КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (34), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.34.1263
УДК 004.056:004.7

Паламарчук Наталія Анатоліївна
провідна наукова співробітниця науково-дослідної лабораторії
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна
ORCID:0000-0001-8818-7794
nataliia.palamarchuk@viti.edu.ua

Паламарчук Світлана Анатоліївна
начальниця науково-дослідного відділу
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна
ORCID:0000-0001-7483-9165
svitlana.palamarchuk@viti.edu.ua

Овсянніков Вячеслав Володимирович
кандидат технічних наук, старший науковий співробітник науково-дослідної лабораторії
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна
ORCID:0000-0003-0186-6220
2081364@gmail.com

Побережець Тетяна Василівна
наукова співробітниця науково-дослідної лабораторії
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна
ORCID:0000-0001-8007-8614
tetiana.poberezhets@viti.edu.ua

Вороной Олександр Васильович
науковий співробітник науково-дослідного відділу
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна
ORCID:0009-0007-1427-4431
avoronoj423@gmail.com

АСПЕКТИ СТВОРЕННЯ ЗАХИЩЕНИХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ

Анотація. У статті розглянуто створення захищених інформаційно-комунікаційних систем в умовах реформування системи кіберзахисту в Україні на основі міжнародних стандартів та практик. Виокремлено нормативні, організаційні та технічні аспекти створення захищених ІКС відповідно до вимог законодавства. Наразі відбувається перехід від класичної моделі створення комплексних систем захисту інформації та їх державної експертизи до ризик-орієнтованого підходу, що ґрунтується на застосуванні профілів безпеки та авторизації систем з безпеки. Розглянуто та проаналізовано складові сучасної інформаційної інфраструктури, зокрема, автоматизовані системи класів 1, 2 і 3, хмарні технології та сервіси/послуги, що надаються централізованими сервісними інфраструктурами, а також підходи до організації захисту за умови обробки державних інформаційних ресурсів або інформації з обмеженим доступом. Серед розповсюджених безпекових сервісів (функцій) виокремлено застосування захищених вузлів доступу до мережі Інтернет, центрів реагування на кіберінциденти (Security Operations Center), кваліфікованих надавачів електронних довірчих послуг та засобів електронної ідентифікації. Окрему увагу приділено організації захисту інформації та кіберзахисту ІКС, розгорнутих у хмарній інфраструктурі (хмарні послуги), на основі моделі спільної відповідальності між провайдером хмарних послуг та власником ІКС. Узагальнено основні підходи до організації захисту інформації (інформаційної безпеки) та кіберзахисту залежно від класу системи, ступеня обмеження доступу до інформації та умов функціонування інформаційної інфраструктури.

Ключові слова: авторизована система з безпеки; автоматизована система; захист інформації; інформаційно-комунікаційна система; кіберзахист; кібербезпеки; комплексна система захисту інформації; технологія хмарних обчислень.

ВСТУП

Постійна інтеграція інформаційних технологій у процеси життєдіяльності обумовлює актуальність та пріоритетність забезпечення захисту інформації та кіберзахисту інформаційно-комунікаційних систем (далі – ІКС, система). При цьому, ІКС, функціонують в умовах ускладнення їхньої архітектури, широкого використання розподілених інформаційних технологій та стрімкого зростання кількості та складності кіберзагроз (особливо з початком повномасштабного військового вторгнення російської федерації), розширення кіберпростору як критично важливої інфраструктури держави, його технологічною основою. Досвід війни в Україні показав, що в ході військового конфлікту реалізуються різноманітні концепції кібератак, які направлені на реалізацію несанкціонованого доступу до ресурсів і даних ІКС та які призводять як до появи нових загроз витоку інформації так і порушення функціонування системи в цілому [1]. Оскільки кіберпростір виступає як платформа для реалізації сучасних гібридних війн, зазначене окреслює актуальність дослідження питань забезпечення захисту інформації в ІКС та їх кіберзахисту.

Постановка проблеми. Наразі в Україні триває реформування системи кіберзахисту, спостерігається еволюція нормативно-правового регулювання у сфері захисту інформації, інформаційної та кібербезпеки, яка спрямована на гармонізацію національних підходів із міжнародними стандартами та практиками [2-4]. За таких умов традиційне розмежування понять “захист інформації”, “кіберзахист” та “кібербезпека” поступово втрачає чіткі межі через їх функціональну взаємозалежність. Зокрема, захист інформації забезпечує базовий рівень збереження конфіденційності, цілісності та доступності інформації, кіберзахист орієнтований на операційне реагування на кіберінциденти в ІКС, кібербезпека охоплює комплекс заходів спрямованих на забезпечення стійкого функціонування кіберпростору. Таким чином, актуальним є аналіз та узагальнення вимог законодавства у сферах захисту інформації, кіберзахисту та кібербезпеки, оскільки фрагментований, розрізнений підхід ускладнює практичну реалізацію систем захисту та знижує загальну кіберстійкість України до сучасних загроз (розглянемо їх на прикладі інтеграції вимог законодавства в умовах реформування системи кіберзахисту в Україні).

Аналіз останніх досліджень і публікацій. Питання захисту інформації, кіберзахисту та кібербезпеки ІКС досліджуються у наукових працях вітчизняних і зарубіжних авторів, а також визначеніні у нормативно-правових актах України, міжнародних стандартах та методичних документах у сфері інформаційної безпеки та технологій [2-4], [7-9]. Значна частина досліджень присвячена питанням побудови систем захисту інформації, управління ризиками інформаційної безпеки, впровадження міжнародних стандартів серії ISO/IEC 27000, підходів NIST [10-16] та розвитку систем кіберзахисту критичної інформаційної інфраструктури [9, 17].

