ГОРБ В. В.,
полковник,
співробітник
(Служба безпеки України)

УДК 343.341:323.28(477)
DOI https://doi.org/10.32842/2078-3736/2023.5.17

НАЧАСНІ ЧИННИКИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

Проведений огляд нормотворчої діяльності уряду України у сфері цифрової трансформації нашої держави та перспективних проєктів, що вже реалізовані або мають бути втілені в найближчому майбутньому. Висвітлені позитивні тенденції впровадження електронного урядування, цифрової економіки, штучного інтелекту, хмарних обчислень, «великих даних» в життя українського народу та констатовано, що незважаючи на триваючу війну в країні присутні сприятливі умови для динамічної цифровізації усіх сфер суспільних відносин і державного управління. Акцентовано увагу на потребі технічного захисту інформації задля унеможливлення завдання шкоди охоронюваним правам людини, громадянина та національним інтересам. Розглянуто основоположні нормативно-правові акти у сфері технічного захисту інформації, сутність персональних даних, класифікацію автоматизованих систем, призначених для їх оброблення, процедуру створення комплексних систем захисту інформації та отримання на них атестату відповідності. Резюмовано, що побудова комплексної системи захисту інформації в інформаційних системах процес довготривалий і дороговартісний, який супроводжується організаційними, інженерними, проектними, пусконалагоджувальними етапами робіт. Висвітлено притаманні проблеми, пов'язані з занадто високою вартістю атестованих засобів технічного захисту інформації, відсутністю комплексних систем захисту інформації в сегментах вже експлуатуємих державних електронних інформаційних ресурсів, ризиками можливого витоку інформації з обмеженим доступом. Сформовано пропозиції щодо необхідності актуалізації концептуальних засад технічного захисту інформації відповідно до реалій нинішнього часу, запозичення релевантного для нашої держави іноземного досвіду, впровадження дієвих алгоритмів захисту інформаційних систем від несанкціонованого доступу.

Ключові слова: *цифровізація, інформаційні системи, технічний захист інформації, комплексна система захисту інформації, персональні дані, інформація з обмеженим доступом, атестат відповідності.*

Horb V. V. Timely factors of technical protection of information in information systems

A review of the rule-making activities of the Government of Ukraine in the field of digital transformation of our country and promising projects that have already been implemented or are to be implemented in the near future has been conducted. Positive trends in the introduction of e-governance, digital economy, artificial intelligence, cloud computing, «big data» into the life of the Ukrainian people are highlighted, and it is stated that despite the ongoing war in the country, there are favorable conditions for the dynamic digitalization of all spheres of public relations and state administration. Attention is focused on the need for technical protection of information in order to prevent damage to protected human rights, citizens

and national interests. The fundamental legal acts in the field of technical information protection, the essence of personal data, the classification of automated systems intended for their processing, the procedure for creating complex information protection systems and obtaining a certificate of compliance for them were considered. It is summarized that the construction of a complex information protection system in information systems is a long-term and expensive process, which is accompanied by organizational, engineering, design, and commissioning stages of work. The inherent problems associated with the too high cost of certified technical information protection means, the lack of comprehensive information protection systems in the segments of already operated state electronic information resources, and the risks of possible leakage of information with limited access are highlighted. Proposals have been made regarding the need to update the conceptual foundations of technical information protection in accordance with the realities of the present time, to borrow foreign experience relevant to our state, and to implement effective algorithms for protecting information systems from unauthorized access.

Key words: *digitization, information systems, technical information protection, comprehensive information protection system, personal data, information with limited access, certificate of compliance.*

Постановка проблеми. Реалізація проєкту «Дія. Цифрова Держава» переслідує амбітну і гуманну мету – зробити взаємодію громадян та бізнесу з державою зручною, прозорою та людяною, забезпечити 100% публічних послуг доступними онлайн до 2024 року. Перспективні світові тенденції вже зараз орієнтовані на впровадження актуальних і стратегічно важливих для економіки та соціуму планів широкомасштабного поширення технологій штучного інтелекту, хмарних обчислень, «великих даних».

Результатом співпраці понад 170 урядів та організацій, які працюють над відкриттям даних на основі спільного набору принципів стала Міжнародна хартія відкритих даних (The Open Data Charter), яка була представлена під час Генеральної Асамблеї ООН у 2015 році [1]. У вересні 2016 року до хартії приєдналась і Україна.

