та систематизація законодавчого регулювання у сфері кібербезпеки. По-друге, потребує подальшого розвитку національна система кіберзахисту, включаючи її інституційні, технічні та міжнародні компоненти. По-третє, особливого значення набуває питання формування належного кадрового потенціалу, розвитку кіберграмотності населення та підготовки фахівців, здатних ефективно діяти в умовах сучасних кіберризиків. Саме поєднання цих напрямів дає можливість сформувати в Україні не фрагментарну модель реагування, а повноцінну систему кіберстійкості [21; 22; 23].

Одним із ключових напрямів удосконалення системи кібербезпеки в Україні є подальший розвиток законодавчого регулювання. Незважаючи на наявність базових нормативно-правових актів, чинна модель правового забезпечення все ще зберігає ознаки фрагментарності. Окремі питання врегульовані на рівні спеціальних законів, стратегічних документів, підзаконних актів і відомчих нормативів, однак між ними не завжди забезпечується належна узгодженість. У результаті виникає ситуація, коли окремі елементи національної системи кібербезпеки розвиваються нерівномірно, а правозастосовна практика стикається з проблемами тлумачення компетенції органів, розмежування повноважень і визначення процедур реагування на кіберінциденти [21].

Законодавче вдосконалення має здійснюватися не шляхом механічного збільшення кількості нормативних актів, а через формування внутрішньо узгодженої системи правового регулювання. Насамперед доцільним є чіткіше визначення понятійного апарату. На практиці такі категорії, як «кібербезпека», «кіберзахист», «кіберстійкість», «кіберінцидент», «критична інформаційна інфраструктура», «управління кіберризиками», нерідко використовуються в

різних актах без достатньої термінологічної єдності. Це ускладнює і нормотворчу діяльність, і практичну реалізацію відповідних правових приписів. Тому одним із пріоритетів має бути уніфікація базових понять, що створить необхідне підґрунтя для подальшої систематизації законодавства.

Крім того, важливою є деталізація процедурних механізмів у сфері кібербезпеки. Законодавство повинно не лише проголошувати загальні принципи та напрями державної політики, а й чітко визначати порядок обміну інформацією про кіберінциденти, механізми міжвідомчої координації, правила взаємодії з приватними суб'єктами, стандарти реагування на атаки та порядок відновлення функціонування систем після інцидентів. Особливої уваги потребують питання юридичної відповідальності за порушення вимог кібербезпеки, зокрема у сферах обслуговування інформаційних систем, захисту державних ресурсів і функціонування об'єктів критичної інфраструктури.

Ще одним напрямом є гармонізація українського законодавства з міжнародними та європейськими підходами. З огляду на стратегічний курс України на інтеграцію до європейського правового простору, національне регулювання має розвиватися з урахуванням сучасних міжнародних стандартів у сфері управління кіберризиками, обміну інформацією про загрози, захисту мережевих та інформаційних систем і забезпечення кіберстійкості. Це важливо не лише для формального зближення правових систем, а й для практичного підвищення ефективності української моделі кібербезпеки, оскільки більшість кіберзагроз сьогодні мають транснаціональний характер.

Важливим орієнтиром у цьому контексті виступає Стратегія кібербезпеки України, яка прямо визначає посилення спроможностей національної системи кібербезпеки як один із пріоритетів державної політики

[21]. Саме тому вдосконалення законодавства має розглядатися не як ізольований правотворчий процес, а як інструмент реалізації довгострокової стратегії держави у сфері безпеки. При цьому особливу увагу слід приділити правовому регулюванню захисту державних електронних інформаційних ресурсів, цифрових публічних послуг, хмарних рішень, засобів електронної ідентифікації та систем, що використовуються в секторі безпеки й оборони.

Не менш важливо, щоб законодавче оновлення базувалося на принципі технологічної нейтральності. Умови функціонування кіберпростору змінюються настільки швидко, що надмірно деталізовані технічні норми швидко застарівають. Саме тому законодавство повинно закріплювати, передусім, загальні принципи, вимоги до стійкості, відповідальності та управління ризиками, залишаючи технічні деталі для стандартів, методик і галузевих регламентів, які можна оновлювати оперативніше. Такий підхід дозволить уникнути постійного відставання правового регулювання від технологічного розвитку.

