УДК 351:35.072
DOI https://doi.org/10.32782/2310-9653-2025-2.9

Т. С. Яровой, доктор наук з державного управління, доцент, завідувач кафедри національної безпеки, менеджменту та публічного адміністрування Чернігівського інституту Інформації, бізнесу і права ЗВО «Міжнародний Науково-технічний університет імені академіка Юрія Бугая»

ЦИФРОВІЗАЦІЯ ПУБЛІЧНОГО УПРАВЛІННЯ В СИСТЕМІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ: ДОСВІД США ТА ПЕРСПЕКТИВИ ЙОГО АПРОКСИМАЦІЇ

Стаття присвячена дослідженню цифровізації державного управління у сфері національної безпеки, з акцентом на досвіді США та потенціалі адаптації цих практик в інших країнах. У ньому проаналізовано критичну важливість інтеграції передових технологій, таких як штучний інтелект, аналіз великих даних і хмарні обчислення, в системи управління органами національної безпеки. Дослідження підкреслило трансформаційну роль таких технологій у вдосконаленні процесів прийняття рішень, міжвідомчої координації та реагування на нові загрози в режимі реального часу.Розглянуто законодавчі та організаційні рамки, які підтримують зусилля Сполучених Штатів у цій сфері, включаючи Федеральний закон про модернізацію інформаційної безпеки FISMA та ініціативи Агентства з кібербезпеки та безпеки інфраструктури CISA. У дослідженні проаналізовано практичну реалізацію цих нормативно-правових актів, зокрема реалізацію таких програм, як Безперервна діагностика та пом'якшення наслідків (CDM) та прийняття Національної стратегії кібербезпеки. Цими зусиллями було підкреслено необхідність узгодження національних і міжнародних цілей у сфері кібербезпеки для вирішення багатогранних викликів безпеці.Виявлено виклики і можливості, пов'язані з цифровізацією, в тому числі етичні дилеми і проблеми приватності, що виникають у зв'язку з використанням технологій спостереження і масового збору даних. У дослідженні проаналізовано публічні дебати навколо таких програм, як PRISM, та їхні наслідки для балансу між індивідуальними правами та імперативами національної безпеки. Також розглянуто складнощі інтеграції застарілих систем із сучасними рішеннями та забезпечення сумісності між федеральними та державними установами.Особливої уваги заслуговують тематичні дослідження, які продемонстрували відчутні результати ініціатив з цифрової трансформації в США. Серед прикладів - системи виявлення загроз у режимі реального часу та міжвідомчі комунікаційні платформи, які покращили час реагування під час кризових ситуацій. Незважаючи на ці досягнення, дослідження виявило поточні виклики, такі як вразливість кібербезпеки та необхідність постійних інновацій. Результати дослідження підкреслили актуальність досвіду США як моделі для інших країн, що прагнуть цифрової модернізації державного управління та національної безпеки.

Ключові слова: *діджиталізація, державне управління, цифровізація публічного управління, забезпечення цифровізації публічного управління, національна безпека, кібербезпека, штучний інтелект, національна кіберстратегія, розвідувальне співтовариство, виявлення загроз, критична інфраструктура, цифрова трансформація, інформаційна безпека.*

T. S. Yarovoi. Digitalisation of public administration in the National security system: US experience and prospects for its approximation

The article examines the digitalisation of public administration in the field of national security, with a focus on the US experience and the potential for adapting these practices in other countries. It analyses the critical importance of integrating advanced technologies, such as artificial intelligence, big data analysis and cloud computing, into national security management systems. The study highlights the transformative role of such technologies in improving decision-making, interagency coordination and real-time response to emerging threats.It examines the legislative and organisational frameworks that support the United States' efforts in this area, including the Federal Information Security Modernisation Act (FISMA) and the Cybersecurity and Infrastructure Security Agency (CISA) initiatives. The study analyses the practical implementation of these regulations, including the implementation of programmes such as Continuous Diagnostics and Mitigation (CDM) and the adoption of the National Cyber Security Strategy. These efforts highlighted the need to align national and international cybersecurity goals to address multifaceted security challenges.The challenges and opportunities associated with digitalisation, including ethical dilemmas and privacy issues arising from the use of surveillance and mass data collection technologies, were identified. The study analyses the public debate around programmes such as PRISM and its implications for the balance between individual rights and national security imperatives. It also examines the challenges of integrating legacy systems with modern solutions and ensuring interoperability between federal and state agencies.Particularly noteworthy are the case studies that demonstrate the tangible results of digital transformation initiatives in the United States. Examples include real-time threat detection systems and interagency communication platforms that have improved response times during crises. Despite these achievements, the study identified ongoing challenges, such as cybersecurity vulnerabilities and the need for continuous innovation. The study's findings highlighted the relevance of the US experience as a model for other countries seeking digital modernisation of public administration and national security.

