

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«УЖГОРОДСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ»
ЮРИДИЧНИЙ ФАКУЛЬТЕТ

**НАУКОВИЙ ВІСНИК
УЖГОРОДСЬКОГО НАЦІОНАЛЬНОГО
УНІВЕРСИТЕТУ**

Серія
ПРАВО

Випуск 90

— *Частина 1* —

Ужгород, 2025

Журнал включено до категорії «Б» щодо видань, в яких можуть публікуватися результати дисертаційних робіт на здобуття наукових ступенів доктора і кандидата наук
(Наказ МОН України від 26.11.2020 № 1471 Про затвердження рішень Атестаційної колегії Міністерства від 26 листопада 2020 року та внесення змін до наказів Міністерства освіти і науки України від 2 липня 2020 року № 886, від 24 вересня 2020 року № 1188).

Науковий вісник включено до міжнародної наукометричної бази
Index Copernicus International (Республіка Польща)

ГОЛОВНИЙ РЕДАКТОР:

Бисага Юрій Михайлович – доктор юридичних наук, професор, Заслужений юрист України, завідувач кафедри конституційного права та порівняльного правознавства юридичного факультету ДВНЗ «Ужгородський національний університет».

ЗАСТУПНИКИ ГОЛОВНОГО РЕДАКТОРА:

Белов Дмитро Миколайович – доктор юридичних наук, професор, Заслужений юрист України, професор кафедри конституційного права та порівняльного правознавства юридичного факультету ДВНЗ «Ужгородський національний університет»;

Заборовський Віктор Вікторович – доктор юридичних наук, професор, професор кафедри цивільного права та процесу, директор НДІ теорії та практики правосуддя юридичного факультету ДВНЗ «Ужгородський національний університет»;

ЧЛЕНИ РЕДКОЛЕГІЇ:

Белова Мирослава Володимирівна – доктор юридичних наук, доцент кафедри конституційного права та порівняльного правознавства юридичного факультету ДВНЗ «Ужгородський національний університет»;

Берч Вероніка Вікторівна – кандидат юридичних наук, доцент кафедри конституційного права та порівняльного правознавства юридичного факультету ДВНЗ «Ужгородський національний університет»;

Бисага Юрій Юрійович – кандидат юридичних наук, доцент кафедри правових дисциплін Карпатського університету ім. Августина Волошина;

Брочкова Катаріна – доктор хабілітований, кандидат юридичних наук, доктор філософії (Словацька республіка);

Булеца Сібілла Богданівна – доктор юридичних наук, професор, завідувач кафедри цивільного права та процесу юридичного факультету ДВНЗ «Ужгородський національний університет»;

Гарагонич Олександр Васильович – доктор юридичних наук, доцент, професор кафедри господарського права та господарського процесу Інституту права Київського національного університету імені Тараса Шевченка;

Гомонай Василь Васильович – доктор юридичних наук, доцент, доцент кафедри конституційного права та порівняльного правознавства юридичного факультету ДВНЗ «Ужгородський національний університет»;

Греца Ярослав Васильович – доктор юридичних наук, доцент, доцент кафедри господарського права юридичного факультету ДВНЗ «Ужгородський національний університет»;

Дешко Людмила Миколаївна – доктор юридичних наук, професор, професор кафедри конституційного права Інституту права Київського національного університету імені Тараса Шевченка;

Жежсихова Мартина – кандидат юридичних наук, доцент Університету імені П.Й.Шафарика (м. Кошице, Словацька Республіка);

Ковач Юліус – доктор юридичних наук, професор, проректор Панєвропської високої школи (м. Братіслава, Словацька Республіка);

Кучарик Рудольф – доктор філософії (Словацька Республіка);

Лазур Ярослав Володимирович – доктор юридичних наук, професор, декан юридичного факультету ДВНЗ «Ужгородський національний університет»;

Манзюк Василь Васильович – кандидат юридичних наук, доцент, доцент кафедри господарського права юридичного факультету ДВНЗ «Ужгородський національний університет»;

