реалізувати комплексний підхід шляхом:

– ухвалення нових законів та нормативних актів, що зобов'яжуть власників об'єктів критичної інфраструктури захищати свої інформаційно-комунікаційні системи;

– упровадження систем виявлення та реагування на кіберінциденти, управління та контролю засобами кіберзахисту (далі – Security Operations Center);

– упровадження автоматизації процесів у роботу Security Operations Center;

– упровадження штучного інтелекту для виявлення кіберзагроз на ранніх етапах;

– упровадження не лише сучасної багатофакторної автентифікації, а й служб каталогів для визначення групових політик та їх реалізації на пристроях мережі;

– упровадження стратегій для швидкого відновлення після кібератак;

– упровадження кіберзахисту хмарних технологій;

– належного фінансування навчання та підвищення кваліфікації персоналу, а також проведення регулярних тренінгів та здійснення симуляції кібератак;

– налагодження постійного обміну інформацією та досвідом із партнерами;

– участі в міжнародних глобальних програмах кіберзахисту.

Ключовою складовою національної безпеки держави є критична інфраструктура. Вразливість критичної інфраструктури до кіберзагроз робить державу вразливою до гібридних загроз. Держави повинні постійно розвивати системи кіберзахисту. Запропонований комплексний підхід дозволить забезпечити кіберзахист критичної інфраструктури держави, стабільність та безпеку суспільства.

1. Паламарчук С., Хусаінов П., Штонда Р. Інформаційна безпека та кібербезпека галузевого сектору: пріоритетні напрями розвитку. Сектор безпеки і оборони України на захисті національних інтересів: актуальні проблеми та завдання в умовах воєнного стану : матеріали ІІІ Міжнар. наук.-практ. конф. (м. Хмельницький, 21 лист. 2024 р.). Хмельницький, 2024. С. 1169–1171. URL : https://dspace.nadpsu.edu.ua/bitstream/123456789/4767/3/НАДПСУ_21.11.2024.pdf.

2. Річний аналітичний огляд: жовтень 2023 – вересень 2024. URL : https://www.rnbo.gov.ua/files/2024/NATIONAL_CYBER_SCC/20250109/Year%20in%20review_UKR_upd.pdf.

**Олексій БЕРВЕНО**
аспірант кафедри
адміністративно-правових дисциплін
та публічного управління
Дніпровського державного
університету внутрішніх справ
(м. Дніпро, Україна)

## ІНФОРМАЦІЙНА БЕЗПЕКА ЯК ЕЛЕМЕНТ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Інформаційна безпека – це стан захищеності систем обробки і зберігання даних, за якого забезпечено конфіденційність, доступність і цілісність інформації, використання й розвиток в інтересах громадян, або комплекс заходів, спрямованих на забезпечення захищеності інформації особи, суспільства і держави від несанкціонованого доступу, використання, оприлюднення, руйнування, внесення змін, ознайомлення, перевірки запису чи знищення (у цьому значенні частіше використовують термін «захист інформації»).

Інформаційна безпека держави характеризується ступенем захищеності і, отже, стійкістю основних сфер життєдіяльності (економіки, науки, техносфери, сфери управління, військової справи, суспільної свідомості та ін.) до небезпечних (дестабілізаційних, деструктивних, суперечних інтересам країни тощо) інформаційних впливів, причому як до впровадження, так і до вилучення інформації.

Поняття інформаційної безпеки не обмежується безпекою технічних інформаційних систем чи безпекою інформації у чисельному чи електронному вигляді, а стосується усіх аспектів захисту даних чи інформації, незалежно від форми, у якій вони перебувають.

У сучасних умовах, передусім в умовах воєнного стану, інформаційна складова національної безпеки держави відіграє надзвичайно важливу роль з огляду на наявні в ній

ризики та загрози, до яких доцільно відносити кібертероризм, кіберзлочинність, агресивну пропаганду, поширення антиконституційних та антидержавних гасел, обмеження доступу населення до публічної інформації тощо.

В Україні регулювання інформаційної безпеки здійснюється за допомогою таких нормативно-правових актів, як: Конституція України, закони України «Про інформацію», «Про Національну програму інформатизації», рішення Ради національної безпеки і оборони України «Про Доктрину інформаційної безпеки України», «Про Стратегію національної безпеки України».