Важливі питання для осмислення інформаційної та кібербезпеки як складових національної безпеки держави охарактеризовані в працях вітчизняних вчених: Хорошка В.О., Юдіна О.К., Богуша В.М., Корченко Л.Г., Бурячок В.Л., Корченка О.Г., Субача І.Ю., Тулюпи С., та ін. У [18] Луценко В.М. розглянуто створення систем захисту інформації на визначених етапах створення ІКС та запропоновано підхід до вдосконалення методики проектування системи захисту інформації на об’єктах інформаційної діяльності та комплексної системи захисту інформації (далі – КСЗІ). У [19], Лукова-Чуйко Н., Наконечний В., Толюпа С., Зюбіна Р. досліджено проблеми захисту критично важливих об’єктів інфраструктури. У [20], С. Тулюпою та С Штаненко проаналізовано системи керування інформаційною безпекою та запропоновано математичну модель взаємовідносин системи керування інформаційною безпекою.

Водночас питання комплексного узагальнення нормативно-організаційних і технічних аспектів створення захищених ІКС залишаються недостатньо дослідженими, систематизованими, висвітлені фрагментарно та містять певні розбіжності.

Метою статті є аналіз та узагальнення вимог законодавства із забезпечення захисту інформації, кіберзахисту та кібербезпеки в умовах реформування системи кіберзахисту в Україні.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Нормативні та організаційні аспекти: Захист інформації в системах історично формувався як сукупність правових, організаційних, технічних та інших заходів, що забезпечують конфіденційність, цілісність, доступність інформації та належний порядок доступу до неї.

При обробці інформації з різними грифами обмеження доступу в сучасних ІКС, питання захисту інформації є одним із пріоритетних, і повинно мати комплексний характер, незалежно від технології побудови ІКС – на власній фізичній інфраструктурі або з використанням хмарних технологій. Захищені ІКС не розглядаються окремо від інформації, яка в них обробляється. Згідно [3]: “об’єктами захисту в

системі є інформація, що обробляється в ній, та програмне забезпечення, яке призначено для обробки цієї інформації".

Традиційно (майже з моменту незалежності України), захист інформації в ІКС, а згодом і захист об'єктів критичної інформаційної інфраструктури забезпечувався шляхом впровадження КСЗІ з підтвердженою відповідністю або системи управління інформаційною безпекою (далі – СУІБ), побудованої відповідно до міжнародних стандартів у сфері інформаційної безпеки.

КСЗІ – взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації. Створення КСЗІ було обов'язковим при умові обробки в ІКС інформації, яка є власністю держави або належить до державної таємниці. Підтвердження відповідності КСЗІ здійснювалося за результатами державної експертизи шляхом експертних випробувань або аналізу декларації. Державна експертиза КСЗІ – це процедура підтвердження відповідності КСЗІ вимогам нормативних документів з питань технічного захисту інформації (далі – ТЗІ) [3].

СУІБ – (англ. – Information Security Management System, ISMS) – являє собою частину загальної системи управління організацією, що заснована на ризик-орієнтованому підході та призначена для створення, реалізації, експлуатації, моніторингу, аналізу, підтримки та вдосконалення інформаційної безпеки організації. Підтвердження відповідності стандарту інформаційної безпеки за результатами процедури з оцінки відповідності національним стандартам України здійснюється органом з оцінки відповідності. Процедура отримання сертифікату відповідності стандарту інформаційної безпеки не застосовується до систем, в яких обробляється інформація, що становить державну таємницю [3].

З прийняттям Закону України "Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури" від 27.03.2025 №4336-IX [2] (далі – Закон №4336-IX) розпочато реформування системи кіберзахисту в Україні, яке оновлює підходи до кіберзахисту та захисту інформації, запроваджує дієві механізми управління ризиками, реагування на кіберзагрози та обов'язкове навчання з кібергігієни (шляхом інтеграції зазначених сфер). Це призвело до внесення змін у базові Закони України, зокрема, "Про захист інформації в ІКС" [3] та "Про основні засади забезпечення кібербезпеки" [4]. Так, згідно [3], державні інформаційні ресурси або інформація з обмеженим доступом мають оброблятися в авторизованих системах з безпеки чи шляхом отримання сертифіката відповідності стандарту інформаційної безпеки (також не застосовується до ІКС, в яких обробляється державна таємниця). Відповідно, змінено підходи до захисту інформації в ІКС від несанкціонованого доступу, від витоку технічними каналами – поки що без змін.

Як відмічалося, зміни законодавства є кроком до реформування системи кіберзахисту, яке здійснюється у відповідності до гармонізованих та міжнародних стандартів та практик (ДСТУ ISO/IEC серій 27001, 27002, 27005, NIST SP 800-53, NIST SP 800-30, NIST SP 800-171(172), NIST SP 800-171A(172A), тощо), фундаментальним елементом у переході від класичної моделі створення КСЗІ та її експертизи, до гнучкого та адаптивного ризик-орієнтованого підходу (розпочинається з оцінки активів, ризиків та загроз), що ґрунтується на авторизації систем з безпеки.

Авторизація з безпеки – рішення щодо можливості функціонування (експлуатації) відповідної системи з урахуванням її відповідності вимогам законодавства, національним стандартам та нормативним документам у сферах технічного захисту, криптографічного захисту та кіберзахисту, що приймається у встановленому законодавством порядку.

Авторизована система з безпеки – інформаційна, електронна комунікаційна, інформаційно-комунікаційна, технологічна система або її окремі елементи, об'єкт критичної інформаційної інфраструктури, в яких запроваджені заходи та/або системи з безпеки інформації, що пройшли авторизацію з безпеки [3].