Мендєшул Марія Василівна – доктор юридичних наук, доцент, професор кафедри цивільного права та процесу юридичного факультету ДВНЗ «Ужгородський національний університет»;

Мраз Станіслав – доктор юридичних наук, професор, ректор Університету Данубіус (м. Сладковічево, Словацька Республіка);

Ондрова Юлія – кандидат юридичних наук, доцент Університету імені П.Й. Шафарика (м. Кошице, Словацька Республіка);

Палінчак Микола Михайлович – доктор політичних наук, професор, декан факультету міжнародних економічних відносин ДВНЗ «Ужгородський національний університет»;

Рогач Іван – кандидат юридичних наук, доцент, юридичний факультет Університету Данубіус (м. Сладковічево, Словацька Республіка);

Рогач Олександр Янович – доктор юридичних наук, професор, проректор з науково-педагогічної роботи ДВНЗ «Ужгородський національний університет»;

Фрідманський Роман Михайлович – кандидат юридичних наук, професор кафедри конституційного права та порівняльного правознавства юридичного факультету ДВНЗ «Ужгородський національний університет»;

Чечерський Віктор Іванович – доктор юридичних наук, офіс Генерального прокурора.

Рекомендовано до друку та поширення через мережу Internet
Вченою радою Державного вищого навчального закладу
«Ужгородський національний університет», протокол № 09 від 29.08.2025 р.

Свідectво про державну реєстрацію друкованого засобу масової інформації серія KB № 21500-11300Р,
видане Державною реєстраційною службою України 24.11.2014 р. Офіційний сайт видання: <https://visnyk-juris-uzhnu.com/>

