Ящук Валентина Ігорівна кандидат економічних наук, доцент кафедри управління інформаційною безпекою, Львівський державний університет безпеки життєдіяльності, Клепарівська, 35, Львів, 79007, тел.: +38 (032) 233-24-79, e-mail:valentina.lender@gmail.com, https // orcid.org / 0000-0003-2651-4918, Researcher ID: F-9466-2019.

РОЛЬ ТА МІСЦЕ СТРАТЕГІЇ КІБЕРБЕЗПЕКИ УКРАЇНИ У ЗАБЕЗПЕЧЕННІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

Вступ. У сучасному світі інформаційна безпека держави стає одним із ключових чинників її стійкості та розвитку. Кіберзагрози, такі як кібератаки, кібершпигунство, кібертероризм, кіберсаботаж, дезінформація, постійно зростають, що робить необхідним розробку та впровадження ефективної стратегії кібербезпеки. Україна, як і інші країни світу, стикається з численними кіберінцидентами, які можуть мати значний вплив на її економіку, політику та суспільство.

Інформаційна безпека є одним із ключових факторів стійкості та розвитку держави. Кібербезпека є невід'ємною складовою інформаційної безпеки. У сучасному світі кіберзлочинність та кібератаки постійно зростають за масштабами та складністю. Україна перебуває у складному геополітичному середовищі, що може сприяти кібератакам та іншим формам цифрової агресії з боку інших країн.

Війна на сході України, яка розпочалась у 2014 році, стала складним гібридним конфліктом, включаючи збройні дії, інформаційну війну та кіберагресію. Військові події на сході України, зокрема в Донецькій та Луганській областях, супроводжувалися активними кібератаками та інформаційною війною.

В умовах цього конфлікту в контексті стратегії кібербезпеки Україна приділяла значну увагу захисту своїх критичних інформаційних

інфраструктур та протидії кіберзагрозам. Ключові аспекти такої стратегії включали захист критичних інфраструктур, розвиток кіберзахисту, інформаційну безпеку, міжнародне співробітництво, експертну та освітню роботу. Зусилля зосереджувались на захисті критичних об'єктів, таких як енергетичні системи, телекомунікаційні мережі, фінансові установи тощо від кібератак. Створювались та вдосконалювались систем кіберзахисту, які включають в себе розробку захисного програмного забезпечення, моніторинг та реагування на кіберінциденти. Проводилась робота із запобіганню дезінформації та пропаганді, яка може посилити дестабілізацію суспільства та підірвати довіру до державних інституцій. Відбувалось посилення взаємодії з міжнародними партнерами та організаціями з метою обміну інформацією та кращого реагування на кіберзагрози. Проводились заходи із підвищення рівня кіберграмотності населення та професіоналів у сфері кібербезпеки, щоб покращити виявлення та реагування на кіберзагрози.

Україна активно переходить до цифрової економіки, що робить її ще більш уразливою перед кіберзагрозами. Збільшення кількості підключених до Інтернету пристроїв і послуг також збільшує потенційні точки вразливості. Нові технології, такі як штучний інтелект, Інтернет речей (IoT), блокчейн тощо, принесли не лише нові можливості, але й нові загрози для кібербезпеки. Втрата довіри до інформаційних систем та ресурсів може призвести до значних економічних та соціальних проблем.

Інформаційні операції та пропаганда в інтернеті стали невід'ємною частиною сучасної гібридної війни. Досвід показує, що з початком повномасштабного вторгнення, правильна стратегія кібербезпеки може визначати інформаційну перевагу. Чинна Стратегія кібербезпеки України затверджена у 2016 році [1]. За цей час ситуація у сфері кібербезпеки значно змінилася, тому виникла потреба у вдосконаленні Стратегії. Впровадження ефективної Стратегії кібербезпеки стає критично важливим завданням для

України, яке має на меті захистити національні інтереси та забезпечити стійкість інформаційної і кібернетичної інфраструктури держави.

Питаннями, які торкаються найрізноманітніших аспектів стратегії кібербезпеки та забезпеченні інформаційної безпеки досліджувались у наукових працях Арістова І. В., Березовської І. Р., Дзьобаня О. П., Калюжного Р. А., Кормича Б. А., Ліпкана В. А., Марущак А. І., Цимбалюка В. С., Юдіна О. К., а також регламентуються численними законами, указами та доктринами [1-14].

Разом з тим, не існує комплексного наукового дослідження, яке б аналізувало роль та місце Стратегії кібербезпеки України у забезпеченні інформаційної безпеки держави. Продовжує залишатись актуальною необхідність у подальших дослідженнях низки питань щодо ефективності реалізації Стратегії через постійний моніторинг її виконання та системи індикаторів стану кібербезпеки. Проблеми, перераховані вище, їхня актуальність обумовили вибір теми дослідження, визначили її мету й завдання.

Метою дослідження є визначення методичних підходів до формування ролі та місця стратегії кібербезпеки України у забезпеченні інформаційної безпеки держави, що є основою захисту національних інтересів та забезпечення стійкості інформаційної і кібернетичної інфраструктури держави в умовах гібридної війни.

Виклад основного матеріалу. Чинна стратегія кібербезпеки України визначає пріоритети, цілі та завдання забезпечення кібербезпеки України з метою створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави [1]. Сьогодні кібербезпека є одним із пріоритетів у системі національної безпеки України. Реалізація зазначеного пріоритету буде здійснюватися шляхом посилення спроможностей національної системи кібербезпеки для протидії кіберзагрозам у сучасному безпековому середовищі. Формуючи нову

Стратегію кібербезпеки України, потрібно враховувати світові тренди в глобальному кіберсередовищі, як фактори впливу на розбудову національної системи кібербезпеки.

У зв'язку з появою нових системних загроз національній безпеці 21 червня 2018 р. було ухвалено новий Закон України «Про національну безпеку України» [2]., який відобразив сучасні безпекові реалії та стратегічні напрямки розвитку сектора безпеки України. Відповідно до п. 9 ч. 1 ст. 1 цього Закону національна безпека — це захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу й інших національних інтересів України від реальних і потенційних загроз. Складові частини національної безпеки наведено на рис. 1.

