МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
НАЦІОНАЛЬНА АКАДЕМІЯ ВНУТРІШНІХ СПРАВ
Інститут заочного та дистанційного навчання

Кафедра теорії, історії та філософії права

КВАЛІФІКАЦІЙНА РОБОТА
для здобуття ступеня вищої освіти магістра

на тему "ПУБЛІЧНЕ УПРАВЛІННЯ ТА АДМІНІСТРУВАННЯ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ"

Виконав:
здобувач 2 курсу 3 групи,
спеціальність 281 «Публічне управління та адміністрування»
Радченко Віталій Олександрович
Номер мобільного телефону:
095 022 11 14

Науковий керівник:
Доцент кафедри теорії, історії та філософії права,
кандидат юридичних наук, доцент
Власенко Валерій Павлович

Кваліфікаційна робота допущена до захисту
«4» грудня 2025 р., протокол № 8
завідувач кафедри теорії,
історії та філософії права,
кандидат юридичних наук, доцент

_____ Юрій КРИВИЦЬКИЙ

Київ-2026

ЗМІСТ

ВСТУП……. 3

РОЗДІЛ 1. ТЕОРЕТИКО-ПРАВОВІ АСПЕКТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ..... 8

1.1. Інформація як правова та соціальна категорія……... 8

1.2. Наукові підходи до розуміння категорії «інформаційна безпека»..... 14

1.3. Захист інформаційних прав і законних інтересів особи у системі інформаційної безпеки…….. 20

Висновки до розділу 1……. 24

РОЗДІЛ 2. АДМІНІСТРАТИВНЕ ТА ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ……. 26

2.1. Елементи системи забезпечення інформаційної безпеки…… 26

2.2. Роль держави в системі захисту інформаційної безпеки ……. 37

2.3. Забезпечення інформаційної безпеки в різних секторах суспільства …….. 43

Висновки до розділу 2…… 52

РОЗДІЛ 3. ПУБЛІЧНЕ УПРАВЛІННЯ ТА АДМІНІСТРУВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: СВІТОВИЙ ДОСВІД ТА НАПРЯМИ ПОДАЛЬШОГО РОЗВИТКУ 55

3.1. Підходи до публічного управління та адміністрування у сфері інформаційної безпеки в Сполучених Штатах Америки та Європейського Союзу…….. 55

3.2. Пріоритетні напрями розвитку адміністрування інформаційної безпеки України…….. 61

Висновки до розділу 3……. 76

ВИСНОВКИ……. 79

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ..... 85

ВСТУП

Актуальність теми. У сучасних умовах посилення цифровізації суспільних процесів, активного розвитку електронного урядування та швидкого обміну інформацією через цифрові канали, питання інформаційної безпеки набувають стратегічного значення для національної безпеки України. Інформаційна безпека охоплює захист державних інформаційних ресурсів, захист прав громадян у цифровому середовищі та протидію інформаційним загрозам як внутрішнього, так і зовнішнього характеру. Це зумовлює необхідність посилення ролі органів публічного управління у формуванні, реалізації та адмініструванні відповідних політик і механізмів захисту інформаційного простору на, що також вказують нормативно-правові акти, зокрема **«Стратегія інформаційної безпеки України», «Стратегія забезпечення державної безпеки», «**Про Доктрину інформаційної безпеки України» та ін.

Практичний аспект полягає у необхідності вжиття заходів щодо запобігання реальним викликам, пов’язаних з кіберзагрозами, витоком інформації, маніпулятивними інформаційними кампаніями та необхідністю ефективної координації між державними органами. Таким чином, зазначене ше раз вказує на те, що дослідження публічного управління та адміністрування інформаційної безпеки є надзвичайно важливим для практичної реалізації державної політики безпеки, удосконалення нормативно-правового забезпечення й підвищення національної стійкості.

Проблеми теорії інформації, інформаційного суспільства та інформації як соціально-правової категорії досліджували вчені Бєляков К. І., Дубас О. П., Пилипчук В. Г., Килимник І. І. та ін. Інформаційне право, інформаційні права людини та теоретико-правові засади інформаційної безпеки були предметом дослідження у працях Цимбалюк В. С., Марущак А. І., Виноградова Г. В.,

Ульянова Г. О., Арістова І. В., Недюха М. П. Максименко Ю. Є., Гріщенко А. О., Шульга В. І. та ін. Адміністративно-правове забезпечення інформаційної безпеки та роль держави досліджували Березовська І. Р., Олійник О. В., Лісовська Ю. П., Колпаков В. К., Соснін О. В., Харченко Л. С., Ліпкан В. А. та ін. Інформаційно-психологічна безпека, пропаганда, дезінформація зацікавили таких вчених Литвиненко О. В., Солодка О. М., Вознюк Є. В., Ничипорчук Н. І. Незважаючи на значний науковий доробок учених у сфері інформаційного права, інформаційної та кібербезпеки, **у контексті адміністративного управління та адміністрування інформаційної безпеки низка питань залишається недостатньо дослідженою або фрагментарно висвітленою п**роблематика механізмів міжвідомчої взаємодії, критеріїв оцінювання ефективності публічного адміністрування, інформаційної безпеки на місцевому рівні, цілісної моделі адміністративного управління інформаційною безпекою, адміністративних процедур і управлінських рішень. Таким чином, наше дослідження сприятиме зміцненню систем управління інформаційною безпекою в Україні та підвищенню ефективності реагування на сучасні інформаційні виклики.

Мета і завдання дослідження. *Метою* є теоретичне та правове дослідження публічного управління та адміністрування у сфері інформаційної безпеки в Україні. Зазначена мета зумовила постановку та виконання таких *завдань*:

– з’ясувати природу інформації як правової та соціальної категорії;

– дослідити наукові підходи до розуміння категорії «інформаційна безпека»;

– розкрити зміст інформаційної безпеки в контексті інформаційних прав і законних інтересів особи;

– з’ясувати та охарактеризувати елементи системи забезпечення інформаційної безпеки;

– визначити роль держави в системі захисту інформаційної безпеки;

– з’ясувати особливості забезпечення інформаційної безпеки в різних секторах суспільства;

– дослідити зарубіжний досвід публічного управління та адміністрування у сфері інформаційної безпеки;

– визначити пріоритетні напрями розвитку адміністрування інформаційної безпеки України, здійснити їх систематизацію.

Об’єктом дослідження є інформаційна безпека як соціальне явище.

Предметом дослідження є публічне управління та адміністрування інформаційної безпеки.

Наукова новизна одержаних результатів полягає в тому, що:

***вперше*:**

обґрунтовано комплексне розуміння інформації в системі публічного управління як одночасно об’єкта правового регулювання, інструмента управлінського впливу та засобу соціальної комунікації, що дозволило довести необхідність державного регулювання саме інформаційних процесів, а не лише інформаційних ресурсів;

системно доведено, що інформаційні права і свободи людини становлять ядро інформаційної безпеки, а державна політика у цій сфері має дуалістичний характер, поєднуючи захист інформаційного суверенітету держави та гарантування прав людини.

удосконалено:

наукові підходи до розуміння категорії «інформаційна безпека» шляхом обґрунтування доцільності застосування комплексного підходу, що поєднує її розуміння як стану захищеності, системи заходів і безперервного управлінського процесу;

структуру системи забезпечення інформаційної безпеки в Україні через деталізацію принципів, засобів, способів, методів та суб’єктів публічного управління.

дістало подальшого розвитку:

теоретичні положення адміністративно-правового забезпечення інформаційної безпеки в частині обґрунтування ризик-орієнтованого та превентивного підходів до публічного адміністрування;

наукові уявлення про напрями модернізації системи адміністрування інформаційної безпеки України шляхом уточнення пріоритетів нормативно-правового, інституційного та міжнародного розвитку.

Методологія дослідження. Для досягнення мети дослідження та виконання поставлених завдань у роботі використовується сукупність загальнонаукових і спеціально-юридичних методів пізнання, що забезпечують комплексний і системний підхід до аналізу публічного управління та адміністрування інформаційної безпеки в Україні.

Аналіз і синтез використовувалися для детального опрацювання змісту поняття «інформаційна безпека», розкриття її складових елементів та узагальнення наукових позицій щодо інформаційних прав і законних інтересів особи.

Формально-юридичний метод сприяв дослідженню нормативно-правових актів України, що регулюють питання інформаційної безпеки, визначення її змісту та правових механізмів реалізації.

Системно-структурний метод дозволив з’ясувати та характеризувати елементи системи забезпечення інформаційної безпеки, визначення взаємозв’язків між суб’єктами публічного управління, об’єктами захисту та інструментами адміністрування.

Порівняльно-правовий метод застосовувався з метою дослідження зарубіжного досвіду публічного управління та адміністрування у сфері інформаційної безпеки та визначення можливостей адаптації позитивних практик до українських реалій.

Метод правового прогнозування сприяв визначенню пріоритетних напрямів розвитку адміністрування інформаційної безпеки в Україні, їх систематизації та формуванню пропозицій щодо вдосконалення публічного управління з урахуванням сучасних викликів.

Практичне значення дослідження публічного управління та адміністрування інформаційної безпеки в Україні полягає в можливості використання отриманих теоретичних узагальнень, висновків і систематизованих матеріалів у науково-дослідницькій діяльності, практичній діяльності органів публічної влади та в освітньому процесі закладів вищої освіти, зокрема:

– у **науково-дослідницькій діяльності р**езультати дослідження можуть бути використані як теоретико-методологічна основа для подальших наукових розвідок у сфері інформаційного права, публічного управління та національної безпеки. Сформульовані підходи до розуміння природи інформації, інформаційної безпеки та ролі держави в її забезпеченні сприятимуть розвитку наукових дискусій, уточненню понятійно-категоріального апарату, а також слугуватимуть підґрунтям для підготовки наукових статей, кваліфікаційних і дисертаційних робіт;

– у **практичній діяльності** матеріали та висновки дослідження можуть бути використані в діяльності органів державної влади та органів місцевого самоврядування під час формування й реалізації державної політики у сфері інформаційної безпеки. Систематизація елементів системи забезпечення інформаційної безпеки, визначення ролі держави та аналіз зарубіжного досвіду можуть сприяти вдосконаленню управлінських рішень, розробленню нормативно-правових актів, програм і стратегій, а також підвищенню ефективності адміністрування інформаційної безпеки в різних секторах суспільства;

– в **освітньому процесі р**езультати дослідження можуть бути використані під час викладання навчальних дисциплін з публічного управління та адміністрування, інформаційного права, національної та інформаційної безпеки. Узагальнені матеріали доцільно застосовувати при підготовці навчальних посібників, методичних рекомендацій, лекційних курсів тощо.

РОЗДІЛ 1. ТЕОРЕТИКО-ПРАВОВІ АСПЕКТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1. Інформація як правова та соціальна категорія

Упродовж розвитку людства інформація завжди відігравала ключову роль як воєнний, політичний, економічний та соціальний чинник, що визначав поступ держав, суспільства і окремих людей у конкретних історичних умовах. Вміння людини збирати, накопичувати, переосмислювати й передавати інформацію стало фундаментальною передумовою формування людини як соціальної істоти. Саме ця здатність дала можливість налагоджувати взаємодію між людьми, передавати досвід і знання наступним поколінням та забезпечила прогрес цивілізації.

Наукове вивчення інформації, сутності та процесів її обробки, збереження, передачі й поширення почалося лише у XX столітті. Інформація стала предметом дослідження кібернетики − науки, що вивчає спільні закономірності управління в технічних системах, живих організмах та соціальних структурах.

У перекладі з латини слово «інформація» (information) означає роз’яснення або уявлення, тобто йдеться про певні відомості чи їх сукупність щодо предметів, явищ та процесів навколишнього світу. Інформація – це наукове поняття, що охоплює обмін відомостями між людьми, між людиною та технікою, між автоматизованими системами; обмін сигналами у світі тварин і рослин; передачу спадкових ознак між клітинами та організмами [1].

Цікаво звернути увагу на підходи до розуміння параметрів інформації, зокрема К. Бєляков до параметрів та критеріїв інформації відносить:

Зміст - обумовлює предметну область інформації. Нерозривно зв'язаний із параметром охоплення, що визначає, обмежує й описує зміст. Критерії: об'єм – загальна кількість інформації; повнота – співвідношення між наявною і

доступною інформацією; вірогідність – можливість досягнення мети при наявності доступної інформації.

Час – фіксує момент або період здійснення інформаційної взаємодії.

Джерело – ідентифікує походження інформації. Нерозривно зв'язаний з параметром охоплення.

Якість – визначає властивості, що відображають ступінь придатності інформації для досягнення мети. Критерії: адекватність – однозначна відповідність інформації відображеному об'єктові; вірогідність – відсутність в інформації схованих помилок; своєчасність – надходження інформації в межах того часу, коли вона корисна для ухвалення рішення; цінність – важливість, необхідність інформації для ухвалення рішення; актуальність – інтегрований критерій, що визначає своєчасність і цінність інформації в сукупності; новизна – вперше отримана інформація; корисність – придатність інформації для визначеної мети; доступність – можливість одержання інформації; захищеність – неможливість несанкціонованого використання (або зміни) інформації; ергономічність – зручність форми чи обсягу інформації; живучість – здатність інформації зберігати свою якість у часі.

Відповідність потребам. Необхідність в одержанні інформації для вирішення конкретних завдань. Критерії: пертинентність – відповідність змісту отриманої інформації потребі користувача; релевантність – відношення значеннєвої близькості між змістом інформації і запитом користувача; повнота – відношення релевантної інформації до усієї наявної; точність – відношення релевантної інформації до загальної сукупності релевантної і нерелевантної інформації; перевіряємість – приступність джерела для підтвердження істинності інформації.

Спосіб фіксації. Закріплення інформації на тих або інших носіях. Критерії: статичний – фіксація інформації в речовинному вигляді; динамічний – фіксація інформації у вигляді, придатному для комунікації по енергетичних каналах.

Мова. Засіб інформаційної взаємодії. Критерії: відсутність мовного бар'єра – фактор, сприятливий для створення, і використання інформації, здійснення

інформаційних взаємодій; наявність мовного бар'єра – фактор, що знижує можливість створення і використання інформації, здійснення інформаційних взаємодій.

Вартість. Упредметнений у продукті (фіксованої інформації) суспільний труд. Критерії: безкоштовна інформація – продукт інформаційної взаємодії, що представляється виробником у безкоштовне користування; платна інформація – продукт інформаційної взаємодії, що має ціну в грошовому вираженні і наданий у використання на платній основі [2, с. 20-21].

У правовій сфері увага традиційно приділялася регулюванню інформаційних процесів, пов’язаних зі сферою державної діяльності та захистом національних інтересів. Уже в найдавніших державах (Єгипет, Вавилон) існували поняття державної таємниці та передбачалися покарання за передачу важливої інформації ворогові. Це можна вважати початковими формами інформаційного права [3].

Існує багато визначень поняття «інформація». У загальному сенсі її розуміють як сукупність певних відомостей, даних або знань. Прийнято виділяти два ключових аспекти існування інформації. Перший − структурний, який відображає рівень впорядкованості чи організації системи або процесу та є їх внутрішньою характеристикою. Другий − відображувальний, пов’язаний зі здатністю об’єктів відображати вплив один одного. Якщо об’єкт змінюється під впливом іншого, то ці зміни містять інформацію про джерело впливу. У неживій природі цей процес пасивний, тоді як у живих істот, особливо в людини, − активний, адже включає не лише сприйняття, а й аналіз, інтерпретацію та передачу інформації.

А. Тоффлер підкреслював, що в сучасних системах державного управління інформація перетворилася на один із ключових ресурсів влади. Тому особливого значення набуває розбудова як внутрішніх комунікаційних систем, так і засобів масової інформації, які не лише забезпечують передачу керуючої інформації, а й формують авторитет державних органів у суспільстві. Інформаційне забезпечення управління сьогодні складається з потоків, каналів

та мереж передачі даних, а також із поєднання людських ресурсів і технологій, що забезпечують їх обробку [4, с. 4].

У тлумачному словнику з обчислювальної техніки вказано, що інформація − це сенс або значення даних, які люди можуть зрозуміти в певному контексті. Комп'ютери ж оперують лише даними без усвідомлення їх змісту [**5**]. Це підкреслює суб'єктивну природу інформації у соціальному вимірі: дані стають інформацією лише тоді, коли людина може їх інтерпретувати. Проте в правовому полі будь-які дані, що мають зовнішню форму, розглядаються як інформація незалежно від того, наскільки вони важливі для конкретної особи.

У межах інформаційного права інформацію розглядають як об'єкт регулювання лише тоді, коли навколо неї виникають суспільні відносини, тобто коли нею реально користуються конкретні особи. Відповідно, об'єктом регулювання є саме інформаційні процеси й відносини. Сьогодні поняття «інформація» є одним із найбільш застосовуваних у науці та практиці.

В кінці XX століття кардинально змінилось уявлення про інформацію та її роль у житті суспільства. Почав формуватися феномен інформаційного суспільства − суспільства, в якому обсяг інформації стрімко зростає, охоплюючи всі сфери людської діяльності. Основними ознаками такого суспільства є високий рівень інформованості населення, вільна діяльність ЗМІ, можливість отримувати об'єктивні дані та їх оцінки, доступність джерел інформації та технічних засобів її одержання.

Р. Кохане та Дж. Най пропонують поділ сучасної інформації на три основні типи: відкриту, комерційну та стратегічну. До відкритої належать телерадіопрограми, політична реклама, масові інформаційні акції, а також дані, доступні в мережі Інтернет. Комерційна інформація − це відомості, створені для продажу чи отримання прибутку, і з кожним роком її стає все більше. Загальний сенс існування інформації полягає в комунікації, а швидкий розвиток комунікаційних технологій багаторазово посилює обсяги та швидкість інформаційного обміну. Це, у свою чергу, спричиняє необхідність оновлення підходів до забезпечення інформаційної безпеки та таємності. Вартість

інформації − один із головних критеріїв її значущості для держави, бізнесу чи громадян [6, с. 85].

Зазначений поділ має значення для юридичного аспекту інформації, що пов’язане передусім зі змістом та впливом, який вона може чинити на суспільні процеси. Саме зміст дозволяє визначати правовий режим інформації: чи становить вона державну або комерційну таємницю, чи є об’єктом авторського права, чи може поширення таких відомостей завдати шкоди державі чи приватним особам, а також чи законним є обмеження доступу до певних даних.

Конституція України (статті 31–35) гарантує низку інформаційних прав громадян [7]. Стаття 34, зокрема, закріплює право кожного збирати, зберігати, використовувати і поширювати інформацію у будь-якій формі. Обмеження цих прав можливе лише на підставі закону.

Закон України «Про інформацію» визначає інформацію як документовані або публічно оголошені відомості про події й явища, що відбуваються в суспільстві, державі чи природі [8]. Таке визначення є гарантією свободи думки, совісті та переконань, оскільки внутрішні переконання людини не регулюються правом. Це означає, що юридичне значення має лише та інформація, яка має зовнішнє вираження і доступна для використання іншими. Отже, інформація стає об’єктом правового регулювання лише тоді, коли включена в суспільний обіг.

Виходячи зі змісту інформації, її можна класифікувати за різними критеріями: за значенням для суспільства та окремих людей, за галузевою приналежністю, за режимом доступу (відкрита та закрита). Відкриту інформацію поділяють на вільну та комерційну, закриту – на приватну, комерційну та державну таємницю.

Закон України «Про інформацію» визначає основні види інформації: статистичну, адміністративну, масову, інформацію про діяльність органів влади, правову інформацію, дані про особу, довідково-енциклопедичну та соціологічну інформацію [8].

Статистична інформація − це офіційні дані, що відображають кількісні показники соціально-економічних та інших процесів. Адміністративна інформація − офіційні дані, які збираються органами влади для виконання їхніх функцій. Масова інформація включає друковану й аудіовізуальну інформацію, яка поширюється через пресу, телебачення, радіо, кіно та інші засоби комунікації [8].