ЗМІСТ

РОЗДІЛ 1. ТЕОРІЯ ТА ІСТОРІЯ ДЕРЖАВИ І ПРАВА; ІСТОРІЯ ПОЛІТИЧНИХ І ПРАВОВИХ ВЧЕНЬ

Арабаджи Н.Б., Згама А.О. КОНЦЕПТУАЛЬНІ ЗАСАДИ ГЕНЕЗИ СУЧАСНОГО ПАРЛАМЕНТАРИЗМУ: ІНТЕГРАЦІЯ ЄВРОПЕЙСЬКИХ ЦІННОСТЕЙ У НАЦІОНАЛЬНИЙ КОНСТИТУЦІОНАЛІЗМ.....	9
Бундак О.А. ЕВОЛЮЦІЯ ПРИНЦИПУ ПОДІЛУ ВЛАДИ В ДЕРЖАВНОМУ ПРАВІ ЗАРУБІЖНИХ КРАЇН.....	15
Волохов О.С. МІЖНАРОДНІ СТАНДАРТИ ПРАВОТВОРЧОСТІ: ПОНЯТТЯ ТА КЛАСИФІКАЦІЇ.....	22
Волошкевич Г.А. СТАНОВЛЕННЯ СЛУЖБИ ПРОБАЦІЇ У ЮВЕНАЛЬНИХ СУДАХ (ДРУГА ПОЛОВИНА ХІХ – ПОЧАТОК ХХ СТОЛІТТЯ).....	29
Гришко В.І., Цевух А.І. АФІНСЬКА ДЕМОКРАТІЯ: ПРАВО ГОЛОСУ, СУД ПРИСЯЖНИХ ТА ВИБОРЧІ МЕХАНІЗМИ.....	36
Гутів Б.І. ЗАКОНОДАВЧА ФУНКЦІЯ ВЕЛИКОГО КНЯЗЯ КИЇВСЬКОЇ РУСІ.....	42
Добренька Н.В., Новак Я.В., Сидоренко В.В. ОСНОВИ ЗАХИСТУ ПРАВ ВІЙСЬКОВОСЛУЖБОВЦІВ ТА ЇХ РОДИН ПІД ЧАС ВІЙНИ В УКРАЇНІ.....	48
Долянська І.М. ГНУЧКІСТЬ ТА АДАПТИВНІСТЬ НОРМ ПРАВА В КОНТЕКСТІ ЮРИДИЧНОЇ ТЕХНІКИ.....	53
Іванов В.П. ЮРИДИЧНІ НАСЛІДКИ ЗЛОВЖИВАННЯ МАТЕРІАЛЬНИМ ПРАВОМ.....	60
Колодій А.М., Колодій О.А., Хальота А.І. МОДЕЛЬНА ПРАВОТВОРЧІСТЬ В УКРАЇНІ: СУЧАСНІСТЬ ТА ПЕРСПЕКТИВИ.....	69
Корженко О.М. КОНЦЕПТУАЛЬНІ ЗАСАДИ НАЦІОНАЛЬНО-ПАТРІОТИЧНОГО ВИХОВАННЯ ПОЛІЦЕЙСЬКИХ У СИСТЕМІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ.....	78
Кривицький Ю.В. МЕТОДОЛОГІЯ ДОСЛІДЖЕННЯ ПРАВОВОЇ РЕФОРМИ: СПРОБА ОПИСУ ГНОСЕОЛОГІЧНОЇ МОЗАЇКИ.....	85
Кротюк О.В. ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ПЛАНУВАННЯ ПРАВОТВОРЧОСТІ В УКРАЇНІ: СТАН ТА ПЕРСПЕКТИВИ УДОСКОНАЛЕННЯ.....	94
Лисенко І.В., Кузьменко О.В., Гаряєва Г.М. АКТУАЛЬНІ ПИТАННЯ ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ В ЮРИДИЧНІЙ ДІЯЛЬНОСТІ.....	100
Марич Н.І. ПРАВО НА ЗАМІНУ ВИКОНАННЯ ОКРЕМИХ ЮРИДИЧНИХ ОБОВ'ЯЗКІВ, НЕСУМІСНИХ ІЗ РЕЛІГІЙНИМИ ЧИ ІНШИМИ ПЕРЕКОНАННЯМИ ЛЮДИНИ: ЗАГАЛЬНОТЕОРЕТИЧНИЙ АСПЕКТ.....	107
Панасюк О.П. КОРУПЦІЯ ТА ЇЇ СОЦІАЛЬНО-ПРАВОВИЙ ВИМІР У НАЦІОНАЛЬНОМУ ТА МІЖНАРОДНОМУ КОНТЕКСТІ.....	117