Рис. 1. Структура національної безпеки України

За вказаними напрямами безпеки здійснюється планування. Документи, що містять довгострокові плани, отримали назву стратегії. Відповідно в законі описуються в загальному вигляді стратегії національної безпеки, воєнної безпеки, громадської безпеки та цивільного захисту України тощо. Окремим нормативним актом затверджено Стратегію кібербезпеки України [1] — документ довгострокового планування, що визначає загрози кібербезпеці України, пріоритети та напрями забезпечення кібербезпеки України з метою створення умов для безпечного

функціонування кіберпростору, його використання в інтересах особи, суспільства і держави [3]. Докладніше структуру вказаного документа наведено на рис. 2.

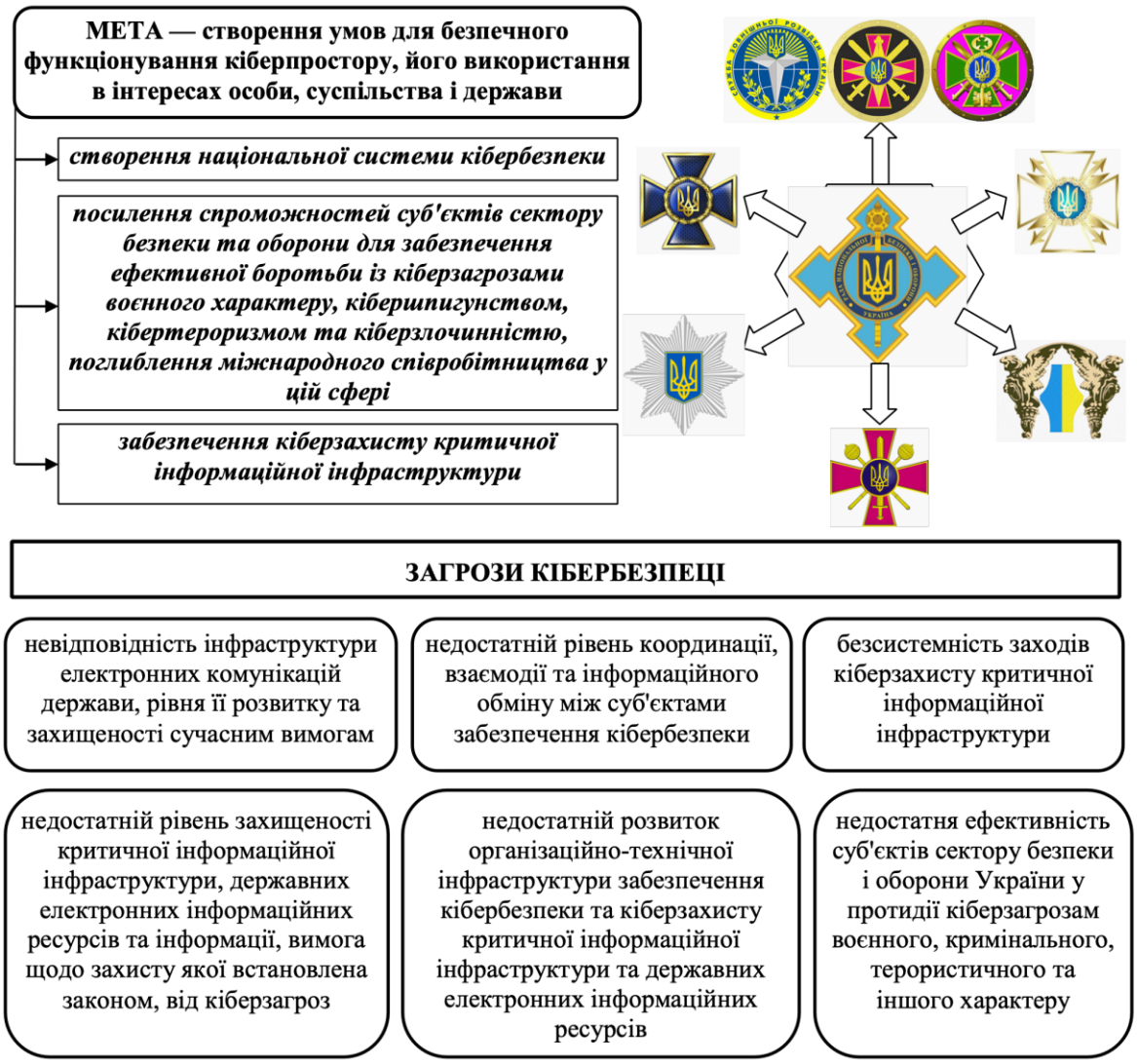

Рис. 2. Основні елементи стратегії кібербезпеки України,

розроблено автором на основі [3].

XXI століття знаменується активним формуванням шостого технологічного укладу (біо-, нано-, інфо-, когнотехнологій, їх конвергенцією) та ризиками, з якими стикається цивілізація внаслідок упровадження новітніх технологій, зокрема їх використання у кіберпросторі.

Питома вага кіберзагроз у сфері загроз національній безпеці країн змінюється, і ця тенденція в процесі розвитку інформаційних технологій та

їх конвергенції з технологіями штучного інтелекту зростає. Посилення такого впливу на функціонування структур управління як національних, так і транснаціональних формує повністю нову безпекову ситуацію з викликами нового технологічного рівня. Міжнародні центри сили зазнають перерозподілу сфер впливу у кіберпросторі, збільшується їх бажання через такий поділ забезпечити втілення власних геополітичних інтересів. Структуру Національної системи забезпечення кібербезпеки у розрізі рівнів управління наведено на рис.3.

Рис. 3. Національна система забезпечення кібербезпеки, *розроблено автором на основі [4].*

Кіберпростір разом з іншими територіями визнано одним з потенційних театрів воєнних дій, тому здатність держави захищати свої національні інтереси в ньому розглядається як важлива складова кібербезпеки. Набирає сили тенденція до створення нового типу військ – кібервійськ, до завдань яких входить не лише забезпечення захисту критичної інформаційної інфраструктури від кібератак, а також проведення превентивних наступальних операцій у кіберпросторі, спрямованих на ураження обчислювальних мереж та інформаційних систем збройних сил

противника, а також виведення з ладу критично важливих об’єктів противника шляхом руйнування інформаційних систем, що керують такими об’єктами.