Отже, удосконалення законодавчого регулювання у сфері кібербезпеки має бути спрямоване на подолання фрагментарності правової бази, уніфікацію понятійного апарату, деталізацію процедур реагування, гармонізацію із міжнародними підходами та закріплення правових механізмів кіберстійкості. Саме послідовна модернізація нормативної основи дозволить створити більш передбачуване, ефективне та стабільне правове середовище для функціонування всієї системи кібербезпеки в Україні.

Другим стратегічним напрямом є розвиток національної системи кіберзахисту як сукупності інституційних, організаційних, технічних та інформаційно-аналітичних механізмів, спрямованих на попередження, виявлення, локалізацію та нейтралізацію кіберзагроз. У сучасних умовах уже недостатньо мати лише окремі уповноважені органи чи формально визначені

повноваження. Потрібна цілісна система, в якій усі елементи діють узгоджено, швидко обмінюються інформацією та здатні працювати в режимі підвищеного навантаження, особливо в умовах воєнного стану та постійних гібридних загроз [21].

Розвиток такої системи передбачає насамперед зміцнення інституційної спроможності суб'єктів кібербезпеки. Йдеться не лише про збільшення кількості структур чи розширення їх формальних компетенцій, а про підвищення ефективності координації між ними. Для цього необхідно вдосконалити механізми стратегічного планування, оперативного управління інцидентами, міжвідомчої комунікації та аналізу кіберзагроз. Особливого значення набуває запровадження єдиного підходу до оцінки ризиків, класифікації інцидентів та визначення пріоритетності реагування. За відсутності такої узгодженості навіть технічно потужні структури можуть діяти несинхронно, що послаблює загальну стійкість системи.

Національна система кіберзахисту повинна будуватися на засадах проактивності. Це означає, що головний акцент має переноситися з реагування на вже реалізовані атаки на прогнозування ризиків, раннє виявлення ознак втручання, моделювання загроз та формування сценаріїв дій у кризових ситуаціях. Для цього необхідні сучасні центри моніторингу, механізми оперативного збору та обробки даних, резервні канали зв'язку, системи швидкого відновлення та постійне оновлення засобів захисту. Умови війни продемонстрували, що кіберзахист не може бути епізодичним або суто відомчим завданням; він має функціонувати як безперервний процес.

Окремим складником розвитку національної системи кіберзахисту є посилення кіберстійкості критичної інфраструктури. Саме вразливість енергетики, зв'язку, транспортних систем, фінансового сектору, медичних інформаційних систем і державних реєстрів найчастіше створює найбільші

ризики для національної безпеки. Тому перспективним є впровадження ризик-орієнтованого підходу, за якого захист будується залежно від критичності об’єкта, ймовірності загрози та масштабу потенційних наслідків. У цьому контексті доцільно запроваджувати обов’язкові вимоги щодо резервування, тестування безперервності діяльності, оцінки вразливостей і проведення регулярних кібернавчань.

Не менш важливою є взаємодія держави з приватним сектором. Значна частина цифрової інфраструктури, сервісів зберігання даних, телекомунікаційних мереж і технологічних платформ перебуває саме у сфері приватного управління. Відтак розвиток національної системи кіберзахисту без сталого публічно-приватного партнерства є практично неможливим. Ефективна модель співпраці має охоплювати обмін інформацією про інциденти, вироблення спільних стандартів безпеки, участь у галузевих тренуваннях, спільне оцінювання ризиків та координацію в кризових умовах. Особливо актуально це для секторів, які забезпечують базові потреби населення та стабільність державного управління.

