Харківський національний університет імені В.Н. Каразіна
Навчально-науковий інститут «Каразінський інститут міжнародних відносин та туристичного бізнесу»
Кафедра міжнародних відносин

КВАЛІФІКАЦІЙНА

РОБОТА МАГІСТРА

на тему: **«ІНФОРМАЦІЙНА БЕЗПЕКА ФРАНЦІЇ В УМОВАХ СУЧАСНИХ МІЖНАРОДНИХ ВИКЛИКІВ»**

Виконав:
студент 2-го курсу, групи УМІБ-61
спеціальності 291 «Міжнародні відносини, суспільні комунікації та регіональні студії»
ОПП «Міжнародна інформаційна безпека»
Гринець Михайло Олександрович
(прізвище, ім'я, по батькові)

Керівник:
к.п.н., доц. Пересипкіна Ірина Валентинівна
(науковий ступінь, вчене звання, прізвище, ім'я, по батькові)

Рецензент:
к.п.н., доц. Калюжна Юлія Іванівна
(науковий ступінь, вчене звання, прізвище, ім'я, по батькові)

ХАРКІВ – 2025 р.

Харківський національний університет імені В. Н. Каразіна
Навчально-науковий інститут «Каразінський інститут міжнародних відносин та туристичного бізнесу»
Кафедра міжнародних відносин
Спеціальність 291 «Міжнародні відносини, суспільні комунікації та регіональні студії»
Освітньо-професійна програма «Міжнародна інформаційна безпека»
Рівень вищої освіти: другий (магістерський)

ЗАТВЕРДЖУЮ
завідувачка кафедри

_____ _____ **Наталія ВІННИКОВА**
«_2_» червня 2025 року
(зі змінами від 10.09.2025; 06.10.2025)

ЗАВДАННЯ
на кваліфікаційну роботу магістра

Гринець Михайло Олександрович

Тема роботи «Інформаційна безпека Франції в умовах сучасних міжнародних викликів»

1. керівник роботи к.п.н., доц. Пересипкіна Ірина Валентинівна
затверджені наказом по університету від «02» червня 2025 року № 4001-5/1324 зі змінами від «10» вересня 2025 року № 4001-5/3049, зі змінами від «6» жовтня 2025 року № 4001-5/3656.
2. Строк подання здобувачем вищої освіти роботи 21 листопада 2025 р.
3. Перелік питань, які потрібно розробити:

– Поняття інформаційної безпеки у міжнародних відносинах
– Структурні елементи та принципи забезпечення інформаційної безпеки держави
– Основні міжнародні виклики інформаційній безпеці
– Інституційна структура системи інформаційної безпеки Франції
– Нормативно-правові засади забезпечення інформаційної безпеки Франції
– Особливості функціонування системи інформаційної безпеки Франції в умовах сучасних міжнародних відносин
– Цифровий суверенітет Франції як національна стратегія інформаційної безпеки
– Міжнародне співробітництво Франції у сфері інформаційної безпеки
– Досвід Франції для України в удосконаленні державної політики інформаційної безпеки в умовах сучасних міжнародних викликів

4. План роботи

№ з/п	Назви етапів роботи	Строк виконання етапів
1	Вибір здобувачем теми КРМ і подання заяви на кафедру; затвердження теми та призначення наукового керівника; складання та затвердження індивідуального завдання на виконання КРМ	19.05.2025-30.06.2025
2	Підготовка вступу і розділу 1 КРМ	01.09.2025-30.09.2025
3	Підготовка розділу 2 КРМ	01.10.2025-15.10.2025
4	Підготовка розділу 3 КРМ	16.10.2025-31.10.2025
5	Підготовка висновків і переліку використаних джерел	03.11.2025-14.11.2025
6	Подання студентом завершеної КРМ науковому керівнику для перевірки та оформлення відгуку, перевірка КРМ на відсутність запозичень	17.11.2025-21.11.2025
7	Попередній розгляд КРМ на комісії від кафедри	24.11.2025-28.11.2025
8	Прийняття кафедрою рішення про допуск роботи до захисту в ЕК, оформлення та зовнішнє рецензування	01.12.2025-05.12.2025
9	Захист КРМ в ЕК і присвоєння випускникам кваліфікації	08.12.2025-24.12.2025

5. Дата видачі завдання: 2 червня 2025 року (зі змінами від 10.09.2025; 06.10.2025).

Здобувач вищої освіти _____ Михайло ГРИНЕЦЬ
(підпис) (ім'я, прізвище)

Керівник роботи _____ Ірина ПЕРЕСИПКІНА
(підпис) (ім'я, прізвище)

ЗМІСТ

ВСТУП

Актуальність теми обумовлена динамічним характером глобального безпекового середовища, у якому цифрові технології, мережеві комунікації та штучний інтелект стають ключовими чинниками політичної і стратегічної конкуренції. Наразі Франція, що виступає однією з провідних держав ЄС та постійним членом Ради Безпеки ООН, дедалі частіше стикається з широким спектром інформаційних загроз, включно з кібератаками на критичну інфраструктуру, масштабними кампаніями дезінформації й іноземними впливами, спрямованими на підрив демократичних інститутів і громадської довіри. При цьому, як свідчить практика останнього десятиліття, інформаційні операції стають невід'ємною складовою геополітичного суперництва, і саме тому здатність держави ефективно реагувати на них визначає рівень її стійкості та стратегічної автономії. Водночас швидка трансформація глобального інформаційного простору обумовлює потребу Франції, з одного боку, удосконалювати власні інституційні механізми забезпечення кіберзахисту, а з іншого – формувати комплексну політику цифрового суверенітету, що охоплює як технологічний, так і нормативно-правовий виміри. З огляду на активізацію гібридних загроз після 2022 року важливими стають також міжнародні ініціативи Франції у сфері інформаційної безпеки, зокрема її участь у програмах ЄС з кіберстійкості, співпраця в межах НАТО та реалізація двосторонніх форматів із партнерами, спрямованих на протидію шкідливим впливам у цифровому середовищі. Крім того, важливо зазначити, що досвід Франції є надзвичайно цінним для України, яка нині перебуває в умовах масштабної інформаційної та кібернетичної війни. Саме тому вивчення французької моделі захисту інформаційного простору, її цифрової стратегії та міжнародних підходів дозволяє окреслити потенційні напрями імплементації передових практик у національну політику нашої держави.

Ступінь вивченості теми. Ступінь наукової розробленості проблеми інформаційної безпеки Франції в умовах сучасних міжнародних викликів загалом є достатньо високим, хоча й відзначається певною фрагментарністю.

На концептуально-теоретичному рівні важливими є напрацювання Гончарова М.В. [1], Дриги Д. [3], Кавина С.Я. [4], які формують базові підходи до розуміння інформаційної та кібербезпеки у європейському контексті. У дослідженнях Карпенка О. [5] висвітлюються аспекти протидії гібридним загрозам, що створює передумови для комплексного аналізу французьких практик. Безпосередньо французьку модель інформаційної безпеки репрезентативно досліджують Фурсай О.В. [10] та Фурсай О. [11], які розкривають інституційну структуру, нормативно-правові рамки та стратегічні напрями політики Франції в кіберсфері. Важливі емпіричні спостереження подає Слободян О.В. [8], аналізуючи інституційний розвиток та механізми захисту критичної інфраструктури. Питання цифрового суверенітету та еволюції національної кіберстратегії розглядають Санжарова Г.Ф., Бак В.І., Санжаров В.А. [7], а також зарубіжні дослідники, зокрема Дарвіш А., Романюк С.Н. [24], Кавин С., Брацук І., Литвиненко А. [46], Лодрен А. [47], Жермен Е. [37]. Теоретичне осмислення цифрового суверенітету у європейському політичному просторі представлено у працях Ватен-Оґуара М. [38], Пеллістранді Ж. [59], Лавлек Б. [49], Ґлязє Ґ. [40], Гайдепрехт С. [42], Тюрк П. [78], які деталізують взаємозв’язок між державними політиками, технологічною автономією та міжнародними викликами. Попри значний масив напрацювань, бракує комплексних досліджень, що інтегрували б правовий, інституційний, технологічний та геополітичний виміри французької інформаційної політики, що й визначає актуальність і наукову новизну теми.

Мета дослідження – визначити особливості забезпечення інформаційної безпеки Франції в умовах сучасних міжнародних викликів.

Завдання дослідження:

– визначити поняття інформаційної безпеки у міжнародних відносинах та її ключові структурні елементи й принципи забезпечення на рівні держави;

– виявити основні міжнародні виклики інформаційній безпеці та їхній вплив на трансформацію сучасних підходів до державної інформаційної політики;

– розкрити інституційну структуру та нормативно-правові засади функціонування системи інформаційної безпеки Франції;

– встановити особливості реалізації французької моделі інформаційної безпеки в умовах сучасних міжнародних відносин;

– з’ясувати можливості імплементації французького досвіду в Україні для удосконалення національної політики інформаційної безпеки в умовах актуальних міжнародних викликів.

Об’єкт дослідження – інформаційна безпека держави в міжнародних відносинах.

Предмет дослідження – система інформаційної безпеки Франції в умовах сучасних міжнародних викликів.

Теоретико-методологічна база дослідження ґрунтується на поєднанні концептуальних підходів та аналітичних методів, що дозволяють комплексно розкрити специфіку функціонування французької моделі інформаційної безпеки. Насамперед дослідження спирається на положення класичних теорій міжнародних відносин, зокрема реалізму та лібералізму, адже, як відомо, саме вони дають змогу пояснити логіку дій держави у сфері забезпечення національної безпеки, включно з інформаційною складовою. Крім того, використано положення теорії інформаційного суспільства, яка дозволяють оцінити вплив цифрової трансформації на вразливість державних інститутів і громадянського суспільства. Методологічно дослідження базується на використанні системного, інституційного та порівняльного аналізу. Системний підхід дає змогу розглядати інформаційну безпеку як цілісну структуру, де поєднані політичні, правові, технологічні та соціальні виміри. Інституційний метод забезпечує аналіз ролі ключових французьких органів – зокрема ANSSI, Міністерства збройних сил та координаційних центрів з кібероборони. Порівняльний аналіз, у свою чергу, дозволяє співвідносити французькі

практики з підходами інших країн ЄС і визначити специфіку національної моделі.

Інформаційна база дослідження охоплює широкий спектр офіційних документів Франції, міжнародних організацій та провідних аналітичних центрів, що дозволяє всебічно проаналізувати особливості забезпечення інформаційної безпеки Франції в умовах сучасних міжнародних викликів. Насамперед використано Національну стратегію цифрової безпеки Франції, Стратегію національної оборони та безпеки, щорічні доповіді Агентства національної безпеки інформаційних систем (ANSSI), а також офіційні комюніке Міністерства збройних сил та Міністерства внутрішніх справ, які містять релевантні дані про кіберінциденти, загрози критичній інфраструктурі та напрями державної політики у сфері цифрового суверенітету. Водночас, важливе значення мають документи Європейського Союзу, зокрема Європейська стратегія кібербезпеки 2020 року, регламент NIS2 і Декларація ЄС щодо боротьби з іноземними інформаційними впливами, що безпосередньо визначають нормативно-правове середовище, у якому функціонує французька система інформаційної безпеки. Окрім цього, інформаційна база містить аналітичні звіти НАТО, OECD та цифрових дослідницьких платформ, які дозволяють зіставити французькі підходи з ширшими міжнародними тенденціями. Не менш вагомими є матеріали провідних аналітичних центрів, таких як RAND Corporation, Brookings Institution, Fondation pour la Recherche Stratégique та Institut Montaigne, що подають глибокий аналіз гібридних загроз, інформаційних операцій та технологічних ризиків. До того ж, у дослідженні використано наукові статті вітчизняних та зарубіжних дослідників, присвячені проблематиці цифрової дипломатії, кібероборони, регулювання інформаційного простору та протидії дезінформації.

Практичне значення отриманих результатів. Практичне значення отриманих результатів для органів влади України полягає насамперед у можливості адаптації та впровадження ефективних елементів французької моделі інформаційної безпеки, яка, як засвідчує практика, має комплексний,

багаторівневий і переважно випереджувальний характер. Оскільки Франція поєднує жорсткі регуляторні механізми з розвитком стратегічних цифрових спроможностей, українські державні інституції, зокрема РНБО, Міністерство цифрової трансформації та профільні підрозділи силового блоку, отримують орієнтири для модернізації власних підходів, насамперед у частині побудови системи стійкості до гібридних впливів. Також, у навчальному процесі Харківського національного університету імені В.Н. Каразіна та інших вищих навчальних закладів при розробці та викладанні дисциплін, за програмами підготовки магістрів міжнародних відносин, суспільних комунікацій та регіональних студій.

Апробація дослідження була здійснена у вигляді публікації тез наукової доповіді для участі у Всеукраїнському науково-практичному круглому столі «Стратегічні напрями зовнішньої політики та дипломатії країн світу» (м. Харків, 21 листопада 2025 р.), на тему: «Features of France’s information security system».

Структура роботи. Кваліфікаційна робота магістра складається зі вступу, трьох розділів, висновків, списку використаних джерел, що налічує 80 найменувань. Загальний обсяг роботи становить 84 сторінки, з яких основного тексту – 75 сторінок.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

1.1.Поняття інформаційної безпеки у міжнародних відносинах

Інформаційна безпека у міжнародних відносинах у сучасних умовах набула статусу одного з ключових структурних елементів глобальної безпеки, адже інформаційний простір перетворився на стратегічний ресурс, що впливає на політичну стабільність, військові рішення, економічний розвиток і суспільну довіру [1, с. 34]. У найзагальнішому розумінні під інформаційною безпекою розуміють стан захищеності інформаційних ресурсів, інфраструктур та процесів обміну даними від внутрішніх і зовнішніх загроз, що здатні порушити їхню конфіденційність, цілісність або доступність. Водночас у міжнародних відносинах це поняття значно ширше, воно включає не лише технічний, але й політичний, дипломатичний, правовий та гуманітарний виміри, які визначають здатність держави чи міжнародної організації протистояти інформаційним загрозам і використовувати інформацію як інструмент впливу. Характерно, що з поширенням цифрових технологій інформаційна безпека перетворилася на багаторівневу систему, де мережеві інциденти, операції впливу, кібератаки, маніпуляції даними, психологічний тиск через соціальні мережі та порушення цифрового суверенітету виступають взаємопов’язаними явищами, а отже, вимагають комплексного, а не фрагментарного підходу. Однак, визначення інформаційної безпеки в різних наукових школах має свої відмінності, що, власне, зумовлює формування кількох методологічних підходів. Технократичний підхід розглядає інформаційну безпеку передусім як захист телекомунікаційних систем, інфраструктур, комп’ютерних мереж і критичних цифрових ресурсів. Його базою є стандарти на кшталт ISO/IEC 27001 чи NIST Cybersecurity Framework, які передбачають управління ризиками, аудит вразливостей та впровадження технічних засобів захисту. У міжнародних відносинах цей підхід особливо активно застосовується в діяльності НАТО, яке, наприклад, після кібернападів

на Естонію 2007 року створило Центр передового досвіду з кібероборони у Таллінні та визначило кіберпростір окремим операційним доменом, нарівні із сушею, морем, повітрям та космосом [18]. Здавалося б, такий підхід є найбільш «очевидним», адже технічні атаки добре вимірюються, проте він не охоплює гуманітарну та політичну складові.

У гуманітарному підході акцент робиться на впливі інформації на свідомість, поведінку та ціннісні орієнтації населення. Іншими словами, мова йде про захист суспільства від пропаганди, дезінформації, когнітивних операцій та маніпуляцій громадською думкою. Прикладом може слугувати російська кампанія втручання у вибори США 2016 року, коли використання бот-мереж, таргетованої реклами та маніпулятивних меседжів у соцмережах перетворило інформацію на інструмент геополітичного впливу. У цьому сенсі інформаційна безпека означає не лише технічний захист, а й стійкість суспільства до маніпулювання. Тому Європейський Союз створив East StratCom Task Force, яка з 2015 року веде моніторинг дезінформаційних кампаній та формує контрнаративи [73].

Політико-правовий підхід розкриває інформаційну безпеку через призму регулювання інформаційного простору, діяльності державних інституцій, міжнародних норм і угод. Як приклад, можна згадати Будапештську конвенцію про кіберзлочинність 2001 року – перший міжнародний документ, що встановив механізми співпраці держав у розслідуванні кіберінцидентів, а також сучасні акти ЄС: Digital Services Act (2022) та Data Governance Act [66; 3]. Поряд із цим існує геополітичний підхід, згідно з яким інформаційна безпека є продовженням змагання держав за вплив у глобальному просторі. Так, Китай активно реалізує стратегію «Цифрового шовкового шляху», пропонуючи країнам Азії, Африки й Латинської Америки телекомунікаційні рішення Huawei, а також інструменти для контролю інформаційного простору, що фактично створює залежність регіонів від китайських технологічних стандартів. США, своєю чергою, просувають концепцію «вільного та відкритого індо-тихоокеанського простору», що включає запобігання

домінуванню Китаю у сфері цифрової інфраструктури [40]. Додатково варто розглянути стратегічний підхід, який об’єднує технічні, політичні, психологічні та правові аспекти, проте акцентує увагу на плануванні, прогнозуванні та управлінні інформаційними ризиками на рівні держави. Франція у Стратегії національної безпеки 2022 року визнала інформаційні операції одним із ключових викликів і створила під егідою Міністерства оборони окреме командування зі стратегічних комунікацій [10].

Попри різноманіття підходів, інформаційна безпека у міжнародних відносинах має декілька універсальних характеристик. По-перше, вона є багатовимірною, адже складається з технологічного, інституційного, правового, когнітивного та культурного компонентів. По-друге, вона є транснаціональною: інформаційні потоки не визнають кордонів, а отже, жодна держава не здатна самостійно гарантувати абсолютний захист. По-третє, її динамічність обумовлена швидким розвитком технологій. У цьому контексті поняття «гібридні інформаційні загрози» набуває особливої ваги. Найбільш показовим є російське вторг нення в Україну 2022 року, яке супроводжувалося системними DDoS-атаками на українські банки та держустанови, створенням десятків пропагандистських Telegram-каналів, масовим поширенням фейків про «недієздатність української влади» та спробами підірвати довіру до партнерів [5]. Як наслідок, держави дедалі частіше інтегрують інформаційну безпеку у свої зовнішньополітичні доктрини. У Франції з 2022 року діє оновлена стратегія, що передбачає активне використання інструментів стратегічної комунікації та боротьби в інформаційному просторі [11].

Водночас інформаційна безпека дедалі частіше розглядається через призму цифрового суверенітету, який означає здатність держави самостійно визначати стандарти функціонування свого інформаційного простору, контролювати критичні технології та регулювати діяльність іноземних корпорацій. Європейський Союз активно просуває ідею «стратегічної автономії», ухвалюючи ініціативи на кшталт Data Governance Act (2022) та Digital Services Act (2023), які встановлюють правила для обробки даних та

відповідальності платформ [38; 15]. Важливо підкреслити, що у міжнародних відносинах інформаційна безпека має і кооперативний вимір. Попри геополітичне суперництво, держави змушені співпрацювати для протидії кіберзлочинності, захисту критичних інфраструктур та стабільності глобальної мережі. Система CERT, угоди про обмін інформацією, діяльність Групи урядових експертів ООН з інформаційної безпеки – усе це приклади створення мінімальних правил поведінки у кіберпросторі.

З огляду на це у міжнародних відносинах формується ще один підхід – соціально-комунікаційний, який наголошує на ролі комунікаційної взаємодії між державами, суспільствами та інституціями. За цим підходом інформаційна безпека є результатом ефективних комунікаційних стратегій, прозорості, відкритості даних та довіри між акторами [1, с. 35]. Додатково у теоретичних підходах до інформаційної безпеки важливе місце посідає концепція критичної інфраструктури. У цьому разі інформаційна безпека розуміється як захист систем енергетики, транспорту, охорони здоров'я, фінансового сектору та оборони від інформаційних або кіберзагроз, що можуть паралізувати їхнє функціонування [80]. Саме такі атаки здійснювалися на Іран у 2010 році за допомогою вірусу Stuxnet, який уразив системи управління ядерними об'єктами; на Україну у 2015–2016 роках, коли було зламано енергетичні компанії та тимчасово відключено електропостачання; на газопровід Colonial Pipeline у США 2021 року, коли діяльність критичного енергетичного об'єкта була паралізована.

Нарешті, варто звернути увагу на те, що формування поняття інформаційної безпеки в міжнародних відносинах значною мірою залежить від культурних та цивілізаційних відмінностей. У США, наприклад, домінує ліберальний підхід, який підкреслює важливість свободи слова, ринкової конкуренції технологічних компаній та мінімального державного втручання. У Європейському Союзі, навпаки, превалює нормативний підхід, орієнтований на захист цифрових прав громадян та забезпечення прозорості діяльності платформ, що знайшло відображення в регулюваннях GDPR, Digital Markets

Act і Digital Services Act [3]. У Китаї ж інформаційна безпека тотожна поняттю державного контролю і включає жорстке регулювання інтернету, цензуру та моніторинг [70]. Ці три моделі створюють глобальну конкуренцію підходів, що відображається на міжнародних нормах, економічних відносинах та стратегічних альянсах [40].

