УДК 343.9: 004.49
DOI https://doi.org/10.32782/2524-0374/2025-5/8

«ЦИФРОВИЙ СУВЕРЕНІТЕТ» ФРАНЦІЇ ТА ЮРИДИЧНЕ ПІДГРУНТЯ НАЦІОНАЛЬНОЇ СТРАТЕГІЇ КІБЕРБЕЗПЕКИ

FRANCE'S "DIGITAL SOVEREIGNTY" AND THE LEGAL BASIS OF THE NATIONAL CYBERSECURITY STRATEGY

Санжарова Г.Ф., старший викладач кафедри романської філології
Київський столичний університет імені Бориса Грінченка

Бак В.І., к.ю.н., доцент,
завідувач кафедри теорії та історії держави і права
Навчально-науковий інститут права Державного податкового університету

Санжаров В.А., к.ю.н.,
доцент кафедри теорії та історії держави і права
Навчально-науковий інститут права Державного податкового університету

Стаття присвячена дослідженню особливостей, інституційного та законодавчого наповнення французької концепції кібербезпеки. Можна стверджувати, що Французька республіка займає чільне місце серед лідерів в області розробки та впровадження сучасних практик кібербезпеки. Відзначено, що головною ознакою французького механізму запобігання злочинності в умовах глобалізації електронних комунікацій є високоцентралізована система національного управління кібербезпекою. Автори вважають, що позиція Французької республіки в галузі кібербезпеки базується на семи ключових принципах: 1) покращення захисту інформаційних систем країни; 2) відбиття кібер-атак шляхом нарощування обороноздатності та стійкості до зловмисної активності в Інтернеті; 3) захист доступності і цілосності Інтернету; утвердження та здійснення цифрового суверенітету Франції; 4) більш ефективне реагування кримінального правосуддя на кіберзлочинність; запобігання поширенню шкідливих онлайн-програм і методів; 5) розвиток і просування суспільної культури інформаційної безпеки; 6) участь у розбудові безпечної та надійної цифрової Європи; 7) підтримка міжнародних дій щодо колективного управління та контролю над кіберпростором. Відзначено, що результатом реалізації французької стратегії кібербезпеки стало визнання країни як «ключової кібердержави» в Групі урядових експертів ООН (UN GGE) із сприяння відповідальній поведінці держав у кіберпросторі в контексті міжнародної безпеки. Зроблено висновок, що Французька республіка постійно і наполегливо дбає про захист та реалізацію свого «цифрового суверенітету», в країні створено дієву систему для розвитку та підтримки сектору кібербезпеки, завчасна імплементація новітніх технологій сприяла запровадженню системи кібербезпеки, яка, як показала остання Олімпіада, здатна протидіяти сучасним викликам та кіберзагрозам.

Ключові слова: кримінальне право, кіберпростір, кібербезпека, кіберзлочин, Стратегія кіберзахисту та кібербезпеки, Національне агентство з безпеки інформаційних систем.

The article is devoted to the study of the features, institutional and legislative content of the French concept of cybersecurity. It can be argued that the French Republic occupies a prominent place among the leaders in the development and implementation of modern cybersecurity practices. It is noted that the main feature of the French mechanism for preventing crime in the context of the globalization of electronic communications is a highly centralized system of national cybersecurity management. The authors believe that the position of the French Republic in the field of cybersecurity is based on seven key principles: 1) improving the protection of the country's information systems; 2) repelling cyber-attacks by increasing defense capabilities and resilience to malicious activity on the Internet; 3) protecting the accessibility and integrity of the Internet; asserting and exercising France's digital sovereignty; 4) more effective criminal justice response to cybercrime; preventing the spread of malicious online programs and methods; 5) developing and promoting a public culture of information security; 6) participating in the construction of a safe and secure digital Europe; 7) supporting international actions for the collective management and control of cyberspace. It was noted that the implementation of the French cybersecurity strategy resulted in the country being recognized as a 'key cyberstate' by the UN Group of Governmental Experts (UN GGE) on Promoting Responsible Behavior of States in Cyberspace in the Context of International Security. It was concluded that the French Republic is constantly and persistently concerned with the protection and implementation of its 'digital sovereignty', an effective system has been created in the country for the development and support of the cybersecurity sector, and the early implementation of the latest technologies has contributed to the introduction of a cybersecurity system, which, as the recent Olympic Games showed, is capable of countering modern challenges and cyber threats.