Важливу роль відіграє правове регулювання збору та поширення інформації про особу. Конституція України запроваджує поняття конфіденційної інформації та забороняє її обіг без згоди особи, за винятком випадків, передбачених законом. Закон «Про інформацію» визначає дані про особу як документовані чи публічно оголошені відомості про її приватне життя, проте чітко не поділяє їх на відкриті та конфіденційні, що дозволяє виділити два типи інформації про особу – відкриту та закриту [8].

Згідно ч. 1 ст. 21 Закону України “Про інформацію”, інформація державних органів та органів місцевого самоврядування – це офіційна документована інформація, яка створюється в процесі поточної діяльності законодавчої, виконавчої та судової влади, органів місцевого самоврядування. Основними джерелами інформації державних органів та органів місцевого самоврядування є законодавчі акти України, інші акти, що приймаються Верховною Радою та її органами, акти Президента України, підзаконні нормативні акти, ненормативні акти державних органів, акти органів місцевого самоврядування.

Кожна інформація має кількісні, змістовні та ціннісні характеристики. Кількість може вимірюватися, наприклад, у байтах або в тому, наскільки вона зменшує невизначеність. Зміст – це те, що людина розуміє з отриманих даних. Цінність – це значення інформації для суспільства чи окремої особи, яке може оцінюватися як у матеріальному, так і в нематеріальному вимірі.

Отже, предметом інформаційної безпеки є тільки та інформація, яка підпадає під національне та міжнародне правове регулювання, а також суспільні відносини, що виникають у процесі її створення, обробки та

поширення. Наявність нормативно-правової бази є ключовим інструментом захисту національних інтересів у будь-якій сфері, оскільки саме вона дозволяє державі діяти ефективно та в межах закону.

1.2. Наукові підходи до розуміння категорії «інформаційна безпека»

Дослідження проблематики та ключових напрямів адміністративно-правового забезпечення інформаційної безпеки спирається на норми Конституції України, де підкреслюється: «Захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу» [ст.17, 7]. Саме ця вимога зумовила потребу в чіткому визначенні змісту поняття інформаційної безпеки, її структури та предмету правових досліджень.

Для якісного аналізу досліджуваної проблеми було уточнено базові поняття, серед яких головним є «інформаційна безпека». Базове поняття «безпека» входить до ширших категорій – «національна безпека», «економічна безпека» тощо, а також є основою для розуміння інформаційної безпеки. У загальному тлумаченні «безпека» означає відсутність загроз для людини, суспільства, держави та довкілля. У словнику української мови безпека визначається як стан, за якого ніщо не становить загрози [9, с.19].

В. Цимбалюк пропонує розглядати поняття «безпека» у трьох аспектах: управлінському (оцінному) – як стан; нормативно-правовому – як систему суспільних відносин; організаційному – як процес [10, с. 213–242; 11, с. 30–33].

На думку В. Забродського та Н. Кизима, безпека характеризується через здатність системи зберігати життєздатність та розвиватися навіть за умов внутрішніх і зовнішніх загроз [12, с. 50].

Особливе місце у дослідженні займає поняття «національна безпека», оскільки воно дає змогу глибше зрозуміти природу інформаційної безпеки та її

взаємозв’язки з іншими сферами державної діяльності. Відповідно до Закону України «Про національну безпеку України», національна безпека визначається як захищеність державного суверенітету, територіальної цілісності, демократичного ладу та інших національних інтересів від реальних і потенційних загроз [13].

Поняття «інформаційна безпека» еволюціонувало протягом останніх десятиліть: у 1960-х роках використовувався термін «комп’ютерна безпека»; у 1970-х – «безпека даних»; у 1990-х відбулася структуризація підходів, до складу яких увійшли конфіденційність, аутентифікація, цілісність, управління доступом тощо [14].

У науковій літературі поняття інформаційної безпеки трактується неоднозначно. Наприклад, О. Литвиненко та О. Додонов визначають інформаційну безпеку як систему захисту та контролю інформаційного простору [15, с.14].

М. Гуцалюк, Н. Гайсенюк та О. Степко розглядають інформаційну безпеку як стан інформаційної сфери суспільства або захищеність інформації й життєво важливих інтересів особи, суспільства і держави [16].

Ряд учених (Р. Калюжний, В. Голубєв, В. Гавловський) пропонують розуміти інформаційну безпеку як суспільні правовідносини. У їхній інтерпретації національна безпека є процесом, а не статичною категорією [17, с. 17–21].

В. Шульга узагальнила наявні підходи до визначення поняття «інформаційна безпека», виділивши кілька основних аспектів. **1. Нормативно-правовий аспект.** На основі аналізу законодавчих актів інформаційну безпеку визначають як складову частину політичної, економічної, оборонної та інших сфер національної безпеки. **2. Доктринальний аспект.** У працях науковців і фахівців пропонуються різні інтерпретації цього терміна:

- інформаційна безпека – це стан правового регулювання та відповідних інституцій безпеки, що гарантують постійну доступність даних, необхідних для

стратегічного управління, а також забезпечують захист інформаційних ресурсів держави;

- інформаційна безпека розглядається як захист об'єкта від інформаційних загроз або негативних впливів, пов'язаних з інформацією, включно з нерозголошенням відомостей, що становлять державну таємницю;

- інформаційна безпека трактується як захищеність установлених законом правил, за якими здійснюються інформаційні процеси в державі, що забезпечують гарантовані Конституцією умови існування та розвитку особи, суспільства і держави.

3. Енциклопедичний аспект. На основі словникових та енциклопедичних джерел інформаційну безпеку визначають як: нормативне формування державної інформаційної політики; забезпечення свободи інформаційної діяльності та права на доступ до інформації в національному інформаційному просторі; розроблення та впровадження безпечних інформаційних технологій; охорону державної таємниці та інформації з обмеженим доступом; захист національного інформаційного простору від поширення спотвореної або забороненої інформаційної продукції [*18*]**.**

Ю. Максименко підкреслює тісний зв'язок інформаційної безпеки з правовим регулюванням, наголошуючи, що право одночасно і підтримує, і формується під впливом безпекових потреб [19, с. 48].

С. Марущак пропонує визначати інформаційну безпеку через комплекс прав людини у сфері інформації: свободу доступу, поширення та отримання даних, а також право на захист приватності та від недостовірної інформації [20,с. 82].

Л. Харченко, В. Ліпкан та О. Логінов трактують інформаційну безпеку як складову національної безпеки та процес управління загрозами, що забезпечує інформаційний суверенітет держави [21, с. 46].

Більшість сучасних дослідників сходяться на тому, що інформаційна безпека є станом захищеності інформаційного середовища держави, що забезпечує його стале функціонування навіть під впливом зовнішніх і внутрішніх загроз. У юридичній енциклопедії інформаційна безпека визначається як вид національної безпеки та важлива державна функція, що охоплює формування інформаційної політики, забезпечення доступу до інформації, охорону державної таємниці, створення безпечних технологій та захист інформаційного простору [1, с. 714].

І. Березовська зазначає, що термін «інформаційна безпека» найчастіше вживається у двох значеннях: як стан (якість) об'єкта та як діяльність із його захисту [22, с. 29].

А. Гріщенко пропонує ввести у науковий обіг поняття «Національна інформаційна безпека» – це такий рівень захищеності національних інтересів особи, суспільства та держави в інформаційній сфері, який досягається завдяки своєчасному виявленню, попередженню та усуненню загроз і проявів агресії в цій сфері. Діяльність із забезпечення національної інформаційної безпеки полягає у вжитті уповноваженими державними органами заходів, спрямованих на створення та підтримання стану захищеності інтересів людини, суспільства і держави шляхом запобігання, недопущення та нейтралізації небезпек в інформаційному просторі. Об'єктами, на які спрямовано діяльність системи забезпечення інформаційної безпеки, виступають людина, суспільство та держава – саме вони потребують захисту від інформаційних загроз [23, с. 131].

У міжнародних дослідженнях інформаційну безпеку зазвичай визначають як захист життєво важливих інтересів держави, суспільства та особи від цілеспрямованих чи випадкових інформаційних впливів (дезінформація, інформаційна війна тощо).

Таким чином, з урахуванням різних підходів інформаційну безпеку доцільно розглядати як комплекс взаємопов'язаних превентивних заходів, спрямованих на захист національних інтересів у сфері інформаційної діяльності, підтримку інформаційного суверенітету та стабільного розвитку

інформаційного простору України. Державна політика у сфері інформаційної безпеки має забезпечувати захист особи, суспільства та держави, інформаційного суверенітету, суспільної свідомості й психіки від реальних і потенційних загроз.

Інформаційна безпека у цьому розумінні – це система дій, спрямованих на гарантування захищеності життєво важливих інтересів, підтримку політичного, економічного, науково-технологічного, гуманітарного розвитку, обороноздатності та функціонування державного управління; попередження маніпуляцій, дезінформації та інших негативних впливів.

Сучасна правова база України демонструє позитивну динаміку у сфері розвитку інформаційної безпеки. Прийняття законів «Про інформацію», «Про доступ до публічної інформації», «Про захист персональних даних» створило умови для демократизації інформаційних процесів та захисту прав громадян. Водночас відсутність завершеного нормативно-правового визначення понятійного апарату інформаційної безпеки ускладнює ефективне адміністративно-правове регулювання цієї важливої сфери.

Наприклад, у **Стратегії інформаційної безпеки закріплено дефініція** «Інформаційна безпека України», що тлумачиться як складова національної безпеки та означає такий рівень захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших життєво важливих інтересів особи, суспільства і держави, за якого належно гарантуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, а також доступ до достовірних і об’єктивних відомостей. У межах цього поняття передбачено функціонування ефективної системи протидії негативним інформаційним впливам, включно з координованим поширенням недостовірних даних, деструктивною пропагандою, іншими інформаційними операціями, а також несанкціонованим розповсюдженням, використанням чи порушенням цілісності інформації з обмеженим доступом [24].

Проведений огляд наукових підходів демонструє, що поняття інформаційної безпеки в українській та міжнародній доктрині є багатогранним і охоплює як стан захищеності, так і комплекс дій, спрямованих на запобігання загрозам. Інформаційна безпека тісно пов’язана з національною безпекою, оскільки забезпечує захист суверенітету, стабільність державного управління, стійкість суспільної свідомості та гарантує реалізацію прав громадян у інформаційній сфері.

Аналіз показує, що вчені трактують інформаційну безпеку через різні підходи – нормативно-правовий, організаційний, доктринальний, енциклопедичний, акцентуючи увагу або на правовідносинах, або на захищеності інформаційного середовища, або на свободах і правах людини в інформаційній сфері. Незважаючи на відмінності, більшість дослідників сходяться в тому, що інформаційна безпека включає комплекс превентивних заходів, спрямованих на забезпечення стійкого функціонування держави, захисту її інформаційного суверенітету та мінімізації впливу зовнішніх і внутрішніх загроз.

Українське законодавство демонструє поступ у напрямі зміцнення правових основ інформаційної безпеки, однак відсутність чіткого й завершеного понятійного апарату все ще гальмує ефективне адміністративно-правове регулювання. Це потребує подальшого вдосконалення законодавства та узгодження наукових підходів для формування цілісної системи інформаційної безпеки.

Отже, інформаційна безпека має розглядатися як стратегічний пріоритет держави, що охоплює захист особи, суспільства й держави, забезпечення інформаційного суверенітету та формування стійкого, захищеного й демократичного інформаційного простору України.

1.3. Захист інформаційних прав і законних інтересів особи у системі інформаційної безпеки

У сучасних умовах суспільно-політичного розвитку інформація набула статусу стратегічного ресурсу. Це природний етап глобальної еволюції, коли розвиток інформаційних і телекомунікаційних технологій спричиняє трансформації в економічних процесах, соціальній структурі, правових інститутах, культурній сфері та державному управлінні. Значна частина ключових інтересів людини, суспільства, держави та світової спільноти сьогодні залежить від рівня розвитку та захищеності інформаційного середовища.

У цьому контексті Конституційний Суд України визначає «охоронюваний законом інтерес» як прагнення особи скористатися певним матеріальним чи нематеріальним благом, що випливає зі змісту об'єктивного права та не оформлене у суб'єктивне право, але водночас підлягає судовому захисту й іншим правовим механізмам охорони [25].

У Законі України «Про Основні засади розвитку інформаційного суспільства…» наголошено, що одним із провідних завдань держави є формування відкритого інформаційного суспільства, орієнтованого на потреби людини, у якому кожний громадянин може створювати, накопичувати й використовувати знання, а також вільно обмінюватися інформацією [26].

Закон України «Про національну безпеку України» визначає національну безпеку як стан захищеності життєво важливих інтересів особи, суспільства та держави, що забезпечує сталий розвиток і своєчасне реагування на потенційні загрози [13]. Національні інтереси трактується як сукупність матеріальних, інтелектуальних і духовних цінностей Українського народу, реалізація яких

забезпечує його розвиток та суверенітет. Центральною їх складовою виступає можливість протидії небезпекам і ризикам [27, с. 58].

Конституція України у ст. 17 визначає захист інформаційної безпеки однією з найважливіших функцій держави [7]. Також у ст. 3 закріплено, що життя, честь, гідність, недоторканність і безпека людини є найвищою соціальною цінністю. Стаття 34 гарантує свободу думки, слова та право кожного збирати, зберігати, використовувати й поширювати інформацію. У сукупності ці норми формують правові гарантії інформаційних прав людини та її юридичної безпеки. Громадяни у сфері державного управління переважно виступають як споживачі інформації та реалізують свої права через доступ до відомостей, необхідних для задоволення індивідуальних чи суспільних потреб [27, с. 28].

Адміністративно-правовий статус особи охоплює права, свободи, охоронювані законом інтереси й обов'язки в адміністративних правовідносинах. Основні інформаційні права громадян визначені у ст. 43 Закону України «Про інформацію» [8]. До них належать: можливість отримувати, використовувати, поширювати та зберігати інформацію, а також право на доступ до відомостей щодо діяльності органів влади.

Забезпечення інформаційної безпеки у сфері прав людини передбачає недопущення розголошення інформації з обмеженим доступом, захист права власності на інформацію та запобігання незаконному обмеженню свободи слова і доступу до інформації. Оскільки людина потребує постійного отримання відомостей про суспільні процеси, інформація стає невід'ємною складовою комунікації та діяльності. Це зумовлює посилений інтерес до регулювання інформаційних відносин і до прав суб'єктів цих відносин. Серед ключових напрямів державної інформаційної політики – забезпечення доступу громадян до інформації, розбудова національних інформаційних мереж, удосконалення правових і організаційних механізмів захисту інформації.

Інформаційна політика України зорієнтована на підтримку свободи слова, безперешкодного доступу до інформації та інших стандартів, характерних для

інформаційного суспільства. Тому головним об’єктом інформаційної безпеки виступає людина, а її права і свободи – ключова цінність, що потребує захисту. Також законодавець об’єднав життєво важливі інтереси суспільства та держави в єдиний перелік. До них належать: захист українського суспільства від деструктивної та агресивної пропаганди, насамперед з боку Російської Федерації; протидія інформаційному впливу Росії, спрямованому на пропаганду війни, розпалювання міжнаціональної та міжрелігійної ворожнечі, спроби насильницької зміни конституційного ладу чи посягання на суверенітет і територіальну цілісність України; забезпечення громадян, підприємств, установ і організацій усіх форм власності достовірною та об’єктивною інформацією; гарантування вільного обігу інформації у межах, визначених законом; розвиток і захист національної інформаційної інфраструктури; збереження та примноження духовних, культурних і моральних надбань Українського народу; забезпечення всебічного розвитку та функціонування української мови в усіх сферах суспільного життя на території України; підтримка вільного розвитку, використання й охорони мов національних меншин та сприяння вивченню мов міжнародного спілкування; посилення інформаційних зв’язків з українською діаспорою та підтримка збереження її етнокультурної самобутності та ін. [28].

Право на інформацію, передбачене Законом України «Про інформацію», гарантується через обов’язок органів влади інформувати про свою діяльність, створення відкритих інформаційних систем, забезпечення доступу до архівів, бібліотек, музеїв, а також через механізми контролю та відповідальності [29, с. 31].

Правозахисні функції держави у сфері інформаційної безпеки регламентовані розділом 5 Закону «Про інформацію». Зокрема, забороняється цензура, втручання у діяльність медіа, необґрунтоване обмеження доступу до інформації, а також передбачено відповідальність за її приховування, спотворення, незаконне поширення, розголошення та інші правопорушення [8].

Інформаційне законодавство покликане гарантувати реалізацію конституційного права кожного на вільне збирання, зберігання і поширення інформації; розвиток України як інформаційної держави; захист авторських прав і права власності на інформаційні ресурси; формування конкурентного інформаційного ринку; ефективне використання національних інформаційних ресурсів та їх захист [30, с. 169].

У третьому розділі Доктрини інформаційної безпеки подано детальний перелік національних інтересів України в інформаційній сфері. До найважливіших інтересів особи віднесено: гарантування конституційних прав і свобод людини щодо збирання, зберігання, використання та поширення інформації; забезпечення права на захист приватного життя; а також убезпечення від шкідливих інформаційно-психологічних впливів [**28**].

Захист прав і свобод у сфері інформаційної безпеки є важливою умовою національної безпеки загалом. Держава має забезпечувати захист громадян від незаконних обмежень та інформаційних загроз. Це сприятиме розвитку демократичних інститутів, зміцненню довіри до влади, активізації громадянського суспільства та формуванню правової держави [31, с. 265].

Доступ до відкритої інформації забезпечується через офіційні публікації, поширення в медіа та надання відповідей на запити зацікавлених осіб. Узагальнення проведеного аналізу дає змогу трактувати «інтерес» в інформаційній сфері як наявність умов і засобів для задоволення усвідомленої потреби шляхом цілеспрямованої діяльності. Зростання ролі законного інтересу пов’язане з розвитком правової держави та індивідуалізацією суспільних відносин. Таким чином, інтереси інформаційної безпеки безпосередньо випливають із фундаментальних цінностей – прав людини, свободи, економічного добробуту. А отже, ключовим інтересом України залишається зміцнення власної державності та захист основних цінностей, серед яких інформаційна безпека займає провідне місце.

Проведений аналіз свідчить, що інформаційні права та законні інтереси є центральним елементом системи інформаційної безпеки України. Їх захист

ґрунтується на конституційних принципах, міжнародних стандартах та розвиненому інформаційному законодавстві. Інформаційна безпека в цьому контексті не зводиться лише до технічного чи організаційного захисту даних – вона охоплює широкий комплекс прав людини, що гарантують свободу слова, доступ до інформації, недоторканність приватного життя та право на достовірні дані.

Забезпечення цих прав є одним із ключових завдань держави, оскільки від рівня їх реалізації залежить розвиток демократії, прозорість влади, формування громадянського суспільства та зміцнення національної безпеки. Інтереси інформаційної безпеки, таким чином, ґрунтуються на фундаментальних цінностях – свободі, гідності людини, праві на інформацію й можливості участі у суспільному житті. Саме захист цих прав визначає стратегічний напрям розвитку України як незалежної, демократичної та інформаційно стійкої держави.

Висновки до розділу 1.