Водночас, попри відмінності, міжнародне співтовариство намагається сформувати мінімальний набір принципів відповідальної поведінки в кіберпросторі. Наприклад, у документах ООН неодноразово підкреслюється необхідність дотримання державами принципу невтручання, поваги до суверенітету, заборони атак на цивільну інфраструктуру, а також важливість міжнародної співпраці та обміну інформацією [45]. Хоча ці норми поки не мають обов'язкової сили, вони стають основою для розвитку майбутнього міжнародного права інформаційної безпеки. Особливої актуальності набуває питання відповідальності держав за діяльність недержавних акторів, яка може здійснюватися під їхнім прихованим або активним заохоченням. Саме тому серед фахівців зростає інтерес до концепції атрибуції, встановлення того, хто саме здійснив кібератаку або інформаційну операцію, що є надзвичайно складним завданням через можливість маскування, використання проксі-серверів та мультинаціональних бот-мереж.

У підсумку можна стверджувати, що сучасні підходи до інформаційної безпеки у міжнародних відносинах перебувають у стані активної еволюції. Вони переходять від вузького технократичного розуміння до комплексної, інтегрованої моделі, яка враховує соціальні, політичні, економічні та технологічні чинники. Інформаційна безпека вже не обмежується захистом мереж, а охоплює захист суспільства, держави, критичної інфраструктури, міжнародних норм і глобального цифрового порядку. Вона вимагає розвитку стійкості, що включає адаптивність демократичних інститутів, підвищення рівня медіаграмотності, удосконалення міжнародної координації та зміцнення потенціалу держав до прогнозування інформаційних загроз. Усе це робить інформаційну безпеку одним із ключових вимірів міжнародних відносин XXI

століття, що формує нову архітектуру глобальної безпеки, визначає характер цифрової взаємодії між державами та стає важливим чинником стратегічного розвитку світової політики.

1.2.Структурні елементи та принципи забезпечення інформаційної безпеки держави

Поступове ускладнення глобального інформаційного середовища зумовлює необхідність чіткого розуміння структурних елементів та принципів забезпечення інформаційної безпеки держави, оскільки саме вони формують цілісну архітектуру захисту від сучасних загроз. Інформаційна безпека, у найширшому значенні, визначається як стан захищеності інформаційних ресурсів, інформаційної інфраструктури та суб'єктів інформаційних відносин від деструктивних впливів, що здатні спричинити завдання шкоди політичній стабільності, національній економіці, обороноздатності або суспільному розвитку. З огляду на це, структурна побудова системи інформаційної безпеки повинна бути багаторівневою, комплексною та адаптивною до зовнішніх і внутрішніх викликів (Таблиця 2.1.).

Таблиця 2.1.

Структурні елементи та принципи забезпечення інформаційної безпеки держави

Структурні елементи	Зміст елемента	Відповідні принципи	Сутність принципу
Нормативно-правовий	Закони, стандарти, регламенти, які визначають правила захисту інформації	Законність, пропорційність	Регулювання безпеки відповідно до права; відповідність заходів рівню загроз
Інституційний	Органи влади, служби безпеки, центри кіберзахисту, розвідка	Відповідальність, кооперація	Чіткий розподіл повноважень; взаємодія між інституціями та

			міжнародними партнерами
Технологічний	Технічні засоби кіберзахисту, криптографія, системи моніторингу	Безперервність, превентивність	Постійне оновлення та попередження загроз
Аналітичний та комунікаційний	Моніторинг інформаційного простору, стратегічні комунікації	Оперативність, наукова обґрунтованість	Швидке реагування та використання сучасних досліджень
Організаційно-управлінський	Координація політики, кризове реагування, управління ризиками	Цілісність, адаптивність	Узгоджена система дій та гнучкість у змінах
Кадровий	Підготовка фахівців, підвищення кваліфікації	Компетентність, відповідальність	Професіоналізм та етичні стандарти персоналу
Соціально-психологічний	Медіаграмотність, інформаційна культура, стійкість суспільства	Прозорість, недискримінаційність	Рівний доступ до інформації та довіра громадян

Насамперед важливою складовою системи є нормативно-правовий елемент, який визначає правила функціонування інформаційного простору, закріплює повноваження органів державної влади та встановлює вимоги щодо захисту інформації. Сучасні держави формують власні правові підходи на основі міжнародних стандартів. Наприклад, Україна ухвалила Закон «Про основні засади забезпечення кібербезпеки України», що встановлює базові принципи захисту критичної інфраструктури, механізми реагування на кіберінциденти та роль державних органів у координації дій. Аналогічно Європейський Союз у 2022 році затвердив оновлену Директиву NIS2, яка поглибила вимоги до кіберстійкості операторів критичних послуг [27]. Цей нормативний фундамент задає рамки для функціонування всієї системи

безпеки, адже без чітких юридичних норм неможливо сформувати ефективні механізми протидії інформаційним загрозам [3].

Наступним структурним елементом виступає інституційна система органів, що відповідають за моніторинг, аналіз і реагування на інформаційні виклики. Вона включає розвідувальні структури, органи кібербезпеки, спеціальні служби, стратегічні комунікаційні центри, підрозділи психологічних операцій тощо. Наприклад, у США за інформаційну безпеку відповідає ціла мережа інституцій, серед яких ключову роль відіграють Агентство національної безпеки (NSA), Кіберкомандування США (USCYBERCOM), а також Департамент внутрішньої безпеки, що координує захист цивільної інфраструктури. У Франції подібні функції виконує Національне агентство з безпеки інформаційних систем (ANSSI), яке займається сертифікацією безпекових рішень, реагуванням на кіберінциденти та розробкою національних стандартів [8]. Зауважимо, що ефективність інституційної структури прямо залежить від рівня міжвідомчої координації, адже інформаційні загрози мають міждисциплінарний характер і часто охоплюють політичну, економічну, військову та соціальну сфери [11].

Технологічний елемент системи включає технічні засоби та програмне забезпечення, спрямовані на захист інформаційної інфраструктури. До них належать системи криптографічного захисту, багаторівневі мережеві фаєрволи, аналітичні платформи для виявлення аномалій, системи моніторингу кіберзагроз, а також технології штучного інтелекту, здатні прогнозувати потенційні атаки. У 2023 році, наприклад, Ізраїль впровадив розширену платформу «Cyber-Dome», яка використовує машинне навчання для відстеження ворожих кібероперацій у режимі реального часу. Такі технологічні рішення значною мірою визначають рівень стійкості держави до інформаційних атак, адже сучасні загрози щораз більше спираються на автоматизовані інструменти та високий рівень технічної підготовки [17].

Комунікаційно-аналітичний елемент забезпечує збирання, обробку, зберігання та поширення актуальної інформації для ухвалення стратегічних

рішень. Він включає центри стратегічних комунікацій, служби пресових моніторингів, інформаційно-аналітичні підрозділи державних органів та спеціалізовані дослідницькі інститути. Особливу роль відіграє аналітика соціальних мереж, оскільки саме цифровий простір стає ключовим майданчиком для поширення дезінформації [68].

Організаційно-управлінський елемент передбачає формування ефективної політики управління ризиками, кризового реагування та забезпечення інформаційної стійкості. Він включає процедури планування, моделювання загроз, навчання персоналу, координацію міждержавної взаємодії. Наприклад, НАТО регулярно проводить навчання «Cyber Coalition», де країни-члени відпрацьовують захист від складних кібероперацій, симулюють багатокомпонентні атаки та розробляють алгоритми взаємодії під час кризових ситуацій [18]. У підсумку організаційно-управлінський елемент визначає рівень готовності системи інформаційної безпеки до практичних ситуацій, коли необхідно швидко ухвалювати рішення та застосовувати наявні ресурси. Не менш важливим структурним елементом є кадровий потенціал – професійні та етичні якості фахівців, що працюють у сфері інформаційної безпеки. Підготовка компетентних кадрів є визначальною, оскільки навіть найсучас ніші технології залишаються ефективними лише у поєднанні з високим рівнем професійної відповідальності та знань. Сучасні держави активно розвивають програми освіти з кібербезпеки та стратегічних комунікацій.

Соціально-психологічний елемент системи охоплює інформаційну грамотність населення, рівень довіри до державних інституцій, стійкість суспільства до маніпуляцій і пропаганди. Не секрет, що інформаційна війна ґрунтується не тільки на технічних інструментах, а й на впливі на свідомість громадян. Тому держави впроваджують програми з медіаграмотності та критичного мислення [32]. Що стосується принципів забезпечення інформаційної безпеки, то вони визначають базові засади, на яких будується вся система, і забезпечують її стабільність. Одним із ключових принципів є

цілісність, яка передбачає поєднання всіх структурних елементів у єдиний механізм. Інформаційна безпека не може бути ефективною, якщо нормативні, технологічні та організаційні заходи функціонують ізольовано [36].

Другим важливим принципом є безперервність, що передбачає постійний моніторинг загроз, регулярне оновлення систем захисту та адаптацію до нових викликів. Інформаційний простір змінюється надзвичайно швидко, тому держави повинні постійно переглядати власні підходи. Наступним принципом є пропорційність, яка означає відповідність заходів безпеки рівню загроз. Це дозволяє уникати надмірного втручання держави у приватне життя громадян і зберігати баланс між безпекою та правами людини [26]. Відкритість і прозорість – ще один принцип, що передбачає залучення громадянського суспільства, бізнесу та експертних груп до формування інформаційної політики. Кооперація є фундаментальним принципом у контексті глобальних інформаційних викликів. Сучасні інформаційні атаки нерідко мають транскордонний характер, тому держави активно співпрацюють у форматі міжнародних організацій, обмінюються даними про загрози, проводять спільні навчання. Яскравим прикладом є взаємодія між ЄС і НАТО, які з 2016 року узгоджують спільні заходи щодо кіберстійкості, зокрема обмін розвідувальними даними та розробку спільних стандартів реагування [75].

Крім того, важливою засадою є принцип превентивності, який наголошує на необхідності не лише реагування на вже здійснені інциденти, а й упередження потенційних загроз. З огляду на стрімкий розвиток цифрових технологій та появу нових форм інформаційно-психологічного впливу, превентивні заходи стають фундаментом довгострокової безпеки. Це включає прогнозування сценаріїв атак, впровадження тестувань на проникнення (penetration testing), проведення аудиту безпеки, а також розробку загальнонаціональних планів реагування на кризові кіберситуації. Наприклад, Естонія після масштабної кібератаки 2007 року створила багаторівневу систему попередження загроз, яка стала взірцем для інших держав, а її Центр

кібероборони НАТО тепер формує аналітичні продукти для всього Альянсу [18].

Водночас принцип відповідальності передбачає, що всі учасники інформаційних відносин, від державних структур до приватних компаній та пересічних громадян, мають дотримуватися правил безпечої поведінки в інформаційному просторі. Як парадоксально це не звучить, проте саме людський фактор залишається найбільш вразливим елементом. За оцінками європейських дослідницьких центрів, понад 80 % кіберінцидентів спричинені помилками або недбалістю користувачів [60]. Тому у багатьох країнах діють програми з підвищення цифрової культури, що включають навчання держслужбовців, тренінги для підприємців та інформаційні кампанії для населення. Такий підхід дозволяє не лише зменшити кількість успішних атак, а й формує культуру відповідального використання цифрових технологій. Справедливість і недискримінаційність у доступі до інформації також належать до принципів системи інформаційної безпеки. Вони забезпечують баланс між захистом та відкритістю державних процесів. Прозорий доступ до суспільно важливої інформації зменшує ризики маніпуляцій і підвищує рівень довіри до державної політики. З іншого боку, нерівність у доступі створює сприятливий ґрунт для поширення дезінформації, оскільки групи населення, позбавлені інформаційної підтримки, стають більш вразливими до зовнішнього впливу. Саме тому Європейський Союз активно інвестує у програми цифрової інклюзії, розширюючи доступ до високошвидкісного інтернету та освітніх ресурсів [25].

Принцип оперативності є визначальним у боротьбі з інформаційними загрозами, коли швидкість реакції часто відіграє більшу роль, ніж обсяг наявних ресурсів. Кібероперації, дезінформаційні кампанії чи технічні інциденти поширюються з надзвичайною динамікою, і зволікання навіть на кілька годин може призвести до серйозних наслідків: крадіжки даних, масштабних перебоїв в роботі інфраструктури або зниження рівня довіри до державної влади. Саме тому багато країн створюють центри реагування 24/7,

які забезпечують постійний моніторинг подій та миттєве інформування відповідальних структур [57]. У контексті забезпечення інформаційної безпеки важливим є також принцип наукової обґрунтованості, що передбачає використання актуальних досліджень у сфері кібербезпеки, інформаційної політики, психології мас та міжнародних відносин. Держави дедалі частіше спираються на експертні аналітичні центри, лабораторії штучного інтелекту, академічні установи для розроблення стратегій протидії новітнім загрозам. У Канаді активно працюють міждисциплінарні дослідницькі групи, які вивчають взаємозв'язок між дезінформацією, політичною поляризацією та технологічними платформами, і результати цих досліджень інтегруються в державну політику безпеки [32].

Особливе місце в системі посідає принцип стратегічної адаптивності, оскільки інформаційне середовище змінюється швидше, ніж нормативно-правові або організаційні механізми. Адаптивність означає гнучкість у політиці, здатність переглядати стратегії, змінювати пріоритети, вдосконалювати інструменти захисту відповідно до нових типів загроз. Так, після початку широкомасштабної війни РФ проти України 2022 року багато держав переглянули підходи до функціонування власних центрів кібероборони, збільшили фінансування стратегічних комунікацій та активізували інформаційну співпрацю на міжнародному рівні [53]. Ще одним важливим принципом, що набуває значення у цифрову добу, є принцип суверенітету держави в інформаційному просторі. Він передбачає право держави самостійно визначати правила функціонування національного сегменту інформаційної інфраструктури, контролювати критичні ресурси та протидіяти іноземному втручанню. У цьому контексті багато країн формують політику цифрового суверенітету, спрямовану на захист власних даних, розвиток національних технологій і забезпечення стійкості інформаційного потенціалу. Наприклад, Франція та Німеччина реалізують ініціативу GAIA-X, мета якої — створити європейську інфраструктуру хмарних технологій, незалежну від домінування технологічних гігантів США та Китаю [7].

Системний аналіз структурних елементів та принципів інформаційної безпеки дає змогу зрозуміти, що інформаційний захист є не лише технічним чи організаційним завданням, а багатовимірним процесом, який охоплює політичні, правові, технологічні, соціальні та психологічні аспекти [1]. Відповідно до цього, держави повинні підходити до формування інформаційної політики комплексно, поєднуючи жорсткі та м'які інструменти впливу. У цьому зв'язку варто окремо наголосити на взаємозалежності між структурними елементами. Наприклад, ефективна робота інституційних органів неможлива без сучасної технологічної бази, тоді як технологічні рішення потребують правової регламентації та етичних стандартів. Аналітичний компонент тісно пов'язаний із кадровим потенціалом, адже якість аналізу визначається компетентністю фахівців. Соціально-психологічний вимір взаємодіє з нормативно-правовим, оскільки саме законодавство формує рамки інформування населення, тоді як якісний рівень інформованості громадян впливає на здатність держави протистояти маніпуляціям. Розглядаючи практичний вимір, можна стверджувати, що сильні держави мають інтегровані моделі, які синхронізують ці елементи. Наприклад, Ізраїль поєднує потужну розвідувальну інфраструктуру, високотехнологічні платформи, системну підготовку кадрів та активні інформаційні кампанії. У результаті країна посідає одне з провідних місць у міжнародних рейтингах кіберстійкості. Україна, своєю чергою, після 2022 року також значно посилила всі безпекові складові: оновила законодавство, впровадила програми кіберосвіти, розгорнула найсучасніші технології та активізувала міжнародну співпрацю [5].

Загалом структурні елементи інформаційної безпеки держави утворюють складну та багатовимірну систему, що поєднує правові, інституційні, технологічні, комунікаційні, соціальні та кадрові складові. Принципи її функціонування забезпечують узгодженість, адаптивність і стійкість цього механізму в умовах постійних інформаційних змін. Уможливлюючи ефективне реагування на загрози, вони створюють фундамент

для безпечного функціонування держави в умовах глобальної цифровізації та зростаючої конкуренції у сфері інформаційного впливу. Таким чином, інформаційна безпека перестає бути вузькотехнічним явищем і перетворюється на стратегічний пріоритет державної політики, від якого безпосередньо залежить національна стабільність, розвиток суспільства та міжнародний авторитет країни.

1.3.Основні міжнародні виклики інформаційній безпеці

У сучасному світі інформаційний простір перетворюється на ключове середовище, у якому розгортаються як внутрішньодержавні, так і глобальні процеси, що безпосередньо впливають на безпеку держав, міжнародних організацій та суспільств. Саме тому міжнародні виклики інформаційній безпеці набувають багатовимірного характеру й охоплюють технологічні, політичні, військові, соціокультурні та економічні аспекти. Під міжнародними викликами інформаційній безпеці зазвичай розуміють сукупність зовнішніх загроз, чинників та тенденцій, які ускладнюють або підривають здатність держав забезпечувати стійкість своїх інформаційних систем, медіапростору, цифрових інфраструктур і стратегічних комунікацій. У цьому контексті інформаційна безпека постає як здатність держави, суспільства та інституцій зберігати цілісність, доступність і конфіденційність інформаційних ресурсів, а також протистояти інформаційному впливу, маніпулятивним практикам і кібератакам, що походять із-за кордону [1, с. 35]. Вже сам характер сучасного міжнародного середовища, позначеного конкуренцією великих держав, глобалізацією цифрових технологій і зростанням залежності від комунікаційних мереж, свідчить про те, що виклики інформаційній безпеці мають комплексний, часто асиметричний характер.

Одним із ключових міжнародних викликів є інтенсифікація кіберзагроз, що охоплюють як атаки на критичну інфраструктуру, так і спроби втручання у політичні процеси. Кіберзагрози визначаються як дії або процеси, спрямовані на порушення функціонування інформаційних систем, доступу до даних або

їхню цілісність. Нерідко вони набувають форми державного або міждержавного протистояння, як це було, наприклад, у 2017 році під час атаки вірусу NotPetya, що уразив об’єкти в Україні та ряді країн ЄС, паралізувавши роботу портів, банків та логістичних компаній [19]. Цей інцидент став яскравим прикладом того, що кіберпростір перетворився на арену міжнародних конфліктів, у яких атаки можуть здійснюватися із території третіх держав або контрольованих акторів, так званих проксі-груп. У зв’язку з цим держави змушені розширювати свої спроможності кіберзахисту, розвивати спеціалізовані агентства та формувати багаторівневі системи реагування, що охоплюють і державний, і приватний сектори [27].

Паралельно з кіберзагрозами посилюється небезпека, пов’язана з інформаційно-психологічними операціями, що спрямовані на маніпулювання масовою свідомістю, дестабілізацію політичних систем або підрив легітимності урядів. Інформаційно-психологічні операції визначаються як комплекс дій, спрямованих на вплив на емоції, мотивацію та раціональне мислення аудиторії з метою зміни її поведінки або політичних переваг [68]. Проблема ускладнюється тим, що з розвитком штучного інтелекту з’явилися нові технології, такі як deepfake-відео, що дозволяють створювати надзвичайно переконливі фальсифікації, здатні провокувати паніку, дискредитацію політичних лідерів або соціальні конфлікти [17]. Таким чином, інформаційні операції стають невід’ємним інструментом гібридної війни, що активно використовується державами для досягнення політичних цілей без прямого застосування військової сили [5].

До числа важливих міжнародних викликів належить і глобальна конкуренція за технологічну першість, що відбувається між США, КНР, ЄС та іншими впливовими акторами. Вона охоплює боротьбу за контроль над критичними технологіями: 5G, квантовими обчисленнями, системами штучного інтелекту, супутниковими мережами та платформами великих даних. Як свідчить приклад суперництва між США та Китаєм, технологічна перевага одночасно означає і контроль над потоками інформації, і здатність формувати

глобальні стандарти кібербезпеки [76]. Китайська ініціатива «Цифровий шовковий шлях», що передбачає розвиток телекомунікаційної інфраструктури у країнах Азії, Африки та Латинської Америки, викликає стурбованість низки держав через можливе використання обладнання для збору даних або посилення залежності від китайських цифрових екосистем. Водночас Сполучені Штати активно інвестують у розвиток AI-технологій оборонного призначення та у зміцнення системи кіберзахисту об'єктів критичної інфраструктури. Зрештою, технологічна конкуренція перетворюється на стратегічний виклик інформаційній безпеці, адже контроль над глобальними технологічними ланцюгами фактично означає контроль над інформаційним простором [40]. Не менш суттєвим міжнародним викликом є поширення транснаціональної кіберзлочинності, яка виходить за межі національних юрисдикцій і часто діє у мережевих структурах, що поєднують учасників із різних країн. Кіберзлочинність включає незаконний доступ до даних, фінансові шахрайства, крадіжки персональної інформації, вимагання через програмне забезпечення-вимагач (ransomware), а також атаки на медичні, банківські т а державні ресурси. У 2021 році Європол зафіксував значне зростання кількості атак типу ransomware, що уразили лікарні у Німеччині, університети у Великій Британії та транспортні компанії у Франції [57]. Оскільки такі злочини часто координуються через Darknet і здійснюються групами, географічно розпорошеними по світу, держави стикаються з труднощами у сфері міжнародного правового співробітництва, екстрадиції та притягнення винних до відповідальності [35].