Згідно змін законодавства [2, 3], авторизовані системи з безпеки створюються з використанням відповідних профілів безпеки (базового, галузевого та/або цільового) для інформації різних грифів та з використанням засобів захисту, які мають позитивний експертний висновок за результатами експертизи у сфері технічного та/або криптографічного захисту інформації. Порядок авторизації з безпеки передбачає встановлення повідомного (декларативного) принципу щодо прийняття рішення про здійснення авторизації з безпеки з урахуванням відповідних профілів безпеки (крім тих, де обробляється державна таємниця) та порядок підтвердження дотримання вимог з безпеки таких систем, а також об'єктів критичної інформаційної інфраструктури відповідно до базового, цільового та галузевого (за наявності) протягом життєвого циклу відповідної системи [7, 8].

Профіль безпеки – це реалізаційно незалежний набір заходів захисту, який відображає потреби в безпеці інформації та приватності особистого життя, що обумовлені цілями та завданнями організації, призначенням інформаційної системи, критичністю інформації та ризиками безпеки [21].

Так, базовим профілем безпеки передбачено [22], [23]: для конфіденційної інформації – 129 заходів безпеки; для службової інформації – 158 заходів безпеки. Для порівняння, заходи безпеки згідно НД ТЗІ 2.5-004-99 "Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу" відповідають лише 35 заходам безпеки базових профілів, з яких 10 частково відповідають вимогам базових профілів, що становить ~20% заходів безпеки згідно сучасних стандартів [1].

Таким чином, наразі йде так званий перехідний період від КСЗІ до авторизованих систем з безпеки, триває процес реалізації норм Закону №4336-IX [2] на рівні держави та відомств, узгоджується підготовка фахівців за цими стандартами (спеціалізаціями). Відомствами здійснюється (здійснено) розробка галузевих/цільових профілів безпеки та приведення у відповідність відомчих нормативних документів. При цьому, КСЗІ (СУІБ), створені та оцінені до набрання чинності Закону України [3] застосовуються відповідно до умов їх створення та не потребують повторного підтвердження відповідності (авторизації) до завершення терміну дії документу про оцінку їх відповідності. В разі обробки в ІКС інформації, що становить державну таємницю, також повинен забезпечуватися захист інформації від витоку технічними каналами, шляхом впровадження комплексу технічного захисту інформації з підтвердженою відповідністю (далі – КТЗІ) [1, 24].

Отож, на даний час, для забезпечення захисту інформації в ІКС застосовується (див. таблиця 1): КСЗІ з підтвердженою відповідністю (дозволено до застосування згідно термінів дії атестатів відповідності/декларацій); авторизовані системи з безпеки (в ІКС, рішення про створення яких прийнято після 18.06.2025); КТЗІ з підтвердженою відповідністю (для ІКС, в яких обробляється державна таємниця).

Отже, з урахуванням викликів сьогодення, нормативна вертикаль у сфері інформаційної та кібербезпеки зазнає масштабних змін, інтегруються міжнародні стандарти та практики для підвищення рівня захисту/кіберзахисту та оптимізації створення самих систем. Нормативна вертикаль за рівнями вимог наведена на рис. 1.

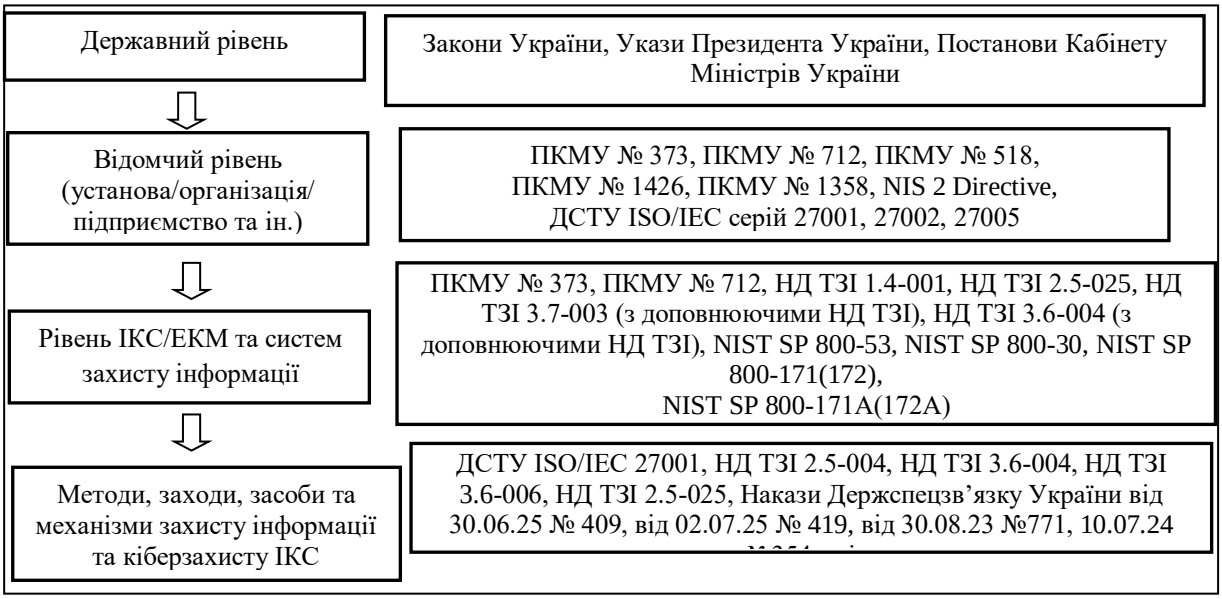

Рис. 1. Рівні вимог щодо захисту інформації та кіберзахисту

З огляду на вищесказане, нормування діяльності у галузі забезпечення кібербезпеки є необхідною умовою підвищення рівня кіберстійкості України в умовах постійного зростання кількості та складності кіберзагроз.