Key words: Criminal Law, Cyberspace, Cybersecurity, Cybercrime, Cyberdefence and Cybersecurity Strategy, National Agency for the Security of Information Systems.

Актуальність. Реагування на зростання кількості, інтенсивності та складності загроз, ризиків і вразливостей через нестримний розвиток інформаційно-комунікаційних технологій в останні роки стало національним пріоритетом Французької республіки. Масова цифровізація сучасних суспільств створює серйозні проблеми для управління, включаючи недобросовісну конкуренцію та шпигунство, дезінформацію та пропаганду, тероризм і злочинність. Кібертехнології змінюють традиційні відносини між державами, недержавними суб'єктами та приватним сектором, цифрові зв'язки та технологічні інновації тепер є невід'ємною частиною сучасних стратегій влади, сприяють зростанню влади нових приватних суб'єктів, які можуть кинути виклик традиційній суверенній владі держав. Протягом 2024 року Національне агентство з безпеки інформаційних систем (ANSSI) обробило на 15% більше подій безпеки ніж у попередньому році – 4386 (3004 повідомлень та 1361 інцидент) [1, с. 5; 2]. Глобальною щоденною небезпекою для всіх французьких організацій стала загроза, яку створює екосистема кіберзлочинців, яка в першу чергу характеризується атаками програм-вимагачів та витоками даних. Серед жертв програм-вимагачів, відомих Національному агентству з безпеки інформаційних систем, особливо постраждали бізнес структури (37%), місцеві органи влади (17%), вищі навчальні заклади (12%) і стратегічні компанії (12%), часто з дуже серйозними наслідками для їх діяльності, репутації та безперервності бізнесу [3]. Спостерігалося збільшення низькотехнологічних, але резонансних атак. Наприклад, кількість розподілених атак типу «відмова в обслуговуванні» (DDoS) проти об'єктів у Франції зросла вдвічі порівняно з 2023 роком, причому під час Олімпій-

ських Ігор цей показник зріс. Французька кіберекосистема гідно впоралася з «олімпійським викликом»: жодна з кібератак не вплинула на проведення заходу [1, с. 7–8].

Аналіз останніх досліджень і публікацій. У 2018 р. було запроваджено «Європейську директиву про безпеку мереж та інформаційних систем» («Network and Information System Security», NIS), яка має на меті забезпечити високий спільний рівень безпеки інформаційних систем Європейського Союзу [4]. Правознавці, як зарубіжні (С. Шміц-Берндт, П. К'яра, с. Романюк, М. Манжікян та інші) [5, с. 289–311; 6], так і вітчизняні (М.О. Мацелик, О.А. Павлюх, Г.Ф. Санжарова та інші) [7, с. 219–227; 8, с. 71–73; 9, с. 28–30] все частіше звертаються як до проблеми імплементації спільного кібербезпекового законодавства, вивчення досвіду протидії кіберзлочинності на національному інституційно-законодавчому рівні окремих країн. Національна стратегія кібербезпеки Французької республіки поступово еволюціонувала від оборонної доктрини «активного захисту» до доктрини «наступальних кіберспроможностей» [10; 11, с. 62–72], вивчення цього процесу безумовно потребує дослідницької уваги.

Мета статті полягає в дослідженні особливостей, інституційного і законодавчого наповнення та реалізації французької концепції кібербезпеки.