Розвиток національної системи кіберзахисту тісно пов’язаний і з міжнародною співпрацею. Транснаціональна природа кіберзагроз зумовлює те, що жодна держава не може ефективно забезпечувати кібербезпеку винятково власними силами. Більшість складних атак використовують розподілену інфраструктуру, міжнародні ланцюги постачання програмного забезпечення, іноземні майданчики поширення шкідливого коду та багаторівневі схеми приховування джерела. Саме тому міжнародний обмін інформацією, координація реагування, участь у спільних ініціативах та інтеграція в мережі колективної безпеки мають ключове значення для України [21].

У цьому аспекті важливими є не лише міждержавні домовленості, а й участь України в системах практичної взаємодії: міжнародних кібернавчаннях, професійних мережах реагування, експертних платформах, спільних програмах з технічної допомоги та освітніх проєктах. Міжнародна співпраця сприяє доступу до передових методик, сучасних технологій, аналітичних рішень і практик побудови кіберстійкості. Крім того, вона дозволяє швидше адаптувати національні механізми до вимог безпекового середовища, яке стрімко змінюється.

Показово, що офіційні документи України в інформаційній сфері прямо пов’язують безпеку держави із необхідністю протидії актуальним викликам і загрозам, а також із формуванням системних спроможностей для захисту національних інтересів [22]. Це дає підстави стверджувати, що міжнародна співпраця у сфері кібербезпеки повинна розглядатися не як додатковий напрям, а як один із базових елементів сучасної безпекової політики держави.

Отже, розвиток національної системи кіберзахисту та міжнародної співпраці має відбуватися шляхом зміцнення інституційної спроможності, удосконалення координації, впровадження проактивних механізмів реагування, посилення захисту критичної інфраструктури, розвитку публічно-приватного партнерства та активного залучення України до міжнародних безпекових ініціатив. Лише за таких умов національна система кібербезпеки зможе відповідати масштабу сучасних викликів.

Окремим і надзвичайно важливим напрямом удосконалення системи кібербезпеки в Україні є підвищення рівня кіберграмотності населення та розвиток системи професійної підготовки фахівців. У сучасних умовах навіть технічно досконалі засоби кіберзахисту не можуть забезпечити належного рівня безпеки, якщо користувачі не володіють базовими навичками цифрової обережності, а держава не має достатньої кількості кваліфікованих

спеціалістів. Значна частина кіберінцидентів пов’язана саме з людським фактором: використанням слабких паролів, недотриманням правил роботи з електронною поштою, ігноруванням оновлень безпеки, необережним поводженням з персональними даними, недостатньою здатністю розпізнавати фішингові повідомлення та інформаційні маніпуляції. Тому кіберграмотність потрібно розглядати не як факультативну навичку, а як необхідний елемент сучасної безпеки особи, суспільства і держави [22].

Підвищення кіберграмотності має охоплювати всі рівні суспільства. Передусім ідеться про широкі інформаційно-освітні заходи для населення, спрямовані на формування базових навичок безпечної поведінки в цифровому середовищі. Це включає роз’яснення основ захисту персональних даних, правил безпечного користування електронними сервісами, механізмів перевірки інформації, способів протидії соціальній інженерії та дезінформації. У сучасних умовах цифрові компетентності безпосередньо пов’язані не лише з індивідуальною безпекою користувача, а й із загальною стійкістю суспільства до кіберзагроз та інформаційно-психологічних впливів.

Особливу роль у формуванні кіберграмотності відіграє система освіти. Необхідно послідовно інтегрувати елементи цифрової безпеки в освітній процес на різних рівнях — від загальної середньої освіти до вищої та післядипломної підготовки. Для школярів доцільним є формування базових моделей безпечної поведінки в інтернеті, навичок критичного сприйняття інформації та розуміння основ цифрової приватності. Для студентів немовних, нетехнічних і непрофільних спеціальностей важливо забезпечити мінімально необхідний рівень знань із цифрової безпеки, оскільки практично будь-яка професійна діяльність сьогодні пов’язана з використанням електронних систем.