Окрему групу викликів становлять загрози, пов'язані з дії авторитарних держав, які активно використовують інформаційний простір для просування власних геополітичних інтересів. Це стосується політики Російської Федерації, що системно застосовує дезінформаційні кампанії, кібератаки та медійні операції з метою підриву єдності ЄС, дискредитації НАТО, впливу на внутрішньополітичні процеси у країнах Східної Європи та руйнування демократичних інституцій [73]. Прикладом є багаторічні інформаційні атаки

на Україну, спрямовані на формування антиукраїнських наративів, виправдання зовнішньої агресії та дестабілізацію суспільної довіри. Аналогічні практики спостерігаються у діяльності Китаю, який, хоча й використовує інші інструменти, активно працює над формуванням позитивного міжнародного іміджу через контрольовані медіаплатформи та розгалужені мережі культурної дипломатії. Додатковий вимір міжнародних викликів пов'язаний із зростанням ролі приватних технологічних корпорацій, які контролюють більшу частину глобального інформаційного простору. Такі платформи, як Meta, Google, X та TikTok, фактично виступають глобальними інформаційними посередниками, що визначають механізми поширення новин, політичної реклами, соціальних меседжів та культурного контенту. Проте держава не завжди має достатні важелі впливу на алгоритми цих платформ, які здатні формувати когнітивні упередження, створювати «інформаційні бульбашки» та сприяти поляризації суспільства. Зокрема, Європейський Союз у 2023 році запровадив Закон про цифрові послуги (Digital Services Act), який став спробою встановити єдині стандарти прозорості алгоритмів і відповідальності платформ за поширення небезпечного контенту [66].

Ще одним важливим викликом є використання штучного інтелекту у воєнній справі та міжнародній політиці. ШІ не лише відкриває нові можливості для аналізу великих масивів даних, прогнозування загроз чи автоматизації оборонних систем, але й створює потенційні ризики для інформаційної безпеки. Штучний інтелект здатний генерувати фальсифіковані повідомлення, симулювати голоси, створювати візуальні матеріали, які важко відрізнити від реальних. У військовій сфері це може призвести до помилкових рішень, провокацій або ненавмисної ескалації конфліктів [17]. Зрештою, ШІ як інструмент автоматизованого інформаційного впливу може прискорювати поширення дезінформації та підвищувати ефективність маніпулятивних кампаній, що ставить нові завдання перед державами й міжнародними організаціями.

Суттєвим міжнародним викликом залишається й нерівномірність розвитку цифрових технологій у світі. Цифрова нерівність між розвиненими країнами та державами, що розвиваються, породжує асиметричні ризики, оскільки країни з менш розвиненою інфраструктурою стають вразливішими до кібератак, дезінформаційних операцій і зовнішнього контролю над їхніми інформаційними мережами [70]. Низка держав Африки, Південної Азії та Латинської Америки часто не мають достатніх ресурсів для розбудови національних центрів кібербезпеки, що робить їх об’єктами для кібершантажу та втручання з боку глобальних технологічних акторів. З іншого боку, навіть розвинені країни стикаються з проблемою критичної залежності від зовнішніх постачальників обладнання, програмного забезпечення та хмарних сервісів, що створює потенційні вразливості у разі політичних або економічних конфліктів. Не можна оминути й проблему правового вакууму в міжнародному регулюванні кіберпростору. Попри численні ініціативи ООН, ОБСЄ та Ради Європи, досі не існує універсальної міжнародно-правової угоди, яка б чітко визначала правила поведінки держав у кіберпросторі [45]. Це створює сприятливий ґрунт для держав, які прагнуть діяти у «сірій зоні», уникаючи відповідальності. Зокрема, дискусії щодо атрибуції кібернападів, пропорційності реагування або юридичних підстав для контрдій залишаються в центрі глобальних дебатів.

Водночас важливо наголосити, що міжнародні виклики інформаційній безпеці не є ізольованими явищами, адже вони взаємодіють між собою, посилюючи загрозливий потенціал та створюючи ефект «каскадних» криз. Наприклад, кібератака на об’єкти критичної інфраструктури може супроводжуватися дезінформаційною кампанією, спрямованою на поширення паніки або дискредитацію урядових інституцій [5]. Подібні сценарії були зафіксовані під час енергетичних криз у Європі, коли технічні перебої в роботі енергомереж супроводжувалися поширенням фейкових меседжів про неспроможність урядів забезпечити стабільне функціонування системи.

Ще одним аспектом, що потребує уваги, є зростаюча роль міжнародних недержавних акторів: транснаціональних рухів, кримінальних мереж та політично мотивованих спільнот, які здатні впливати на інформаційний простір окремих країн без прямої підтримки держав. Наприклад, діяльність групи Anonymous під час російсько-української війни 2022 року показала, що недержавні актори можуть здійснювати масштабні інформаційно-кібернетичні кампанії, спрямовані проти державних структур, військових відомств або медіаорганізацій [17]. В умовах стрімкого розвитку інформаційних технологій міжнародні виклики посилюються також через глобалізацію комунікаційних потоків, які стають надзвичайно швидкими та практично неконтрольованими. Події 2022-2024 років, пов’язані з розповсюдженням фейкових відео, створених за допомогою штучного інтелекту, підтверджують, що навіть високорозвинені демократії не завжди можуть оперативно реагувати на нові форми інформаційних маніпуляцій [32].

Зважаючи на все зазначене, особливої уваги потребує питання формування міжнародних режимів та багатосторонніх механізмів протидії інформаційним загрозам. Регіональні організації, такі як Європейський Союз, НАТО та ОБСЄ, уже здійснюють спроби розробити спільні підходи до протидії кібератакам, дезінформації та іншим видам інформаційних впливів. Наприклад, ЄС створив Європейську систему реагування на дезінформацію та спеціальну групу StratCom East, яка моніторить та аналізує прокремлівські наративи [68]. НАТО, зі свого боку, зосереджує увагу на посиленні кіберзахисту країн-членів та координації дій у разі виникнення масштабних кібератак [18]. Певним чином міжнародні виклики пов’язані і з проблемою суверенітету у цифрову епоху. «Цифровий суверенітет» стає центральним концептом, який визначає можливість держави самостійно визначати політику у сфері цифрових технологій, захищати персональні дані громадян, регулювати діяльність іноземних платформ та забезпечувати національну безпеку [38]. У відповідь на міжнародні виклики, такі як іноземне втручання, інформаційні операції або контроль над критичними технологіями, багато

держав посилюють національне законодавство, створюють агентства з питань кіберзахисту та розробляють стратегії цифрової трансформації. Наприклад, Франція, Німеччина та Литва у 2021-2023 роках ухвалили низку нормативних актів, спря мованих на захист критичної цифрової інфраструктури та посилення інформаційної стійкості [7].

Водночас, незважаючи на ці кроки, міжнародні виклики залишаються серйозним випробуванням для систем інформаційної безпеки. Проблемою залишається неоднаковий рівень готовності держав до реагування на загрози, які змінюються швидше, ніж встигають оновлюватися політичні стратегії [56]. Крім того, зростання міжнародних викликів інформаційній безпеці вимагає переосмислення підходів до формування глобальної цифрової етики. Питання використання штучного інтелекту, автоматизованих систем впливу, масового збору даних та контролю над інформацією стають об’єктом інтенсивних дискусій на рівні міжнародних організацій [76].

У підсумку, зазначимо, що міжнародні виклики інформаційній безпеці є складним феноменом, що охоплює взаємопов’язані сфери: від кіберзагроз і дезінформації до технологічної конкуренції та цифрового суверенітету. Вони трансформують підходи держав до захисту інформаційного простору, стимулюють розвиток нових інституцій та міжнародних механізмів і, разом з тим, загострюють суперечності між ключовими глобальними акторами. Ефективна протидія цим викликам потребує комплексного підходу, що включає зміцнення національного законодавства, розвиток міждержавного співробітництва, інвестиції в технології та підвищення інформаційної грамотності населення.

Висновки до розділу 1

Підсумовуючи зазначимо, що поняття інформаційної безпеки у міжнародних відносинах постає як багатовимірна та динамічна категорія, що охоплює захищеність інформаційного простору держави, здатність протистояти зовнішньому впливу та зберігати стабільність комунікаційних

інфраструктур. Іншими словами, інформаційна безпека сьогодні розглядається не лише як технічний чи військовий аспект, але й як ключовий елемент політичної та соціальної стійкості, який забезпечує можливість держави ефективно функціонувати в умовах глобальної конкуренції та швидких технологічних змін. Водночас, варто підкреслити, що її зміст постійно змінюється під впливом трансформації світової політики та появи нових акторів, здатних формувати інформаційний порядок.

Узагальнюючи структурні елементи та принципи забезпечення інформаційної безпеки держави, необхідно зазначити, що сучасні системи захисту базуються на комплексному підході, який передбачає взаємодію правових, організаційних, технологічних та дипломатичних механізмів. До таких елементів належать: нормативно-правове регулювання, інституційна координація, розвиток кіберінфраструктури, підвищення цифрової грамотності населення, а також формування стійкого медіасередовища. Принципи прозорості, пропорційності, відповідальності та міжнародного співробітництва визначають характер дій держави, спрямованих на забезпечення її інформаційного суверенітету, що, у свою чергу, дозволяє ефективно реагувати на комплексні загрози.

Враховуючи основні міжнародні виклики інформаційній безпеці, слід визнати, що їх масштаби та інтенсивність зростають на тлі геополітичних конфліктів, гібридних операцій, цифрової трансформації та посилення ролі негосударственних акторів. Зокрема, дезінформаційні кампанії, кібератаки на критичну інфраструктуру, маніпулювання суспільною думкою через соціальні мережі та змагання держав за контроль над стратегічними даними створюють нову конфігурацію ризиків. Отже, комплексне розуміння поняття інформаційної безпеки, чітко вибудувана система її забезпечення та усвідомлення спектра міжнародних викликів формують основу для розробки ефективної державної політики, здатної гарантувати стабільність і стійкість держави в глобальному інформаційному середовищі.

РОЗДІЛ 2. ОСОБЛИВОСТІ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ФРАНЦІЇ

2.1.Інституційна структура системи інформаційної безпеки Франції

Інституційна структура системи інформаційної безпеки Франції вирізняється високим рівнем централізації, чіткою ієрархією компетенцій та здатністю швидко адаптуватися до нових викликів, що особливо важливо в умовах стрімкої цифровізації міжнародних відносин [8]. З огляду на те, що сучасні загрози мають багатовимірний характер, від кібератак і транснаціональної дезінформації до технологічної конкуренції та атак на інфраструктурні об’єкти, Франція вибудувала комплексну систему інституцій, яка охоплює політичний, військовий, розвідувальний, технологічний та громадський сектори. У центрі цієї системи стоїть держава, яка не лише координує ключові напрями інформаційної політики, але й визначає стратегічні пріоритети, забезпечує регуляторні умови та інтегрує діяльність різних суб’єктів [10]. Перш за все, ядром французької моделі є Національне агентство з безпеки інформаційних систем (ANSSI), створене у 2009 році та підпорядковане Генеральному секретаріату з питань оборони та національної безпеки (SGDSN) [37]. ANSSI виконує роль головного органу, відповідального за кіберзахист державного сектору, критичної інфраструктури та стратегічних підприємств. З одного боку, саме ANSSI здійснює аудит безпеки, розробляє національні стандарти, проводить сертифікацію програмного забезпечення й обладнання, а також координує реагування на кіберінциденти. З іншого боку, агентство виступає аналітичним і стратегічним центром, який формує рекомендації для уряду та визначає ключові напрями розвитку цифрового суверенітету [7]. Наприклад, у 2020 році ANSSI розробила оновлені вимоги до кіберзахисту операторів критичної інфраструктури в енергетичному та транспортному секторах, що стало відповіддю на різке зростання атак типу ransomware у Європі [60].

Характерною рисою французької моделі є тісний зв’язок між інформаційною безпекою та оборонним комплексом. Центральне місце тут займає Міністерство збройних сил, у структурі якого функціонує Командування кібероборони (COMCYBER), створене у 2017 році [2]. Воно відповідає за проведення оборонних та наступальних кібероперацій, що офіційно закріплено у Стратегії оборони Франції в кіберпросторі [12]. COMCYBER співпрацює з розвідувальними службами та бере участь у забезпеченні безпеки військових операцій за кордоном, де кіберзагрози дедалі частіше використовуються як інструмент гібридного впливу. Ключовим елементом горизонтальної координації є Генеральний секретаріат з питань оборони та національної безпеки (SGDSN), який виконує функцію міжвідомчого центру стратегічного планування та кризового управління [52]. Саме SGDSN готує щорічні доповіді з оцінки загроз, координує дії силових відомств, опрацьовує нормативно-правові ініціативи та відповідає за реалізацію Національної стратегії кібербезпеки.

Невід’ємною складовою системи інформаційної безпеки є французькі спеціальні служби. Серед них особливе місце посідає Головне управління внутрішньої безпеки (DGSI), відповідальне за протидію кібертероризму, екстремізму та іноземному впливу, а також Головне управління зовнішньої безпеки (DGSE), яке забезпечує кіберрозвідку та проводить операції зі збору інформації у цифровому середовищі [24]. Відомим прикладом ефективності DGSE стала операція зі знешкодження міжнародної шпигунської мережі у 2018 році, яка намагалася отримати доступ до даних про оборонні контракти Франції за допомогою фішингових кампаній проти державних службовців.

У сфері регуляторної політики важливу роль відіграє Вища аудіовізуальна рада (ARCOM), яка здійснює нагляд за медіасектором, дотриманням норм інформаційної етики та протидією маніпулятивному контенту. Її активність значно зросла після ухвалення в 2018 році «Закону про протидію інформаційним маніпуляціям», який став одним із перших у Європі нормативних актів, спрямованих на боротьбу з фейковими новинами у

передвиборчий період [8]. Варто підкреслити, що французька модель не обмежується державними інституціями, оскільки ефективність інформаційної безпеки значною мірою залежить від участі приватного сектору. Саме тому Франція активно залучає технологічні компанії до розроблення рішень для кіберзахисту, а також заохочує створення національних дата-центрів і розвиток власних платформ хмарних обчислень. Прикладом такої співпраці є ініціатива GAIA-X, у межах якої французькі компанії Atos, OVHcloud і Dassault Systèmes спільно з німецькими партнерами працюють над створенням європейської інфраструктури обміну даними, що має забезпечити цифровий суверенітет ЄС [38].

Інституційна структура Франції також включає науково-дослідні та освітні центри, які сприяють підготовці кваліфікованих кадрів у сфері кібербезпеки. Завдяки співпраці між ANSSI та академічними інституціями у 2022 році було розроблено нову навчальну програму для державних службовців, спрямовану на формування навичок реагування на інформаційні кризи [21]. Оскільки Франція є учасницею декількох міжнародних структур: ЄС, НАТО, ООН, її інституційна система тісно інтегрована з європейськими та євроатлантичними механізмами кібербезпеки [18]. Французькі експерти беруть участь у розробці тактичних сценаріїв для навчань Cyber Coalition, що дозволяє гармонізувати підходи держав-членів до кібероперацій. Крім того, важливо наголосити, що Франція вибудувала свою інституційну модель інформаційної безпеки таким чином, щоб забезпечити постійний обмін даними між відомствами, що дозволяє уникати дублювання функцій та оперативно реагувати на комплексні інформаційні інциденти. Наприклад, під час масштабної кібератаки на французькі медичні заклади у 2021 році (атака на лікарню в місті Дакс), ANSSI, Міністерство охорони здоров’я, поліція кібербезпеки та місцеві органи влади діяли як єдина система, координуючи дії щодо відновлення сервісів, ідентифікації векторів атаки та забезпечення безперервності медичних послуг [69]. Цей випадок яскраво продемонстрував

ефективність інтегрованого управління інформаційними кризами, що є однією з ключових сильних сторін французької системи [8].

Водночас специфічним елементом французької моделі є наявність єдиного національного центру обробки кіберінцидентів, що функціонує на базі ANSSI [8]. Центр забезпечує роботу цілодобової гарячої лінії для державних органів та стратегічних підприємств, які стикаються з кібератаками. Через нього проходить більшість повідомлень про інциденти на національному рівні, що дозволяє здійснювати централізовану аналітику, формувати статистику кіберзагроз і надавати рекомендації щодо попередження подібних атак у майбутньому. Наприклад, статистичний звіт ANSSI за 2023 рік продемонстрував, що найбільш уразливими секторами залишаються охорона здоров'я, транспорт та урядові інформаційні системи [57]. Важливо також зауважити, що в рамках SGDSN функціонує Національна рада кібербезпеки, яка виконує консультативно-наукову роль [52]. До складу ради входять провідні науковці, фахівці IT-сектору, представники бізнесу та аналітичних центрів. Це дозволяє забезпечувати постійний зв'язок між інституційною системою та науковими дослідженнями, своєрідний міст між теорією і практикою. Саме ця рада розробила рекомендації щодо адаптації французької кіберполітики до загроз, пов'язаних зі штучним інтелектом, зокрема щодо ризиків автономних систем, глибоких фейків і алгоритмічних маніпуляцій громадською думкою [17].

Однією з ключових тенденцій розвитку інституційної системи інформаційної безпеки Франції стало посилення ролі місцевих органів влади, які дедалі частіше стають об'єктами кіберзагроз. З цією метою у 2022 році уряд започаткував програму «Cyber France Résilience», спрямовану на підготовку місцевих адміністрацій до реагування на кібератаки [34]. Програма передбачає фінансування оновлення технічної інфраструктури, проведення навчань, створення регіональних центрів цифрової готовності та розробку стандартів для малих муніципалітетів. Завдяки цій програмі вже у 2023 році понад 1500

муніципалітетів отримали базові інструменти кіберзахисту, що суттєво підвищило загальний рівень стійкості державного сектору.

Важливим напрямом інституційної роботи є також забезпечення захисту виборчих процесів, які у світлі подій останнього десятиліття стали однією з головних цілей зовнішніх інформаційних впливів. У Франції створено спеціальну міжвідомчу платформу «Viginum», яка відстежує іноземні цифрові впливи, аналізує дезінформаційні кампанії та здійснює оперативну комунікацію з громадськістю щодо виявлених загроз [79]. Під час виборів 2022 року Viginum виявила десятки скоординованих інформаційних операцій, зокрема кампанії з використанням бот-мереж та фейкових акаунтів, спрямовані на дискредитацію окремих кандидатів. Суттєву роль у французькій системі відіграє і сектор стратегічних комунікацій, який інтегровано у діяльність Міністерства закордонних справ. Дипломатичні відомства Франції активно працюють над формуванням позитивного іміджу країни у міжнародному інформаційному просторі, протидією зовнішній пропаганді та просуванням французьких цінностей [35]. Зокрема, у 2023 році МЗС Франції створило спеціальний підрозділ з аналізу дезінформації в африканському регіоні, де активізувалася діяльність російських та китайських інформаційних структур.

У контексті розвитку національної безпеки важливо наголосити на діяльності Агентства національних частот (ANFR), яке опікується питаннями управління радіочастотним спектром, що є критичним ресурсом як для військових систем, так і для цивільних комунікацій. Зокрема, ANFR відповідає за безпечне впровадження технологій 5G, які, з одного боку, відкривають значні можливості для цифрового розвитку, а з іншого – несуть ризики пов’язані з потенційними вразливостями мереж. Франція запровадила суворі правила сертифікації обладнання 5G, що дозволило мінімізувати ризики використання неякісних або небезпечних технологічних рішень [51].

Не менш важливою частиною системи є судові та прокурорські інституції, які забезпечують реальне правозастосування у сфері інформаційної безпеки. Прокуратура Франції створила спеціалізовані підрозділи з

розслідування кіберзлочинів, що дозволяє забезпечити оперативність розгляду справ та відповідність судової практики сучасним цифровим реаліям [46]. Інституційна система Франції передбачає також високий рівень міжнародної координації, зокрема в рамках ЄС. Париж активно долучається до розробки європейських законодавчих ініціатив, таких як Директива NIS2, Регламент про цифрові послуги (DSA) і Регламент про цифрові ринки (DMA) [27; 66]. Це впливає не лише на внутрішню політику Франції, але й формує спільний європейський підхід до інформаційної безпеки. Зауважимо, що у будові французької інституційної системи інформаційної безпеки спостерігається тенденція до посилення стратегічного рівня прогнозування. У 2024 році уряд створив Центр передбачення кіберзагроз, який використовує методи аналізу великих даних, математичне моделювання та штучний інтелект для прогнозування майбутніх ризиків [52].

