ПРИВАТНЕ АКЦІОНЕРНЕ ТОВАРИСТВО
«ВИЩІЙ НАВЧАЛЬНИЙ ЗАКЛАД»
МІЖРЕГІОНАЛЬНА АКАДЕМІЯ УПРАВЛІННЯ ПЕРСОНАЛОМ
Навчально-науковий інститут управління, економіки та бізнесу
Кафедра публічного управління

«Допущено до захисту»
Завідувач кафедри

_____

І.А. Семенець-Орлова

«_____» _____ 2026 р.

ДИПЛОМНА РОБОТА

на здобуття другого (магістерського) рівня вищої освіти

на тему:

«ФОРМУВАННЯ ДІЄВОЇ МОДЕЛІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ»

Виконала: студентка групи
ТУ-8-24-М1ПУА (2.0 здс)
Спеціальності 281 Публічне управління
та адміністрування
Шершун Оксана Михайлівна
Керівник: заст. зав. кафедри., Кузьменко Г.О.

Київ 2026

АНОТАЦІЯ

Шершун Оксана Михайлівна «Формування дієвої моделі інформаційної безпеки держави»

Дипломна робота на здобуття другого (магістерського) рівня вищої освіти за спеціальністю «Публічне управління та адміністрування» – Міжрегіональна Академія управління персоналом – Київ, 2026.

У магістерській роботі визначено теоретичні засади формування системи інформаційної безпеки держави. Проаналізовано сучасний стан інформаційної безпеки України, основні інформаційні та кібернетичні загрози, а також діяльність органів державної влади у сфері забезпечення інформаційної та кібернетичної безпеки. Запропоновано напрями формування дієвої моделі інформаційної безпеки держави, зокрема удосконалення державної політики у сфері інформаційної безпеки, розвиток стратегічних комунікацій, підвищення рівня медіаграмотності населення, посилення кіберзахисту та захисту критичної інформаційної інфраструктури.

Ключові слова: інформаційна безпека держави, кібербезпека, стратегічні комунікації, дезінформація, інформаційні загрози, кібератаки, медіаграмотність, критична інформаційна інфраструктура, кіберзахист.

SUMMARY

Shershun Oksana Mykhailivna “Formation of an effective model of state information security”

Master’s thesis for obtaining the second (Master’s) level of higher education in the specialty “Public Administration” – Interregional Academy of Personnel Management – Kyiv, 2026.

The master’s thesis defines the theoretical foundations of the formation of the state information security system. The current state of information security in Ukraine, the main information and cyber threats, as well as the activities of public authorities in the field of information and cyber security are analyzed. The directions for forming an effective model of state information security are proposed, including improvement of

state policy in the field of information security, development of strategic communications, increasing media literacy of the population, strengthening cybersecurity and protection of critical information infrastructure.

Key words: state information security, cybersecurity, strategic communications, disinformation, information threats, cyberattacks, media literacy, critical information infrastructure, cyber protection.

ЗМІСТ

ВСТУП	5
РОЗДІЛ 1 ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ	9
1.1. Поняття, сутність та складові інформаційної безпеки держави	9
1.2. Інформаційна безпека держави в системі національної безпеки України як наукова проблема	19
1.3. Нормативно-правове забезпечення інформаційної безпеки в Україні	23
1.4. Міжнародний досвід у формуванні інформаційної безпеки держави	27
Висновки до розділу 1	33
РОЗДІЛ 2 СУЧАСНИЙ СТАН ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ	35
2.1. Загрози та виклики інформаційній безпеці України в сучасних умовах	35
2.2. Кібербезпека в системі інформаційної безпеки держави	39
2.3. Діяльність органів державної влади у формуванні інформаційної безпеки держави	48
Висновки до розділу 2	58
РОЗДІЛ 3 ФОРМУВАННЯ ДІЄВОЇ МОДЕЛІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ	60
3.1. Основні напрями удосконалення державної політики у сфері інформаційної безпеки	60
3.2. Впровадження сучасних механізмів протидії інформаційним загрозам, кібератакам та дезінформації	70
Висновки до розділу 3	73
ВИСНОВКИ	75
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	78

ВСТУП

Актуальність теми.

У сучасних умовах цифрової трансформації суспільства, розвитку глобального інформаційного простору та повномасштабної агресії Російської Федерації проти України питання забезпечення інформаційної безпеки держави набувають особливої актуальності. Інформаційний простір став окремим середовищем стратегічного протиборства, у межах якого активно здійснюються інформаційно-психологічні операції, кібератаки, дезінформаційні кампанії, маніпулятивний інформаційний вплив та втручання у функціонування державних інформаційних ресурсів і критичної інфраструктури.

Сучасні інформаційні загрози мають комплексний характер і охоплюють політичну, воєнну, економічну, соціальну та гуманітарну сфери. Особливо небезпечними є кібератаки на державні інформаційно-комунікаційні системи, використання соціальних мереж для інформаційного впливу, поширення фейкової інформації, технологій deepfake та AI-генерованого контенту. За таких умов забезпечення інформаційної безпеки держави стає одним із ключових напрямів державної політики та важливою складовою національної безпеки України.

Актуальність дослідження зумовлена також необхідністю вдосконалення державної політики у сфері інформаційної безпеки, розвитку системи стратегічних комунікацій, підвищення рівня медіаграмотності населення, посилення міжвідомчої координації та впровадження сучасних механізмів кіберзахисту державних інформаційних ресурсів і критичної інформаційної інфраструктури.

Об’єкт дослідження – модель забезпечення інформаційної безпеки України в умовах цифрової трансформації суспільства та сучасних гібридних загроз.

Предмет дослідження – організаційно-правові, інституційні, технологічні та комунікаційні механізми формування дієвої моделі інформаційної безпеки держави.

Мета дослідження полягає у розробленні теоретично обґрунтованих та практично орієнтованих підходів до формування дієвої моделі інформаційної безпеки держави в умовах цифрової трансформації та сучасних інформаційних і кібернетичних загроз.

Для досягнення поставленої мети визначено такі завдання дослідження:

– проаналізувати теоретичні підходи до визначення сутності інформаційної безпеки держави;

– дослідити основні складові системи інформаційної безпеки України;

– визначити сучасні інформаційні та кібернетичні загрози національній безпеці України;

– проаналізувати діяльність органів державної влади у сфері забезпечення інформаційної та кібернетичної безпеки;

– дослідити сучасний стан стратегічних комунікацій та механізмів протидії дезінформації;

– визначити напрями вдосконалення державної політики у сфері інформаційної безпеки;

– обґрунтувати необхідність розвитку медіаграмотності населення та підвищення інформаційної стійкості суспільства;

– розробити практичні рекомендації щодо формування дієвої моделі інформаційної безпеки держави.

Робоча гіпотеза дослідження ґрунтується на припущенні, що ефективне забезпечення інформаційної безпеки держави в умовах сучасних гібридних загроз можливе за умови комплексного поєднання організаційно-правових, технологічних, інформаційно-комунікаційних та освітніх механізмів, спрямованих на підвищення кіберстійкості держави, захист інформаційного простору та формування суспільної стійкості до дезінформації й інформаційно-психологічних операцій.

Теоретичною основою дослідження стали наукові праці вітчизняних та зарубіжних учених у сфері інформаційної безпеки, кібербезпеки, стратегічних комунікацій, державного управління та національної безпеки, зокрема праці В.

Гур'єва, Т. Мужанової, Н. Титової, Н. Вінера, К. Шеннона та інших науковців. Теоретичну основу також становлять положення Конституції України, законів України у сфері інформації та кібербезпеки, Стратегії інформаційної безпеки України, Стратегії кібербезпеки України та міжнародних стандартів у сфері кіберзахисту.

Методологічну базу дослідження становлять загальнонаукові та спеціальні методи дослідження. У роботі застосовано методи аналізу, синтезу, узагальнення, системного підходу, порівняльного аналізу, нормативно-правового аналізу, структурно-функціонального аналізу, а також методи вторинного аналізу статистичної інформації та інформаційно-аналітичного дослідження. Використання зазначених методів дало змогу комплексно дослідити сучасний стан інформаційної безпеки України та визначити напрями вдосконалення механізмів її забезпечення.

Стисла характеристика вибірки дослідження

У межах дослідження використано статистичні та аналітичні дані щодо діяльності органів державної влади у сфері інформаційної та кібернетичної безпеки, матеріали офіційних державних ресурсів, результати аналізу інформаційних та кібернетичних загроз, а також дані, отримані в одному зі структурних підрозділів органу державної влади.

Теоретичне значення роботи полягає у поглибленні наукових підходів до розуміння сучасної системи інформаційної безпеки держави, визначенні взаємозв'язку між інформаційною безпекою, кібербезпекою та стратегічними комунікаціями, а також у розвитку підходів до формування інформаційної стійкості держави в умовах сучасних гібридних загроз.

Практичне значення одержаних результатів полягає у можливості використання запропонованих рекомендацій та підходів у діяльності органів державної влади під час удосконалення державної політики у сфері інформаційної безпеки, розвитку системи стратегічних комунікацій, організації заходів із протидії дезінформації та забезпечення кіберзахисту державних інформаційних ресурсів.

Апробація результатів дослідження.

Основні положення та результати магістерського дослідження були апробовані під час участі у науково-практичних конференціях та обговоренні окремих аспектів дослідження у професійному середовищі.

Структура магістерської роботи.

Магістерська робота складається зі вступу, трьох розділів, загальних висновків та списку використаних джерел. Загальний обсяг роботи становить ___ сторінок. Список використаних джерел налічує 30 найменувань.

РОЗДІЛ 1
ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

1.1. Поняття, сутність та складові інформаційної безпеки держави

Інформація (від латинського слова «informacio» - роз'яснення, виклад) - це відомості (або їх сукупність) про предмети, явища і процеси оточуючого нас світу. Інформація - це абстрактне поняття. Інформація не існує сама по собі - вона укладена в структурі об'єкта або системи, в знаках і символах, зафіксованих на матеріальних носіях [4].

Комунікативна концепція розглядає інформацію як сферу спілкування і сферу загальнонаукової рефлексії, передбачає взаємоактуалізацію смислів (а не механічне переміщення інформації) і становить зміст комунікативних процесів. Функціональна концепція інформації представлена двома різновидами: кібернетичною, яка вважає, що інформація (інформаційні процеси) є у всіх самоврядних (технічних, біологічних, соціальних) системах, і антропоцентристською, у рамках якої інформація інтерпретується як особливість живих, самоврядних систем або ж свідомих істот, як основна передумова і умова оптимального управління. Атрибутивна концепція використовує більш широке поняття, розуміючи інформацію як віддзеркалення різноманітності в будь-яких об'єктах і процесах, як у живій, так і в неживій природі. При цьому інформація визначається як міра неоднорідності розподілу матерії та енергії в просторі і в часі. У логіко-семантичних теоріях інформації інформація розглядається як зменшення або подолання невизначеності.

Отже, під інформацією нині розуміють:

- відомості, повідомлення про що-небудь, якими обмінюються люди;
- сигнали, імпульси, образи, що циркулюють у технічних (кібернетичних) пристроях;
- кількісну міру усунення невизначеності (ентропії), міру організації системи;

- відображення різноманітності в будь-яких об'єктах і процесах неживої і живої природи.

В Україні на законодавчому рівні (Закон України «Про інформацію») закріплено таке визначення: «інформація – це документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому природному середовищі».

До основних ознак інформації відносять: невичерпність; вимірність; двоєдинство інформації та її носія; фізична невідчужуваність інформації від її творця, власника, споживача; наявність організаційної форми, структури у вигляді інформаційних систем, документів, бібліотек тощо; цінність; поширюваність.

Серед основних властивостей інформації виділяють: об'єктивність, достовірність, повнота, точність, актуальність, корисність, цінність, зрозумілість, доступність, стислість тощо.

Об’єктивність — властивість інформації відображати реальний стан речей незалежно від чиєїсь думки або оцінки.

Достовірність — властивість інформації бути правдивою, перевіреною та такою, що відповідає дійсності.

Повнота — властивість інформації містити достатній обсяг відомостей для прийняття рішення або розуміння ситуації.

Точність — властивість інформації правильно та без помилок відображати факти, події чи дані.

Актуальність — властивість інформації бути своєчасною та відповідати поточному моменту часу.

Корисність — властивість інформації приносити практичну користь для виконання певних завдань або досягнення мети.

Цінність — властивість інформації мати значущість для користувача та впливати на прийняття рішень.

Зрозумілість — властивість інформації бути легкою для сприйняття та однозначного тлумачення.

Доступність — властивість інформації бути доступною для отримання та використання за наявності відповідних прав доступу.

Стислість — властивість інформації передавати основний зміст коротко, без зайвих деталей.

Закон України «Про інформацію» поділяє інформацію на такі види:

- інформація про фізичну особу;
- інформація довідково-енциклопедичного характеру;
- екологічна інформація;
- інформація про товар (роботу, послугу);
- науково-технічна інформація;
- податкова інформація;
- правова інформація;
- статистична інформація;
- соціологічна інформація;
- критична технологічна інформація.

За порядком доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом. Будь-яка інформація є відкритою, крім тієї, що віднесена законом до інформації з обмеженим доступом.

Розглядаючи сутність поняття «інформаційна безпека», слід відзначити, що в англійській мові є два терміни, які однаково перекладаються на українську мову, однак мають відмінний зміст: «safery» і «security». Перший з них означає стан захищеності об’єкта, другий – акцентує на діяльності із забезпечення цього стану.

Тому інформаційну безпеку визначають і як стан, який характеризується відсутністю небезпеки, тобто чинників і умов, які загрожують безпосередньо об’єкту (індивіду, спільноті, державі) з боку інформаційно-комунікаційного середовища, і як можливість, здатність об’єкта надійно захиститися, нейтралізувати, протидіяти різним інформаційним загрозам.

В найзагальнішому випадку інформаційна безпека – це стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави. [3].

Відповідно до Закону України «Про національну безпеку України», 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, інформацію про складові інформаційної безпеки наведено на (рис.1).

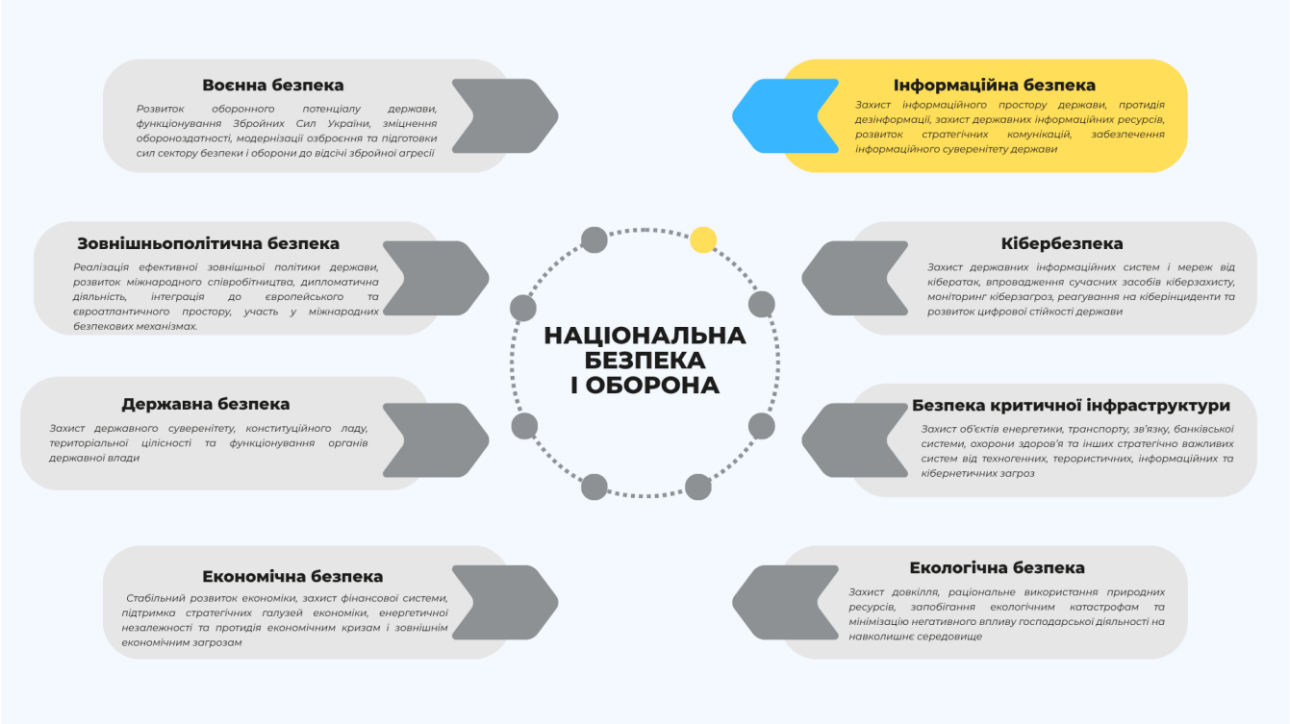


Рис.1 Складові інформаційної безпеки держави.