Водночас все більш і більш активно застосовується поєднання традиційних та нетрадиційних стратегій і тактик з використанням цифрових інформаційних технологій. Зокрема, Російська Федерація ефективно реалізує концепцію інформаційного протиборства, базовану на симбіозі бойових дій у кіберпросторі та інформаційних операцій, механізми якої успішно використовуються в процесі гібридної війни проти України. Країни ЄС, НАТО, провідні міжнародні компанії та експерти одностайно визнають Російську Федерацію і її дії у кіберпросторі головною загрозою міжнародній кібербезпеці. Її розвідувально-підривна діяльність у цифровому просторі є частиною гібридної війни, яку вона проводить проти України. Така деструктивна активність створює реальну загрозу вчинення актів кібертероризму та кібердиверсій стосовно національної інформаційної інфраструктури.

Прогнозується зростання інтенсивності міждержавного протиборства і розвідувально-підривної діяльності у цифровому просторі, що проявлятимуться, насамперед, у розширенні кола країн, які намагатимуться створити власну кіберрозвідку, оволодіти передовими технологіями розвідувально-підривної діяльності у кіберпросторі, посилити державний контроль за національними сегментами мережі Інтернет. При цьому отримуватиме поширення розроблення інструментарію, що передбачає накопичення великих масивів даних щодо поведінки людини, соціальних груп та використання передових досягнень у сфері штучного інтелекту. Негативною ознакою технологічного розвитку, пов’язаного із загальним поширенням цифрових технологій, розширенням Інтернет-середовища, є критично зростаючий технічний рівень інструментарію втілення кіберзагроз, від чого ландшафт таких загроз охоплює все більше сфер

життєдіяльності. Кібератаки, їх різновиди стають все більш інтелектуальними та небезпечними, створюючи реальну загрозу критичній інфраструктурі.

Зловмисники активно працюють над пошуком вразливостей у активах (систем управління) і розробляють для цього унікальні за своїми характеристиками: універсальне шкідливе програмне забезпечення, віруси-шифрувальники, ботнети, які виконують розподілені атаки (DDoS) на операційні мережі, виробничі системи, що використовують хмарні сервіси, а також атаки на ланцюги поставок. З урахуванням прогресу у технологіях штучного інтелекту протягом наступних 5-10 років масштаби та наслідки таких втручань будуть зростати. Розширення використання кіберпростору терористичними організаціями (кібертероризм) стає глобальним трендом. Цьому сприяє загальна цифрова трансформація систем управління та життєзабезпечення, що безперервно розширює кількість об'єктів кібертероризму та потенційних об'єктів кібератак. Об'єктами терористичних кібератак вважаються об'єкти атомної енергетики, системи управління електропостачанням, авіаційний та залізничний транспорт, магазини стратегічних видів сировини, системи водопостачання, а також хімічні й біологічні об'єкти.

Нові виклики приносить перехід на 5G-мережі, робота яких в суттєвій мірі залежить від правильної роботи програмного забезпечення, що через новизну технології може створити нові, не повністю передбачені загрози. Технології «Інтернету речей», «розширеної реальності», «розумних міст» активно доповнюються новими – «гіперавтоматизацією», «розумним компонуванням бізнесу», «кібербезпековою мережею», «розподіленою хмарою», «Інтернет-поведінкою» тощо.

Радикально змінюючи глобальний лад, пандемія коронавірусу COVID-19 матиме тривалий вплив на світовий порядок. Зростає залежність від цифрових засобів спілкування, що ставить під загрозу обмін

інформацією, захист персональних даних. Кіберзлочинці, експлуатуючи пандемію, все більше застосовують нові методи кібератак, що примушує уряди впроваджувати додаткові механізми протидії, забезпечуючи доступ до необхідних пристроїв, функціонування електронних ресурсів і систем. Поширення загроз та ускладнення їх впровадження змушує уряди провідних країн удосконалювати архітектуру національних систем кібербезпеки, змінювати стратегію протидії. Зміни до моделі протидії пов'язані з розумінням неможливості побудувати абсолютно невразливі системи захисту. Практика показує, що будь-які інформаційно-комунікаційні системи можуть бути пошкоджені кібератакою, тому важливо виявляти вразливості та реагувати на них для мінімізації можливих збитків.

Швидкоплинний цифровий світ потребує формування більш збалансованої та ефективної національної системи кібербезпеки, яка зможе гнучко адаптуватися до змін безпекового оточення, забезпечуючи громадянам України безпечне функціонування національного сегмента кіберпростору та створюючи нові можливості для цифровізації всіх сфер суспільного життя. Україна розвивається здатною забезпечити свій соціально-економічний прогрес у цифровому світі, що вимагає здобуття здатності ефективно стримувати деструктивні втручання в кіберпросторі, досягнення кіберстійкості на всіх рівнях та сприяння взаємодії всіх суб'єктів забезпечення кібербезпеки на основі партнерства та співпраці.

Все, викладене вище зумовлює необхідність дослідження засад розбудови національної системи кібербезпеки, відповідно до якої Україна прагне створити максимально відкритий, вільний, стабільний і безпечний кіберпростір, де враховуються права і свободи людини, підтримуються соціальний, політичний і економічний розвиток. На рис. 4 наведено структурну схему взаємодії складників системи кібербезпеки для цифрової держави. В процесі реалізації Стратегії кібербезпеки України за період з 2016 по 2020 роки, державі вдалося сформувати основу

національної системи кібербезпеки. Україна значно розширила свій потенціал, що дозволяє подальшу розбудову національної системи кібербезпеки на основі стримування, кіберстійкості та сприяння взаємодії.