Отже, дослідивши питання про природу інформації як правової та соціальної категорії, наукові підходи до розуміння категорії «інформаційна безпека», про зміст інформаційної безпеки в контексті інформаційних прав і законних інтересів особи можемо зробити наступні висновки:

інформація є базовою соціально-правовою категорією, що супроводжує розвиток людства та виступає визначальним ресурсом у політичній, економічній, воєнній і соціальній сферах. У правовому вимірі інформація набуває значення об’єкта регулювання лише за умови її включення в суспільні відносини та наявності зовнішньої форми вираження. **Багатогранність поняття «інформація» зумовлює різноманітність наукових підходів до її**

розуміння, зокрема структурного, відображувального, комунікативного та ціннісного. Це свідчить про міждисциплінарний характер інформації та необхідність комплексного правового регулювання інформаційних відносин**,** що виникають у процесі її створення, збирання, обробки, зберігання, доступу та поширення. Саме ці процеси формують предмет правового впливу та визначають правовий режим інформації. **Формування інформаційного суспільства кардинально змінює роль інформації,** перетворюючи її на стратегічний ресурс держави та інструмент впливу на суспільну свідомість. Це актуалізує питання правового забезпечення доступу до інформації, її достовірності, захищеності та безпеки;

інформаційна безпека є складовою національної безпеки України та розглядається в науці як багатовимірне явище: як стан захищеності інформаційного середовища, як система правових, організаційних та превентивних заходів,і як процес управління інформаційними загрозами. **Відсутність єдиного універсального визначення інформаційної безпеки в науковій доктрині** зумовлена складністю самої категорії та різницею дослідницьких підходів. Водночас переважна більшість учених сходяться на тому, що її ключовою метою є захист життєво важливих інтересів особи, суспільства та держави в інформаційній сфері;

інформаційні права і законні інтереси особи становлять ядро системи інформаційної безпеки. Захист свободи слова, права на доступ до інформації, недоторканності приватного життя та захисту від деструктивних інформаційних впливів є необхідною умовою демократичного розвитку держави. **Держава відіграє провідну роль у забезпеченні інформаційної безпеки,** реалізуючи її через нормативно-правове регулювання, інформаційну політику та діяльність уповноважених органів. Водночас ефективність цієї діяльності значною мірою залежить від ефективності адміністрування, узгодженості законодавства та чіткості понятійного апарату. **Інформаційна безпека має розглядатися як стратегічний пріоритет державної політики**,

спрямований на захист інформаційного суверенітету, забезпечення прав людини, стійкість суспільної свідомості та стабільне функціонування демократичної правової держави.

РОЗДІЛ 2. АДМІНІСТРАТИВНЕ ТА ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

2.1. Елементи системи забезпечення інформаційної безпеки

Аналіз основних підходів до забезпечення інформаційної безпеки свідчить, що українське законодавство вже сформувало необхідні теоретичні передумови для створення системи принципів організації та управління у сфері інформаційної безпеки. Водночас подальша конкретизація існуючих принципів і формування нових, більш ефективних підходів залишається актуальним завданням.

Оскільки будь-який принцип управління має своє функціональне призначення, вони дозволяють окреслити сталі характеристики об’єкта незалежно від умов. Управління інформаційною безпекою на основі таких принципів означає здатність виявляти й використовувати потенціал системи для підтримання її стабільних якостей у часі та просторі. Тому формування цілісної системи принципів управління інформаційною безпекою підвищує методологічний рівень відповідності механізмів інформаційної безпеки соціально-економічним умовам держави.

В. Колпаков у своїх працях визначає принципи державного управління як закономірності, що пізнані теорією і практикою та зафіксовані в поняттях управлінської науки. Він виокремлює три групи принципів:

1. соціально-політичні (демократизм, участь населення в управлінні, рівність, законність, гласність, об’єктивність);

2. організаційні принципи побудови апарату управління (галузевий, функціональний, територіальний);

3. організаційні принципи функціонування (нормативність, колегіальність, єдиноначальність, поділ праці, відповідальність, оперативна самостійність) [32, с. 21–22].

Принципи забезпечення інформаційної безпеки, таким чином, виступають базовими положеннями для функціонування всієї системи національної безпеки та регулювання поведінки громадян, державних і суспільних інституцій у цій сфері. Їх поділяють на загальні (гуманізм, соціальна справедливість, об'єктивність, ефективність, опора на довіру суспільства, поєднання відкритості та професійної таємниці, законність) і спеціальні, серед яких першорядним визначено принцип глобальності.

Закон України «Про національну безпеку України» визначає такі ключові принципи: верховенство права, пріоритет прав людини, мирні засоби вирішення конфліктів, адекватність заходів захисту, розмежування повноважень органів влади, демократичний цивільний контроль, використання міжнародних механізмів безпеки [13].

Застосування норм законодавства у сфері кібербезпеки та ухвалення суб'єктами владних повноважень рішень з метою реалізації Закону України «Про основні засади забезпечення кібербезпеки України» здійснюється з обов'язковим дотриманням таких принципів:

1. принципу мінімально необхідного регулювання, відповідно до якого рішення і заходи суб'єктів владних повноважень мають бути обґрунтовано необхідними та достатніми в мінімальному обсязі для досягнення мети і виконання завдань, визначених цим Законом;

2. принципу об'єктивності та правової визначеності, що передбачає максимально повне застосування норм національного й міжнародного права щодо прав, обов'язків і повноважень органів державної влади, підприємств, установ, організацій та громадян у сфері кібербезпеки;

3. принципу забезпечення захисту прав користувачів інформаційно-комунікаційних систем, послуг у сфері захисту інформації та кіберзахисту, а

також споживачів електронних комунікаційних послуг, зокрема прав на невтручання в приватне життя та захист персональних даних;

4. принципу прозорості, згідно з яким рішення або заходи суб'єктів владних повноважень повинні бути належним чином мотивовані та доведені до відома осіб, яких вони стосуються, до моменту набрання ними чинності або початку їх застосування;

5. принципу збалансованості вимог і відповідальності, який полягає у забезпеченні рівноваги між встановленням відповідальності за порушення вимог кібербезпеки та кіберзахисту і недопущенням запровадження надмірних вимог чи обмежень;

6. принципу недискримінації, відповідно до якого рішення, дії чи бездіяльність суб'єктів владних повноважень не повинні призводити до необґрунтованого обмеження або нерівності в юридичному чи фактичному обсязі прав і обов'язків осіб [33].

Узагальнено принципи забезпечення інформаційної безпеки, що включають:

– пріоритет прав і свобод людини;

– верховенство права;

– відповідальність держави перед громадянами;

– комплексність підходів;

– єдність і взаємозв'язок напрямів безпеки;

– чітке розмежування повноважень органів влади;

– участь у міжнародних системах;

– превентивність, оперативність і адекватність захисних заходів [31].

Методологія адміністративного права та система методів державного управління інформаційною безпекою мають реалізовувати ідейні засади, закладені Конституцією України: пріоритетність прав людини, розбудова демократичної правової держави, формування національної ідеї, захист особи, суспільства та держави від загроз.

Наука адміністративного права виділяє різні класифікації методів державного управління: адміністративні та економічні; морально-політичні; морально-ідеологічні; методи переконання, заохочення й примусу тощо. На думку В. Колпакова, їх різноманітність зумовлена широким спектром функцій державного управління. Методи відображають владний вплив суб’єкта управління, є формою реалізації повноважень та завжди мають конкретного адресата [32, с. 183–184].

Методи правового регулювання реалізуються Верховною Радою, що встановлює законодавчі норми у сфері інформаційної безпеки, визначає повноваження та відповідальність суб’єктів, систему контролю та порядок забезпечення діяльності [31].

Методи державного управління у сфері інформаційної безпеки проявляються у діяльності виконавчої влади, яка забезпечує виконання підзаконних актів, контролює дотримання правових норм та організовує заходи із запобігання загрозам.

Серед ключових методів управління в інформаційною безпекою виділяють:

– метод системності, що дозволяє бачити сукупність суб’єктів інформаційної безпеки як єдину структуру;

– метод централізації та ієрархічності, який забезпечує підпорядкованість і чітку організацію органів влади;

– метод координації, що регулює співпрацю між органами;

– метод примусу, спрямований на забезпечення виконання правових вимог;

– адміністративно-політичний метод, пов'язаний із формуванням політики держави;

– метод прогнозування та планування, необхідний для попередження загроз та стратегічного реагування.

Правовими способами адміністрування у сфері інформаційної безпеки є дозволи, заборони та зобов’язання. На практиці управління такими способами

можна вважати ліцензування та сертифікація, встановлення юридичної відповідальності за інформаційні правопорушення, управлінські приписи та розпорядження; контроль і нагляд за дотриманням законодавства; застосування адміністративного примусу, фінансування заходів інформаційної безпеки, державна підтримка розвитку інформаційної інфраструктури, стимулювання інновацій у сфері захисту інформації.

Правові засоби забезпечення інформаційної безпеки охоплюють приписи, заборони й дозволи [32, с. 56–57]. І. Березовська виділяє дозвільні, реєстраційні та примусові адміністративно-правові засоби [34].

Політичні засоби стосуються забезпечення реального народовладдя, цивілізованої політичної конкуренції та врахування позицій суспільства при формуванні політики. Ідеологічні засоби відіграють роль у консолідації нації, при цьому Конституція гарантує ідеологічний плюралізм. Ю. Тодика підкреслює, що навіть багатоманітність є певною державною ідеологією, яка уникає монополізму та формує національну ідею [35, с. 40–41].

Інформаційні засоби державної політики включають формування суспільної підтримки напрямів інформаційної безпеки, викриття джерел інформаційних впливів та координацію інформаційної діяльності органів влади. Технологічні засоби охоплюють організаційно-технічні, інженерні, криптографічні та інші інструменти, що забезпечують функціонування системи інформаційної безпеки у всіх сферах державної діяльності.

Інформаційні засоби становлять собою елементи державної інформаційної політики, спрямовані на підтримку реалізації внутрішнього і зовнішнього політичного курсу держави. До них належать:

– формування у населення позитивного ставлення до напрямів, заходів і цілей державної політики у сфері інформаційної безпеки;

– виявлення внутрішніх і зовнішніх джерел негативних інформаційних та інформаційно-психологічних впливів, спрямованих проти України, а також надання їм належної правової оцінки відповідно як до норм чинного законодавства, так і до міжнародного права;

– забезпечення узгодженої діяльності інформаційних підрозділів і служб усіх гілок влади, спрямованої на інформування громадян України та міжнародної спільноти про державну політику у відповідній сфері, а також гармонізацію оцінок подій та процесів у цій галузі.

Технологічні засоби – це комплекс організаційних, організаційно-технічних, інженерно-технічних, криптографічних та спеціальних інструментів, що забезпечують створення та належне функціонування правового режиму системи інформаційної безпеки.

Вибір конкретних технологічних засобів визначається напрямами забезпечення інформаційної безпеки, а саме:

– гарантування безпечного функціонування всіх елементів національного інформаційного простору, включно з об’єктами та суб’єктами;

– забезпечення інформаційної безпеки в політичній, економічній, оборонній сферах, у сфері державної безпеки та правопорядку, соціально-гуманітарній, науково-технологічній, екологічній та безпосередньо інформаційній;

– створення системи охорони та технічного захисту інформації, що становить державну таємницю або має обмежений доступ;

– виявлення інформаційних та інформаційно-психологічних впливів на особу, суспільні та державні інституції; виявлення кібератак, застосування проти України інформаційної зброї, а також протидія і нейтралізація джерел внутрішніх і зовнішніх загроз [31].

Засоби кадрового забезпечення – це система прийомів і способів добору та розподілу кадрів на посадах органів державного управління з урахуванням професійної підготовки та моральних характеристик. Така система включає ефективно організовані навчальні програми, спеціалізовані курси підготовки кадрів для різних рівнів державного управління та напрямів забезпечення інформаційної безпеки.

Матеріально-технічні та фінансові засоби забезпечення визначаються як економічні інструменти створення умов для формування та підтримання

функціонування державної системи інформаційної безпеки, діяльності органів державної влади й місцевого самоврядування, їхніх спеціальних підрозділів і служб. Вони забезпечують можливість застосування засобів, заходів та сил інформаційного протистояння з метою охорони національних інтересів.

Діяльність суб'єктів адміністративно-правового забезпечення інформаційної безпеки виступає одночасно основною формою реалізації правового регулювання у відповідній сфері та їхньою ключовою функцією. Вона полягає у виконанні наданих повноважень для розв'язання завдань державного управління щодо захисту інформаційної безпеки особи, суспільства та держави.

До елементів системи забезпечення інформаційної безпеки України, поряд із центральними та місцевими органами виконавчої влади, органами державної влади та місцевого самоврядування, підприємствами й організаціями різних форм власності, належать також громадські об'єднання та окремі громадяни, які беруть участь в інформаційних процесах.

У науковій літературі виділяють кілька рівнів системи суб'єктів забезпечення інформаційної безпеки в Україні:

– рівень Президента України, який очолює Раду національної безпеки і оборони;

– законодавчий рівень, що визначає правові засади інформаційної безпеки, статус її суб'єктів, структуру органів влади та їх компетенцію;

– виконавчий рівень, який включає значну кількість органів державної виконавчої влади;

– рівень судових органів (зокрема Конституційного Суду) та прокуратури, які стежать за дотриманням правових норм у сфері інформаційної безпеки;

– правоохоронний рівень, представлений МВС, спеціальними службами й органами безпеки, що здійснюють оперативно-розшукову та превентивну діяльність;

– функціональний рівень, представлений інститутами держави, що реалізують комплекс заходів з інформаційної безпеки;

– науково-дослідний рівень.

Суб’єктами забезпечення інформаційної безпеки є організації, служби, інститути та окремі фахівці (оперативні працівники, співробітники служб безпеки, інженерно-технічні спеціалісти служб захисту інформації тощо), які виконують практичні заходи щодо реалізації механізмів інформаційної безпеки.

Особливо важливу роль у системі органів забезпечення інформаційної безпеки відіграє Міністерство внутрішніх справ України. У Національній поліції функціонує кіберполіція, яка протидіє злочинам у сфері інформаційної безпеки, включно з:

– соціальною інженерією як технологією маніпуляції людьми в інтернет-просторі;

– malware – створенням та поширенням вірусів і шкідливих програм;

– незаконним контентом, що пропагує екстремізм, тероризм, наркотики, порнографію, насильство;

– рефайлінгом – незаконною підміною телефонного трафіку [36, с. 34-35].

Наукові дослідження свідчать, що основними об’єктами інформаційної безпеки можуть бути: держава та її національні інтереси в інформаційній сфері; підприємство чи організація; особа (її свідомість, психіка); інформація як така.

У трьох перших випадках об’єкт має активну природу, що передбачає потребу в захисті від негативних впливів, а також у зміцненні стійкості. У випадку з інформацією необхідний її захист та збереження.

Забезпечення інформаційної безпеки підприємств здійснюється двома групами суб’єктів:

– перша група – це працівники підприємства, що підпорядковуються його керівництву; серед них виокремлюють спеціалізовані служби (служби інформаційної або економічної безпеки) та неспеціалізовані підрозділи (наприклад, юридичний відділ), а також увесь персонал, який відповідно до посадових обов’язків має забезпечувати інформаційну безпеку;

– друга група – незалежні органи та організації, діяльність яких впливає на інформаційну безпеку підприємства, але які не є складовою його структури.

Ключова роль у захисті критичної інфраструктури належить телекомунікаціям. Міжнародний досвід численних інцидентів цілеспрямованого застосування інформаційно-комунікаційних технологій для виведення з ладу важливих об’єктів засвідчує новий рівень інформаційного протистояння у кіберпросторі. Багаторічна статистика активності шкідливих програм демонструє необхідність суттєвого вдосконалення підходів у сфері інформаційної безпеки.

Суб’єкт забезпечення інформаційної безпеки – це фізична чи юридична особа або інше утворення, що має правосуб’єктність і виступає учасником інформаційних відносин, наділене юридичними правами та обов’язками, діє відповідно до цілей і завдань забезпечення інформаційної безпеки та застосовує засоби й методи адміністративно-правового регулювання.

Система суб’єктів забезпечення інформаційної безпеки – це інтегрована, синергетична сукупність елементів, що перебувають у правовідносинах, обумовлених функціями інформаційної безпеки. Вона характеризується єдністю та багаторівневістю.

Перший рівень включає три групи суб’єктів: фізичних і юридичних осіб, публічно-правові утворення та їхні підсистеми. Наступні рівні формують спеціальні суб’єкти адміністративного права, диференціація яких зумовлена особливостями регулювання відповідних правовідносин.

Таким чином, система забезпечення інформаційної безпеки включає низку елементів, основним серед яких є в першу чергу принципи, що розглядаються як базові положення, основні ідейні орієнтири, правові механізми та правила адміністративного регулювання діяльності всіх суб’єктів в Україні, що закріплені в адміністративно-правових нормах і спрямовані на формування та реалізацію державної політики у сфері інформаційної безпеки. До ключових принципів забезпечення інформаційної безпеки належать:

– пріоритет прав, свобод та законних інтересів громадянина;

– верховенство права і рівність усіх суб’єктів правовідносин перед законом;

– відповідальність держави перед громадянином за власну діяльність;

– комплексний підхід до вирішення завдань інформаційної безпеки;

– єдність і взаємозалежність напрямів інформаційної безпеки;

– чітке розподілення повноважень та відповідальності між органами державної влади й місцевого самоврядування;

– участь у міжнародних та регіональних системах інформаційної безпеки;

– оперативність, своєчасність, превентивність і відповідність заходів загрозам, що виникають.

Методи адміністративно-правового регулювання відносин між владними та невладними суб'єктами у сфері інформаційної безпеки поширюються на всі сфери функціонування особи, суспільства й держави: економічну, соціально-культурну та адміністративно-політичну. Вони мають розглядатися в контексті методів державного управління, що має стати основою методології адміністративного права, спрямованого на побудову та функціонування державної системи інформаційної безпеки.

Адміністративне право включає широкий спектр правових засобів – приписи, заборони, дозволи.

Політичні засоби спрямовуються на забезпечення реального народовладдя, цивілізованої політичної конкуренції, врахування позицій громадян при формуванні державної політики.

Ідеологічні засоби забезпечують об'єднання народу навколо національної ідеї та формують правове підґрунтя державотворення.

Соціальні засоби відображають сутність регулювання відносин у сфері соціального управління.

Інформаційні, технологічні, кадрові, матеріально-технічні та фінансові засоби забезпечують реалізацію державної політики інформаційної безпеки в цілому.

Суб'єктами забезпечення інформаційної безпеки є фізичні та юридичні особи, а також інші утворення, які мають правосуб'єктність і діють у межах інформаційних правовідносин, використовуючи адміністративно-правові

методи захисту. Система таких суб'єктів є багаторівневою та узгодженою, складаючись із загальних учасників (осіб, організацій і публічно-правових структур) і спеціальних суб'єктів, діяльність яких визначається специфікою регулювання окремих сфер інформаційної безпеки.

Засади адміністративно-правового забезпечення інформаційної безпеки сприяють утвердженню прав і свобод людини; подоланню декларативності законодавства та безвідповідальності окремих посадовців; забезпеченню верховенства права; усуненню правової невизначеності та хаотичності діяльності суб'єктів; об'єднанню зусиль державних і недержавних інституцій у сфері інформаційної безпеки; забезпеченню дієвості адміністративної правоздатності та дієздатності суб'єктів; ефективному використанню міжнародних систем безпеки; оперативності й адекватності управлінських рішень; формуванню централізованої, ієрархічної системи державного управління інформаційною безпекою; координації діяльності всіх суб'єктів у відповідній сфері; удосконаленню законотворчого процесу з урахуванням міжнародного досвіду; подоланню недооцінки адміністративно-правових методів на користь економічних; збереженню правонаступництва держави незалежно від політичних змін.

Система забезпечення інформаційної безпеки ґрунтується на комплексі принципів, методів, засобів та суб'єктів, що охоплюють правові, політичні, організаційні та технологічні аспекти діяльності держави. Ефективність цієї системи залежить від узгодженості дій усіх суб'єктів влади, чіткого нормативного регулювання та здатності держави своєчасно реагувати на сучасні інформаційні загрози. Вирішальним чинником залишається пріоритет прав і свобод людини та конституційних цінностей, які визначають стратегічний напрям розвитку національної політики інформаційної безпеки.