Технічні (технологічні) аспекти: Наразі технічна складова згідно законодавства України представлена трьома класами автоматизованих систем (далі – АС), технологіями хмарних обчислень (послуг), у межах яких формуються вимоги до захисту інформації та кіберзахисту, а також ін. системами (засобами), що забезпечують реалізацію механізмів (функцій) захисту в межах інформаційної інфраструктури.

АС (ІКС) являє собою організаційно-технічну систему, що об'єднує обчислювальну систему, фізичне середовище, персонал і інформацію (це базові елементи, які впливають на формування вимог до захисту). За сукупністю характеристик АС виділяють три ієрархічні класи АС [25]:

АС класу “1” – локалізований одномашинний однокористувачевий комплекс; АС класу “2” – локалізований багатомашинний багатокорстувачевий комплекс; АС класу “3” – розподілений багатомашинний багатокорстувачевий комплекс. Для АС класів “1” та “2” характерним є функціонування в межах контрольованої зони установи, тоді як АС класу “3” передбачає використання глобальних мереж, зокрема мережі Інтернет. Окремим технологічним підходом є використання технології хмарних обчислень, яка забезпечує дистанційний доступ на вимогу користувача до хмарної інфраструктури через електронні комунікаційні мережі.

Хмарна інфраструктура – сукупність програмно-апаратних ресурсів, сервісів та мережевої інфраструктури, що забезпечують централізоване зберігання, обробку, передачу та доступ до даних і інформаційних сервісів через мережу.

Хмарні ресурси – будь-які технічні та програмні засоби або інші компоненти інформаційної (автоматизованої) системи, доступ до яких забезпечують технології хмарних обчислень, зокрема процесорний час (обчислювальна потужність), місце у сховищах даних, обчислювальні мережі, бази даних і комп’ютерні програми [5].

Відповідно, сучасні підходи до створення захищених ІКС характеризуються переходом від локалізованого використання будь-яких ресурсів в межах кожної окремої системи (наприклад, за функціональною діяльністю – база даних персоналу, СЕДО, тощо) та реалізації механізмів захисту (функцій) в ній, до використання централізованої сервісної інформаційної інфраструктури та інфраструктури безпеки.

У такій моделі окремі функції захисту інформації та кіберзахисту реалізуються як зовнішні або успадковані сервіси, що можуть надаватись іншим ІКС за умови виконання встановлених вимог безпеки та забезпечення довіреної взаємодії між системами. До таких сервісів безпеки можуть належати: засоби захищеного доступу до мережі Інтернет; центр моніторингу та реагування на кіберінциденти (Security Operations Center, SOC, SOC); електронні довірчі послуги; електронна ідентифікація та автентифікація; сервіси управління доступом та політиками безпеки, тощо.

Засоби захищеного доступу до мережі Інтернет. Підключення ІКС до мережі Інтернет повинно здійснюватися із застосуванням систем захищеного доступу або через захищені вузли доступу до мережі Інтернет (далі – ЗВІД), на яких створено КСЗІ (СУІБ) відповідно до законодавства. ЗВІД є обов’язковим для державних органів та критичної інфраструктури України, що підключені до Національної телекомунікаційної мережі. Система захищеного доступу до мережі Інтернет є складовою технологічної інфраструктури кіберзахисту, в межах якої реалізуються функції моніторингу, виявлення та реагування на кіберінциденти, зокрема із застосуванням SOC [26, 27].

SOC забезпечує централізований контроль стану безпеки ІКС, збір та аналіз подій безпеки, виявлення аномальної активності, реагування на кіберінциденти та координацію заходів кіберзахисту. В сучасних умовах SOC розглядається як сервісна платформа кіберзахисту, функціональні можливості якої можуть надаватися іншим ІКС за моделлю “безпека як послуга” (Security as a Service).

Електронні довірчі послуги забезпечують реалізацію механізмів електронної ідентифікації, автентифікації, електронного підпису, підтвердження цілісності електронних даних та захищеного електронного документообігу в ІКС. Надання таких послуг здійснюється Кваліфікованими надавачами електронних довірчих послуг відповідно до законодавства [6 Закон].

Інтегрована система електронної ідентифікації забезпечує інтеграцію механізмів електронної ідентифікації та автентифікації у державних ІКС із використанням єдиних вимог, форматів і протоколів для забезпечення захисту інформації та персональних даних [6, 28]. Електронна ідентифікація здійснюється відповідно до схем електронної ідентифікації з використанням засобів автентифікації, з-поміж яких найбільш поширеними є кваліфікований електронний підпис (далі – КЕП), MobileID та Дія.Підпис. При цьому, для електронної ідентифікації юридичних осіб переважно використовується КЕП, для фізичних осіб – MobileID та BankID.

Захист інформації та кіберзахист хмарної інфраструктури. Особливістю забезпечення захисту інформації та кіберзахисту ІКС, розгорнутих на хмарній інфраструктурі, є розподіл функцій безпеки між провайдером хмарної інфраструктури та користувачем сервісу (клієнтом) відповідно до моделі спільної відповідальності (Shared Responsibility Model). З боку провайдера та користувачів системи забезпечується виконання вимог законодавства у сфері захисту інформації та кіберзахисту, зокрема щодо впровадження авторизованих систем з безпеки або СУІБ відповідно до визначених цільових профілів безпеки та вимог. Провайдер (адміністратор хмари) відповідає за безпеку хмарної інфраструктури, включаючи фізичний захист ЦОД, мережеву та серверну інфраструктуру, віртуалізацію, резервування, моніторинг і реагування на кіберінциденти. Клієнт відповідає за безпеку гостьових систем і сервісів, зокрема управління доступом, оновлення програмного заезпечення, захист даних, моніторинг подій безпеки, резервне копіювання та реагування на інциденти. Такий підхід забезпечує розмежування зон

відповідальності між ними та дозволяє реалізувати багатоешелонований захист інформації в хмарній інфраструктурі [5, 29, 30].