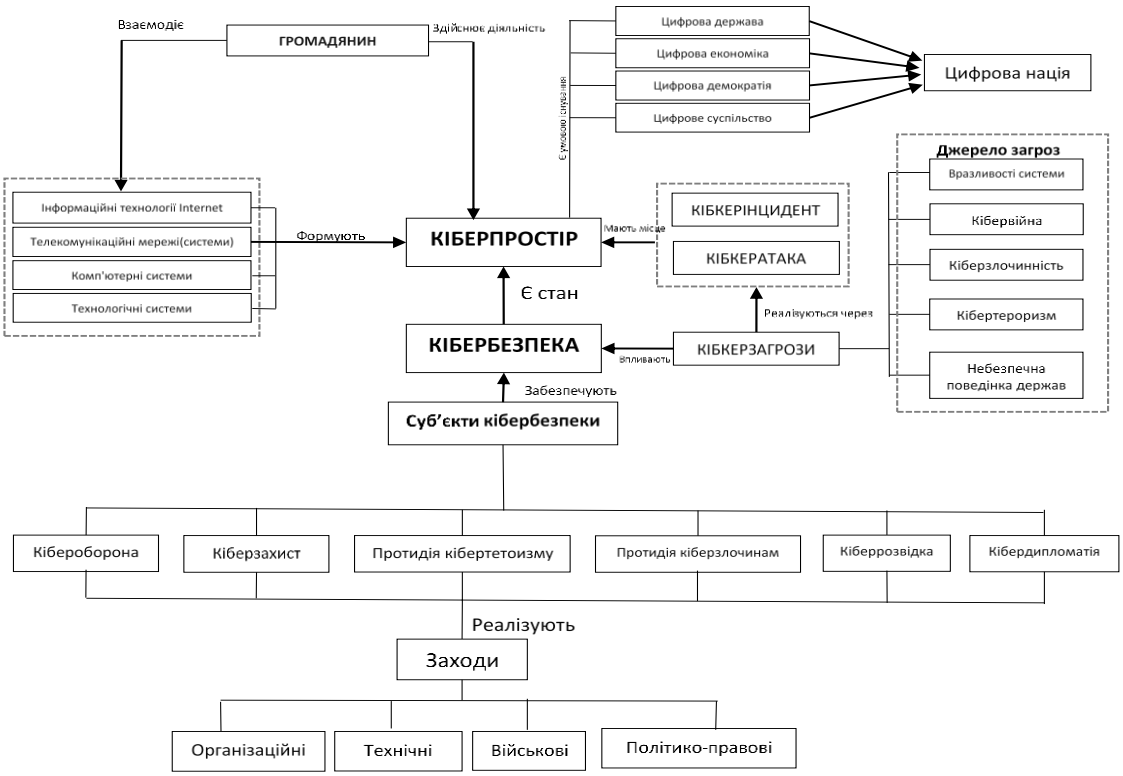

Рис. 4. Кібербезпека для цифрової держави, *розроблено автором на основі [4].*

При розбудові національної системи кібербезпеки на основі стримування, кіберстійкості та сприяння взаємодії в Україні відбулось посилення спроможностей національної системи кібербезпеки для запобігання збройній агресії проти України у кіберпросторі або через нього, нейтралізації розвідувально-підривної діяльності, мінімізації загроз кіберзлочинності та кібертероризму (стримування); набуття здатності швидко адаптуватися до внутрішніх і зовнішніх загроз у кіберпросторі, підтримання стабільного функціонування національної інформаційної інфраструктури, зокрема об'єктів критичної інформаційної інфраструктури (кіберстійкість); забезпечення розвитку комунікації, координації та партнерства між суб'єктами забезпечення кібербезпеки на національному

рівні, розвитку стратегічних відносин у сфері кібербезпеки з ключовими іноземними партнерами, насамперед з Європейським Союзом і НАТО та їх державами-членами, співробітництво у цій сфері з іншими державами та міжнародними організаціями на основі національних інтересів України (взаємодія). Розвиток національної системи кібербезпеки на таких принципах дасть можливість розширити запропоновані та рекомендовані дії на всі галузі економіки та сфери діяльності. З цією метою держава залучає до вирішення завдань щодо забезпечення кібербезпеки в національному масштабі крім основних суб'єктів національної системи кібербезпеки, на яких базувалася на початковій стадії формування національної системи кібербезпеки, широке коло суб'єктів забезпечення кібербезпеки, у тому числі суб'єктів господарювання, громадські об'єднання та окремих громадян України. Ключову об'єднувальну та координаційну роль у цьому процесі відіграє Національний координаційний центр кібербезпеки.

Сьогодні держава розвиває національну систему кібербезпеки, спираючись на такі принципи [1, 4-7, 14], як розуміння та аналіз цифрового середовища і глобальних трендів у сфері кібербезпеки, з урахуванням особливостей нашої країни, та невідступне захист національних інтересів; заходи щодо удосконалення законодавства у галузі кібербезпеки та оперативна актуалізація відповідно до плинних безпекових умов; орієнтація на суспільство з метою сприяння його економічному і соціальному зростанню, встановлення правил безпечного використання Інтернету; забезпечення балансу між потребами держави і правами громадян, дотриманням законності та основних цінностей, включаючи права людини і свободу слова; відкритість і створення умов для активної участі всіх зацікавлених сторін з урахуванням їхніх потреб і зобов'язань; розподіл матеріальних і фінансових ресурсів для вирішення конкретних завдань у сфері кібербезпеки; проактивний підхід, включаючи застосування систем попередження кібератак та вжиття випереджувальних заходів; забезпечення

демократичного цивільного контролю за роботою національної системи кібербезпеки. Реалізація цих принципів спрямована на посилення кібербезпеки та захисту прав громадян та держави в цифровому середовищі.

Прискорений розвиток та взаємопроникнення інформаційних технологій приносить за собою не лише значні соціальні переваги, але й збільшення кіберзагроз у всіх сферах життєдіяльності. Україна має відповідний потенціал для розширення своїх можливостей у сфері кібербезпеки для адекватного протистояння сучасним викликам і загрозам.

Деякі з цих викликів для України у сфері кібербезпеки включають активне використання кіберзасобів у міжнародній конкуренції за світове лідерство, що супроводжується змагальним розвитком засобів кібербезпеки та реалізацією кіберзагроз під час швидких змін інформаційно-комунікаційних технологій.