Схвалена Кабміном у 2017 році «Концепція розвитку електронного урядування в Україні» є основним документом у сфері реформування системи державного управління шляхом розвитку електронного урядування як одного з першочергових пріоритетів [2]. Досягнення цілей Концепції здійснюється за такими основними принципами як «цифровий за замовчуванням», одноразового введення інформації, сумісність за замовчуванням, доступність та залучення громадян, відкритість і прозорість, довіра та безпека.

У грудні 2020 року схвалена «Концепція розвитку штучного інтелекту в Україні», що визначає пріоритетні напрями і основні завдання розвитку технологій штучного інтелекту для задоволення прав та законних інтересів фізичних та юридичних осіб, побудови конкурентоспроможної національної економіки, вдосконалення системи публічного управління в Україні [3].

Основною метою Закону України «Про особливості надання публічних (електронних публічних) послуг» (№1689-IX від 15.07.2021 р.) є запровадження режиму «без паперів» (paperless). Відтепер державні органи в Україні не мають права вимагати у громадян паперові документи, довідки та посвідчення, якщо ця інформація є в державних реєстрах. Також закріплений терміни «електронна публічна послуга» – послуга, що надається органами державної влади, органами місцевого самоврядування, підприємствами, установами, організаціями, які перебувають в їх управлінні, у тому числі адміністративна послуга (у тому числі в автоматичному режимі), яка надається з використанням інформаційно-телекомунікаційних систем на підставі заяви, поданої в електронній формі з використанням інформаційно-телекомунікаційних систем, або без подання такої заяви [4].

У цьому ж році, в межах Закону України «Про стимулювання розвитку цифрової економіки в Україні» (№ 1667-IX від 15.07.2021 р.) врегульовані організаційні, правові та

фінансові засади функціонування правового режиму «Дія Сіті», запровадженого з метою стимулювання розвитку цифрової економіки в Україні шляхом створення сприятливих умов для ведення інноваційного бізнесу, розбудови цифрової інфраструктури, залучення інвестицій, а також талановитих спеціалістів [5].

Для пришвидшення цифровізації в Україні у 2021 році Мінцифри впровадила унікальну посаду – CDTO (Chief Digital transformation Officer), тобто заступники з цифрової трансформації, які сьогодні вже є в кожному міністерстві та поступово з'являються в обласних державних адміністраціях та громадах. Задля реалізації повноважень Мінцифри в регіонах у штатах обласних державних адміністрацій функціонують департаменти і управління цифрової трансформації, інформаційних технологій та електронного урядування.

Наприкінці 2022 року актуалізовано Закон України «Про Національну програму Інформатизації», що визначає особливості реалізації державної політики у сфері інформатизації для забезпечення потреб та розвитку інформаційного суспільства, впровадження інформаційно-комунікаційних та цифрових технологій [6].

Навіть в умовах війни клімат для цифровізації в Україні можна охарактеризувати як сприятливий, а цикл законодавчих ініціатив як динамічний.

Водночас, насичення новостворених інформаційних систем персональними даними про особу, відомостями, що становлять службову інформацію і міститься в документах суб'єктів владних повноважень, зібрані у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни обумовлює необхідність завчасної організації їх технічного захисту, адже витік такої інформації може завдати шкоди як охоронюваним правам людини і громадянина, так і національним інтересам в цілому.

Аналіз останніх досліджень і публікацій. Науково-дослідні розробки у сфері технічного захисту інформації, пошук дієвих моделей безпеки, алгоритмів захисту від несанкціонованих дій беруть свій початок з п'ятдесятих років минулого століття від моменту винаходу першого програмованого електронного комп'ютеру.

Наукові розвідки у галузі інформаційної безпеки, технічного захисту інформації проводили Рибальский О.В., Хахановський В.Г., Кудінов В.А. Питанням протидії протиправній діяльності у сфері інформаційних технологій, інтелектуальної власності присвячені дослідження Кондратьєва Я.Ю., Ніколаюк С.І., Никифорчук Д.Й., Томма Р.П., Барко В.І. Адміністративно-правові основи кібербезпеки в умовах гібридної війни досліджувались Веселовою Л.Ю., оригінальний алгоритм захисту персональних даних від атак зловмисників досліджував Лаптєв С.О. Початок російського вторгнення надав імпульс для наукового осмислення досі невідомих проблем протидії ворогові у кіберпросторі. Провідну роль у фіксації статистичних показників кібератак з боку країни-агресора, розробці інструкцій для громадян із попередження, розпізнавання та локалізації кібератак відіграє Державна служба спеціального зв'язку та захисту інформації України, зокрема, Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA.