Інформаційна безпека України - складова частина національної безпеки України, стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, існує

ефективна система захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом.

Базовою характеристикою інформаційної безпеки слід вважати імовірність появи загрози підвищеного ризику реалізації загрози або небезпеки для індивіда, суспільства та держави. Критерієм ефективності забезпечення інформаційної безпеки є високий рівень безпеки при мінімумі відповідних витрат. Отже, можна говорити про структуру поняття інформаційної безпеки. Основним її елементом є життєво важливі інтереси соціальної системи, які співвідносяться із зовнішніми чинниками у вигляді інтересів наднаціональних або інших національно-державних структур у межах міжнародного співтовариства. Зсередини національно-державного утворення його життєво важливі інтереси перебувають у взаємодії з інтересами елементів, які складають це утворення. У ролі останніх виступають соціальні групи, еліта, організації, партії, релігійні та етнічні утворення, рухи тощо. Сукупність внутрішніх і зовнішніх інформаційних загроз створюють передумови для порушення безпечного функціонування системи державного управління. Вагомість інформаційно-комунікаційних процесів у сучасному світі дає підстави розглядати забезпечення інформаційної безпеки як одне з глобальних і пріоритетних завдань органів державного управління, вирішенню якого мають бути підпорядковані політична, економічна, воєнна, культурна та інші види діяльності системи державного управління.

Термін «забезпечення інформаційної безпеки» означає діяльність, сукупність заходів і загалом здатність суспільства і держави гарантувати бажаний захищений стан.

Забезпечення інформаційної безпеки передбачає наявність трьох складових: діяльність, засоби та суб’єкти (рис.2).



Рис.2 Складові забезпечення інформаційної безпеки.

З огляду на виділення двох складових інформаційної безпеки держави, суспільства (інформаційно-технічної та інформаційно-психологічної), визначають дві групи об'єктів інформаційної безпеки:

- соціальні:

особа - її права та свободи в інформаційній сфері, психіка, в т.ч. свідомість та підсвідоме, особиста інформація;

суспільство - його духовні цінності, засади солідарної діяльності;

держава - її конституційний лад, суверенітет, ефективне функціонування;

- технічні: інформаційні ресурси, інформаційно-комунікаційна інфраструктура, в тому числі інформаційно-комунікаційні системи різного масштабу і різного призначення, технології та засоби обробки, зберігання, передавання інформації.

Групи об'єктів інформаційної безпеки наведено на (рис.3).



Рис 3. Об'єкти інформаційної безпеки.

Суб'єктами забезпечення інформаційної безпеки є:

- держава, яка здійснює функції у цій галузі через органи законодавчої, виконавчої та судової влади;
- комерційні, громадські, інші організації та об'єднання;
- громадяни, які відповідно до законодавства мають права й обов'язки щодо участі у забезпеченні безпеки держави.

Головну роль при цьому відіграє держава, яка відповідно до чинного законодавства повинна забезпечувати інформаційну безпеку на рівні особи (дотримання прав і свобод особи в інформаційній сфері, сприяння формуванню раціонального, критичного мислення на основі принципів свободи вибору, забезпечення захисту конфіденційної інформації особи), суспільства (формування якісного інформаційно-аналітичного простору, забезпечення плюралізму, багатоканальності отримання інформації, незалежної діяльності ЗМІ) і держави (інформаційно-аналітичне забезпечення діяльності державних органів, інформаційне забезпечення внутрішньої і зовнішньої політики держави, функціонування системи захисту інформації з обмеженим доступом, протидія правопорушенням в інформаційній сфері, комп'ютерним злочинам тощо).

Держава — формує державну політику у сфері інформаційної безпеки, створює нормативно-правову базу та забезпечує захист національного інформаційного простору.

Органи державної влади — здійснюють контроль, координацію та реалізацію заходів із інформаційної та кібербезпеки. В Україні до них належать, зокрема:

- Рада національної безпеки і оборони України,
- Служба безпеки України,
- Державна служба спеціального зв'язку та захисту інформації України,
- Міністерство оборони України,
- Генеральний штаб ЗСУ,
- Національна поліція України,
- Міністерство цифрової трансформації України,
- Національна рада України з питань телебачення і радіомовлення,
- Міністерство культури та стратегічних комунікацій України.
- Центр протидії дезінформації,
- Державна служба України з надзвичайних ситуацій,
- Міністерство внутрішніх справ України.

Підприємства, установи та організації — забезпечують захист власних інформаційних систем, мереж і ресурсів від загроз та несанкціонованого доступу.

Громадяни — дотримуються правил інформаційної безпеки, захищають персональні дані та відповідально використовують інформаційні ресурси.

Міжнародні організації та партнери — сприяють міжнародному співробітництву у сфері кібербезпеки та протидії інформаційним загрозам.

Наукові та освітні установи — здійснюють дослідження, підготовку фахівців і розробку нових технологій захисту інформації.

Взаємодію суб'єктів інформаційної безпеки наведено на (рис.4).



Рис.4. Взаємодія суб’єктів інформаційної безпеки.

У залежності від об’єктного складу (особи, суспільства або держави, що є об’єктом) визначають такі види інформаційної безпеки:

- особисту (безпеку конкретної особи),
- суспільну (безпека суспільства),
- державну (безпеку окремої держави),
- міжнародну (безпеку багатьох держав, світового співтовариства загалом).

Основні аспекти інформаційної безпеки:

- забезпечення доступу суб'єктів до повної, достовірної інформації для їх життєдіяльності, освіти та розвитку, реалізації прав та обов'язків в суспільстві;
- захист суб'єкта від деструктивних інформаційних впливів;
- реалізація гарантій конституційних прав і свобод людини і громадянина, що стосуються діяльності в інформаційній сфері,
- захист від несанкціонованого впливу на інформацію, що належить суб'єкту (охорона персональних даних, державної таємниці, службової інформації та інших видів інформації обмеженого доступу);
- захист інформаційної інфраструктури групи суб'єктів (організації, держави) від руйнівних впливів (випадкових або навмисних, природного або штучного характеру).

Як зазначають вітчизняні дослідники В. Бондаренко та О. Литвиненко, основними цілями політики інформаційної безпеки Україні є такі:

- реалізація конституційних прав громадян, суспільства та держави на інформацію;
- захист інформаційного суверенітету України, зокрема, національного інформаційного ресурсу, систем формування суспільної свідомості;
- забезпечення рівня інформаційної достатності для прийняття рішень державним установам, підприємствам та громадянам;
- належна присутність країни у світовому інформаційному просторі.

Виходячи з цього, завданнями політики забезпечення інформаційної безпеки можна вважати:

а) виявлення, оцінка та прогнозування поведінки джерел загроз інформаційній безпеці, що здійснюється шляхом оперативного моніторингу інформаційної обстановки;

б) вироблення, координація та введення єдиної державної політики у галузі інформаційної безпеки;

в) створення та експлуатація систем забезпечення інформаційної безпеки;

г) розробка, координація та запровадження єдиної державної політики в галузі міжнародних інформаційних відносин, зокрема у напрямку формування іміджу держави.

Інформаційна безпека забезпечує захист інформаційного суверенітету держави, інформаційної інфраструктури, державних інформаційних ресурсів та суспільної свідомості від внутрішніх і зовнішніх загроз. Вона спрямована на недопущення негативного інформаційного впливу, маніпулювання громадською думкою, поширення дезінформації, інформаційної пропаганди та втручання у функціонування державних інформаційних систем.

Особливого значення інформаційна безпека набуває в умовах глобалізації та розвитку цифрових технологій. Сучасні інформаційні загрози мають значний вплив на політичну стабільність, економіку, діяльність органів державної влади та обороноздатність країни. У зв’язку з цим інформаційна безпека стала одним із пріоритетних напрямів державної політики у сфері національної безпеки.

1.2. Інформаційна безпека держави в системі національної безпеки України як наукова проблема

Інформація проявляється в інформаційних процесах в природі, в суспільстві і техніці, а також в процесі розумової діяльності людини щодо сприйняття навколишньої дійсності. «Відкриття» поняття інформації сучасною наукою відбулося в середині XX століття і, на сьогодні представлено багато підходів до розуміння поняття «інформація», які часто несумісні і протирічать одна одній. На думку засновника вчення про кібернетику Н. Вінера, інформація є інформація, а не матерія і не енергія. З цього визначення випливає, що інформація - не існуючий реально об'єкт, а розумова абстракція, тобто вона є створена людським розумом. Однією з перших є статистична теорія інформації, розроблена К. Шенноном і викладена в серії його робіт в 1948 році. Саме він увів термін «інформація», яку розумів у вузькому технічному аспекті, основний акцент робив на кількісній її оцінці. Недоліком подібного підходу є те, що він абстрагується від осмисленості і цінності інформації для споживача.

У науковій літературі, а також на рівні національного законодавства існує досить багато варіантів визначення поняття інформаційної безпеки. Основну групу становлять бачення, у рамках яких інформаційну безпеку держави розглядають як стан, тенденції розвитку, умови життєдіяльності соціуму, його структур, інститутів і установ, за яких забезпечується збереження їх якісного, вільного, відповідного власній природі та інноваційного функціонування.

Деякі науковці розглядають інформаційну безпеку через призму розвитку інформаційного простору держави, суспільства і розуміють під нею стан захищеності інформаційного середовища, за якого забезпечується його формування, використання й розвиток в інтересах особистості, суспільства, держави незалежно від впливу внутрішніх та зовнішніх інформаційних загроз. Під інформаційним середовищем мають на увазі сферу діяльності суб'єктів, пов'язану із створенням, обробленням та обміном інформації.

Проблематику інформаційної безпеки досліджувало багато зарубіжних та українських вчених, які розглядали її як складову національної безпеки, інформаційного суспільства та державного управління.

Наприклад, М. Кастельс, який досліджував інформаційне суспільство, мережеві комунікацій та вплив інформації на державу і суспільство, у своїй праці The Information Age: Economy, Society and Cuiture описав перехід людства до інформаційної епохи, у якій інформація та знання стають основою влади, а цифрові комунікацій формують новий тип суспільства. Він пояснив, як інформаційні впливи можуть змінювати політичні та соціальні процеси, описав роль кіберпростору як важливого елементу державної безпеки. Його ідеї стали основою для дослідження інформаційних війн, розвитку концепції кібербезпеки, формуванню державної інформаційної політики та вивченню цифрової стійкості держав.

Серед українських науковців значний внесок у дослідження інформаційної безпеки зробив Георгій Почепцов — один із провідних фахівців у сфері інформаційних війн, стратегічних комунікацій та інформаційного впливу. У

своїх працях він обґрунтував, що інформаційний простір є окремою сферою протиборства між державами, а інформаційні операції стали важливим інструментом сучасної гібридної війни. Науковець досліджував механізми формування суспільної думки, маніпулятивні технології та роль масових комунікацій у забезпеченні національної безпеки.

Важливий внесок у розвиток теоретичних засад національної та інформаційної безпеки України зробив Володимир Горбулін. У своїх дослідженнях він акцентував увагу на необхідності формування системного підходу до забезпечення національної безпеки держави в умовах сучасних гібридних загроз. Учений наголошував на важливості інтеграції інформаційної, кібернетичної та воєнної складових безпеки в єдину систему державного управління.

Проблеми правового забезпечення інформаційної безпеки та інформаційного суверенітету держави досліджував Володимир Ліпкан. У своїх працях він розглядав інформаційну безпеку як складову національної безпеки та визначав механізми державного управління у сфері захисту інформаційного простору. Значну увагу вчений приділяв питанням нормативно-правового регулювання інформаційних відносин та формуванню державної інформаційної політики.

Питання інформаційної безпеки в контексті філософії, соціальних комунікацій та розвитку інформаційного суспільства досліджували також Олександр Дзьобань, Валерій Петрик, Дмитро Дубов та інші українські науковці. У своїх роботах вони аналізували сучасні інформаційні загрози, механізми протидії дезінформації, розвиток стратегічних комунікацій та забезпечення інформаційної стійкості держави.

Після початку повномасштабної агресії Російської Федерації проти України значна увага українських науковців зосереджена на дослідженні гібридної війни, інформаційно-психологічних операцій, кіберзагроз та механізмів забезпечення стійкості державних інституцій до зовнішніх інформаційних впливів. Це сприяло активному розвитку наукових досліджень у сфері інформаційної та

кібернетичної безпеки, а також удосконаленню державної політики у сфері захисту національного інформаційного простору.

Інформаційна безпека є складною багатовимірною категорією, яка формується на стику багатьох наукових напрямів. Її дослідження здійснюється у межах державного управління, права, політології, соціології, психології, кібернетики, інформаційних технологій та військових наук. Саме міждисциплінарний характер обумовлює існування великої кількості підходів до трактування сутності інформаційної безпеки та механізмів її забезпечення.

У науковому середовищі відсутнє єдине універсальне визначення поняття «інформаційна безпека». Одні дослідники розглядають її як стан захищеності інформаційного простору держави від внутрішніх і зовнішніх загроз. Інші — як систему суспільних відносин, спрямованих на захист національних інтересів в інформаційній сфері. Частина науковців акцентує увагу на технічному аспекті інформаційної безпеки, ототожнюючи її з кібербезпекою та захистом інформаційно-комунікаційних систем, тоді як інші підкреслюють гуманітарний аспект, пов’язаний із захистом суспільної свідомості від деструктивних інформаційних впливів.

Наукові дискусії також стосуються співвідношення понять «інформаційна безпека», «кібербезпека», «інформаційний суверенітет», «інформаційна стійкість» та «інформаційна оборона». Зокрема, кібербезпека часто розглядається як складова інформаційної безпеки, яка зосереджується переважно на технічному захисті інформаційних систем і мереж. Водночас інформаційна безпека охоплює ширший спектр питань, включаючи захист суспільства від пропаганди, дезінформації, психологічних операцій та маніпулятивних інформаційних впливів.

Особливої актуальності наукові дослідження інформаційної безпеки набули в умовах розвитку інформаційного суспільства та цифрової трансформації державного управління. Швидке поширення цифрових технологій, електронних комунікацій, соціальних мереж і систем електронного урядування створює нові можливості для розвитку держави, але одночасно формує нові інформаційні

ризики та загрози. У зв’язку з цим виникає необхідність розроблення комплексних механізмів забезпечення інформаційної безпеки, які б поєднували правові, організаційні, технічні та комунікаційні інструменти.

Крім того, інформаційна безпека є динамічним явищем, що постійно змінюється під впливом розвитку технологій, геополітичної ситуації та трансформації форм інформаційного протиборства. Сучасні інформаційні війни, кібератаки, використання штучного інтелекту для інформаційних операцій, маніпулювання громадською думкою через цифрові платформи та соціальні мережі формують нові виклики для держави та суспільства. Це потребує постійного оновлення наукових підходів до розуміння сутності інформаційної безпеки та вдосконалення механізмів її забезпечення.