Виклад основного матеріалу. Сектор інформаційно-комунікативних технологій постійно зміцнює своє значення для орієнтованої на послуги сучасної французької економіки (80% економіки покладається на інформаційні мережі чи ІТ-послуги). У 2012 році реальному вираженні загальний дохід від сектору електронних комунікацій у Франції перевищив 50 мільярдів євро (понад 4,5% ВВП), це є третім за величиною показником у ЄС [10, с. 3]. Рівень проникнення інтернету станом на 2019 рік (92,3%) перевищив середній показник по ЄС (90,4%), інфраструктурою фіксованого широкосмугового доступу покрито 100% території країни [11, с. 62]. Вражаюче зростання цифрової економіки та інформаційно-комунікаційної інфраструктури Франції значною мірою є результатом урядової «Програми майбутніх інвестицій» («Investissements d'Avenir») 2010 року, яка включала початковий фонд у розмірі 35 мільярдів євро для державних інвестицій у технологічні та промислові проекти, а потім додаткові 12 мільярдів євро у 2013 році. Значні інвестиції були спрямовані на цифрову економіку: 69 мільйонів євро на дослідження хмарних обчислень, 83 мільйони євро на проекти «розумних мереж» та 70 мільйонів євро на розробку високошвидкісних (30 Мбіт/с) широкосмугових інтернет-супутників. Одним з головних завдань реформи державної політики було надання пріоритету цифровому адмініструванню. За даними Євростату у 2013 році 60% населення Франції використовували Інтернет для отримання доступу до державних послуг (податкові надходження, соціальні виплати, запити на адміністративні документи тощо), майже 30% податкових звітів про надходження було подано через онлайн-сервіси [10, с. 6–7]. Один з проектів реіндустріалізації країни спрямований на розвиток кібербезпеки у Франції [3].

Огляд кіберзагроз 2024 року зазначив, що минулий рік характеризувався постійним тиском як на національну екосистему кібербезпеки, так і на найважливіші інформаційні системи. Зловмисники (хакери), яких вважають пов'язаними зі стратегічними інтересами Росії, проводили атаки, керуючись насамперед пошуком інформації, яка могла б підтримати їхні військові чи дипломатичні зусилля [12]. Франція атрибувала кілька кібератак Fancy Bear проти французьких інтересів, державних служб, приватних компаній з 2021 року, організаторам Олімпійських та Паралімпійських ігор 2024 року російській службі військової розвідки (ГРУ) [1, с. 7–9; 3, с. 14–19]. Вважається, що раніше ГРУ було причетне до кібератаки на TV5 Monde у 2015 році, а також до спроби дестабілізації виборчого процесу у Франції у 2017 році. Зловмисники (хакери), яких вважають пов'язаними зі стратегічними інтересами Китаю, опікувались насамперед інтересами стратегічної та економічної розвідки [13].

Підхід Франції до побудови національної кібербезпеки зосереджується на мобілізації різноманітних ресурсів не лише урядом, але й громадянським суспільством, пріоритетом для посилення стійкості основних електронних послуг і кібербезпекових систем у Франції є співпраця між державою, приватним сектором і громадянським суспільством. Загалом ця позиція Французької республіки базується на семи ключових принципах: 1) покращення захисту інформаційних систем країни; 2) відбиття кібератак шляхом нарощування обороноздатності та стійкості до зловмисної активності в Інтернеті; 3) захист доступності і цілосності Інтернету; утвердження та здійснення цифрового суверенітету Франції; 4) більш ефективне реагування кримінального правосуддя на кіберзлочинність; запобігання поширенню шкідливих онлайн-програм і методів; 5) розвиток і просування суспільної культури інформаційної безпеки; 6) участь у розбудові безпечної та надійної цифрової Європи; 7) підтримка міжнародних дій щодо колективного управління та контролю над кіберпростором [11, с. 63].