У підсумку, інституційна структура системи інформаційної безпеки Франції являє собою складний, але добре збалансован ий механізм, який поєднує стратегічні, оперативні, аналітичні та регуляторні компоненти. Сильними сторонами цієї моделі є міжвідомча координація, високий рівень інтеграції з європейськими та міжнародними структурами, активна участь приватного сектору та наукової спільноти, а також потужна правова база, яка забезпечує чітке розмежування повноважень і відповідальності. Саме багаторівневість, комплексність і здатність до адаптації роблять французьку модель однією з найефективніших у Європі та дозволяють їй успішно протистояти наявним і майбутнім інформаційним загрозам.

2.2.Нормативно-правові засади забезпечення інформаційної безпеки Франції

Формування нормативно-правових засад забезпечення інформаційної безпеки Франції ґрунтується на поєднанні традиційних принципів французької правової системи, сучасних вимог цифрової трансформації та постійного оновлення стратегічних підходів до захисту інтересів держави в

інформаційному просторі [11]. Відповідно, правове забезпечення інформаційної безпеки у Франції є багаторівневим, включає конституційні норми, спеціалізоване законодавство, підзаконні акти, стратегічні документи національної безпеки, а також регламенти та директиви Європейського Союзу, які є обов'язковими для імплементації. Саме тому інформаційна безпека розглядається як комплексне явище, що охоплює захист критичної інформаційної інфраструктури, протидію кібератакам, регулювання діяльності цифрових платформ, охорону персональних даних та забезпечення стійкості державних інституцій до інформаційних загроз зовнішнього й внутрішнього походження. Важливо підкреслити, що правові основи у сфері інформаційної безпеки Франції еволюціонували синхронно зі зміною характеру загроз. На початку 2000-х років головний акцент робився на захисті державних інформаційних систем та протидії хакерським атакам, однак уже після масштабних кібератак на урядові структури у 2007-2010 рр. французька держава переглянула підходи до кіберзахисту. Зокрема, у 2009 році було створено Агентство національної безпеки інформаційних систем (ANSSI), яке стало ключовим суб'єктом реалізації державної політики у сфері кібербезпеки [8]. Законодавча база була значно розширена, щоб надати ANSSI повноваження щодо аудиту, координації та реагування на інциденти [37]. У цьому сенсі нормативно-правові акти Франції поєднують превентивний та реактивний механізми, забезпечуючи комплексний підхід до захисту інформаційного простору держави.

Суттєву роль відіграє Конституція Франції 1958 року, яка, хоч і не містить прямого поняття «інформаційна безпека», закладає фундаментальні принципи, на яких базуються відповідні правові політики. Вона гарантує свободу інформації, недоторканність приватного життя, свободу висловлювання та право на доступ до публічної інформації. Водночас, відповідно до конституційної доктрини, ці свободи можуть бути обмежені в інтересах національної безпеки та громадського порядку, що дає державі можливість формувати нормативні механізми протидії кіберзагрозам і

незаконному використанню інформаційних технологій [25]. Саме цей баланс між правами громадян і обов'язками держави лежить в основі французької моделі регулювання інформаційної безпеки. Якщо говорити про спеціальне законодавство, то центральне місце займає Оборонний кодекс Франції, який визначає інформаційну безпеку як складову національної оборони та встановлює обов'язки органів влади щодо забезпечення захисту інформаційних систем критичної інфраструктури [20]. У статтях L.2321-1 та L.2321-2 чітко зазначено, що стратегічні мережі, телекомунікаційні системи держави та об'єкти критичної інфраструктури мають перебувати під особливим державним контролем. Визначення критично важливих об'єктів включає енергетичні компанії, транспортні системи, банківську сферу, охорону здоров'я, телекомунікації та оборонну промисловість. Наприклад, після інциденту з атакою на систему охорони здоров'я у Версалі у 2022 році норми щодо кіберзахисту медичних закладів були посилені, а вимоги до аудиту інформаційних систем – оновлені [69].

Ще одним важливим актом є Закон про цифрову Республіку (Loi pour une République numérique), ухвалений у 2016 році, який значно підсилив регулювання цифрової сфери [22]. Закон містить положення щодо відкритості державних даних, захисту персональної інформації та підвищення кіберстійкості підприємств. Наприклад, він зобов'язує приватні компанії повідомляти про інциденти кібербезпеки, що становлять загрозу громадянам або державним структурам. Цей підхід демонструє той факт, що Франція послідовно переходить від моделі централізованого державного контролю до більш інтегрованої моделі співпраці держави, бізнесу та громадянського суспільства у сфері інформаційної безпеки. Не менш значущою є роль французьких законів у сфері протидії тероризму та захисту національної безпеки. Зокрема, після серії терактів у Парижі у 2015 році було ухвалено ряд актів, що розширили повноваження розвідувальних служб, дозволили використання систем масового спостереження та посилили контроль за інтернет-комунікаціями. Закон «Про розвідку» (Loi sur le Renseignement) 2015

року встановив правові рамки для перехоплення електронних даних, моніторингу мережевого трафіку та використання спеціальних алгоритмів для виявлення підозрілої активності в цифровому середовищі [24].

Важливою складовою нормативно-правової системи Франції є також регулювання захисту персональних даних. У цьому контексті вирішальне значення має Закон про інформатику та свободи (Loi Informatique et Libertés), вперше ухвалений у 1978 році та суттєво оновлений у 2018 році для приведення у відповідність з Загальним регламентом ЄС про захист даних (GDPR) [41]. Закон визначає правила о бробки персональної інформації, встановлює обов'язки організацій щодо забезпечення її безпеки та регламентує діяльність Національної комісії з питань інформатики та свобод (CNIL), одного з найвпливовіших наглядових органів у Європі. Суттєву роль відіграє і європейський вимір нормативно-правового регулювання. Франція, як член ЄС, зобов'язана імплементувати європейські регламенти та директиви у сфері кібербезпеки. Найважливішою серед них є Директива NIS (2016/1148) та її оновлена редакція NIS2 (2022), які встановлюють підвищені вимоги до кіберстійкості операторів критичних послуг [27]. У Франції ці положення впроваджує ANSSI, координуючи діяльність приватного сектору та державних інституцій.

Важливо зазначити, що у французькій правовій системі активно застосовуються концепції цифрового суверенітету та автономії. Прийнята у 2021 році стратегія «France Relance» та оновлена стратегія цифрового суверенітету 2023 року визначають принципи контролю над національними цифровими інфраструктурами, розвиток вітчизняних хмарних сервісів (наприклад, проект Gaïa-X) та зменшення залежності від іноземних технологічних компаній [7]. Таким чином, цифровий суверенітет набуває статусу окремого напрямку державної політики інформаційної безпеки [38].

Загалом нормативно-правові засади забезпечення інформаційної безпеки Франції демонструють системність, послідовність і водночас гнучкість у реагуванні на глобальні виклики [10]. Франція поєднує національні

законодавчі інструменти з європейськими директивами, розширює повноваження спеціалізованих агентств і водночас забезпечує дотримання прав людини в цифровій сфері. Водночас сучасний розвиток інформаційних технологій актуалізує питання відповідальності цифрових платформ, що також знайшло своє відображення у французькому законодавстві. Зокрема, у 2020 році Франція однією з перших у Європі запровадила закон, спрямований на боротьбу з маніпулятивним контентом і ненавистю в інтернеті (так званий «Loi Avia») [66]. Хоча частину норм було змінено, ініціатива заклала основу для подальшого формування національної моделі цифрової відповідальності платформ, яка у подальшому інтегрувалася з європейським Актом про цифрові служби (DSA), що вступив у дію у 2024 році.

Окремої уваги потребує правове регулювання протидії дезінформації, яке Франція суттєво посилила на тлі загострення геополітичного протистояння, втручання іноземних держав у виборчі процеси та масштабних кампаній впливу, спрямованих проти ЄС і НАТО. У 2018 році ухвалено закон «Проти маніпуляції інформацією» (Loi contre la manipulation de l'information), який передбачає можливість судового блокування фейкових новин під час виборчої кампанії, зобов'язує платформи надавати прозору інформацію про джерела фінансування політичної реклами та відкриває доступ громадськості до даних про власників інформаційних ресурсів [32]. Як приклад, під час президентських виборів 2022 року ці положення дозволили ефективніше контролювати поширення недостовірних матеріалів, зокрема в соціальних мережах і на зовнішніх платформах, що зменшило вплив іноземних інформаційних операцій на передвиборчу комунікацію.

Важливим елементом системи є запровадження стандартів безпеки для операторів критично важливої інфраструктури. У цьому контексті ANSSI розробляє і впроваджує обов'язкові технічні вимоги, включно з сертифікацією IT-продуктів, аудитами безпеки, обов'язком ідентифікації ризиків та регулярним оновленням протоколів кіберзахисту [62]. Наприклад, для енергетичного сектору у 2021 році запроваджено нові вимоги до управління

інцидентами, що передбачають негайне повідомлення ANSSI про будь-яку загрозу, яка може вплинути на безперервність роботи інфраструктури. Ці норми є обов'язковими і підкріплені адміністративною відповідальністю.

У французькому праві особливе місце посідає регулювання шифрування. На відміну від деяких країн, Франція не забороняє використання криптографії, проте встановлює суворі умови щодо доступу державних органів до зашифрованих даних у випадках загрози національній безпеці або розслідування тяжких злочинів [39]. Так, відповідно до Закону про електронні комунікації та Законів про внутрішню безпеку, постачальники послуг електронного зв'язку зобов'язані сприяти доступу до даних у межах юридично санкціонованих процедур. Цей механізм дозволяє зберігати баланс між необхідністю захисту приватної комунікації та інтересами боротьби зі злочинністю. Законодавство Франції також активно регулює сферу штучного інтелекту, яка розглядається як новий стратегічний напрям інформаційної безпеки. Хоча окремого закону про штучний інтелект ще не прийнято, уряд адаптує національну правову базу до вимог Європейського акту про ШІ (AI Act), який встановлює жорсткі правила щодо систем високого ризику [17]. Франція вже ухвалила низку підзаконних актів, спрямованих на забезпечення прозорості алгоритмів у сфері публічних послуг, недопущення дискримінаційних практик та регулювання використання біометричних технологій. Наприклад, у 2022 році було обмежено застосування розпізнавання облич у публічних місцях, крім випадків, пов'язаних із загрозами тероризму. Це свідчить про прагнення захистити громадянські свободи, не знижуючи рівень загальної безпеки.

Помітним стратегічним кроком стало ухвалення Національної стратегії кібербезпеки (2021), що окреслює ключові напрями розвитку нормативної бази на найближче десятиліття [51]. У документі визначено такі пріоритети, як зміцнення національного кіберсуверенітету, розвиток французької кіберіндустрії, підвищення безпеки державних сервісів, а також розширення міжнародної співпраці, особливо в межах ЄС і НАТО [7, с. 42-43]. На основі

цієї стратегії було ініційовано оновлення регулятивних механізмів, у тому числі підвищення вимог до постачальників хмарних сервісів, контроль за іноземними інвестиціями у сфері ІКТ та створення нових стандартів корпоративної кіберстійкості. Французька держава приділяє значну увагу також питанням освіти, цифрової грамотності та підготовки кадрів у сфері інформаційної безпеки. Закон «Про оновлення системи освіти у цифрову епоху» (2021) зобов'язує навчальні заклади впроваджувати програми з кібергігієни, а державні органи – проводити регулярні тренінги зі стійкості до інформаційних впливів [8]. Таким чином, нормативно-правове регулювання виходить за межі безпосереднього реагування на загрози й охоплює превентивні заходи, спрямовані на формування стійкого суспільства, здатного протистояти інформаційним маніпуляціям.

Зазначимо, що нормативно-правові засади забезпечення інформаційної безпеки Франції є складною, багатовимірною та динамічною системою, яка поєднує елементи національного та європейського права, стратегічне планування, інституційну координацію та жорсткі механізми контролю за дотриманням правових норм. Центральною особливістю французької моделі є прагнення досягти збалансованості між захистом національних інтересів і збереженням демократичних цінностей, таких як свобода слова, право на приватність і прозорість діяльності держави. Більш того, еволюція цієї системи демонструє тренд до посилення кіберсуверенітету, розвитку власних технологічних рішень та інтеграції в європейські ініціативи, що дозволяє Франції залишатися одним із ключових акторів у формуванні міжнародної політики інформаційної безпеки. Саме тому нормативно-правова база Франції нині розглядається як одна з найрозвиненіших і найкомплексніших у Європі [10], а її досвід стає важливим орієнтиром для держав, які прагнуть модернізувати власні моделі інформаційної безпеки та адаптувати їх до викликів цифрової епохи.

2.3.Особливості функціонування системи інформаційної безпеки Франції в умовах сучасних міжнародних відносин

Функціонування системи інформаційної безпеки Франції в умовах сучасних міжнародних відносин характеризується складною й багаторівневою взаємодією державних інституцій, приватного сектору, наукових центрів та міжнародних партнерів, що разом формують стійку та адаптивну модель реагування на загрози [10]. Водночас саме еволюція глобального політичного середовища, зокрема зростання гібридних загроз, іноземних інформаційно-психологічних операцій, кібератак, технологічної конкуренції та зміни балансу сил між провідними державами, змушує Францію шукати нові інструменти забезпечення цифрового суверенітету, удосконалювати наявні механізми захисту та посилювати нормативно-правові й технічні інфраструктури. Іншими словами, сучасні умови вимагають від французької системи протидії загрозам одночасно гнучкості, інноваційності та високого рівня координації, адже інформаційна безпека дедалі більше стає стратегічною складовою національної безпеки загалом. Передусім варто зазначити, що Франція розглядає інформаційну безпеку не лише у вузькому технічному вимірі, а значно ширше, як здатність держави забезпечити цілісність інформаційного простору, стійкість цифрової інфраструктури, захист критично важливих даних та протидію дезінформаційним кампаніям, які можуть завдати шкоди політичній стабільності та демократичним інститутам [8]. Це визначення випливає з багатьох стратегічних документів, серед яких Cyberdefense Strategy, Defence and National Security Strategic Review 2022 та Loi de Programmation Militaire. Таке широке розуміння інформаційної безпеки дає змогу Франції діяти комплексно та системно, охоплюючи як кіберсферу, так і гуманітарно-комунікативний вимір загроз.

Особливу роль відіграє діяльність Національного агентства з безпеки інформаційних систем (ANSSI), яке функціонує як ключовий центр формування політики кіберзахисту, а також як оперативний орган, що реагує на інциденти у державному й приватному секторах [37]. Важливо підкреслити,

що ANSSI не лише координує реагування на кібератаки, а й встановлює стандарти безпеки для критичної інфраструктури та сертифікує програмне забезпечення й обладнання. Після масштабних кібератак на французькі медіа та муніципальні системи у 20202022 рр. агентство посилило вимоги до захисту мереж органів влади, водночас ініціювавши обов'язкові аудити інформаційних систем для підприємств, що працюють у секторах енергетики, транспорту та охорони здоров'я [60]. Таким чином, система здатна оперативно адаптуватися до нових загроз, що є її ключовою особливістю.

Водночас важливу роль у забезпеченні інформаційної безпеки відіграє Міністерство збройних сил Франції, яке реалізує політику кібероборони та здійснює військові кібероперації захисного й наступального характеру. Після ухвалення Доктрини військових кібероперацій у 2019 році Франція офіційно визнала кіберпростір повноцінним театром воєнних дій, що зумовило появу чітко структурованої системи управління оборонними операціями в цифровому середовищі [47]. У межах кіберкомандування створено окремі підрозділі для моніторингу кіберактивності Китаю, Росії та Ірану, що демонструє глобальний характер загроз і необхідність постійного аналізу поведінки потенційних противників.

Окрім того, важливо наголосити на політичному та дипломатичному вимірі інформаційної безпеки Франції. У сучасних умовах іноземні дезінформаційні кампанії становлять значну загрозу для демократії, виборчих процесів та суспільної довіри. Відповіддю на такі виклики стало створення міжвідомчої структури VIGINUM у 2021 році, яка спеціалізується на виявленні, аналізі та нейтралізації інформаційних впливів іноземного походження у французькому цифровому просторі [31]. Наприклад, у 2022 році VIGINUM виявила й публічно розкрила координаційну мережу російських акаунтів, які поширювали маніпулятивні меседжі щодо французької підтримки України [79]. Такий підхід не лише захищає внутрішній інформаційний порядок, а й формує проактивну позицію Франції в боротьбі з дезінформацією на міжнародному рівні. Показовим є те, що французька система не

обмежується боротьбою з зовнішніми зловмисниками, але й активно спрямована на підвищення цифрової стійкості суспільства. Значну увагу приділено просвітницьким програмам, які реалізуються у школах та вищих навчальних закладах, а також у співпраці з громадськими організаціями. Програми з медіаграмотності, впроваджені Міністерством культури та Міністерством освіти, мають на меті навчити громадян критично оцінювати інформацію, розпізнавати фейки та розуміти механізми маніпуляцій [32].

У контексті сучасних міжнародних відносин важливо підкреслити, що Франція активно співпрацює з Європейським Союзом та НАТО у сфері кібербезпеки. Наприклад, участь у Європейському кіберкомандуванні (EU Cyber Command) або внесок у розробку Європейського акта про кіберстійкість (Cyber Resilience Act) демонструють прагнення Франції до гармонізації стандартів та створення колективної системи реагування на загрози [27]. Крім того, Франція є активним учасником спільних кібернавчань НАТО «Cyber Coalition» та ЄС «Cyber Europe», що дозволяє її фахівцям постійно вдосконалювати навички реагування в умовах симульованих криз [18]. Взаємодія з міжнародними структурами підсилює французьку модель інформаційної безпеки, роблячи її інтегрованою в європейський та трансатлантичний простір. Суттєвою особливістю французької системи інформаційної безпеки є її стратегічна орієнтація на цифровий суверенітет [7]. Це поняття передбачає здатність держави контролювати власні цифрові платформи, критичні технології, канали передачі даних та інфраструктурні елементи, мінімізуючи залежність від іноземних компаній [38]. Тому Франція інвестує в розвиток національних хмарних рішень, удосконалення супутникових систем зв’язку та підтримку європейських технологічних проєктів, таких як GAIA-X. У 2023–2024 роках уряд профінансував створення кількох нових дата-центрів, що мають відповідати найвищим стандартам безпеки та працювати виключно під французькою юрисдикцією [34]. Це дозволяє знизити стратегічні ризики, пов’язані з можливим втручанням інших держав через комерційні технологічні платформи.

Не менш важливим є розвиток партнерства з приватним сектором, адже саме бізнес володіє широким спектром технологічних ресурсів і компетенцій, необхідних для забезпечення безпеки цифрової інфраструктури. Французькі IT-компанії, такі як Thales, Orange Cyberdefense та Atos, активно залучені до створення рішень у сфері кіберзахисту, проведення аудиту та реагування на інциденти [16]. При цьому держава створює стимули для інновацій, підтримуючи стартапи у сфері штучного інтелекту, криптографії та аналізу поведінкових моделей у кіберпросторі. Значна частина цих технологій надалі інтегрується у державний сектор, що свідчить про наявність ефективної моделі державно-приватного партнерства.

Зміни у глобальному середовищі також посилюють необхідність удосконалення правової бази. Франція регулярно оновлює законодавство, адаптуючи його до нових загроз. Наприклад, у межах останніх реформ запроваджено обов’язкове повідомлення про кіберінциденти для великого бізнесу та органів влади, розширено вимоги до захисту персональних даних, а також посилено контроль за соціальними мережами щодо видалення незаконного контенту [66]. Однією з відмінних рис французької моделі є також поєднання традиційних підходів безпеки з інноваційними технологіями. Зокрема, у сфері кіберзахисту дедалі активніше використовуються рішення на основі штучного інтелекту, машинного навчання та великих даних [17]. У 2024 році Міністерство збройних сил запустило програму з впровадження алгоритмів ШІ у військові комунікаційні системи, що має забезпечити більшу автономність та швидкість прийняття рішень у цифрових операціях. Важливо підкреслити, що систему інформаційної безпеки Франції формує також високий рівень міжвідомчої координації [11]. Уряду вдалося створити модель, в якій діяльність ANSSI, VIGINUM, кіберкомандування, Міністерства внутрішніх справ, МЗС та інших органів об’єднана єдиними стратегічними цілями. У періоди кризових ситуацій функціонує спеціальний механізм швидкого прийняття рішень, що передбачає оперативний обмін інформацією та узгоджені дії між силовими структурами та цивільними службами.

Наприклад, під час президентських виборів 2022 року держава застосувала комплекс заходів, від моніторингу онлайн-впливів до посиленої кіберохорони виборчої інфраструктури, що дозволило уникнути масштабних атак або спроб маніпулювання результатами [77].