26 серпня 2021 р. Президент України підписав указ, яким увів в дію рішення Ради національної безпеки і оборони України від 14 травня 2021 р. «Про Стратегію кібербезпеки України». У концепції зазначається: «Економічна, науково-технічна, інформаційна сфера, сфера державного управління, оборонно-промисловий і транспортний комплекси, інфраструктура електронних комунікацій, сектор безпеки і оборони України стають все більш уразливими для розвідувально-підривної діяльності іноземних спецслужб у кіберпросторі. Цьому сприяє широка, подекуди домінуюча, присутність в інформаційній інфраструктурі України організацій, груп, осіб, які прямо чи опосередковано пов'язані з Російською Федерацією».

Для реалізації державної політики щодо захисту в кіберпросторі державних інформаційних ресурсів та інформації прийнятий Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017. Цей закон став основою розвитку державної системи захисту від мережевих погроз.

На підставі Закону України «Про національну безпеку України» та з метою захисту інформаційного простору України у липні 2023 р. Національний центр оперативно-технічного управління мережами телекомунікацій України видав розпорядження № 461/1292 про блокування списку доменних імен.

Важливим наслідком поширення інформаційних та комунікаційних технологій і їх впровадження у всі сфери суспільного життя стало створення правових, організаційних та технологічних передумов для розвитку демократії, що забезпечує громадянам можливість вільного пошуку, отримання, передачі, створення та поширення інформації.

Однак із новими можливостями участі громадян у політиці, формування нового виміру реалізації національних інтересів можна спостерігати й підвищення ймовірності появи нових загроз, джерела яких можуть мати як природний (помилки, стихійні лиха, випадкові події), так і умисний характер (умисне та цілеспрямоване використання ЗМІ, спеціальних програм для здійснення кібератак та ін.).

В умовах науково-технічного прогресу можна виокремити такі групи інформаційно-технічних загроз інформаційної безпеки та розвитку держави в цілому.

Перша група пов'язана з розвитком новітньої інформаційної зброї, здатної впливати як на психіку та свідомість людей, так і на інформаційно-технічну інфраструктуру суспільства. Йдеться про поширення пропаганди та дезінформації, що може призводити до маніпуляції даними або їх фальсифікації, що впливає на політичні процеси, сприяє дестабілізації режимів тощо.

Друга група загроз стосується нового класу соціальних злочинів, що базуються на використанні сучасних ІКТ, таких як махінації з електронними коштами та комп'ютерне хуліганство. Особливо актуальним стає питання інформаційної безпеки в контексті зростання транснаціональної кіберзлочинності та кібертероризму. У цьому випадку під загрозою опиняється конфіденційність, оскільки кібератаки можуть бути спрямовані на різні джерела конфіденційної інформації з метою шпигунства, крадіжки персональних даних, шахрайства або «крадіжки особистості».

Третя група загроз пов'язана із використанням ІКТ у політичних цілях на національному та міжнародному рівнях, що обумовлено зростанням впливу ЗМІ на процес розроблення, прийняття та реалізації політичних рішень, функціонування механізму політичної влади та розвиток політичного процесу.

Сучасні загрози інформаційній безпеці як важливому елементу національної безпеки вимагають комплексного підходу до формування єдиного механізму забезпечення інформаційної безпеки та кібербезпеки в ЄС. Так, у 2004 році було створено Агентство Європейського Союзу з мережевої та інформаційної безпеки (ENISA). Місія ENISA полягає в підвищенні обізнаності про мережеву та інформаційну безпеку, а також у розвитку та просуванні культури мережевої та інформаційної безпеки в суспільстві на благо громадян, споживачів, підприємств та організацій державного сектора в Союзі.

У 2013 р. було висловлено ідею про Стратегію кібербезпеки Європейського Союзу, а у 2016 р. – ухвалено Директиву 2016/11481 про безпеку мережевих та інформаційних систем (далі – NIS), що передбачає заходи для досягнення високого загального рівня безпеки мережевих та інформаційних систем у рамках ЄС з метою поліпшення функціонування внутрішнього ринку. Кожна держава-член ЄС має ухвалити національні рамки, що охоплюватимуть національну стратегію щодо забезпечення безпеки мережевих та інформаційних систем і призначення органів, для успішного виконання положень Директиви NIS.