Таким чином, інформаційна безпека держави виступає не лише практичною сферою забезпечення захисту національних інтересів, а й важливою науковою проблемою, яка потребує комплексного міждисциплінарного дослідження та формування сучасної моделі державної інформаційної політики.

1.3. Нормативно-правове забезпечення інформаційної безпеки в Україні

Інформаційна безпека в Україні забезпечується системою нормативно-правових актів, які регулюють діяльність держави у сфері захисту інформаційного простору, інформаційних ресурсів, кібербезпеки та критичної інформаційної інфраструктури. Нормативно-правове забезпечення інформаційної безпеки є важливим елементом державної політики у сфері національної безпеки та спрямоване на створення ефективного механізму протидії сучасним інформаційним загрозам.

Основу нормативно-правового регулювання у сфері інформаційної безпеки в Україні становить Конституція України, яка закріплює право громадян на інформацію, захист персональних даних, свободу слова та гарантує захист суверенітету і національної безпеки держави. Конституція визначає, що забезпечення інформаційної безпеки є однією з найважливіших функцій держави.

Зокрема, у статті 17 Конституції України вказано: «Захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу», це положення закріплює інформаційну безпеку як одну з ключових складових національної безпеки держави нарівні з воєнною та економічною безпекою.

Стаття 32 Конституції України містить положення щодо захисту інформації про особу:

«Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах захисту персональних даних, інформаційної приватності та обмеження незаконного доступу до інформації.

Стаття 31 Конституції України гарантує таємницю листування, телефонних розмов та інших комунікацій: «Кожному гарантується таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції». Ця норма є основою: захисту електронних комунікацій, кіберзахисту приватних даних, безпеки телекомунікаційних систем.

Стаття 34 Конституції України гарантує право на інформацію та свободу слова: «Кожному гарантується право на свободу думки і слова, на вільне вираження своїх поглядів і переконань». Ця стаття закріплює право вільно збирати, зберігати, використовувати, поширювати інформацію.

Але водночас Конституція дозволяє обмеження цього права: «…в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання правопорушенням чи злочинам, для охорони здоров’я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя». Ця норма створює конституційний баланс між свободою інформації та необхідністю забезпечення інформаційної безпеки держави.

Закон України від 2 жовтня 1992 року № 2657-XII «Про інформацію» є базовим законом у сфері інформаційних відносин. Він визначає поняття інформації; права та обов'язки суб'єктів інформаційних відносин; види інформації; порядок доступу до інформації; основи захисту інформації. цей закон закладає правові основи інформаційного суверенітету та захисту інформаційних прав громадян.

Закон України від 21 червня 2018 року № 2469-VIII «Про національну безпеку України» визначає основи та принципи державної політики у сфері національної безпеки. Інформаційна безпека розглядається як одна зі складових національної безпеки держави. Закон визначає загрози національним інтересам в інформаційній сфері та суб'єктів забезпечення безпеки та закріплює необхідність забезпечення інформаційної та кібернетичної безпеки як важливого напряму державної політики в умовах сучасних гібридних загроз.

Закон України «Про захист інформації в інформаційно-комунікаційних системах» від 5 липня 1994 року № 80/94-ВР регулює питання технічного та криптографічного захисту інформації в державних інформаційних системах. Закон визначає: вимоги до комплексних систем захисту інформації; порядок захисту державних інформаційних ресурсів; відповідальність за порушення вимог інформаційної безпеки.

Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII - це ключовий нормативний акт у сфері кібербезпеки. Він визначає: основи національної системи кібербезпеки, встановлює повноваження державних органів, регламентує захист критичної інформаційної інфраструктури, визначає поняття кіберзагроз та кібератак. У цьому законі кібербезпека розглядається як складова інформаційної безпеки держави.

Закон України «Про державну таємницю» від 21 січня 1994 року № 3855-XII визначає порядок охорони інформації, що становить державну таємницю, та механізми її захисту в інтересах національної безпеки.

Закон України «Про захист персональних даних» від 1 червня 2010 року № 2297-VI регулює питання захисту персональних даних та інформаційної приватності громадян відповідно до європейських стандартів.

Стратегія інформаційної безпеки України, введена в дію Указом Президента України від 28 грудня 2021 року № 685/2021 визначає актуальні виклики та загрози інформаційній безпеці України в інформаційній сфері. Стратегічні цілі та завдання, спрямовані на протидію таким загрозам, на захист прав осіб на інформацію та захист персональних даних. Особлива увага приділяється протидії інформаційній агресії Російської Федерації. Основними напрямами забезпечення інформаційної безпеки України є стійкість та взаємодія, для яких потрібно виконати відповідні цілі та завдання, наведені Стратегії (7 Стратегічних цілей).

Стратегія кібербезпеки України, уведена в дію Указом Президента України від 26 серпня 2021 року № 447/2021 визначає пріоритети державної політики у сфері кіберзахисту, розвитку національної системи кібербезпеки та захисту критичної інфраструктури та акцентує увагу на необхідності забезпечення кіберстійкості держави в умовах гібридної війни. Забезпечення кібербезпекиє одним із пріоритетів у системі національної безпеки України та буде здійснюватися шляхом посилення спроможностей національної системи кібербезпеки для протидії кіберзагрозам у сучасному безпековому середовищі.
У документі передбачено посилення захисту державних інформаційних ресурсів, вдосконалення системи реагування на кібератаки та координацію діяльності суб’єктів кібербезпеки.

Постанова Кабінету Міністрів України від 19 червня 2019 року № 518 «Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури». У документі визначено базові вимоги до кіберзахисту критичної інфраструктури, порядок організації систем захисту таких об, вимоги до управління кіберризиками та механізми реагування на кіберінциденти.

Постанова Кабінету Міністрів України від 21 лютого 2025 р. №205 «Деякі питання створення, адміністрування та забезпечення функціонування засобу

інформатизації» визначає організаційні та процедурні засади створення, модернізації та введення в експлуатацію засобів інформатизації у державних органах. Документ регламентує порядок реалізації проєктів інформатизації, вимоги до документації, процедури введення систем у промислову експлуатацію та контроль за функціонуванням засобів інформатизації.

Що стосується інформаційної і кібербезпеки, то постанова має важливе значення для впровадження систем кіберзахисту, NAC, систем моніторингу безпеки та інших державних ІТ-рішень.

Сучасна система нормативно-правового забезпечення інформаційної безпеки України потребує подальшого вдосконалення. Це пов’язано зі стрімким розвитком цифрових технологій, появою нових кіберзагроз, поширенням дезінформації та необхідністю забезпечення ефективного функціонування системи державного управління у сфері інформаційної безпеки.

Одним із пріоритетних напрямів удосконалення законодавства є:

- гармонізація українського законодавства з європейськими стандартами;
- удосконалення механізмів захисту критичної інформаційної інфраструктури;
- розвиток механізмів міжвідомчої взаємодії;
- удосконалення правового регулювання цифрового середовища.

Таким чином, нормативно-правове забезпечення інформаційної безпеки України є важливим інструментом реалізації державної політики у сфері національної безпеки та створює правові основи для захисту інформаційного простору держави, протидії сучасним інформаційним загрозам та забезпечення кіберстійкості України.

1.4. Міжнародний досвід у формуванні інформаційної безпеки держави

У сучасних умовах забезпечення інформаційна безпека є одним із пріоритетних напрямів державної політики більшості розвинених країн світу. Стрімкий розвиток цифрових технологій, глобалізація інформаційного простору, поширення кібератак та інформаційних операцій зумовили необхідність

формування ефективних систем захисту інформаційного середовища держави. Зарубіжний досвід свідчить, що успішне забезпечення інформаційної безпеки можливе лише за умов комплексного підходу, який поєднує нормативно-правові, організаційні, технічні та управлінські механізми.

Американська модель інформаційної безпеки формувалася поступово під впливом глобалізації, розвитку цифрових технологій, терористичних загроз, кібератак та інформаційних операцій іноземних держав.

Одним із ключових елементів американської моделі є Національна стратегія кібербезпеки (National Cyber Strategy), яка базується на принципах активного кіберзахисту, стримування кіберзагроз, розвитку кіберстійкості держави, міжнародної співпраці, захисту демократичних інституцій від інформаційного впливу.

У Стратегії визначено основні загрози інформаційній та кібернетичній безпеці, напрями державної політики, механізми реагування на кіберзагрози, захист критичної інфраструктури, співпрацю держави та приватного сектору.

Ключову роль у забезпеченні інформаційної та кібернетичної безпеки США виконує Cybersecurity and Infrastructure Security Agency (CISA), створене у структурі Міністерства внутрішньої безпеки США. CISA координує взаємодію між: федеральними органами, приватним сектором, енергетичними компаніями, фінансовими установами та телекомунікаційними операторами.

Основними функціями CISA є:

- моніторинг кіберзагроз;
- реагування на кіберінциденти;
- координація захисту критичної інфраструктури;
- обмін інформацією про загрози;
- співпраця з приватними компаніями;
- захист державних інформаційних ресурсів.

За даними CISA (Cybersecurity and Infrastructure Security Agency), основними кіберзагрозами для державних органів, критичної інфраструктури та суспільства

у 2025 році роках залишаються ransomware-атаки, фішинг, експлуатація вразливостей та атаки на критичну інфраструктуру.

Ransomware (програми-вимагачі/шифрувальники) став однією з наймасовіших кіберзагроз для критичної інфраструктури США. За даними FBI IC3 та CISA, у 2024 році кількість скарг щодо ransomware-атак на критичну інфраструктуру) зросла на 9% порівняно з 2023 роком.

У 2025 році FBI отримало понад 3600 повідомлень про ransomware-інциденти із загальними збитками понад 32 млн доларів.

Найчастіше атаки спрямовувались на:критичне виробництво, медичні установи, державні органи, фінансовий сектор, IT-компанії.

За даними CISA та Verizon DBIR 2025: фішингові атаки залишаються одним із головних векторів проникнення у федеральних мережах: системне вторгнення становило 65% інцидентів, пов’язаних із зовнішніми атаками, а ransomware фігурував у 44% усіх розслідуваних порушень безпеки.

У 2025 році CISA заблокувала 2,62 млрд шкідливих з’єднань у федеральних мережах і ще 371 млн — у середовищах критичної інфраструктури.

CISA підтримує каталог Known Exploited Vulnerabilities (KEV), який містить перелік вразливостей, що активно експлуатуються зловмисниками. Згідно даних каталогу у 2025 році зафіксовано рекордне зростання кількості нових вразливостей, і більшість з них виявлено за перше півріччя 2025 року (21 000).

Американська модель інформаційної безпеки активно використовує стандарти National Institute of Standards and Technology (NIST). Стандарти NIST є основою американської моделі інформаційної та кібернетичної безпеки. Вони визначають механізми управління кіберризиками, вимоги до захисту інформаційних систем, реагування на кіберінциденти та забезпечення стійкості державної і критичної інфраструктури до сучасних кіберзагроз.

Найвідомішими з них є NIST Cybersecurity Framework, NIST SP 800-53, NIST SP 800-171. Зазначені стандарти використовуються в державних органах, секторі оборони, критичній інфраструктурі та приватних компаніях.

National Institute of Standards and Technology Cybersecurity Framework (NIST Cybersecurity Framework) — це базова модель управління кібербезпекою, розроблена для державних органів і приватних організацій США. Стандарт визначає основні процеси забезпечення кібербезпеки та управління ризиками.

Framework складається з п’яти основних функцій:

Identify (ідентифікація загроз і активів);

Protect (захист систем і даних);

Detect (виявлення інцидентів);

Respond (реагування на інциденти);

Recover (відновлення після атак).

Стандарт широко використовується для побудови систем управління інформаційною безпекою та оцінки кіберризиків.

NIST SP 800-53 — це набір вимог і контролів безпеки для державних інформаційних систем США.

Документ містить:

вимоги до контролю доступу;

аудит і моніторинг;

управління ризиками;

реагування на інциденти;

захист мереж;

безперервність функціонування;

захист персональних даних.

Стандарт використовується федеральними органами США та організаціями критичної інфраструктури для побудови комплексної системи кіберзахисту.

NIST SP 800-171 визначає вимоги до захисту контрольованої некласифікованої інформації (CUI) у недержавних інформаційних системах.

Документ встановлює вимоги щодо: автентифікації користувачів, шифрування даних, контролю доступу, захисту мереж, журналювання подій та реагування на кіберінциденти.

Стандарт широко застосовується компаніями-підрядниками, які працюють із державними органами США, зокрема у сфері оборони та критичної інфраструктури.

Досвід Естонії, це ще один успішний приклад побудови сучасної моделі інформаційної та кібернетичної безпеки держави. Естонія вважається однією з найбільш цифровізованих держав світу та прикладом ефективного поєднання електронного урядування, цифрової трансформації та високого рівня кіберстійкості держави.

Формування сучасної системи інформаційної безпеки Естонії значною мірою було зумовлене масштабними кібератаками 2007 року, коли державні інформаційні ресурси країни зазнали серії потужних DDoS-атак.

У результаті кібератак було тимчасово порушено роботу державних електронних сервісів, банківських систем та засобів масової інформації. Ці події стали одним із перших прикладів масштабної кібератаки на державу та продемонстрували критичну залежність сучасного суспільства від цифрової інфраструктури.

Враховуючи зазначене, Естонія суттєво переглянула підходи до забезпечення інформаційної та кібернетичної безпеки. Основою естонської моделі стала інтеграція кібербезпеки у систему національної безпеки та цифрового державного управління. Держава почала активно інвестувати у розвиток систем кіберзахисту та захист критичної інфраструктури, цифрову ідентифікацію, резервування державних даних, кіберосвіту та міжнародне співробітництво у сфері кібербезпеки.

Після кібератак 2007 року було створено систему резервування державних даних та цифрової безперервності функціонування держави. Естонія стала однією з перших країн, яка впровадила концепцію «data embassy» — цифрових дата-центрів за межами держави для резервного зберігання критично важливих державних даних.

Однією з ключових особливостей естонської моделі є високий рівень цифровізації державного управління. У країні функціонує система електронного

урядування (e-Government), яка забезпечує надання більшості державних послуг в електронній формі. Громадяни Естонії мають можливість: використовувати електронний підпис, отримувати доступ до державних реєстрів через єдину цифрову систему та отримувати державні послуги онлайн, голосувати через Інтернет, реєструвати бізнес дистанційно.

Основою цифрової інфраструктури Естонії є система X-Road — захищена платформа обміну даними між державними органами, банками, медичними установами та іншими суб'єктами інформаційних відносин. Система забезпечує: захищений обмін даними, автентифікацію користувачів та журналювання доступу, цілісність інформації та криптографічний захист інформації.

Важливою складовою моделі інформаційної безпеки Естонії є система цифрової ідентифікації громадян. Кожен громадянин має електронну ID-картку, яка використовується для доступу до державних сервісів, отримання медичних та фінансових послуг, електронного підпису, електронного голосування.

Значну увагу Естонія приділяє міжнародному співробітництву у сфері кібербезпеки. В Таллінні знаходиться Центр передового досвіду НАТО з кібероборони — NATO Cooperative Cyber Defence Centre of Excellence, який займається дослідженнями у сфері кібербезпеки, навчанням фахівців та проведенням міжнародних кібернавчань, розробленням рекомендацій щодо кібероборони.

6 травня 2023 року Україна стала повноцінним членом Об'єднаного центру передових технологій з кібероборони НАТО (CCDCOE) зі статусом країни-контрибутора. З цієї нагоди у Центрі, що знаходиться в Таллінні (Естонська Республіка), відбулася спеціальна церемонія підняття прапору нашої держави як нового члена CCDCOE.