Швидкоплинність розвитку ІТ-індустрії, інформаційних технологій, перебудова архітектури та принципів роботи інформаційних систем обумовлюють сталу актуальність питань технічного захисту інформації та наукового пізнання даної сфери людської діяльності.

Мета статті. Висвітлити нормативно-правове регулювання технічного захисту інформації в державних інформаційних системах, реальний стан справ у даній сфері, найбільш актуальні проблемні питання. Акцентувати увагу на нагальній потребі впровадження систем захисту інформації з обмеженим доступом та сформувати пропозиції щодо подолання існуючих негативних чинників.

Виклад основного матеріалу. Статтею 11 Закону України «Про інформацію» визначено, що інформація про фізичну особу або персональні дані – це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована [7]. Збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах нацбезпеки, економічного добробуту та захисту прав людини не допускається. До конфіденційної інформації про

фізичну особу належать, зокрема, дані про її національність, освіту, сімейний стан, релігійні переконання, стан здоров'я, а також адреса, дата і місце народження.

Конфіденційна інформація являється інформацією з обмеженим доступом про фізичну особу, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, а також інформація, визнана такою на підставі закону.

Процес оброблення персональних даних передбачає будь-яку дію або сукупність дій, таких як збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання і поширення (розповсюдження, реалізація, передача), знеособлення, знищення персональних даних, у тому числі з використанням інформаційних (автоматизованих) систем [8].

Питання щодо обов'язковості вжиття заходів із забезпечення захисту інформації та кіберзахисту визначені Стратегією кібербезпеки України (№447/2021).

Законом України «Про захист інформації в інформаційно-комунікаційних системах» встановлено вимогу у відношенні державних інформаційних ресурсів або інформації з обмеженим доступом, в тому числі і персональних даних. Вони повинні оброблятися в системі із застосуванням комплексної системи захисту інформації *(взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації, далі – КСЗІ)* з підтвердженою відповідністю.

Підтвердження відповідності та проведення державної експертизи засобів технічного і криптографічного захисту інформації здійснюються в порядку, встановленому законодавством. Для створення комплексної системи захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, використовуються засоби криптографічного захисту інформації, які мають позитивний експертний висновок за результатами державної експертизи у сфері криптографічного захисту інформації, та засоби технічного захисту інформації, які мають позитивний експертний висновок за результатами державної експертизи у сфері технічного захисту інформації або сертифікат відповідності, виданий акредитованим органом з оцінки відповідності [9].

Одним із напрямів цифровізації в органах публічної влади, секторі безпеки і оборони є повсюдне впровадження комп'ютерів, локальних та Глобальної інформаційних мереж, інформаційних систем тощо. Взаємодія таких органів і військових формувань між собою, діалог з суспільством передбачає доступ до численних інформаційних ресурсів та обумовлену цим обробку персональних даних громадян, службової інформації. Тож питання впровадження КСЗІ поряд з експлуатацією таких інформаційних систем є безкомпромісним.

Діюче законодавство, зокрема НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу» [10] встановлює класифікацію автоматизованих систем (АС) в залежності від мети їх використання та топології пов'язаних з ними мереж.

Зокрема, АС класу 1 – це однокомп'ютерний комплекс, розрахований на використання обмеженим колом користувачів (не більше 8), що не має підключення до локальної мережі та мережі Інтернет. Зазвичай використовується для обробки інформації з грифами обмеження доступу «Для службового користування» (четверта категорія), «Таємно» (третя категорія), «Цілком таємно» (друга категорія). АС класу 1 це ноутбук чи стаціонарний комп'ютер у захищеному варіанті виконання, комплекс додаткового програмного забезпечення (антивірус, засоби розмежування доступу тощо), а також перелік визначених системних налаштувань, що розташований у спеціально обладнаному для нього приміщенні.

АС класу 2 представляє собою багатомашинний багатокористувачевий комплекс, об'єднаний в одну локальну мережу, що не підключена до мережі Інтернет. Вона також може використовуватись для обробки конфіденційної, службової, таємної інформації, є локальною мережею з персональних комп'ютерів у захищеному виконанні і серверів.