Щодо професійної підготовки фахівців, то тут мова повинна йти про побудову цілісної освітньої екосистеми у сфері кібербезпеки. Вона має охоплювати фундаментальну підготовку у закладах вищої освіти, спеціалізовану практичну підготовку, безперервне професійне навчання, перепідготовку та підвищення кваліфікації. Важливим кроком у цьому напрямі є наявність затверджених стандартів вищої освіти за спеціальністю 125 «Кібербезпека» для різних рівнів підготовки, зокрема бакалаврського і магістерського, що формує єдину рамку компетентностей і результатів навчання [23].

Водночас сам факт наявності стандартів не означає автоматичного вирішення проблеми кадрового дефіциту. Підготовка фахівців у сфері кібербезпеки повинна відповідати реальним потребам держави, сектору безпеки й оборони, критичної інфраструктури та приватного бізнесу. Це означає, що освітні програми мають бути орієнтовані не лише на теоретичне засвоєння матеріалу, а й на розвиток практичних навичок: аналіз кіберінцидентів, управління ризиками, роботу з мережевою інфраструктурою, реагування на атаки, цифрову криміналістику, захист інформаційних систем, безпеку програмного забезпечення та розуміння правових аспектів кібербезпеки. Не менш важливо забезпечити міждисциплінарність підготовки, оскільки сучасний фахівець із кібербезпеки має поєднувати технічні знання з правовою, аналітичною та управлінською компетентністю.

Перспективним напрямом є тісніше поєднання освітнього процесу з практикою. Йдеться про залучення роботодавців до формування освітніх програм, розширення баз практики, створення кіберлабораторій, участь студентів у моделюванні кіберінцидентів, проведенні навчальних кіберполігонів, конкурсів, стажувань і дослідницьких проєктів. Умови війни показали, що підготовка фахівця повинна бути максимально прикладною,

оскільки від здатності швидко аналізувати інцидент і приймати рішення часто залежить стійкість цілих систем.

Окремого значення набуває підвищення кваліфікації працівників державного сектору. Значна кількість службовців, які працюють із державними реєстрами, електронним документообігом, цифровими сервісами та інформаційними системами, не є професійними кіберфахівцями, однак саме їхні дії часто визначають рівень захищеності установи. Тому системна підготовка має охоплювати не лише вузькопрофільних спеціалістів, а й державних службовців, посадових осіб місцевого самоврядування, працівників судової системи, правоохоронних органів, освітніх і медичних закладів. Для цієї категорії особливо важливими є короткострокові програми, тренінги, модулі з інформаційної гігієни та сценарії реагування на інциденти.

Крім того, формування кадрового потенціалу потребує вирішення низки системних проблем: конкуренції державного і приватного секторів за кваліфікованих фахівців, недостатнього фінансування освітньої та дослідницької інфраструктури, обмежених можливостей для прикладної підготовки, нерівномірного розвитку освітніх програм у різних регіонах. Саме тому державна політика в цій сфері має включати не лише затвердження стандартів, а й підтримку дослідницьких центрів, розвиток академічної та професійної мобільності, стимулювання наукових досліджень у сфері кібербезпеки, а також створення привабливих умов для роботи фахівців у державному секторі.

У ширшому значенні кіберграмотність і підготовка кадрів є елементами національної кіберстійкості. Стійкість держави визначається не лише наявністю програмно-технічних засобів захисту, а й тим, наскільки суспільство в цілому здатне відповідально функціонувати в цифровому середовищі, а професійна спільнота — забезпечувати захист на належному

рівні. Тому інвестиції в освіту, підготовку фахівців, професійний розвиток і просвітницькі програми мають розглядатися як інвестиції у національну безпеку.

Таким чином, підвищення рівня кіберграмотності та підготовка фахівців є одним із базових напрямів удосконалення системи кібербезпеки в Україні. Реалізація цього напряму передбачає розвиток масової цифрової просвіти, інтеграцію питань кібербезпеки в освітній процес, удосконалення стандартів і програм професійної підготовки, посилення практичної складової навчання, підвищення кваліфікації працівників державного сектору та формування довгострокової кадрової політики у сфері кіберзахисту. Саме за таких умов Україна зможе не лише реагувати на сучасні кіберзагрози, а й системно зміцнювати власну кіберстійкість.