Санжарова Г.Ф., Сіренко О.В., Санжаров В.А. ІТАЛІЙСЬКА КІБЕРБЕЗПЕКОВА АРХІТЕКТУРА: ЗАХИСТ КРИТИЧНОЇ ІНФРАСТРУКТУРИ, ТЕХНІЧНІ, ПРАВОВІ ТА ІНСТИТУЦІЙНІ НОВОВВЕДЕННЯ.....	124
Саранчук О.В. ФОРМИ УЧАСТІ НАСЕЛЕННЯ У ЗДІЙСНЕННІ ПРАВОСУДДЯ В РОСІЙСЬКІЙ ІМПЕРІЇ ХІХ СТОЛІТТЯ НА ПРИКЛАДІ ВОЛОСНИХ СУДІВ ТА ОРГАНІВ МІСЦЕВОГО САМОВРЯДУВАННЯ ПІВДНЯ УКРАЇНИ.....	130
Стаднік І.В., Михайліна Т.В. СПРАВЕДЛИВІСТЬ ЯК ОСНОВОПОЛОЖНИЙ ПРАВОВИЙ ПРИНЦИП: ІСТОРИЧНА ЕВОЛЮЦІЯ ТА СУЧАСНЕ ЗНАЧЕННЯ.....	137
Степаненко Н.В. ВЖИВАННЯ СПЕЦІАЛЬНОЇ ТЕРМІНОЛОГІЇ, ДЕТАЛІЗАЦІЯ ТА СИСТЕМНІСТЬ ВИКЛАДУ НОРМАТИВНОГО МАТЕРІАЛУ ЯК ЗАСОБИ ЗАБЕЗПЕЧЕННЯ ЧІТКОСТІ ЗМІСТУ НОРМ ПРАВА В ЮРИДИЧНІЙ ТЕХНІЦІ.....	149
Сухонос В.В. ГРОМАДЯНСЬКЕ СУСПІЛЬСТВО ЯК СУБ'ЄКТ ЗАБЕЗПЕЧЕННЯ МІЖНАРОДНОЇ ТЕХНІЧНОЇ ДОПОМОГИ: ПОЛІТИКО-ПРАВОВИЙ ТА ІСТОРИЧНИЙ ВИМІРИ.....	155
Тараконич Т.І. УПОРЯДКУВАННЯ ЗАКОНОДАВСТВА: ДОКТРИНАЛЬНИЙ ПІДХІД.....	163
Токарчук О.В. КОНЦЕПТУАЛЬНІ ЗАСАДИ СОЦІАЛЬНО-ДЕМОГРАФІЧНОЇ БЕЗПЕКИ: НАЦІОНАЛЬНИЙ ВИМІР.....	169
Федушак-Паславська Г.М. ПРИРОДНО-ПРАВОВА КОНЦЕПЦІЯ – ГЕНЕРАТОР ЦІННОСТЕЙ ЄВРОПЕЙСЬКОЇ ІДЕНТИЧНОСТІ.....	175
Якименко Т.С. СУДОВІ ДЕФЕРАНСИ (JUDICIAL DEFERENCE) ТЛУМАЧЕННЯМ АДМІНІСТРАТИВНИХ ОРГАНІВ У США ТА ВИСНОВКИ ДЛЯ УКРАЇНИ: ЧИ ПОВАЖАЮТЬ СУДДІ ЗАКОНОДАВЦЯ?.....	181
Ярмол Л.В., Олійник Я.С. ЮРИДИЧНИЙ МЕХАНІЗМ ЗАБЕЗПЕЧЕННЯ ПРАВ ЛЮДИНИ В УКРАЇНІ: ПОНЯТТЯ, ЕЛЕМЕНТИ, СТАН І НАПРЯМИ ВДОСКОНАЛЕННЯ.....	206
РОЗДІЛ 2. КОНСТИТУЦІЙНЕ ПРАВО; МУНІЦИПАЛЬНЕ ПРАВО	
Бадида А.Ю. «ПРІОРИТЕТНЕ ПИТАННЯ КОНСТИТУЦІЙНОСТІ» VS «КОНСТИТУЦІЙНА СКАРГА»: У ПОШУКУ ЕФЕКТИВНОСТІ ІНСТИТУТІВ.....	213
Батанов О.В. СТАНОВЛЕННЯ ТА ФУНКЦІОНУВАННЯ ІНСТИТУТУ ДИТЯЧОГО ОМБУДСМАНА У КОНТЕКСТІ ЮВЕНАЛІЗАЦІЇ КОНСТИТУЦІЙНОГО ПРАВА.....	219
Голуб В.К. ПОНЯТТЯ, СУТНІСТЬ ТА СУБ'ЄКТИ КОНСТИТУЦІЙНОГО ПРАВА НА АЛЬТЕРНАТИВНУ (НЕВІЙСЬКОВУ) СЛУЖБУ.....	228
Гончар О.О. НАЛЕЖНА КВАЛІФІКАЦІЯ ЯК ВИЗНАЧАЛЬНА ВИМОГА ДО КАНДИДАТА НА ПОСАДУ СУДДІ КОНСТИТУЦІЙНОГО СУДУ УКРАЇНИ.....	238
Гришко Л.М. ДЕЯКІ ПИТАННЯ ВИЗНАЧЕННЯ МЕТИ ЗАБЕЗПЕЧЕННЯ РЕПРОДУКТИВНИХ ПРАВ ЛЮДИНИ.....	248