2.2. Роль держави в системі захисту інформаційної безпеки

Інформаційна безпека традиційно трактується як складова або окрема підсистема національної безпеки держави. Українське законодавство приділяє цій сфері особливу увагу, підкреслюючи її значення в загальній архітектоніці безпекової політики. Так, відповідно до ч. 1 ст. 17 Конституції України, визначено: «Захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу» [7]. У цьому контексті інформаційна безпека поставлена в один ряд із ключовими елементами державності – територіальною цілісністю та суверенітетом, хоча за своїм змістом ці категорії не є тотожними чи однопорядковими.

Будь-який аспект національної безпеки, включно з інформаційною безпекою, базується на феномені державного суверенітету. Саме суверенітет, «політико-юридична властивість державної влади, що означає її верховенство та повноту всередині держави, а також незалежність і рівноправність у зовнішніх зносинах» [37], надає державним органам повноваження і право вживати заходів для забезпечення інформаційної безпеки. У Декларації про державний суверенітет України визначено, що державний суверенітет – це «верховенство, самостійність, повнота і неподільність влади Республіки в межах її території та незалежність і рівноправність у зовнішніх зносинах» [38]. Оскільки питання інформаційної безпеки тісно пов’язане з національною безпекою, її підґрунтям є не лише державний суверенітет, але й суверенітет народу та нації як суб’єктів інформаційних правовідносин.

Розгляд інформаційної безпеки неодмінно зумовлює появу питання щодо існування окремого різновиду суверенітету – інформаційного суверенітету. Закон України «Про інформацію» містить відповідну дефініцію, однак її зміст конкретно не розкрито. У ст. 53 цього Закону зазначено, що «основою інформаційного суверенітету України є національні інформаційні ресурси» [8],

однак сам термін не має законодавчого визначення. Під інформаційними ресурсами України розуміється вся інформація, яка їй належить, незалежно від форми, змісту, часу або місця створення. Держава самостійно формує такі ресурси та розпоряджається ними відповідно до законодавства та міжнародних договорів. Таким чином, у межах Закону «Про інформацію» інформаційний суверенітет фактично ототожнюється з правом держави володіти, формувати та управляти інформаційними ресурсами. Водночас така інтерпретація скоріше відображає реалізацію державою прав власника, а не змістовне наповнення категорії суверенітету.

Здійснення інформаційного суверенітету включає такі напрями: законодавче визначення стратегічних цілей розвитку й захисту національного інформаційного простору; встановлення регулятивних механізмів діяльності іноземних суб'єктів у національному інформаційному просторі; формування та забезпечення захисту інтересів України у глобальному інформаційному просторі; гарантування інформаційної безпеки держави [37].

Ст. 54 Закону «Про інформацію» визначає гарантії забезпечення інформаційного суверенітету, зокрема: виключне право власності держави на інформаційні ресурси, створені за рахунок державного бюджету; розбудову національних систем інформації; визначення режиму доступу іноземних держав до інформаційних ресурсів України; використання ресурсів на основі рівноправного міжнародного співробітництва [8].

У ч. 2 ст. 19 Міжнародного пакту про громадянські і політичні права, ратифікованого Україною, закріплено право людини на свободу вираження поглядів, що включає можливість шукати, отримувати та поширювати інформацію незалежно від кордонів і способу передачі [39]. У цьому акті підкреслюється універсальність принципу свободи інформації та заперечується можливість її обмеження державними межами.

Разом із тим, ч. 3 ст. 19 Пакту передбачає, що реалізація цього права може бути обмежена законом для захисту прав інших осіб, державної безпеки, громадського порядку, здоров'я чи моралі населення. Це означає, що

міжнародне право прямо визнає випадки законного втручання держави в інформаційну сферу. Подібний баланс інтересів закріплено і в Європейській конвенції про захист прав і основоположних свобод людини [40].

Ст. 10 Конвенції гарантує свободу отримання та поширення інформації, але одночасно надає державі право встановлювати обмеження, зокрема вимагати ліцензування телерадіомовлення та кінопідприємств. Також допускається встановлення законом формальностей, умов та покарань, необхідних у демократичному суспільстві для захисту національної безпеки, територіальної цілісності, громадського порядку, запобігання злочинам чи заворушенням, захисту репутації, моралі, охорони здоров'я, а також для запобігання розголошенню конфіденційної інформації або для забезпечення авторитету судової влади [40].

Таким чином, міжнародні стандарти вказують, що у демократичній державі втручання влади в інформаційні процеси має відбуватися виключно шляхом правового регулювання, а не через монополізацію інформаційних ресурсів чи встановлення єдиної інформаційної політики, що могло б порушувати свободу інформації.

Державний суверенітет є неподільним і охоплює всі сфери державного життя. Однак у контексті інформаційних процесів доцільніше вести мову не про «інформаційний суверенітет», а про інформаційну компетенцію держави – тобто комплекс її повноважень щодо регулювання інформаційних відносин. Сучасний етап розвитку суспільства висуває вимогу визнання інформаційної функції держави, у межах якої реалізуються й механізми забезпечення інформаційної безпеки.

Важливе значення має ч. 1 ст. 17 Конституції України, де захист інформаційної безпеки визначено однією з основних функцій держави. Проте повноваження держави в інформаційній сфері не обмежуються питаннями безпеки. Ч. 4 ст. 32 Конституції гарантує судовий захист інформаційних прав особи, а ч. 3 ст. 34 – право держави встановлювати законні обмеження інформаційних прав з метою захисту національної безпеки, територіальної

цілісності, громадського порядку, здоров’я, моралі, прав та репутації інших осіб, а також для запобігання розголошенню конфіденційної інформації та забезпечення належного функціонування правосуддя [7].

Згідно з ч. 2 ст. 3 Конституції України, саме права людини і їх гарантії визначають зміст діяльності держави, яка несе відповідальність перед людиною. Утвердження та забезпечення прав людини є головним обов'язком держави. Правові засади діяльності держави в інформаційній сфері деталізуються також у спеціальному законодавстві. Зокрема, Національна програма інформатизації визначає головною метою забезпечення громадян достовірною, повною та своєчасною інформацією з використанням сучасних технологій та гарантування інформаційної безпеки [41].

Особливості здійснення інформаційної функції держави визначаються специфікою інформаційних та комунікаційних процесів: їх відкритістю, масштабністю й здатністю до швидкого поширення. Водночас сфера державного втручання обмежується необхідністю забезпечення прав людини, що формує межі компетенції держави в інформаційній галузі. Аналіз системи міжнародних актів та національного законодавства – таких як Закони України «Про Основні засади розвитку інформаційного суспільства...», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про Національну програму інформатизації», «Про електронні документи та електронний документообіг», «Про електронний цифровий підпис», «Про телекомунікації», а також відповідних указів Президента та постанов Кабінету Міністрів – дає можливість окреслити конкретні випадки правомірного державного втручання та допустимі нормативні обмеження.

На підставі цих актів можна виділити три ключові напрями інформаційної компетенції держави:

1. регулювання інформаційних відносин з метою захисту національної безпеки, територіальної цілісності, громадського порядку та законності;

2. забезпечення прав і свобод громадян, охорони здоров’я та моралі;

3. регулювання комерційної інформації з метою захисту економічних інтересів держави та національного інформаційного ринку.

Вказані аспекти визначають складність і багатовимірність державної політики у сфері інформації. Оскільки інформаційні процеси пронизують усі сфери суспільного життя – економіку, політику, науку, культуру, оборону – то мова частіше йде не про єдину інформаційну політику, а про інформаційний компонент окремих напрямів державної діяльності: безпекової, правозахисної, економічної тощо.

Невід'ємним елементом реалізації державної політики у сфері інформаційних відносин є інформаційна інфраструктура. Вона становить основу як стратегічних ресурсів, що формують обороноздатність держави, так і інформаційного ринку, який значною мірою визначає економічний потенціал та перспективи розвитку країни.

У Законі України «Про Національну програму інформатизації» визначено основні нормативні засади функціонування інформаційної сфери. Зокрема, в документі подано такі ключові поняття:

• **Адміністрування засобу інформатизації** – це вид управлінської діяльності, який здійснює власник або технічний адміністратор під час експлуатації інформаційного засобу. Його мета – забезпечити керованість такого засобу та/або його доступність для користувачів інформаційно-комунікаційних систем.

• **Електронна демократія** – форма суспільних відносин, за якої громадяни й організації залучаються до державотворчих процесів, державного управління та місцевого самоврядування через широке використання інформаційно-комунікаційних технологій. Це сприяє більш активній участі громадян у публічному житті, підвищує прозорість ухвалення рішень, забезпечує підзвітність державних інституцій та покращує комунікацію влади з громадянами.

• **Електронне урядування** – форма організації державного управління, орієнтована на підвищення його ефективності, прозорості та відкритості. Вона передбачає застосування ІКТ для створення нової моделі держави, спрямованої на задоволення потреб громадян [42].

Положення статті 2 цього Закону також підкреслюють інформаційну функцію держави. **Національна програма інформатизації** визначається як комплекс завдань, програм, проєктів і робіт, спрямованих на розвиток інформаційного суспільства шляхом раціонального використання ресурсів та координації діяльності державних органів, органів місцевого самоврядування та суб'єктів різних форм власності.

• Програма має на меті забезпечити: розробку, впровадження та використання інформаційно-комунікаційних технологій у державному управлінні, місцевому самоврядуванні та суспільному житті; реалізацію заходів, спрямованих на розвиток електронного урядування й електронної демократії; створення та розвиток системи державних інформаційних ресурсів; рівний доступ громадян до інформаційно-комунікаційних технологій та підвищення їх цифрової грамотності; удосконалення процедури надання публічних (зокрема електронних) послуг; організацію інформаційної взаємодії органів державної влади й місцевого самоврядування через електронний документообіг та інші цифрові інструменти [42].

Отже, інформаційна безпека є невід'ємною частиною національної безпеки, що закріплено на конституційному рівні та підтверджено аналізом міжнародних актів. Суверенітет держави формує базу для реалізації повноважень у сфері інформаційної безпеки, однак поняття «інформаційний суверенітет» радше відображає управління державою інформаційними ресурсами, ніж окремий різновид суверенітету.

Держава має право втручатися в інформаційні процеси лише в межах, визначених міжнародним та національним правом, і такі втручання мають бути

необхідними та пропорційними. Інформаційна політика держави є комплексною та багатовимірною, оскільки інформаційні процеси пронизують усі сфери суспільного життя.

Інформаційна компетенція держави охоплює три основні сфери: національна безпека та порядок, права людини і суспільна мораль, комерційна інформація й економічні інтереси. Інформаційна інфраструктура виступає ключовою умовою реалізації державної інформаційної політики, забезпечуючи як безпекові, так і економічні потреби держави.

2.3. Забезпечення інформаційної безпеки в різних секторах суспільства

Одним із стратегічних завдань сучасної України є розвиток безпечного інформаційного суспільства, орієнтованого на потреби людини, де пріоритетами виступають створення, нагромадження, поширення та вільний обмін інформацією і знаннями. Динамічне зростання значення інформаційної сфери відображає загальний рівень суспільного прогресу. Водночас залежність національної безпеки від ефективності забезпечення інформаційної безпеки посилюється пропорційно розвитку інформаційних технологій, інформаційних систем та державноправових механізмів їх регулювання.

Державно-правовий механізм забезпечення інформаційної безпеки можна визначити як системно організований комплекс державних інституцій, покликаних формувати та реалізовувати політику у сфері інформаційної безпеки, взаємодія яких регламентується нормами та принципами права. Такий механізм охоплює три взаємозалежні структурні ланки. Перша – інституціональний компонент, що включає державні органи, залучені до формування та реалізації інформаційно-безпекової політики. Друга – система ролей і правовідносин, що виникають у процесі здійснення цієї політики, а також форми й методи діяльності її суб’єктів. Третя – правовий механізм, який

становить ієрархічно впорядковану сукупність правових норм і принципів, що визначають зміст, напрям і процедури реалізації політики інформаційної безпеки. Ефективність функціонування всієї системи залежить від належної роботи кожної з її складових.

На наше переконання у структурі механізму інформаційної безпеки простежується класична для адміністративного права тріада: суб'єкти, правовідносини та норми права. Такий підхід відповідає системній теорії державного управління та дозволяє проводити комплексний аналіз інформаційної політики не лише як нормативної, а як управлінсько-комунікативної діяльності держави.

В умовах інтеграції України до міжнародної кіберцивілізації інформаційна безпека набуває особливої значущості, оскільки ефективність функціонування інформаційного суспільства зумовлюється рівнем науково-технічного розвитку та використанням комп'ютерних технологій у глобальних телекомунікаційних мережах [43]. У зв'язку зі становленням глобального інформаційного суспільства та включенням України до світового інформаційного простору посилюється необхідність удосконалення правового механізму забезпечення інформаційної безпеки. Однією з найважливіших особливостей інформаційного суспільства є здатність кожної людини не лише створювати інформацію та знання, а й вільно отримувати до них доступ, активно використовувати й поширювати їх. Головна мета такого суспільства полягає у створенні умов, за яких людина може повною мірою розкрити свій інтелектуальний потенціал, розвивати здібності та покращувати якість власного життя [44, с. 55]

Герменевтичний аналіз Стратегії інформаційної безпеки [24] дозволяє зробити короткі узагальнення ключових напрямів інформаційної безпеки в різних сферах суспільства, а саме:

Протидія дезінформації та інформаційним операціям. Україна повинна запобігати та швидко реагувати на дезінформацію, пропаганду та гібридні впливи, особливо з боку держави-агресора. Це передбачає створення системи

раннього виявлення інформаційних загроз, посилення відповідальності за поширення неправдивих даних, захист інформаційного простору в Інтернеті, координацію між державними органами й громадянським суспільством, протидію вербуванню громадян до незаконних формувань та заборону інформаційного продукту, який популяризує державу-агресора чи закликає до насильства. В цьому контексті Д. Смотрич акцентує увагу на проблемі безпеки соціальної мережі, за допомогою якої військовослужбовці можуть ненавмисно розкрити важливі відомості. Тому одним із ключових завдань державної безпеки є своєчасне виявлення подібних ризиків і їх ефективна нейтралізація.

Заходи, спрямовані на захист інформації та забезпечення безпеки, умовно поділяються на дві основні категорії: забезпечення захисту інформаційних систем від пошкодження, а інформації від витоку та несанкціонованого перехоплення; охорона психічного стану особового складу від цілеспрямованого інформаційно-психологічного впливу.

Реалізація цих заходів має здійснюватися комплексно, із залученням сучасних наукових досягнень та новітніх програмних рішень.

До першої групи належать такі заходи: захист військових об’єктів і розміщеної на них комп’ютерної техніки від ураження вогнем або навмисного виведення з ладу; протидія віддаленим кібератакам, зокрема шляхом упровадження програмних засобів повного периметрового захисту, таких як DLP- та SIEM-системи; недопущення витоку або умисного викрадення інформації, що становить державну чи військову таємницю; забезпечення радіоелектронного захисту; використання захищених комп’ютерних платформ і програмного забезпечення, стійких до прихованих уразливостей у коді; розроблення та застосування засобів електронної розвідки; свідоме використання соціальних мереж з метою дезінформації противника; захист і стабільність систем зв’язку.

До другої групи заходів відносяться: запобігання цілеспрямованому психологічному тиску на військовослужбовців; коригування та нейтралізація інформаційних повідомлень, що поширюються потенційним противником [45, с. 125].

Розвиток української культури та зміцнення громадянської ідентичності. Культура є основою суспільної єдності. Завдання включають підтримку української мови, кіно, телерадіовиробництва й книговидання; розвиток мов національних меншин; зміцнення зв'язків з українською діаспорою; підвищення довіри до державних інститутів; залучення ветеранів до формування державницьких цінностей.

Підвищення медіакультури та медіаграмотності. Українське суспільство має бути здатним протистояти маніпуляціям та дезінформації. Це забезпечується через просвітницькі програми з медіаграмотності, підтримку діяльності й професійного розвитку медіафахівців, удосконалення рекламного законодавства та розвиток соціально відповідального медіабізнесу. **Захист прав людини у сфері інформації.** Необхідно гарантувати доступ до достовірної інформації, захист приватності й свободу вираження поглядів. Основні завдання включають вдосконалення законодавства щодо доступу до інформації та персональних даних, захист журналістів, моніторинг дотримання прав на окупованих територіях, боротьбу з незаконним контентом та забезпечення інформаційної безпеки військовослужбовців.

Інформаційна реінтеграція громадян з тимчасово окупованих територій. Україна має відновити інформаційний зв'язок із громадянами на окупованих територіях. Це передбачає поширення українського інформаційного продукту, розширення мовлення, спростування російських пропагандистських наративів, інформування про політику України та дії окупаційної влади, а також зміцнення відчуття спільності й підтримки територіальної цілісності.

Розвиток стратегічних комунікацій. Потрібно забезпечити ефективний діалог між державою та суспільством у кризових ситуаціях, формувати позитивний імідж України за кордоном, інформувати міжнародну спільноту про події в Україні та поширювати український інформаційний продукт за межами держави. Важливим є також впровадження бренду Ukraine Now та створення системи іномовлення.

Розвиток інформаційного суспільства та культури діалогу. Ціль передбачає підтримку відкритих суспільних дискусій, розвиток телерадіомереж, належне фінансування суспільного мовника, розширення доступу до українського контенту в регіонах, зміцнення інформаційної інфраструктури та підтримку аналітичних і наукових досліджень в інформаційній сфері.

Важливим кроком у формуванні правових засад інформаційної безпеки у сфері реклами стало ухвалення Закону України «Про рекламу». Цей нормативний акт об’єднав положення кількох галузей права – адміністративного, цивільного, державного – що зумовлено багатовимірністю рекламної діяльності та необхідністю її комплексного правового регулювання. Закон закріплює ключові принципи рекламної діяльності, визначає вимоги до створення, поширення та споживання реклами [46].

Сучасні тенденції свідчать про тісний взаємозв’язок рекламної сфери з використанням об’єктів авторського права та суміжних прав. Учасниками правовідносин у сфері реклами дедалі частіше виступають автори оригінальних творів, які використовуються у рекламних матеріалах. Закон «Про рекламу», визначаючи статус виробника реклами, не ототожнює його з автором, а питання, пов’язані з використанням об’єктів авторського права, відносить до компетенції закону про авторське право та суміжні права [47, с. 87].

У цьому контексті спостерігається колізійність правового регулювання між рекламним та авторським законодавством, що потребує узгодження. Відсутність чіткої дефініції «авторства» в рекламному процесі ускладнює

реалізацію авторських прав і створює прогалини у сфері юридичної відповідальності.

Суспільний вимір інформаційної безпеки у сфері реклами є найбільш чутливим до інформаційних впливів, оскільки охоплює механізми формування громадської думки, діяльність мас-медіа, комунікаційні структури політичних і громадських інституцій, а також умови реалізації конституційних прав на свободу вираження поглядів і доступ до інформації. У правовій площині безпека інформаційних відносин у рекламній сфері означає створення нормативної основи, яка забезпечує функціонування рекламної діяльності та захист прав її суб'єктів [48].

П. Остапишин слушно зазначає, що інформаційна безпека у сфері реклами є складовою частиною як системи національної безпеки, так і інформаційного суспільства, причому обидві системи не можуть бути повноцінними без цього елемента [49, с. 370]. Забезпечення інформаційної безпеки у сфері реклами базується на принципах верховенства права, пріоритету прав людини, своєчасного реагування на загрози, чіткого розподілу повноважень між органами влади та використання міжнародних механізмів колективної інформаційної безпеки.

Об'єктами безпеки інформаційних відносин у рекламній сфері є рекламна інформація та рекламна діяльність, які повинні здійснюватися з повагою до прав людини, морально-культурних цінностей суспільства та конституційних засад державності. Реалізація інформаційно-безпекової політики у рекламі забезпечується діяльністю низки державних інституцій: Президента України, Верховної Ради, РНБО, СБУ, Міністерства інформаційної політики, а також органів виконавчої влади та місцевого самоврядування. Вказаний спектр суб'єктів демонструє поліцентричність державної системи інформаційної безпеки, однак також виявляє проблему дублювання повноважень та недостатньої координації між органами.