У 2019 р. було ухвалено Закон про кібербезпеку, спрямований на досягнення високого рівня кібербезпеки, кіберстійкості та довіри в Європейському Союзі.

У 2020 р. Європейська комісія презентувала нову стратегію ЄС у сфері безпеки на період 2020–2025 рр., зосередивши увагу на пріоритетних галузях, у яких ЄС може зробити свій внесок у підтримку держав-членів у зміцненні безпеки для всіх, хто живе в Європі. Від боротьби з тероризмом та організованою злочинністю, запобігання та виявлення гібридних загроз і підвищення стійкості критичної інфраструктури до просування кібербезпеки та сприяння дослідженням та інноваціям – стратегія визначає інструменти й заходи, які необхідно розробити впродовж наступних 5 років для гарантування безпеки в нашому фізичному та цифровому середовищі. Дана стратегія визначає 4 стратегічні пріоритети для дій на рівні ЄС:

– стійке до майбутнього середовище безпеки – люди покладаються на ключові інфраструктури, онлайн і офлайн, і для їхнього забезпечення запропоновано нові правила ЄС щодо захисту та забезпечення стійкості критичної інфраструктури, фізичної та цифрової. Визначено необхідність створення Об'єднаного кіберпідрозділу як платформи для структурованого і скоординованого співробітництва, а також наголошено на необхідності міжнародного партнерства для подальшого запобігання, стримування і реагування на кібератаки, просування стандартів ЄС для підвищення рівня кібербезпеки країн-партнерів;

– боротьба із загрозами, що розвиваються, що передбачає зміцнення потенціалу правоохоронних органів у сфері цифрових розслідувань;

– захист європейців від тероризму та організованої злочинності, що передбачає ініціювання кроків зі зміцнення законодавства про безпеку кордонів і більш ефективного використання наявних баз даних. Співпраця з країнами, що не входять до ЄС, і міжнародними організаціями також матиме ключове значення в боротьбі з тероризмом;

– сильна європейська екосистема безпеки, яка має формуватися на основі зміцнення мандату Європолу, та подальший розвиток Євроюсту для тіснішого зв'язку між судовими та правоохоронними органами.

Зміцнення інформаційної безпеки визначається як пріоритетний напрям формування національної безпеки і в Україні. Національний інформаційний простір України зазнає суттєвих загроз, які становлять небезпеку для функціонування держави, її політичного та економічного розвитку, інтеграції у європейські та євроатлантичні структури.

Повертаючись до визначення інформаційної безпеки в нормативних актах України, слід зауважити, що в Законі України «Про національну безпеку України» встановлено: «державна політика у сферах національної безпеки і оборони спрямовується на забезпечення воєнної, зовнішньополітичної, державної, економічної, інформаційної, екологічної безпеки, безпеки критичної інфраструктури, кібербезпеки України та на інші її напрями». Отже, інформаційна безпека розглядається в контексті національної безпеки.

Таким чином, електронні послуги, нові технології, інформаційні системи та мережі міцно увійшли в наше повсякденне життя, а навмисні інциденти, що призводять до порушення роботи IT-сервісів і критично важливої інфраструктури, являють собою серйозну загрозу для її функціонування.

У міру розвитку інформаційно-комунікаційних технологій поняття «інформаційна безпека» стало набувати дедалі виразнішого технічного змісту. Під нею розуміють захищеність інформаційного середовища, яке, своєю чергою, трактують як сукупність інформаційних ресурсів, систем розповсюдження, формування і використання інформації та інформаційної інфраструктури.

Європейська модель інформаційної безпеки формується на основі концепції захисту інформаційних систем, що переважно охоплює сфери діяльності, які безпосередньо пов'язані з використанням технічних засобів збирання, оброблення, захисту, розповсюдження та використання інформації. Тому в межах цієї платформи оперують такими поняттями, як «кібербезпека», «кіберзагрози», «кібератаки». Однак необхідно звернути увагу й на інший бік інформаційної безпеки: деструктивний інформаційний вплив на свідомість населення та

замовчування про сучасні інструменти кібервпливу (ботнети, спам, фішинг тощо).

