УДК 004.056.53:006.03:351.86

DOI: https://doi.org/10.32782/2413-2675/2024-58-9

Босак І.М.
аспірант кафедри теоретичної та прикладної економіки,
Інститут адміністрування, державного управління та професійного розвитку
Національного університету «Львівська політехніка»
ORCID: https://orcid.org/0009-0000-7880-9043
Bosak Ivan
Institute of Public Administration, Governance and Professional Development
of Lviv Polytechnic National University

Данилович-Кропивницька М.Л.
к.е.н, доцент,
доцент кафедри теоретичної та прикладної економіки,
Інститут адміністрування, державного управління та професійного розвитку
Національного університету «Львівська політехніка»
ORCID: https://orcid.org/0000-0003-3963-5524
Danylovych-Kropyvnytska Marta
Institute of Public Administration, Governance and Professional Development
of Lviv Polytechnic National University

АНАЛІЗ СВІТОВОГО ДОСВІДУ ФОРМУВАННЯ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В КОНТЕКСТІ ПУБЛІЧНОГО УПРАВЛІННЯ

ANALYSIS OF THE WORLD EXPERIENCE OF FORMING AN INFORMATION SECURITY SYSTEM IN THE CONTEXT OF PUBLIC ADMINISTRATION

Анотація. Стаття присвячена питанням забезпечення функцій публічного управління інформаційною безпекою в умовах сучасних викликів. Процеси інформатизації охопили всі сфери життєдіяльності людини, що призвело до виникнення нових загроз. У сучасному світі, де електронні технології стають необхідністю для забезпечення ефективності функцій публічного управління, питання інформаційної безпеки є ключовим і актуальним. У статті досліджено тенденції розвитку публічного управління інформаційною безпекою як ключового механізму забезпечення безпеки держави. Визначено питання інформаційної безпеки як елемента державної оборонної політики, що має особливу актуальність в умовах повномасштабної військової агресії. Уточнено місце та роль системи регулювання інформаційного забезпечення процесів управління на державному рівні. Достатню увагу приділено особливостям забезпечення інформаційної безпеки у публічному управлінні через аналіз сучасних інформаційних загроз. Розглядаючи світовий досвід, було виявлено ключові чинники успіху та проблеми, з якими стикаються органи державного управління у їх подоланні.

Ключові слова: публічне управління, інформаційна безпека, кіберзагрози, інформатизація, кібербезпека.

Постановка проблеми. Розвиток новітніх інформаційних технологій вимагає постійного удосконалення показників захищеності інформаційних ресурсів у суб'єктів публічного управління, а також можливостей інформаційних технологій та програмних засобів, що використовуються при забезпеченні інформаційної безпеки. Недосконалі та застарілі механізми публічного управління інформаційною безпекою, недостатність науково обґрунтованих методів і технологічних рішень для вдосконалення цієї системи призводить до непоправних наслідків як для держави, так і для громадян.

Інформаційна безпека є основою реалізації функцій публічного управління, оскільки в умовах сучасного інформаційного суспільства всі напрями державної політики мають бути захищені. Інформаційне забезпечення процесів є основою формування суспільного розвитку

у XXI столітті, отже ефективність процесів публічного управління має пряму залежність від можливості держави забезпечувати захист та ефективну систему управління інформацією. Проблеми інформаційної безпеки на сьогодні актуалізуються значним зростанням ролі накопичення, обробки та поширення інформації, зокрема, в ухваленні стратегічних, військових, політичних та економічних рішень. У зв'язку з цим набуває актуальності питання про те, наскільки сучасна система публічного управління здатна відповідати на виклики, поставлені глобальною діджиталізацією.

Аналіз останніх досліджень і публікацій. Загальні питання безпеки висвітлювали в своїх працях В. Антипенко, О. Бєглий, І. Лукашук, А. Назаренко, Л. Тимченко та інші. Правові засади забезпечення національної безпеки на сучасному етапі вивчав В. Антонов.

Різні аспекти забезпечення інформаційної безпеки держави загалом та окремих її складових досліджували вчені: В. Дудикевич, І. Опірський, П. Гаранюк, В. Зачепило, А. Партика та інші. Також К. Захаренко досліджував інформаційну безпеку як базову складову управління в рамках сучасних світових ринків та процесів цифрової трансформації економіки.

