УДК 343.9: 004.49
DOI https://doi.org/10.24144/2307-3322.2025.90.1.17

ІТАЛІЙСЬКА КІБЕРБЕЗПЕКОВА АРХІТЕКТУРА: ЗАХИСТ КРИТИЧНОЇ ІНФРАСТРУКТУРИ, ТЕХНІЧНІ, ПРАВОВІ ТА ІНСТИТУЦІЙНІ НОВОВВЕДЕННЯ

Санжарова Г. Ф.,
старший викладач кафедри романської філології
Київського столичного університета імені Бориса Грінченка
ORCID: 0000-0002-0557-9192
e-mail: h.sanzharova@kubg.edu.ua

Сіренко О. В.,
кандидат юридичних наук, доцент,
доцент кафедри теорії та історії держави і права ННІ права
Державного податкового університету
ORCID: 0000-0002-6567-2321
e-mail: o.v.sirenko@dpu.edu.ua

Санжаров В. А.,
кандидат юридичних наук,
доцент кафедри теорії та історії держави і права ННІ права
Державного податкового університету
ORCID: 0000-0003-4075-8572
e-mail: v.a.sanzharov@dpu.edu.ua

Санжарова Г.Ф., Сіренко О.В., Санжаров В.А. Італійська кібербезпекова архітектура: захист критичної інфраструктури, технічні, правові та інституційні нововведення.

Стаття присвячена дослідженню італійської архітектури кібербезпеки, стратегії та організаційних засад захисту критичної інфраструктури країни, логіки технічних, правових та інституційних нововведень в сфері кіберзахисту Італійської Республіки. Встановлено, що Італія зробила перші регуляторні кроки щодо кібербезпеки відносно пізно порівняно з іншими європейськими державами – у 2013 році («Декрет Монті»). Друга італійська стратегія кібербезпеки («Декрет Джентілоні») мала на меті впорядкуівння інституційної екосистеми кібербезпеки відповідно до вимог європейської «Директиви про мережеву та інформаційну безпеку (NIS)». Аналіз еволюції італійської кібербезпеки дозволяє стверджувати, що між стратегіями 2013 і 2018 років більшість змін стосувалися інституційної бази (зменшення кількості учасників з дублюючими функціями; централізація структури), а не формулювання політики кібербезпеки. Відповідно до «Директиви NIS» була створена національна команда для реагування на комп'ютерні інциденти («Команда реагування на інциденти комп'ютерної безпеки», CSIRT). Констатовано, що подальшому розвитку послідовної та всеосяжної правової бази в галузі кібербезпеки сприяло створення так званого «національного периметру кібербезпеки» («Perimetro di Sicurezza Nazionale Cibernetica»). Законодавцями чітко визначені «критичні технології»: штучний інтелект, робототехніка, напівпровідники, кібербезпека, аерокосмічна промисловість, оборона, зберігання енергії, квантові, ядерні, нано- та біо-технології. Відзначено, що за останні роки Італія зміцнила свої можливості кіберзахисту шляхом створення Національного агентства кібербезпеки (ACN), якому було доручено реалізовувати нову (третю) Національну стратегію кібербезпеки на 2022–2026 роки. Автори вважають, що широкий набір заходів, передбачених італійським законодавством, значною мірою відповідає вимогам кібербезпеки, розробленим інститутами ЄС. Зроблено висновок, що гнучке національне законодавство засноване на постановах уряду дозволяє уникнути надмірної нормативної бази, оскільки в нього можна легко і відносно швидко вносити поправки.

Ключові слова: кримінальне право, кіберпростір, кібербезпека, кіберзлочин, Національне агентство з кібербезпеки, Національна стратегія кібербезпеки, Національний периметр кібербезпеки.

Sanzharova G.F., Sirenko O.V., Sanzharov V.A. Italian cybersecurity architecture: protection of critical infrastructure, technical, legal and institutional innovations.