Естонська модель також характеризується високим рівнем взаємодії держави та суспільства у сфері кібербезпеки. У країні активно розвивається кіберосвіта, проводяться програми підвищення цифрової грамотності населення, навчання державних службовців та спеціалістів із кібербезпеки.

Для України досвід Естонії є особливо актуальним у контексті цифрової трансформації державного управління та розвитку електронних сервісів, в частині, що стосується впровадження захищених систем електронного урядування, створення систем резервування державних даних, інтеграції кібербезпеки у цифрову трансформацію держави, забезпечення кіберстійкості критичної інфраструктури.

Висновки до розділу 1

У результаті проведеного дослідження можна зробити висновок, що інформаційна безпека є однією з ключових складових національної безпеки держави та важливою складовою захисту державного суверенітету, суспільної стабільності й національних інтересів. В умовах цифрової трансформації та розвитку інформаційного суспільства інформаційний простір став окремою сферою стратегічного протистояння, у межах якого проводяться інформаційно-психологічні операції, кібератаки, маніпулятивні інформаційні впливи та кампанії з поширення дезінформації.

У роботі проаналізовано основні теоретичні підходи до розуміння понять «інформація» та «інформаційна безпека». Визначено, що інформаційна безпека поєднує інформаційно-технічну й інформаційно-психологічну складові. Її забезпечення охоплює захист інформаційних ресурсів, державних інформаційних систем, критичної інформаційної інфраструктури, а також суспільної свідомості від деструктивних інформаційних впливів.

Визначено, що сучасні інформаційні загрози характеризуються підвищеною динамічністю та комплексністю. Особливо небезпечними для України є кібератаки, дезінформація, інформаційно-психологічні операції та втручання у функціонування державних інформаційних ресурсів, їх детально розглянуто в цьому розділі. Аналіз системи інформаційної безпеки дає змогу зробити висновок, що ефективна система інформаційної безпеки повинна ґрунтуватися на поєднанні стратегічних комунікацій, моніторингу інформаційного простору, кіберзахисту, розвитку медіаграмотності населення та міжвідомчої координації.

У дослідженні проаналізовано нормативно-правове забезпечення інформаційної безпеки України. Встановлено, що основу правового регулювання становлять нормативно-правові акти з питань інформаційної та кібербезпеки, які визначають пріоритети державної політики цій сфері, визначають механізми протидії кіберзагрозам та забезпечення національних інтересів від дезінформації та ворожих впливів. Доведено, що сучасні виклики потребують подальшого вдосконалення законодавства та гармонізації його з міжнародними стандартами.

Дослідження міжнародного досвіду доводить, що ефективне забезпечення інформаційної безпеки можливе лише за умов комплексного підходу, який поєднує організаційні, правові, технічні та комунікаційні механізми. Таким чином, забезпечення інформаційної безпеки держави є одним із пріоритетних напрямів державної політики та важливою умовою забезпечення кіберстійкості держави.

РОЗДІЛ 2 СУЧАСНИЙ СТАН ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

2.1. Загрози та виклики інформаційній безпеці України в сучасних умовах

До основних чинників, що негативно впливають на стан інформаційної безпеки та суспільної стійкості України, належать:

- гібридна агресія та інформаційно-психологічні операції з боку іноземних держав, зокрема Російської Федерації;
- поширення дезінформації, фейкових новин та маніпулятивного контенту;
- кібератаки на державні інформаційні ресурси та критичну інфраструктуру;
- недостатній рівень кіберстійкості окремих державних інформаційних систем;
- використання соціальних мереж і цифрових платформ для інформаційного впливу;
- маніпулювання громадською думкою через інформаційні технології;
- поширення технологій deepfake та AI-генерованого контенту;
- концентрація медіавласності та політичний вплив на інформаційний простір;
- недостатній рівень цифрової грамотності населення;
- залежність від іноземних цифрових сервісів та програмного забезпечення;
- загрози витоку персональних даних і кібершпигунства;
- необхідність подальшого вдосконалення системи стратегічних комунікацій держави.

Основними реальними та потенційними загрозами інформаційній безпеці України є:

1) у зовнішньополітичній сфері:

- поширення у світовому інформаційному просторі викривленої, недостовірної та упередженої інформації, що завдає шкоди національним інтересам України;

- прояви кіберзлочинності, кібертероризму, що загрожують стабільному та безпечному функціонуванню національних інформаційно-комунікаційних систем;
- зовнішні негативні інформаційні впливи на суспільну свідомість і засоби масової інформації, а також Інтернет (соціальні мережі; Telegram, TikTok, YouTube, цифрові платформи, AI-контент, deepfake, бот-мережі), тощо;

2) у сфері державної безпеки:

- негативні інформаційні впливи, спрямовані на підрив конституційного ладу, суверенітету, територіальної цілісності й недоторканності кордонів України;
- використання засобів масової інформації, Інтернету для пропаганди сепаратизму за етнічною, мовною, релігійною й іншими ознаками;
- несанкціонований доступ до інформаційних ресурсів органів державної влади;
- розголошення інформації, яка становить державну та іншу передбачену законодавством таємницю, а також конфіденційної інформації, що є власністю держави;

3) у воєнній сфері:

- порушення встановленого регламенту збирання, оброблення й передавання інформації з обмеженим доступом в органах військового управління та на підприємствах оборонно-промислового комплексу України;
- несанкціонований доступ до інформаційних ресурсів, незаконне збирання та використання інформації з питань оборони;
- реалізація програмно-математичних заходів із метою порушення функціонування інформаційних систем у сфері оборони України;
- перехоплення інформації в телекомунікаційних мережах, радіоелектронне глушіння засобів зв’язку та управління;

- інформаційно-психологічний вплив на населення України, у тому числі особовий склад військових формувань, із метою послаблення їх готовності до оборони держави та погіршення іміджу військової служби;

4) у внутрішньополітичній сфері:

- недостатня розвиненість інститутів громадянського суспільства, недосконаліть партійно-політичної системи, непрозорість політичної та громадської діяльності, що створює передумови для обмеження свободи слова, маніпулювання суспільною свідомістю;
- негативні інформаційні впливи, у тому числі із застосуванням спеціальних засобів, на індивідуальну та суспільну свідомість;
- поширення суб'єктами інформаційної діяльності викривленої, недостовірної та упередженої інформації;

5) в економічній сфері:

- відставання вітчизняних наукоємних і високотехнологічних виробництв, особливо у сфері телекомунікаційних засобів і технологій;
- недостатній рівень інформатизації економічної сфери, зокрема кредитно-фінансової системи, промисловості, сільського господарства, сфери державних закупівель;
- несанкціонований доступ, порушення встановленого порядку роботи з інформаційними ресурсами в галузях національної економіки, викривлення інформації в таких ресурсах;
- використання неліцензованого програмного забезпечення, засобів і комплексів оброблення інформації;
- недостатній рівень розвитку національної інформаційної інфраструктури;

6) у соціальній та гуманітарній сферах:

- відставання України від розвинутих держав за рівнем інформатизації соціальної та гуманітарної сфер, насамперед освіти, охорони здоров'я, соціального забезпечення, культури;

- недодержання прав людини і громадянина на отримання інформації, необхідної для захисту їхніх соціально-економічних прав;
- поширення в ЗМІ деструктивного інформаційного контенту: жорстокості, порнографії, зневажливого ставлення до людської й національної гідності тощо;
- тенденція до витіснення з інформаційного простору та молодіжної культури українських мистецьких творів, народних традицій і форм дозвілля;
- послаблення суспільно-політичної, міжетнічної та міжконфесійної єдності суспільства;
- відставання розвитку українського кінематографу, книговидання, книгорозповсюдження й бібліотечної справи від рівня розвинутих держав;

7) у науково-технічній сфері:

- зниження наукового потенціалу в галузі інформатизації та зв'язку;
- низька конкурентоспроможність вітчизняної інформаційної продукції на світовому ринку;
- відтік за кордон наукових кадрів і суб'єктів права інтелектуальної власності;
- недостатній захист від несанкціонованого доступу до інформації внаслідок використання іноземних інформаційних технологій і техніки;
- неконтрольована експансія сучасних інформаційних технологій, що створює передумови технологічної залежності України;

8) в екологічній сфері:

- приховування, несвоєчасне надання інформації або надання недостовірної інформації населенню про надзвичайні екологічні ситуації чи надзвичайні ситуації техногенного та природного характеру;
- недостатня надійність інформаційно-телекомунікаційних систем збору, обробки й передачі інформації в умовах надзвичайних ситуацій.

Діяльність органів виконавчої влади у сфері забезпечення інформаційної безпеки України має бути зосереджена на конструктивному поєднанні діяльності

держави, громадянського суспільства та людини за трьома головними напрямами:

- інформаційно-психологічному, зокрема щодо забезпечення конституційних прав і свобод людини й громадянина, створення сприятливого психологічного клімату в національному інформаційному просторі для затвердження загальнолюдських та національних моральних цінностей;
- технологічного розвитку, зокрема стосовно розбудови та інноваційного оновлення національних інформаційних ресурсів, впровадження новітніх технологій створення, оброблення та поширення інформації;
- захисту інформації, зокрема щодо забезпечення конфіденційності, цілісності й доступності інформації, у тому числі технічного захисту інформації в національних інформаційних ресурсах від кібернетичних атак.

У зв'язку з посиленням негативного зовнішнього впливу на інформаційний простір України, що загрожує розмиванню суспільних цінностей і національної ідентичності, недостатніми залишаються обсяги вироблення конкурентного національного інформаційного продукту. Стан безпеки інформаційно-комунікаційних систем в галузі державного управління, фінансової і банківської сфери, енергетики, транспорту, внутрішніх та міжнародних комунікацій не на достатньо високому рівні.

Формування сприятливих зовнішніх умов для розвитку та безпеки держави потребує належного рівня забезпечення інформаційної безпеки в процесі інтеграції України до глобального інформаційного суспільства. У сучасних умовах інформаційна безпека є однією з ключових складових національної безпеки держави та визначається як стан захищеності національних інтересів України в інформаційній сфері.

2.2. Кібербезпека в системі інформаційної безпеки держави

У сучасному науковому та нормативно-правовому дискурсі інформаційна безпека та кібербезпека є взаємопов'язаними, але не тотожними поняттями. Традиційно кібербезпека розглядалася як складова інформаційної безпеки, що

забезпечує захист інформаційно-комунікаційних систем та цифрової інфраструктури. Водночас розвиток цифрових технологій, зростання кількості кібератак і поява нових кіберзагроз зумовили виокремлення кібербезпеки в самостійний напрям державної політики у сфері національної безпеки. Саме тому Закон України «Про національну безпеку України» визначає інформаційну безпеку та кібербезпеку як окремі, хоча й взаємопов’язані складові системи національної безпеки держави.

Зокрема, тому що:

- інформаційні загрози – це не лише кіберзагрози, наприклад: поширення фейкової новини про «взяття Києва за 3 дні та капітуляції України» є загрозою інформаційній безпеці, навіть якщо не відбулося жодного зламу інформаційних систем;
- інформаційна війна може відбуватися без кібератак, наприклад: поширення фейкової новини про те, що російські військові окупували Малу Токмачку здійснено з метою деморалізації населення та є елементом інформаційної війни без технічного втручання в інформаційні системи;
- кібербезпека має технічний характер, наприклад: DDoS-атака на об’єкт критичної інфраструктури або зараження інформаційної системи шкідливим програмним забезпеченням (malware) належать до сфери кібербезпеки, оскільки пов’язані із захистом комп’ютерних мереж, серверів та комунікаційних систем;

Але, оскільки інформаційна безпека та кібербезпека направлені на забезпечення стану захищеності життєво важливих інтересів людини, суспільства і держави від деструктивних інформаційних впливів, варто розглядати ці два поняття нерозривно, як важливі складові національної безпеки України.

Також варто зазначити, що інформаційна безпека є як самостійною сферою національної безпеки України, так і невід'ємною складовою кожної із її сфер, у тому числі й кібербезпеки, лежить в основі кібербезпеки. Це обумовлює необхідність розгляду її понять з урахуванням сталого понятєвого апарату і завдань національної безпеки.

Правові та організаційні засади функціонування державної системи кібербезпеки визначаються Законом України «Про основні засади забезпечення кібербезпеки України», який закріплює поняття національної системи кібербезпеки, її суб'єктів та основні напрями державної політики у сфері кіберзахисту.

Відповідно до статті 8 зазначеного Закону, національна система кібербезпеки є сукупністю суб'єктів забезпечення кібербезпеки та взаємопов'язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного і технічного захисту національних інформаційних ресурсів, кіберзахисту об'єктів критичної інфраструктури.

Для більш повного розуміння місця кібезбезпеки у системі інформаційної безпеки держави доцільно розглянути основні поняття, що використовуються у сфері кібербезпеки. У Законі України «Про основні засади забезпечення кібербезпеки України» наведено наступні терміни:

кібербезпека – захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі;

кіберпростір – середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних;

кіберзахист – сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак,

ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем;

інцидент кібератаки (кіберінцидент) - подія або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактора) та/або таких, що мають ознаки можливої (потенційної) кібератаки, які становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами, створюють імовірність порушення штатного режиму функціонування таких систем (у тому числі зриву та/або блокування роботи системи, та/або несанкціонованого управління її ресурсами), ставлять під загрозу безпеку (захищеність) електронних інформаційних ресурсів;

кіберзагроза - наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об’єктів;

Кібербезпека є важливим елементом національної безпеки держави. Через стрімку цифровізацію держави та суспільства, через те, що більшість державних, фінансових, оборонних і комунікаційних процесів сьогодні функціонують за допомогою інформаційних, електронно-комунікаційних та інформаційно-комунікаційних систем, зростає кількість кібератак, витоків даних, кібершпигунства та загроз для критичної інфраструктури, і як наслідок – це негативно впливає на національну безпеку держави.

Об’єктами кібербезпеки є:

1) конституційні права і свободи людини і громадянина;

2) суспільство, сталий розвиток інформаційного суспільства та цифрового комунікативного середовища;

3) держава, її конституційний лад, суверенітет, територіальна цілісність і недоторканність;

4) національні інтереси в усіх сферах життєдіяльності особи, суспільства та держави;

5) об’єкти критичної інфраструктури.

Об’єктами кіберзахисту є:

1) інформаційні, електронні комунікаційні та інформаційно-комунікаційні системи всіх форм власності, в яких обробляються національні інформаційні ресурси та/або які використовуються в інтересах органів державної влади, органів місцевого самоврядування.

2) об’єкти критичної інформаційної інфраструктури;

3) інформаційні, електронні комунікаційні та інформаційно-комунікаційні системи, які використовуються для задоволення суспільних потреб та/або реалізації правовідносин у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу.

Основу формування ефективної системи кібербезпеки України та забезпечення її функціонування складають державні органи та спеціалізовані суб’єкти, які здійснюють координацію, моніторинг, реагування на кіберінциденти, захист державних інформаційних ресурсів та критичної інфраструктури.

Координація діяльності у сфері кібербезпеки як складової національної безпеки України здійснюється Президентом України через очолювану ним Раду національної безпеки і оборони України (через Національний координаційний центр кібербезпеки).

Кабінет Міністрів України є органом, що забезпечує реалізацію державної політики у сфері кібербезпеки та координує діяльності центральних органів виконавчої влади у сфері кіберзахисту.

Відповідно до статті 2 Закон України «Про основні засади забезпечення кібербезпеки України» основними суб’єктами національної системи кібербезпеки є Державна служба спеціального зв’язку та захисту інформації України (Державний центр кіберзахисту та національна команда реагування на кіберінциденти CERT-UA), Національна поліція України (Департамент кіберполіції), Служба безпеки України (Департамент кібербезпеки), Міністерство оборони України та Генеральний штаб Збройних Сил України,

розвідувальні органи України, Національний банк України, Міністерство закордонних справ України, галузеві та регіональні CSIRT.

Основні види кіберзагроз наведено на (рис.5).