Жмакін С.А. УДОСКОНАЛЕННЯ ПРАВОВИХ МЕХАНІЗМІВ РЕАЛІЗАЦІЇ ПОВНОВАЖЕНЬ УПОВНОВАЖЕНОГО ВЕРХОВНОЇ РАДИ УКРАЇНИ З ПРАВ ЛЮДИНИ У СФЕРІ ЗАХИСТУ ЕКОЛОГІЧНИХ ПРАВ.....	256
Завальнюк С.В. КОНСТИТУЦІЙНИЙ СУД УКРАЇНИ ЯК ІНСТИТУТ ПОДОЛАННЯ ПРАВОВИХ ПРОГАЛИН У НАЦІОНАЛЬНІЙ ПРАВОВІЙ СИСТЕМІ.....	262
Захарчук І.В. ЦИФРОВІ ПРАВА ГРОМАДЯН УКРАЇНИ: КОНСТИТУЦІЙНО-ПРАВОВЕ ЗАКРІПЛЕННЯ ТА МЕХАНІЗМИ РЕАЛІЗАЦІЇ.....	268
Кириченко Ю.В., Шулежко І.А. ПРАВО ГРОМАДЯН НА СОЦІАЛЬНИЙ ЗАХИСТ В УКРАЇНІ ТА ЄВРОПЕЙСЬКИХ ДЕРЖАВАХ: ПОРІВНЯЛЬНО-ПРАВОВІ АСПЕКТИ КОНСТИТУЦІЙНОГО РЕГУЛЮВАННЯ.....	274
Коваль Т.В. ОБМЕЖЕННЯ ЩОДО ВНЕСЕННЯ ЗМІН ДО КОНСТИТУЦІЇ: ПОРІВНЯЛЬНО-ПРАВОВИЙ АСПЕКТ.....	279
Котенджи Е.О. КОНСТИТУЦІЙНІ ГАРАНТІЇ ТА ЮРИДИЧНИЙ ЗАХИСТ ПРАВА НА ЖИТЛО В УМОВАХ ПОВНОМАСШТАБНОЇ ЗБРОЙНОЇ АГРЕСІЇ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ ПРОТИ УКРАЇНИ: МІЖ ПРАВОМ І РЕАЛЬНІСТЮ.....	285
Кузнєцов А.С. ВЕРХОВЕНСТВО ПРАВА ЯК ПРИНЦИП МУНІЦИПАЛЬНОЇ ПРАВОТВОРЧОСТІ.....	294
Марцеляк О.В. ДЕЦЕНТРАЛІЗАЦІЯ ВЛАДИ ЯК ПРІОРИТЕТНИЙ НАПРЯМ СУЧАСНОГО ВІТЧИЗНЯНОГО ДЕРЖАВОТВОРЕННЯ.....	301
Монастирський М.В. ДИСТАНЦІЙНЕ ГОЛОСУВАННЯ УКРАЇНСЬКИХ ГРОМАДЯН ЗА КОРДОНОМ НА ПЕРШИХ ПОВОЄННИХ ВИБОРАХ І РЕФЕРЕНДУМІ ПРО ВСТУП УКРАЇНИ ДО ЄВРОПЕЙСЬКОГО СОЮЗУ.....	308
Омелько І.І. КОНСТИТУЦІЙНЕ ЗАКРІПЛЕННЯ ПРИНЦИПУ ВЗАЄМОДІЇ ГІЛОК ВЛАДИ: ДОСВІД УКРАЇНИ І ЗАРУБІЖНИХ КРАЇН.....	314
Павлович-Сенета Я.П., Лозинський Ю.Р. СТАНОВЛЕННЯ ТА ПЕРСПЕКТИВИ РОЗВИТКУ МІСЦЕВОГО САМОВРЯДУВАННЯ В УКРАЇНІ.....	321
Середа І.Л. ПЕРСОНАЛЬНІ ДАНІ В УМОВАХ ВОЄННОГО СТАНУ: КОНСТИТУЦІЙНО-ПРАВОВІ ОБМЕЖЕННЯ ТА ГАРАНТІЇ.....	327
Туряниця В.В. ПРАВОВЕ ЗАКРІПЛЕННЯ НОВОЇ СУТІ ПОНЯТЬ ІНОЗЕМНА МОВА, МОВА ВОРОГА, ВОРОЖА МОВА ТА ЇХ ТРАКТУВАННЯ В НАЦІОНАЛЬНИХ ЗАКОНОДАВСТВАХ ПОСТРАДІАНСЬКИХ РЕСПУБЛІК.....	336
Фурса С.Я., Фурса Є.І., Регушевський Е.Є. КОНСТИТУЦІЯ УКРАЇНИ ТА МЕХАНІЗМ ЗАБЕЗПЕЧЕННЯ ЇЇ ДІЄВОСТІ (НА ПРИКЛАДІ ЗАХИСТУ ПРАВ ЛЮДИНИ У КОНСТИТУЦІЙНОМУ ТА ЦИВІЛЬНОМУ СУДОЧИНСТВІ).....	342
Чепис О.І. ВІРТУАЛЬНА ІДЕНТИЧНІСТЬ В КОНТЕКСТІ ПРАВ ЛЮДИНИ.....	349