Отже, за результатами аналізу та узагальнення вимог законодавства у сферах захисту інформації, кіберзахисту та кібербезпеки виокремлено нормативні, організаційні та технічні (технологічні) аспекти організації безпеки ІКС. При їх реалізації необхідно враховувати ступінь обмеження доступу до інформації, що обробляється в системі, її клас та інші технологічні особливості, які впливають на забезпечення захисту. Це дозволило узагальнити основні підходи до організації захисту інформації та кіберзахисту різних ІКС (див. таблицю 1).

Таблиця 1

Основні підходи до організації захисту інформації та кіберзахисту ІКС

№ з/п	Клас АС / Вид інформації	АС кл. 1	АС кл. 2	АС кл. 3	Технології хмарних обчислень (хмарні послуги)
1.	Відкрита, конфіденційна або службова інформація	КСЗІ або СУІБ або Авторизована система з безпеки з використанням відповідного профілю	КСЗІ або СУІБ або Авторизована система з безпеки з використанням відповідного профілю	КСЗІ або СУІБ або Авторизована система з безпеки з використанням відповідного профілю; SOC; КНЕДП	КСЗІ або СУІБ або Авторизована система з безпеки з використанням відповідного профілю; SOC; КНЕДП
2.	Державна таємниця (секретна інформація)	КСЗІ або Авторизована система з безпеки з використанням відповідного профілю; КТЗІ	КСЗІ або Авторизована система з безпеки з використанням відповідного профілю; КТЗІ	КСЗІ або Авторизована система з безпеки з використанням відповідного профілю; КТЗІ; SOC; КНЕДП	ЗАБОРОНЕНО

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У статті проаналізовано вимоги нормативно-правових актів у сфері захисту інформації, кіберзахисту та кібербезпеки, визначено основні складові інформаційної інфраструктури, розглянуто концептуальні підходи до організації захисту інформації та кіберзахисту ІКС в залежності від ступеня обмеження доступу до інформації та класів систем. Очевидно, що пріоритетна увага наразі приділяється АС класу 3, а також ряду сервісів/послуг, що надаються сервісними інфраструктурами, як то центри обробки даних, хмарні сервіси, центри реагування на кіберінциденти та кваліфіковані надавачі електронних довірчих послуг, тощо. Узагальнено основні підходи до організації захисту інформації та кіберзахисту ІКС.

Перспективами подальших досліджень є удосконалення підходів до оцінки ризиків і кіберстійкості ІКС, а також розроблення практичних методик інтеграції хмарних технологій, сервісів моніторингу безпеки та автоматизованих засобів реагування на кіберінциденти в єдину систему кіберзахисту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Palamarchuk, S., Martyniuk, V., Ovsiannikov, V., & Shuhalii, O. (2025). Transitional period of legislative changes regarding information protection and cybersecurity of information and communication systems. In Proceedings of the V International Scientific and Practical Conference “Communication Systems and Technologies, Informatization and Cybersecurity: Current Issues and Development Trends” (pp. 184–185). VITI. https://mitit.mil.gov.ua/page/science
2. Verkhovna Rada of Ukraine. (2025). Pro vnesennia zmin do deiakykh zakoniv Ukrainy shchodo zakhystu informatsii ta kiberzakhystu derzhavnykh informatsiinykh resursiv, obiektiv krytychnoi informatsiinoi

infrastruktury [On amendments to certain laws of Ukraine regarding information protection and cybersecurity of state information resources and critical information infrastructure facilities] (Law of Ukraine No. 4336-IX, March 27, 2025). https://zakon.rada.gov.ua/laws/show/4336-20#Text