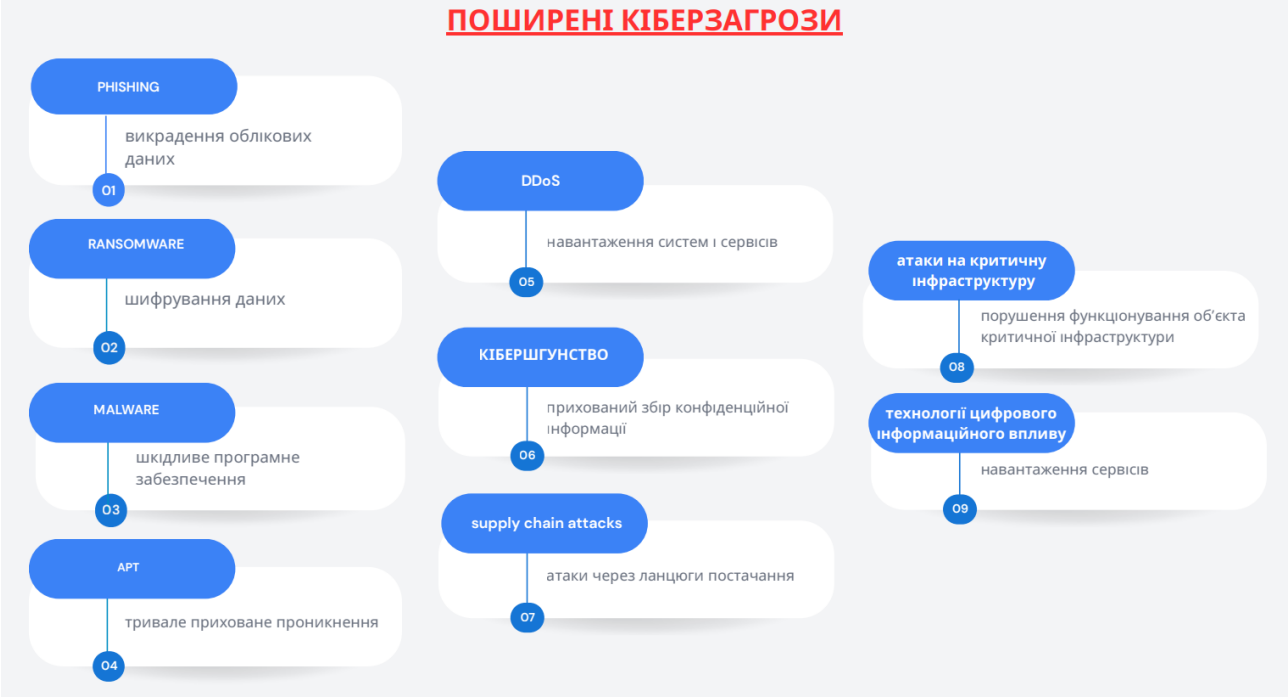


Рис.5. Основні види кіберзагроз.

CERT-UA здійснено ідентифікацію кластерів хакерських угруповань та агентів кіберзагроз, умовних UAC-груп, які здійснюють кібератаки проти державних органів, сектору безпеки і оборони, об'єктів критичної інфраструктури та IT-систем, тощо та систематизовано їх діяльність, що дозволяє відстежувати характер кібератак, аналізувати методи та інструменти атак, прогнозувати потенційні кіберзагрози та відповідним чином реагувати на інциденти.

Основними напрямами діяльності UAC-груп є кібершпигунство, фішинг, розповсюдження шкідливого програмного забезпечення, викрадення облікових даних, атаки на критичну інфраструктуру, компроментація державних інформаційних ресурсів та інформаційно-психологічні операції.

Найбільш активні Ukrainian Cyber Actors (агенти загроз/UAC-групи):

1. UAC-0010 (Gamaredon, Primitive Bear) найактивніше угруповання, підрозділ ФСБ РФ. Щоденне викрадення до 100 000 файлів. Використовують легітимні сервіси (Telegram, Cloudflare, Telegra.ph). У звітах CERT-UA вони згадуються як головна загроза через масовість. Масові розсилки шкідливого ПЗ та динамічна зміна IP-адрес кожні 15 хвилин.

2. UAC-0002 (Sandworm) залишаються найнебезпечнішими в контексті деструктивних операцій, хоча їхніх атак кількісно менше, ніж у Gamaredon. Атакують енергетику, медіа та логістичні вузли. У 2025 році вони фокусувалися на створенні «закладок» для тривалого перебування в мережах критичної інфраструктури.

3. UAC-0001 (APT28, Fancy Bear) – група ГУ ГШ РФ, що відзначається блискавичною швидкістю. Використовують zero-day вразливості (наприклад Microsoft Office), у 2026 році CERT-UA звітував про їхні атаки з використанням вразливості CVE-2026-21509.

4. UAC-0184 спеціалізується на шпигунстві за силами безпеки і оборони України. В 2025-2026 роках відійшли від традиційного фішингу на користь месенджерів (Viber, Signal, WhatsApp). Використовують соціальну інженерію (спілкування з жертвою протягом тижнів) для доставки Remcos RAT.

5. UAC-0252 виявлені на початку 2026 року. Використовують стілери нового покоління (SHADOWSNIFF та SALATSTEALER) для швидкого викрадення паролів та конфіденційних даних.

6. UAC-0255 У березні 2026 року зафіксована їхня кампанія з мімікрії під команду CERT-UA – вони розсилали листи «від імені фахівців з кіберзахисту», щоб заразити системи шкідливою програмою AGEWHEEZE.

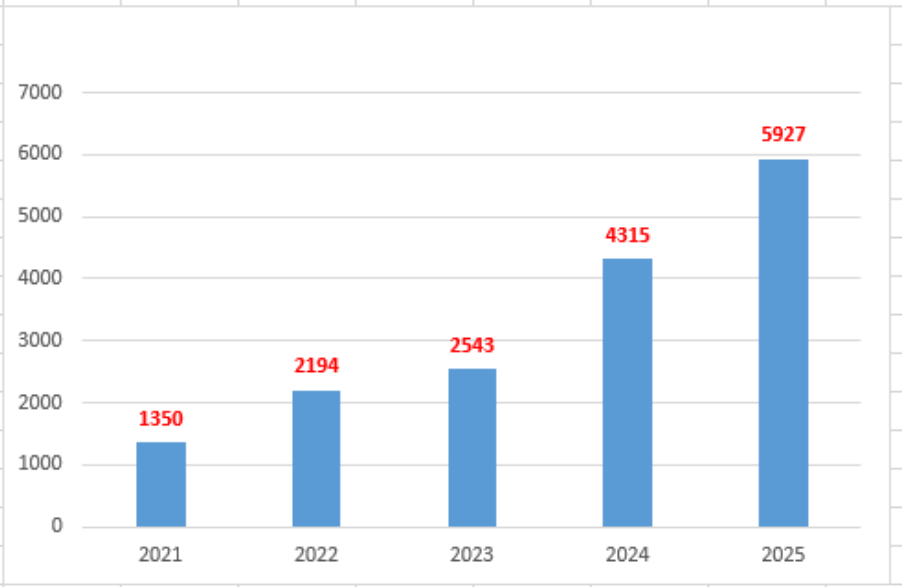
Далі наведено статистичні дані зареєстрованих кіберінцидентів національною командою реагування на кіберінциденти CERT-UA та додано інформацію, отриману студентом в результаті проходження підвищення кваліфікації за напрямом кібербезпеки на національній платформі підготовки керівників з кібербезпеки CDTO CAMPUS на початку 2026 року.

Зростання загальної кількості кіберінцидентів пов’язано із зростанням кількості атак, та зі збільшенням можливості фахівців з кібербезпеки до їх виявлення, підвищення кіберобізнаності населення. Кібершахраї масштабують операції, застосовують автоматизовані масові розсилки та цілеспрямовані атаки силами професійних угрупувань, а це свідчить, що інтенсивність протистояння в кіберпросторі постійно зростає. Російська Федерація продовжує застосовувати комбіновані методи атак в кіберпросторі для отримання стратегічно важливої інформації, зокрема плани Сил оборони України, дані оборонно-промислової сфери, логістичні і фінансові ресурси громадян. Для цих цілей все частіше використовують шкідливе програмне забезпечення для прихованого збору даних. Ці типи атак, а також фішинг, наразі є наймасовішими інструментами зловмисників.

Найбільш поширеними методами, які застосовували зловмисники під час кібератак у 2025 році є: розповсюдження шкідливого програмного забезпечення – 2058 випадків, фішинг – 1727 випадків, зараження шкідливим програмним забезпеченням -988 випадків, компрометація облікових записів – 425 випадків.

Статистичні дані щодо виявлення кіберінцидентів наведено на (рис.6).

Загальна кількість зареєстрованих інцидентів	
рік	*кількість*
2021	1350
2022	2194
2023	2543
2024	4315
2025	5927



Критичні та високопріоритетні інциденти	
рік	*кількість*
2021	403
2022	1048
2023	367
2024	59
2025	12

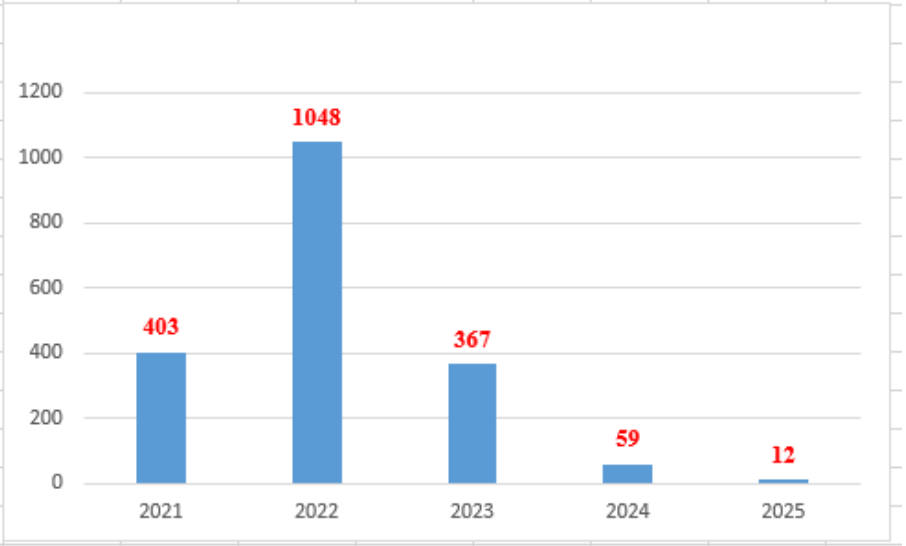


Рис.6. Статистичні дані виявлення інцидентів.

Найчастіше зловмисники здійснюють атаки на органи місцевої влади, урядові організації, сектор оборони, сектор енергетики, комерцію та електронні комунікації (рс.7).

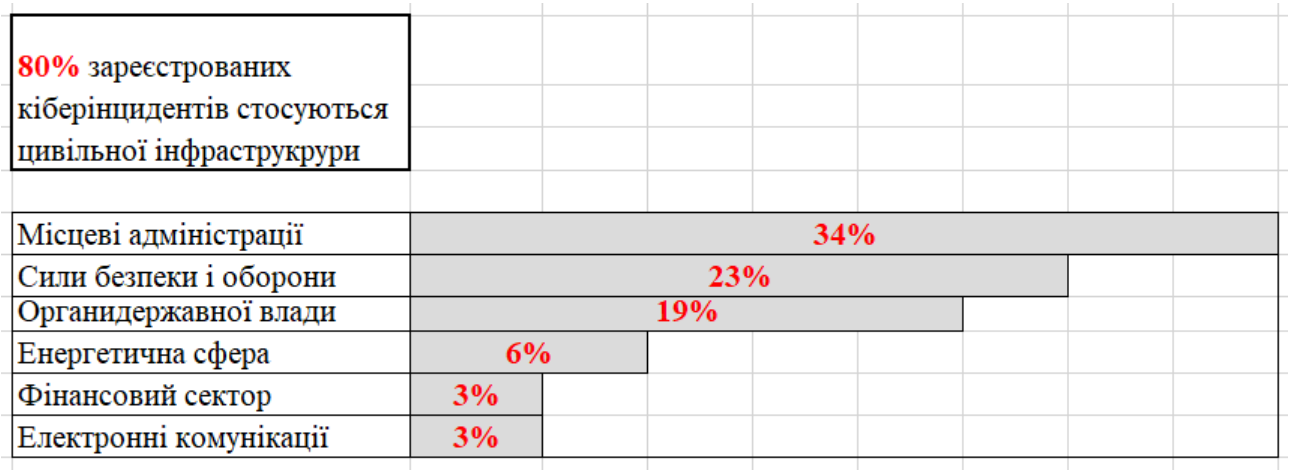


Рис.7. Аналіз кіберінцидентів.

Атаки на критичну інфраструктуру є однією з найбільш небезпечних сучасних кіберзагроз, оскільки спрямовані на порушення функціонування об'єктів і систем, що забезпечують життєдіяльність держави та суспільства. Кібератаки на такі об'єкти можуть призводити до значних економічних збитків, дестабілізації суспільства та створення загроз національній безпеці держави.

2.3. Діяльність органів державної влади у формуванні інформаційної безпеки України

Попри активний розвиток інформаційної безпеки в Україні, сучасний механізм управління у цій сфері все ще має низку проблем і недоліків, які негативно впливають на ефективність захисту національного інформаційного простору та кіберстійкість держави. В умовах воєнного стану в Україні, постійних кібератак та інформаційної агресії ці проблеми набувають особливої актуальності.

Діяльність органів державної влади у сфері формування інформаційної безпеки держави здійснюється відповідно до пріоритетів національної безпеки держави та положень Стратегії інформаційної безпеки. Основною метою такої діяльності є забезпечення захисту національного інформаційного простору, протидія дезінформації та інформаційним операціям, захист прав громадян на

доступ до достовірної інформації, а також зміцнення стійкості держави до сучасних інформаційних та кіберзагроз.

Для мінімізації та нейтралізації інформаційного впливу Російської Федерації Україна реалізує комплекс нормативно-правових, організаційних, технологічних, безпекових та інформаційно-просвітницьких заходів.

Зокрема, сформовано систему стратегічних документів та нормативно-правових актів з питань інформаційної безпеки та протидії дезінформації. Зокрема Радою національної безпеки і оборони України яка уповноважена координувати державну політику у сфері національної, інформаційної та кібербезпеки схвалено Стратегію інформаційної безпеки України, уведену в дію Указом Президента України «Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 в якій визначено, що забезпечення інформаційної безпеки України є однією з найважливіших функцій держави. Зазначена Стратегія визначає актуальні виклики та загрози національній безпеці України в інформаційній сфері, стратегічні цілі та завдання, спрямовані на протидію таким загрозам, захист прав осіб на інформацію та захист персональних даних. Для забезпечення реалізації Стратегії затверджено план заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року (не втратив чинність). У Законі України «Про Раду національної безпеки і оборони України» деталізовано функції РНБО щодо координації та контролю діяльності органів виконавчої влади у сфері національної безпеки; підготовки пропозицій щодо забезпечення інформаційної безпеки; координації заходів із захисту інформаційного простору держави.

На постійній основі удосконалюється законодавство щодо протидії дезінформації, інформаційним операціям та пропаганді держави-агресора, зокрема: Закон України «Про медіа» містить норми щодо заборони пропаганди держави-агресора та обмеження поширення медіаконтенту РФ. Він спрямований на забезпечення реалізації права на свободу вираження поглядів, права на отримання різнобічної, достовірної та оперативної інформації, на забезпечення плюралізму думок і вільного поширення інформації, на захист національних

інтересів України та прав користувачів медіа-сервісів, регулювання діяльності у сфері медіа відповідно до принципів прозорості, справедливості та неупередженості, стимулювання конкурентного середовища, рівноправності і незалежності медіа та визначає правовий статус, порядок формування, діяльності та повноваження Національної ради України з питань телебачення і радіомовлення. На підставі Рішення РНБО, що введене в дію Указом Президента України №106/2021 утворено Центр протидії дезінформації. Основними завданнями Центру визначено: виявлення та аналіз дезінформації; протидія пропаганді; реагування на інформаційні кампанії РФ; запобігання маніпулюванню громадською думкою; координація суб'єктів інформаційної безпеки. Центр протидії дезінформації є державним регулятором щодо застосування санкцій до медіа.