CONTENTS

SECTION 1. THEORY AND HISTORY OF THE LAW AND THE STATE; HISTORY OF POLITICAL AND LEGAL DOCTRINES

Arabadji N.B., Zghama A.O. CONCEPTUAL FOUNDATIONS OF THE GENESIS OF MODERN PARLIAMENTARISM: INTEGRATION OF EUROPEAN VALUES INTO NATIONAL CONSTITUTIONALISM.....	9
Bundak O.A. THE EVOLUTION OF THE PRINCIPLE OF SEPARATION OF POWERS IN THE PUBLIC LAW OF FOREIGN COUNTRIES.....	15
Volokhov O.S. INTERNATIONAL STANDARDS OF LAW-MAKING: THE CONCEPT AND CLASSIFICATIONS.....	22
Voloshkevych H.A. FORMATION OF PROBATION SERVICE IN JUVENILE COURTS IN THE SECOND HALF OF THE 19TH – EARLY 20TH CENTURY.....	29
Grishko V.I., Tsevukh A.I. ATHENIAN DEMOCRACY: THE RIGHT TO VOTE, JURY TRIAL AND ELECTORAL MECHANISMS.....	36
Hutiv B.I. THE LEGISLATIVE FUNCTION OF THE GRAND PRINCE OF KYIVAN RUS.....	42
Dobrenka N.V., Novak Y.V., Sydorenko V.V. FUNDAMENTALS OF PROTECTING THE RIGHTS OF MILITARY PERSONNEL AND THEIR FAMILIES DURING THE WAR IN UKRAINE.....	48
Dolianovska I.M. FLEXIBILITY AND ADAPTABILITY OF LEGAL NORMS IN THE CONTEXT OF LEGAL TECHNIQUE.....	53
Ivanov V.P. LEGAL CONSEQUENCES OF ABUSE OF SUBSTANTIVE RIGHTS.....	60
Kolodiy A.M., Kolodiy O.A., Khalota A.I. MODEL LAWMAKING IN UKRAINE: MODERNITY AND PROSPECTS.....	69
Korzhenko O.M. CONCEPTUAL FOUNDATIONS OF NATIONAL-PATRIOTIC EDUCATION OF POLICE OFFICERS IN THE SYSTEM OF NATIONAL SECURITY OF UKRAINE.....	78
Kryvytskyi Y.V. METHODOLOGY OF LAW REFORM RESEARCH: AN ATTEMPT TO DESCRIBE THE EPISTEMOLOGICAL MOSAIC.....	85
Krotyuk O.V. LEGAL SUPPORT FOR THE PLANNING OF LAWMAKING IN UKRAINE: CURRENT STANCE AND PERSPECTIVE FOR IMPROVEMENT.....	94
Lysenko I.V., Kuzmenko O.V., Gariaieva G.M. CURRENT ISSUES OF USING ARTIFICIAL INTELLIGENCE TECHNOLOGY IN LEGAL ACTIVITIES.....	100
Marych N.I. THE RIGHT TO SUBSTITUTE THE FULFILLMENT OF CERTAIN LEGAL OBLIGATIONS THAT ARE INCOMPATIBLE WITH A PERSON'S RELIGIOUS OR OTHER BELIEFS: A GENERAL THEORETICAL ASPECT.....	107
Panasiuk O.P. CORRUPTION AND ITS SOCIO-LEGAL DIMENSION IN THE NATIONAL AND INTERNATIONAL CONTEXT.....	117