Франція підписала Будапештську конвенцію про кіберзлочинність 2001 року; Республіка розглядає використання Інтернету терористами як глобальну проблему, яка потребує інноваційних міжнародних рішень: використання новітніх технологій (включаючи штучний інтелект та машинне навчання) для прискорення ідентифікації зловмисного контенту. Країна співпрацює в тісному партнерстві з ООН (включаючи ініціативу «Технології проти тероризму») та ЄС.

Як політичний пріоритет «кібербезпека» була визначена у червні 2008 р. у третій Білій книзі французького уряду про оборону та національну безпеку (численні посилання на «кібератаки» і навіть «кібервійну/кібервійни»). Документ містив комплексний 15-річний стратегічний план, який передбачав суттєвий перегляд безпеки та оборони Франції від тогочасної пасивної оборонної стратегії до «глибокої активної оборонної стратегії», що мала поєднувати внутрішній захист систем із постійним спостереженням, швидким реагуванням і наступальними діями, підтримуючи зусилля, спрямовані на розвиток наступальних кіберспроможностей. «Біла книга» окреслила чотири ключові сфери забезпечення національної безпеки, які потребували особливої уваги та інвестицій у «довгостроковій перспективі»: 1) визначення загальної концепції, яка включала б всі дії у можливій кібервійні; 2) розробка спеціалізованих засобів (мережева цифрова зброя, технічна та операційна лабораторія тощо); 3) формулювання доктрини наступальних можливостей кібервійни (планування, виконання, оцінка дій); 4) запровадження відповідної та регулярно оновлюваної підготовки персоналу спеціалізованих підрозділів [14].

Національним органом безпеки та захисту французьких інформаційних систем, який відстежує, виявляє та координує реакцію на кібератаки, є створене у липні 2009 року Національне агентство з безпеки інформаційних систем (Agence nationale de la sécurité des systèmes d'information, ANSSI) (Указ № 2009–834 від 7 липня 2009 р.), яке безпосередньо підпорядковане Голові Генерального секретаріату з питань національної оборони та безпеки (Secrétariat général de la défense et de la sécurité nationale, SGDSN) і діє під керівництвом Прем'єр-міністра (Закон № 2013–1168 від 18 грудня 2013 р.) [15]. Бюджет цієї організації складав приблизно 20 мільйонів євро на рік у другій половині 2010-х рр. (наразі 29 млн.), а кількість співробітників зросла за цей період майже вдвічі [12]. Гендиректором ANSSI з 04.01.2023 р. є Вєнсан Стрю-

бель. В 2011 році ANSSI розробила «Стратегію кіберзахисту та кібербезпеки», яка проголосила чотири стратегічні цілі для Франції: 1) стати глобальною державою кіберзахисту, доєднавшись до кола основних держав у цій галузі, але зберігши власну автономію; 2) захищати свободу прийняття рішень у Франції шляхом захисту суверенної інформації, запобігати втручанню у виборчі процеси; 3) покращити безпеку цифрових продуктів і послуг, запобігати поширенню шкідливих онлайн-програм і методів; підвищити кібербезпеку національних критичних інфраструктур; 4) сприяти загальній безпеці в кіберпросторі [11, с. 63; 16].

Французька позиція з кібербезпеки поступово уточнювалась та деталізовувалась в серії подальших документів та оглядів: 1) «Біла книга з питань оборони та національної безпеки» 2013 року («White Paper on Defense and National Security», Міністерство Оборони) [17]; 2) «Національна стратегія цифрової безпеки» 2015 року («National Digital Security Strategy», Прем'єр-міністр, 2015); 3) «Стратегічний огляд оборони та національної безпеки» за 2017 рік («Defense and National Security Strategic Review», Міністр Європи та закордонних справ); 4) «Стратегічний огляд кіберзахисту» 2018 року («The Strategic Review of Cyber Defense», Генеральний секретаріат оборони та національної безпеки,). У кожному з нормативних документів національні цілі кібербезпеки залишалися в основному незмінними: забезпечення національного цифрового суверенітету та сильної відповіді проти кібер-зловмисних дій; створення системи інформування та залучення широкої громадськості, бізнесу та промисловості; перетворення цифрової безпеки на конкурентний актив для французьких компаній; та зміцнення позицій Франції на міжнародному рівні [11, с. 67].