The article is devoted to the study of the Italian cybersecurity architecture, the strategy and organizational principles of protecting the country's critical infrastructure, and the logic of technical, legal, and institutional innovations in the field of cyber defense of the Italian Republic. It has been established that Italy took its first regulatory steps on cybersecurity relatively late compared to other European countries – in 2013 ('Monti Decree'). The second Italian cybersecurity strategy ('Gentiloni Decree') aimed to streamline the institutional cybersecurity ecosystem in accordance with the requirements of the European 'Network and Information Security (NIS) Directive'. An analysis of the evolution of Italian cybersecurity suggests that between the 2013 and 2018 strategies, most of the changes concerned the institutional framework (reduction of the number of actors with overlapping functions; centralization of the structure) rather than the formulation of cybersecurity policy. In accordance with the 'NIS Directive', a national team was established to respond to computer incidents ('Computer Security Incident Response Team', CSIRT). It was noted that the further development of a consistent and comprehensive legal framework in the field of cybersecurity was facilitated by the creation of the so-called 'national cybersecurity perimeter' ('Perimetro di Sicurezza Nazionale Cibernetica'). Lawmakers have clearly defined 'critical technologies': artificial intelligence, robotics, semiconductors, cybersecurity, aerospace, defense, energy storage, quantum, nuclear, nano- and bio-technologies. It was noted that in recent years, Italy has strengthened its cyber defense capabilities by creating the National Cyber Security Agency (ACN), which was tasked with implementing the new (third) National Cyber Security Strategy for 2022–2026. The authors believe that the wide range of measures provided for by Italian legislation largely complies with the cybersecurity requirements developed by EU institutions. It is concluded that flexible national legislation based on government decrees avoids excessive regulatory framework, as it can be amended easily and relatively quickly.

Key words: Criminal Law, Cyberspace, Cybersecurity, Cybercrime, National Cybersecurity Agency, National Cybersecurity Strategy, National Cybersecurity Perimeter.

Постановка проблеми: За останні 5 років кількість виявлених кібер-інцидентів демонструє однозначну тенденцію до значного зростання: середньомісячний показник зріс зі 156 у 2020 році до 295 у 2024 році. У 2024 році річне зростання інцидентів, виявлених з публічних джерел, становило 27,4% (з 2779 до 3541). Рік за роком зростав середній рейтинг серйозності виявлених інцидентів, що є показником додаткового множника збитків. У 2024 році, як і в 2023 році, кібер-інциденти, класифіковані як «критичні» або «серйозні», становили приблизно 80% від загальної кількості (у 2020 році – 50%) [1, с. 9]. Згідно «Звіту Clusit 2024 про безпеку ІКТ в Італії» («Rapporto Clusit 2024 sulla sicurezza ICT in Italia») за п'ять років з 2019 по 2023 роки було виявлено 653 кібер-атаки значної серйозності. З них 310 було зареєстровано у 2023 році, тобто кількість кібер-атак, спрямованих проти Італії, зросла на 65% порівняно з попереднім роком. Як кількісний, так і якісний (43% інцидентів мали високий рівень наслідків) рівень інцидентів ІТ-безпеки в Італії постійно зростають [2, с. 9]. Найчастіше мішенню кіберзлочинців є державний сектор (19%), виробництво (13%), транспорт (12%), множинні цілі (11%), фінанси/страхування (9%) та оптова/роздрібна торгівля (9%) [2, с. 27]. Розподілена відмова в обслуговуванні є найпоширенішою технікою атак у 2023 році (36%) для ураження італійських підприємств та установ, при цьому шкідливе програмне забезпечення стає менш поширеним (зниження з 53% у 2022 році до 33% у 2023 році) [2, с. 41]. Кількість кібер-інцидентів, що сталися у 2024 році в Італії зросла на 15% порівняно з 2023 роком [1, с. 9]. Здійснені кіберзлочинцями у 2023 році атаки в середньому призвели до більш критичних наслідків ніж в попередні роки. Значно зросли долі «шпигунства» та «інформаційної війни», атак з критичним впливом, перейшовши від значень, близьких до 50% до значень близько 70%. Цю тенденцію, спеціалісти пояснюють посиланням на російсько-український та ізраїльсько-палестинський конфлікти, які, принаймні з точки зору кібербезпеки, охоплюють багато країн [2, с. 25].