Органи державної влади здійснюють заходи для блокування російських соціальних мереж, медіаплатформ, телеканалів, інтернет-сервісів, тощо які використовуються для поширення пропаганди; блокується діяльність інформаційних мереж впливу; здійснюють моніторинг інформаційного простору на наявність дезінформації, фейків та маніпулятивного контенту; обмежується діяльність окремих медіаструктур та осіб, причетних до інформаційної підтримки агресії РФ.

Прикладом реалізації державної політики щодо захисту інформаційного простору України стало запровадження у 2017 році санкцій проти російських соціальних мереж «ВКонтакте» та «Одноклассники», а також сервісів компаній «Яндекс» і Mail.ru Group. Відповідне рішення РНБО України було введене в дію Указом Президента України №133/2017 та передбачало блокування доступу до зазначених ресурсів з метою протидії російській пропаганді та захисту національної безпеки держави.

Служба безпеки України, розвідувальні органи та інші суб'єкти сектору безпеки здійснюють моніторинг інформаційного простору на предмет наявності медіаресурсів, Telegram-каналів, сайтів, блогерів або організацій, що поширюють російську пропаганду та виправдовують агресію РФ, закликають до

зміни конституційного ладу, поширюють дезінформацію, здійснюють інформаційно-психологічні операції проти України тощо. За результатами аналізу Рада національної безпеки і оборони України розглядає матеріали та ухвалює рішення про застосування персональних, секторальних або спеціальних економічних санкцій.

Відповідне рішення РНБО (санкції) вводиться у дію указом Президента України та стає обов'язковими до виконання на території України.

З метою недопущення панічних настроїв серед населення, захисту суспільної стабільності, протидії спробам розпалювання міжнаціональної, релігійної та соціальної ворожнечі та підтримання довіри до державних інституцій держава створила окремі механізми реагування на інформаційні атаки.

Центр протидії дезінформації та Служба безпеки України регулярно спростовують фейки щодо воєнних дій (фейки про «капітуляцію України»; неправдиві повідомлення про «оточення» українських міст; дезінформацію щодо втрат Збройних Сил України; фальшиві повідомлення про евакуацію органів державної влади тощо.

Такі спростування оперативно публікуються на урядовому порталі та офіційних веб сайтах державних органів та верифікованих сторінках у соціальних мережах, через повідомлення в офіційних Telegram-каналах органів державної влади.

Державні органи систематично спростовують фейки про «тотальну мобілізацію всіх чоловіків», неправдиву інформацію про «закриття кордонів» та маніпуляції щодо діяльності територіальних центрів комплектування. З метою протидії інформаційним операціям щодо мобілізації органи державної влади публікують офіційні роз'яснення, проводять брифінги, зокрема Міністерство оборони України та Генеральний штаб ЗСУ.

З метою недопущення паніки серед населення та стабілізації суспільної ситуації після масованих атак РФ органи державної влади, зокрема Президент України, Державна служба України з надзвичайних ситуацій, Міністерство

внутрішніх справ України, Укренерго, тощо оперативно інформують громадян щодо безпекових ризиків та наслідків ударів та руйнувань, жертв серед населення, стану енергосистеми та аварійних відключень, реального стану критичної інфраструктури та іншого.

Держава активно використовує інструменти публічної дипломатії, зв'язків з громадськістю та інформаційно-психологічних операцій для захисту державних інтересів, протидії ворожій пропаганді та забезпечення національної безпеки.

У складі державних установ сформовано комунікаційні команди або відділ прес-служби, які займаються публічними заявами, формуванням меседжів та комунікують з населенням. Для формування єдиної позиції комунікаційна команда (відділ) обговорює ключові моменти та погоджує інформацію, яку буде донесено Президентом чи представниками міністерств та відомств до громадськості.

Одним із важливих аспектів стратегічних комунікацій є так звана «політика єдиного голосу», яка полягає в тому що всі державні інституції узгоджують свої меседжі та позиції, перш ніж оприлюднити офіційну заяву. Це забезпечує єдність, узгодженість та створює довіру до влади. В Україні цей принцип почав активно застосовуватись з початком повномасштабного вторгнення, він забезпечив потребу населення під час кризових ситуацій чіткою, єдиною та зрозумілою інформацією.

Система стратегічних комунікацій України включає комплекс державних органів, установ та інформаційних платформ, діяльність яких спрямована на координацію офіційного інформування населення та протидію інформаційним загрозам (рис.8.).



Рис. 8. Система стратегічних комунікацій.

Ключову координаційну роль у цій системі відіграє Рада національної безпеки і оборони України, правову основу діяльності якої визначають Конституція України та Закон України «Про Раду національної безпеки і оборони України». РНБО координує діяльність органів сектору безпеки і оборони у сфері інформаційної безпеки та здійснює контроль за виконанням рішень у цій сфері.

Важливим елементом системи є Центр протидії дезінформації при РНБО, створений відповідно до Указу Президента України від 11 березня 2021 року № 106/2021.

Основними завданнями Центру протидії дезінформації є:

- моніторинг інформаційного простору;
- аналіз інформаційно-психологічних операцій;
- спростування дезінформації;
- координація міжвідомчих комунікацій;
- попередження інформаційних загроз.

До системи стратегічних комунікацій також входять: Офіс Президента України, Міністерство оборони України, Генеральний штаб ЗСУ, Служба безпеки України, Державна служба спеціального зв'язку та захисту інформації України, CERT-UA, обласні військові адміністрації, суспільне мовлення.

Прикладом реалізації системи стратегічних комунікацій держави в умовах воєнного стану є єдиний телемарафон «Єдині новини».

Національний телемарафон «Єдині новини» виник як відповідь на інформаційні виклики, що постали перед Україною після повномасштабного вторгнення Росії 24 лютого 2022 року. В умовах воєнного стану держава потребувала оперативного, достовірного та координованого інформування населення, а також ефективної протидії російській пропаганді та дезінформації.

Ініціатива створення телемарафону була підтримана державними органами, зокрема Радою національної безпеки і оборони України (РНБО), яка ухвалила відповідне рішення, введене в дію Указом Президента України від 19 березня 2022 року № 152/2022. Координацію роботи телемарафону здійснює Міністерство культури та стратегічних комунікацій України спільно з Національною радою з питань телебачення і радіомовлення. Основною метою стало забезпечення інформаційної стабільності, недопущення паніки серед населення та створення єдиного джерела офіційних новин. До телемарафону приєдналися провідні загальнонаціональні телеканали, серед яких: «1+1», «ICTV», «Інтер», «Рада», «Суспільне» та інші. Вони об'єднали свої ресурси та почали працювати в ротаційному режимі, формуючи єдину інформаційну сітку мовлення. Це дало змогу ефективно розподіляти роботу редакцій, уникати дублювання контенту та створювати безперервний потік новин.

У межах телемарафону транслюються звернення Президента України, офіційні повідомлення органів влади, проводяться брифінги представників сектору безпеки й оборони, надається перевірена інформація щодо наслідків російських атак, досягнень та успіхів Збройних Сил України, міжнародна військова підтримка України, тощо.

Важливою складовою стратегічних комунікацій є система кризових комунікацій органів державної влади. Її функціонування передбачає:

- оперативне інформування населення;
- координацію офіційних повідомлень;
- реагування на кризові ситуації;
- протидію дезінформації;
- забезпечення інформаційної безпеки держави.

Під час ракетних атак, кібератак або надзвичайних ситуацій органи державної влади використовують: офіційні вебресурси, Telegram-канали, YouTube, Facebook, системи оповіщення населення, проводять офіційні брифінги та пресконференції.

Що стосується міжнародної співпраці, то Україна активно співпрацює з міжнародними партнерами у сфері стратегічних комунікацій, кібербезпеки та боротьби з дезінформацією. Основними партнерами України є: Північноатлантичний альянс (NATO), зокрема Об'єднаний центр передових технологій з кібероборони (CCDCOE), Європейський Союз, зокрема , East StratCom Task Force та міжнародні безпекові структури у сфері стратегічних комунікацій, кібербезпеки та інформаційної протидії.

Міжнародно-правовою основою співробітництва України з NATO у сфері стратегічних комунікацій, інформаційної безпеки та безпекової політики є Хартія про особливе партнерство між Україною та Організацією Північно-Атлантичного договору від 9 липня 1997 року, Декларація про доповнення Хартії від 21 серпня 2009 року та План дій Україна — NATO, ухвалений 22 листопада 2002 року. Вказані документи визначають механізми політичного діалогу, консультацій, розвитку стратегічних комунікацій, інформаційної стійкості та інтеграції стандартів NATO у секторі безпеки і оборони України.

Що стосується медіаграмотності населення, яка сприяє формуванню стійкості суспільства до дезінформації, пропаганди, маніпуляцій та психологічного впливу, то держава намагається забезпечити ефективну політику шляхом виконання комплексу дій, спрямованих на формування у населення

навичок критичного сприйняття інформації, протидії дезінформації та безпечного користування медіапростором. Така політика не обмежується освітніми або інформаційними кампаніями, а охоплює законодавчі, організаційні, освітні та технологічні механізми.

Держава створила законодавчу основу для розвитку медіаграмотності, інформаційної безпеки та стратегічних комунікацій.

Зокрема, Закон України «Про інформацію» визначає гарантії права громадян на інформацію. Відповідно до статті 6 держава забезпечує доступ до інформації, обов'язок органів влади інформувати суспільство та здійснення контролю за дотриманням інформаційного законодавства.

Стаття 7 Закону України «Про інформацію» гарантує захист права особи на інформацію та забороняє незаконне обмеження доступу до неї. Це створює правову основу для отримання громадянами достовірної інформації та протидії маніпуляціям.

Закон України «Про медіа» закріпив поняття медіаграмотності та визначив органи, відповідальні за формування державної політики у цій сфері. Зокрема, функції щодо реалізації політики медіаграмотності покладені на Міністерство культури та стратегічних комунікацій України.

Стратегія інформаційної безпеки України, затверджена Указом Президента №685/2021, визначає одним із напрямів забезпечення інформаційної стійкості суспільства та протидію інформаційним операціям держави-агресора. Документ передбачає розвиток стратегічних комунікацій, взаємодію держави із суспільством та захист громадян від дезінформації.

Крім того, рішення Ради національної безпеки і оборони України у сфері інформаційної безпеки передбачають координацію діяльності органів влади щодо протидії інформаційним загрозам, фейкам та інформаційно-психологічним операціям. Практично це реалізується через навчання державних службовців, офіційні інформаційні кампанії, роботу державних та громадських фактчекінгових проєктів, розвиток цифрової грамотності населення, інформування громадян через офіційні канали державних органів.

Наприклад, платформа «Дія» та її освітній напрям «Дія.Освіта» є одним із практичних інструментів державної політики у сфері підвищення цифрової та медіаграмотності населення. Через цю платформу держава реалізує елементи стратегічних комунікацій, спрямованих на формування інформаційної стійкості суспільства. Основна ідея полягає в тому, що громадян навчають безпечно користуватися цифровими технологіями, критично сприймати інформацію та протидіяти дезінформації. Це особливо важливо в умовах гібридної війни, коли інформаційний простір використовується як інструмент впливу на населення.

На платформі «Дія.Освіта» розміщуються освітні серіали, курси цифрової грамотності, матеріали з кібергігієни, навчання перевірці інформації, рекомендації щодо безпечної поведінки в інтернеті, матеріали про захист персональних даних.

Якщо розглянути статистику за результатами дослідження «Індекс медіаграмотності українців 2020–2025» (шоста хвиля дослідження), проведеного незалежним українським громадським проєктом Детектор медіа, то виявимо такі результати:

Основні результати дослідження за 2025 рік:

- 69% українців мають рівень медіаграмотності вище середнього або високий;
- 60% — мають рівень вище середнього;
- 9% — високий рівень;
- 27% — нижчий за середній;
- 4% — низький рівень медіаграмотності.

Дослідники зазначають, що загальний рівень медіаграмотності залишається значно вищим, ніж до початку повномасштабної війни, хоча у 2025 році вже не спостерігається такого різкого зростання, як у 2022 році.

Динаміка індексу медіаграмотності (2020–2025) за десятибальною шкалою:

- 2020 — 4,8;
- 2021 — 4,8;
- 2022 — 5,9;

- 2023 — 5,4;
- 2024 — 5,2;
- 2025 — 5,2.

Виходячи із зазначеного, розуміємо, що повномасштабна війна стала фактором різкого підвищення інформаційної уважності населення. Тому українці почали частіше перевіряти інформацію, користуватися офіційними джерелами, критичніше ставитися до новин у Telegram та соцмережах, краще розпізнавати російську пропаганду.

Ось декілька важливих тенденцій.

- молодь має найвищий рівень медіаграмотності (18-35 років) через високий рівень цифрової компетентності, активне користування онлайн-ресурсами та кращу адаптацію до цифрового середовища;
- освіта прямо впливає на рівень медіаграмотності, тому серед громадян із середньою освітою 46% мають низький або нижчий за середній рівень медіаграмотності, а серед людей з вищою освітою цей показник становить лише 17%;
- соціальні мережі залишаються головним джерелом новин;
- виник новий показник – ШІ-грамотність, це пов’язано із поширенням генеративного ШІ, deepfake-відео, штучно створених фото, автоматизованих ботів тощо.

Висновки до розділу 2

У результаті проведеного дослідження встановлено, що інформаційна безпека є однією з ключових складових національної безпеки держави та важливим елементом захисту державного суверенітету, суспільної стабільності й національних інтересів. В умовах цифрової трансформації та розвитку інформаційного суспільства інформаційний простір став окремою сферою стратегічного протиборства, у межах якого здійснюються інформаційно-психологічні операції, кібератаки, маніпулятивні інформаційні впливи та кампанії з поширення дезінформації.

У результаті проведеного дослідження встановлено, що сучасний стан інформаційної безпеки України характеризується високим рівнем зовнішніх та внутрішніх загроз, зумовлених гібридною агресією Російської Федерації, активним застосуванням інформаційно-психологічних операцій, дезінформації, кібератак та маніпулятивного інформаційного впливу. Інформаційний простір України став одним із ключових напрямів протиборства, що безпосередньо впливає на національну безпеку, суспільну стабільність та функціонування державних інституцій.

У дослідженні визначено основні загрози інформаційній безпеці України, серед яких поширення фейкових повідомлень, використання соціальних мереж та цифрових платформ для інформаційного впливу, кібератаки на державні інформаційні ресурси та критичну інфраструктуру, витоки персональних даних, кібершпигунство, застосування технологій deepfake та AI-генерованого контенту. Встановлено, що сучасні інформаційні загрози мають комплексний характер та охоплюють зовнішньополітичну, воєнну, економічну, соціальну, науково-технічну та гуманітарну сфери.

Проаналізовано місце кібербезпеки у системі інформаційної безпеки держави. Встановлено, що стрімка цифровізація держави та суспільства зумовлює постійне зростання кількості кіберзагроз, фішингових атак, шкідливого програмного забезпечення та спроб компрометації державних інформаційних систем.

У роботі досліджено діяльність основних суб’єктів національної системи кібербезпеки України, зокрема Ради національної безпеки і оборони України, Державної служби спеціального зв’язку та захисту інформації України, CERT-UA, Служби безпеки України, Національної поліції України, Міністерства оборони України та інших органів сектору безпеки і оборони.