Інформаційна безпека виступає інтегративною складовою національної безпеки та має формуватися на захищеності інтересів особистості, суспільства і держави. А найважливішим завданням системи забезпечення національної інформаційної безпеки є вдосконалення правового регулювання, включно з детальнішим врегулюванням захисту інформації; використання найефективніших сучасних методів і способів захисту інформації; удосконалення системи інформаційної безпеки; впровадження сучасних інформаційних технологій в управлінську діяльність; пріоритетність розвитку інформаційних технологій (програмне забезпечення, інновації та застосування нанотехнологій в інформаційній безпеці, а також в інформаційній сфері).

1. Боднар І. Р. Інформаційна безпека як основа національної безпеки. *Mechanism of an Economic Regulation.* 2014. № 1 (63). С. 68–75.
2. Милосердна І. М. Інформаційна безпека як елемент національної безпеки: теоретичний вимір та особливості впровадження. *Політикус*. 2024. Вип. 4. С. 179–185.
3. Ільницька У. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам. *Humanitarian vision.* 2016. Vol. 2. Num. 1. P. 27–32.
4. Олійник О. В. Принципи забезпечення інформаційної безпеки України. *Юридичний вісник.* 2016. Вип. 4 (41). С. 72–78.
5. Ліпкан В. А. Теоретичні основи та елементи національної безпеки України. Київ : Текст, 2003. 600 с.
6. Гуцалюк М. В. Організація захисту інформації : навч. посібник. Київ : Альтерпрес, 2012. 224 с.

**Олександра БІЛОЦЕРКІВСЬКА**
аспірант Харківського національного
педагогічного університету
імені Г. С. Сковороди
(м. Харків, Україна)
*https://orcid.org/0009-0001-1329-9553*

## ГІБРИДНІ ЗАГРОЗИ ТА ІНФОРМАЦІЙНА БЕЗПЕКА: ФАКТОРИ СТІЙКОСТІ ІНСТИТУТІВ ПУБЛІЧНОЇ ВЛАДИ

Сучасний світ характеризується зростаючою складністю та динамічністю геополітичних процесів. У цих умовах гібридні загрози, що поєднують військові та невійськові методи впливу, стають дедалі актуальнішими. Вони спрямовані на підрив національної безпеки, дестабілізацію суспільства та девальвацію фундаментальних цінностей демократичного світу. Особливого значення набуває інформаційна безпека, адже саме інформаційний простір є однією з ключових дискутивних площин у гібридній війні.

Інститути публічної влади, такі як органи державної влади, місцевого самоврядування, судові та правоохоронні органи, є фундаментом будь-якої демократичної держави. Саме вони забезпечують реалізацію волі народу, захист прав громадян, підтримання громадського порядку та стабільність суспільства. Проте, в умовах сучасних гібридних загроз, ці інститути опиняються під особливим прицілом. Гібридні загрози спрямовані, перш за все, на підрив легітимності влади та дестабілізацію суспільства. Інформаційний простір відіграє ключову роль у цих гібридних операціях. Дезінформація, пропаганда, кібератаки та інші форми інформаційного впливу можуть бути використані для дискредитації інститутів влади, поширення паніки та хаосу, створення штучних конфліктів та розколів у суспільстві [1; 2; 6].

У цих умовах стійкість інститутів публічної влади, їх здатність ефективно функціонувати в умовах інформаційного тиску та маніпуляцій є критично важливою для забезпечення національної безпеки та збереження демократичних цінностей. Стійкі інститути влади здатні протистояти інформаційним атакам, зберігати довіру громадян, забезпечувати стабільність та правопорядок, а також ефективно реагувати на виклики, що постають перед суспільством. Необхідність адаптації системи владних інституцій до нових викликів, розробка ефективних механізмів протидії гібридним загрозам та забезпечення інформаційної безпеки зумовлюють високу актуальність дослідження факторів стійкості інститутів публічної влади в умовах гібридних загроз. Про це свідчать численні праці