Італія почала займатися питаннями національної кібербезпеки пізно порівняно з іншими європейськими державами – наприклад, Францією [3, с. 42–45; 4, с. 75–82], Великою Британією

[5, с. 28–30] та Німеччиною [6, с. 219–227; 7, с. 289–311]. На думку президентів Clusit Габріеле Фаджолі (2013–2024) та Анни Ваккареллі (2025) Італія протягом останніх років залишається однією з найбільш постраждалих від кіберзлочинної діяльності країн [2; 1, с. 9]. У 2024 році 10% зареєстрованих на світовому рівні кібер-нападів припадають на долю Італії (0,7% населення та 1,8% світового ВВП); для порівняння: Франція – 4%, Німеччина – 3%, Велика Британія – 3% [1, с. 9]. Тим цікавіше проаналізувати прийняті рішення відносно впорядкування кібербезпекової архітектури до сучасних мінливих викликів та загроз, запровадження технічних та правових запобіжників для захисту критичної інфраструктури.

Стан опрацювання проблематики: Прогрес цифровізації та постійно зростаючий взаємозв'язок між «реальним» та цифровим середовищами (Інтернет речей тощо) підвищують інтерес кіберзлочинців до даних та інформації, доступних в Інтернеті. Кібербезпека стрімко розвивається, як через поширення генеративного штучного інтелекту, який змінює схеми кібер-атак та кібер-захисту, так і через зростаючий «професіоналізм» кіберзлочинців, які використовують дедалі складніші методи. Кількість кіберзлочинців і кількість кібер-інцидентів постійно зростають завдяки продажу «атак» більш досвідченими кіберугрупованнями злочинцям із середніми та низькими навичками, це також значно збільшує ймовірну аудиторію потенційних жертв. Італійські та європейські дослідники приділяють значну увагу вивченню італійського досвіду створення та поступового вдосконалення кібербезпекової архітектури, розробки стратегії протидії кіберзлочинності та запровадження єдиного європейського законодавства до кіберпростору: Джамп'єро Джакомелло (Giacomello), Томмазо Де Зан (De Zan), Луїджі Мартино (Martino), П'єр Джорджо К'яра (Chiara), Андреа Спациани (Spaziani) та інші [8, с. 199–218; 9, с. 121–131; 7, с. 219–227; 4, с. 87–91]. Певні розвідки з цієї проблематики з'явилися останнім часом у вітчизняній науці (А. Шевченко, О. Павлюх, В. Санжаров) [10, с. 80–82].

Метою цієї статті є дослідження італійської архітектури кібербезпеки, стратегії та організаційних засад захисту критичної інфраструктури країни, логіки технічних, правових та інституційних нововведень в сфері кіберзахисту Італійської Республіки.

Виклад основного матеріалу: Італія за всіма показниками є сучасним суспільством з розвиненою економікою, але на відміну від інших членів G7 повільніше впроваджує нові технології та інтегрує їх в економіку, довгий час країна повільніше реагувала на кібер-вразливості. Перша комп'ютерна мережа Італії була створена в 1980 році, в 1986 році вона підключилася до Інтернету (тоді ARPANET) після Великої Британії, Німеччини та Норвегії. Італійський уряд постійно підтримував і підтримує Інтернет як каталізатор економічного зростання, збільшення туризму, зниження витрат на зв'язок та підвищення ефективності державних операцій. Найвиразнішою рисою інформаційного суспільства Італії є надзвичайний розвиток мобільної телефонії та мобільного інтернету. Втім традиційні партнери і союзники Італії не завжди підтримують італійські ініціативи: так ЄС та Сполучені Штати висловили серйозну стурбованість після того як навесні 2019 року після підписання меморандуму про взаєморозуміння з Китаєм, за яким Італія відкривала свою інфраструктуру 5G для китайців. До того ж сучасна концепція кібербезпеки є ширшою, ніж суто технічний вимір ІТ-безпеки, оскільки включає контроль за інформаційним простором (видалення певного контенту або цілих веб-сайтів загалом тощо), що в свою чергу пов'язане з обмеженням індивідуальних свобод [9, с. 121-122].

Габріеле Фаджолі акцентував увагу на відставанні Італії в галузі цифрових навичок, що продемонстрував індекс DESI Європейської Комісії, яка у «Звіті за 2023 рік» поставила Республіку на передостаннє місце з двадцяти семи країн за базовими цифровими навичками та на останнє місце за випускниками з ІКТ. Частка жінок серед фахівців з ІКТ становить 16%, що значно нижче середнього показника по ЄС – 18,9%. Ситуація з інвестиціями в кібербезпеку наступна: у 2023 році Італія витратила 2,149 мільярда євро, це дорівнює приблизно 0,12% ВВП. Для порівняння такі європейські країни, як Франція та Німеччина, витрачають вдвічі більше; а США – 0,3% ВВП [2, с. 5].