3. Verkhovna Rada of Ukraine. (1994). Pro zakhyst informatsii v informatsiino-telekomunikatsiinykh systemakh [On information protection in information and telecommunication systems] (Law of Ukraine No. 80/94-VR, July 5, 1994). https://zakon.rada.gov.ua/laws/show/80/94-вр#Text
4. Verkhovna Rada of Ukraine. (2017). Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy [On the basic principles of ensuring cybersecurity of Ukraine] (Law of Ukraine No. 2163-VIII, October 5, 2017). https://zakon.rada.gov.ua/laws/show/2163-19#Text
5. Verkhovna Rada of Ukraine. (2022). Pro khmarni posluhy [On cloud services] (Law of Ukraine No. 2075-IX, February 17, 2022). https://zakon.rada.gov.ua/laws/show/2075-20#Text
6. Verkhovna Rada of Ukraine. (2017). Pro elektronnu identyfikatsiiu ta elektronni dovirchi posluhy [On electronic identification and electronic trust services] (Law of Ukraine No. 2155-VIII, October 5, 2017). https://zakon.rada.gov.ua/laws/show/2155-19#Text
7. Cabinet of Ministers of Ukraine. (2025). Deiaki pytannia zakhystu informatsiinykh, elektronnykh komunikatsiinykh, informatsiino-komunikatsiinykh, tekhnolohichnykh system [Certain issues of protection of information, electronic communication, information and communication, and technological systems] (Resolution No. 712, June 18, 2025). https://zakon.rada.gov.ua/laws/show/712-2025-%D0%BF#Text
8. Cabinet of Ministers of Ukraine. (2006). Pro zatverdzhennia Minimalnykh vymoh do zakhystu informatsiinykh, elektronnykh komunikatsiinykh, informatsiino-komunikatsiinykh ta tekhnolohichnykh system [On approval of minimum requirements for the protection of information, electronic communication, information and communication, and technological systems] (Resolution No. 373, March 29, 2006). https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF#Text
9. Cabinet of Ministers of Ukraine. (2019). Pro zatverdzhennia Zahalnykh vymoh do kiberzakhystu obiektiv krytychnoi infrastruktury [On approval of general requirements for cybersecurity of critical infrastructure facilities] (Resolution No. 518, June 19, 2019). https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text
10. National Institute of Standards and Technology. (2020). Security and privacy controls for information systems and organizations (NIST Special Publication 800-53 Rev. 5). https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf
11. National Institute of Standards and Technology. (2012). Guide for conducting risk assessments (NIST Special Publication 800-30 Rev. 1). https://csrc.nist.gov/pubs/sp/800/30/r1/final
12. European Parliament & Council of the European Union. (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No. 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). Official Journal of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555&qid=1708526
13. International Organization for Standardization, International Electrotechnical Commission, & Institute of Electrical and Electronics Engineers. (2023). Systems and software engineering – System life cycle processes (ISO/IEC/IEEE 15288:2023, 2nd ed.). https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=116499
14. International Organization for Standardization, International Electrotechnical Commission, & Institute of Electrical and Electronics Engineers. (2026). Systems and software engineering – Software life cycle processes (ISO/IEC/IEEE 12207:2026, 2nd ed.). https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=77957
15. DSTU ISO/IEC 27001:2023. (2023). Informatsiina bezpeka, kiberbezpeka ta zakhyst konfidentsiinosti. Systemy keruvannia informatsiinoiu bezpekoiu. Vymohy [Information security, cybersecurity and privacy protection. Information security management systems. Requirements] (ISO/IEC 27001:2022, IDT). https://online.budstandart.com/ua/catalog/doc
16. International Organization for Standardization & International Electrotechnical Commission. (2022). Information security, cybersecurity and privacy protection – Guidance on managing information security risks (ISO/IEC 27005:2022). https://www.iso.org/standard/80585.html
17. Administration of the State Service of Special Communications and Information Protection of Ukraine. (2025). Pro zatverdzhennia Bazovykh zakhodiv z kiberzakhystu, Metodychnykh rekomendatsii shchodo zdiisnennia bazovykh zakhodiv z kiberzakhystu [On approval of basic cybersecurity measures and methodological recommendations for implementing basic cybersecurity measures] (Order No. 54, January 30, 2025). https://surl.lt/ywfofy

18. Lutsenko, V. M. (2011). Correspondence of the stages of building information protection systems to the stages of creating automated systems. Zakhyst Informatsii, (3). https://www.docsity.com/ru/vidpovidnist-etapiv-pobudovi-sistem-zahistu-informaciji-stadiyam-stvorennya-avtomatizovanih-sistem/4654185/
19. Lukova-Chuiko, N., Nakonechnyi, V., Toliupa, S., & Ziubina, R. (2020). Problems of protection of critical infrastructure facilities. Information Systems and Technologies Security, 1(2), 31–39. https://doi.org/10.17721/10.17721/ISTS.2020.1.31-39
20. Toliupa, S., & Shtanenko, S. (2023). Mathematical model of information security management system relationships. Information Systems and Technologies Security, 1(6), 28–36. https://doi.org/10.17721/ISTS.2023.1.28-36
21. Administration of the State Service of Special Communications and Information Protection of Ukraine. (2024). Poriadok vyboru zakhodiv zakhystu informatsii, vymoha shchodo zakhystu yakoi vstanovlena zakonom ta ne stanovyt derzhavnoi taiemnytsi, dlia informatsiinykh system [Procedure for selecting information protection measures for information systems where the information protection requirement is established by law and the information does not constitute a state secret] (ND TZI 3.6-006-24; Order No. 234, April 30, 2024). https://surl.li/gliojs
22. Administration of the State Service of Special Communications and Information Protection of Ukraine. (2025). Pro zatverdzhennia bazovoho profiliu bezpeky systemy, de obrobliaietsia vidkryta abo konfidentsiina informatsiia [On approval of the basic security profile for a system processing open or confidential information] (Order No. 409, June 30, 2025). https://cip.gov.ua/ua/docs/nakaz-pro-zatverdzhennya-bazovogo-profilyu-bezpeki-sistemi-de-obroblyayetsya-vidkrita-abo-konfidenciina-informaciya
23. Administration of the State Service of Special Communications and Information Protection of Ukraine. (2025). Pro zatverdzhennia bazovoho profiliu bezpeky systemy, de obrobliaietsia sluzhbova informatsiia [On approval of the basic security profile for a system processing official information] (Order No. 419, July 2, 2025). https://cip.gov.ua/ua/docs/nakaz-administraciyi-derzhspeczv-yazku-vid-02-07-2025-419-pro-zatverdzhennya-bazovogo-profilyu-bezpeki-sistemi-de-obroblyayetsya-sluzhbova-informaciya
24. Palamarchuk, N. A., Palamarchuk, S. A., Poberezhets, T. V., & Martyniuk, V. V. (2026). Information protection and cybersecurity of information and communication systems in the defense sector: Trends of changes and issues. In Proceedings of the IV International Scientific and Practical Conference “Security and Defense Sector of Ukraine in Protection of National Interests: Current Problems and Tasks under Martial Law” (pp. 1131–1134). NADPSU Publishing House. https://dspace.nadpsu.edu.ua/handle/123456789/5873
25. Department of Special Telecommunication Systems and Information Protection of the Security Service of Ukraine. (1999). Klasyfikatsiia avtomatyzovanykh system i standartni funktsionalni profili zakhyshchenosti obrobliuvanoi informatsii vid nesanktsionovanoho dostupu [Classification of automated systems and standard functional security profiles for processed information against unauthorized access] (ND TZI 2.5-005-99; Order No. 22, April 28, 1999).
26. Cabinet of Ministers of Ukraine. (2020). Deiaki pytannia funktsionuvannia Natsionalnoi elektronnoi komunikatsiinoi merezhi [Certain issues concerning the functioning of the National Electronic Communication Network] (Resolution No. 1358, December 16, 2020). https://zakon.rada.gov.ua/laws/show/1358-2020-%D0%BF#Text
27. Administration of the State Service of Special Communications and Information Protection of Ukraine. (2023). Pro zatverdzhennia Polozhennia pro systemu zakhyshchenoho dostupu derzhavnykh orhaniv do merezhi Internet [On approval of the regulation on the system of secure Internet access for state authorities] (Order No. 771, August 30, 2023). https://zakon.rada.gov.ua/laws/show/z1624-23#Text
28. Cabinet of Ministers of Ukraine. (2023). Pro zatverdzhennia Polozhennia pro intehrovanu systemu elektronnoi identyfikatsii [On approval of the regulation on the integrated electronic identification system] (Resolution No. 1150, November 3, 2023). https://zakon.rada.gov.ua/laws/show/1150-2023-%D0%BF#Text
29. Radchenko, M. M., Dykyi, O. V., Palamarchuk, N. A., Palamarchuk, S. A., & Bondarenko, O. Ye. (2021). Approaches to information protection in information and telecommunication systems built using cloud technologies. Visnyk VITI. Communication and Information Systems, (2), 82–95. https://www.viti.edu.ua/files/zbk/2021/2021-2.pdf
30. Zhylin, A., Divitskyi, A., & Kozachok, A. (2019). Problems of information resources protection when using cloud technologies. Information Technology and Security, 7(2), 171–182. https://ela.kpi.ua/handle/123456789/33886