У працях В. Новородовського розглядаються основні виклики і загрози для національної безпеки України з розвитком інформаційних технологій в умовах російсько-української війни.

Питання інформаційної війни вивчали західні науковці K. Wesolowski, C. Perez, A. Nair, F. Paziuk, B. Lewis, G. Wilde, J. Sherman.

З точки зору предмету дослідження недостатньо вивченими залишаються питання публічного управління інформаційною безпекою держави та окремих її елементів.

Метою роботи є дослідження особливостей забезпечення інформаційної безпеки у публічному управлінні, аналіз сучасних загроз та досвіду інших країн у їх подоланні.

Виклад основного матеріалу. Сьогодні інтенсивна інформатизація доторкнулася всіх сфер життя суспільства і є одним з найбільш визначальних глобальних чинників подальшого соціально-економічного, інтелектуального та духовного розвитку людства. Разом з тим, світова спільнота вступає в новий етап своєї історії, який має всі підстави характеризуватись як епоха інформаційних війн.

Інформаційна складова також є ключовим елементом війни російської федерації проти нашої держави. Це створює реальні загрози національній безпеці України, оскільки вітчизняна інформаційна інфраструктура на тимчасово окупованих територіях цілеспрямовано руйнується, здійснюються кібератаки проти України, а канали для поширення інформації про актуальну суспільно-політичну ситуацію в країні блокуються. Крім того, деструктивні інформаційні операції проводяться на тлі розгортання потужної пропагандистської кампанії проти України, спрямованої, зокрема, на недопущення реалізації цивілізаційного вибору українського суспільства. Тому, в умовах стрімкого розвитку інформаційного суспільства та глобального інформаційного простору, а також широкого використання інформаційно-комунікаційних технологій в усіх сферах життя, проблеми інформаційної безпеки набувають особливого значення. У той же час, Україна розглядає питання створення комплексної системи оцінки інформаційних загроз та оперативного реагування на них одним із стратегічних пріоритетів забезпечення інформаційної безпеки, особливо це стосується сфери публічного управління.

Поняття публічного управління інформаційною безпекою можна визначити як процес керування заходами, спрямованими на захист конфіденційної інформації від несанкціонованого доступу, використання, розголошення та знищення на рівні держави, організацій або громадян. Цей процес може включати створення відповідних законодавчих актів, установлення відповідних органів контролю та нагляду, проведення навчань та тренінгів з питань інформаційної безпеки, а також встановлення відповідних технологій та систем безпеки для захисту конфіденційної інформації. Метою публічного управління інформаційною безпекою є забезпечення безпеки конфіденційної інформації від потенційних загроз, таких як кібератаки, віруси, шпигунське та інше шкідливе програмне забезпечення [1].

Однак, публічне управління інформаційною безпекою може також здійснюватися на рівні окремих організацій або громадян. Це може включати створення відповідних політик та процедур управління інформаційною безпекою, проведення навчань та тренінгів з питань інформаційної безпеки, а також встановлення відповідних технологій та систем безпеки для захисту конфіденційної інформації [2–3].

Сфера державного управління є важливим виробником інформації, оскільки тут поширюється правова, економічна, статистична, політична, наукова та інші види інформації, а також збираються та обробляються дані про юридичних та фізичних осіб. Споживачами інфор-

мації є державні інституції, приватні компанії та громадяни.

Інформатизація сфери публічного управління має свої недоліки. По-перше, можливість втрати інформації, яку в більшості випадків можна усунути за допомогою заходів захисту. По-друге, використання спеціальних навичок, іноді високого рівня складності, для роботи з відповідним програмним забезпеченням, які можливо забезпечити за допомогою навчання. Проблеми, з якими стикаються публічні адміністрації на різних стадіях інформатизації процесів, залежать не лише від фактичних технологічних інструментів. Інформатизація державного сектору має розглядатися з цілісної точки зору: політичної, адміністративної та культурної складових.

Очевидно, що технологічно більш розвинені країни водночас є більш вразливими в інформаційному просторі. В умовах широкої мережевої інтеграції зростає взаємозв'язок і взаємозалежність інформаційних просторів держав. Саме тому питання протидії загрозам в інформаційній сфері має як національний, так і глобальний вимір.