ВИСНОВКИ

У результаті проведеного дослідження теоретико-правових основ кібербезпеки як елемента національної безпеки, а також аналізу сучасного стану її нормативно-правового забезпечення та практичних аспектів функціонування в Україні, можна сформулювати низку узагальнюючих висновків.

По-перше, встановлено, що кібербезпека є складною, багатовимірною категорією, яка поєднує правові, технічні, організаційні та соціальні елементи. У правовому аспекті вона визначається як стан захищеності життєво важливих інтересів людини, суспільства та держави у кіберпросторі, тоді як у науковій доктрині розглядається також як процес і система заходів, спрямованих на запобігання, виявлення та нейтралізацію кіберзагроз. Таким чином, кібербезпека виступає не лише результатом, а й безперервною діяльністю, що забезпечує стійкість функціонування інформаційного середовища.

По-друге, доведено, що кібербезпека є невід'ємною складовою національної безпеки держави. В умовах цифровізації суспільства та розвитку інформаційних технологій вона безпосередньо впливає на політичну стабільність, економічну безпеку, обороноздатність і соціальну стійкість держави. Кіберзагрози здатні порушувати функціонування органів державної влади, дестабілізувати економічні процеси та впливати на суспільну свідомість, що обумовлює їх високий рівень небезпеки.

По-третє, встановлено, що сучасні кіберзагрози мають комплексний, динамічний і транснаціональний характер. Вони включають широкий спектр впливів — від технічних атак на інформаційні системи до інформаційно-психологічних операцій. Особливу небезпеку становлять кібератаки на об'єкти критичної інфраструктури, а також використання кіберпростору як

інструменту гібридної війни. Вплив таких загроз поширюється на всі сфери суспільного життя, включаючи державне управління, економіку та соціальні процеси.

По-четверте, проаналізовано національне законодавство України у сфері кібербезпеки, яке характеризується наявністю базових нормативно-правових актів, проте зберігає певні ознаки фрагментарності. Незважаючи на створення правової основи для функціонування системи кібербезпеки, існує потреба у її подальшій систематизації, удосконаленні та гармонізації з міжнародними стандартами. Важливу роль у цьому процесі відіграють міжнародно-правові документи та досвід інших держав, які сприяють формуванню сучасних підходів до забезпечення кібербезпеки.

По-п’яте, встановлено, що ефективність забезпечення кібербезпеки значною мірою залежить від функціонування системи державних органів та їх взаємодії з приватним сектором. Сучасна модель кіберзахисту передбачає активне залучення суб’єктів господарювання, які володіють значною частиною інформаційної інфраструктури, а також розвиток публічно-приватного партнерства. Водночас існують проблеми координації, розмежування повноважень та обміну інформацією між суб’єктами, що потребує подальшого вдосконалення.

По-шосте, у роботі визначено ключові проблеми забезпечення кібербезпеки в Україні, серед яких: технологічна вразливість інформаційних систем, недосконалість нормативно-правового регулювання, дефіцит кваліфікованих кадрів та інституційні недоліки. Ці проблеми мають системний характер і взаємопов’язані між собою, що ускладнює їх вирішення та потребує комплексного підходу.

По-сьоме, доведено, що в умовах війни кібербезпека набуває стратегічного значення як складова гібридного протиборства. Кібератаки,

інформаційно-психологічні операції та вплив на критичну інфраструктуру використовуються як інструменти дестабілізації держави. Це обумовлює необхідність підвищення рівня кіберстійкості, розвитку системи реагування на кіберінциденти та посилення міжнародної співпраці.

По-восьме, обґрунтовано основні напрями вдосконалення системи кібербезпеки в Україні. До них належать: удосконалення законодавчого регулювання, розвиток національної системи кіберзахисту, розширення міжнародної співпраці, підвищення рівня кіберграмотності населення та формування кадрового потенціалу. Реалізація цих напрямів дозволить підвищити ефективність функціонування системи кібербезпеки та забезпечити належний рівень захисту національних інтересів.