Окреслюючи особливості функціонування системи інформаційної безпеки Франції, варто зазначити, що вона базується на чотирьох ключових принципах: превентивність, адаптивність, автономність і міжнародна інтегрованість [8]. Превентивність полягає у систематичному прогнозуванні загроз та підготовці до них заздалегідь. Адаптивність – у здатності швидко реагувати на нові форми загроз, які постійно змінюються. Автономність – у прагненні зберегти контроль над критичними технологіями та цифровими ресурсами. І нарешті, міжнародна інтегрованість забезпечує можливість колективної відповіді на глобальні проблеми, які жодна країна не може подолати самостійно [7]. Варто наголосити, що функціонування системи інформаційної безпеки Франції в умовах сучасних міжнародних відносин відбувається не ізольовано, а в контексті глобальної конкуренції, яка охоплює як технологічний, так і ціннісний виміри. З одного боку, Франція змушена реагувати на нові моделі гібридних операцій, що поєднують кібератаки, інформаційний тиск, маніпулятивну дипломатію та економічні інструменти впливу [5]. З іншого боку, вона має підтримувати свою конкурентоспроможність як центр технологічних інновацій і гарант демократичних стандартів, що визначають її позиції в Європейському Союзі та світі. Таким чином, інформаційна безпека стає не просто механізмом захисту, а інструментом стратегічної проєкції сили та формування міжнародного іміджу держави.

Крім того, дедалі помітнішою стає роль Франції як ініціатора глобальних дискусій про етичні аспекти цифрових технологій. Наприклад, Париж активно просуває міжнародні норми відповідальної поведінки держав у кіберпросторі, виступає за розробку глобальних стандартів щодо штучного інтелекту та підтримує ініціативи зі створення безпечного інформаційного середовища на

рівні ООН та ЄС. У цьому контексті важливо згадати Паризький заклик до довіри та безпеки в кіберпросторі (Paris Call for Trust and Security in Cyberspace), який став платформою для співпраці понад 120 держав, компаній та організацій [35]. Саме ця ініціатива демонструє здатність Франції виступати глобальним лідером у питаннях кіберстійкості та інформаційної безпеки. Показовим є і те, що Франція значну увагу приділяє боротьбі з іноземними інформаційними впливами, які часто спрямовані на підрив соціальної єдності та довіри до державних інституцій. У відповідь створюються спеціалізовані аналітичні прилади та методики, що дозволяють виявляти «аномальні інформаційні потоки», неавтентичні акаунти, мережі ботів та координовані маніпулятивні кампанії. Зокрема, методологія VIGINUM передбачає аналіз поведінки інформаційних акторів на основі критеріїв технічної активності, повторюваності контенту та часової синхронізації [79]. Такий підхід дає змогу не лише виявляти операції впливу, а й розуміти логіку їхнього розгортання, що значно посилює ефективність реагування.

Водночас сучасне середовище ставить перед Францією нові виклики, пов’язані з розвитком штучного інтелекту, генеративних моделей, технологій deepfake та автоматизованого створення контенту. Саме ці інструменти суттєво ускладнюють процес ідентифікації джерел дезінформації та створюють ризик появи «масштабованих фейкових екосистем», здатних одночасно впливати на різні сегменти суспільства. Реагуючи на такі загрози, Франція розширює технічний потенціал ANSSI та VIGINUM для роботи з алгоритмами виявлення штучно створеного контенту [17]. У 2024 році було запущено дослідницький проєкт, спрямований на розробку систем маркування синтетичних матеріалів, що може стати частиною ширшої європейської політики цифрового маркування ШІ-контенту. Не менш важливою складовою є взаємозв’язок інформаційної безпеки з економічною та енергетичною безпекою. Оскільки сучасні технології часто стають інструментом геоекономічного тиску, Франція особливу увагу приділяє захисту об’єктів критичної інфраструктури, від АЕС та транспортних мереж до телекомунікаційних систем. Система кіберзахисту

EDF та RTE, наприклад, постійно модернізується відповідно до рекомендацій ANSSI та стандартів NIS2 [27]. Крім того, Франція раніше за інші країни ЄС запровадила заборону на використання обладнання певних виробників у мережах 5G, аргументуючи це високими ризиками втручання [38]. Такі рішення демонструють взаємозалеж ність інформаційних і стратегічних інтересів, що формують політику енергетичної незалежності та цифрової автономії.

Важливим елементом французької моделі є її гнучкість і здатність до швидкої перебудови у разі появи непередбачуваних загроз. Наприклад, під час пандемії COVID-19 Франція зіткнулася з небаченим зростанням числа кібератак на лікарні, медичні центри та страхові компанії. Відповіддю стало створення спеціальних кризових команд кіберзахисту, які діяли у режимі цілодобової координації між ANSSI, Міністерством охорони здоров’я та приватними консультативними фірмами [69]. Завдяки цьому вдалося мінімізувати збитки та не допустити тривалих збоїв у роботі медичних систем. Цей приклад демонструє, що французька модель здатна зберігати системну цілісність навіть у кризових ситуаціях.

Ще одним важливим аспектом є роль стратегічних комунікацій. Франція активно використовує інструменти стратегічної комунікації для формування стійкості суспільства, пояснення ризиків та боротьби з пропагандою. Міністерство закордонних справ регулярно публікує офіційні викриття іноземних інформаційних операцій, що підвищує прозорість та довіру громадян до державної політики. Водночас у Збройних силах створено спеціальні підрозділи, відповідальні за протидію пропаганді, які працюють у тісному зв’язку з інформаційно-аналітичними службами [48]. В умовах зростання міждержавної напруги важливим чинником стає і питання міжнародної співпраці. Франція розуміє, що жодна держава не може ефективно забезпечити інформаційну безпеку самостійно, тому активно розвиває партнерства з країнами ЄС, США, Канадою, а також країнами Індо-Тихоокеанського регіону. Наприклад, у 2023 році було підписано французько-

японську угоду про кіберспівпрацю, спрямовану на обмін даними щодо загроз, проведення спільних навчань та розробку механізмів швидкого реагування. Водночас Франція бере участь у програмі НАТО CCDCOE [18].

Загалом система інформаційної безпеки Франції демонструє значну стійкість, однак перед нею постають і нові виклики, що потребують подальшого вдосконалення. Серед найактуальніших, ризики, пов'язані з квантовими технологіями, які у майбутньому можуть зламати існуючі криптографічні алгоритми; зростання кількості приватних військових і цифрових акторів, які діють у тіні держав; а також конкуренція глобальних платформ, що мають можливість впливати на інформаційні процеси поза межами національних юрисдикцій. У відповідь Франція вже інвестує у квантову криптографію, створює наукові консорціуми для аналізу майбутніх технологій і бере участь у регуляторних ініціативах ЄС.

Висновки до розділу 2

Узагальнюючи результати аналізу, слід підкреслити, що інституційна структура системи інформаційної безпеки Франції демонструє високий рівень комплексності, внутрішньої узгодженості та стратегічної орієнтації на довгострокову стійкість держави в умовах зростаючої турбулентності міжнародного середовища. Вона включає чітко розмежовані, але водночас взаємодоповнювані компетенції ключових органів — зокрема, Національного агентства з безпеки інформаційних систем (ANSSI), Міністерства оборони, Міністерства внутрішніх справ, а також координаційні механізми міжвідомчої співпраці під керівництвом Ради національної оборони та безпеки. Така багаторівнева модель, як показує досвід Франції, дозволяє забезпечити оперативність реагування на кіберінциденти, ефективність стратегічного планування та, що особливо важливо, інтеграцію інформаційної безпеки у ширшу систему національної та європейської оборонної політики.

Не менш значущим компонентом є нормативно-правові засади, що формують політичні, правові та організаційні рамки функціонування всієї

системи. Франція, керуючись вимогами ЄС, зокрема Директивою NIS2, а також власними законодавчими актами, виробила сучасну регуляторну архітектуру, у якій поєднано жорсткі стандарти кіберзахисту, вимоги до критичної інфраструктури, механізми контролю за цифровими платформами та стратегічні положення щодо цифрового суверенітету. Власне, ця правова база забезпечує не лише відповідність міжнародним нормам, але й підвищує спроможність держави протидіяти як зовнішнім, так і внутрішнім загрозам.

Узагальнюючи особливості функціонування системи інформаційної безпеки Франції в умовах сучасних міжнародних відносин, можна стверджувати, що держава демонструє проактивний і водночас адаптивний підхід, заснований на поєднанні технологічних інновацій, політичної консолідації та міжнародної кооперації. Зокрема, Франція активно просуває ідею європейської цифрової автономії, посилює співробітництво з НАТО та ЄС, розвиває партнерства з приватним сектором, що дозволяє їй не лише ефективно реагувати на актуальні виклики, але й формувати порядок денний інформаційної безпеки на глобальному рівні. У підсумку французька модель засвідчує, що системний підхід, інституційна цілісність і нормативна визначеність є критично важливими чинниками забезпечення інформаційної стійкості сучасної держави.

РОЗДІЛ 3. ШЛЯХИ ВДОСКОНАЛЕННЯ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ФРАНЦІЇ В УМОВАХ СУЧАСНИХ МІЖНАРОДНИХ ВИКЛИКІВ

3.1. Цифровий суверенітет Франції як національна стратегія інформаційної безпеки

Французьке бачення інформаційної безпеки нерозривно пов'язане з концептом цифрового суверенітету, який упродовж останніх двох десятиліть перетворився на повноцінну національну стратегію, спрямовану на забезпечення контролю над критичною інфраструктурою, даними, технологіями та комунікаційними ресурсами. В узагальненому вигляді цифровий суверенітет можна визначити як здатність держави самостійно приймати рішення щодо управління цифровою інфраструктурою, технологічними системами та інформаційними потоками, запобігаючи зовнішньому тиску, втручанню чи залежності від іноземних суб'єктів [40]. У випадку Франції цей підхід має, по-перше, виразно політичний, по-друге, стратегічний, а по-третє, безпековий характер, адже він поєднує питання національної оборони, економічної стійкості та захисту демократичних інститутів. Невипадково французькі дослідники, зокрема П. Белланже, А. Робер та інші, наголошують, що цифровий простір стає «новою формою території», яку держава має так само оберігати, як кордони на суші, морі чи в повітрі [49].

З огляду на це, Франція послідовно формує багаторівневу систему цифрового суверенітету, в центрі якої перебуває прагнення зменшити залежність від глобальних технологічних гігантів та забезпечити контроль над ключовими елементами цифрової інфраструктури. Першим важливим кроком стала поява у 2009 році Агентства національної безпеки інформаційних систем (ANSSI), яке отримало повноваження координувати кіберзахист державних органів та стратегічних підприємств, а також розробляти стандарти стійкості та сертифікації цифрових продуктів [8]. Згодом, у 2013 та 2018 роках,

ухвалення оборонних та цифрових стратегій сприяло інституційному закріпленню цифрового суверенітету як однієї з пріоритетних політик, що особливо актуалізувалося після масштабних кібератак на французькі інфраструктури, таких як атака на телеканал TV5Monde у 2015 році чи спроби втручання в президентські вибори 2017 року [37]. У цьому контексті держава розглядає цифровий суверенітет не лише як оборонний механізм, але й як інструмент економічної конкурентоспроможності. Зокрема, Франція активно інвестує у розвиток власної хмарної інфраструктури, створюючи моделі «суверенного хмари» – cloud souverain, які покликані забезпечити локальне зберігання даних та захист від юрисдикцій інших держав, зокрема від американського законодавства щодо доступу до даних (наприклад, CLOUD Act) [71]. У 2021 році уряд оголосив про «Стратегію національного хмарного розвитку», у межах якої підтримуються проєкти OVHcloud, Orange та Atos – компаній, здатних забезпечити технологічну основу для незалежної цифрової інфраструктури [7]. Хоча попередні спроби створення суверенного хмарного сервісу, такі як Cloudwatt і Numergy, завершилися частковим провалом, вони дозволили Франції сформувати досвід і виробити нову модель партнерств, у якій ключова роль відводиться сертифікованим постачальникам, здатним гарантувати відповідність стандартам безпеки ANSSI.

Паралельно із цим Париж посилює регулювання цифрового середовища. На законодавчому рівні цифровий суверенітет реалізується через низку правових актів, серед яких особливе значення мають Loi de Programmation Militaire (LPM) 2019–2025 років, що визначає вимоги до кіберстійкості критично важливих операторів; закон про боротьбу з дезінформацією 2018 року; а також нормативні положення щодо захисту даних та кібергігієни [46]. Франція також активно імплементує загальноєвропейські стандарти, зокрема, регламент GDPR, Директиву NIS2, Акт про кіберстійкість та інші документи, однак при цьому наполягає на необхідності збереження національної автономії в питаннях управління даними [27]. У 2022 році президент Е. Макрон наголосив, що цифровий суверенітет є «ключем для збереження політичної

суб'єктності Франції в XXI столітті», підкресливши важливість розвитку власних напівпровідникових технологій, штучного інтелекту та квантових систем [78].

Водночас цифровий суверенітет у французькій інтерпретації ґрунтується не лише на інфраструктурній автономії, але й на спроможності самостійно захищати цифровий простір у разі загроз. Саме тому Франція сформувала потужний кібероборонний компонент, який охоплює як сили Міністерства збройних сил, так і підрозділи Міністерства внутрішніх справ. У доповіді «Strategie Cyberdefense» 2021 року наголошується, що Франція здатна не лише запобігати атакам, а й здійснювати активні контрдії, включно з офіційно визнаною можливістю проведення кібероперацій у рамках оборони [47]. Цей підхід демонструє зміщення акценту з пасивного захисту до проактивного забезпечення цифрової переваги. Не менш важливо, що цифровий суверенітет охоплює також інформаційно-комунікаційну складову. У сучасних умовах, коли інформаційний простір стає ареною стратегічного суперництва, Франція прагне контролювати шляхи поширення інформації, захищати свою комунікаційну інфраструктуру та протидіяти іноземним впливам. Наприклад, після численних випадків дезінформаційних кампаній з боку Росії, Ірану та Китаю французькі органи влади започаткували спеціальні програми моніторингу та викриття інформаційних маніпуляцій, а також розвивають власні ініціативи стратегічних комунікацій. Одним із ключових інструментів стала платформа Viginum, створена в 2021 році для відстеження та аналізу іноземних інформаційних впливів у цифровому середовищі [79].

Важливо, що французький цифровий суверенітет має також виразний європейський вимір. Париж виступає одним із головних лобістів концепції «європейського суверенітету» в цифровій сфері та активно просуває ініціативи, спрямовані на зменшення залежності ЄС від зовнішніх гравців. Зокрема, Франція підтримує розвиток проєкту GAIA-X – загальноєвропейської цифрової інфраструктури, яка має створити простір довірчих даних та забезпечити захищені умови для обміну інформацією між

бізнесом і державами [15]. Водночас французька позиція також полягає в тому, що ЄС повинен мати можливість протистояти тиску з боку США та Китаю, які домінують у виробництві ключових технологій, включно з процесорами, хмарними сервісами та платформами штучного інтелекту [42]. Однак, незважаючи на амбітність і масштабність поставлених цілей, реалізація цифрового суверенітету стикається з низкою об'єктивних труднощів. По-перше, Франція залишається залежною від імпортних компонентів у сфері мікроелектроніки, а виробництво власних напівпровідників поки що не здатне повністю задовольнити потреби оборонного, енергетичного чи телекомунікаційного секторів [70]. По-друге, французькі технологічні компанії, хоч і демонструють високий рівень розвитку, не можуть конкурувати з глобальними корпораціями у масштабах інвестицій, досліджень та інновацій. По-третє, внутрішня реалізація цифрових стратегій часто наштовхується на бюрократичні бар'єри, фрагментацію компетенцій та різні підходи приватного сектору й держави до питань безпеки.

Разом з тим, попри ці обмеження, Франція демонструє високу стійкість та послідовність у впровадженні принципів цифрового суверенітету [10]. Важливо, що ця концепція еволюціонує від оборонної доктрини до комплексної моделі управління цифровим середовищем, яка охоплює освіту, науку, економіку, інформаційні потоки та міжнародну взаємодію. Усе це дозволяє стверджувати, що цифровий суверенітет Франції функціонує як цілісна стратегія національної інформаційної безпеки, яка поєднує інституційні, технологічні, правові та оборонні компоненти [7]. Більше того, французький підхід до цифрового суверенітету впливає на загальноєвропейські дискусії щодо того, як саме країни ЄС повинні вибудовувати власні цифрові екосистеми, забезпечувати захист даних та формувати стратегічну автономію в умовах глобальної нестабільності [78].

Особливо важливо, що французький цифровий суверенітет має глибоке ідеологічне підґрунтя. Він базується на переконанні, що держава повинна залишатися центральним актором у захисті суспільства від цифрових загроз, а

не передавати контроль приватним корпораціям або іноземним юрисдикціям [49]. Таке розуміння визначає особливий характер французької політики: вона залишається державоцентричною, водночас не відмовляючись від співпраці з бізнесом, наукою та громадськістю. У сфері регуляції цифрових платформ Франція виступає одним із найактивніших ініціаторів посилення вимог до прозорості алгоритмів, боротьби з мікротаргетингом та обмеженням монополістичних практик технологічних гігантів [25]. Цим країна не лише захищає користувачів, але й зміцнює власний суверенітет, не допускаючи домінування іноземних платформ у політичних чи інформаційних процесах. Франція також намагається подолати ключове протиріччя цифрової епохи, між швидкістю глобальних технологічних змін і повільністю демократичних процедур ухвалення рішень. У відповідь на це вона створює гнучкі формати взаємодії, від публічно-приватних платформ до спеціальних інноваційних фондів, які дозволяють швидше впроваджувати нові рішення у сфері кіберзахисту та управління даними. Державна програма «France 2030» передбачає значні інвестиції у квантові технології, штучний інтелект і кібербезпеку, що має на меті зменшити залежність від інших держав у перспективних галузях та посилити стратегічну автономію в довгостроковому вимірі [33; 34].

Безумовно, французький підхід до цифрового суверенітету не позбавлений викликів. Експерти вказують, що надмірне регулювання може уповільнювати інновації, а жорсткі вимоги безпеки, стримувати розвиток малих і середніх технологічних компаній [21]. Проте, як свідчить аналіз національних стратегій, Франція прагне знайти компроміс: не блокувати розвиток цифрової економіки, але й не допускати ситуації, за якої іноземні технології повністю визначатимуть її вектор розвитку. Саме тому політика цифрового суверенітету включає елементи «розумної відкритості», коли співпраця з іноземними партнерами можлива лише за умов збереження контролю над критично важливими ресурсами та дотримання суворих стандартів безпеки [42].

Зрештою французька концепція цифрового суверенітету має особливе стратегічне значення з огляду на роль країни в Європейському Союзі. Франція часто виступає ініціатором загальноєвропейських стратегічних дискусій про те, наскільки ЄС повинен бути самостійним у цифровому просторі, і наполягає, що справжня європейська оборона та безпека неможливі без технологічної автономії [15]. Це особливо проявляється в дискусіях довкола перспектив співпраці з країнами НАТО, використання іноземних хмарних сервісів у межах оборонних структур чи створення єдиної системи управління даними в межах ЄС. У цьому сенсі Франція відіграє роль каталізатора – країни, яка формує бачення майбутньої європейської цифрової стійкості [78]. Продовження розвитку цифрового суверенітету Франції залежатиме від того, наскільки держава зможе зберегти баланс між глобальними технологічними потоками та необхідністю захисту власних стратегічних інтересів. З одного боку, Франція прагне інтегруватися у міжнародні технологічні процеси, адже ізоляція була б згубною для інновацій. З іншого, вона категорично відстоює право на політичну і технологічну автономію. Саме ця подвійність робить французьку модель цікавою для аналізу: вона одночасно прагне незалежності та міжнародного впливу, внутрішньої стійкості та зовнішньої відкритості [40].

У перспективі цифровий суверенітет Франції лише посилюватиметься, адже зростання ролі штучного інтелекту, автоматизованих систем прийняття рішень і високоточного кіберозброєння робитиме цифрову сферу ще вразливішою до маніпуляцій та атак. Саме тому Франція вже сьогодні приділяє особливу увагу етичному регулюванню AI, прозорості алгоритмів та формуванню довірчих середовищ для використання даних. Це дозволить державі не лише захищати свої ресурси, але й задавати стандарти для союзників у Європейському Союзі та за його межами. Усе це свідчить про те, що французький цифровий суверенітет є не просто внутрішньою політикою, а зовнішньополітичним ресурсом, який формує імідж Франції як держав и, здатної протистояти глобальним технологічним викликам. У ширшому контексті стратегічної автономії Франції цифровий суверенітет

перетворюється на фундамент довгострокової моделі розвитку, у якій цифрові інновації, кібербезпека, регулювання та міжнародне співробітництво об’єднані в єдину структуру. Вона гнучко реагує на нові виклики, переосмислює традиційні підходи до безпеки та впроваджує нові методи державного управління у сфері цифрових технологій. Інакше кажучи, цифровий суверенітет стає не лише елементом інформаційної безпеки, але й ключовою передумовою політичного суверенітету XXI століття. Це підтверджує французьку тезу: держава, яка не контролює свої цифрові ресурси, фактично втрачає контроль над власним майбутнім.