В Італії регуляторна база з питань управління та політики кібербезпеки викладені у двох документах: 1) «Quadro Strategico Nazionale» (QSN), який визначає обов'язки та ролі інституцій, залучених до кібербезпеки; 2) «Piano Nazionale» (PN), який окреслює національні цілі та плани дій для їх досягнення [11]. Разом ці два документи утворюють італійську стратегію кібербезпеки. Перша італійська стратегія кібербезпеки була сформульована в декреті уряду Маріо Монті від 24 січня 2013 року («DPCM Monti»): вперше було окреслено архітектурну основу національної

кібербезпеки та захисту критичної інфраструктури [9, с. 122–123; 4, с. 87]. Управління кібербезпекою здійснює Голова Ради міністрів Італії (Прем'єр-міністр), який відповідає за прийняття Національної стратегічної рамкової програми кібербезпеки та Національного плану кіберзахисту та кібербезпеки. Міжвідомчий комітет з питань безпеки Республіки (Comitato interministeriale per la sicurezza della Repubblica, CISR) надає консультації, регуляторні та організаційні пропозиції. «Декрет» відводив значну роль на операційному рівні Департаменту інформації з безпеки (DIS) та різним агентствам (AISI, AISE, AgID). Крім того, декретом було створено Ядро кібербезпеки (NSC) у складі Військової ради та низку додаткових структур – Міжвідомчого відділу кібернетичних криз (NISP), Наукового комітету, приватних операторів, Національного центру боротьби з інформаційними злочинами з захисту критичної інфраструктури (CNAIPIC) та Групи реагування на комп'ютерні надзвичайні ситуації (CERT) [11, с. 9–12].

Друга італійська стратегія кібербезпеки була опублікована 17 лютого 2017 року як «Декрет Джентілоні» («Decreto Gentiloni») [4, с. 88] після набрання чинності європейської «Директиви про мережеву та інформаційну безпеку (NIS)» і мала на меті впорядкування (зменшення складності) інституційного управління кібербезпекою. Директива NIS набула чинності в італійському законодавстві у формі законодавчого декрету № 65 у червні 2018 року та стимулювала деякі відповідні зміни в італійській інституційній екосистемі кібербезпеки [7, с. 295, вин. 23]. Головною відмінністю від управління кібербезпекою, встановленого у 2013 році, є роль Генерального директора Департаменту безпеки та розвідки (Dipartimento Informazioni per la Sicurezza, DIS), який отримав більш пряму та помітну роль у визначенні загальної політики, спрямованої на покращення безпеки систем та мереж [9, с. 125-126]. Новий План кібербезпеки містив окремий План дій, який передбачав створення Об'єднаного командування кібернетичних операцій (Comando Interforze Operazioni Cibernetiche, CIOC) і пропонував низку нових ініціатив, як от створення національних центрів: 1) досліджень та розробок у галузі кібербезпеки задля аналізу шкідливих програм, управління безпекою, захисту критичної інфраструктури та аналізу загроз; 2) криптографії для встановлення шифрів, розробки національного алгоритму і блокчейну, та оцінки безпеки [9, с. 124]. Президії Ради Міністрів підпорядковується створена відповідно до Директиви NIS італійська команда для реагування на комп'ютерні інциденти («Команда реагування на інциденти комп'ютерної безпеки», CSIRT). Італійська CSIRT налічує 30 фахівців; бюджет з 2019 року складає 700000 євро (початкові інвестиції – 2000000 євро) [9, с. 125].