Key words: *digitalisation, public administration, digitalization of the public administration, ensuring the digitization of public administration, national security, cybersecurity, artificial intelligence, national cyber strategy, intelligence community, threat detection, critical infrastructure, digital transformation, information security.*

Постановка завдання. Обґрунтування актуальності теми дослідження. Діджиталізація державного управління в контексті національної безпеки є критично важливою сферою дослідження через зростаючу складність і частоту сучасних загроз безпеці. Інциденти у сфері кібербезпеки, геополітична напруженість та глобальна взаємозалежність, вимагають передових технологічних рішень для забезпечення ефективного врядування та національної оборони. США, як світовий лідер у сфері цифрових інновацій та політики національної безпеки, пропонує комплексну модель інтеграції цифрових технологій у державне управління.

Актуальність цього дослідження ще більше підкреслюється зростаючою залежністю урядів від цифрових платформ для покращення процесу прийняття рішень, оптимізації міжвідомчої координації та покращення можливостей реагування в режимі реального часу. Цифрові інструменти, такі як штучний інтелект, аналіз великих даних і хмарні обчислення, докорінно змінили алгоритми функціонування органів безпеки, пропонуючи можливості для виявлення, запобігання і реагування на загрози з безпрецедентною ефективністю.

У світлі зростаючої важливості цифрової стійкості для національної безпеки дослідження розглядає своєчасне і критично важливе питання. Вивчаючи досвід США та досліджуючи його потенціал для адаптації в інших контекстах, дослідження надає практичні рекомендації для політиків і практиків у всьому світі.

Аналіз останніх досліджень і публікацій. Узагальнення останніх досліджень і публікацій, свідчить про зростаючий інтерес до цифровізації у сфері національної безпеки, зокрема – інтеграції передових технологій, таких як штучний інтелект, великі дані та хмарні обчислення. Дослідники акцентують увагу на необхідності модернізації законодавчої бази та забезпеченні міжвідомчої співпраці (Гнатюк С., Поліщук Ю., Сотніченко Ю., Жаксігулова Д., Ковальчук В. В., Браун С., Флаерті А., Гіллум Дж., Апуццо М.). Значну увагу приділено питанням кібербезпеки, захисту критичної інфраструктури та вирішенню етичних дилем, пов'язаних із захистом приватності даних.

Мета дослідження — аналіз досвіду США щодо цифровізації державного управління в системі національної безпеки та вивчення перспектив адаптації та наближення цих практик в інших країнах.

Виклад основного матеріалу. Цифровізація державного управління в Сполучених Штатах, особливо в сфері національної безпеки, ґрунтується на надійній і динамічній політичній базі, розробленій з урахуванням нових загроз і технологічних досягнень. Серед основоположних законодавчих актів, Федеральний закон про модернізацію інформаційної безпеки FISMA відіграє ключову роль у встановленні всеосяжних стандартів захисту федеральних інформаційних систем [1]. Прийнятий з метою модернізації та посилення попередніх рамок, FISMA зобов'язує федеральні агентства розробляти, документувати та впроваджувати надійні програми кібербезпеки, які відповідають принципам управління ризиками, з акцентом на постійний моніторинг, можливості реагування на інциденти та міжвідомчу співпрацю.

Доповнюючи FISMA, Агентство з кібербезпеки та безпеки інфраструктури CISA відіграє важливу роль у координації зусиль державного та приватного секторів з метою захисту критичної інфраструктури країни. Як провідна організація з ініціатив у сфері кібербезпеки, CISA надає оперативні ресурси, технічну експертизу та розвіддані про загрози для посилення безпеки федеральних, регіональних та місцевих органів влади, а також приватних підприємств [2]. Ініціативи агентства, такі як програма безперервної діагностики та пом'якшення наслідків CDM, є прикладом проактивних заходів, вжитих для покращення видимості загроз у режимі реального часу та оптимізації протоколів реагування на інциденти в різних секторах.