У лютому 2018 року «Стратегічний огляд кіберзахисту» представив переоцінку кіберстратегії Франції та пов'язаної з нею структури військових сил. В січні 2019 року міністр оборони Франції Флоранс Парлі підтвердив перехід Республіки від оборонної доктрини «активного захисту» до доктрини «наступальних кіберспроможностей». В жовтні 2018 року було офіційно заявлено, що при використанні Інтернету Міністерство оборони Франції та Національна асамблея Франції більше не будуть покладатися на іноземні цифрові компанії. У 2023 році закон про військове програмування на 2024–2030 роки розширив можливості ANSSI, зокрема, щодо пошуку технічних маркерів та блокування доменних імен, що використовуються зловмисниками (Закон № 2023-703) [2].

Французька Республіка не підтримує створення з метою більш детальної специфікації норм, правил і принципів використання кіберпростору будь-яких нових юридично обов'язкових міжнародних інструментів «спеціально для питань кібербезпеки». Франція надає перевагу розвитку підходу «м'якого права» там, де існуючі міжнародні норми виявляються недостатніми. Втім, у деяких випадках позиція Франції щодо тлумачення та застосовності міжнародного права до кіберпростору не позбавлена суперечностей; наприклад, вона висловила підтримку законності «попереджувального самозахисту» від кібератак [11, с. 68].

Генеральний секретар ООН призначив Францію (як ключову кібердержаву) для участі в роботі Групи урядових експертів ООН з розробок у сфері інформації та телекомунікацій у контексті міжнародної безпеки (UN GGE). Французькі спеціалісти приймали участь в підготовці прийнятих консенсусом звітів міжнародної експертної групи, які деталізували нормативну базу для відповідальної поведінки держав у кіберпросторі (GGE 2013, 2015). Звіти GGE є досить загальними у обговореннях і рекомендаціях; значною мірою це відображає нездатність Групи досягти консенсусу щодо вирішення питання застосування принципів та норм міжнародного права до кіберпростору та кібероперацій. Проте було погоджено, що принципи та норми міжнародного права – не обмежуючись Статутом Організації Об'єднаних Націй (ООН), міжнародним гуманітарним правом і дотриманням прав людини – застосовуються до використання державами кіберпростору, у тому числі в контексті міжнародних та неміжнародних збройних конфліктів (GGE, 2015). Як член Великої сімки Франція 11 квітня 2017 року схвалила Декларацію G7 про відповідальну поведінку держав у кіберпросторі («Луккська декларація»). У контексті міжнародної співпраці та захисту від небезпек, спричинених зловмисним використанням кібертехнологій Луккська декларація підтвердила точку зору G7 про те, що міжнародне право та Статут ООН є життєво важливими для стабільності та підтримки миру та безпеки у кіберпросторі. Під час свого головування у G7 у 2019 році Франція зосередила зусилля G7 на покращенні стійкості фінансового сектора до кіберзагроз.

У листопаді 2018 року Франція запустила велику незалежну ініціативу під назвою «Паризький заклик до довіри та безпеки в кіберпросторі» («Paris Call for Trust and Security in Cyberspace»). Ця ініціатива Франції була спробою «взяти на себе відповідальність» за майбутнє глобальне управління кіберпростором. «Паризький заклик» («Paris Call») пропонує низку загальних принципів, якими має керуватися поведінка як державних, так і недержавних суб'єктів з метою забезпечення «відкритого, безпечного, стабільного, доступного та мирного кіберпростору». «Паризький заклик» підтримав застосовність міжнародного права та прав людини до кібер-сфери та нагадав про низку принципів, таких як відповідальна поведінка держав, державна монополія на законне насильство та визнання конкретних обов'язків приватних зацікавлених сторін, які повинні сприяти розвитку структури управління кіберпростором. «Паризький заклик» сприяв досягненню довіри та безпеки в кіберпросторі як спільної відповідальності широкого кола учасників, він включав поширення міжнародної відповідальності за кібербезпеку на приватних суб'єктів, зокрема, це стосувалося проектування, інтеграції, розгортання та обслуговування їхніх продуктів, процесів і цифрових послуг. «Заклик» отримав підтримку великої кількості держав (включно з усіма членами Європейського Союзу), багатонаціональних компаній (включно з Microsoft і Facebook) та організацій громадянського суспільства [11, с. 67–69].