Освіта, наука та виховання як ціннісні чинники адміністративно-правового забезпечення інформаційної безпеки.

Невід'ємною умовою успішного розвитку національної інформаційної сфери є інтелектуальний потенціал суспільства, що формується через систему освіти, науки та виховання. Високий рівень інформаційно-правової культури та професійної підготовки спеціалістів у сфері інформаційної безпеки є визначальними елементами загальнонаціональної системи гарантій інформаційної безпеки. В умовах реформування вищої освіти особливої важливості набуває створення цілісної системи підготовки та перепідготовки кадрів у цій сфері.

А. Марущак наголошує на необхідності застосування традиційних методологічних підходів юридичної науки до дослідження питань інформаційної безпеки, серед яких: обґрунтування правового регулювання інформаційних відносин; визначення базових понять категоріального апарату; аналіз повноважень суб'єктів інформаційно-безпекових відносин; дослідження юридичної відповідальності за порушення у цій сфері [50, с. 37].

Інформаційно-просвітницька діяльність є важливим інструментом реалізації державної влади, спрямованим на підвищення рівня інформаційної культури суспільства та формування об'єктивного розуміння інформаційно-безпекових процесів. Її складовою є громадянська освіта, метою якої є формування відповідальної громадянської позиції та здатності осіб протидіяти маніпулятивним медіавпливам.

Національна модель громадянської освіти у контексті вивчення медіа включає такі елементи: розуміння ролі інформації в суспільстві; ознайомлення з діяльністю засобів масової інформації; аналіз функцій ЗМІ; усвідомлення їх впливу на політичне життя; формування навичок взаємодії громадян та медіа у процесі розвитку громадянського суспільства [51, с. 89]. У цьому контексті простежується інтеграція підходів медіаграмотності, громадянської освіти та правової культури, що відповідає європейським тенденціям розвитку інформаційної стійкості населення.

На сьогодні наша держава робить акцент на такі механізми реалізації інформаційної безпеки [24]:

Координаційна роль РНБО України. Рада національної безпеки і оборони координує діяльність органів виконавчої влади у сфері інформаційної безпеки, використовуючи, зокрема, можливості Центру протидії дезінформації. Роль РНБО ґрунтується на ст. 107 Конституції України, яка визначає її основним координаційним органом у сфері національної безпеки. У цьому контексті інформаційна безпека розглядається як складова національної безпеки, що відповідає положенням Закону «Про національну безпеку України». Створення Центру протидії дезінформації є проявом адаптації державної системи до нових типів гібридних загроз.

Повноваження Кабінету Міністрів України. Формує та реалізує державну інформаційну політику, забезпечує інформаційний суверенітет, спрямовує діяльність міністерств і фінансує програми у сфері інформаційної безпеки. Уряд затверджує план заходів із реалізації Стратегії, який є обов’язковим для органів виконавчої влади. Кабінет Міністрів України виступає центральним суб’єктом у реалізації державної інформаційної політики відповідно до ст. 116 Конституції України. Наявність плану заходів забезпечує ієрархічну узгодженість рішень і дозволяє інтегрувати інформаційну політику у загальний механізм управління безпекою держави.

Взаємодія з місцевим самоврядуванням і громадянським суспільством. Органи державної влади спільно з місцевими радами, Центром протидії дезінформації та інститутами громадянського суспільства виконують Стратегію відповідно до урядового плану. Таке положення відображає сучасну доктрину "багаторівневого врядування", відповідно до якої ефективна інформаційна безпека неможлива без участі локальних громад та неурядових структур.

Центральний орган виконавчої влади у сфері інформації. Цей орган: здійснює нормотворчу діяльність у сфері інформаційної безпеки, визначає

пріоритети розвитку інформаційної сфери, разом із Міністерством Закордонних Справа України формує позитивний міжнародний імідж України.

Нормативна діяльність цього органу забезпечує практичну реалізацію принципу правової визначеності у сфері інформації. Співпраця з Міністерством Закордонних Справа свідчить про розуміння інформаційної політики як інструмента «м'якої сили».

Функції Міністерства оборони та сил оборони. Сили оборони здійснюють: моніторинг та прогнозування інформаційних загроз, проведення інформаційних операцій, розвиток системи стратегічних комунікацій, забезпечення інформаційної безпеки військових структур, взаємодію з медіа, протидію інформаційним атакам, спрямованим проти сектору оборони.

Ці функції узгоджуються з концепцією «інформаційної оборони», що у світовій науці розглядається як ключова складова сучасних воєнних доктрин, зокрема NATO StratCom.

Участь наукових установ. До виконання Стратегії можуть залучатися науково-дослідні інститути, які забезпечують експертний супровід та аналітичну підтримку. Залучення науки відповідає принципу evidence-based policy (політика, заснована на доказах), що є ознакою зрілої державної інформаційної політики.

Нормативно-правове забезпечення. Стратегія інформаційної безпеки реалізується шляхом системного перегляду та оновлення законодавства у сфері інформаційної безпеки. Цей механізм забезпечує адаптацію правової системи до динамічних змін у кіберсередовищі та відповідає доктрині «правової еволюції» (law adaptation to technological change), що є ключовою для сучасного інформаційного права.

Отже, забезпечення інформаційної безпеки України у сфері реклами, а також у ширшому контексті функціонування інформаційного суспільства, є

багатоаспектним завданням, яке передбачає узгоджену роботу державних інституцій, розвинену нормативно-правову базу та високий рівень інформаційної культури громадян. Ефективність державноправового механізму інформаційної безпеки залежить від цілісності інституційної структури, чіткості правового регулювання та здатності держави реагувати на сучасні інформаційні загрози. Ключову роль відіграють освіта, наука й виховання, які формують інтелектуальний фундамент національної інформаційної політики та сприяють підвищенню стійкості суспільства до деструктивних інформаційних впливів.

Висновки до розділу 2.

Отже, досліджуючи питання, пов’язані з з’ясуванням та характеристикою елементів системи забезпечення інформаційної безпеки, роллю держави в системі захисту інформаційної безпеки, особливостями забезпечення інформаційної безпеки в різних секторах суспільства, ми дійшли наступних висновків:

держава виступає ключовим суб’єктом формування й реалізації інформаційної політики, водночас її втручання в інформаційні процеси має здійснюватися виключно в межах принципів законності, доцільності, пропорційності, верховенства права тощо. **Адміністративно-правове забезпечення інформаційної безпеки ґрунтується на комплексному використанні методів і засобів державного управління**, зокрема владно-розпорядчих, координаційних, інформаційних, економічних, політичних та

ідеологічних. **Адміністративно-правові методи забезпечення інформаційної безпеки поєднують превентивний і оперативний характер,** що передбачає не лише реагування на вже наявні загрози, а й прогнозування, планування та запобігання негативним інформаційним впливам. Їх поєднання дозволяє забезпечити ефективне реагування на сучасні інформаційні загрози. **Система суб'єктів забезпечення інформаційної безпеки має багаторівневий і узгоджений характер** та включає як загальних суб'єктів (органи державної влади, юридичних і фізичних осіб), так і спеціалізовані органи, діяльність яких визначається особливостями окремих секторів інформаційної безпеки;

інформаційна безпека обґрунтовано розглядається як невід'ємна складова національної безпеки держави, що має конституційне закріплення та визначальне значення в системі публічної влади України. Аналіз норм Конституції України, спеціального інформаційного законодавства та міжнародно-правових актів засвідчує, що забезпечення інформаційної безпеки ґрунтується на феномені державного суверенітету, однак не зводиться до нього механічно й потребує чіткого дотримання балансу між інтересами держави та правами людини. Поняття «інформаційний суверенітет», попри його використання в науковому дискурсі, не набуло самостійного, концептуально завершеного змісту та радше відображає сукупність повноважень держави щодо формування, володіння та управління національними інформаційними ресурсами. У цьому контексті більш обґрунтованим є підхід, відповідно до якого йдеться про інформаційну компетенцію держави як комплекс правомірних владних повноважень у сфері регулювання інформаційних відносин. Таке регулювання допускається виключно на підставі закону, з легітимною метою та за умови дотримання принципів правової держави. Це унеможливлює монополізацію інформаційного простору державою та зумовлює правовий, а не адміністративно-директивний характер інформаційної політики. Інформаційна компетенція держави охоплює, по-перше, захист національної безпеки та публічного порядку, по-друге, гарантування прав і

свобод людини та охорону суспільної моралі, по-третє, регулювання комерційної інформації з метою захисту економічних інтересів і національного інформаційного ринку. Особливу роль у реалізації зазначеної компетенції відіграє розвиток інформаційної інфраструктури та інститутів електронного урядування й електронної демократії, які одночасно слугують інструментами підвищення ефективності державного управління й важливою умовою забезпечення інформаційної безпеки. У підсумку, інформаційна безпека постає як системне правове явище, ефективність якого визначається не обсягом державного втручання, а його правовою визначеністю, інституційною узгодженістю та орієнтацією на пріоритет прав і свобод людини;

забезпечення інформаційної безпеки в різних секторах суспільства в Україні постає як комплексне, багатоаспектне та міждисциплінарне завдання, тісно пов’язане з процесами становлення інформаційного суспільства, національної безпеки та євроінтеграційного розвитку держави. Проведений аналіз свідчить, що ефективність інформаційної безпеки зумовлюється функціонуванням цілісного державно-правового механізму, який включає інституційний компонент, систему правовідносин та нормативно-правову основу, об’єднані спільною метою захисту національного інформаційного простору. Інформаційна безпека охоплює ключові сфери суспільного життя – оборону, культуру, освіту, науку, рекламу, медіасередовище, права людини та стратегічні комунікації. Особливе значення в сучасних умовах мають заходи протидії дезінформації, інформаційно-психологічним операціям і гібридним загрозам, а також забезпечення інформаційного суверенітету держави в умовах збройної агресії та глобалізації інформаційних процесів. Важливу роль у системі інформаційної безпеки відіграє сфера реклами, яка безпосередньо впливає на формування громадської думки та потребує чіткого нормативного врегулювання з урахуванням балансу між свободою вираження поглядів, захистом прав людини й інтересами національної безпеки. Не менш значущими є освіта, наука та інформаційно-просвітницька діяльність, які формують

інформаційну культуру, медіаграмотність і правову свідомість громадян, підвищуючи стійкість суспільства до деструктивних інформаційних впливів. Реалізація Стратегії інформаційної безпеки України засвідчує прагнення держави до системної, науково обґрунтованої та скоординованої політики у цій сфері за участю органів державної влади, місцевого самоврядування, громадянського суспільства й наукових установ. У підсумку, інформаційна безпека в різних секторах суспільства має розглядатися як невід'ємна складова національної безпеки та сталого розвитку України, ефективність якої залежить від узгодженості інституційних дій, адаптивності правового регулювання та рівня інформаційної зрілості суспільства.

РОЗДІЛ 3. ПУБЛІЧНЕ УПРАВЛІННЯ ТА АДМІНІСТРУВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: СВІТОВИЙ ДОСВІД ТА НАПРЯМИ ПОДАЛЬШОГО РОЗВИТКУ

3.1. Підходи до публічного управління та адміністрування у сфері інформаційної безпеки в Сполучених Штатах Америки та Європейського Союзу

Початок системного правового врегулювання питань інформаційної безпеки припав на кінець XX століття, коли стрімке поширення сучасних інформаційних технологій і наслідки інформаційної революції – економічні, політичні та військові – поставили перед державами принципово нові виклики **(трансформація кіберсередовища, включно з розбудовою Інтернету та комп'ютерних мереж)**https://www.nvppp.in.ua/vip/2025/3/37.pdf?utm_source=chatgpt.com**.** Першими державами, які почали формувати комплексні підходи до інформаційної політики та захисту інформаційної безпеки, стали Сполучені Штати Америки та Японія, а пізніше до цього процесу долучилася більшість високорозвинених країн, які почали розбудовувати власні системи управління інформаційними процесами та захисту інформаційних ресурсів [52].

У США, історично домінує технологічна складова інформаційної політики, зорієнтована на прискорення інновацій, водночас забезпечуючи національну безпеку через нормативно-правове регулювання та державні стандарти. У державах Європейського Союзу акцент робиться на соціальних вимірах інформаційної безпеки, зокрема на захисті прав людини та приватності через комплексне законодавство та директиви, що встановлюють уніфіковані стандарти та підходи для всіх членів ЄС [53].

У США правове регулювання інформаційної безпеки почалося ще на початку XX століття: перший закон про захист інформації був ухвалений у 1906 р., що відображає довгу традицію законодавчого реагування на питання захисту даних і доступу до інформації [52]. Одним із ключових нормативних актів став **Закон про свободу інформації 1966 р.** який закріпив принцип відкритості інформації уряду та зобов'язав відомства оприлюднювати офіційні документи та рішення, що є важливою складовою демократичних і прозорих державних систем. Нормативи щодо приватності та захисту персональних даних були закріплені в ряді актів, включно з положеннями, що стали підґрунтям для подальшого розвитку законодавства про кібербезпеку [54].

У 1986 р. США ухвалили **Закон про конфіденційність електронних комунікацій,** який розширив правові обмеження урядового доступу до електронних комунікацій, захищаючи приватність цифрових даних [**54**]. У тому ж році був ухвалений **Закон про комп'ютерне шахрайство та зловживання**, який встановив кримінальну відповідальність за комп'ютерні злочини, включаючи несанкціонований доступ до систем та даних [*55*]. У 1987–1988 рр. **Закон про комп'ютерну безпеку** визначив роль Національного інституту стандартів і технологій (NIST) у розробці стандартів захисту інформаційних систем як державних, так і приватних [*56*].

Пізніше **Закон про обмін та захист кіберрозвідувальних даних** запропонував механізми обміну інформацією про кіберзагрози між державними органами та приватним сектором, що мало посилити спроможності реагування на складні загрози **(хоча законодавство не було остаточно прийняте Сенатом) [57]**. Сучасна інформаційна політика США поєднує у собі як вимоги національної безпеки, так і захист основних прав людини, включно з гарантіями свободи слова та приватності, передбаченими Першою поправкою до Конституції США. До ключових пріоритетів національної інформаційної політики Сполучених Штатів Америки належать: підтримка наукових досліджень і розробок у сфері інформаційних та комунікаційних технологій,

визначення стратегічних напрямів їх розвитку, а також стимулювання поширення технічних знань і можливостей в економічному середовищі. Важливе місце відводиться сприянню технологічному обміну між науково-дослідними установами та бізнес-структурами, активному впровадженню інновацій на ринках.

Окремим напрямом є створення й модернізація інформаційної інфраструктури, здійснення контролю за її функціонуванням, розбудова глобальних комунікаційних систем та аналіз їх впливу на міжнародні, національні й приватні пріоритети. Значна увага приділяється відновленню балансу, порушеного розвитком новітніх технологій, між основними інформаційними цінностями, а саме: захистом конфіденційної інформації, сприйняттям інформації як суспільного блага, як економічного ресурсу та як невід'ємного елементу існування держави. Це передбачає формування нових механізмів контролю та регулювання сучасних інформаційних відносин.

Водночас пріоритетами залишаються забезпечення недоторканності приватного життя, захист персональної та конфіденційної інформації на різних рівнях і в різних сферах державного управління та приватного сектору, а також розроблення й реалізація цілісної урядової політики у сфері інформації та комунікацій [58, с. 25].

Дослідження та глибокий аналіз досвіду Європейського Союзу й провідних західноєвропейських держав є вагомим чинником у процесі становлення та забезпечення стабільного функціонування системи інформаційної безпеки України. Водночас доцільно зважати на рівень соціально-економічного розвитку цих країн, тривалість формування ними сучасних систем інформаційної безпеки, їх концептуальний зміст, а також специфіку національних підходів до розв'язання проблем у цій надзвичайно важливій сфері.

У Європейському Союзі правове регулювання інформаційної безпеки ґрунтується на принципі високого рівня захисту прав і свобод особи, який реалізується через директиви та регламенти, що встановлюють обов'язкові стандарти для країн-членів. Однією з ключових є **NIS Directive** (2016), яка була першою спільно європейською законодавчою ініціативою у сфері безпеки мереж та інформаційних систем [59].

У резолюції Генеральної Асамблеї ООН «Досягнення у сфері інформатизації і телекомунікацій у контексті міжнародної безпеки» (1999 р.) питання забезпечення інформаційної безпеки було визначено як одна з глобальних проблем сучасного світу. Представники держав наголошували, що активне застосування новітніх інформаційних технологій і засобів впливу з боку високорозвинених країн щодо менш технологічно розвинених призвело до трансформації глобального та регіонального балансів сил. Це, своєю чергою, спричинило появу нових сфер протистояння між традиційними й новими центрами світової сили, створило умови для здобуття переваг у сфері інформаційних технологій і маніпулювання суспільною свідомістю, а також відкрило можливості для масштабної експансії із застосуванням видів озброєнь, не врегульованих міжнародним правом [60].

З огляду на універсальний характер і надзвичайну актуальність проблеми інформаційної безпеки в епоху інформаційного суспільства, держави – члени ООН дійшли згоди щодо уніфікації термінології та визначення змісту ключових понять у сфері міжнародного інформаційного співробітництва. Зокрема, «міжнародна інформаційна безпека» трактується як взаємодія суб'єктів міжнародних відносин у межах операцій із підтримання сталого миру, що базується на захисті міжнародної інфосфери, глобальної інформаційної інфраструктури та суспільної свідомості світової спільноти від наявних і потенційних інформаційних загроз. Під «інфосферою» розуміється міжнародний інформаційний простір, який охоплює інформаційні потоки, ресурси та всі сфери життєдіяльності цивілізації [60; 61].

Складові міжнародної інформаційної безпеки, визначені ООН і закріплені у відповідній резолюції, спрямовані насамперед на досягнення головної мети – підтримання сталого миру. У сучасних умовах мирне співіснування та розвиток людства забезпечуються комплексом політичних, дипломатичних, економічних, військових і інформаційних заходів. При цьому кожен із зазначених напрямів містить інформаційний компонент, що свідчить про комплексний характер поняття міжнародної інформаційної безпеки.

Ключовим елементом є захист міжнародної інфосфери, яка включає глобальний інформаційний простір, його потоки й ресурси всіх сфер діяльності цивілізації, зокрема й інформаційні ресурси, пов’язані з діяльністю світової спільноти щодо забезпечення сталого миру. Окреме виділення захисту глобальної інфраструктури, що забезпечує функціонування цього простору, підкреслює важливість даного напряму у системі міжнародної інформаційної безпеки.

Отже, поняття «міжнародна інформаційна безпека» охоплює:

– захист інфосфери та глобальної інфраструктури, що передбачає правове регулювання діяльності суб’єктів міжнародних відносин і реалізацію узгоджених правових, організаційних та інженерно-технічних заходів;

– захист суспільної свідомості світової спільноти шляхом застосування інформаційно-ідеологічних та інформаційно-психологічних засобів, оскільки суспільна свідомість формується системою ідей, цінностей і уявлень, що проявляються в політиці, моралі, культурі, мистецтві та релігії. Це актуалізує питання вироблення спільних, підтриманих міжнародною спільнотою норм, принципів і правил поведінки суб’єктів глобальної інформаційної інфраструктури, а також формування відповідних світоглядних орієнтирів на національному рівні.

16 січня 2023 року набула чинності Директива (ЄС) 2022/2555, яка замінила Директиву (ЄС) 2016/1148. ENISA вважає, що NIS2 покращує існуючий стан кібербезпеки в ЄС шляхом: створення необхідної структури управління кіберкризами; підвищення рівня гармонізації щодо вимог безпеки та зобов'язань щодо звітності; заохочення держав-членів запроваджувати нові сфери інтересів, такі як ланцюги поставок, управління вразливостями, базовий Інтернет та кібергігієна; впровадження нових ідей, таких як експертні оцінки, для покращення співпраці та обміну знаннями між державами-членами; охоплення більшої частки економіки та суспільства шляхом включення більшої кількості секторів, що означає, що більше суб'єктів господарювання зобов'язані вживати заходів для підвищення рівня кібербезпеки [59].