В розвинених суспільствах до критичної інфраструктури зазвичай відносять банківську справу та фінанси, громадську безпеку та порядок, зв'язок, служби екстреної допомоги, енергетичний сектор (виробництво, транспортування та розподіл), державне управління, системи охорони здоров'я, транспорт та логістика, водопостачання, інформаційні послуги та засоби масової інформації, постачання продуктів харчування. Особливістю Італії протягом значного часу була відсутність офіційного реєстру критичної інфраструктури (КІ). «Декрет» визначив компетентні органи, яким відведена роль моніторингу національного застосування Директиви NIS: 1) Міністерство економічного розвитку (Ministero dello Sviluppo Economico) для енергетичного та цифрового секторів; 2) Міністерство інфраструктури та транспорту для транспортного сектору; 3) Міністерство економіки та фінансів для банківської та фінансово-ринкової інфраструктури; 4) Міністерство охорони здоров'я для медичного сектору; 5) Міністерство навколишнього середовища, захисту земель та моря для постачання та розподілу питної води. «Законодавчий декрет» передбачав включення всіх цих органів до складу Спільного технічного комітету при Президії Ради Міністрів. «Декретом Джентілоні» було створено новий Центр національної оцінки та сертифікації (CVCN) у складі Міністерства економічного розвитку, завданням якого є оцінка безпеки продуктів та послуг для критично важливої національної інфраструктури [9, с. 124-125].

Особливістю Італії певний час була відсутність національних законів чи то будь-яких письмових або чітко сформульованих юридично обов'язкових договорів, що визначають учасників, відповідальність та розподіл ризиків державно-приватного партнерства в сфері захисту критичної інфраструктури від кібератак. Законодавство спрямоване на суб'єкти господарювання, як державні, так і приватні, які надають послуги або виконують важливі функції для держави в секторах, що вважаються найбільш ризикованими (оборона, енергетика, телекомунікації, бізнес та фінанси, транспорт, критичні технології тощо) та потребують посиленої безпеки було підсумовано в Законодавчому указі від 21 вересня 2019 року (DL 105/2019; DL 133/2019) про створення «периметру національної кібербезпеки» («Perimetro di Sicurezza Nazionale Cibernetica») [10, с. 80–82]. Суб'єк-

ти, що входять до «периметра», повинні вживати суворіших заходів безпеки, таких як складання переліку відповідних ІКТ-активів, повідомлення CVCN про придбання ІКТ-активів, систем та послуг, а також повідомлення CSIRT про будь-які інциденти, пов'язані з ІКТ-активами [4, с. 89].

Третя італійська стратегія кібербезпеки була опублікована в 2021 році (DL 82/2021). За останні п'ять років Італія зміцнила свої можливості кіберзахисту шляхом створення Національного агентства кібербезпеки (Agenzia per la cybersicurezza nazionale, ACN), якому було доручено реалізувати Національну стратегію кібербезпеки [4, с. 88-89]. Іншими сферами відповідальності Національного агентства кібербезпеки є координація діяльності з кібербезпеки між державними суб'єктами на національному рівні, впровадження заходів щодо забезпечення кібербезпеки та кіберстійкості для розвитку італійської цифровізації, виробничої системи та державних адміністрацій, а також сприяння національній та європейській автономії щодо ІТ-продуктів та процесів, що мають стратегічне значення для захисту національних інтересів у цій галузі. Агентство відповідно до «Директиви NIS» відповідає за розслідування порушень та накладення адміністративних санкцій.

У травні 2022 року Національне агентство кібербезпеки (ACN) представило «Національну стратегію кібербезпеки на 2022–2026 роки» та «План її впровадження» [12]. «Стратегія» визначає три ключові цілі (захист, реагування та розвиток) та пов'язані з ними заходи, розділені на тематичні області. Дії, пов'язані із захистом, охоплюють такі питання, як контроль технологій, правова база, ситуаційна обізнаність, кіберстійкість державного управління, національна інфраструктура, шифрування та протидія дезінформації. Кризове управління, національні кіберслужби, навчання, атрибуція, боротьба з кіберзлочинністю та можливості стримування – це сфери, на які спрямовані зусилля, пов'язані з реагуванням. Нарешті, ціль розвитку включає дії, пов'язані з Національним центром координації, національним та європейським розвитком технологій, Національним парком безпеки, кіберпростором як фактором конкурентоспроможності та безпечною цифровізацією держави [4, с. 89].