АС класу 3 – багатокомп'ютерний комлпекс, розрахований на чимале коло користувачів і об'єднаний в одну або декілька локальних мереж з доступом до Інтернету. У такій системі зазвичай циркулює як інформація з обмеженим доступом, так і відкрита інформація. АС

класу 3 є мережею з комп'ютерів і серверів в незахищеному варіанті виконання. Включає ряд керованих комутаторів, маршрутизаторів, систему виявлення атак, апаратний або програмний мережевий екран, антивірус, засоби розмежування доступу і т. ін, а за необхідності ще і комплекс засобів технічного і криптографічного захисту інформації.

Відтак організація цифрової взаємодії в держорганах, силових структурах через використання інформаційних систем зазвичай передбачає побудову автоматизованих систем класу 3, де передбачена циркуляція з обмеженим доступом.

Згідно чинного законодавства України, підтвердженням належного рівня захисту інформації в інформаційній системі, що надає право обробки в ній інформації з обмеженим доступом є наявність Атестату відповідності КСЗІ.

Створення КСЗІ описане у НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі» [11]. Ініціатор самостійно або через підрядну організацію відпрацьовує технічне завдання на КСЗІ, яке погоджує з Державною службою спеціального зв'язку та захисту інформації України. Надалі керуючись техзавданням, ініціатор проектує, впроваджує та вводить КСЗІ у дослідну експлуатацію. Після отримання заявки ініціатора Держспецзв'язок призначає організатора державної експертизи КСЗІ з відповідною ліцензією. За результатами проведення експертних випробувань проект експертного висновку подається до Держспецзв'язку, який у разі його відповідності передбаченим вимогам, видає атестат відповідності КСЗІ.

Тобто побудова КСЗІ в сучасних умовах процес непростий, він довготривалий і дороговартісний, адже включає себе регламентовану послідовність етапів робіт: організаційних, інженерних, проектних, пусконалагоджувальних. Терміни їх проведення можуть становити від декількох місяців, а вартість стартувати від сотень тисяч гривень.

Відповідно до Положення про державну експертизу у сфері технічного захисту інформації експертиза КСЗІ проводиться шляхом експертних випробувань або шляхом аналізу декларації [12]. Перший шлях – передбачає побудову КСЗІ «з нуля» та проходження усіх визначених етапів її створення. Аналіз і реєстрація декларації передбачає використання технічних рішень «під ключ» і суттєво спрощують процедуру побудови КСЗІ. Такі рішення включають готові засоби, заходи захисту інформації від витоку технічними каналами, організаційно-технічні рішення для впровадження типових компонентів КСЗІ з чинним позитивним експертним висновком за результатами державної експертизи в сфері ТЗІ (актом атестації комплексу ТЗІ).

На офіційному веб-сайті Держспецзв'язку наявний у доступі «Перелік засобів ТЗІ, які мають експертний висновок про відповідність до вимог технічного захисту інформації», що включає понад 430 найменувань засобів, їх призначення та контактну інформацію виробників. В переліку є захищені комп'ютери, програмне забезпечення, мережеве обладнання, засоби ТЗІ тощо.

Водночас проведений моніторинг цінових пропозицій показав, що сумарна вартість АС класу 1 з атестатом КЗСІ для обробки інформації з найвищим грифом «Таємно», виготовленій з використанням загальнодоступних на ІТ-ринку України засобів електронно-обчислювальної техніки, периферійного обладнання, програмного забезпечення відрізняється від аналогічного екземпляра без пакету дозвільної документації на обробку інформації з обмеженим доступом щонайменше втричі у бік здорожчання.

Беручи до уваги присутність в АС класу 3 великої кількості комп'ютерів і можливо інших інформаційних систем, серверного, мережевого обладнання та спеціалізованого програмного забезпечення, обсяг робіт зі створення КСЗІ значно більший, а згадане цінове співвідношення може змінюватись лише у бік зростання.

Наряду з завданнями у сфері інформатизації та цифровізації до основних завдань підпорядкованих CDTO регіональних департаментів і управлінь цифрового розвитку, цифрових трансформацій і цифровізації віднесено реалізацію державної та формування регіональної політики у сфері кіберзахисту, технічного захисту інформації, вимога щодо захисту якої встановлена законом.

Відповідно до Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, відповідальність за забезпечення захисту інформації в системі, своєчасне розроблення необхідних для цього заходів та створення системи захисту, згідно покладається на керівника або заступника керівника організації, яка є власником чи розпорядником системи, та керівників її структурних підрозділів, що забезпечують створення та експлуатацію системи [13]. Організація та проведення робіт із захисту інформації в системі здійснюється службою захисту інформації, яка утворюється згідно з рішенням керівника організації.