Утворене **Європейське агентство з мережевої та інформаційної безпеки (ENISA)** підтримує реалізацію політик та законодавства ЄС у сфері кібербезпеки та сприяє технічній координації між державами [63].

Ці заходи доповнюються новими законодавчими ініціативами, такими як **Cyber Resilience Act,** що встановлює вимоги щодо безпеки продуктів із цифровими елементами в ЄС **(станом на 2024 р.) [**64].

Важливим напрямом є розвиток електронного урядування та е-демократії. Європейська політика інформатизації від початку була спрямована на забезпечення практичної користі для громадян – доступність послуг, прозорість влади, цифровізацію рутинних процедур.

З 2000 р. в ЄС реалізовуються програми eEurope, спрямовані на створення інформаційного суспільства для всіх. Плани дій «e-Europe 2002», «e-Europe 2005», «e-Government і-2010» та «Цифровий порядок денний для Європи» сформували підвалини сучасних цифрових державних сервісів, відкритих даних та електронної взаємодії.

У ЄС існує диференціація між інформаційною безпекою особи, суспільства, держави та міжнародною інформаційною безпекою. У такому сенсі на 56-й сесії Генеральної Асамблеї ООН було розширено зміст поняття інформаційної безпеки: наголошувалося на необхідності захисту персональних

даних, недопущенні несанкціонованих змін інформації та забезпеченні надійності постачання технологій і послуг. Особливо підкреслювалося, що недостатній рівень захисту критичних інформаційних ресурсів створює ризики міжнародній безпеці. Домінантною стала орієнтація на інтереси людини, що зумовило активний розвиток правового регулювання у сферах: захисту персональних даних, доступу до інформації, електронної демократії, протидії кіберзлочинності.

Європейський підхід характеризується високим рівнем правового регулювання та соціальної відповідальності держав у сфері інформаційних відносин, а також пріоритетом прав людини над інтересами держави.

Аналіз американської та європейської моделей інформаційної безпеки демонструє суттєві концептуальні відмінності між ними. США історично орієнтовані на технічну перевагу, ринкові механізми та розширення повноважень держави в питаннях національної безпеки, особливо після 2001 р. Європейський Союз, навпаки, поставив у центрі уваги права людини, захист персональних даних і розвиток соціально орієнтованої цифрової інфраструктури.

Обидві моделі є успішними, але їхня ефективність зумовлена різними ціннісними пріоритетами: у США – безпекою та технологічним домінуванням, у ЄС – людською гідністю, соціальною стабільністю та демократичним контролем. Порівняння цих систем дозволяє сформувати комплексне бачення інформаційної безпеки як багатовимірного явища, у якому технічна, правова та соціальна складові повинні доповнювати одна одну.

3.2. Пріоритетні напрями розвитку адміністрування інформаційної безпеки України

Ефективне гарантування інформаційної безпеки на рівні індивіда, суспільства та держави потребує формування кожною країною власної концептуальної та ідеологічної основи. На цій базі вибудовується узгоджене бачення діяльності суб'єктів, відповідальних за захист інформаційного простору, визначається нормативно-правовий масив, що окреслює їхні повноваження та відповідальність, а також формується цілісна державна політика адміністративно-правового забезпечення інформаційної безпеки України.

Поточний стан глобального інформаційного середовища зумовлюється низкою чинників, серед яких: масштабна поширеність кібертероризму, кіберзлочинності та інших викликів інформаційній безпеці; зростання протягом останніх десятиліть проявів інформаційної агресії та насильства; активізація явищ агресивної реклами, маніпулятивних практик впливу на свідомість, проведення інформаційно-психологічних операцій; за оцінками американських експертів, понад 100 держав світу здійснюють розробку інформаційної зброї чи її компонентів (у той час як засоби масового ураження розробляються приблизно у 20 країнах); потенційні наслідки застосування сучасної інформаційної зброї, відповідно до висновків фахівців європейських країн, України і США, можуть бути співмірними з використанням зброї масового ураження; новітні інформаційні ризики становлять реальну загрозу міжнародному правопорядку та безпеці людства [65, с. 3-7].

Щодо забезпечення кібербезпеки, в Україні розроблено та діє **Стратегія кібербезпеки України, де** визначено, що пріоритетами забезпечення кібербезпеки України є: убезпечення кіберпростору задля захисту суверенітету держави та розвитку суспільства; захист прав, свобод і законних інтересів громадян України у кіберпросторі; європейська і євроатлантична інтеграція у сфері кібербезпеки [**66**].

У цьому контексті Доктрина інформаційної безпеки України виступає базовим документом для вибудови державної політики у сфері протидії

деструктивному інформаційному впливу, насамперед з боку Російської Федерації в умовах гібридної війни. Доктрина окреслює засади формування державної інформаційної політики та визначає орієнтири для розроблення стратегічних і програмних документів, спрямованих на вдосконалення правового, методичного, технічного та організаційного забезпечення інформаційної безпеки [67].

Основою Доктрини є принципи поваги до прав і свобод людини, захисту її гідності та законних інтересів, а також протекції суспільних та державних інтересів і забезпечення територіальної цілісності та суверенітету України. В контексті цього принципу беззаперечним є категорія « вимога безпеки», що визначається як - твердження, яке виражає конкретну потребу в безпеці інформації (активу), включно із супутніми обмеженнями та умовами. Вимога безпеки, що висувається до інформації, інформаційної (автоматизованої) системи чи організації, може походити з різних джерел, серед яких, наприклад, закони, нормативно-правові акти Кабінету Міністрів України, нормативні документи, міжнародні, національні та галузеві стандарти, накази, директиви, правила (політики), положення, а також потреби конкретної організації [68].

Відповідно до Закону України «Про інформацію», державна інформаційна політика охоплює такі напрями: забезпечення доступу до інформації, рівні можливості її створення, поширення, використання та захисту; розвиток інформаційного суспільства; прозорість діяльності органів влади; розбудова інформаційних систем і електронного урядування; оновлення та збереження національних інформаційних ресурсів; забезпечення інформаційної безпеки; активізація міжнародної співпраці у сфері інформації [8].

Комплекс заходів у сфері інформаційної безпеки має бути спрямований на захист життєво важливих інтересів людини, суспільства та держави шляхом запобігання загрозам та належного реагування на них. Беручи до уваги положення нормативно-правових актів України, а саме: Про національну безпеку України, Про інформацію, Доктрину інформаційної безпеки України,

Про Національну програму інформатизації, Про основні засади забезпечення кібербезпеки України, загрози інформаційній безпеці можна класифікувати наступним чином.

1. Зовнішньополітична сфера. Серед головних загроз: розповсюдження у світовому інформаційному просторі викривленої інформації про Україну; поширення кіберзлочинності та кібертероризму; зовнішні інформаційні атаки на суспільну свідомість через медіа та інтернет.

2. Сфера державної безпеки. Окреслено ризики: інформаційні впливи, спрямовані на підрив державного ладу і суверенітету; інформаційне сприяння сепаратизму; витік секретної та конфіденційної інформації; несанкціонований доступ до державних ресурсів.

3. Воєнна сфера. До ключових загроз належать: порушення правил поводження з інформацією з обмеженим доступом; збір розвідувальних даних про оборону; кібератаки на військові інформаційні системи; радіоелектронне перехоплення інформації; інформаційно-психологічний тиск на військових та населення.

4. Внутрішньополітична сфера. Проблеми включають: нерозвиненість інститутів громадянського суспільства; маніпуляції суспільною думкою; поширення недостовірної інформації; інформаційні атаки на свідомість громадян.

5. Економічна сфера. Наголошено на: технологічному відставанні; недостатній інформатизації економіки; використанні неліцензійного програмного забезпечення; недорозвиненій інформаційній інфраструктурі.

6. Соціальна та гуманітарна сфера. Серед загроз виокремлюють: низький рівень інформатизації освіти, медицини, культури; порушення інформаційних прав громадян; поширення контенту, що суперечить культурним цінностям; витіснення української культурної продукції; послаблення єдності суспільства.

7. Науково-технологічна сфера. Проблеми охоплюють: зниження наукового потенціалу; відтік фахівців; технологічна залежність від іноземних ІТ-рішень; низька конкурентоспроможність українських технологій.

8. Екологічна сфера. Визначено такі ризики: приховування або спотворення інформації про надзвичайні ситуації; ненадійність телекомунікаційних систем в умовах надзвичайних ситуацій; недостатня інформатизація органів влади.

Концепція превентивних заходів інформаційної безпеки України у цих сферах передбачає комплексний підхід, що охоплює формування цілісної державної політики та нормативно-правової бази з урахуванням міжнародних стандартів, удосконалення адміністративно-деліктного законодавства й посилення відповідальності за інформаційні правопорушення, створення спеціалізованих координаційних інституцій, реформування законодавства у сфері медіа та інформаційних відносин, забезпечення відкритого доступу до публічної інформації, розвиток електронного урядування, а також науково-аналітичну розробку теорії інформаційних загроз; ключовим завданням цих заходів є захист свідомості людини, суспільства і держави від маніпулятивних впливів, зміцнення інформаційного суверенітету та збереження національних і духовних цінностей як основи стабільного демократичного розвитку. [69, с. 103-107].

Концепція превентивних заходів передбачає: формування системної державної політики інформаційної безпеки; удосконалення законодавства про адміністративні правопорушення у сфері інформаційної безпеки; створення спеціалізованого координаційного органу; реформування чинного законодавства з інформаційної безпеки; розвиток механізмів відкритого доступу до публічної інформації; вдосконалення системи електронного урядування; розроблення єдиної теорії інформаційних загроз [69, с. 107-108].

Наступним блоком питань щодо забезпечення інформаційної безпеки є Удосконалення єдиної системи національних електронних інформаційних ресурсів. Недостатній рівень упорядкованості державних інформаційних ресурсів утруднює доступ до суспільно значущих даних. Найважливішими завданнями є: створення інтегрованого державного інформаційного ресурсу; забезпечення взаємодії між органами влади всіх рівнів; усунення дублювання

функцій та оптимізація обміну даними; розроблення нормативної бази для інтеграції відомчих інформаційних систем.

Реалізація завдання щодо формування та забезпечення ефективного функціонування інтегрованих державних інформаційних ресурсів вимагає вирішення комплексу питань, пов'язаних із узгодженим створенням і веденням таких ресурсів міністерствами та іншими відомствами, а також із розробленням відповідної нормативно-правової бази, необхідної для забезпечення їх інтеграції та скорочення витрат різних видів ресурсів. Передусім це стосується органів виконавчої влади, які володіють розгалуженими, територіально розподіленими інформаційними інфраструктурами, спрямованими на збирання даних по всій території України та їх обробку в інтересах центральних і місцевих органів влади, а також організацій і громадян держави. [**70**].

Діяльність органів виконавчої влади у сфері забезпечення інформаційної безпеки в Україні має бути зосереджена на конструктивному поєднанні діяльності держави, громадянського суспільства та людини за трьома головними напрямами: інформаційно-психологічний вектор (захист прав людини, формування позитивного інформаційного середовища); технологічний розвиток (створення та оновлення ІТ-інфраструктури); захист інформації (забезпечення конфіденційності, цілісності, доступності, зокрема технічного захисту від кібератак).

Протидія поширенню фейкової інформації та запобігання формуванню психоемоційної залежності в осіб підліткового віку є важливими складовими забезпечення інформаційної безпеки. Як приклад, у Німеччині діє Закон про захист мереж, відомий раніше як «Закон про Facebook», який покладає на соціальні медіаплатформи обов'язок видаляти неправдиві новини та повідомлення з мовою ненависті протягом 24 годин. Дія цього закону поширюється насамперед на такі платформи, як Facebook, Twitter, YouTube та інші ресурси, що мають понад 2 мільйони користувачів у Німеччині. Санкції застосовуються виключно в межах німецької юрисдикції, водночас міністр юстиції Німеччини Хайко Маас, який виступив ініціатором цього закону,

наголосив на необхідності впровадження аналогічних механізмів на рівні всього Європейського Союзу.

У 2022 році набув чинності Закон ЄС про цифрові послуги (DSA), спрямований на обмеження шкідливого контенту, захист приватності та свободи слова. Цей Закон розроблений з метою підвищення рівня безпеки користувачів в онлайн-середовищі та недопущення поширення шкідливого контенту, який є незаконним або суперечить правилам користування платформами, зокрема такого, що містить пропаганду геноциду чи анорексії. Водночас цей акт спрямований на гарантування захисту базових прав громадян Європейського Союзу, зокрема права на приватність і свободу вираження поглядів.

Наступним кроком ЄС стало ініціювання обмежень доступу до соціальних мереж для дітей віком до 16 років, про що повідомляє Європейський парламент. Євродепутати обґрунтовують цю ініціативу результатами досліджень, згідно з якими 78 % підлітків віком від 13 до 17 років перевіряють свої електронні пристрої щонайменше один раз на годину, а кожен четвертий має ознаки залежності від смартфона. Передбачається, що діти віком від 13 до 16 років зможуть користуватися соціальними мережами лише за згодою батьків, а також підтримується розробка спеціального додатка для перевірки віку користувачів (eID) [**71**].

Національна інформаційна політика США щодо зазначеного питання акцентує увагу на: розвитку наукових досліджень у галузі комунікацій; стимулюванні поширення інновацій; створенні високотехнологічної інформаційної інфраструктури; захисті приватності; формуванні збалансованої інформаційної політики держави [58, с. 24-25].

Вагомим кроком у напрямі підвищення рівня захисту інформаційної безпеки особи є запровадження інституту, подібного до інформаційного комісара, як самостійного та незалежного органу, діяльність якого була б спрямована на гарантування і захист прав та свобод людини в інформаційній сфері. Інститут Інформаційного комісара на сьогодні функціонує в таких

державах, як Туреччина, Словаччина, Велика Британія, Португалія та Словенія. Практика зазначених країн переконливо засвідчує, що відповідна незалежна інституція зосереджує свою діяльність на захисті прав громадян, представників журналістської спільноти та громадських активістів у питаннях доступу до інформації, а також наділена комплексом повноважень щодо забезпечення належного рівня захисту персональних даних.

Доцільність створення єдиного органу інформаційного комісара, у компетенції якого поєднувалися б реалізація права на доступ до публічної інформації та захист персональних даних, підтримується й експертами Ради Європи. Зокрема, керівник офісу Ради Європи в Україні М. Енберг охарактеризував цю ініціативу як «ключову рекомендацію Ради Європи щодо аналізу та розмежування повноважень державних органів у сфері інформаційної політики та медіа в Україні» [72].

О. Солодка звертає увагу на те, що на сучасному етапі розвитку Україна має зосередити зусилля на двох базових векторах: по-перше, формуванні внутрішнього інформаційного простору як сучасного, структурованого та конкурентоспроможного; по-друге, забезпеченні сталої інформаційної присутності держави на міжнародній арені та просуванні її позитивного іміджу у світі [73].

До ключових напрямів державної політики у сфері національної безпеки України в інформаційному вимірі належать: гарантування інформаційного суверенітету України; удосконалення механізмів державного регулювання розвитку інформаційної сфери шляхом створення належних нормативно-правових та економічних умов для розвитку національної інформаційної інфраструктури й ресурсів, упровадження інноваційних технологій, а також наповнення внутрішнього і глобального інформаційного простору об’єктивною та достовірною інформацією про Україну; активне залучення медіа до процесів запобігання та протидії корупції, зловживанню службовим становищем та іншим явищам, що становлять загрозу національній безпеці; забезпечення безумовного дотримання конституційних прав і свобод, зокрема свободи слова,

права на доступ до інформації та захист персональних даних, а також недопущення неправомірного втручання органів державної влади, органів місцевого самоврядування та їх посадових осіб у діяльність медіа й журналістів, заборони цензури, дискримінації в інформаційній сфері та переслідування журналістів за політичні переконання, виконання професійних обов'язків чи критику; реалізація системних заходів щодо захисту національного інформаційного простору та протидії процесам монополізації інформаційної сфери України [13].

Серед пріоритетних напрямів удосконалення системи забезпечення інформаційної безпеки О. Солодка виокремлює: розвиток і вдосконалення правового забезпечення інформаційної безпеки шляхом формування її концептуальних засад; визначення або уточнення завдань, функцій та повноважень суб'єктів, відповідальних за забезпечення інформаційної безпеки України; гарантування інформаційного суверенітету держави з метою запобігання інформаційній залежності та інформаційній експансії з боку іноземних держав чи міжнародних організацій; стимулювання розвитку міжнародного співробітництва в інформаційній сфері в умовах перегляду його принципів і механізмів, а також посилення міжнародно-правової відповідальності за використання інформаційних сил і засобів, що негативно впливають або створюють загрози людині, суспільству й державі; зміцнення організаційних засад забезпечення інформаційної безпеки, зокрема шляхом вирішення проблем координації діяльності відповідних суб'єктів у сфері протидії інформаційній агресії та гарантування кібернетичної безпеки України; формування ефективної системи державно-приватного партнерства у сфері інформаційної безпеки; запровадження механізмів демократичного контролю за діяльністю державних суб'єктів у цій сфері; розвиток комунікаційної політики у взаємовідносинах «держава – суспільство» [73].

М. Шевчук акцентує увагу на тому, що стрімкий розвиток цифрових технологій обумовлює необхідність постійного пристосування законодавства до нових викликів і загроз у сфері інформаційної безпеки. Така адаптація

передбачає не лише оновлення чинних правових норм, а й створення нових регуляторних механізмів, спрямованих на забезпечення:

прогнозування – своєчасного виявлення потенційних загроз і ризиків у сфері інформаційної безпеки та впровадження превентивних заходів;

ефективного моніторингу – системного спостереження за станом інформаційного простору з метою виявлення прогалин і аналізу причин їх виникнення;

оперативного реагування – розроблення чітких і дієвих алгоритмів реагування на виявлені прогалини, що дає змогу мінімізувати їх негативні наслідки.

Важливою складовою забезпечення інформаційної безпеки є налагодження взаємодії між усіма зацікавленими суб'єктами з метою ефективного обміну інформацією та узгодження спільних дій у сфері протидії загрозам [74, с. 385].

Технології машинного навчання та штучного інтелекту на сьогодні перетворилися на одні з ключових інструментів у системі кібербезпеки. Їх застосування дозволяє здійснювати обробку та аналіз надзвичайно великих масивів інформації, виявляти приховані закономірності, а також ідентифікувати аномальні прояви, що можуть свідчити про потенційні або вже реалізовані порушення безпеки.

Однією з основних причин виникнення інцидентів у сфері безпеки залишаються людські помилки. Вони можуть допускатися на різних етапах функціонування систем захисту – починаючи від неправильного налаштування технічних засобів безпеки й завершуючи неадекватним або несвоєчасним реагуванням на сигнали тривоги. Для зменшення впливу людського фактора необхідним є впровадження програм навчання персоналу та підвищення рівня його обізнаності, однак цих заходів недостатньо. Організаціям доцільно також розробляти та впроваджувати ефективні політики безпеки, а також використовувати автоматизовані системи управління, що дозволяє знизити залежність від ручних операцій і, відповідно, мінімізувати ризик помилок [75].

Формування стійкої та усвідомленої культури безпеки має визначальне значення для результативності заходів у сфері кібербезпеки. Така культура повинна охоплювати всі рівні організаційної структури – від вищого управлінського персоналу до рядових працівників. Розвинена культура безпеки стимулює співробітників дотримуватися встановлених стандартів і найкращих практик, своєчасно інформувати про підозрілі дії або події, а також активно підтримувати ініціативи, спрямовані на підвищення рівня захищеності. Для її формування необхідними є безперервне навчання, налагоджена внутрішня комунікація та чітка демонстрація прихильності керівництва до питань безпеки [76].