Крім того, Національна стратегія кібербезпеки, оприлюднена у 2023 році, окреслює комплексну дорожню карту для зміцнення цифрової інфраструктури Сполучених Штатів перед сучасними викликами. Стратегія наголошує на п'яти ключових напрямках: захист критичної інфраструктури, протидія кіберзагрозам, зміцнення міжнародного партнерства, інвестиції в стійкість до кіберзагроз і сприяння підзвітності серед зацікавлених сторін [3]. Стратегія підкреслює необхідність використання передових технологій, сприяння державно-приватній співпраці та узгодження національних цілей з глобальними нормами для вирішення багатогранних аспектів кібербезпеки в сучасну епоху.

Практична реалізація цифровізації в органах національної безпеки була відзначена трансформаційними досягненнями у впровадженні технологій, оперативній інтеграції та розбудові потенціалу. Розвідувальні служби, зокрема Центральне розвідувальне управління і Агентство національної безпеки, здійснили значні ініціативи з цифрової трансформації, спрямовані на підвищення їхньої оперативної ефективності. Вони включають інтеграцію алгоритмів штучного інтелекту ШІ в робочі процеси розвідувального аналізу, що дозволяє швидко обробляти величезні обсяги неструктурованих даних для виявлення дієвих інсайтів. Такі можливості дозволили аналітикам виявляти закономірності, оцінювати ризики і прогнозувати загрози з більшою точністю і ефективністю.

Аналітика великих даних стала наріжним каменем цифрових операцій, надаючи відомствам можливість консолідувати та інтерпретувати величезні масиви даних, отримані з різних платформ і джерел. Міністерство внутрішньої безпеки США DHS використовує передові аналітичні інструменти для моніторингу та оцінки транскордонної діяльності, що дозволяє владі виявляти незаконну торгівлю, несанкціонований в'їзд та інші загрози безпеці з підвищеною точністю [4]. Об'єднання даних з різних джерел, в тому числі систем спостереження, біометричних баз даних і мереж зв'язку, забезпечує цілісний підхід до виявлення і пом'якшення загроз.

Рішення на основі хмарних обчислень також відіграють важливу роль у зміцненні міжвідомчої співпраці і раціоналізації розподілу ресурсів. Прийняття Розвідувальним співтовариством структури Інформаційно-технологічного підприємства Розвідувального співтовариства ICITE підкреслює важливість хмарної інфраструктури для поліпшення обміну інформацією і оперативної злагодженості [5]. Платформа полегшує безпечний доступ в режимі реального часу до секретної і несекретної інформації, гарантуючи, що розвідувальні служби працюють з синхронізованими цілями і єдиною системою ситуаційної обізнаності.

Варті уваги історії успіху демонструють відчутні переваги цих зусиль з діджиталізації. Під час нещодавніх інцидентів з кібербезпеки, пов'язаних з критичною інфраструктурою, системи виявлення загроз в режимі реального часу дозволили відомствам швидко виявити і нейтралізувати потенційні порушення, мінімізувавши збитки і забезпечивши безперервність роботи. Так само міжвідомчі комунікаційні платформи, розроблені в рамках ICITE, уможливили безперешкодну координацію під час масштабних надзвичайних ситуацій, гарантуючи, що важлива інформація надходитиме до осіб, які приймають рішення, без затримок і вузьких місць.

Незважаючи на трансформаційний характер цих досягнень, вони не позбавлені викликів. Відомства стикаються з такими проблемами, як забезпечення безпеки даних у взаємопов'язаних системах, вирішення етичних питань, пов'язаних з технологіями спостереження, і управління складнощами інтеграції застарілих систем з сучасними рішеннями. Незважаючи на ці перешкоди, досвід Сполучених Штатів підкреслює трансформаційний потенціал цифровізації в посиленні оперативних можливостей і стійкості систем національної безпеки.

Цифровізація державного управління в рамках національної безпеки Сполучених Штатів, попри трансформацію, зіткнулася з низкою серйозних викликів, які потребують постійної уваги та адаптації. Серед них особливо помітними залишаються вразливості та ризики кібербезпеки, оскільки зростаюча залежність від взаємопов'язаних систем і цифрових інфраструктур створює розширену поверхню для атак з боку супротивників. Федеральні агентства зіткнулися з такими інцидентами, як кібератака SolarWinds, коли сучасні стійкі загрози проникли в критичні мережі, продемонструвавши вразливість навіть найзахищеніших систем до витончених кіберторгнень [6]. Цей інцидент підкреслив необхідність постійного інвестування в передові механізми виявлення загроз, архітектури нульової довіри і проактивні стратегії захисту для зменшення потенціалу підриву або експлуатації систем національної безпеки.