3.2. Міжнародне співробітництво Франції у сфері інформаційної безпеки

Франція послідовно формує багаторівневу систему міжнародного співробітництва у сфері інформаційної безпеки, що, по-перше, ґрунтується на її статусі одного з ключових центрів технологічного розвитку Європейського Союзу, а по-друге, відображає прагнення держави забезпечити стабільність цифрового середовища в умовах зростаючих глобальних загроз. У сучасних міжнародних відносинах саме інформаційний простір стає ареною боротьби за політичний вплив, економічні переваги та стратегічну автономію, тому Франція, як держава з розвиненою кіберінфраструктурою й високим рівнем цифровізації, активно залучається до формування глобальних режимів кібербезпеки, укладення двосторонніх і багатосторонніх угод, а також створення спільних інституційних механізмів реагування на кіберінциденти. Водночас, на відміну від багатьох інших європейських держав, вона не обмежується суто оборонними підходами. Париж, виходячи зі стратегічного бачення «цифрового суверенітету» [38], прагне бути і нормотворцем, і модератором, і провайдером інноваційних рішень у сфері інформаційної безпеки.

При цьому міжнародне співробітництво Франції вибудовується за кількома ключовими напрямами. Насамперед, йдеться про участь у структурах

Європейського Союзу та НАТО, адже ці організації не лише встановлюють загальні стандарти безпеки, але й створюють практичні механізми обміну інформацією, кіберрозвідки та координації операцій [18]. Так, у межах ЄС Франція активно взаємодіє з Європейським агентством з кібербезпеки (ENISA), з Європейською службою зовнішніх дій, зокрема з Центром ситуаційної обізнаності й аналізу (EU INTCEN), а також із CSIRTs Network – мережею національних центрів реагування на кіберінциденти [4]. Завдяки цій взаємодії удосконалюється обмін тактичними даними про загрози, зокрема щодо атак на критичну інфраструктуру, фішингових кампаній, спроб дезінформаційного впливу або методів проникнення, пов'язаних з діяльністю хакерських угруповань, таких як APT28 чи APT29. Паралельно з європейськими механізмами, Франція послідовно розвиває співробітництво в межах НАТО. У цьому контексті показовим є її участь у робочих групах і стратегічних ініціативах Альянсу, зокрема NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) в Таллінні, де французькі експерти беруть участь у навчаннях Locked Shields – найбільшому у світі тренуванні з відбиття масштабних кібернападів [18]. Завдяки участі в Альянсі Франція має можливість координувати оборонні й наступальні кіберспроможності, гармонізувати доктринальні підходи та підвищувати стійкість спільного інформаційного простору в умовах ескалації гібридних загроз з боку Росії та інших держав-акторів.

Не менш важливим виміром є двосторонні формати співпраці. Франція має розгалужену мережу партнерств, що віддзеркалюють її глобальні інтереси та технологічний розвиток ключових союзників. Одним із пріоритетних напрямів виступає співробітництво зі Сполученими Штатами Америки, адже саме США, володіючи потужними розвідувальними, технологічними та аналітичними можливостями, вважаються ключовим партнером Франції у боротьбі з кібератаками та шкідливими інформаційними операціями [8]. Зокрема, між Парижем і Вашингтоном існує налагоджений обмін даними між спецслужбами (NSA та DGSE), узгоджуються алгоритми реагування на

інциденти, координуються підходи до протидії дезінформаційним кампаніям, а також розвивається співпраця у сфері захисту виборчої інфраструктури. Особливо важливим цей напрям став після масштабних атак 2017 року на сервери партії Е. Макрона, коли США надали оперативну технічну підтримку французьким фахівцям. Крім США, Франція підтримує активне партнерство з Великою Британією. Незважаючи на Brexit, ця співпраця не лише збереглася, але й отримала новий імпульс завдяки прагматичному фокусуванню на кіберзагрозах як спільному виклику [8]. Французькі структури ANSSI та британський Національний центр кібербезпеки (NCSC) регулярно проводять спільні навчання, обмінюються даними про кіберінциденти, узгоджують технічні стандарти щодо захисту енергетичної та телекомунікаційної інфраструктури.

Так само важливими партнерами залишаються Німеччина та Італія – дві ключові держави ЄС, із якими Франція розвиває синхронізовану політику у сфері цифрової безпеки. З Німеччиною співпраця має стратегічний характер і спирається на спільні проєкти в рамках «франко-німецького цифрового простору», що включає обмін технологічними рішеннями, координацію наукових досліджень та створення єдиного європейського стандарту кіберстійкості [46]. Проєкти GAIA-X, Європейський акт про кіберстійкість (2023) і домовленості щодо побудови єдиного ринку хмарних технологій стали платформою для поглиблення цифрово-інформаційного партнерства між двома державами. Франція активно розвиває співробітництво і з Іспанією. Обидві країни мають спільні виклики, пов’язані з діяльністю транснаціональних хакерських угруповань, гібридними кампаніями Росії в Європі та загрозами критичній енергетичній інфраструктурі [5]. Мадрид і Париж обмінюються даними через національні CERT-платформи, беруть участь у спільних проектах NIS2 та посилюють системи моніторингу щодо загроз, спрямованих на фінансовий сектор.

У ширшому європейському контексті Франція бере участь у діяльності таких інституцій, як Організація економічного співробітництва та розвитку

(ОЕСР), ОБСЄ та Рада Європи, де обговорюються питання етичного використання ШІ, цифрових прав громадян, транскордонного доступу до цифрових доказів, а також вироблення механізмів відповідальності держав за кібератаки [35]. Наприклад, у межах Ради Європи Франція є прихильницею Конвенції про кіберзлочинність (Будапештської конвенції), а також активно підтримує розробку другого додаткового протоколу, що посилює інструменти міжнародного співробітництва з доступу до електронних доказів.

Ще одним стратегічним напрямом є партнерство з Ізраїлем, який вважається одним із світових лідерів у сфері кібербезпеки [8]. Франція цікавиться передовими розробками ізраїльських компаній, а також досвідом держави в питаннях боротьби з високоточними кібератаками, моніторингу кіберзагроз у реальному часі та захисту оборонних систем. Окрему увагу Франція приділяє співпраці з Канадою та Японією. З Канадою партнерство спрямоване на розвиток стандартів захисту даних і спільні дослідження у сфері штучного інтелекту, тоді як із Японією Франція співпрацює в межах «Стратегічного діалогу з питань кібербезпеки», що охоплює питання захисту критичної інфраструктури та забезпечення стійкості глобальних ланцюгів постачання [35].

Варто підкреслити, що міжнародне співробітництво Франції ґрунтується не лише на оборонних механізмах. Значну увагу держава приділяє формуванню глобальної цифрової політики, зокрема через ініціативу «Паризький заклик до довіри та безпеки в кіберпросторі» (Paris Call for Trust and Security in Cyberspace), яка була започаткована у 2018 році та об’єднує понад 80 держав, 350 міжнародних компаній і 150 громадських організацій [35]. Безумовно, співпраця не обмежується виключно демократичними державами. Франція підтримує робочі контакти з Індією, Сінгапуром та Південною Кореєю: трьома азійськими економіками, що мають потужні цифрові індустрії та ефективні моделі захисту кіберпростору [35].

Узагальнюючи динаміку розвитку міжнародного співробітництва Франції в сфері інформаційної безпеки, слід зазначити, що її стратегія

вибудувана на поєднанні жорстких інструментів кібероборони та «м'яких» механізмів дипломатичного й політичного впливу. Така багатокомпонентність дозволяє Франції ефективно реагувати на різні типи загроз, від технічно складних кібератак до інформаційно-психологічних операцій, спрямованих на дестабілізацію суспільства або підрив демократичних процесів. У цьому контексті важливо наголосити, що Франція є однією з небагатьох держав Європи, що мають офіційно сформовану доктрину наступальних кібероперацій, яку вона, утім, реалізує в тісній координації з партнерами [47]. Таким чином, міжнародне співробітництво перетворюється на інструмент зміцнення не лише оборонного, але й стримувального потенціалу Франції у цифровому середовищі [10].

Зокрема, співпраця зі США та Великою Британією дає змогу Франції отримувати доступ до передових аналітичних інструментів та розвідувальних даних, що дозволяє оперативно виявляти нові кіберзагрози [8]. Водночас партнерство з Німеччиною сприяє формуванню єдиного європейського підходу до цифрової безпеки, особливо у напрямі технологічної автономії [46]. Співробітництво з Ізраїлем і Японією, навпаки, має виразну інноваційну спрямованість [8]. Не менш важливим є й середземноморський напрям, у межах якого Франція взаємодіє з Італією, Іспанією та Грецією. Ці держави зазнають підвищеного тиску через активність різноманітних кіберугруповань і діяльність злочинних мереж, що використовують цифровий простір для торгівлі зброєю, наркотиками та персональними даними [14]. Франція та Італія в рамках спільних тренувань SIMOS запропонували моделі реагування на атаки на морські об'єкти інфраструктури, а Іспанія та Франція спільно відпрацьовують алгоритми протидії фішинговим кампаніям, спрямованим на державні установи.

Загалом міжнародна діяльність Франції у сфері інформаційної безпеки базується також на розвитку глобальних цифрових норм. Однією з ключових її амбіцій є формування універсальних правил поведінки держав у кіберпросторі [10]. Париж активно лобіює ініціативи з підвищення прозорості використання

кіберзасобів, відповідального застосування штучного інтелекту та захисту цифрових прав громадян. Такі зусилля реалізуються, серед іншого, у межах ООН та ЄС. Саме Франція ініціювала рекомендації щодо створення глобальних принципів кіберетики, покликаних забезпечити безпечний розвиток інформаційних технологій і мінімізувати ризики їхнього використання для воєнних чи терористичних цілей [45].

Специфічним напрямом є взаємодія з країнами Глобального Півдня, де Франція прагне зміцнювати свій вплив та формувати партнерства у стратегічно важливих регіонах. У цьому контексті особливо показовими є відносини з Марокко, Сенегалом, Кот-д'Івуаром та Тунісом [35]. Париж реалізує програми підвищення цифрової грамотності, модернізації систем кіберзахисту, розвитку національних CERT-центрів та навчання кадрів для кібербезпеки. У співпраці з Тунісом Франція підтримує проєкти з побудови сучасних телекомунікаційних мереж, а з Марокко – ініціативи щодо захисту банківської інфраструктури від фінансових кіберзагроз. Натомість співробітництво з Сенегалом і Кот-д'Івуаром орієнтоване на розвиток цифрових сервісів у державному управлінні, що підвищує їхню стійкість перед інформаційними маніпуляціями. Важливо й те, що Франція усвідомлює необхідність міжнародної координації в питаннях боротьби з дезінформацією. Париж активно підтримує програми, спрямовані на протидію російським інформаційним операціям, особливо в країнах Східної Європи та Північної Африки. У межах ЄС Франція є одним з ініціаторів посилення діяльності EUvsDisinfo та створення нових платформ швидкого реагування на інформаційні атаки, що дозволяють державам-членам обмінюватися даними про кампанії впливу в режимі реального часу [68].

Що стосується співпраці з Україною, Франція відіграє значну роль у зміцненні кіберстійкості української держави в умовах триваючої російської агресії. Париж надає технічну допомогу українським органам влади у сфері кіберзахисту, бере участь у тренінгах для фахівців Держспецзв'язку та розвиває спільні аналітичні програми з виявлення російських інформаційно-психологічних операцій [9]. Крім того, Франція підтримує українську участь у

європейських ініціативах цифрової трансформації, що розширює доступ українських інституцій до європейських технологічних ресурсів.

Поєднання всіх цих напрямів дозволяє Франції формувати гнучку та адаптивну систему міжнародної взаємодії у сфері інформаційної безпеки. Завдяки цьому вона зміцнює власні можливості, сприяє створенню безпечного цифрового простору в Європі та світі, а також забезпечує стратегічні позиції в умовах глобальної кіберконкуренції. У підсумку можна ксазначити, що міжнародне співробітництво стало одним із ключових елементів французької моделі інформаційної безпеки, що дозволяє ефективно поєднувати технологічний потенціал, політичний вплив та інституційну координацію задля протидії сучасним інформаційним та кіберзагрозам.

3.3. Досвід Франції для України в удосконаленні державної політики інформаційної безпеки в умовах сучасних міжнародних викликів

У сучасному глобальному середовищі, де інформація дедалі частіше використовується як інструмент політичного, економічного й військово-стратегічного впливу, стає очевидним, що держави вимушені шукати нові моделі забезпечення національної інформаційної безпеки, здатні ефективно відповідати на складні, багатовимірні та швидкоплинні загрози. Саме досвід Франції, яка вважається одним із провідних європейських лідерів у сфері кіберзахисту, цифрового суверенітету та стратегічних інформаційних комунікацій, має вагоме значення для України. Він демонструє, з одного боку, ефективні інституційні та нормативні рішення, а з іншого – гнучкі механізми адаптації до нових викликів. Відтак, аналіз французької моделі та її потенційної імплементації в Україні створює основу для формування дієвих рекомендацій, спрямованих на вдосконалення національної політики у сфері інформаційної безпеки. Загалом французький підхід ґрунтується на концепції цифрового суверенітету як ключового елементу державної безпеки [7]. Цей термін, який активно використовується у французьких офіційних документах і стратегіях, передбачає спроможність держави самостійно визначати правила

функціонування цифрового простору, забезпечувати захист критичної інформаційної інфраструктури та контролювати доступ до стратегічно важливих даних [38]. У Стратегії національної безпеки Франції 2021 року підкреслюється, що «панування у цифровій сфері є обов'язковою умовою суверенітету держави» [12]. Україна, яка переживає безпрецедентний тиск у сфері інформаційної безпеки, від масштабних кібератак до системних інформаційно-психологічних операцій, також потребує формування цілісної концепції цифрового суверенітету. Зіставляючи досвід Франції з українською ситуацією, слід зазначити, що наша держава вже здійснила фундаментальні кроки у цьому напрямі (зокрема, ухвалення Стратегії кібербезпеки України 2021 року та активний розвиток інституційного середовища), проте інтеграція французького досвіду могла б суттєво пришвидшити формування дієвої системи стійкості.

Не менш важливим компонентом є інституційна організація системи інформаційної безпеки у Франції. Центральну роль відіграє Агентство з національної безпеки інформаційних систем (ANSSI), створене у 2009 році та структуроване як координаційний центр державної політики у сфері кіберзахисту [8]. ANSSI відповідає за моніторинг кіберзагроз, здійснення аудиту безпеки державних і приватних структур, реагування на інциденти, сертифікацію обладнання, а також забезпечення стратегічної комунікації у кризових ситуаціях [13]. Для України надзвичайно цінним може стати саме принцип централізації, властивий французькій моделі, адже нинішня українська система складається з низки інституцій: Державної служби спеціального зв'язку та захисту інформації, Міністерства цифрової трансформації, СБУ, РНБО, Національного координаційного центру кібербезпеки, але між ними нерідко бракує чіткої розподіленості функцій і формалізованої взаємодії [10]. Водночас французька практика інституційної взаємодії пропонує Україні цікаві моделі партнерства між державою та приватним сектором. Франція активно впроваджує програми державно-приватного співробітництва, серед яких особливу роль відіграє система

сертифікації провайдерів безпеки, а також регулярні спільні навчання з кіберзахисту [16]. Наприклад, ініціатива «Cybermalveillance.gouv.fr» створює платформу для взаємодії громадян, бізнесу та держави щодо реагування на інциденти. Україні варто перейняти принцип багаторівневої комунікації з недержавними суб'єктами, адже саме приватні компанії володіють значною частиною критичної інфраструктури та мають високі технологічні спроможності.

У сфері нормативно-правового забезпечення Франція сповідує принцип превентивності, що особливо проявляється у регулюванні захисту критичної інформаційної інфраструктури. Зокрема, французьке законодавство передбачає обов'язкові вимоги до кіберзахисту для операторів важливих послуг, а також значні санкції у разі недотримання цих вимог [46]. В Україні подібні норми лише формуються, і впровадження строгих стандартів, на приклад французьких, змогло б підвищити рівень системної стійкості. Крім того, Франція активно імплементує норми ЄС, такі як директива NIS2 [27], яка підвищує вимоги до безпеки цифрових послуг і критичних секторів. Суттєве місце у французькій моделі займає боротьба з дезінформацією, яка розглядається не лише як безпековий виклик, а як загроза демократичній стабільності. Франція однією з перших у Європі ухвалила спеціальний закон проти маніпуляцій інформацією під час виборчих кампаній (2018 р.), який передбачає механізми оперативного блокування фейкових новин, прозорість фінансування політичної реклами та розширення повноважень медіарегулятора [10]. Україна, яка потерпає від системних інформаційно-психологічних операцій з боку РФ, могла б використати французький досвід для створення спеціалізованих процедур протидії дезінформаційним загрозам, особливо під час виборів або кризових подій.

Окремої уваги заслуговує французький досвід побудови системи стратегічних комунікацій. Після активізації гібридних загроз у 2014–2015 роках французький уряд створив комплексний механізм комунікаційного реагування, що включає як оперативний аналіз загроз, так і координацію

повідомлень між різними міністерствами [11]. Наприклад, французьке Міністерство збройних сил має спеціальний підрозділ — DICoD (Délégation à l'information et à la communication de la Défense), який відповідає за формування наративів, інформаційне супроводження військових операцій та протидію маніпуляціям [48]. Зрештою, французький досвід підсилюється активною міжнародною взаємодією, зокрема в межах ЄС, НАТО, ООН, а також двосторонніх партнерств у сфері кібербезпеки [9]. Україна, яка уже поглибила співпрацю з НАТО у сфері кібербезпеки та бере участь у програмах ЄС, могла б і надалі переймати досвід Франції в побудові мережі міжнародної солідарності щодо протидії гібридним загрозам.

Варто також зазначити, що Франція активно розвиває власний технологічний сектор, зокрема у галузях штучного інтелекту, криптографії та розробки національного програмного забезпечення [33]. У 2020-х роках країна започаткувала низку державних інвестиційних програм, спрямованих на створення конкурентоспроможних цифрових рішень, які могли б замінити залежність від іноземних технологій, особливо американських і китайських [34]. Разом з тим, упровадження французьких підходів слід адаптувати до українських реалій, що включають як особливості правового поля, так і умови воєнного часу. Україна має свої унікальні переваги, як-от досвід відбиття гібридних атак, високий рівень цифровізації державних послуг, а також тісну взаємодію з міжнародними партнерами. Тому імплементація французьких моделей має враховувати наявний потенціал і спрямовуватися передусім на усунення прогалин: інституційних, комунікаційних, нормативних [5]. Отже, французький досвід у сфері інформаційної безпеки може бути надзвичайно корисним для України в умовах сучасних міжнародних викликів. Він охоплює широкий спектр елементів, від концептуальних підходів до цифрового суверенітету та інституційної реформи до практичних рішень у боротьбі з дезінформацією, зміцнення кіберзахисту та розвитку стратегічних комунікацій [7]. За умови адаптації та інтеграції цих елементів у національну політику Україна матиме шанс значно підвищити свою стійкість до гібридних загроз,

зміцнити стратегічні позиції у міжнародному середовищі та забезпечити надійний фундамент для розвитку безпечної цифрової держави.

Важливо усвідомлювати, що застосування французького досвіду не є механічним копіюванням інституційних моделей чи правових норм. Навпаки, йдеться про формування гнучкої, адаптивної та цілісної системи, що поєднує найкращі практики європейських держав із власними напрацюваннями України [8]. Саме тому, аналізуючи французьку модель, слід звернути увагу на низку додаткових аспектів, які можуть посилити національну політику у сфері інформаційної безпеки.

Перш за все, слід виділити роль освіти та підготовки фахівців. Франція створила багаторівневу систему професійної освіти у сфері кібербезпеки, що включає спеціалізовані університетські програми, підготовку експертів у військових академіях та незалежні курси, спрямовані на розвиток цифрової грамотності населення. Крім того, ANSSI реалізує програми сертифікації фахівців, забезпечуючи стандартизацію кваліфікацій і формування професійних компетенцій на національному рівні [60]. Україна, яка зіштовхується з браком експертів, змогла б адаптувати цей підхід, створивши централізовану систему підготовки спеціалістів, включно з інтеграцією програм кібербезпеки до навчальних планів провідних університетів, а також створенням лабораторій цифрової безпеки для студентів.