Важливо зазначити, що міжнародна спільнота ще не прийшла до спільного розуміння ключових термінів з інформаційної безпеки в сфері державного управління. Країни по-різному трактують та визначають її межі. Можна виділити два основні підходи до визначення інформаційної безпеки: широкий та вузький. Згідно з широким, поняття інформаційної безпеки включає в себе як інформаційно-технічний, так і інформаційно-психологічний аспекти. Такий підхід відповідає баченню країн пострадянського простору, Китаю та низки інших держав. Вони визначають інформаційну безпеку як стан захищеності особи, суспільства і держави та їхніх інтересів від загроз, деструктивних та інших негативних впливів в інформаційному просторі. У той же час, США застосовують вужчий підхід, обмежуючи термін "інформаційна безпека" технологічними аспектами і визначаючи її як захист інформації, інформаційних систем і мереж від несанкціонованого доступу, використання, розкриття, пошкодження, модифікації або знищення з метою забезпечення її цілісності, конфіденційності та доступності [4].

Основою правового забезпечення інформаційної безпеки у США є федеральний закон про управління інформаційною безпекою (FISMA). Він визначає систему керівних принципів і стандартів безпеки для захисту урядової інформації та операцій. Ця система управління ризиками була підписана як частина Закону про електронний уряд 2002 року, яка згодом оновлювалася і доповнювалася. З 2002 року сфера застосування FISMA поширилася і на державні установи, які адмініструють федеральні програми, а також на приватні компанії та постачальників послуг, які мають контракти з урядом США. Невиконання вимог закону може призвести до скорочення федерального фінансування або інших санкцій.

Закон про електронний уряд був прийнятий з метою покращення управління послугами та процесами, зокрема федеральними витратами на інформаційну безпеку. FISMA був одним із найважливіших нормативних актів у Законі про електронний уряд, оскільки запропонував метод зменшення ризиків для безпеки федеральних даних, наголошуючи на економічній ефективності.

На його основі розроблено низку політик безпеки, яких повинні дотримуватися федеральні агентства. Зокрема, FISMA вимагає від федеральних агентств та інших установ, на які поширюється його дія, розробити, задокументувати та впровадити програми інформаційної безпеки в масштабах всієї установи. Ці програми повинні бути здатні захистити конфіденційні дані. Закон також покладає певні обов'язки на Національний інститут стандартів і технологій (NIST) та Адміністративно-бюджетне управління (OMB). Посадові особи агентства – керівники інформаційних служб та генеральні інспектори, повинні проводити щорічні огляди програми інформаційної безпеки агентства та звітувати в OMB, яке використовує ці дані для виконання своїх наглядових функцій, а також для надсилання щорічних звітів до Конгресу.

Активну політику щодо забезпечення інформаційної безпеки проводить й Європейський Союз (ЄС). Гарантування міжнародної інформаційної безпеки та її складової – кібербезпеки стало одним із пріоритетних напрямів її діяльності.

У 2001 р. Комісією ЄС було представлено перший документ «Мережева та інформаційна безпека: європейський політичний підхід», в якому представлена концепція вирішення проблеми інформаційної безпеки. У ньому використовується термін «мережева та інформаційна безпека», який трактується як здатність мережі або інформаційної системи чинити опір випадковим подіям або зловмисним діям, які становлять загрозу доступності, автентичності, цілісності та конфіденційності даних, що зберігаються або передаються, а також послуг, що надаються через ці мережі і системи [5].

За останні роки органи влади ЄС ухвалили низку нормативно-правових актів, які визна-