Питання конфіденційності та етики даних також стали складними викликами, особливо в контексті балансування між необхідністю надійних заходів національної безпеки і захистом індивідуальних прав і громадянських свобод. Збір та аналіз величезних обсягів персональних даних, часто полегшений сучасними технологіями спостереження та аналітикою великих даних, викликав занепокоєння щодо надмірного використання та потенційних зловживань. Публічні дебати навколо таких програм, як PRISM, розкриті викривачами, висвітлили етичні дилеми, притаманні практиці масового збору даних, коли межа між безпекою і приватним життям стає все більш розмитою [7]. Політики і спецслужби повинні обережно долати ці суперечності, гарантуючи, що правові рамки і механізми нагляду є достатньо надійними, щоб запобігати зловживанням і водночас забезпечувати ефективне проведення операцій з гарантування безпеки.

Інтероперабельність між відомствами і системами є ще однією значною перешкодою в процесі цифровізації, оскільки інтеграція застарілих систем із сучасними технологіями часто створює проблеми сумісності і призводить до операційної неефективності. Децентралізований характер федеральної системи управління Сполучених Штатів у поєднанні з різним рівнем технічної спроможності відомств ускладнює зусилля зі створення безперешкодного обміну даними та механізмів спільної роботи. Неспроможність повністю інтегрувати критичні системи між відомствами, особливо під час надзвичайних ситуацій або інцидентів у сфері кібербезпеки, може призвести до затримок у реагуванні та зниження ефективності скоординованих дій [8]. Такі зусилля, як створення Підприємства інформаційних технологій розвідувального співтовариства ICITE, спрямовані на вирішення цих проблем, але досягнення повної оперативної сумісності вимагає значного виділення ресурсів, міжвідомчої співпраці і довгострокової прихильності до технологічної модернізації.

Цифровізація державного управління в Сполучених Штатах, зокрема в системі національної безпеки, підтримується значними фінансовими інвестиціями і демонструє вимірюваний вплив на різні операційні виміри. Тенденції федеральних витрат на цифровізацію та кібербезпеку відображають пріоритетність технологічного прогресу як наріжного каменю державного управління. Звіти Адміністративно-бюджетного управління АБУ свідчать про постійне зростання фінансування кібербезпеки: з 14 мільярдів доларів у 2020 році до приблизно 18,8 мільярда доларів у 2023 році [9]. Зазначені показники ілюструють узгоджені зусилля федеральних відомств, спрямовані на модернізацію інфраструктури, підвищення стійкості кібербезпеки та впровадження передових технологій для захисту критично важливих систем і даних. Слід зазначити, що на Міністерство внутрішньої безпеки (DHS) та Міністерство оборони (DoD) припадає значна частка цих витрат, що підкреслює ключову роль цифровізації у забезпеченні національних інтересів.

Показники впливу ще більше підкреслюють відчутні переваги цих інвестицій, демонструючи покращення часу реагування, рівня виявлення загроз та економічної ефективності. Впровадження систем моніторингу загроз

у реальному часі у федеральних відомствах призвело до помітного скорочення середнього часу, необхідного для виявлення і реагування на кіберінциденти. У звіті Агентства кібербезпеки і безпеки інфраструктури CISA зазначено, що середній час від виявлення до усунення кіберзагроз скоротився на 35% у період з 2019 по 2022 рік, що відображає ефективність передової аналітики, штучного інтелекту і автоматизованих інструментів реагування. Очевидним є також підвищення рівня виявлення загроз, оскільки спецслужби використовують алгоритми машинного навчання для обробки величезних масивів даних і виявлення потенційних ризиків для безпеки з підвищеною точністю. Застосування цих технологій не лише зменшило операційну неефективність, але й підвищило точність розвідувальних оцінок, що дозволило керівникам національної безпеки приймати більш обґрунтовані рішення.

Економічні переваги цифровізації в державному управлінні є не менш значними, про що свідчить підвищення ефективності витрат і оптимізація ресурсів. Впровадження хмарних обчислень в розвідувальному співтоваристві зменшило залежність від дорогих, розрізнених застарілих систем і водночас забезпечило більшу масштабованість і гнучкість в операціях. Консолідувавши можливості зберігання і аналізу даних у спільній хмарній інфраструктурі, відомства досягли значної економії коштів, вивільнивши ресурси для інших важливих ініціатив у сфері безпеки. Крім того, інтеграція предиктивної аналітики в процеси державного управління сприяла більш ефективному розподілу ресурсів під час кризового управління, тим самим мінімізуючи фінансові втрати, пов'язані із затримкою або неадекватним реагуванням.