Франція відіграє активну роль у роботі ОБСЄ з усунення можливих вразливих для держав наслідків використання кібертехнологій. Превентивна дипломатія включає ухвалення та реалізацію заходів зі зміцнення довіри, які зосереджені на посиленні міждержавної прозорості та передбачуваності комунікації, готовності до співпраці в сфері кібербезпеки. Франція розробила широку мережу двосторонніх і багатосторонніх партнерств для розширення свого впливу на вирішення міжнародних кіберпроблем. Франція підтримує бачення та концепцію єдиного цифрового ринку ЄС. Стратегія Єдиного цифрового ринку ЄС спрямована на відкриття цифрових можливостей для людей і бізнесу та посилення позицій Європи як світового лідера в цифровій економіці, забезпечуючи вільний рух людей, послуг і капіталу за умов високого рівня захисту споживачів і персональних даних, незалежно від національності чи місця проживання. Франція є членом-засновником Глобального форуму з кіберекспертизи (GFCE), глобальної платформи для країн, міжнародних організацій і приватних компаній для обміну найкращими практиками та досвідом щодо використання кібердомену для комунікації, інновацій та сталого соціального розвитку та економічного зростання («кіберпотенціал»).

Висновки. Таким чином, треба відзначити, що, по-перше, позиція Французької республіки в галузі кібербезпеки базується на семи ключових принципах: 1) покращення захисту інформаційних систем країни;

2) відбиття кібер-атак шляхом нарощування обороноздатності та стійкості до зловмисної активності в Інтернеті; 3) захист доступності і цілосності Інтернету; утвердження та здійснення цифрового суверенітету Франції; 4) більш ефективне реагування кримінального правосуддя на кіберзлочинність; запобігання поширенню шкідливих онлайн-програм і методів; 5) розвиток і просування суспільної культури інформаційної безпеки; 6) участь у розбудові безпечної та надійної цифрової Європи; 7) підтримка міжнародних дій щодо колективного управління та контролю над кіберпростором. По-друге, Французька республіка постійно і наполегливо дбає про захист та реалізацію свого «цифрового суверенітету», в країні створено дієву систему для розвитку та підтримки сектору кібербезпеки, завчасна імпліментація новітніх технологій сприяла запровадженню системи кібербезпеки, яка, як показала остання Олімпіада, здатна протидіяти сучасним викликам та кіберзагрозам. Головною ознакою французького механізму запобігання злочинності в умовах глобалізації електронних комунікацій є високоцентралізована система національного управління кібербезпекою. Результатом реалізації французької стратегії кібербезпеки стало визнання країни як «ключової кібердержави» в Групі урядових експертів ООН (UN GGE) із сприяння відповідальній поведінці держав у кіберпросторі в контексті міжнародної безпеки.