Поряд із централізованим збиранням і зберіганням журналів аудиту з широкого спектра пристроїв і програмного забезпечення, оперативним оповіщенням про інциденти інформаційної безпеки та виконанням нормативних вимог, системи моніторингу подій інформаційної безпеки повинні виконувати низку додаткових завдань. До них належать: розроблення рекомендацій щодо оптимального налаштування параметрів аудиту в кінцевих системах; класифікація подій і визначення пріоритетності інцидентів; здійснення аудиту та моніторингу подій інформаційної безпеки на всіх рівнях трирівневої архітектури прикладних систем (рівень баз даних, дії користувачів у бізнес-додатках або на вебсервері); підготовка пропозицій щодо проведення оперативно-розшукових заходів у відповідь на інциденти, що виникли; збирання доказової бази для подальшого розслідування порушень; контроль перебігу розслідування інцидентів і встановлення осіб, причетних до правопорушень, та інші заходи [76, с. 122].

Правове забезпечення інформаційної безпеки в сучасних умовах характеризується багатовимірністю, динамічністю та підвищеною складністю, що обумовлює необхідність застосування системного, міждисциплінарного й адаптивного підходу. В умовах інтенсивного розвитку інформаційних технологій, зростання масштабів і складності кіберзагроз, а також посилення ролі цифрового середовища у всіх сферах суспільного життя традиційні моделі

правового регулювання виявляються малоефективними. У зв’язку з цим першочерговим завданням стає переосмислення та актуалізація базових принципів інформаційної безпеки відповідно до викликів цифрової епохи, а також оновлення інституційних, нормативних і технологічних засад регуляторної політики.

Особливого значення набувають принципи превентивності, технологічної нейтральності, пропорційності, правомірності та адаптивності, які повинні становити методологічний фундамент сучасного інформаційного права. Також потребують перегляду методи правового впливу на інформаційні процеси, зокрема через розроблення нових законодавчих актів із чітко окресленим предметом регулювання, впровадження гнучких механізмів правового моніторингу, удосконалення інститутів юридичної відповідальності за правопорушення у сфері інформації та зміцнення інституційної спроможності суб’єктів, відповідальних за безпеку цифрового простору. Надзвичайно актуальним є формування концепції інформаційного суверенітету як стратегічної основи державної політики у сфері інформаційної безпеки, що передбачає контроль над критичною інформаційною інфраструктурою, запобігання зовнішньому втручанню в національний інформаційний простір і нормативне закріплення пріоритету національних інтересів у цифровій сфері відповідно до міжнародних стандартів та реальних безпекових викликів, з якими стикається Україна [77, с. 9].

Інформаційна безпека підприємства як складова корпоративної безпеки полягає у забезпеченні надійного захисту конфіденційної, критичної та публічної інформації від несанкціонованого доступу, витоку, втрати або несанкціонованої модифікації. Реалізація цього завдання ґрунтується на дотриманні основних принципів: конфіденційності, що передбачає надання доступу до інформації виключно уповноваженим особам; цілісності, яка полягає у недопущенні змін або пошкодження даних; доступності, що забезпечує своєчасний і повний доступ до інформаційних ресурсів.

Для імплементації відповідної стратегії необхідним є впровадження комплексу заходів, зокрема: формування політики безпеки шляхом розроблення чітких і зрозумілих правил доступу, обробки та зберігання інформації; технічне посилення захисту через використання систем шифрування, антивірусного програмного забезпечення, засобів контролю доступу та моніторингу; підвищення рівня обізнаності персоналу шляхом організації навчальних заходів; запровадження інцидент-менеджменту з визначенням процедур реагування на інциденти; орієнтація на міжнародні стандарти інформаційної безпеки з метою забезпечення системності та ефективності впроваджених рішень [78].

Відповідно до Стратегії кібербезпеки України, затвердженої Указом Президента України від 26.08.2021 № 447/2021, до основних викликів у сфері кібербезпеки належать активне використання кіберзасобів у міжнародній конкуренції; змагальний характер розвитку технологій кібербезпеки в умовах стрімкого прогресу інформаційно-комунікаційних технологій, зокрема хмарних і квантових обчислень, мереж 5G, великих даних, Інтернету речей та штучного інтелекту; мілітаризація кіберпростору та розвиток кіберзброї; наслідки пандемії COVID-19, що спричинили масову цифровізацію суспільних відносин; а також впровадження нових цифрових сервісів і механізмів електронної взаємодії без належної оцінки ризиків та системного забезпечення кібербезпеки [66].

У сучасних умовах питання забезпечення інформаційної безпеки України набуває особливої ваги з огляду на тривалу збройну агресію з боку Російської Федерації. Основними проблемами залишаються кіберзагрози, інформаційна війна, технологічні виклики та психологічний вплив на населення. Для ефективного реагування на ці загрози необхідним є комплексний підхід, що поєднує модернізацію систем кіберзахисту, розвиток стратегій протидії дезінформації, оновлення технічної інфраструктури та підвищення психологічної стійкості суспільства. Лише узгоджена взаємодія державних органів, інститутів громадянського суспільства та міжнародних партнерів

здатна забезпечити належний рівень захисту й стійкості національного інформаційного простору України, який є фундаментальною складовою національної безпеки та державного суверенітету.

Отже, на основі зазначеного вище можна зробити наступні висновки.

Україна, як і більшість держав світу, перебуває у середовищі зростаючих інформаційних ризиків, що включають кіберзлочинність, інформаційну агресію, маніпулятивний вплив та технологічні залежності. Доктрина інформаційної безпеки України формує стратегічну рамку для побудови політики у сфері протидії гібридним загрозам і визначає пріоритети щодо захисту прав громадян та національних інтересів.

Система інформаційної безпеки потребує міжсекторального підходу, який би враховував політичні, економічні, воєнні, соціальні, технологічні та екологічні чинники. Ключовим завданням є розбудова інтегрованої національної системи інформаційних ресурсів, що забезпечить якісний та оперативний обмін даними між органами влади, усуне дублювання функцій та підвищить ефективність управління.

Захист суспільної свідомості стає одним із центральних напрямів, що включає протидію фейкам, інформаційним операціям, маніпуляціям та захист дітей у цифровому середовищі. Міжнародний досвід (ЄС, США) демонструє необхідність поєднання нормативного регулювання, технологічних інновацій та міжвідомчої координації для забезпечення інформаційної безпеки.

Пріоритетним є створення системи превентивних заходів, зокрема оновлення законодавства, формування спеціалізованих інституцій, розвиток електронного урядування та розроблення національної теорії інформаційних загроз. Комплексний розвиток інформаційної сфери визначається не лише технологічною модернізацією, але й захистом прав людини, культурної ідентичності та суспільної єдності.

Численні підходи до розуміння напрямів і сфер інформаційної безпеки обумовлюють можливість здійснення узагальнення та класифікації напрямів розвитку адміністрування інформаційної безпеки в Україні.

1. **Нормативно-правовий (інституційно-правовий) напрям о**хоплює формування та розвиток правових і організаційних засад інформаційної безпеки: розроблення доктрин, стратегій, концепцій і програм; удосконалення інформаційного законодавства, адміністративно-деліктних норм; визначення повноважень і координації суб'єктів інформаційної безпеки; формування інститутів демократичного контролю (інформаційний комісар); забезпечення інформаційного суверенітету держави. **Ключовий аспект -** регулювання та гарантування основоположних прав та свобод людини і громадянина.

2. **Політико-інформаційний та ідеологічний напрям с**прямований на захист політичної стабільності та демократичних цінностей: протидія інформаційній агресії, дезінформації та пропаганді; захист конституційного ладу, суверенітету, територіальної цілісності; забезпечення свободи слова, недопущення цензури; формування позитивного міжнародного іміджу держави. **Ключовим аспектом є** стабілізація та легітимація.

3. **Інформаційно-психологічний (гуманітарний) напрям о**хоплює захист особистості та суспільної свідомості: протидія маніпуляції, психологічним операціям, мові ненависті; захист дітей і підлітків від залежності та шкідливого контенту; збереження національної ідентичності, культури, мовного простору; формування культури інформаційної та кібергігієни. **Ключовим аспектом є** захист людини та соціальної стійкості.

4. **Технологічний та інфраструктурний напрям с**прямований на розвиток і захист технічної основи інформаційного простору: розбудова національної інформаційної інфраструктури; створення та інтеграція державних електронних ресурсів; розвиток електронного урядування; захист критичної інформаційної інфраструктури; впровадження автоматизованих систем моніторингу. **Ключовим аспектом слід вважати** забезпечення стійкості та функціональності систем.

5. **Кібербезпековий напрям в**иступає спеціалізованим сегментом інформаційної безпеки: протидія кіберзлочинності, кібертероризму, кібершпигунству; захист інформаційно-телекомунікаційних систем; моніторинг

подій і реагування на інциденти; управління ризиками та забезпечення живучості систем. **Ключовим аспектом є** превентивно-оперативне реагування на загрози.

6. **Економічний та корпоративний напрям п**ов'язаний із захистом економічних інтересів і бізнес-середовища: захист інформаційних ресурсів підприємств; запобігання витоку комерційної та фінансової інформації; розвиток національних високотехнологічних галузей; дотримання стандартів інформаційної безпеки. Головним питанням є забезпечення **Ключова функція:** економічної стабільності та конкурентноспроможності.

7. **Науково-технологічний та інноваційний напрям о**хоплює інтелектуальний потенціал держави, що забезпечується шляхом: розвитку наукових досліджень у сфері ІКТ; запобігання технологічній залежності; захисту інтелектуальної власності; підвищення конкурентоспроможності інформаційної продукції. **Ключовим аспектом є** стратегічно-розвивальні заходи.

8. **Міжнародний напрям в**ідображає зовнішній вимір інформаційної безпеки, реалізація якого можлива шляхом: міжнародного співробітництва у сфері інформаційної безпеки; імплементації стандартів ЄС і Ради Європи; участі у глобальному інформаційному просторі; протидії транснаціональним інформаційним загрозам. **Ключовим аспектом є** координаційна та інтеграційна **функція.**

Висновки до розділу 3.

Отже, підсумовуючи розгляд питань щодо зарубіжного досвіду публічного управління та адміністрування у сфері інформаційної безпеки, пріоритетних напрямів розвитку адміністрування інформаційної безпеки України, є підстави сформулювати наступні висновки:

формування систем публічного управління та адміністрування у сфері інформаційної безпеки в Сполучених Штатах Америки та країнах Європейського Союзу відбувалося як реакція на глобальні трансформації інформаційного суспільства та зростання ролі інформаційних і комунікаційних технологій у забезпеченні національної та міжнародної безпеки. Інформаційна безпека набула статусу стратегічного напряму державної політики, що інтегрує правові, організаційні, технічні та соціальні механізми управління. Американська модель інформаційної безпеки характеризується історичною спадкоємністю правового регулювання, технологічною орієнтацією та активним залученням приватного сектору до реалізації державної політики. Вона ґрунтується на поєднанні ринкових механізмів, державних стандартів і жорстких інструментів протидії кіберзагрозам, що посилює спроможність держави забезпечувати національну безпеку в умовах динамічного розвитку кіберсередовища. Водночас у межах цієї моделі зберігається прагнення до балансу між безпековими інтересами та конституційними гарантіями свободи слова і приватності.

Європейський Союз сформував іншу концептуальну парадигму інформаційної безпеки, у центрі якої перебуває людина, її права і свободи. Європейський підхід вирізняється високим рівнем нормативної уніфікації, розвитком наднаціональних інституцій (зокрема ENISA) та впровадженням комплексних директив і регламентів, що забезпечують узгодженість політик кібербезпеки в державах-членах. Соціальна спрямованість, захист персональних даних і розвиток електронного урядування розглядаються як невід’ємні складові інформаційної безпеки.

Порівняння американської та європейської моделей засвідчує їх концептуальну відмінність, зумовлену різними ціннісними орієнтирами та історико-політичними умовами розвитку. Якщо для США пріоритетними є технологічне лідерство та безпекова ефективність, то для ЄС – демократичний контроль, соціальна відповідальність держави та пріоритет прав людини. Водночас обидві моделі підтверджують необхідність комплексного підходу до

інформаційної безпеки як багатовимірного явища, що виходить за межі національних кордонів і потребує міжнародної координації;

розвиток адміністрування інформаційної безпеки України відбувається в умовах зростаючої складності та багатовимірності інформаційних загроз, зумовлених цифровізацією суспільних відносин, гібридною війною, глобалізацією інформаційного простору та стрімким технологічним прогресом. Інформаційна безпека постає не лише як техніко-правова категорія, а як системне соціально-правове явище, що охоплює захист особи, суспільства і держави в політичному, економічному, гуманітарному, воєнному та міжнародному вимірах. Нормативно-правова база України, зокрема Доктрина інформаційної безпеки та Стратегія кібербезпеки України, формує концептуальні орієнтири державної політики у цій сфері та визначає пріоритетність превентивного підходу, поєднання правового регулювання з організаційними, інституційними та технологічними механізмами. Водночас ефективність такої політики значною мірою залежить від чіткого розмежування повноважень суб’єктів інформаційної безпеки, належної координації між ними, а також від дотримання принципів пропорційності, правомірності й поваги до прав і свобод людини.

Обґрунтовано, що ключовими пріоритетами розвитку адміністрування інформаційної безпеки України є: удосконалення нормативно-правового та інституційного забезпечення; протидія інформаційній агресії та маніпулятивному впливу; захист суспільної свідомості та національної ідентичності; розвиток національної інформаційної інфраструктури й електронного урядування; посилення кібербезпекових механізмів; захист економічних та корпоративних інформаційних ресурсів; стимулювання науково-технологічного розвитку; активізація міжнародного співробітництва та імплементація європейських стандартів.

Таким чином, адміністрування інформаційної безпеки України має розвиватися на основі комплексного, міжсекторального та адаптивного підходу,

що поєднує превентивні й реактивні заходи, інноваційні технології, правові гарантії та демократичний контроль. Реалізація зазначених пріоритетних напрямів створює передумови для підвищення стійкості національного інформаційного простору, зміцнення державного суверенітету та забезпечення сталого демократичного розвитку України в умовах сучасних інформаційних викликів.

ВИСНОВКИ

За підсумками проведеного теоретико-правового дослідження публічного управління та адміністрування у сфері інформаційної безпеки в Україні досягнуто поставленої мети та виконано визначені завдання, що дозволяє сформулювати такі узагальнені висновки.

1. У результаті з'ясування природи інформації як правової та соціальної категорії встановлено, що інформація в системі публічного управління виступає не лише об'єктом правового регулювання, а й інструментом управлінського впливу та соціальної комунікації. Доведено, що юридичного значення інформація набуває виключно за умови її об'єктивації та включення у суспільні відносини, що обґрунтовує необхідність державного регулювання інформаційних процесів, а не лише окремих інформаційних ресурсів. Визначено, що сучасний етап розвитку інформаційного суспільства трансформував інформацію у стратегічний ресурс держави, що безпосередньо впливає на стабільність публічного управління та національну безпеку.

2. На підставі аналізу наукових підходів до розуміння категорії «інформаційна безпека» узагальнено, що в науковій доктрині домінують три основні підходи: інформаційна безпека як стан захищеності; як система правових, організаційних і превентивних заходів; як безперервний управлінський процес. Обґрунтовано, що для сфери публічного управління найбільш релевантним є комплексний підхід, який поєднує всі три зазначені складові. Встановлено, що відсутність єдиного понятійного підходу у законодавстві ускладнює формування цілісної моделі адміністративно-правового забезпечення інформаційної безпеки в Україні.

3. У ході дослідження змісту інформаційної безпеки в контексті інформаційних прав і законних інтересів особи доведено, що інформаційні права людини становлять ядро системи інформаційної безпеки. Виявлено, що чинна модель державної політики у сфері інформаційної безпеки має подвійну

спрямованість: з одного боку – захист інформаційного суверенітету держави, з іншого – гарантування конституційних прав і свобод людини. Обґрунтовано, що недотримання цього балансу призводить або до надмірного обмеження свободи інформації, або до зниження рівня захищеності інформаційного простору.

4. У результаті аналізу елементів системи забезпечення інформаційної безпеки встановлено, що така система в Україні складається з принципів, засобів, методів, суб'єктів забезпечення інформаційної безпеки

Принципи забезпечення інформаційної безпеки становлять базові, концептуальні засади, які визначають спрямованість, зміст і межі діяльності суб'єктів публічного управління у цій сфері. До загальноуправлінських принципів належать: принцип законності, відповідно до якого всі заходи у сфері інформаційної безпеки здійснюються виключно на підставі Конституції та законів України; принцип пріоритету прав і свобод людини, що передбачає неприпустимість обмеження інформаційних прав особи інакше як у випадках, прямо передбачених законом; принцип гласності та прозорості, який забезпечує відкритість діяльності органів публічної влади у сфері інформаційної політики; принцип відповідальності, що зобов'язує суб'єктів управління нести юридичну відповідальність за порушення законодавства у сфері інформаційної безпеки.

До спеціальних принципів забезпечення інформаційної безпеки належать: принцип системності, який вимагає комплексного підходу до захисту інформаційного простору; принцип превентивності, що орієнтує систему не лише на реагування, а й на попередження інформаційних загроз; принцип збалансованості інтересів особи, суспільства і держави, який забезпечує узгодження приватних і публічних інтересів; принцип міжвідомчої координації, що передбачає узгоджену діяльність усіх суб'єктів системи інформаційної безпеки; принцип адаптивності, який забезпечує гнучке реагування на нові інформаційні виклики та загрози.

Визначено, що засобами забезпечення інформаційної безпеки є інструменти, за допомогою яких реалізуються завдання та функції публічного

управління у цій сфері. До правових засобів належать: норми Конституції України; закони та підзаконні нормативно-правові акти у сфері інформації, кібербезпеки, захисту персональних даних; стратегії, доктрини, концепції та державні програми інформаційної безпеки.

Організаційні засоби включають: створення та функціонування уповноважених органів; визначення їх повноважень і компетенції; механізми міжвідомчої взаємодії та координації.

Інформаційно-аналітичні засоби охоплюють: моніторинг інформаційного простору; аналіз інформаційних загроз; прогнозування інформаційних ризиків.

Технічні та технологічні засоби спрямовані на: захист інформаційних систем і ресурсів; забезпечення цілісності, конфіденційності та доступності інформації; кіберзахист державних інформаційних ресурсів.

Досліджено способи забезпечення інформаційної безпеки, що відображають управлінський вплив суб’єктів публічної влади на інформаційні відносини. До правових способів належать: нормотворчість; ліцензування та сертифікація; встановлення юридичної відповідальності за інформаційні правопорушення.

Адміністративні способи включають: управлінські приписи та розпорядження; контроль і нагляд за дотриманням законодавства; застосування адміністративного примусу.

Економічні передбачають: фінансування заходів інформаційної безпеки; державну підтримку розвитку інформаційної інфраструктури; стимулювання інновацій у сфері захисту інформації.

Сформульовано дефініцію «суб’єкти забезпечення інформаційної безпеки» – це учасники публічних та приватних відносин, які наділені відповідними повноваженнями та відповідальністю. До основних суб’єктів публічного управління належать: Верховна Рада України; Президент України; Кабінет Міністрів України; Рада національної безпеки і оборони України; центральні органи виконавчої влади (СБУ, Мінцифри, МВС, інші); органи місцевого самоврядування.

Спеціалізованими суб’єктами є: органи кібербезпеки; уповноважені органи у сфері захисту персональних даних; регулятори у сфері інформації та медіа.

До недержавних суб’єктів належать: суб’єкти господарювання; засоби масової інформації; громадські організації.

Таким чином, принципи, засоби, способи,методи та суб’єкти забезпечення інформаційної безпеки утворюють цілісну систему публічного управління, ефективність якої залежить від узгодженості нормативно-правового регулювання, інституційної спроможності держави та рівня взаємодії з громадянським суспільством. Їх комплексне застосування забезпечує стабільність інформаційного простору, захист прав людини та інформаційний суверенітет України.