Італійський підхід до кібердипломатії це насамперед орієнтація на міжнародну співпрацю з наданням переваги міжнародним та багатостороннім форумам над двосторонніми домовленостями. Позиція Італії в ОБСЄ полягає в активному просуванні ідеї впровадження «Заходів зміцнення довіри в кіберпросторі» (Постійна рада ОБСЄ, 2013, 2016). Під час головування Італії у Великій сімці у 2017 році (в рамках Кібергрупи G7) було прийнято декларацію про правила відповідальної поведінки держав у кіберпросторі (так звана «Луккська декларація»), яка, серед іншого: 1) визнала переважну роль держав у процесі побудови безпечнішого та стабільнішого кіберсередовища; 2) легітимність декларації має базуватися на діяльності, що здійснюється Генеральною Асамблеєю ООН та ОБСЄ; 3) підкреслила важливість застосування чинного міжнародного права до кіберсфери [9, с. 127].

Висновок: Таким чином, можна стверджувати, що:

1) Італія зробила перші регуляторні кроки щодо кібербезпеки відносно пізно порівняно з іншими європейськими державами;

2) стратегії 2013 («Декрет Монті») і 2018 («Декрет Джентілоні») років стосувалися насамперед формуівння інституційної бази кібербезпеки (централізація структури; прибирання дублюючих функцій);

3) італійська стратегія і створення «національного периметру кібербезпеки» мали на меті впорядкування інституційної екосистеми кібербезпеки відповідно до вимог європейської «Директиви про мережеву та інформаційну безпеку (NIS)»;

4) Італія зміцнила свої можливості управління кібербезпекою та здатність виявляти, аналізувати, оцінювати та керувати ІТ-ризиками за допомогою превентивних та пом'якшувальних заходів створенням Національного агентства кібербезпеки (ACN), якому доручено реалізовувати нову (третю) Національну стратегію кібербезпеки на 2022–2026 роки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Rapporto Clusit sulla sicurezza ICT in Italia e nel mondo. 2025. Milano, 2025. 402 p.
2. Rapporto Clusit 2024 sulla sicurezza ICT in Italia. Milano, 2024. 376 p.
3. Санжарова Г.Ф., Бак В.І., Санжаров В.А. «Цифровий суверенітет» Франції та юридичне підґрунтя національної стратегії кібербезпеки. *Юридичний науковий електронний журнал*. 2025. № 5. С. 42–45. DOI https://doi.org/10.32782/2524-0374/2025-5/8.

4. Gaie C., Karpiuk M., Spaziani A. Cybersecurity in France, Poland and Italy. *Studia Iuridica Lublinensia*. 2025. Vol. 34. (1). S. 73–95. DOI: http://dx.doi.org/ 10.17951/sil.2025.34.1.73-95.
5. 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. DOI https://doi.org/10.32782/2524-0374/2023-9/5.
6. 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. DOI https://doi.org/ 10.33244/2617-4154.3(12).2023.219-227.
7. 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. DOI: https://doi.org/10.1365/ s43439-022-00058-7.
8. Giacomello G. Va Pensiero: The Evolution of Italy's Information Society. *Italy From Crisis To Crisis: Political Economy, Security and Society in the 21st Century*. London-New York: Routledge, 2018. P. 199–218.
9. De Zan T., Giacomello G., Martino L. Italy's cyber security architecture and critical infrastructure. *Routledge Companion to Global Cyber-Security Strategy* / ed. S.N. Romaniuk, M. Manjikian. London-New York: Routledge, 2021. P. 121–131.
10. Шевченко А.Є., Павлюх О.А., Санжаров В.А. Питання кібербезпеки в сучасному італійському законодавстві: національний безпековий периметр. *Наукові тренди постіндустріального суспільства*: матеріали IV Міжнар. наук. конференції, м. Суми, 31 березня 2023 р. Вінниця: Європейська наукова платформа, 2023. С. 80–82. DOI: https://doi.org/10.36074/mcnd-31.03.2023.
11. Piano Nazionale per la protezione cibernetica e la sicurezza informatica, 2017. 36 p. Uhttps://www.governo.it/sites/governo.it/files/piano-nazionale-cyber-2017.pdf (дата звернення: 24.06.2025).
12. Strategia Nazionale di Cybersicurezza 2022–2026. 32 p. URL: https://www.acn.gov.it/portale/documents/20119/87708/ACN_Strategia.pdf/6d98daf1-f3df-91e3-189d-df85f60402b6?t=1704461393347 (access: 9.6.2024).