Тематичні дослідження успішних ініціатив з діджиталізації дають конкретне уявлення про практичне застосування цих технологій. Під час сезону лісових пожеж 2020 року Федеральне агентство з надзвичайних ситуацій FEMA використовувало передову аналітику даних і географічні інформаційні системи ГІС для координації зусиль з реагування на стихійні лиха в декількох штатах. Агрегуючи в режимі реального часу дані про поширення пожежі, щільність населення та наявність ресурсів, FEMA змогло оптимізувати плани евакуації та визначити пріоритети розгортання аварійного персоналу і матеріалів [10]. Такий підхід не лише підвищив ефективність операцій з реагування, але й пом'якшив вплив на постраждалі громади, скоротивши час, необхідний для відновлення та відбудови.

Міністерство охорони здоров'я і соціальних служб HHS використовувало цифрові платформи для координації міжвідомчих зусиль під час пандемії COVID-19, застосовуючи інформаційні панелі для відстеження рівня інфікування, пропускної здатності лікарень і показників розподілу вакцин. Такий централізований підхід до управління даними сприяв швидкому прийняттю рішень і впорядкуванню комунікації між федеральними, державними та місцевими органами влади, забезпечуючи ефективний і справедливий розподіл критично важливих ресурсів.

Наведені статистичні та емпіричні результати підкреслюють трансформаційний потенціал цифровізації в державному управлінні, її здатність підвищувати операційну ефективність, покращувати можливості виявлення загроз і реагування на них, а також приносити значні економічні вигоди. Оскільки федеральні відомства продовжують інвестувати в цифрову інфраструктуру та вдосконалювати її, уроки, отримані з цих ініціатив, слугуватимуть цінним орієнтиром для інших країн, які прагнуть модернізувати свої системи державного управління та зміцнити основи національної безпеки.

Висновки та перспективи подальших досліджень. Цифровізація державного управління в системі національної безпеки стала невід'ємною складовою сучасного врядування, про що свідчать трансформаційні зрушення, які спостерігаються у Сполучених Штатах Америки. Інтеграція передових технологій, таких як штучний інтелект, аналіз великих даних і хмарні обчислення, значно розширила операційні можливості федеральних відомств, уможлививши більш ефективне виявлення загроз, поліпшення міжвідомчої координації та прийняття більш обґрунтованих рішень. Законодавча база, зокрема Федеральний закон про модернізацію інформаційної безпеки, а також стратегічні ініціативи під керівництвом таких відомств, як Агентство кібербезпеки та інфраструктурної безпеки, створили міцну основу для цих досягнень, забезпечивши узгодження зусиль з цифровізації з цілями національної безпеки.

Перспективи подальших досліджень лежать у кількох ключових сферах. Вивчення передових заходів кібербезпеки, таких як квантові обчислення і технологія блокчейн, має значний потенціал для підвищення стійкості критичної інфраструктури. Порівняльні дослідження, що аналізують зусилля інших розвинених країн у сфері діджиталізації, можуть забезпечити ширше розуміння найкращих практик та альтернативних підходів. Крім того, дослідження соціально-політичних наслідків цифровізації, зокрема її впливу на суспільну довіру, демократичне врядування та міжнародне співробітництво, залишаються критично важливими для формування ефективної та справедливої політики.

Підсумовуючи, можна сказати, що хоча цифровізація державного управління пропонує безпрецедентні можливості для зміцнення національної безпеки, вона також створює складні виклики, які потребують міждисциплінарного підходу. Продовжуючи вдосконалювати політику, інвестувати в технології та сприяти глобальній співпраці, уряди можуть використати весь потенціал цифровізації для задоволення мінливих вимог XXI століття.

Список використаних джерел:

1. Federal Information Security Modernization Act of 2014 (FISMA 2014). *America`s Cyber Defense Agency.* URL: https://surl.li/zpmszc

2. Гнатюк С.О., Поліщук Ю.Я., Сотніченко Ю.О., Жаксигулова Д.Д. Аналіз кращих світових практик щодо захисту критичної інформаційної інфраструктури. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*. 2020. № 2(10). С. 184–196. URL: https://doi.org/10.28925/2663-4023.2020.10.184196 .