Особливу увагу приділено діяльності органів державної влади у сфері протидії дезінформації та інформаційним операціям. Визначено, що Україна реалізує комплекс нормативно-правових, організаційних та інформаційно-комунікаційних заходів, спрямованих на захист національного інформаційного

простору, блокування російських інформаційних ресурсів, спростування фейкової інформації та формування стійкості суспільства до деструктивного інформаційного впливу. Важливе значення у цьому процесі мають Центр протидії дезінформації, система стратегічних комунікацій держави, кризові комунікації та політика «єдиного голосу».

Дослідження показало, що важливим елементом забезпечення інформаційної безпеки держави є розвиток медіаграмотності населення. Встановлено, що повномасштабна війна сприяла підвищенню рівня інформаційної уважності громадян, активнішому використанню офіційних джерел інформації та критичнішому сприйняттю інформаційного контенту.

Таким чином, сучасний стан інформаційної безпеки України характеризується необхідністю комплексного поєднання інформаційних, кібербезпекових, правових, організаційних та комунікаційних механізмів. Ефективне забезпечення інформаційної безпеки держави можливе лише за умов постійного вдосконалення системи кіберзахисту, розвитку стратегічних комунікацій, зміцнення міжнародного співробітництва та підвищення рівня медіаграмотності населення.

РОЗДІЛ 3
ФОРМУВАННЯ ДІЄВОЇ МОДЕЛІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

3.1. Основні напрями удосконалення державної політики у сфері інформаційної безпеки

Основними напрямами вдосконалення державної політики (рис. 9) у сфері інформаційної безпеки є:

Крок 1 - удосконалення законодавства,

Крок 2 - покращення механізмів взаємодії державних органів,

Крок 3 - розвиток стратегічних комунікацій,

Крок 4 - підвищення медіаграмотності населення,

Крок 5 - посилення кібербезпеки та захисту критичної інфраструктури.



Рис.9. Напрями удосконалення державної політики у сфері інформаційної безпеки.

У процесі дослідження нормативно-правового забезпечення інформаційної безпеки України було встановлено, що значна частина чинних нормативно-правових актів у цій сфері потребує перегляду та актуалізації. Це зумовлено стрімким розвитком цифрових технологій, трансформацією інформаційного середовища, появою нових інформаційних та кіберзагроз, а також зміною безпекової ситуації після початку повномасштабної агресії Російської Федерації проти України.

Частина нормативних документів була розроблена в умовах, коли сучасні інформаційні загрози, зокрема інформаційно-психологічні операції, дезінформаційні кампанії у соціальних мережах, deepfake-технології, штучний інтелект, бот-мережі та масштабні кібератаки, ще не мали такого рівня

поширення. Унаслідок цього окремі положення законодавства не повною мірою відповідають сучасним викликам у сфері інформаційної безпеки.

Крім того, окремі концепції, програми та стратегії мають завершений строк дії або фактично втратили актуальність через зміну державної політики, реформування системи стратегічних комунікацій та адаптацію України до стандартів Європейського Союзу і НАТО. Це створює потребу у формуванні сучасної, системної та узгодженої нормативно-правової бази у сфері інформаційної безпеки держави.

Зокрема, такими нормативно-правовими актами є Доктрина інформаційної безпеки України (2017 року), Концепція розвитку цифрової економіки та суспільства України на 2018–2020 роки, Закон України «Про інформацію» (1992 року), Закон України «Про захист інформації в інформаційно-комунікаційних системах», тощо.

Проведений аналіз нормативно-правового забезпечення у сфері інформаційної безпеки України свідчить про наявність значної кількості нормативно-правових актів, які частково втратили актуальність у зв’язку зі стрімкою цифровою трансформацією суспільства, розвитком сучасних інформаційних технологій та зміною характеру інформаційних загроз в умовах гібридної війни.

Окремі нормативні документи містять застарілі підходи до забезпечення інформаційної безпеки, не враховують сучасні механізми поширення дезінформації, використання штучного інтелекту, цифрових платформ, соціальних мереж та інформаційно-психологічних операцій. Крім того, частина концепцій, програм та стратегій має завершений строк дії або потребує суттєвого перегляду відповідно до сучасних безпекових викликів та євроінтеграційних процесів України.

У зв’язку з цим одним із пріоритетних напрямів удосконалення державної політики у сфері інформаційної безпеки має стати системне оновлення нормативно-правової бази, її гармонізація зі стандартами Європейського Союзу

та НАТО, а також адаптація до сучасного цифрового середовища та новітніх інформаційних загроз.

У Стратегії інформаційної зазначено, що в Україні ще не створено достатньо дієвого механізму координації між усіма органами влади, залученими до протидії інформаційним загрозам. Насамперед потрібно посилити єдиний координаційний центр або механізм взаємодії між РНБО, Міністерством культури та стратегічних комунікацій, Мінцифри, СБУ, Держспецзв'язку, Нацрадою з питань телебачення і радіомовлення, ЗСУ та місцевими адміністраціями. Це дозволить швидше реагувати на фейки, інформаційно-психологічні операції, кібератаки та кризові ситуації.

Що стосується розвитку стратегічних комунікацій держави, то органи влади мають не лише спростовувати фейки, а й завчасно пояснювати суспільству державну політику, рішення у сфері оборони, мобілізації, євроінтеграції, цифровізації та безпеки.

Одним із ключових напрямів є проактивна комунікація з громадянами. Органи влади повинні не чекати появи фейків або інформаційних атак, а завчасно пояснювати суспільству зміст, мету та очікувані результати державних рішень. Особливо це стосується сфер оборони, мобілізації, національної безпеки, цифровізації, кіберзахисту, європейської інтеграції та реформування державного управління. Недостатнє або несвоєчасне інформування населення створює інформаційний вакуум, який швидко заповнюється маніпулятивними повідомленнями, дезінформацією та інформаційно-психологічними операціями противника.

Важливою складовою стратегічних комунікацій є забезпечення прозорості діяльності державних органів. Регулярне офіційне інформування, публічне пояснення рішень та відкритість державних інституцій сприяють підвищенню рівня суспільної довіри та зниженню рівня соціальної напруги. У кризових умовах оперативна та достовірна інформація стає одним із факторів забезпечення національної безпеки та суспільної стабільності.

Підвищення медіаграмотності населення може здійснюватися через комплекс організаційних, освітніх, інформаційних та нормативно-правових заходів, реалізованих державою у взаємодії з освітніми установами, громадськими організаціями, засобами масової інформації та цифровими платформами.

У сучасних умовах інформаційного протиборства та активного поширення дезінформації розвиток медіаграмотності є одним із ключових елементів забезпечення інформаційної безпеки держави та формування стійкості суспільства до маніпулятивних інформаційних впливів.

Одним із основних напрямів є інтеграція медіаграмотності до системи освіти. Це може включати впровадження окремих навчальних курсів або тематичних модулів у закладах загальної середньої, професійної та вищої освіти. Такі програми повинні охоплювати навички критичного мислення, перевірки достовірності джерел інформації, розпізнавання фейкових повідомлень, маніпуляцій, пропаганди, бот-мереж та інформаційно-психологічних операцій. Особливу увагу доцільно приділяти практичним навичкам перевірки фото-, відео- та текстового контенту, аналізу джерел інформації, а також безпечній поведінці в соціальних мережах.

Для державних службовців та працівників критичної інфраструктури доцільним є проведення регулярних тренінгів і курсів з інформаційної безпеки та кібергігієни.

Окремого значення набуває співпраця держави з цифровими платформами та соціальними мережами. Це може включати створення механізмів оперативного маркування фейкових повідомлень, обмеження поширення дезінформації, протидію бот-мережам та координацію дій щодо блокування інформаційних ресурсів, які використовуються для інформаційно-психологічних операцій проти держави. Також важливим є розвиток офіційних державних каналів комунікації у соціальних мережах для швидкого поширення перевіреної інформації.

Важливо також забезпечити доступність програм медіаграмотності для різних категорій населення, зокрема людей похилого віку, внутрішньо переміщених осіб, дітей та мешканців сільських територій, які можуть бути більш вразливими до маніпулятивного інформаційного впливу.

Що стосується кібербезпеки, то особливого значення набуває захист критичної інформаційної інфраструктури, до якої належать інформаційно-комунікаційні системи органів державної влади, енергетичного сектору, фінансової системи, транспортної галузі, телекомунікацій, медичної сфери та інших об’єктів, порушення функціонування яких може становити загрозу національній безпеці. У зв’язку з цим важливим завданням держави є впровадження сучасних технологій та моделей кіберзахисту, зокрема:

- SOC-центрів моніторингу безпеки;
- SIEM-систем аналізу подій інформаційної безпеки;
- NAC-рішень контролю доступу до мережі;
- багаторівневого резервування даних;
- криптографічного захисту інформації.
- Zero Trust Architecture;
- XDR/EDR-платформ;
- систем моніторингу та реагування на інциденти.

Також необхідно вдосконалити механізми резервування та відновлення державних інформаційних ресурсів, особливо в умовах воєнного стану. Повномасштабна війна показала критичну важливість резервного копіювання, географічно розподілених дата-центрів, захищених хмарних рішень, безперервності функціонування державних реєстрів та електронних сервісів.

Необхідно забезпечити розвиток кадрового потенціалу у сфері кібербезпеки, зокрема: розширювати підготовку фахівців, особливо жінок, впроваджувати спеціалізовані освітні програми, проводити регулярні кібернавчання, підвищувати рівень кібергігієни державних службовців.

В умовах тривалої збройної агресії Російської Федерації проти України кіберпростір став одним із ключових доменів протистояння. Стійкість держави,

безперебійне функціонування критичної інфраструктури, захист державних реєстрів і цифрових сервісів для громадян безпосередньо залежать від наявності достатньої кількості висококваліфікованих фахівців і фахівчинь у сфері кібербезпеки. Водночас національний ринок праці характеризується глибоким структурним дефіцитом таких кадрів, який посилюється мобілізацією, міграцією та демографічними втратами.

За цих умов недостатнє залучення жінок до сектору кібербезпеки формує системну втрату потенціалу, яку держава не може дозволити собі ігнорувати. Жінки готові та здатні активно закривати кадровий дефіцит, проте стикаються з численними структурними, законодавчими, культурними та організаційними бар'єрами — від відсутності профорієнтації в школах і гендерних стереотипів у закладах вищої освіти до неформальних обмежень кар'єрного зростання та браку гнучкості зайнятості в умовах воєнного стану.

Особливу роль у розвитку системи інформаційної безпеки відіграють жінки-керівники структурних підрозділів державних органів. Вони здійснюють:

- координацію діяльності підрозділів кіберзахисту;
- управління процесами реагування на кіберзагрози;
- організацію міжвідомчої взаємодії;
- впровадження сучасних механізмів інформаційної безпеки;
- розробку стратегій цифрової стійкості державних установ.

Жінки-керівники у сфері кібербезпеки сприяють розвитку сучасної управлінської культури, підвищенню ефективності державного управління та формуванню інклюзивного професійного середовища у сфері цифрової безпеки. Важливе значення також має їх участь у міжнародному співробітництві, реалізації проєктів цифрової трансформації та впровадженні стандартів Європейський Союз і НАТО у сфері кіберзахисту.

За даними міжнародних досліджень, жінки все ще недостатньо представлені у сфері кібербезпеки. Згідно зі звітом ISC2 Women in Cybersecurity Report, жінки становлять приблизно 20–25% світової кібербезпекової робочої сили. У 2025 році

середній показник присутності жінок у кібербезпекових командах становив близько 22%, тоді як чоловіки складали близько 78% працівників цієї сфери.

Щодо України, офіційна статистика саме по підрозділах кіберзахисту органів виконавчої влади є обмеженою та не публікується у повному обсязі. Однак доступні дослідження свідчать про поступове зростання кількості жінок у сфері ІТ та інформаційної безпеки. За даними українських досліджень ІТ-ринку, жінки становлять близько 24–28% фахівців ІТ-сфери України.

У державному секторі частка жінок у підрозділах кібербезпеки традиційно нижча за загальний рівень представництва жінок у державній службі, оскільки кібербезпека тривалий час вважалася переважно «технічною» та чоловічою сферою. За оцінками профільних досліджень та міжнародних звітів, у підрозділах кіберзахисту державних органів жінки можуть становити орієнтовно 20–25% персоналу, тоді як чоловіки — близько 75–80%.

Попри це, останніми роками спостерігається позитивна тенденція до збільшення участі жінок у сфері кібербезпеки та цифрового управління. В Україні жінки дедалі частіше займають керівні посади у сфері ІТ, цифрової трансформації та інформаційної безпеки. За окремими дослідженнями, жінки займають близько 30–40% керівних посад у технологічному та професійному секторі України, що перевищує середні показники багатьох країн Європи.

Важливим чинником розвитку жіночого лідерства у сфері кібербезпеки є:

- розвиток цифрової освіти;
- підтримка STEM-напрямів серед жінок;
- міжнародні програми професійної підготовки;
- впровадження принципів гендерної рівності у державному секторі;
- створення професійних спільнот жінок у сфері кібербезпеки.

Водночас існують певні проблеми, які стримують активніше залучення жінок до сфери кібербезпеки:

- гендерні стереотипи;
- недостатня популяризація технічних професій серед дівчат;
- нерівномірне представництво на керівних посадах;

- дефіцит наставництва та професійної підтримки;
- психологічні бар’єри щодо роботи у сфері безпеки та оборони.

Таким чином, жінки відіграють дедалі важливішу роль у забезпеченні інформаційної та кібернетичної безпеки державного сектору України. Їх професійна діяльність та управлінська участь сприяють розвитку сучасної системи кіберзахисту, цифрової стійкості держави та підвищенню ефективності публічного управління у сфері інформаційної безпеки.

Нижче наведено статистичні дані, отримані за результатами дослідження, проведеного в одному зі структурних підрозділів органу державної влади, щодо відсоткового співвідношення посад категорій «Б» та «В», які обіймають фахівці у сфері інформаційної безпеки та кіберзахисту. Відповідно до отриманих результатів, близько 20% працівників зазначеного структурного підрозділу становлять жінки.

Посади державної служби категорії **«Б»** Департаменту цифровізації Держмитслужби		
Загальна кількість посадових осіб підрозділу інформаційної та кібербезпеки	Кількість жінок у підрозділі	% від загальної кількості
9	**2**	**22**

Посади державної служби категорії **«В»** Департаменту цифровізації Держмитслужби		
Загальна кількість посадових осіб підрозділу інформаційної та кібербезпеки	Кількість жінок у підрозділі	% від загальної кількості
49	**11**	**22**



Рис.10. Статистичні дані відсоткового співвідношення посад категорій «Б» та «В» в апараті державного органу.

Посади державної служби категорії «Б» територіальних органів Держмитслужби		
Загальна кількість посадових осіб підрозділу інформаційної та кібербезпеки	Кількість жінок у підрозділі	% від загальної кількості
31	**7**	**23**

Посади державної служби категорії «В» територіальних органів Держмитслужби		
Загальна кількість посадових осіб підрозділу інформаційної та кібербезпеки	Кількість жінок у підрозділі	% від загальної кількості
96	**37**	**39**



Рис.11. Статистичні дані відсоткового співвідношення посад категорій «Б» та «В» в територіальних органах державного органу.

3.2. Впровадження сучасних механізмів протидії інформаційним загрозам, кібератакам та дезінформації

Сучасні механізми протидії інформаційним загрозам, кібератакам та дезінформації базуються на комплексному поєднанні організаційних, технологічних, інформаційних та правових заходів, спрямованих на забезпечення інформаційної безпеки держави, захист критичної інформаційної інфраструктури та підвищення стійкості суспільства до деструктивних інформаційних впливів. В умовах гібридної війни та активного розвитку цифрових технологій держава повинна забезпечувати не лише реагування на загрози, а й їх своєчасне виявлення, прогнозування та попередження.