Досягнення амбітних цілей проєкту «Цифрова держава», достатнього рівня інформаційної взаємодії Збройних сил України, правоохоронних, розвідувальних органів, державні органи спеціального призначення з правоохоронними функціями потребує захисту охороняємих законом даних від несанкціонованих дій. Організація такого захисту повинна бути комплексною і всеосяжною, тобто поширюватися на всі потенційно уразливі елементи і ділянки інформаційних систем. Однак сьогодні, на думку автора, стрімкі процеси цифровізації в країні протікають з випередженням процесів впровадження КСЗІ.

Так, анонсовані у 2020 році атестати відповідності КСЗІ [14] на систему електронної взаємодії державних електронних інформаційних ресурсів «Трембіта» та її підсистему «Вулик» стосуються лише їх програмних комплексів. Тобто, у разі відкриття чергового центру надання адміністративних послуг, уся розгорнута в ньому мережа комп'ютерів у складі інформаційної системи підлягає обов'язковій процедурі створення КЗСІ в загальноприйнятому порядку. Як наслідок, відсутність КЗСІ в окремому регіональному сегменті або секторі загальнодержавних інформаційних ресурсів створює загрози конфіденційності, цілісності і доступності наших персональних даних.

Прийнята парламентаріями ще у 1997 році «Концепція технічного захисту інформації в Україні», визначає основи державної політики у сфері захисту інформації інженерно-технічними заходами, принципи формування і проведення державної політики у цій сфері, основні функції організаційних структур [15]. Незважаючи на її понад 20-ти річну давність, такі напрями державної політики у сфері ТЗІ, як удосконалення правових механізмів організаційного забезпечення ТЗІ; удосконалення чинних та розроблення нових нормативних документів з питань ТЗІ; забезпечення створення підрозділів ТЗІ в органах державної влади та органах місцевого самоврядування, академіях наук, Збройних Силах, інших військових формуваннях, органах внутрішніх справ, на підприємствах, в установах і організаціях всіх форм власності, діяльність яких пов'язана з інформацією, що підлягає технічному захисту; розвиток міжнародного співробітництва в сфері ТЗІ; пріоритетне створення вітчизняних конкурентоспроможних інформаційних технологій та розвиток виробництва засобів забезпечення ТЗІ, зберігають свою актуальність і сьогодні.

Оцифровування нинішнього буття та обумовлене ним примноження обсягів кіберфізичного простору ставить перед нами складну проблему: з одного боку цифрова трансформація, впровадження інформаційних систем та досягнень ІТ-галузі покликані забезпечувати суспільні блага, а з іншого створюють останньому загрози, пов'язані з можливим втручанням у приватне життя і порушенням стану захищеності національних інтересів. Основним інструментом нейтралізації таких загроз є розроблення дієвих організаційно-правових та інженерно-технічних механізмів функціонування інформаційних систем та їх невід'ємних елементів – КСЗІ.

Сьогодні на фоні оптимістичних обнародувань проєктів цифровізації в різних державних органах існує чималий пласт невирішених питань, пов'язаних з невідповідністю інформаційних систем вимогам нормативно-правових актів у сфері технічного захисту інформації. Частина з них вирішується паралельно з експлуатацією інформаційних систем, решта посилається на умови воєнного стану і крайньої необхідності.

Як підсумок, перейти рубікон на даному напрямі цифрового розвитку України означає відшукати шляхи оптимального співвідношення таких категорій як час і гроші. На

думку автора, починати треба з реновації концептуальних засад технічного захисту інформації шляхом максимально можливого зменшення бюрократичних процедур побудови КСЗІ, розробки механізмів державного регулювання ціноутворення на атестовані засоби ТЗІ, збільшення бюджетних асигнувань, уніфікації організаційних і апаратно-програмних рішень на стадіях проєктування інформаційних систем, збільшення штату фахівців з ТЗІ в органах влади, секторі безпеки і оборони, організація підвищення їх кваліфікації на регулярній основі.

Через призму Шевченківських слів «І чужому научайтесь, й свого не цурайтесь…» варто провести запозичення найбільш релевантних для України положень міжнародних стандартів інформаційної безпеки ISO/IEC 15408-1 та ISO/IEC 27001, модифікацію діючого нині НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» задля їх адаптації до умов сучасності.

Замість сьогоднішнього надмірного формалізму запровадити експертне дослідження впровадженої КСЗІ з тестуванням на несанкціоноване проникнення, адже масовані DDoS-атаки у 2012, 2022 роках на веб-сайти державних органів засвідчили, що серед них були блоковані ресурси і з КСЗІ.