3. Ковальчук В. В. Управління інформаційною безпекою: американський досвід. *Безпека держави.* 2023. № 3. С. 89–98. URL: https://journals.uran.ua/bdi/article/view/290991 .

4. Department of Defense Dictionary of Military and Associated Terms. (2016). *Joint Chiefs of Staff.* URL: https://irp.fas.org/doddir/dod/jp1_02.pdf .

5. Зінченко О.В., Іщеряков С.М., Прокопов С.В., Сєрих С.О., Василенко В.В. Хмарні технології. *Державний університет телекомунікацій* 2020. с. 74 URL: https://duikt.edu.ua/ua/lib/1/category/2128/view/2048

6. Evasive attacker leverages SolarWinds supply chain compromises with Sunburst backdoor (2020). *Threat Intelligence*. URL: https://surl.li/vcnpfn

7. Braun, S. Flaherty, A. Gillum, J. Apuzzo, M. (2013). Secret to PRISM Program: Even Bigger Data Seizures. *Associated Press*. URL: https://surl.li/bajtgs

8. Національний інститут стратегічних досліджень. Основні положення нової Стратегії національної безпеки США. *Національний інститут стратегічних досліджень.* 2022 URL: https://surl.li/euzggn 9. Federal Cybersecurity Funding FY. *Administrative and budgetary management.* 2021. URL: https://surl.li/bmkfec

10. FEMA Strategic Plan 2022-2026. (2022). *Federal Emergency Management Agency.* URL: https://www.fema.gov/about/reports-and-data/guidance.

References:

1. Federal Information Security Modernization Act of 2014 (FISMA 2014). *America`s Cyber Defense Agency.* URL: https://surl.li/zpmszc [English].

2. Gnatyuk, S., Polishchuk, Y., Sotnichenko, Y., & Zhaksigulova, D. (2020). Analiz krashchykh svitovykh praktyk shchodo zakhystu krytychnoi informatsiinoi infrastruktury [Analysis of the best global practices in protecting critical information infrastructure]. *Elektronne fakhove naukove vydannia «Kiberbezpeka: osvita, nauka, tekhnika» - Electronic professional scientific publication "Cybersecurity: Education, Science, Technology",* 2(10), 184–196. URL: https://doi.org/10.28925/2663-4023.2020.10.184196 [Ukraine].

3. Kovalchuk V. V. (2023). Upravlinnia informatsiinoiu bezpekoiu: amerykanskyi dosvid [Information Security Management: American Experience]. *Bezpeka derzhavy - State Security,* 3, 89–98. URL: https://journals.uran.ua/bdi/article/view/290991 [Ukraine].

4. Department of Defense Dictionary of Military and Associated Terms. (2016). *Joint Chiefs of Staff.* URL: https://irp.fas.org/doddir/dod/jp1_02.pdf . [English].

5. Zinchenko O.V., Ishcheriakov S.M., Prokopov S.V., Sierykh S.O., Vasylenko V.V. (2020). Khmarni tekhnolohii [Cloud technologies]. Derzhavnyi universytet telekomunikatsii - State University of Telecommunications, 74 URL: https://duikt.edu.ua/ua/lib/1/category/2128/view/2048 [Ukraine].

6. Evasive attacker leverages SolarWinds supply chain compromises with Sunburst backdoor (2020). *Threat Intelligence*. URL: https://surl.li/vcnpfn [English].

7. Braun, S. Flaherty, A. Gillum, J. Apuzzo, M. (2013). Secret to PRISM Program: Even Bigger Data Seizures. *Associated Press*. URL: https://surl.li/bajtgs [English].

8. Natsionalnyi instytut stratehichnykh doslidzhen. Osnovni polozhennia novoi Stratehii natsionalnoi bezpeky SShA. Natsionalnyi instytut stratehichnykh doslidzhen [National Institute for Strategic Studies. Key Provisions of the New US National Security Strategy*] (*2022). *Natsionalnyi instytut stratehichnykh doslidzhen - National Institute for Strategic Studies.* URL: https://surl.li/bmkfec [Ukraine].9. Federal Cybersecurity Funding FY. *Administrative and budgetary management.* (2021). URL: https://surl.li/bmkfec [English].

10. FEMA Strategic Plan 2022-2026. (2022). *Federal Emergency Management Agency.* URL: https://www.fema.gov/about/reports-and-data/guidance. [English].