Мілітаризація кіберпростору та збільшення технологічних можливостей кіберзброї дозволяє проведення прихованих кібератак та взяття під контроль критичних інформаційних систем. Зростає технологічний рівень протиправних посягань на інтереси держави та суспільства з використанням методів соціальної інженерії та криптотехнологій. Вплив пандемії COVID-19 на економічну діяльність та соціальну поведінку через широке використання електронних сервісів та інформаційно-комунікаційних систем посилило загрозу порушення прав громадян у кіберпросторі.

Цифрова трансформація, яка є одним із пріоритетів розвитку України, створює нові виклики у сфері кібербезпеки. Впровадження нових технологій та цифрових послуг вимагає системного підходу до кібербезпеки та оцінки ризиків. Без цього існує ризик втрати довіри громадян до процесів цифрової трансформації.

Сучасні світові тренди в розвитку кібербезпекового середовища створюють різноманітні виклики для України, які виявляються у внутрішніх

процесах та явищах країни. Одним із головних джерел загроз є активне використання кіберпростору в гібридній агресії з боку Росії. Росія відома своєю активною кіберагресією проти України, спрямованою на деструктивний вплив на органи державної влади, системи управління військами, а також на об’єкти критичної інфраструктури. Ця діяльність включає в себе розвідувальні операції, кібершпигунство та кібердиверсії, які мають серйозний потенціал для завдання шкоди Україні. Також зростає загроза кібертероризму, що пов'язано з кіберможливостями Росії та використанням кіберпростору для фінансування терористичних груп. Недостатня взаємодія з міжнародними партнерами у сфері кібербезпеки ускладнює боротьбу з цією загрозою.

У зв'язку з цим, Україні необхідно посилити свої зусилля у напрямку кібербезпеки, зокрема шляхом нарощування кіберзахисту критично важливих об'єктів інфраструктури, збільшення співпраці з міжнародними партнерами та розвитку власних кіберзбройних сил. Таким чином можна ефективно протистояти сучасним кіберзагрозам та забезпечити безпеку та стабільність в кіберпросторі.

Зростання кіберзлочинності в Україні становить серйозну загрозу для державних інформаційних ресурсів, суспільних процесів і особистих даних громадян. Це призводить до значних матеріальних втрат і підриву довіри суспільства до інформаційних технологій. Основні проблеми, які спричиняють цю ситуацію, наведено в табл. 1.

Таблиця 1

Основні проблеми зростання кіберзлочинності в Україні

№ з/п	Назва проблеми	Суть проблеми
1	Низький рівень кіберграмотності населення	Брак знань у сфері кібербезпеки серед пересічних користувачів електронних послуг створює ідеальне середовище для кіберзлочинців.
2	Недостатній кіберзахист державних інформаційних	Державні інформаційні ресурси і об'єкти критичної інфраструктури недостатньо захищені від кібератак, що може призвести до серйозних наслідків.

	ресурсів	
3	Технологічна залежність від іноземних виробників ІКТ	Висока технологічна залежність України від іноземних виробників продукції ІКТ збільшує її уразливість до кіберзагроз, оскільки відсутні належні стандарти безпеки та механізми контролю виробництва.
4	Недостатня увага до кіберзахисту при автоматизації державного управління	Деякі державні органи не належним чином оцінюють ризики, пов'язані з кібербезпекою, під час впровадження автоматизації процесів управління.
5	Відсутність національних стандартів безпеки	Відсутність сучасних національних стандартів щодо безпеки ланцюга поставок та оцінки відповідності інформаційно-комунікаційних систем підвищує ризики втрати конфіденційності, цілісності та доступності інформації.

Для зменшення цих загроз Україні необхідно вдосконалити свою стратегію кібербезпеки, покращити кіберграмотність населення, зміцнити захист державних інформаційних ресурсів, сприяти розвитку внутрішніх кіберзахисних стандартів та механізмів контролю, а також активно співпрацювати з міжнародними партнерами у цій сфері.

Сьогодні в Україні стикаються зі значними викликами у сфері кібербезпеки, які породжують різноманітні загрози та проблеми. Наведені в табл. 2.

Таблиця 2

Виклики у сфері кібербезпеки

№ з/п	**Назва**	**Зміст виклику**
1	Недостатній кіберзахист підприємств та організацій	Багато підприємств і установ не забезпечують належний рівень кіберзахисту своїх інформаційних ресурсів, що може призвести до порушень прав користувачів та шкодить довірі до цифрової трансформації.
2	Зростаюча складність кіберзагроз	Інструментарій кіберзлочинців стає все різноманітнішим і високотехнологічним, що ускладнює протидію таким загрозам.
3	Збільшення кількості кібератак	Набуває поширення кібератаки, спрямовані на викрадення конфіденційних даних та персональної інформації з використанням соціальної інженерії.
4	Фішинг та використання шкідливого програмного забезпечення	Зростає ризик фішингових атак, ботнетів та шкідливих програм, які можуть завдати серйозної шкоди інформаційним системам.

5	Витоки персональних даних	Витоки інформації з баз даних створюють загрозу конфіденційності та безпеки даних громадян.
6	Кібератаки на розробників програмного забезпечення	Кіберзлочинці здійснюють атаки на розробників програмного забезпечення з метою зараження додатків та завдання шкоди великій кількості користувачів.
7	Недоліки в нормативно-правовій базі	Недосконаліть законодавства у сфері кібербезпеки та низька правова відповідальність за порушення вимог законодавства.
8	Відсутність належної структурної організації та фінансування	Брак відповідних структурних підрозділів та недостатнє фінансування робіт з кіберзахисту.
9	Низький рівень кіберграмотності	Відсутність системи підвищення цифрової грамотності громадян та недостатня обізнаність суспільства щодо кіберзагроз та кіберзахисту.

Для ефективної боротьби з цими загрозами Україні потрібно вдосконалити законодавство, забезпечити належний рівень кіберзахисту на всіх рівнях та підвищити кіберграмотність населення. Також важливо підвищити фінансування робіт з кіберзахисту та підвищити рівень кваліфікації фахівців у цій галузі.