5. Визначаючи роль держави в системі захисту інформаційної безпеки, обґрунтовано, що держава є ключовим координуючим суб’єктом, який формує правові рамки, визначає стратегічні пріоритети та забезпечує реалізацію державної політики у цій сфері. Доведено, що ефективність державного управління інформаційною безпекою безпосередньо залежить від якості адміністративних процедур, прозорості управлінських рішень та рівня інституційної спроможності уповноважених органів.

6. У процесі дослідження особливостей забезпечення інформаційної безпеки в різних секторах суспільства встановлено, що універсальні управлінські механізми є недостатньо ефективними. Обґрунтовано необхідність секторального підходу до адміністрування інформаційної безпеки з урахуванням специфіки державного управління, медіасфери, приватного сектору та соціального середовища. Доведено, що ігнорування цієї специфіки призводить до зниження ефективності державних заходів та зростання інформаційних ризиків.

7. На основі аналізу зарубіжного досвіду публічного управління та адміністрування інформаційної безпеки встановлено, що найбільш ефективними є моделі, які ґрунтуються на стратегічному плануванні, міжвідомчій координації, залученні приватного сектору та громадянського

суспільства, а також на системі постійного моніторингу інформаційних загроз. Доведено можливість адаптації окремих елементів цього досвіду до українських умов, зокрема у сфері координації та стратегічного управління.

8. У результаті визначення та систематизації пріоритетних напрямів розвитку адміністрування інформаційної безпеки України обґрунтовано, що подальший розвиток цієї сфери має відбуватися за такими ключовими напрямами:

а) удосконалення нормативно-правового забезпечення адміністрування інформаційної безпеки. В межах цього напряму пропонується передбачити в чинних стратегіях і державних програмах уніфікацію понятійного апарату у сфері інформаційної безпеки шляхом закріплення базових дефініцій («інформаційна загроза», «інформаційна стійкість», «інформаційно-психологічний вплив»); чітке розмежування повноважень суб'єктів публічного управління у сфері інформаційної безпеки з метою уникнення дублювання функцій;

б) інституційне посилення системи публічного адміністрування інформаційної безпеки. Тут доцільно закласти у державних програмах посилення координаційної ролі центральних органів виконавчої влади у сфері інформаційної безпеки, розвиток міжвідомчих механізмів взаємодії між органами державної влади та органами місцевого самоврядування, створення або вдосконалення постійно діючих координаційних платформ для обміну інформацією про загрози;

в) запровадження ризик-орієнтованого підходу до адміністрування інформаційної безпеки. В межах цього напряму пропонується передбачити перехід від реактивної моделі реагування на інформаційні загрози до превентивної моделі управління ризиками; систематичний моніторинг інформаційного простору та оцінку інформаційних ризиків тощо;

г) розвиток секторального підходу до адміністрування інформаційної безпеки. У чинних стратегіях доцільно закріпити: диференційовані механізми забезпечення інформаційної безпеки залежно від специфіки окремих секторів

(державне управління, медіасфера, економіка, соціальна сфера), врахування особливостей інформаційних загроз у кожному секторі суспільства, залучення профільних суб'єктів до формування та реалізації заходів інформаційної безпеки;

д) розширення міжнародного співробітництва у сфері інформаційної безпеки, що охоплює: адаптацію європейських та євроатлантичних стандартів адміністрування інформаційної безпеки, участь України у міжнародних програмах і механізмах обміну інформацією про загрози, використання зарубіжного досвіду стратегічного планування та міжсекторальної взаємодії.

Запропоновані напрями розвитку адміністрування інформаційної безпеки мають системний характер і можуть бути використані як практичні пропозиції до чинних державних стратегій та програм. Їх реалізація забезпечить перехід від фрагментарного регулювання до комплексної, превентивної та людиноцентричної моделі публічного управління інформаційною безпекою в Україні.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Юридична енциклопедія / Відп. ред. Ю. С. Шемшученко. Київ. : Укр. енциклопедія, 1998. 1999. Т. 2. 744 с.

2. Бєляков К.І. Інформація в праві: теорія і практика : Монографія. Київ. Видавництво "КВІЦ", 2006. 116 с .

3. Кормич Б. А. Державно-правовий механізм митної політики. *Актуальні проблеми держави і права*. Одеса: Юридична Література, 2001. Вип. 11. С. 432 – 436

4. . Toffler A. Powershift. Knowledge, wealth, and the violence at the edge of the 21- century. New York: Bantam books, 1990. 586 p.

5. Пройдаков Е. М., Теплицький Л. А. Англо-український тлумачний словник з обчислювальної техніки, Інтернету і програмування.. Вид. 1-ше. Київ: СофтПрес, 2005. 546 с.

6. Johnston C.B. Global news access. The impact of new communications technologies. Westport: Praeger publishers, 1998. P. 85.

7. Конституція України : Основний Закон від 28 черв. 1996 р. URL : http://zakon2.rada.gov.ua

8. Про інформацію. Закон України від 2 жовтня 1992 р. Відомості Верховної Ради України. 1992. № 48. Ст. 650.

9. .Короткий тлумачний словник української мови / За ред. Д. Г. Гринчишина. 2-е вид., переробл. і доп. Київ. : Рад. шк., 1988. 320 с.

10. Цимбалюк В. С. Основи інформаційного права України: Навч. посібн . / За ред. М. Я. Швеця, Р. А. Калюжного, П. В. Мельника. Київ : Знання, 2004. 274 с.

11. Цимбалюк В. С. Інформаційна безпека підприємницької діяльності: визначення сутності та змісту поняття за умов входження України до інформаційного суспільства (глобальної кіберцивілізації). Підприємництво, держава, право. 2004. № 3. С. 88 – 91.

12. Забродський В. А., Кізім. Н. А. Власність, економічна безпека та держава. Харків: Бізнес-інформ, 1997. 96 с.

13. Про національну безпеку України. Закон України. **21.06.2018. №** 2469-VIII. URI : https://zakon.rada.gov.ua/laws/show/2469-19#Text

14. Какашкін Д., Шарікова О. Жаров А. Нормативно-правове забезпечення інформаційної безпеки України. 2010 р. URL : http://nc.ufei.ukrsat.com/Kyrsi%2020004/tezi/images_ tezi/054

15. Литвиненко О. В. Спеціальні інформаційні операції та пропагандистські кампанії: Монографія. Київ: Сатсанга, 2000. 222 с.

16. Гуцалюк М.В. Гайсенюк Н.А. Організація захисту інформації: Навч. посіб. Київ, 2005. 389 с.

17. Степко О. М. Аналіз головних складових інформаційної безпеки держави. Інститут міжнародних відносин Національного авіаційного університету. 2011. URL : http: // www.nbuv.gov.ua/portal/ Soc Gum/ Nviminou/ 2011 1/83-92.pdf

18. *Шульга В. І* Сучасні підходи до трактування поняття інформаційна безпека. Ефективна економіка 2015. № 4. URL : http://www.economy.nayka.com.ua/?op=1&z=5514

19. Максименко Ю. Є. Теоретико-правові засади забезпечення інформаційної безпеки України: дис. … канд. юрид. наук: 12.00.01. Київ, 2007. 186 с.

20. Марущак А. І. Інформаційне право. Доступ до інформації: Навч. посіб. Київ, 2007. 280 с.

21. Харченко Л. С., Ліпкан В. А. , Логінов О. В. Інформаційна безпека України: Глосарій; за заг. ред. Р. А. Калюжного. Київ : Текст , 2004. 136 с.

22. Березовська І. Р. Адміністративно-правові засоби забезпечення інформаційної безпеки України: дис. ... канд. юрид. наук : 12.00.07 / І. Р. Березовська; Нац. акад. внутр. справ України. Київ, 2012. 238 с.

23. Гріщенко А.О. Підходи до розуміння категорії “інформаційна безпека” та правові засади її забезпечення. *Інформація і право*. № 4(35)/2020. С. 119-133.

24. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки". *Указ Президента України. URL : https://zakon.rada.gov.ua/laws/show/685/2021#Text*

25. Рішення Конституційного Суду України у справі за конституційним поданням 50 народних депутатів України щодо офіційного тлумачення окремих положень частини першої статті 4 Цивільного процесуального кодексу України (справа про охоронюваний законом інтерес) : від 01.12.2004 р. URL : http://zakon1.rada.gov.ua/laws/show/v018p710-04.

26. Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки: Закон України від 9 січ. 2007 р. № 537-V // Відом. Верховної Ради України. 2007. № 12. Ст. 102.

27. Недюха М. П. Правова ідеологія українського суспільства : Монографія. Київ : «МП Леся», 2012. 400 с.

28. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року “Про Доктрину інформаційної безпеки України”: Указ Президента України від 25.02.17 р. № 47/2017. URL : https://www.president.gov.ua/documents/472017-21374

29. Виноградова Г.В. Інформаційне право України: Навч. Посіб. Київ: МАУП, 2006. 144 с.

30. Арістова І. В. Державна інформаційна політика та її реалізація в діяльності ОВС України: організаційно-правові засади : дис. д-ра юрид. наук: 12.00.07. Харків, 2002. 408 с.

31. Олійник О. В. Інформаційна безпека України: доктрина адміністративно-правового регулювання : дис ... д-ра юрид. наук: 12.00.07. Ін-т законодавства Верховної Ради України. Київ, 2013. 451 с.

32. Колпаков В. К. Адміністративне право України: Підручник. Київ : Юрінком Інтер, 1999. 736 с.

33. Про основні засади забезпечення кібербезпеки України. Закон України **від 05.10.2017 № 2163-VIII.** URL : https://zakon.rada.gov.ua/laws/show/2163-19#Text

34. Березовська І. Р. Адміністративно-правові засоби забезпечення інформаційної безпеки України: автореф. дис. на здобуття наук. ступ. канд. юрид. наук : спец. 12.00.07 „Адміністративне право і процес; фінансове право; інформаційне право". Київ, 2012. 18 с.

35. Конституційне право України: Підручн. для студентів вищих навч. закладів / За заг. ред. Ю. М. Тодики, В. С. Журавського. Київ : ІнЮре, 2002. 544 с.

36. Казанчук І. Д., Яценко В. П. Особливості правового регулювання діяльності Національної поліції України у сфері забезпечення інформаційної безпеки в Україні. Право і безпека. 2020. № 4 (79). С. 32-38.

37. Проект Закону України "Про інформаційний суверенітет та інформаційну безпеку України" від 12 серпня 1999 р.. Вноситься народним депутатом України Чижем І.С. (в.о. 190). Текст № 1207-d. URL : http://www.rada.kiev.ua/

38. Декларація про державний суверенітет України від 16 липня 1990 р. Відомості Верховної Ради України. 1990 № 31. Ст. 429.

39. Міжнародний пакт про громадянські і політичні права. Прийнято 16 грудня 1966 року Генеральною Асамблеєю ООН. Док. ООН A/RES/2200 A (XXI). URL : https://zakon.rada.gov.ua/laws/show/995_043#Text

40. Конвенція про захист прав і основних свобод людини 1950 року, Перший протокол та протоколи № 1, 4, 6, 7, 9, 10 та 11 до Конвенції (Рим, 4.XI.1950). URL : https://zakon.rada.gov.ua/laws/show/995_004#Text

41. Про Концепцію Національної програми інформатизації. Закон України від 4 лютого 1998 року № 75/98-ВР. Відомості Верховної Ради України. 1998. № 27- 28. Ст. 182.

42. Про Національну програму інформатизації. Закон України 01.12.2022 № 2807-IX. URL : https://zakon.rada.gov.ua/laws/show/2807-20#Text

43. Цимбалюк В. С. Сутність інформаційної безпеки в умовах входження України до глобальної кіберцивілізації. *Науковий вісник академії ДПС України*. 2007. № 4. С. 174–178.

44. Килимник І. І. Інформаційне суспільство та інформаційна безпека. Нові виклики та шляхи подолання інформаційних загроз. *Науковий вісник Ужгородського Національного Університету.* Серія Право. 2023. Випуск 76. Частина 2. С.53-57.

45. Смотрич Д.В. Браілко Л. Інформаційна безпека в умовах воєнного стану. Науковий вісник Ужгородського Національного Університету. Серія ПРАВО. 2023. Випуск 77: частина 2. С. 121-127.

46. Про рекламу. Закон України від 03.07.1996 № 270/96-ВР. URL : https://zakon.rada.gov.ua/laws/show/270/96-%D0%B2%D1%80#Text

47. Ульянова Г.О. Форми захисту авторських прав. *Південноукраїнський правничий часопис*. 2008. №2 С. 169 – 170.

48. Шульга О. А. Управління рекламно-інформаційною діяльністю підприємства. *Підприємництво і торгівля*. 2023. № 38. С. 84–93. URL : https://doi.org/10.32782/2522-1256-2023-38-11.

49. Остапишин П. П. Забезпечення інформаційної безпеки у галузі реклами: методологічні підходи . *Науковий вісник НЛТУ України*. 2003. Вип. 23.7. Ст. 368–372.

50. Марущак А. І. Інформаційна безпека як об'єкт дослідження правової науки. *Актуальні проблеми управління інформаційною безпекою держави* : зб. матер. наук.-прак. конф., 17 березня 2010 року м. Київ. : Наук. вид. відділ НА СБ України, 2010. С. 36−41.

51. Дубас О.П. Інформаційний розвиток сучасної України у світовому контексті : монографія. Київ : Ґенеза, 2004. 208 с.

52. Вознюк Євгенія, Ничипорчук Наталія. Секрет успіху США у сфері інформаційної безпеки. *Міжнародні відносини, суспільні комунікації та регіональні студії*. 2018. № 1 (3). С. 66–71. URL : https://doi.org/10.29038/2524-2679-2018-01-66-71.

53. NIS2 Directive: securing network and information systems. Shaping Europe's digital future. URL : https://digital-strategy.ec.europa.eu/en/policies/nis2-directive?utm_source=chatgpt.com.

54. Electronic Communications Privacy Act of 1986. Wikipedia. URL : https://en.wikipedia.org/wiki/Electronic_Communications_Privacy_Act?utm_source=chatgpt.com.

55. Computer Fraud and Abuse Act. Wikipedia. URL : *https://en.wikipedia.org/wiki/Computer_Fraud_and_Abuse_Act?utm_source=chatgpt.com.*

56. Computer Security Act of 1987. Wikipedia. URL : *https://en.wikipedia.org/wiki/Computer_Security_Act_of_1987?utm_source=chatgpt.com.*

57. Cyber Intelligence Sharing and Protection Act. Wikipedia. URL : https://en.wikipedia.org/wiki/Cyber_Intelligence_Sharing_and_Protection_Act?utm_source=chatgpt.com.

58. Соснін О. В. Державна політика в галузі управління інформаційним ресурсом України: дис. докт. політ. наук : 23.00.02. Київ. 2003. 395 с.

59. NIS 2 strengthens cybersecurity across the EU by setting higher standards for essential services. European Union Agency for Cybersecurity. 2016/1148. URL: https://www.enisa.europa.eu/topics/state-of-cybersecurity-in-the-eu/cybersecurity-policies/nis-directive-2?utm_source=chatgpt.com#contentList.

60. Досягнення в сфері інформатизації та телекомунікацій в контексті міжнародної безпеки : резолюція Генеральної Асамблеї ООН A/RES/56/19 від 29 листоп. 2001 р. // БД «Документи» / Організація Об'єднаних Націй. URL : http://www.worldlii.org/int/other/UNGA/2001/

61. Олійник О.В. Інформаційний простір як основа соціальноекономічного, політичного і культурного забезпечення інформаційної безпеки в Україні. *Бюлетень Міністерства юстиції України*. 2012. № 4. 286 286 С. 98-104.

62. Досягнення у сфері інформатизації і телекомунікацій в контексті міжнародної безпеки: резолюція Генеральної Асамблеї ООН A/RES/54/49 від 1 груд. 1999 р. // БД «Документи» / Організація Об’єднаних Націй. URL : http://www.worldlii.org/int/other/UNGA/2001/

63. ENISA holds a central role in supporting the implementation of Union policy and law regarding cybersecurity Cybersecurity policies. URL: https://www.enisa.europa.eu/topics/state-of-cybersecurity-in-the-eu/cybersecurity-policies?utm_source=chatgpt.com#contentList

64. Cyber Resilience Act. Regulation 2024/2847. Wikipedia. URL : https://en.wikipedia.org/wiki/Cyber_Resilience_Act?utm_source=chatgpt.com

65. Пилипчук В.Г. Системні правові проблеми формування інформаційного суспільства : зб. наук. ст. та тез ; наукове повідомлення за матеріалами міжнародної науково-практичної конференції. *Інформаційне суспільство і держава : проблеми взаємодії на сучасному етапі.* (Харків, 26 жовтня 2012 р.). Х. : НДІ державного будівництва та місцевого самоврядування, 2012. 214 с.

66. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України" *Указ Президента України* від 26 серпня 2021 року № 447/2021. URL : https://zakon.rada.gov.ua/laws/show/447/2021#Text

67. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України». Указ Президента від № 25.11.2017 р. 47/2017. URL : https://www.president.gov.ua/documents/472017-21374

68. Про затвердження Методичних рекомендацій щодо забезпечення кіберзахисту автоматизованих систем управління технологічними процесами. Наказ Адміністрації державної служби спеціального зв'язку та захисту інформації України. 29.05.2023 № 463. URL : https://zakon.rada.gov.ua/rada/show/v0463519-23#Text

69. Лісовська Ю. П. Концепція превентивних заходів у системі інформаційної безпеки України: адміністративно-правовий аспект. *Наукові праці МАУП.* Серія : Юридичні науки. 2017. Вип. 1. С. 103-109.

70. Регламент Європейського парламенту і ради (ЄС) 2019/881 від 17 квітня 2019 року про Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA) та про сертифікацію кібербезпеки інформаційно-комунікаційних технологій, а також про скасування Регламенту (ЄС) № 526/2013 (Акт про кібербезпеку). URL : https://zakon.rada.gov.ua/laws/show/984_024-19#Text

71. Children should be at least 16 to access social media, say meps. News European Parliament. URL : https://www.europarl.europa.eu/news/en/press-room/20251120IPR31496/children-should-be-at-least-16-to-access-social-media-say-meps

72. Рада Європи рекомендує створити офіс інформаційного комісара в Україні. URL: http://www.eurointegration.com.ua/news/2017/03/1/7062377/

73. Солодка О. М. Сучасні тенденції міжнародної політики забезпечення інформаційної безпеки. *Інформаційна безпека людини, суспільства, держави.* 2013. № 3. С. 25-29.

74. Шевчук М. О. Аналіз національного законодавства про інформаційну безпеку. *Юридичний науковий електронний журнал*. № 1/2025. С. 383–386. URL : http://lsej.org.ua/1_2025/89.pdf

75. Гарасим Ю. Р., Ромака В. А., Рибій М. М. Аналіз процесу управління ризиками інформаційної безпеки в процесі забезпечення властивості живучості систем. *Вісник Національного університету «Львівська політехніка». «Автоматика, вимірювання та керування».* 2013. № 756. С. 105–123.

76. Гордієнко С., Кобус О. Питання вдосконалення процесів виявлення і обробки подій та інцидентів інформаційної безпеки. *Інформаційна безпека людини, суспільства, держави*. 2025. № 1(37). С. 117–137. URL : https://journals.uran.ua/ispss/article/view/312748

77. Чистоклетов Л., Буняк Р. Принципи та методи удосконалення правового забезпечення інформаційної безпеки в сучасному вимірі. *Академічні візії*. 2025. № 44. URL : https://academy-vision.org/index.php/av/article/view/2096

78. Мащенко М. А., Іпполітов Є. М. Формування стратегії посилення інформаційної безпеки підприємства. *Економіка та суспільство*. 2024. Вип. 70. URL : https://doi.org/10.32782/2524-0072/2024-70-147