Одним із ключових аспектів, який варто перейняти, є концепція стійкості суспільства. Франція приділяє значну увагу підвищенню рівня обізнаності громадян щодо інформаційних загроз. Протягом останніх років французький уряд проводить національні кампанії протидії фейкам, спрямовані на виявлення та спростування маніпулятивного контенту, а також підвищення медіаграмотності [32]. В Україні необхідно посилити подібні ініціативи, адже тривала агресія РФ супроводжується широкомасштабними спробами формування деструктивних наративів. У сфері технологічного забезпечення французький досвід також виглядає надзвичайно актуальним. Франція активно інвестує у створення національних дата-центрів, розвиток хмарних

технологій, шифрування та захист державних реєстрів. Одним із ключових напрямів є мінімізація залежності від іноземних IT-компаній, що відповідає логіці цифрового суверенітету [38]. Україна, яка використовує низку зовнішніх технологічних рішень у сфері безпеки, може проаналізувати французький досвід для розбудови власних, більш автономних цифрових платформ. У контексті протидії гібридним загрозам одним із найефективніших рішень Франції стало створення спеціалізованих центрів аналізу інформаційних операцій. У 2017 році французьке Міністерство оборони заснувало Центр кібероперацій (COMCYBER), який займається координацією оборонних кібердій та аналізом інформаційних атак [20]. Також активно працює Центр протидії іноземним впливам (Viginum), що виконує функції моніторингу, верифікації та аналізу дезінформаційних кампаній [79]. Для України створення подібного багатофункціонального центру могло б значно підвищити ефективність національної системи реагування.

Не менш важливою є взаємодія Франції з Європейським Союзом. Франція виступає одним із ініціаторів поглиблення співпраці між державами-членами щодо кіберстійкості, зокрема в межах Європейського центру з кібербезпеки та координаційних механізмів ЄС [27]. Україна, яка прагне інтегруватися у європейську інфраструктуру цифрової безпеки, може використати досвід Франції для посилення співпраці з відповідними європейськими інституціями [9]. Впровадження французького досвіду також передбачає розвиток системи національного стратегічного прогнозування, що є одним із найсильніших елементів французької моделі. Завдяки системі регулярного стратегічного планування, зокрема «Білому документу з оборони та національної безпеки» та Національній стратегічній ревю, Франція прогнозує тенденції розвитку загроз на найближчі десятиліття [52]. Україна, зважаючи на тривалість військової агресії та постійне зростання цифрових ризиків, може застосувати аналогічні підходи шляхом формування інституції довгострокового планування в секторі інформаційної безпеки [6].

Ще один важливий напрям – це вдосконалення кризової комунікації. Франція розробила комплексний механізм взаємодії між державними органами у період інформаційних загроз або надзвичайних ситуацій [77]. Система передбачає оперативність, чіткість і централізованість повідомлень, що дозволяє запобігти хаосу та зменшити можливості для розповсюдження дезінформації. Важливим також є французький досвід створення системи раннього попередження про кіберінциденти. У Франції провідні державні установи та оператори важливих послуг зобов'язані негайно повідомляти про будь-які кібератаки ANSSI, що дозволяє централізовано оцінити масштаби загрози та координувати заходи реагування [27]. Для України впровадження аналогічної практики могло б значно підвищити рівень оперативності реагування.

Таким чином, досвід Франції відкриває широкі перспективи для вдосконалення державної політики інформаційної безпеки України. Він демонструє комплексний підхід, що поєднує нормативну визначеність, інституційну координацію, технічну модернізацію та розвиток суспільної стійкості. Україна може адаптувати ці підходи з урахуванням власних потреб, що дозволить створити ефективну модель протидії сучасним інформаційним викликам та забезпечити стабільність у цифровому середовищі. Зрештою, саме синтез національного досвіду та найкращих світових практик забезпечить країні стійкість перед обличчям інформаційної експансії та стане основою для зміцнення національного суверенітету у XXI ст..

Висновки до розділу 3

Узагальнюючи результати проведеного дослідження, слід наголосити, що цифровий суверенітет Франції поступово перетворюється на одну з ключових засад її національної стратегії забезпечення інформаційної безпеки, оскільки саме він створює фундамент для формування стійкої цифрової інфраструктури, здатної протистояти як зовнішнім, так і внутрішнім загрозам. Власне, інтеграція принципів контролю над критичними технологіями,

розвитку національних ІТ-компаній, підтримки інновацій та зменшення залежності від іноземних цифрових платформ демонструє прагнення Франції до стратегічної автономії в інформаційному просторі. Більше того, це дає можливість центральній владі гарантувати безперервність функціонування державних сервісів у разі кіберінцидентів, а також зміцнювати захист персональних даних громадян відповідно до вимог європейського регулювання.

У цьому контексті, між іншим, зростає значення міжнародного співробітництва Франції, яке ґрунтується на поєднанні багатосторонніх та двосторонніх форматів взаємодії. Як відомо, країна активно бере участь у діяльності ЄС, НАТО, ООН, а також ініціює партнерства з провідними державами у сфері обміну кіберекспертизою, координації дій щодо протидії кіберзлочинності та вироблення спільних технологічних стандартів. Підтримка Францією міжнародних норм відповідальної поведінки держав у кіберпросторі підсилює глобальну архітектуру інформаційної безпеки й сприяє формуванню передбачуваного середовища, що особливо важливо в умовах конкуренції провідних держав за вплив у цифровій сфері.

Водночас досвід Франції є надзвичайно корисним для України, адже він демонструє, яким чином можна поєднати стратегічне бачення цифрового розвитку з дієвою інституційною системою кіберзахисту. Для України особливо актуальними є підходи до регулювання цифрового простору, розвиток національних технологічних потужностей, створення центрів реагування на кіберзагрози, а також розбудова партнерств з європейськими структурами. Отже, адаптація французьких напрацювань може суттєво посилити українську модель інформаційної безпеки, зробивши її більш стійкою, гнучкою та здатною ефективно реагувати на сучасні міжнародні виклики.

ВИСНОВКИ

У результаті дослідження особливостей забезпечення інформаційної безпеки Франції в умовах сучасних міжнародних викликів, зроблено наступні висновки:

1. Визначено, що поняття інформаційної безпеки у міжнародних відносинах охоплює комплекс заходів, спрямованих на захист інформаційного суверенітету держави, стабільність її політичної системи, стійкість комунікаційної інфраструктури та формування стійких механізмів протидії гібридним загрозам. Як показало дослідження, інформаційна безпека є багатовимірним феноменом: вона включає технічний, правовий, інституційний, дипломатичний та когнітивний рівні, які у взаємодії забезпечують захист держави від дезінформації, кібератак, інформаційних маніпуляцій та зовнішнього втручання. Її ключовими структурними елементами, відповідно, виступають система стратегічного планування, сучасні засоби кіберзахисту, ефективні комунікаційні інструменти держави, а також нормативно-правові механізми, що гарантують відповідальність за порушення інформаційної безпеки. Принципи її забезпечення, зокрема превентивність, комплексність, міжвідомча координація, міжнародна співпраця та пріоритет національного суверенітету, формують концептуальну основу для державної політики у цій сфері.

2. У свою чергу, аналіз міжнародних викликів показує, що сучасне інформаційне середовище є надзвичайно динамічним і конфліктогенним. Гібридні загрози, кібершпигунство, маніпулятивні інформаційні кампанії, використання штучного інтелекту у дезінформаційних операціях, транснаціональна діяльність хакерських угруповань – усе це суттєво трансформує підходи держав до формування інформаційної політики. Зокрема, держави вимушені покладатися на багаторівневі системи захисту, посилювати міжнародну комунікацію, розвивати кібердипломатію, а також активно співпрацювати з приватним сектором. Як наслідок, інформаційна безпека еволюціонує від суто технічної сфери до комплексного політико-

правового інституту, що охоплює регулювання діяльності цифрових платформ, забезпечення прозорості онлайн-контенту та запобігання зовнішньому втручанню у демократичні процеси.

3. Зазначимо, що модель інформаційної безпеки Франції демонструє високий рівень інституціоналізації та комплексності, що дозволяє розглядати її як показовий зразок сучасної державної політики у відповідній сфері. Її інституційна структура спирається на широкий спектр спеціалізованих органів. Центральне місце займає Національне агентство з безпеки інформаційних систем (ANSSI), що відповідає за кіберзахист, аудит критичної інфраструктури, реагування на кіберінциденти та формування стандартів безпечної цифрової взаємодії. Важливу роль також відіграють Міністерство оборони, Міністерство внутрішніх справ, Генеральний секретаріат з оборони та національної безпеки (SGDSN), а також дипломатичні структури, що забезпечують зовнішній вимір інформаційної політики. Нормативно-правові засади цієї моделі закріплені у Стратегії національної безпеки, Законі про військове програмування, Національній стратегії кібербезпеки та у численних підзаконних актах, які визначають стандарти стійкості цифрової інфраструктури, відповідальність операторів критичної інфраструктури, а також вимоги до захисту персональних даних (зокрема в межах GDPR). Важливим елементом є концепція цифрового суверенітету, яка передбачає захист національного інформаційного простору, підтримку розвитку власних технологій і контроль над стратегічними комунікаційними ресурсами.

4. Особливості реалізації французької моделі проявляються у її системності, стратегічній гнучкості та здатності адаптуватися до нових викликів. По-перше, Франція активно розвиває національні технічні рішення та інвестує в кіберіндустрію, що підсилює її позиції як одного з лідерів у сфері європейської кібербезпеки. По-друге, країна розробляє механізми швидкого реагування на інформаційні інциденти, що дозволяє ефективно протидіяти спробам дестабілізації. По-третє, французька політика передбачає чітке розмежування відповідальності між державою, приватним сектором та

громадянським суспільством, що дає змогу забезпечити комплексність і прозорість заходів безпеки. Нарешті, Франція активно використовує інформаційну дипломатію, включаючи взаємодію в межах ЄС, НАТО, ООН та двосторонніх партнерств.

5. Аналіз можливостей застосування французького досвіду в Україні засвідчив його високу актуальність та практичну цінність. Україна, яка вже тривалий час перебуває під тиском гібридної агресії, потребує системного зміцнення своїх інформаційних інституцій. Зокрема, доцільним виглядає створення єдиного координаційного центру, аналогічного французькому SGDSN, який би забезпечував міжвідомчу узгодженість рішень. Також важливо посилити роль незалежного аудиту кіберзахисту, розширити нормативно-правову базу щодо відповідальності цифрових платформ і операторів критичної інфраструктури, а також активізувати міжнародну цифрову дипломатію. У цьому контексті корисним може бути й досвід Франції у сфері підвищення стійкості суспільства до дезінформації, передусім через розвиток медіаграмотності, державних комунікацій та співпраці з громадськими ініціативами.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Гончаров М.В. Дослідження поняття «інформаційна безпека». *Науковий вісник Ужгородського національного університету. Серія: Право*. 2024. Вип. 82. ч. 1. С. 34-37. URL: https://doi.org/10.24144/2307-3322.2024.82.1.4 (дата звернення: 6.10.2025)

2. Горун О.Ю. Зарубіжний досвід правового забезпечення та особливостей створення кібервійськ на прикладі деяких держав НАТО. *Науковий вісник Міжнародного гуманітарного університету. Серія: Юриспруденція.* 2023. № 64. DOI: https://doi.org/10.32841/2307-1745.2023.64.7

3. Дрига Д. Аналіз правових механізмів забезпечення інформаційної безпеки інформаційної інфраструктури Європейського Союзу. *Herald of Khmelnytskyi National University. Economic Sciences*. 2024. № 334(5). С. 46–51. DOI: https://doi.org/10.31891/2307-5740-2024-334-7

4. Кавин С.Я. Правові засади забезпечення кібербезпеки в державах – членах Європейського Союзу. *Актуальні проблеми держави і права*. 2020. Вип. 51. С. 51-58. URL: https://doi.org/10.32837/apdp.v0i87.2797 (дата звернення: 6.10.2025)

5. Карпенко О. Європейський досвід протидії гібридним загрозам: уроки для України. Інвестиції: практика та досвід. 2024. № 41. 70–76. URL: https://iepjournal.com/journals/41/2024_41_12_Karpenko.pdf (дата звернення: 6.10.2025)

6. Національний інститут стратегічних досліджень (НІСД). Порівняльний аналіз підходів до стратегічного планування у сфері оборони у Франції. *Аналітичні записки НІСД.* 09.04.2025. URL: https://niss.gov.ua/doslidzhennya/natsionalna-bezpeka/porivnyalnyy-analiz-pidkhodiv-do-stratehichnoho-planuvannya-u (дата звернення: 6.10.2025)

7. Санжарова Г. Ф., Бак, В. І., Санжаров, В. А. France’s «Digital Sovereignty» and the Legal Basis of the National Cybersecurity Strategy. *Юридичний науковий електронний журнал*. 2025 (5). P. 42-45. ISSN 2524-0374

8. Слободян О. В. Cyber security in France: policy framework and institutional development. *Вісник Національної академії внутрішніх справ*. 2023. Т. 126. № 3. С. 145–153. URL: https://elar.navs.edu.ua/bitstreams/9a748b92-6e13-4f20-b94f-67c0e8a968a7/download (дата звернення: 6.10.2025)

9. Франція та Україна об'єдналися для посилення потенціалу кібербезпеки (проект «Розбудова потенціалу кібербезпеки для України» (CCBU) в межах Талліннського механізму). *Європейський Союз.* 11 лютого 2025 р. URL: https://eufordigital.eu/uk/france-and-ukraine-unite-to-enhance-cybersecurity-capacity/ (дата звернення: 6.10.2025)

10. Фурсай О. В. Політика інформаційної безпеки Французької Республіки в умовах міжнародно-політичних трансформацій: дис. … д-ра філософії: 291 Міжнародні відносини, суспільні комунікації та регіональні студії. Київ, 2024. 225 с.

11. Фурсай О. Система забезпечення інформаційної безпеки Франції. *Вісник Львівського університету. Серія філософсько-політологічні студії.* 2021. Випуск 34. С. 222–227. DOI: https://doi.org/10.30970/PPS.2021.34.29

12. Actualisation stratégique 2021. *Ministère des Armées.* Paris, 2021. 55 p. URL: https://www.defense.gouv.fr/sites/default/files/dgris/REVUE%20STRAT%202021%2004%2002%202021%20FR.pdf (Last accessed: 6.10.2025)

13. Annual Review 2021. *Agence nationale de la sécurité des systèmes d'information.* Paris, 2022. URL: https://cyber.gouv.fr/en/en/annual-review-2021 (Last accessed: 6.10.2025)

14. Beretas C. P. The Most Important Types of Cyber Attacks that France is Expected to Face in the Future and the Cyber Security Measures it Must Implement to Protect Critical. *Universal Library of Engineering Technology*. 2024. URL: https://www.ulopenaccess.com/ulpages/fulltextULETE?ArticleID=ULETE20230101001 (Last accessed: 6.10.2025)

15. Bertrand B. Le droit au service de la souveraineté numérique de l'UE. Annales des Mines. *Série « Enjeux numériques ».* 2023. № 23. С. 122–126. URL: https://www.cairn.info/revue-enjeux-numeriques-2023-1-page-122.htm (Last accessed: 6.10.2025)

16. Calcara A., Marchetti R. State-industry relations and cybersecurity governance in Europe. *Review of International Political Economy*. 2022. Vol. 29, Issue 4. P. 1237–1262. DOI: https://doi.org/10.1080/09692290.2021.1918743

17. Cristiano F., Broeders D., Delerue F., Douzet F., Géry A. Artificial intelligence and international conflict in cyberspace. 2023. 279 p. URL: https://library.oapen.org/bitstream/handle/20.500.12657/62917/1/9781000895896.pdf (Last accessed: 6.10.2025)

18. Cyber defence. NATO Official Topic Page. *NATO.* 30.07.2024. URL: https://www.nato.int/en/what-we-do/deterrence-and-defence/cyber-defence

19. Cyber threat overview 2021. *Agence nationale de la sécurité des systèmes d'information.* Paris, 2025. URL: https://cyber.gouv.fr/en/publications/cyber-threat-overview-2021 (Last accessed: 6.10.2025)

20. Cyberdéfense. Champs confrontationnels. *Ministère des Armées.* 2022. URL: https://www.defense.gouv.fr/dgris/approches-thematiques/champs-confrontationnels/cyberdefense (Last accessed: 6.10.2025)

21. Cybersécurité, passons à l'échelle. *Institut Montaigne.* Paris, 2023. URL: https://www.institutmontaigne.org/publications/cybersecurite-passons-lechelle (Last accessed: 6.10.2025)

22. Cybersecurity in France: laws, trends and challenges. *NegativePID.* 2025. URL: https://negativepid.com/en/cybersecurity-in-france (Last accessed: 6.10.2025)

23. Cybersecurity: the threat level remains high. *IHEDN.* IHEDN Analyses. 2023. URL: https://ihedn.fr/en/notre-selection/cybersecurite-le-niveau-de-menace-demeure-eleve (Last accessed: 6.10.2025)

24. Darwish A., Romaniuk S. N. Cyber security in the French Republic. *Companion to global cyber-security.* 2021. 11 p. URL: https://www.taylorfrancis.com/chapters/edit/10.4324/9780429399718-7/cyber-security-french-republic-amber-darwish-scott-romaniuk (Last accessed: 6.10.2025)

25. De Gregorio G. The rise of digital constitutionalism in the European Union. *International Journal of Constitutional Law. 2021*. Vol. 19. № 1. P. 41–70. URL: https://academic.oup.com/icon/article/19/1/41/6279890 (Last accessed: 6.10.2025)

26. De Spiegeleire S., Maas M., Sweijs T. Human Rights in the Digital Age. Santa Monica, CA: RAND Corporation, 2021. URL: https://www.rand.org/pubs/research_reports/RR3163.html (Last accessed: 6.10.2025)

27. Directive (EU) 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2). *European Union. Official Journal of the EU.* 27.12.2022. URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng (Last accessed: 6.10.2025)

28. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive). *Official Journal of the European Union. European Parliament; Council of the European Union.* 27.12.2022. L 333. P. 80–152. URL: http://data.europa.eu/eli/dir/2022/2555/oj (Last accessed: 6.10.2025)

29. Enhancing the Digital Security of Critical Activities and Infrastructures. *OECD.* Paris, 2021. URL: https://www.oecd.org/digital/enhancing-the-digital-security-of-critical-activities.htm (Last accessed: 6.10.2025)

30. Etat de la menace informatique sur le secteur des transports urbains. *Agence nationale de la sécurité des systèmes d'information.* Paris: ANSSI, 2025. URL: https://cyber.gouv.fr/actualites/etat-de-la-menace-informatique-sur-le-secteur-des-transports-urbains (Last accessed: 6.10.2025)

31. Face à l'ingérence numérique étrangère, une réponse désormais opérationnelle mais deux stratégies à formaliser. *Revue Défense Nationale*. 2025. n°

884 (hors-série). URL: https://www.defnat.com/e-RDN/vue-article-cahier.php?carticle=1659&cidcahier=1367 (Last accessed: 6.10.2025)

32. Facts not Fakes: Tackling Mis- and Disinformation. *OECD.* Paris, 2024. URL: https://www.oecd.org/governance/facts-not-fakes.htm (Last accessed: 6.10.2025)

33. France 2030 : stratégie d'accélération cybersécurité. *Direction générale des Entreprises.* 19.11.2024. URL: https://www.entreprises.gouv.fr/priorites-et-actions/autonomie-strategique/soutenir-linnovation-dans-les-secteurs-strategiques-16 (Last accessed: 6.10.2025)

34. France 2030: la stratégie nationale pour la cybersécurité s'accélère (synthèse). *Gouvernement de la République française.* Paris, 2024. URL: https://www.info.gouv.fr/upload/media/content/0001/11/ea43598f5e8ae2a46c22b9f806cdec1904832b5c.pdf (Last accessed: 6.10.2025)

35. France's international action to fight cyber crime (9 January 2025). *Ministry for Europe and Foreign Affairs.* 09.01.2025. URL: https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/news/article/france-s-international-action-to-fight-cyber-crime-9-jan-2025 (Last accessed: 6.10.2025)

36. Galinec D. Cyber security and cyber defense: Challenges and building of cyber resilience conceptual model. International Journal of Applied Sciences &. 2023. URL: https://www.wseas.com/journals/asd/2022/a20asd-010(2022).pdf (Last accessed: 6.10.2025)

37. Germain E. Cyber security seen through the prism of ANSSI. *Revue Défense Nationale.* 2021. 2021/2. № 837. C. 84–88. DOI: https://doi.org/10.3917/rdna.837.0084. URL: https://shs.cairn.info/journal-revue-defense-nationale-2021-2-page-84?lang=en (Last accessed: 6.10.2025)

38. Watin-Augouard M. La souveraineté numérique à l'épreuve de la métamorphose numérique. *Revue Défense Nationale.* 2022. 2022/10. № 855. C. 7–13. DOI: https://doi.org/10.3917/rdna.855.0007. URL: https://shs.cairn.info/revue-defense-nationale-2022-10-page-7?lang=fr (Last accessed: 6.10.2025)

39. Sirvent T. Cryptography – the basis/foundation of digital sovereignty. *Revue Défense Nationale*. 2022. 2022/10. № 855. C. 59–66. URL: https://shs.cairn.info/journal-revue-defense-nationale-2022-10-page-59?lang=en shs.cairn.info+1