Широкомаштабна інституціалізація технологій Artificial intelligence, Cloud Technology, BigData у світі поглине і Україну, сподіваємось у найближчому майбутньому. Вимоги до таких об'єднаних конфігурованих обчислювальних ресурсів у сфері захисту інформації та кібербезпеки, які по суті являються метасистемами, потенційно обширні. Вказані обставини вимагають стратегічного та упереджувального бачення завтрашнього дня і вжиття комплексних організаційно-правових заходів вже сьогодні.

Список використаних джерел:

1. Офіційний веб-сайт The International Open Data Charter, URL: https://opendatacharter.net/who-we-are/.

2. Розпорядження Кабінету Міністрів України від 20 вересня 2017 р. № 649-р «Про схвалення Концепції розвитку електронного урядування в Україні», редакція від 20.09.2017, URL: https://zakon.rada.gov.ua/laws/show/649-

2017-%D1%80#top, (дата звернення: 25.09.2023).

3. Розпорядження Кабінету Міністрів України від 2 грудня 2020 р. № 1556-р «Про схвалення Концепції розвитку штучного інтелекту в Україні», редакція від 29.12.2021. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text, (дата звернення: 25.09.2023).

4. Закон України «Про особливості надання публічних (електронних публічних) послуг» 15 липня 2021 року № 1689-IX, редакція від 31.03.2023. URL: https://zakon.rada.gov.ua/laws/show/1689-20#Text, (дата звернення: 25.09.2023).

5. Закон України «Про стимулювання розвитку цифрової економіки в Україні» від 15 липня 2021 року № 1667-IX, редакція від 01.01.2023. URL: https://zakon.rada.gov.ua/laws/show/1667-20#Text, (дата звернення: 25.09.2023).

6. Закон України «Про Національну програму інформатизації» від 01.12.2022 р. № 2807-IX, редакція від 01.12.2022. URL: https://zakon.rada.gov.ua/laws/show/2807-20#Text, (дата звернення: 25.09.2023).

7. Закон України «Про інформацію» від 02.10.1992 року № 2657-XII, редакція від 27.07.2023. URL: https://zakon.rada.gov.ua/laws/show/2657-12#n148, (дата звернення: 25.09.2023).

8. Закон України від 1 червня 2010 року № 2297-VI «Про захист персональних даних», редакція від 27.10.2022. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text, (дата звернення: 25.09.2023).

9. Закон України «Про захист інформації в інформаційно-комунікаційних системах» від 5 липня 1994 року № 80/94-ВР, редакція від 01.07.2022. URL: https://zakon.rada.gov.ua/laws/show/80/94%D0%B2%D1%80#top, (дата звернення: 25.09.2023).

10. Нормативний документ ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу», затверджений наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації СБУ від 28 квітня 1999 р. № 22, редакція від 15.10.2008. URL: https://tzi.ua/assets/files/%D0%9D%D0%94-%D0%A2%D0%97%D0%86-2.5-005--99.pdf, (дата звернення: 25.09.2023).

11. Нормативний документ ТЗІ 3.7-003-2005 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі», затверджений наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації СБУ від 08.11.2005 р. № 125, редакція від 28.12.2012. URL: https://tzi.com.ua/downloads/3.7-003-2005.pdf, (дата звернення: 25.09.2023).

12. Наказ Адміністрації ДССЗЗІ від 16 травня 2007 року № 93 «Про затвердження Положення про державну експертизу у сфері технічного захисту інформації», редакція від 11.10.2022. URL: https://zakon.rada.gov.ua/laws/show/z0820-07#Text, (дата звернення: 25.09.2023).

13. Постанова Кабінету Міністрів України від 29 березня 2006 р. № 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах», редакція від 21.10.2022, URL: https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF#Text. (дата звернення: 25.09.2023).

14. Веб-сайт Мінцифри URL: https://thedigital.gov.ua/news/otrimano-atestat-vidpovidnosti-kompleksnoi-sistemi-zakhistu-informatsii-yadra-sistemi-trembita.

15. Постанова Кабінету Міністрів України від 8 жовтня 1997 р. № 1126 «Про затвердження Концепції технічного захисту інформації в Україні», редакція від 13.10.2011. URL: https://zakon.rada.gov.ua/laws/show/1126-97-%D0%BF#Text, (дата звернення: 25.09.2023).