Sanzharova G.F., Sirenko O.V., Sanzharov V.A. ITALIAN CYBERSECURITY ARCHITECTURE: PROTECTION OF CRITICAL INFRASTRUCTURE, TECHNICAL, LEGAL AND INSTITUTIONAL INNOVATIONS.....	124
Saranchuk O.V. FORMS OF PUBLIC PARTICIPATION IN THE ADMINISTRATION OF JUSTICE IN THE RUSSIAN EMPIRE IN THE 19TH CENTURY: THE CASE OF VOLOST' COURTS AND LOCAL SELF-GOVERNMENT IN SOUTHERN UKRAINE.....	130
Stadnik I.V., Mikhailina T.V. JUSTICE AS A FOUNDATIONAL LEGAL PRINCIPLE: HISTORICAL EVOLUTION AND CONTEMPORARY RELEVANCE.....	137
Stepanenko N.V. THE USE OF SPECIAL TERMINOLOGY, DETAILING, AND SYSTEMATIC PRESENTATION OF NORMATIVE MATERIAL AS MEANS OF ENSURING THE CLARITY OF LEGAL NORMS IN LEGAL DRAFTING TECHNIQUE.....	149
Sukhonos V.V. CIVIL SOCIETY AS AN ENTITY OF PROVIDING INTERNATIONAL TECHNICAL ASSISTANCE: POLITICAL, LEGAL AND HISTORICAL DIMENSIONS.....	155
Tarakhonich T.I. STREAMLINING LEGISLATION: A DOCTRINAL APPROACH.....	163
Tokarchuk O.V. CONCEPTUAL FOUNDATIONS OF SOCIO-DEMOGRAPHIC SECURITY: THE NATIONAL DIMENSION.....	169
Fedushchak-Paslavska H.M. THE NATURAL LAW CONCEPT AS A GENERATOR OF EUROPEAN IDENTITY VALUES.....	175
Yakymenko T.S. JUDICIAL DEFERENCE TO ADMINISTRATIVE INTERPRETATIONS IN THE USA AND CONCLUSIONS FOR UKRAINE: DO JUDGES RESPECT LAWMAKERS?.....	181
Yarmol L.V., Oliinyk Ya.S. LEGAL MECHANISM FOR ENSURING HUMAN RIGHTS IN UKRAINE: CONCEPT, ELEMENTS, STATUS, AND AREAS FOR IMPROVEMENT.....	206
SECTION 2. CONSTITUTIONAL LAW; MUNICIPAL LAW	
Badyda A.Yu. “PRIORITY QUESTION OF CONSTITUTIONALITY” VS “CONSTITUTIONAL COMPLAINT”: IN SEARCH OF THE EFFECTIVENESS OF INSTITUTIONS.....	213
Batanov O.V. THE FORMATION AND FUNCTIONING OF THE INSTITUTION OF THE OMBUDSMAN FOR CHILDREN IN THE CONTEXT OF THE JUVENILISATION OF CONSTITUTIONAL LAW.....	219
Holub V.K. CONCEPT, ESSENCE AND SUBJECTS OF THE CONSTITUTIONAL RIGHT TO ALTERNATIVE (NON-MILITARY) SERVICE.....	228
Honchar O.O. PROPER QUALIFICATION AS A DEFINITIVE REQUIREMENT FOR CANDIDATES TO THE POSITION OF JUDGE OF THE CONSTITUTIONAL COURT OF UKRAINE.....	238