40. Glasze G. Contested Spatialities of Digital Sovereignty. *Geopolitics.* 2023. URL: https://www.tandfonline.com/doi/full/10.1080/14650045.2023.2195129 (Last accessed: 6.10.2025)

41. Guide pratique RGPD – Sécurité des données personnelles (édition 2024). *Commission nationale de l'informatique et des libertés (CNIL).* Paris, 2024. URL: https://www.cnil.fr/sites/cnil/files/2024-03/cnil_guide_securite_personnelle_2024.pdf (Last accessed: 6.10.2025)

42. Heidebrecht S. From market liberalism to public intervention: digital sovereignty and changing European Union digital single market governance. *Journal of Common Market Studies. 2024.* Vol. 62. № 1. P. 205–223. URL: https://onlinelibrary.wiley.com/doi/10.1111/jcms.13530 (Last accessed: 6.10.2025)

43. Iliopoulou-Penot A. La Constitution numérique européenne. *Revue française de droit administratif.* 2023. № 5. P. 945–959. URL: https://www.lexisnexis.fr (Last accessed: 6.10.2025)

44. Jacuch A. Comparative analysis of cybersecurity strategies. European Union strategy and policies. P*olish and selected countries strategies. Online journal modelling the new Europe.* 2021. URL: https://www.ceeol.com/search/article-detail?id=1010016 (Last accessed: 6.10.2025)

45. Johnstone I., Sukumar A., Trachtman J. Building an International Cybersecurity Regime: Multistakeholder Diplomacy. books.google.com. 2023. URL: https://books.google.com/books?hl=en&lr=&id=XQXXEAAAQBAJ&oi=fnd&pg=PR7&dq=France+cybersecurity+international+challenges&ots=-Z-giIcMQL&sig=p6B5r17UMZhTiFLkeAkuBio7OpA (Last accessed: 6.10.2025)

46. Kavyn S., Bratsuk I., Lytvynenko A. Regulatory and legal enforcement of cyber security in countries of the European Union: The experience of Germany and France. Teisė. 2021. URL: https://www.zurnalai.vu.lt/teise/article/download/25171/24464 (Last accessed: 6.10.2025)

47. Laudrain A. France's new offensive cyber doctrine. Lawfare. 2023. URL: https://www.lawfaremedia.org/article/frances-new-offensive-cyber-doctrine (Last accessed: 6.10.2025)

48. Les armées se dotent d'une doctrine militaire de lutte informatique d'influence (L2I). *Ministère des Armées.* 22.10.2021. URL: https://www.defense.gouv.fr/ema/actualites/armees-se-dotent-dune-doctrine-militaire-lutte-informatique-dinfluence-l2i (Last accessed: 6.10.2025)

49. Loveluck B. Souveraineté numérique et concurrence des régimes politiques : origines et perspectives. Revue des droits et libertés fondamentaux. 2025. RDLF 2025, chron. № 47. URL: https://revuedlf.com/droit-international/souverainete-numerique-et-concurrence-des-regimes-politiques-origines-et-perspectives (Last accessed: 6.10.2025)

50. Mer, espace et cyberespace : nouveaux défis de sécurité. Note n° 10/22. *Fondation pour la recherche stratégique.* Paris, 2022. URL: https://www.frstrategie.org/sites/default/files/documents/publications/notes/2022/202210.pdf (Last accessed: 6.10.2025)

51. National Cybersecurity Strategy – France. 2023. *ENISA.* URL: https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/additional-documents/FR_NCSS_PRESENTATION_2023_en.pdf (Last accessed: 6.10.2025)

52. National Strategic Review 2025. *Secrétariat général de la défense et de la sécurité nationale.* Paris, 2025. URL: https://www.sgdsn.gouv.fr/files/files/Publications/20250713_NP_SGDSN_RNS2025_EN_0.pdf (Last accessed: 6.10.2025)

53. NATO 2022 Strategic Concept. *NATO.* Madrid, 29.06.2022. URL: https://www.nato.int/en/about-us/official-texts-and-resources/strategic-concepts/nato-2022-strategic-concept (Last accessed: 6.10.2025)

54. Nguyen C. D. Digital cultural heritage in the crossfire of conflict: cyber threats and cybersecurity perspectives. Insights. 2024. URL: https://insights.uksg.org/articles/10.1629/uksg.647(Last accessed: 6.10.2025)

55. Observatoire du monde cybernétique. Programme de recherche. *Fondation pour la Recherche Stratégique.* Paris, 2022. URL: https://www.frstrategie.org/programmes-de-recherche/observatoire-du-monde-cybernetique (Last accessed: 6.10.2025)

56. Odebade A. T., Benkhelifa E. A comparative study of national cyber security strategies of ten nations. *arXiv preprint arXiv:2303.13938.* 2023. URL: https://arxiv.org/abs/2303.13938 (Last accessed: 6.10.2025)

57. Panorama de la cybermenace 2023. *Agence nationale de la sécurité des systèmes d'information (ANSSI).* Paris, 2024. URL: https://www.cert.ssi.gouv.fr/uploads/CERTFR-2024-CTI-001.pdf (Last accessed: 6.10.2025)

58. Panorama de la cybermenace 2024. *Agence nationale de la sécurité des systèmes d'information.* Paris: ANSSI, 2025. URL: https://www.cert.ssi.gouv.fr/uploads/CERTFR-2025-CTI-003.pdf (Last accessed: 6.10.2025)

59. Pellistrandi J. Digital sovereignty and resilience. *Revue Défense Nationale.* 2022. № 855. URL: https://www.defnat.com/sommaires/sommaire.php?cidrevue=855 (Last accessed: 6.10.2025)

60. Rapport annuel 2022 : Défendre et assister. *Agence nationale de la sécurité des systèmes d'information.* Paris, 2023. URL: https://cyber.gouv.fr/sites/default/files/document/ANSSI_rapport_annuel_2022.pdf (Last accessed: 6.10.2025)

61. Rapport d'activité 2022. *Agence nationale de la sécurité des systèmes d'information (ANSSI).* Paris, 2023. URL: https://cyber.gouv.fr/actualites/le-rapport-dactivite-2022-de-lanssi-est-en-ligne (Last accessed: 6.10.2025)

62. Rapport d'activité 2023 – Dispositifs réglementaires. *ANSSI.* Paris, 2024. URL: https://cyber.gouv.fr/sites/default/files/document/Rapport_activite_2023_dispositifs%20re%CC%81glementaires.pdf (Last accessed: 6.10.2025)

63. Rapport d'activité 2023. *Agence nationale de la sécurité des systèmes d'information (ANSSI).* Paris, 2024. URL: https://cyber.gouv.fr/publications/rapport-dactivite-2023-de-lanssi (Last accessed: 6.10.2025)

64. Rapport d'activité 2023. *ANSSI.* Paris, 2024. URL: https://cyber.gouv.fr/sites/default/files/document/Rapport%20d%27activit%C3%A9%202023%20de%20l%27ANSSI.pdf (Last accessed: 6.10.2025)

65. Rapport d'activité 2024 de l'ANSSI. *Agence nationale de la sécurité des systèmes d'information.* Paris: ANSSI, 2025. URL: https://cyber.gouv.fr/publications/rapport-dactivite-2024-de-lanssi cyber.gouv.fr+1

66. Regulation (EU) 2022/2065 of 19 October 2022 on a Single Market for Digital Services (Digital Services Act). *European Union*. Official Journal of the EU. 27.10.2022. URL: https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng (Last accessed: 6.10.2025)

67. Revue nationale stratégique 2022. *Secrétariat général de la défense et de la sécurité nationale (SGDSN).* Paris, 2022. URL: https://www.sgdsn.gouv.fr/publications/revue-nationale-strategique-2022 (Last accessed: 6.10.2025)

68. Second EEAS Report on Foreign Information Manipulation and Interference (FIMI) Threats. *European External Action Service.* Brussels, 2024. URL: https://euneighbourseast.eu/news/publications/second-eeas-report-on-foreign-information-manipulation-and-interference-threats/ (Last accessed: 6.10.2025)

69. Secteur de la santé – État de la menace informatique. *Agence nationale de la sécurité des systèmes d'information.* Paris: CERT-FR / ANSSI, 2024. URL: https://www.cert.ssi.gouv.fr/cti/CERTFR-2024-CTI-010/ (Last accessed: 6.10.2025)

70. Shoker A. Digital Sovereignty Strategies for Every Nation. Applied *Cybersecurity & Internet Governance.* 2022. Vol. 1. № 1. P. 1–17. URL: https://www.acigjournal.com/Digital-Sovereignty-Strategies-for-Every-Nation%2C184285%2C0%2C2.html (Last accessed: 6.10.2025)

71. Souveraineté numérique : définition, enjeux et réglementations. *Oodrive.* 2024. URL: https://www.oodrive.com/fr/blog/securite-des-donnees/souverainete-numerique-definition-enjeux-et-reglementations (Last accessed: 6.10.2025)

72. Stratégie nationale d'accélération pour la cybersécurité (France 2030). *Ministère de l'Économie, des Finances et de la Souveraineté industrielle et numérique.* Paris, 2022. URL: https://www.economie.gouv.fr/strategie-nationale-acceleration-cybersecurite (Last accessed: 6.10.2025)

73. Tackling Foreign Information Manipulation and Interference (FIMI): First EEAS Report. *European External Action Service.* Brussels, 2023. URL: https://www.eeas.europa.eu/eeas/tackling-fimi-report (Last accessed: 6.10.2025)

74. Tackling foreign information manipulation and interference : Communication COM(2022) 452 final. *European Commission.* Brussels, 02.09.2022. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022DC0452 (Last accessed: 6.10.2025)

75. The EU's Cybersecurity Strategy for the Digital Decade : Joint Communication JOIN(2020) 18 final. *European Commission; High Representative of the Union for Foreign Affairs and Security Policy.* Brussels, 16.12.2020. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020JC0018 (Last accessed: 6.10.2025)

76. The geopolitics of AI and the rise of digital sovereignty. *Brookings Institution.* 08.12.2022. URL: https://www.brookings.edu/articles/the-geopolitics-of-ai-and-the-rise-of-digital-sovereignty/ (Last accessed: 6.10.2025)

77. Tournay V., Saez G. La résilience de l'État face aux menaces informationnelles. CEVIPOF Policy Brief, no. 1. Paris, Sciences Po, 2025. URL: https://www.sciencespo.fr/cevipof/files/Note_resilienceetat_VT_juin2025_CEVIPOF.pdf (Last accessed: 6.10.2025)

78. Türk P. La souveraineté numérique européenne, vers une troisième voie? *Pouvoirs.* 2024. № 190. С. 79–90. URL: https://revue-pouvoirs.fr/la-souverainete-numerique-europeenne-vers-une-troisieme-voie (Last accessed: 6.10.2025)

79. Viginum. RNN : une campagne de manipulation de l'information complexe et persistante. Rapport. Paris, 19.06.2023. URL: https://www.sgdsn.gouv.fr (Last accessed: 6.10.2025)

80. Weiss M., Biermann F. Cyberspace and the protection of critical national infrastructure. *Journal of Economic Policy Reform*. 2023. Vol. 26. Issue 3. P. 250–267. DOI: https://doi.org/10.1080/17487870.2021.1905103 (Last accessed: 6.10.2025)

АНОТАЦІЯ

Гринець М.О. Інформаційна безпека Франції в умовах сучасних міжнародних викликів (магістерська робота). Харків: ХНУ імені В. Н. Каразіна, 2025. 84 с. (рукопис).

Кваліфікаційна робота магістра присвячена визначенню особливостей забезпечення інформаційної безпеки Франції в умовах сучасних міжнародних викликів. Об'єкт дослідження – інформаційна безпека держави в міжнародних відносинах. Предмет дослідження – система інформаційної безпеки Франції в умовах сучасних міжнародних викликів.

У першому розділі визначено поняття інформаційної безпеки у міжнародних відносинах та її ключові структурні елементи й принципи забезпечення на рівні держави; виявлено основні міжнародні виклики інформаційній безпеці та їхній вплив на трансформацію сучасних підходів до державної інформаційної політики.

У другому розділі розкрито інституційну структуру та нормативно-правові засади функціонування системи інформаційної безпеки Франції**;** встановлено особливості реалізації французької моделі інформаційної безпеки в умовах сучасних міжнародних відносин.

У третьому розділі з'ясовано можливості імплементації французького досвіду в Україні для удосконалення національної політики інформаційної безпеки в умовах актуальних міжнародних викликів**.**

Ключові слова: інформаційна безпека; Франція; міжнародні виклики; кібербезпека; гібридні загрози; дезінформація; кібероборона; цифровий суверенітет.

ANNOTATION

Hrynets M.O. Information security of France in the face of modern international challenges (master's work). Kharkiv: V. N. Karazin Kharkiv National University, 2025. 84 p. (manuscript).

The master's qualification work is devoted to determining the features of ensuring France's information security in the context of modern international challenges. The object of research is the information security of the state in international relations. The

subject of research is the information security system of France in the context of modern international challenges.

The first section defines the concept of information security in international relations and its key structural elements and principles of ensuring it at the state level; the main international challenges to information security and their impact on the transformation of modern approaches to state information policy are identified.

The second section reveals the institutional structure and regulatory and legal principles of the functioning of the French information security system; the features of the implementation of the French model of information security in the context of modern international relations are established.

The third section examines the possibilities of implementing French experience in Ukraine to improve national information security policy in the context of current international challenges.

Keywords: information security; France; international challenges; cybersecurity; hybrid threats; disinformation; cyber defense; digital sovereignty.

ВІДГУК

на кваліфікаційну роботу магістра
студента 2-го курсу групи УМІБ-61 денної форми навчання
спеціальності 291 «Міжнародні відносини,
суспільні комунікації та регіональні студії»
освітньо-професійної програми
«Міжнародна інформаційна безпека»
Навчально-наукового інституту «Каразінський інститут
міжнародних відносин та туристичного бізнесу»
Харківського національного університету імені В.Н. Каразіна
Гринця Михайла Олександровича
на тему «Інформаційна безпека Франції в умовах сучасних міжнародних викликів»

1.Актуальність теми зумовлюється стрімкою трансформацією глобального безпекового середовища, у якому інформація дедалі частіше використовується як стратегічний ресурс і як інструмент впливу. Франція, будучи ядерною державою, постійною членкинею Ради Безпеки ООН та одним із ключових акторів Європейського Союзу й НАТО, опиняється в епіцентрі гібридних загроз, що поєднують кібероперації, дезінформаційні кампанії, атаки на критичну інфраструктуру та маніпулятивні інформаційні впливи з боку недружніх державних і недержавних акторів. Особливо гострою проблемою стало втручання у внутрішньополітичні процеси, поширення фейкових наративів, спрямованих на послаблення суспільної довіри до демократичних інституцій, а також атаки на енергетичні, оборонні та цифрові системи. У цих умовах Франція змушена модернізувати національну систему інформаційної безпеки, посилювати взаємодію з європейськими партнерами й формувати комплексну модель протидії гібридним ризикам.

2. Позитивні аспекти в роботі. Зміст роботи повністю відповідає обраній темі. Робота складається зі вступу, трьох розділів, висновків та списку використаних джерел. Позитивними рисами кваліфікаційної роботи магістра є системність та послідовність викладення матеріалу.

3. Недоліки роботи. В той же час, автору слід було б приділити більше уваги ілюстративній частині роботи, однак це не впливає на роботу вцілому.

4. Практична цінність висновків і рекомендацій. Практичне значення отриманих результатів для органів влади України полягає насамперед у можливості адаптації та впровадження ефективних елементів французької моделі інформаційної безпеки, яка, як засвідчує практика, має комплексний, багаторівневий і переважно випереджувальний характер. Оскільки Франція поєднує жорсткі регуляторні механізми з розвитком стратегічних цифрових

спроможностей, українські державні інституції, зокрема РНБО, Міністерство цифрової трансформації та профільні підрозділи силового блоку, отримують орієнтири для модернізації власних підходів, насамперед у частині побудови системи стійкості до гібридних впливів.

5. Загальна оцінка дипломної роботи та її допуск/не допуск до захисту перед ЕК. Кваліфікаційна робота магістра Гринця Михайла Олександровича на тему «Інформаційна безпека Франції в умовах сучасних міжнародних викликів» заслуговує на позитивну, а її автор гідний присвоєння кваліфікації магістра міжнародних відносин, суспільних комунікацій та регіональних студій.

Керівник кваліфікаційної роботи,
кандидат політичних наук, доцент,
доцент кафедри міжнародних відносин,
міжнародної інформації та безпеки
Харківського національного

університету імені В.Н. Каразіна  Пересипкіна І. В.

РЕЦЕНЗІЯ

на кваліфікаційну роботу магістра
студента 2-го курсу групи УМІБ-61 денної форми навчання
спеціальності 291 «Міжнародні відносини,
суспільні комунікації та регіональні студії»
освітньо-професійної програми
«Міжнародна інформаційна безпека»
Навчально-наукового інституту «Каразінський інститут
міжнародних відносин та туристичного бізнесу»
Харківського національного університету імені В.Н. Каразіна
Гринця Михайла Олександровича
на тему «Інформаційна безпека Франції в умовах сучасних міжнародних викликів»

1. Актуальність теми зумовлена стрімкою еволюцією загроз, що формують нестабільне глобальне середовище та вимагають від держави проактивних рішень. Сьогодні, коли цифровізація пронизує всі сфери суспільного життя, Франція стикається з дедалі складнішими кібератаками, оркестровано поширеними дезінформаційними кампаніями та спробами зовнішнього втручання у політичні процеси. Особливої ваги питання набуло після посилення геополітичної конкуренції між провідними державами, зокрема РФ і КНР, що, у свою чергу, стимулює активне застосування інструментів інформаційного впливу. Крім того, зростає роль недержавних акторів, які завдяки доступу до високих технологій здатні завдавати значної шкоди національним інституціям. Важливо й те, що, будучи ключовим членом ЄС та НАТО, Франція не лише забезпечує власний інформаційний суверенітет, але й впливає на колективні механізми європейської та трансатлантичної безпеки. Отже, дослідження французького підходу до протидії гібридним загрозам, удосконалення кіберзахисту, захисту критичної інфраструктури та розвитку інформаційної стійкості є надзвичайно важливим для розуміння сучасних тенденцій у сфері безпеки, а також для адаптації ефективних практик в інших країнах, включно з Україною.

2. Характеристика якості виконання кожного розділу роботи. У першому розділі «ТЕОРЕТИЧНІ ЗАСАДИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ» визначено поняття інформаційної безпеки у міжнародних відносинах та її ключові структурні елементи й принципи забезпечення на рівні держави; виявлено основні міжнародні виклики інформаційній безпеці та їхній вплив на трансформацію сучасних підходів до державної інформаційної політики.

У другому розділі «ОСОБЛИВОСТІ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ФРАНЦІЇ » розкрито інституційну структуру та нормативно-правові засади функціонування системи інформаційної безпеки Франції; встановлено особливості реалізації французької моделі інформаційної безпеки в умовах сучасних міжнародних відносин.

У третьому розділі «ШЛЯХИ ВДОСКОНАЛЕННЯ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ В УМОВАХ СУЧАСНИХ МІЖНАРОДНИХ ВИКЛИКІВ» з'ясовано можливості імплементації французького досвіду в Україні для удосконалення національної політики інформаційної безпеки в умовах актуальних міжнародних викликів.

3. Ступінь обґрунтованості висновків роботи. Висновки достатньо обґрунтовані та відповідають поставленим завданням у кваліфікаційній роботі.

4. Використання в дипломній роботі останніх досліджень. Варто відзначити, що автором проаналізовано значний обсяг фактологічного матеріалу. Був здійснений детальний аналіз обраної проблематики, наукові методи використані коректно. Проаналізовано великий спектр вітчизняної та зарубіжної наукової літератури.

5. Позитивні сторони роботи. Зміст роботи повністю відповідає обраній темі. Робота складається зі вступу, трьох розділів, висновків і списку використаних джерел. В дипломній роботі присутня системність та послідовність викладення матеріалу.

6. Недоліки роботи. Доцільно було б більше уваги приділити теоретичній частині дослідження, однак це не впливає негативно на дипломну роботу в цілому.

7. Практичне значення. Практичне значення отриманих результатів полягає у формуванні для органів державної влади України цілісного, доказового та концептуально узгодженого підходу до зміцнення національної інформаційної безпеки з урахуванням французького досвіду реагування на сучасні міжнародні виклики.

8. Загальна оцінка кваліфікаційної роботи. Кваліфікаційна робота магістра Гринця Михайла Олександровича на тему «Інформаційна безпека Франції в умовах сучасних міжнародних викликів» заслуговує на позитивну, а її автор гідний присвоєння кваліфікації магістра міжнародних відносин, суспільних комунікацій та регіональних студій.

Рецензент:
кандидат політичних наук, доцент,
доцент кафедри політології,
соціології і культурології
Харківського національного педагогічного
університету імені Г. С. Сковороди КАЛЮЖНА Юлія Іванівна

Підпис [illegible]
засвідчується зав. загальним відділом

04.12.2023