Таким чином, кібербезпека в сучасних умовах виступає ключовим елементом національної безпеки України, а її забезпечення є комплексним завданням, що потребує узгоджених дій держави, суспільства та приватного сектору. Подальший розвиток системи кібербезпеки має ґрунтуватися на принципах системності, адаптивності, міжнародної інтеграції та орієнтації на сучасні виклики цифрового середовища.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 11.03.2026).

2. Про національну безпеку України: Закон України від 21.06.2018 № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19 (дата звернення: 11.03.2026).

3. Литвиненко О. В. Національна безпека України: навчальний посібник. Київ: Центр навчальної літератури, 2020. 304 с.

4. Дубов Д. В. Кібербезпека: світові тенденції та виклики для України: монографія. Київ: НІСД, 2019. 312 с.

5. Гнатюк С. О. Кібербезпека в Україні: правові та організаційні засади: монографія. Київ: НАУ, 2021. 256 с.

6. Ткачук Т. Ю. Основи кібербезпеки: навчальний посібник. Київ: КПІ ім. Ігоря Сікорського, 2020. 220 с.

7. Коваленко В. В. Кібербезпека в системі національної безпеки України: теоретико-правові аспекти: монографія. Харків: Право, 2021. 320 с.

8. Конституція України: Закон України від 28.06.1996 № 254к/96-ВР (зі змінами). Київ: Відомості Верховної Ради України, 1996. 141 с.

9. Про інформацію: Закон України від 02.10.1992 № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12 (дата звернення: 13.03.2026).

10. Конвенція Ради Європи про кіберзлочинність (Будапештська конвенція) від 23.11.2001. URL: https://zakon.rada.gov.ua/laws/show/994_575 (дата звернення: 14.03.2026).

11. Directive (EU) 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and

information systems across the Union. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L1148 (дата звернення: 13.034.2026).

12. Марущак А. І. Міжнародне співробітництво у сфері кібербезпеки: правові аспекти: монографія. Київ: Юрінком Інтер, 2021. 280 с.

13. Шеломенцев В. П. Державне управління у сфері кібербезпеки: теоретико-правові засади: монографія. Київ: Національна академія державного управління при Президентові України, 2020. 280 с.

14. Пилипчук В. Г. Публічно-приватне партнерство у сфері кібербезпеки: теоретико-правові засади: монографія. Київ: Юрінком Інтер, 2021. 240 с.

15. Корченко О. Г. Основи кібербезпеки: монографія. Київ: НАУ, 2019. 300 с.

16. Радзієвська О. Г. Правове забезпечення кібербезпеки в Україні: сучасний стан та перспективи розвитку: монографія. Київ: Юрінком Інтер, 2020. 260 с.

17. Баранов О. А. Кібербезпека в Україні: проблеми та перспективи розвитку: наукова доповідь. Київ: НІСД, 2021. 120 с.

18. Горбулін В. П. Світова гібридна війна: український фронт: монографія. Київ: НІСД, 2017. 496 с.

19. Козюра В. Д. Захист критичної інфраструктури в умовах гібридних загроз: монографія. Київ: НУОУ ім. Івана Черняховського, 2021. 280 с.

20. Почепцов Г. Г. Інформаційні війни: теорія і практика: монографія. Київ: Києво-Могилянська академія, 2015. 312 с.

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

України від 26.08.2021 № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021 (дата звернення: 16.03.2026).

22. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки»: Указ Президента України від 28.12.2021 № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021 (дата звернення: 17.03.2026).

23. Затверджені стандарти вищої освіти. Спеціальність 125 «Кібербезпека»: офіційна сторінка Міністерства освіти і науки України. URL: https://mon.gov.ua/osvita-2/vishcha-osvita-ta-osvita-doroslikh/naukovo-metodichna-rada-ministerstva-osviti-i-nauki-ukraini/zatverdzheni-standarti-vishchoi-osviti (дата звернення: 18.03.2026).