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (34), 2026
ISSN 2663 – 4023

Nataliia Palamarchuk
Leading Researcher of the Research Laboratory
Heroes of Kruty Military Institute of Information and Telecommunication Technologies, Kyiv, Ukraine
ORCID:0000-0001-8818-7794
nataliia.palamarchuk@viti.edu.ua

Svitlana Palamarchuk
Head of the Research Department
Heroes of Kruty Military Institute of Information and Telecommunication Technologies, Kyiv, Ukraine
ORCID:0000-0001-7483-9165
svitlana.palamarchuk@viti.edu.ua

Viacheslav Ovsiannikov
Candidate of technical sciences, Senior Researcher of the Research Laboratory
Heroes of Kruty Military Institute of Information and Telecommunication Technologies, Kyiv, Ukraine
ORCID:0000-0003-0186-6220
2081364@gmail.com

Tetiana Poberezhets
Researcher of the Research Laboratory
Heroes of Kruty Military Institute of Information and Telecommunication Technologies, Kyiv, Ukraine
ORCID:0000-0001-8007-8614
tetiana.poberezhets@viti.edu.ua

Olexander Voronoi
Researcher of the Research Department
Heroes of Kruty Military Institute of Information and Telecommunication Technologies, Kyiv, Ukraine
ORCID:0009-0007-1427-4431
avoronoj423@gmail.com

ASPECTS OF CREATING SECURED INFORMATION AND COMMUNICATION SYSTEMS

Abstract. The article considers the creation of secure information and communication systems in the context of the reform of the cyber defense system in Ukraine based on international standards and practices. The normative, organizational and technical aspects of creating secure ICS in accordance with the requirements of the legislation are highlighted. Currently, there is a transition from the classical model of creating complex information protection systems and their state expertise to a risk-oriented approach based on the use of security profiles and authorization of security systems. The components of modern information infrastructure are considered and analyzed, in particular, automated systems of classes 1, 2 and 3, cloud technologies and services/services provided by centralized service infrastructures, as well as approaches to organizing protection when processing state information resources or information with limited access. Among the widespread security services (functions), the use of secure Internet access nodes, cyber incident response centers (Security Operations Center), qualified providers of electronic trust services and electronic identification means are highlighted. Special attention is paid to the organization of information protection and cyber protection of ICS deployed in cloud infrastructure (cloud services), based on the model of joint responsibility between the cloud service provider and the ICS owner. The main approaches to the organization of information protection (information security) and cyber protection are summarized depending on the class of the system, the degree of restriction of access to information and the conditions of operation of the information infrastructure.