Hryshko L.M. SOME ISSUES OF DETERMINING THE GOAL OF ENSURING HUMAN REPRODUCTIVE RIGHTS.....	248
Zhmakin, S.A. IMPROVING LEGAL MECHANISMS FOR EXERCISING THE POWERS OF THE UKRAINIAN PARLIAMENT COMMISSIONER FOR HUMAN RIGHTS IN ENVIRONMENTAL PROTECTION.....	256
Zavalniuk S.V. THE CONSTITUTIONAL COURT OF UKRAINE AS AN INSTITUTION FOR OVERCOMING LEGAL GAPS IN THE NATIONAL LEGAL SYSTEM.....	262
Zakharchuk I.V. DIGITAL RIGHTS CITIZENS OF UKRAINE: CONSTITUTIONAL AND LEGAL ENTRENCHMENT AND IMPLEMENTATION MECHANISMS.....	268
Kyrychenko Y.V., Shulezhko I.A. THE RIGHT OF CITIZENS TO SOCIAL PROTECTION IN UKRAINE AND EUROPEAN STATES: COMPARATIVE LEGAL ASPECTS OF CONSTITUTIONAL REGULATION.....	274
Koval T.V. LIMITATIONS ON AMENDMENTS TO THE CONSTITUTION: A COMPARATIVE LEGAL ASPECT.....	279
Kotendzhy E.O. CONSTITUTIONAL GUARANTEES AND LEGAL PROTECTION OF THE RIGHT TO HOUSING UNDER THE CONDITIONS OF THE FULL-SCALE ARMED AGGRESSION OF THE RUSSIAN FEDERATION AGAINST UKRAINE: BETWEEN LAW AND REALITY.....	285
Kuznietsov A.S. THE RULE OF LAW AS A PRINCIPLE OF MUNICIPAL LAWMAKING.....	294
Martselyak O.V. DECENTRALIZATION OF POWER AS A PRIORITY DIRECTION OF MODERN DOMESTIC STATE-BUILDING.....	301
Monastyrskiy M.V. REMOTE VOTING OF UKRAINIAN CITIZENS ABROAD IN THE FIRST POST-WAR ELECTIONS AND REFERENDUM ON UKRAINE'S ACCESSION TO THE EUROPEAN UNION.....	308
Omelko I.I. CONSTITUTIONAL CONSOLIDATION OF THE PRINCIPLE OF INTERACTION BETWEEN BRANCHES OF POWER: THE EXPERIENCE OF UKRAINE AND FOREIGN COUNTRIES.....	314
Pavlovych-Seneta Ya.P., Lozynsky Yu.R. FORMATION AND PROSPECTS FOR THE DEVELOPMENT OF LOCAL SELF-GOVERNMENT IN UKRAINE.....	321
Sereda I.L. PERSONAL DATA UNDER MARTIAL STATE: CONSTITUTIONAL AND LEGAL RESTRICTIONS AND GUARANTEES.....	327
Turyanitsa V.V. LEGAL CONSOLIDATION OF THE NEW ESSENCE OF THE CONCEPTS OF FOREIGN LANGUAGE, ENEMY LANGUAGE, HOSTILE LANGUAGE AND THEIR INTERPRETATION IN THE NATIONAL LEGISLATION OF POST-SOVIET REPUBLICS.....	336
Fursa S.Ya., Fursa E.I., Regushevsky E.Ye. CONSTITUTION OF UKRAINE AND THE MECHANISM FOR ENSURING ITS EFFECTIVENESS (ON THE EXAMPLE OF HUMAN RIGHTS PROTECTION IN CONSTITUTIONAL AND CIVIL PROCEEDINGS).....	342
Chepis O.I. VIRTUAL IDENTITY IN THE CONTEXT OF HUMAN RIGHTS.....	349

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 університету 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 впорядкування 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 односторонню 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 зростає 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 посиленням 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 заходів 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 Мартіно (Martino), П'єр Джорджо К'яра (Chiara), Андреа Спаціани (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 розвинутою 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 IT-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 (KI). «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 формування 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](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. U<https://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).