Забезпечення кібербезпеки для України стає вельми важливим у контексті сучасних глобальних викликів, оскільки цифрова інфраструктура є критичним компонентом національної безпеки. Визначення пріоритету забезпечення кібербезпеки допомагає запобігти серйозним загрозам для державних інформаційних ресурсів, промислових систем, та особистих даних громадян.

Стратегічні цілі забезпечення кібербезпеки включають розвиток ефективної системи захисту від кібератак, підвищення кіберграмотності населення та розвиток кадрового потенціалу у цій сфері. Постійна модернізація та удосконалення кіберзахисту є стратегічним завданням для забезпечення стійкості інформаційних систем та захисту національних інтересів. Забезпечення кібербезпеки є не лише національним пріоритетом, але й ключовою умовою для стабільного розвитку держави та її інтеграції у сучасний цифровий світ.

Сьогодні пріоритетами забезпечення кібербезпеки України є по-перше, убезпечення кіберпростору задля захисту суверенітету держави та розвитку суспільства; захист прав, свобод і законних інтересів громадян України у кіберпросторі; європейська і євроатлантична інтеграція у сфері кібербезпеки, а по-друге, формування нової якості національної системи кібербезпеки, що потребує чіткого та зрозумілого визначення стратегічних цілей, які мають бути досягнуті протягом періоду реалізації Стратегії [1]. На рис. 5 наведено дерево цілей реалізації Стратегії кібербезпеки України.

Рис. 5. Дерево цілей реалізації Стратегії кібербезпеки України, *розроблено автором на основі [1].*

Для формування потенціалу стримування (С) при розбудові національної системи кібербезпеки на основі стримування, кіберстійкості та сприянню взаємодії до 2026 року держава повинна досягти стратегічних цілей, наведених на рис. 5.

Для досягнення дієвої кібероборони (ціль С.1) Україна має не лише

створити та розвивати ефективні (у тому числі кадрово та технологічно) підрозділи з повноваженнями ведення збройного протиборства в кіберпросторі, але й сформувати належну правову, організаційну, технологічну модель їх функціонування та застосування, що неможливо без: ефективної взаємодії основних суб'єктів національної системи кібербезпеки та сил оборони під час проведення заходів з кібероборони, належного навчання та фінансового забезпечення таких структур, систематичного проведення кібернавчань, оцінки спроможностей та ефективності підрозділів, розроблення та імплементації індикаторів оцінки їх діяльності [1].

Для посилення спроможностей у протидії розвідувально-підривній діяльності у кіберпросторі та кібертероризму (ціль С.2.) Україна забезпечить безперервне здійснення контррозвідувальних заходів з виявлення, попередження та припинення розвідувально-підривної діяльності іноземних держав, актів кібершпигунства та кібертероризму, усунення умов, що їм сприяють, та причин їх виникнення для убезпечення інтересів держави, суспільства і окремих громадян.

З метою посилення спроможностей у протидії кіберзлочинності (ціль С.3.) правоохоронні та державні органи спеціального призначення з правоохоронними функціями набудуть спроможностей для мінімізації загроз кіберзлочинності, посилять свій технологічний і кадровий потенціал для проведення превентивних заходів та розслідування кіберзлочинів.

В процесі розвитку асиметричних інструментів стримування (ціль С.4.) потрібно створити необхідні умови для забезпечення стримування агресивних дій у кіберпросторі проти України шляхом застосування економічних, дипломатичних, розвідувальних заходів, а також залучення потенціалу неурядового сектору [1].

Для набуття кіберстійкості (К) при розбудові національної системи кібербезпеки на основі стримування, кіберстійкості та сприянню взаємодії

до 2026 року держава повинна досягти стратегічних цілей, наведених на рис. 5.

З метою посилення національної кіберготовності та кіберзахисту (ціль К.1.) потрібно запровадити та реалізовувати чіткі та зрозумілі для всіх стейкхолдерів заходи з посилення національної кіберготовності в інтересах забезпечення економічного добробуту та захисту прав та свобод кожного українського громадянина. Кіберготовність полягає у здатності всіх стейкхолдерів, насамперед суб'єктів сектору безпеки і оборони, своєчасно й ефективно реагувати на кібератаки, забезпечити режим постійної готовності до реальних та потенційних кіберзагроз, виявлення та усунення передумов до їх виникнення, забезпечивши тим самим кіберстійкість, насамперед об’єктів критичної інформаційної інфраструктури.

В процесі підвищення професійного вдосконалення, розбудови кіберобізнаного суспільства та розвитку науково-технічного забезпечення кібербезпеки (ціль К.2.) виникає потреба у проведенні докорінної реформи системи підготовки та підвищення кваліфікації фахівців у сфері кібербезпеки. Забезпеченні збереження наявного кваліфікованого кадрового потенціалу суб’єктів кібербезпеки. Стимулюванні дослідження і розробки у сфері кібербезпеки з урахуванням появи нових кіберзагроз і викликів, створенні національних інформаційних систем, платформ і продуктів. Вітчизняний науково-технічний потенціал першочергово залучатиметься до вирішення завдань забезпечення кібербезпеки держави. Кібергігієна, цифрові навички, кіберобізнаність щодо сучасних кіберзагроз та протидії ним мають стати невід’ємними елементами освіти кожного українського громадянина [].

Для забезпечення безпечних цифрових послуг (ціль К.3) виникає потреба у досягненні балансу між потребами українського суспільства, вітчизняного ринку, економіки держави та необхідністю забезпечити безпеку в кіберпросторі; забезпеченні надійностіта безпеки цифрових

послуг з моменту створення та протягом усього їхнього життєвого циклу.

Для набуття взаємодії (В) при розбудові національної системи кібербезпеки на основі стримування, кіберстійкості та сприянні взаємодії до 2026 року держава повинна досягти стратегічних цілей, наведених на рис. 5.