Одним із ключових напрямів є протидія інформаційним загрозам, зокрема інформаційно-психологічним операціям, маніпулятивним повідомленням та кампаніям із підриву довіри до державних інституцій. Для цього використовуються системи моніторингу інформаційного простору та соціальних мереж, які дозволяють виявляти поширення фейкових повідомлень, активізацію

бот-мереж, аномальну інформаційну активність та координовані інформаційні кампанії. Важливу роль у цьому процесі відіграють технології OSINT, аналітичні платформи збору даних та інструменти автоматизованого аналізу інформаційного контенту.

Суттєвим елементом протидії інформаційним загрозам є розвиток стратегічних комунікацій держави. Органи державної влади повинні здійснювати проактивне інформування населення, оперативно надавати офіційні роз'яснення та забезпечувати швидке спростування недостовірної інформації. Це дозволяє мінімізувати ризики дестабілізації суспільства та знижує ефективність інформаційно-психологічних операцій противника. Водночас важливим є підвищення рівня медіаграмотності населення шляхом проведення освітніх програм, навчання критичному мисленню та формування навичок перевірки достовірності інформації.

Для протидії кібератакам застосовується комплекс технічних механізмів кіберзахисту. До них належать міжмережеві екрани (firewall), системи виявлення та запобігання вторгненням (IDS/IPS), рішення класу EDR для захисту кінцевих точок, антивірусний захист, системи багатофакторної автентифікації та криптографічний захист інформації. Особливе значення має захист державних інформаційних ресурсів, серверної інфраструктури, систем електронного документообігу та офіційних каналів електронної комунікації.

Важливим сучасним механізмом є впровадження центрів моніторингу та реагування на кіберінциденти — SOC (Security Operations Center), які забезпечують безперервний моніторинг подій безпеки, аналіз інцидентів та оперативне реагування на загрози. У таких центрах використовуються системи SIEM та SOAR, які дозволяють автоматизувати процеси збору журналів подій, виявлення аномалій, аналізу кіберзагроз та реагування на інциденти. Це забезпечує своєчасне виявлення спроб несанкціонованого доступу, DDoS-атак, шкідливого програмного забезпечення та інших кіберзагроз.

Окрему роль відіграє управління вразливостями інформаційних систем. Державні органи повинні регулярно проводити аудит інформаційної безпеки,

тестування на проникнення, сканування вразливостей та своєчасне оновлення програмного забезпечення. Це дозволяє мінімізувати ризики компрометації інформаційних ресурсів та запобігати використанню відомих вразливостей зловмисниками.

У сфері протидії дезінформації важливими механізмами є фактчекінг, перевірка джерел інформації та співпраця з незалежними фактчекінговими організаціями. Держава також повинна взаємодіяти із цифровими платформами та соціальними мережами щодо маркування фейкового контенту, обмеження діяльності бот-мереж та блокування ресурсів, які використовуються для поширення дезінформації та проведення інформаційно-психологічних операцій (рис.12).



Рис. 12. Механізми протидії інформаційним загрозам, кібератакам та дезінформації.

Висновки до розділу 3

У результаті проведеного дослідження встановлено, що формування дієвої моделі інформаційної безпеки держави потребує комплексного поєднання нормативно-правових, організаційних, технологічних, комунікаційних та освітніх механізмів. В умовах гібридної війни, цифрової трансформації та постійного зростання інформаційних і кібернетичних загроз забезпечення інформаційної безпеки держави повинно здійснюватися системно та на основі сучасних підходів до управління інформаційним простором і кіберзахистом.

У дослідженні визначено основні напрями вдосконалення державної політики у сфері інформаційної безпеки, серед яких: оновлення нормативно-правової бази, розвиток міжвідомчої взаємодії, удосконалення стратегічних комунікацій, підвищення рівня медіаграмотності населення та посилення кібербезпеки й захисту критичної інформаційної інфраструктури. Встановлено, що чинна система нормативно-правового забезпечення частково не відповідає сучасним викликам, пов’язаним із розвитком цифрових технологій, використанням штучного інтелекту, поширенням deepfake-технологій, бот-мереж та сучасних інформаційно-психологічних операцій.

Обґрунтовано необхідність посилення координації між державними органами, залученими до забезпечення інформаційної безпеки, а також розвитку системи стратегічних комунікацій держави. Визначено, що органи державної влади повинні забезпечувати не лише спростування дезінформації, а й здійснювати проактивне інформування населення щодо державної політики, безпекових рішень та реформ. Важливу роль у цьому процесі відіграють прозорість діяльності державних інституцій, кризові комунікації та політика «єдиного голосу».

У роботі встановлено, що підвищення медіаграмотності населення є одним із ключових елементів забезпечення інформаційної стійкості суспільства. Розвиток критичного мислення, навичок перевірки інформації та безпечного користування цифровими платформами сприяє зниженню впливу дезінформації та інформаційно-психологічних операцій.

Окрему увагу приділено питанням кібербезпеки та захисту критичної інформаційної інфраструктури. Встановлено, що ефективна система кіберзахисту повинна базуватися на впровадженні сучасних технологій та моделей безпеки, зокрема SOC-центрів, SIEM-систем, NAC-рішень, XDR/EDR-платформ, багатофакторної автентифікації, криптографічного захисту інформації та концепції Zero Trust Architecture. Важливим напрямом є також розвиток систем резервування даних, забезпечення безперервності функціонування державних інформаційних ресурсів та вдосконалення механізмів реагування на кіберінциденти.

У дослідженні також акцентовано увагу на необхідності розвитку кадрового потенціалу у сфері інформаційної та кібернетичної безпеки. Встановлено, що в умовах дефіциту фахівців особливого значення набуває розширення участі жінок у сфері кібербезпеки, підтримка STEM-освіти, розвиток професійних спільнот та створення інклюзивного професійного середовища. Доведено, що жінки дедалі активніше беруть участь у формуванні сучасної системи кіберзахисту держави та займають важливі управлінські посади у сфері цифрової безпеки.

Таким чином, формування дієвої моделі інформаційної безпеки держави повинно базуватися на інтеграції сучасних технологій кіберзахисту, стратегічних комунікацій, розвитку медіаграмотності, міжвідомчої координації та удосконалення державної політики у сфері інформаційної безпеки. Реалізація зазначених напрямів сприятиме зміцненню інформаційного суверенітету, кіберстійкості та національної безпеки України.

ВИСНОВКИ

У результаті проведеного дослідження встановлено, що інформаційна безпека держави є однією з ключових складових національної безпеки України та важливим елементом забезпечення державного суверенітету, суспільної стабільності, захисту прав громадян і сталого функціонування державних інституцій. В умовах цифрової трансформації суспільства та повномасштабної агресії Російської Федерації інформаційний простір став окремим середовищем стратегічного протиборства, у межах якого здійснюються інформаційно-психологічні операції, кампанії дезінформації, кібератаки та інші форми деструктивного інформаційного впливу.

У роботі проаналізовано теоретичні засади формування системи інформаційної безпеки держави, визначено її сутність, основні складові, об’єкти та суб’єкти забезпечення. Встановлено, що сучасна інформаційна безпека має комплексний характер та поєднує інформаційно-технічну і інформаційно-психологічну складові. Інформаційна безпека охоплює захист державних інформаційних ресурсів, інформаційно-комунікаційних систем, критичної інформаційної інфраструктури, а також захист суспільної свідомості від маніпулятивного інформаційного впливу.

У процесі дослідження визначено основні сучасні загрози інформаційній безпеці України, серед яких: інформаційно-психологічні операції, поширення дезінформації та фейкових повідомлень, кібератаки на державні інформаційні ресурси, використання соціальних мереж і цифрових платформ для інформаційного впливу, кібершпигунство, deepfake-технології та AI-генерований контент. Доведено, що сучасні інформаційні загрози мають комплексний характер та охоплюють політичну, воєнну, економічну, соціальну й гуманітарну сфери.

Проаналізовано місце кібербезпеки у системі інформаційної безпеки держави. Встановлено, що кібербезпека є невід’ємною складовою національної

безпеки та спрямована на забезпечення захисту інформаційних, електронно-комунікаційних та інформаційно-комунікаційних систем, державних інформаційних ресурсів і критичної інфраструктури. Визначено основні суб'єкти національної системи кібербезпеки України, їх функції та механізми взаємодії у сфері реагування на кіберінциденти та забезпечення кіберзахисту.

У роботі досліджено діяльність органів державної влади у сфері формування інформаційної безпеки України. Встановлено, що Україна реалізує комплекс нормативно-правових, організаційних, технологічних та інформаційно-комунікаційних заходів, спрямованих на протидію дезінформації, інформаційним операціям та кібератакам. Важливу роль у цьому процесі відіграють система стратегічних комунікацій держави, Центр протидії дезінформації, CERT-UA, кризові комунікації та механізми міжвідомчої координації.

Проведений аналіз нормативно-правового забезпечення інформаційної безпеки України засвідчив необхідність його подальшого вдосконалення та адаптації до сучасних викликів цифрового середовища. Встановлено, що окремі нормативно-правові акти, концепції та стратегії частково втратили актуальність і потребують оновлення з урахуванням сучасних інформаційних та кібернетичних загроз, розвитку цифрових технологій, інтеграції стандартів Європейського Союзу та NATO.

Обґрунтовано необхідність розвитку стратегічних комунікацій держави, які повинні базуватися на принципах проактивного інформування населення, прозорості діяльності органів влади, оперативного реагування на інформаційні загрози та формування довіри суспільства до державних інституцій. Важливим напрямом забезпечення інформаційної стійкості суспільства визначено розвиток медіаграмотності населення, критичного мислення та навичок безпечного використання цифрових технологій.

У роботі запропоновано основні напрями формування дієвої моделі інформаційної безпеки держави, серед яких: удосконалення державної політики у сфері інформаційної безпеки, посилення міжвідомчої взаємодії, розвиток стратегічних комунікацій, підвищення рівня медіаграмотності населення, впровадження сучасних технологій кіберзахисту та забезпечення захисту критичної інформаційної інфраструктури.

Встановлено, що ефективна система кіберзахисту держави повинна базуватися на використанні сучасних технологій та механізмів безпеки, зокрема SOC-центрів, SIEM-систем, NAC-рішень, XDR/EDR-платформ, багатофакторної автентифікації, криптографічного захисту інформації та концепції Zero Trust Architecture. Також важливого значення набуває розвиток систем резервування даних, безперервності функціонування державних інформаційних ресурсів та механізмів реагування на кіберінциденти.

Окрему увагу приділено розвитку кадрового потенціалу у сфері інформаційної та кібернетичної безпеки. Доведено, що в умовах дефіциту фахівців важливим напрямом є підтримка цифрової освіти, STEM-напрямів, професійної підготовки та розширення участі жінок у сфері кібербезпеки та цифрового управління.

Доведено, що формування дієвої моделі інформаційної безпеки держави повинно здійснюватися на основі комплексного поєднання правових, організаційних, технологічних, освітніх та комунікаційних механізмів. Реалізація запропонованих у дослідженні напрямів сприятиме зміцненню інформаційного суверенітету України, підвищенню кіберстійкості держави, ефективності системи стратегічних комунікацій та забезпеченню національної безпеки в умовах сучасних гібридних загроз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Конституція України : Закон України від 28 черв. 1996 р. № 254к/96-ВР. URL: http://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text.
2. Про національну безпеку України : Закон України від 21 черв. 2018 р. № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text.
3. Про інформацію : Закон України від 2 жовт. 1992 р. № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text.
4. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовт. 2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.
5. Про медіа : Закон України від 13 груд. 2022 р. № 2849-IX. URL: https://zakon.rada.gov.ua/laws/show/2849-20#Text.
6. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» : Указ Президента України від 28 груд. 2021 р. № 685/2021. URL: https://www.president.gov.ua/documents/6852021-41069.
7. Про Стратегію кібербезпеки України : Рішення Ради національної безпеки і оборони України від 14 трав. 2021 р. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 28.05.2026).
8. Гур'єв В. І., Мехед Д. Б., Ткач Ю. М., Фірсова І. В. Інформаційна безпека держави : навч. посіб. Ніжин : Чернігівський національний технологічний університет, 2018. 288 с.
9. Мужанова Т. М. Інформаційна безпека держави : навч. посіб. Київ : Державний університет телекомунікацій, 2019. 164 с.
10. Титова Н. М., Рідей Н. М., Настрадін В. П. та ін. Інформаційна безпека та кібербезпека держави : навч. посіб. Київ : Ліра-К, 2024. 554 с.
11. Інформаційна безпека держави : конспект лекцій / Національний університет «Чернігівська політехніка». Чернігів, 2023. URL: https://ir.stu.cn.ua/server/api/core/bitstreams/2b51cde5-e3b7-4803-9d6d-b99d311b3fae/content.
12. Вінер Н. Кібернетика, або керування і зв'язок у тварині та машині. Київ : Основи, 2004. 287 с.
13. Shannon C. E. A Mathematical Theory of Communication. Bell System Technical Journal. 1948. Vol. 27. P. 379–423.
14. Центр протидії дезінформації при РНБО України : офіц. сайт. URL: https://cpd.gov.ua/.
15. Детектор медіа : офіц. сайт. URL: https://detector.media/.
16. Медіаграмотність : підручник / за ред. В. Ф. Іванова, О. В. Волошенюк. Київ : Центр вільної преси, 2016. URL: http://library.ippro.com.ua/attachments/article/552/Медіаграмотність.pdf.
17. Стратегічні комунікації в умовах гібридної війни: погляд від волонтера до науковця. URL: https://msj.ukma.edu.ua/wp-

content/uploads/2024/01/Stratehichni_komunikatsii_v_umovakh_hibrydnoi_viiny_-pohliad_vid_volontera_do_naukovtsia.pdf.

18. CERT-UA : офіц. сайт урядової команди реагування на комп'ютерні надзвичайні події України. URL: https://cert.gov.ua/.

19. CERT-UA у 2025 році опрацювала майже 6000 кіберінцидентів : офіц. повідомлення Держспецзв'язку України. URL: https://cip.gov.ua/ua/news/cert-ua-u-2025-roci-opracyuvala-maizhe-6000-kiberincidentiv-kilkist-vorozhikh-atak-zrosla-na-37.

20. National Cybersecurity Strategy. Washington : The White House, 2023. 35 p. URL: https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

21. Cybersecurity Framework / National Institute of Standards and Technology (NIST). URL: https://www.nist.gov/cyberframework.

22. Security and Privacy Controls for Information Systems and Organizations / NIST Special Publication 800-53 Rev. 5. URL: https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final.

23. Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations / NIST Special Publication 800-171 Rev. 3. URL: https://csrc.nist.gov/pubs/sp/800/171/r3/final.

24. Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective / NATO CCDCOE. URL: https://ccdcoe.org/library/publications/analysis-of-the-2007-cyber-attacks-against-estonia-from-the-information-warfare-perspective/.

25. Data Embassy / e-Estonia. URL: https://e-estonia.com/solutions/e-governance/data-embassy/.

26. Тренінг проведення інструктажів та тренінгів з кібергігієни в державному секторі / CDTO Campus. URL: https://www.cdto-campus.com/ua/programs/trening-provedennya-instruktazhiv-ta-treningiv-z-kibergigiieni-v-derzhavnomu-sektori.

27. Official Alerts & Statements / Cybersecurity and Infrastructure Security Agency (CISA). URL:.

28. FBI reports cyber threats to critical infrastructure intensify as US cybercrime losses hit $21 billion. URL: https://industrialcyber.co/reports/fbi-reports-cyber-threats-to-critical-infrastructure-intensify-as-us-cybercrime-losses-hit-21-billion-exposes-risk/.

29. Reuters. Complaints about ransomware attacks on US infrastructure rise. URL: https://www.reuters.com/world/us/complaints-about-ransomware-attacks-us-infrastructure-rise-9-fbi-says-2025-04-23/.

30. DeepStrike. Vulnerability Statistics 2025. URL: https://deepstrike.io/blog/vulnerability-statistics-2025 (дата звернення: 28.05.2026).