чають різні підходи до забезпечення інформаційної безпеки в державах-членах ЄС: Рамкове рішення Ради ЄС 2005/222/JHA щодо нападу на інформаційні системи від 24 лютого 2005 р., яка встановлює правила визначення кримінальних злочинів та санкцій у сфері неправомірного впливу на інформаційні системи; Повідомлення Комісії ЄС «На шляху до загальної політики в сфері боротьби з кіберзлочинністю» від 22 травня 2007 р., в якому даються визначення терміну «кіберзлочинність» та основні напрями політики ЄС щодо інформаційної безпеки; Стратегія кібербезпеки ЄС «Відкритий, надійний та безпечний кіберпростір» від 07 лютого 2013 р., яка рекомендує державам-членам ЄС розвивати міжнародну співпрацю у протидії загрозам у кіберпросторі; Повідомлення Комісії ЄС «Захист Європи від широкомасштабних кібератак та руйнувань: посилення рівня підготовленості, безпеки та стійкості» від 30 березня 2009 р., в якому визначено основні заходи для посилення безпеки критичної інформаційної інфраструктури Європи та її здатності протистояти зовнішнім загрозам; Директива Європейського парламенту і Ради ЄС щодо заходів по забезпеченню високого загального рівня безпеки мережевих та інформаційних систем у всьому Союзі від 6 липня 2016 р., яка закріпила єдині правила та вимоги в сфері кібербезпеки для всіх держав-членів ЄС (підвищення спроможності системи кібербезпеки на національному рівні, підвищення рівня європейської співпраці і запровадження управління ризиками та зобов'язання сповіщати про кіберінциденти операторів базових послуг та провайдерів цифрових послуг тощо) [6].

З метою вдосконалення системи інформаційної безпеки в ЄС був створено спеціалізовану організаційну систему. Важливу роль у ній відіграє Європейське агентство з питань мережевої та інформаційної безпеки (ENISA), яке було створено 10 березня 2004 р. До основних завдань ENISA входить вдосконалення мережевої та інформаційної безпеки в ЄС, просування культури мережевої та інформаційної безпеки, яка приносить користь громадянам ЄС, споживачам, підприємствам і громадським організаціям, а також сприяння безперебійному функціонуванню внутрішнього ринку ЄС. [7]. Усвідомлюючи, що ефективність забезпечення інформаційної безпеки в ЄС також залежить від розвитку взаємодії держав у рамках міжнародних органів, в структурі Європейського поліцейського офісу у 2013 р був утворений Європейський центр боротьби з кіберзлочинністю. Центру здійснює свою діяльність з метою розслідування шахрайства через інтернет-мережі, а також розслідування злочинів, що посягають на безпеку критично важливої інфраструктури та інформаційних систем ЄС [8].

ЄС сьогодні активно вдосконалює власні сектори безпеки у інформаційному просторі у відповідності до сучасних викликів шляхом впорядкування нормативної бази, що має забезпечити цілісність державної політики в даній сфері; збільшення чисельності підрозділів, що забезпечують інформаційну безпеку; розробка європейських керівних принципів щодо забезпечення інформаційної безпеки; посилення контролю за національним інформаційним простором; зміцнення захисних механізмів для критичної інформаційної інфраструктури ЄС тощо.

Усвідомлюючи актуальність проблеми забезпечення інформаційної безпеки як складової системи національної безпеки, більшість держав світу почали впроваджувати внутрішні комплексні заходи з кібербезпеки. Ці заходи пов'язані, перш за все, з розробкою і вдосконаленням національного законодавства в даній галузі і створенням спеціалізованих структур, що відповідають за безпеку в кіберпросторі. Кібербезпека на сьогодні є стратегічною проблемою державного значення, яка зачіпає всі верстви населення. Державна політика з кібербезпеки служить засобом посилення національної безпеки і надійності інформаційних систем держави. Стратегії з кібербезпеки були прийняті у США, Швеції, Естонії, Фінляндії, Чехії, Франції, Німеччині, Литві, Великобританії, Канаді, Японії, Індії, Австралії, Новій Зеландії, Колумбія та інших. Список країн наочно показує, що проблема кібербезпеки визнається актуальною в усьому світі [9].

Не залишилась осторонь цієї проблеми й Україна, яка 15 березня 2016 р. схвалила Стратегію кібербезпеки України, що визначає пріоритети та напрямки кібербезпеки і є ключовим структурним елементом у формуванні політики інформаційної безпеки світового рівня [10].

Основи інформаційної безпеки України закладено ще у Конституції, яка разом із Законами України «Про інформацію», «Про захист інформації в інформаційно-комунікаційних системах», «Про захист персональних даних», «Про державну таємницю», «Про національну безпеку України» та ін. становлять законодавчу основу сфери забезпечення інформаційної безпеки держави, оскільки їх основним призначенням є врегулювання відносин в інформаційній сфері.