З метою зміцнення системи координації (ціль В.1.) держава повинна створити умови для ефективної взаємодії суб'єктів забезпечення кібербезпеки в процесі розбудови та функціонування національної системи кібербезпеки, а також для результативних спільних дій під час попередження, відбиття та нейтралізації наслідків кібератак та кіберінцидентів. Також виникає потреба у координації діяльності усіх стейкхолдерів задля подолання кризових ситуацій у кібербезпеці.

Для формування нової моделі відносин у сфері кібербезпеки (ціль В.2.) виникає потреба у запровадженні сервісної моделі державної участі у заходах з кіберзахисту, за якої держава сприйматиметься не як джерело вимог, а як партнер у розбудові національної системи кібербезпеки [1, 3].

Для забезпечення прагматичного міжнародного співробітництва (ціль В.3.) відносини з міжнародними партнерами потрібно спрямувати як на розвиток взаємної довіри для спільної відповіді на кібератаки і подолання кризових ситуацій у кібербезпеці, так і на суто практичну співпрацю: обмін інформацією про кібератаки та кіберінциденти, проведення спільних кібероперацій та розслідування міжнародних кіберзлочинів, регулярні кібернавчання та тренінги, обмін досвідом та найкращими практиками.

Посилення спроможностей національної системи кібербезпеки здійснюється шляхом виконання стратегічних завдань, спрямованих на досягнення визначених цілей. Цей процес є ключовим завданням у забезпеченні національної безпеки, який досягається шляхом виконання стратегічних завдань, спрямованих на досягнення визначених цілей.

Стратегічні завдання, орієнтовані на підвищення рівня готовності до кібернападів, включають у себе не лише підвищення свідомості

громадськості про кібербезпеку, але й забезпечення підвищення кваліфікації фахівців з кібербезпеки та розвиток відповідних кадрових ресурсів. Важливими аспектами посилення системи кібербезпеки є також постійна модернізація та удосконалення її, що сприяє запобіганню кіберзлочинності та захисту особистих даних громадян. Зокрема, підвищення обізнаності громадськості щодо кібербезпеки сприяє зниженню ризиків та підвищує загальний рівень захищеності, що в свою чергу є ключовим фактором для забезпечення національної безпеки та стабільності держави.

Головним зовнішньополітичним пріоритетом України у сфері кібербезпеки має бути зміцнення євроінтеграційних процесів шляхом уніфікації підходів, практик і засобів забезпечення кібербезпеки з усталеними стандартами ЄС і НАТО, вжиття інших затверджених із стратегічними іноземними партнерами заходів, спрямованих на підвищення кіберстійкості України, розвиток можливостей національної системи кібербезпеки та захист національних інтересів у кіберпросторі.

Україна повинна приділяти увагу спільній з партнерами протидії міжнародному тероризму, виявленню, попередженню і припиненню злочинів проти миру і безпеки людства, іншим протиправним діям, що порушують міжнародний правопорядок та інтереси демократичної світової спільноти, заснованню на договірній основі з партнерськими спецслужбами країн-членів ЄС і НАТО взаємовигідному обміну інформацією та досвідом щодо забезпечення національної безпеки у кіберпросторі, використанню кращих світових практик, активно здійснювати інші спільні заходи, що сприятимуть розвитку наукової, матеріально-технічної бази та кадрового потенціалу у сфері кібербезпеки.

Україна повинна співпрацювати з міжнародними партнерами, організаціями та іншими заінтересованими сторонами, які поділяють спільне бачення майбутнього кіберпростору як глобального, відкритого,

вільного, стабільного та безпечного, в основі якого дотримання прав людини, основних свобод та демократичних цінностей, які гарантують соціально-економічний та політичний розвиток України. Наша держава має продовжувати активну участь у міжнародному діалозі з питань відповідальної поведінки держав у кіберпросторі на основі дотримання принципів міжнародного права, Статуту ООН, а також добровільних необов'язкових норм, правил та принципів відповідальної поведінки держави. Це потребуватиме більшої координації та консолідації заінтересованих сторін на міжнародних форумах, в яких Україна має бути не лише учасником, але й ініціатором та організатором.

Виходячи з того, що Інтернет давно став суспільним надбанням, істотно вийшов за межі суто національних інтересів, наша держава повинна максимально сприяти мультистейкходерській (багатосторонній) моделі управління Інтернетом, підтримуючи міжнародні, регіональні та національні дискусії з цього питання, сприяючи залученню до цього процесу приватного сектору, наукових та освітніх кіл, громадянського суспільства. Україна сприятиме подальшому дотриманню міжнародного права та стандартів у галузі прав людини, заохочуватиме застосування найкращих практик, а також активізує свої зусилля щодо запобігання зловживанню новими технологіями. Для цього держава повинна підвищити участь і партнерство в міжнародних процесах стандартизації та сертифікації у сфері кібербезпеки, розширити представництво в міжнародних, регіональних та інших органах стандартизації, організаціях, що займаються розробленням стандартів та сертифікацією у цій сфері.

У питаннях розроблення стандартів у сферах нових технологій (зокрема щодо штучного інтелекту, хмарних технологій, квантових обчислень та квантових комунікацій) та базової архітектури Інтернету Україна повинна дотримуватись позиції, що Інтернет повинен лишатися глобальним та відкритим, технології мають спрямовуватися на людину,

забезпечувати її базові свободи, гарантувати невтручання у її особисте життя, забезпечувати її конфіденційність у кіберпросторі, а будь-які обмеження в цій частині мають здійснюватися лише відповідно до закону. Використання технологій має бути законним, безпечним та етичним.

Враховуючи взаємопов'язаність сучасного кіберпростору та з метою розвитку співпраці між державою, приватним сектором економіки, науковими і освітніми колами та громадянським суспільством у сфері кібербезпеки, Україна повинна вдосконалювати національний кіберпростір як глобальний, відкритий, вільний, стабільний і, перш за все, безпечний, що є гарантією успішного розвитку країни.

В процесі реалізації Стратегії [1, 4-5, 7] Україна повинна зробити кібербезпеку одним з основних питань своєї міжнародної діяльності, посилюючи для цього потенціал своїх зовнішньополітичних структур та кіберпотенціал держави. З цією метою Україна має розвивати мережу партнерства у сфері кібербезпеки, розбудовуючи наявні та створюючи нові формати і механізми міжнародного співробітництва. Процес реалізації Стратегії має бути максимально прозорим, відкритим та супроводжуватися демократичним цивільним контролем.