ЛІТЕРАТУРА

1. Panorama de la cybermenace 2024. URL: https://www.cert.ssi.gouv.fr/uploads/CERTFR-2025-CTI-003.pdf (дата звернення: 26.05.2025).
2. Panorama de la cybermenace 2023. URL: https://www.cert.ssi.gouv.fr/cti/ CERTFR-2024-CTI-001/ (дата звернення: 26.03.2025).
3. Rapport d'activité 2024, l'ANSSI. *Cyber.gouv.fr.* : веб-сайт. URL: https:// cyber.gouv.fr/publications/rapport-dactivite-2024-de-lanssi (дата звернення: 24.03.2025).
4. Network and Information System Security. *Nis-2-directive*: веб-сайт. URL: https://www.nis-2-directive.com (дата звернення: 28.03.2025).
5. Schmitz-Berndt S., Chiara P.G. One step ahead: mapping the Italian and German cybersecurity laws against the proposal for a NIS2 directive. *International Cybersecurity Law Review*. 2022. Vol. 3. P. 289–311.
6. Routledge Companion to Global Cyber-Security Strategy / ed. S.N. Romaniuk, M. Manjikian. London-New York: Routledge, 2021. 656 p.
7. Павлюх О.А., Санжарова Г.Ф., Санжаров В.А. Виклики сучасної кібербезпеки: інституційні і правові відповіді Німеччини. *Ірпінський юридичний часопис. Серія: право*. 2023. Вип. 3 (12). С. 219–227.
8. Санжарова Г.Ф., Мацелик М.О., Санжаров В.А. Еволюція стратегії кібербезпеки Німеччини протягом останніх трьох десятиліть: інституційний та правничий виміри. *Наукові тренди постіндустріального суспільства*: матеріали IV Міжнар. наук. конф., м.Суми, 31 бер. 2023 р. Вінниця: ЄНП, 2023. С. 71–73.
9. Мацелик М.О., Санжарова Г.Ф., Санжаров В.А. Третя національна стратегія кібербезпеки Великої Британії: політика «на майбутнє» в динамічному технічному середовищі. *Юридичний науковий електронний журнал*. 2023. № 9. С. 28–30.
10. Brangetto P. National Cyber Security Organisation: France. Tallinn: NATO CCD COE, 2015. 18 p. URL: https://ccdcoe.org/uploads/2018/10/CS_ organisation_FRANCE_032015_0.pdf (дата звернення: 28.08.2024).
11. Danvish A., Romaniuk S.N. Cyber security in the French Republic. *Routledge Companion to Global Cyber-Security Strategy* / ed. S.N. Romaniuk, M. Manjikian. London-New York: Routledge, 2021. P. 62–72.
12. Russian Foreign Intelligence Service (SVR) Exploiting JetBrains TeamCity CVE Globally. *Cisa.gov*: веб-сайт. URL: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-347a (дата звернення : 28.05.2025).
13. Raggi M. IOC Extinction? China-Nexus Cyber Espionage Actors Use ORB Networks to Raise Cost on Defenders. *App.tidalcyber.com*: веб-сайт. URL: https://app.tidalcyber.com/references/3852fe26-53ad-504f-9328-7e249d121ebd (дата звернення : 28.05.2025).
14. Mallet J.-C. Défense et Sécurité nationale: le Livre blanc, 2008. *Vie-publique.fr* : веб-сайт. URL: https://www.vie-publique.fr/rapport/29834-defense-et-securite-nationale-le-livre-blanc (дата звернення : 28.05.2025).
15. Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), Défense et sécurité des systèmes d'information. Stratégie de la France, 2011. *Sgdsn. gouv.fr*: веб-сайт. URL: https://www.sgdsn.gouv.fr/notre-organisation/composantes/ agence-nationale-de-la-securite-des-systemes-dinformation (дата звернення : 28.05. 2025) .
16. Défense et sécurité des systèmes d'information. Stratégie de la France. *Enisa.europa.eu* : веб-сайт. URL: https://www.enisa.europa.eu/sites/default/files/ all_files/Cyber_strategie_de_la_France.pdf (дата звернення : 28.05.2025).
17. Livre blanc sur la défense et la sécurité nationale 2013. URL: https://sofia.medicalistes.fr/spip/IMG/pdf/Le_Livre_Blanc_de_la_Defense_et_de_la_Securite_Nationale-_tome_2_les_auditions.pdf (дата звернення: 28.05.2025).