Із початком повномасштабного військового вторгнення російської федерації в Україну питання інформаційної безпеки стоїть порч із питаннями військової та політичної безпеки, а, отже, нових пріоритетів набувають і процеси реалізації функцій публічного управління у системі інформаційної безпеки. Публічне управління інформаційною безпекою в умовах війни спрямоване на такі напрямки: безпека та захист персональних даних та державної таємниці; моніторинг та регулювання інформаційного простору у сфері боротьби з елементами інформаційної війни; інформаційний супровід процесів публічного управління; цифровізація та автоматизація процесів.

Результатом виникнення нових викликів у сфері публічного управління інформаційною безпекою в умовах війни було впровадження низки законодавчих ініціатив з метою удосконалення системи інформаційної безпеки держави, серед яких:

– Постанова КМУ від 12.03.2022 р. № 263 «Деякі питання реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі»;

– Розпорядження КМУ від 14.04.2023 р. № 328-р «Про затвердження плану заходів з реалізації Стратегії забезпечення державної безпеки»;

– Розпорядження КМУ від 04.04.2023 р. № 299 «Про затвердження плану заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року»;

– Розпорядження КМУ від 30.03.2023 р. № 272-р «Про затвердження плану заходів з реалізації Стратегії забезпечення державної безпеки».

Згідно з доктриною інформаційної безпеки України [11], актуальними загрозами національним інтересам та національній безпеці України в інформаційній сфері є:

– проведення спеціальних інформаційних операцій, спрямованих на підрив обороноздатності, деморалізацію особового складу Збройних сил України та інших військових формувань, провокування екстремістських проявів, розпалювання панічних настроїв, загострення і дестабілізацію соціально-політичної та соціально-економічної ситуації, розпалювання міжетнічних і міжрелігійних конфліктів в Україні;

– держава-агресор проводить спеціальні інформаційні операції в інших країнах з метою створення негативного іміджу України у світі;

– інформаційна експансія країн-агресорів та підконтрольних їм структур, особливо за рахунок розвитку власної інформаційної інфраструктури на території України та інших країн;

– інформаційний контроль держави-агресора на тимчасово окупованих територіях;

– недостатній розвиток державної інформаційної інфраструктури, що обмежує здатність ефективно реагувати на інформаційні атаки та активно діяти в інформаційному полі для реалізації національних інтересів України;

– неефективність національної інформаційної політики, неповнота законів, що регулюють суспільні відносини в інформаційній сфері;

– невизначеність стратегічного курсу, недостатній рівень культури соціальних медіа;

– поширення заклику до радикальних дій з просування концепції ізоляціонізму та автономії, що співіснують в регіонах України [12].

Висновки і пропозиції. Для розв'язання стратегічних проблем інформаційної безпеки України важливо розробити чітку та системну стратегію інформаційної безпеки, яка охоплює всі аспекти та сектори суспільства, включаючи державний, громадянське суспільство та бізнес. Для цього потрібно створити національні центри аналізу та реагування, які будуть відстежувати, аналізувати та оперативно реагувати на кіберзагрози та нові вектори атак; вдосконалити заходи з кібербезпеки для критично важливих об'єктів. Для запобігання можливим кібератакам забезпечити постійний моніторинг і аналіз нових тенденцій у сфері кібербезпеки для своєчасного виявлення та протидії потенційним загрозам, розробити й вдосконалити законодавчу базу в галузі кібербезпеки, що відповідає сучасним викликам та міжнародним стандартам.

Забезпечення інформаційної безпеки в сфері публічного управління є актуальною та важливою проблемою в контексті інформаційної безпеки держави. Тому важливою рекомендацією є впровадження єдиної системи забезпечення інформаційної безпеки державного управління. Розвинені системи електронного документообігу існують в органах державної влади та місцевого самоврядування, але єдиної системи електронного документообігу в Україні немає. Проаналізований досвід також підкреслив важливість активної співпраці між урядовим, приватним та громадським секторами. Спільна стратегія та обмін інформацією допомагають створювати узгоджений фронт у боротьбі з кіберзагрозами.