Першочерговим завданням для України є розроблення та запровадження індикаторів стану кібербезпеки на основі системного моніторингу виявлення і прогнозування кіберзагроз, що надасть змогу фіксувати досягнення або недоліки функціонування системи кібербезпеки.

Крім того, важливим напрямом є розроблення інтегральної системи оцінювання новітніх технологій, що безпосередньо мають вплив на кіберстійкість держави, створення інструментів (стандарти, протоколи, сертифікати тощо) з оцінювання ефективності використання новітніх технологій з протидії кібератакам. Ефективність реалізації

Стратегії повинна визначатися через постійний моніторинг її виконання та спиратися на чітку систему розроблених індикаторів стану

кібербезпеки. Індикатори мають визначати прогрес, якого досягли суб'єкти забезпечення кібербезпеки в реалізації Стратегії з таких питань, як: виконання стратегічних завдань у межах цілей (в розрізі завдань); досягнення стратегічних цілей (в розрізі цілей); ступінь впливу заходів, що здійснюються, на національну систему кібербезпеки та цифрову трансформацію держави. Запровадження індикаторів стану кібербезпеки забезпечить покращення процесу моніторингу виконання Стратегії кібербезпеки у реальному часі з використанням сучасних веб-ресурсів (онлайн-платформ), прозорість вжитих заходів для суспільства та держави.

Посилення впливу національної системи кібербезпеки на суспільний розвиток буде визначатися за визначеними критеріями: підвищення рівня довіри населення до держави щодо безпечності кіберпростору; формування безпечного інформаційного суспільства, в якому до заходів кібербезпеки крім державних інституцій залучені приватні суб'єкти та громадяни; позитивний вплив на захист національних інтересів у сфері кібербезпеки (як приклад, рівень впливу на розвиток ситуації, пов'язаної з агресією Російської Федерації проти України).

За допомогою розгалуженої системи індикаторів визначатиметься стан досягнення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави. Система індикаторів повинна включати базові індикатори стану кібербезпеки, індикатори розвитку національної системи кібербезпеки та індикатори стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, що дасть можливість комплексно оцінювати результативність та ефективність реалізації Стратегії кібербезпеки.

Визначені концептуальні підходи до подальшого розвитку національної системи кібербезпеки базуються на:

– загальному розумінні та аналізі кіберсередовища, світових кібертрендів

(з урахуванням національних особливостей), незаперечному захисті національних інтересів України;

- стійкості у вдосконаленні законодавства у галузі кібербезпеки;
- спрямованості на економічний і соціальний прогрес суспільства;
- забезпеченні балансу між потребами держави і правами громадян, додержанні законності, процесуальних гарантій та засобів правового захисту;
- чіткому визначенні ролей, потреб і обов'язків при вирішенні завдань кібербезпеки на різній складності рівні;
- орієнтації на ризики при забезпеченні кібербезпеки та кіберзахисту;
- впровадженні механізмів партнерства між державним і приватним сектором у галузі кібербезпеки;
- активному підході, який передбачає проведення запобіжних заходів;
- забезпеченні демократичного цивільного контролю за функціонуванням національної системи кібербезпеки.

Метою реалізації Стратегії кібербезпеки України на 2021–2025 роки [1] визначено створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства, держави. Документ ґрунтується на засадах стримування, кіберстійкості та взаємодії.

Отже, в процесі проведеного дослідження розглянуто сутність та значення інформаційної безпеки держави, а також проаналізовано основні кіберзагрози, досліджено Стратегію кібербезпеки України, її цілі, завдання та основні положення, проведено оцінювання впливу Стратегії кібербезпеки України на забезпечення інформаційної безпеки держави, а також будуть вироблено пропозиції щодо її вдосконалення.

Дослідження дозволило визначити роль та місце Стратегії кібербезпеки України у системі забезпечення інформаційної безпеки держави, оцінити ефективність Стратегії кібербезпеки України, розробити пропозиції щодо вдосконалення Стратегії кібербезпеки України. Результати

дослідження можуть бути використані для вдосконалення Стратегії кібербезпеки України, а також для розроблення та впровадження інших заходів, спрямованих на посилення інформаційної безпеки держави.

Список використаних джерел:

1. Стратегія кібербезпеки України. [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/447/2021#Text.
2. Про національну безпеку України: Закон України. [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/2469-19#Text.
3. Правові засади кібергігієни [Електронний ресурс]. Режим доступу: https://https://drive.google.com/file/d/1EPd677wdTA32Fbi5RzoobUk2CvcolQAW/view.
4. Стратегія національної безпеки України, затверджена Указом Президента України від 14 вересня 2020 року № 392. [Електронний ресурс]. Режим доступу: https://www.president.gov.ua/documents/3922020-35037.
5. Про основні засади забезпечення кібербезпеки України: Закон України. Урядовий кур'єр, № 215, 2017.
6. Про Державну службу спеціального зв’язку та захисту інформації України: Закон України. [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/3475-15#Text.
7. Про основні засади забезпечення кібербезпеки: Закон України. [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19#Text.
8. Про захист інформації в інформаційно-комунікаційних системах: Закон України. [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.

9. Про національну систему конфіденційного зв’язку : Закон України. [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/2919-14#Text.
10. Про критичну інфраструктуру: Закон України. [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/1882-20#Text.
11. Про електронну ідентифікацію та електронні довірчі послуги: Закон України. [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/2155-19#Text.
12. Про Кібербезпеку: Закон України. [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19.
13. Доктрина інформаційної безпеки України: [Електронний ресурс]. Режим доступу: https://www.president.gov.ua/documents/472017-21374
14. Національна стратегія розвитку інформаційного суспільства в Україні на 2017-2020 роки. [Електронний ресурс]. Режим доступу: https://www.nas.gov.ua/siaz/ways_of_development_of_ukrainian_science/article/12116.1.083.pdf.