Література:

1. Чмир Я. Сучасні проблеми інформаційної безпеки України та перспективні напрями їх вирішення. *Наукові праці Міжрегіональної Академії управління персоналом. Політичні науки*

та публічне управління. 2022. № 2(62). С. 149–154. DOI: https://doi.org/10.32689/2523-4625-2022-2(62)-23
2. Сердюк І.А. Підходи публічного управління до інформаційної безпеки особистості. *Публічне урядування.* 2022. № 3 (31). С. 53–59. DOI: https://doi.org/10.32689/2617-2224-2022-3(31)-7
3. Савченко О.С. Проблеми запровадження цифровізації у систему публічного управління. *Таврійський науковий вісник. Серія: Публічне управління та адміністрування.* 2022. № 3, С. 102–108. DOI: https://doi.org/10.32851/tnv-pub.2022.3.14
4. Федеральний закон про інформаційну безпеку. 2014. URL: https://www.govinfo.gov/content/pkg/PLAW-113publ283/pdf/PLAW-113publ283.pdf (дата звернення: 10.03.2024).
5. Мережева та інформаційна безпека: пропозиція щодо європейського політичного підходу. 2001. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52001DC0298 (дата звернення: 10.03.2024).
6. Щодо заходів для забезпечення високого спільного рівня безпеки мережевих та інформаційних систем по всьому Союзу. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN (дата звернення: 10.03.2024).
7. Агентство Європейського Союзу з мережевої та інформаційної безпеки (2013). URL: https://www.enisa.europa.eu/about-enisa (дата звернення: 10.03.2024).
8. Гассельбах К., Завгородня І. Боротьба з інтернет-злочинністю. 2013. URL: http://p.dw.com/p/17HRW (дата звернення: 10.03.2024).
9. Войціховський А.В. Інформаційна безпека як складова системи національної безпеки (міжнародний і зарубіжний досвід). *Вісник Харківського національного університету імені В. Н. Каразіна.* Серія «Право». 2020. Випуск 29. С. 281–288. DOI: https://doi.org/10.26565/2075-1834-2020-29-38
10. Указ Президента України Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України". 2021. URL: https://zakon.rada.gov.ua/aws/show/447/2021 (дата звернення: 10.03.2024).
11. Указ Президента України №47/2017 Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України». 2017. URL: https://www.president.gov.ua/documents/472017-21374 (дата звернення: 10.03.2024).
12. Ніщименко О.А. Інформаційна безпека України на сучасному етапі розвитку держави і суспільства. *Наше право.* 2016. № 1. С. 17–23.

References:

1. Chmyr Ya. (2022) Suchasni problemy informatsiinoi bezpeky Ukrainy ta perspektyvni napriamy yikh vyrishennia [Modern problems of information security of Ukraine and perspective directions of their solution. Scientific works of the Interregional Academy of Personnel Management]. *Naukovi pratsi Mizhrehionalnoi Akademii upravlinnia personalom. Politychni nauky ta publichne upravlinnia – Scientific works of the Interregional Academy of Personnel Management. Political science and public administration*, vol. 2(62), pp. 149–154. DOI: https://doi.org/10.32689/2523-4625-2022-2(62)-23
2. Serdiuk I. A. (2022) Pidkhody publichnoho upravlinnia do informatsiinoi bezpeky osobystosti [Public administration approaches to personal information security]. *Publichne uriaduvannia – Public governance*, vol. 3(31), pp. 53–59. DOI: https://doi.org/10.32689/2617-2224-2022-3(31)-7
3. Savchenko O. S. (2022) Problemy zaprovadzhennia tsyfrovizatsii u systemu publichnoho upravlinnia [Problems of introducing digitalization into the public administration system]. *Tavriiskyi naukovyi visnyk. Seriia: Publichne upravlinnia ta administruiuvannia – Tavrian Scientific Bulletin. Series: Public management and administration*, vol. 3, pp. 102–108. DOI: https://doi.org/10.32851/tnv-pub.2022.3.14
4. Federalnyi zakon pro informatsiinu bezpeku [Federal Information Security Act] Available at: https://www.govinfo.gov/content/pkg/PLAW-113publ283/pdf/PLAW-113publ283.pdf (accessed March 10, 2024).
5. Merezheva ta informatsiina bezpeka: propozytsiia shchodo yevropeiskoho politychnoho pidkhodu [Network and information security: proposal for a european policy approach]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52001DC0298 (accessed March 10, 2024).
6. Shchodo zakhodiv dlia zabezpechennia vysokoho spilnoho rivnia bezpeky merezhevykh ta informatsiinykh system po vsomu Soiuzu [Concerning measures for a high common level of security of network and information systems across the Union]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN (accessed March 10, 2024).
7. Ahentstvo Yevropeiskoho Soiuzu z merezhevoi ta informatsiinoi bezpeky [European Union Agency for Network and Information Security]. Available at: https://www.enisa.europa.eu/about-enisa (accessed March 10, 2024).
8. Hasselbakh K., & Zavhorodnia I. (2013). Borotba z internet-zlochinnistiu [Fighting Internet Crime]. Available at: http://p.dw.com/p/17HRW (accessed March 10, 2024).
9. Voiţikhovskyi A. V. (2020) Informatsiina bezpeka yak skladova systemy natsionalnoi bezpeky (mizhnarodnyi i zarubizhnyi dosvid) [Information Security as a Component of National Security System (International and Foreign Experience)]. *Visnyk Kharkivskoho natsionalnoho universytetu imeni V. N. Karazina. Seriia «PRAVO» – Bulletin of V. N. Karazin Kharkiv National University. Series "Law"*, vol. 29, pp. 281–288. DOI: https://doi.org/10.26565/2075-1834-2020-29-38
10. Ukaz Prezydenta Ukrainy Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14 travnia 2021 roku "Pro Stratehiiu kiberbezpeky Ukrainy" [Decree of the President of Ukraine On the Decision of the National Security and Defense Council of Ukraine of May 14, 2021 "On the Cybersecurity Strategy of Ukraine"]. Available at: https://zakon.rada.gov.ua/laws/show/447/2021 (accessed March 10, 2024).
11. Ukaz Prezydenta Ukrainy № 47/2017 Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 29 hrudnia 2016 roku «Pro Doktrynu informatsiinoi bezpeky Ukrainy» [Decree of the President of Ukraine No. 47/2017 On the Decision of the National Security and Defense Council of Ukraine of December 29, 2016 "On the Information Security Doctrine of Ukraine"]. Available at: https://www.president.gov.ua/documents/472017-21374 (accessed March 10, 2024).
12. Nishchymenko O. A. (2016) Informatsiina bezpeka Ukrainy na suchasnomu etapi rozvytku derzhavy i suspilstva [Information Security of Ukraine at the Present Stage of State and Society Development]. *Nashe pravo – Our law*, vol. 1, pp. 17–23.

Summary. The article is devoted to the issues of ensuring the functions of public information security management in the context of modern challenges. Informatization processes have covered all spheres of human life, which has led to the emergence of new threats. In today's world, where electronic technologies are becoming a necessity to ensure the effectiveness of public administration functions, the issue of information security is a key and urgent one. The problems of information security are currently being actualized by a significant increase in the role of accumulation, processing and dissemination of information, in particular, in making strategic, military, political and economic decisions. In this regard, the question of how well the modern public administration system is able to respond to the challenges posed by global digitalization is becoming relevant. The purpose of the paper is to study the peculiarities of ensuring information security in public administration, to analyze current threats and the experience of other countries in overcoming them. In analyzing certain aspects of information security, the paper uses methods of description and classification, as well as methods of studying causal relationships, in particular, the combination of similarities and differences. The article examines the trends in the development of public information security management as a key mechanism for ensuring the security of the State. The author identifies the issue of information security as an element of the State defense policy, which is of particular relevance in the context of full-scale military aggression. The concept of public management of information security can be defined as the process of managing measures aimed at protecting confidential information from unauthorized access, use, disclosure and destruction at the level of the State, organizations or citizens. This process may include the creation of appropriate legislation, the establishment of appropriate control and supervisory bodies, the conduct of information security education and training, and the installation of appropriate security technologies and systems to protect confidential information. The place and role of the system of regulation of information support of management processes at the state level are clarified. Sufficient attention is paid to the peculiarities of ensuring information security in public administration through the analysis of modern information threats. Considering the world experience, the author identifies the key success factors and the problems faced by public administration in overcoming them. We consider it expedient to create national analysis and response centers that will monitor, analyze and respond promptly to cyber threats and improve cybersecurity measures for critical facilities.

Key words: public administration, information security, cyber threats, informatization, cybersecurity.