Key words: authorized security system; automatization system; information security; information and communication system; cybersecurity; comprehensive information security system; cloud computing technology.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Palamarchuk, S., Martyniuk, V., Ovsiannikov, V., & Shuhalii, O. (2025). Transitional period of legislative changes regarding information protection and cybersecurity of information and communication systems. In Proceedings of the V International Scientific and Practical Conference “Communication Systems and Technologies, Informatization and Cybersecurity: Current Issues and Development Trends” (pp. 184–185). VITI. https://mitit.mil.gov.ua/page/science
2. Verkhovna Rada of Ukraine. (2025). Pro vnesennia zmin do deiakykh zakoniv Ukrainy shchodo zakhystu informatsii ta kiberzakhystu derzhavnykh informatsiinykh resursiv, obiektiv krytychnoi informatsiinoi infrastruktury [On amendments to certain laws of Ukraine regarding information protection and cybersecurity of state information resources and critical information infrastructure facilities] (Law of Ukraine No. 4336-IX, March 27, 2025). https://zakon.rada.gov.ua/laws/show/4336-20#Text
3. Verkhovna Rada of Ukraine. (1994). Pro zakhyst informatsii v informatsiino-telekomunikatsiinykh systemakh [On information protection in information and telecommunication systems] (Law of Ukraine No. 80/94-VR, July 5, 1994). https://zakon.rada.gov.ua/laws/show/80/94-вр#Text
4. Verkhovna Rada of Ukraine. (2017). Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy [On the basic principles of ensuring cybersecurity of Ukraine] (Law of Ukraine No. 2163-VIII, October 5, 2017). https://zakon.rada.gov.ua/laws/show/2163-19#Text
5. Verkhovna Rada of Ukraine. (2022). Pro khmarni posluhy [On cloud services] (Law of Ukraine No. 2075-IX, February 17, 2022). https://zakon.rada.gov.ua/laws/show/2075-20#Text
6. Verkhovna Rada of Ukraine. (2017). Pro elektronnu identyfikatsiiu ta elektronni dovirchi posluhy [On electronic identification and electronic trust services] (Law of Ukraine No. 2155-VIII, October 5, 2017). https://zakon.rada.gov.ua/laws/show/2155-19#Text
7. Cabinet of Ministers of Ukraine. (2025). Deiaki pytannia zakhystu informatsiinykh, elektronnykh komunikatsiinykh, informatsiino-komunikatsiinykh, tekhnolohichnykh system [Certain issues of protection of information, electronic communication, information and communication, and technological systems] (Resolution No. 712, June 18, 2025). https://zakon.rada.gov.ua/laws/show/712-2025-%D0%BF#Text
8. Cabinet of Ministers of Ukraine. (2006). Pro zatverdzhennia Minimalnykh vymoh do zakhystu informatsiinykh, elektronnykh komunikatsiinykh, informatsiino-komunikatsiinykh ta tekhnolohichnykh system [On approval of minimum requirements for the protection of information, electronic communication, information and communication, and technological systems] (Resolution No. 373, March 29, 2006). https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF#Text
9. Cabinet of Ministers of Ukraine. (2019). Pro zatverdzhennia Zahalnykh vymoh do kiberzakhystu obiektiv krytychnoi infrastruktury [On approval of general requirements for cybersecurity of critical infrastructure facilities] (Resolution No. 518, June 19, 2019). https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text
10. National Institute of Standards and Technology. (2020). Security and privacy controls for information systems and organizations (NIST Special Publication 800-53 Rev. 5). https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf
11. National Institute of Standards and Technology. (2012). Guide for conducting risk assessments (NIST Special Publication 800-30 Rev. 1). https://csrc.nist.gov/pubs/sp/800/30/r1/final
12. European Parliament & Council of the European Union. (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No. 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). Official Journal of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555&qid=1708526
13. International Organization for Standardization, International Electrotechnical Commission, & Institute of Electrical and Electronics Engineers. (2023). Systems and software engineering – System life cycle processes (ISO/IEC/IEEE 15288:2023, 2nd ed.). https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=116499
14. International Organization for Standardization, International Electrotechnical Commission, & Institute of Electrical and Electronics Engineers. (2026). Systems and software engineering – Software life cycle processes (ISO/IEC/IEEE 12207:2026, 2nd ed.). https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=77957
15. DSTU ISO/IEC 27001:2023. (2023). Informatsiina bezpeka, kiberbezpeka ta zakhyst konfidentsiinosti. Systemy keruvannia informatsiinoiu bezpekoiu. Vymohy [Information security, cybersecurity and

privacy protection. Information security management systems. Requirements] (ISO/IEC 27001:2022, IDT). https://online.budstandart.com/ua/catalog/doc

16. International Organization for Standardization & International Electrotechnical Commission. (2022). Information security, cybersecurity and privacy protection – Guidance on managing information security risks (ISO/IEC 27005:2022). https://www.iso.org/standard/80585.html
17. Administration of the State Service of Special Communications and Information Protection of Ukraine. (2025). Pro zatverdzhennia Bazovykh zakhodiv z kiberzakhystu, Metodychnykh rekomendatsii shchodo zdiisnennia bazovykh zakhodiv z kiberzakhystu [On approval of basic cybersecurity measures and methodological recommendations for implementing basic cybersecurity measures] (Order No. 54, January 30, 2025). https://surl.lt/ywfofy
18. Lutsenko, V. M. (2011). Correspondence of the stages of building information protection systems to the stages of creating automated systems. Zakhyst Informatsii, (3). https://www.docsity.com/ru/vidpovidnist-etapiv-pobudovi-sistem-zahistu-informaciji-stadiyam-stvorennya-avtomatizovanih-sistem/4654185/
19. Lukova-Chuiko, N., Nakonechnyi, V., Toliupa, S., & Ziubina, R. (2020). Problems of protection of critical infrastructure facilities. Information Systems and Technologies Security, 1(2), 31–39. https://doi.org/10.17721/10.17721/ISTS.2020.1.31-39
20. Toliupa, S., & Shtanenko, S. (2023). Mathematical model of information security management system relationships. Information Systems and Technologies Security, 1(6), 28–36. https://doi.org/10.17721/ISTS.2023.1.28-36
21. Administration of the State Service of Special Communications and Information Protection of Ukraine. (2024). Poriadok vyboru zakhodiv zakhystu informatsii, vymoha shchodo zakhystu yakoi vstanovlena zakonom ta ne stanovyt derzhavnoi taiemnytsi, dlia informatsiinykh system [Procedure for selecting information protection measures for information systems where the information protection requirement is established by law and the information does not constitute a state secret] (ND TZI 3.6-006-24; Order No. 234, April 30, 2024). https://surl.li/gliojs
22. Administration of the State Service of Special Communications and Information Protection of Ukraine. (2025). Pro zatverdzhennia bazovoho profiliu bezpeky systemy, de obrobliaietsia vidkryta abo konfidentsiina informatsiia [On approval of the basic security profile for a system processing open or confidential information] (Order No. 409, June 30, 2025). https://cip.gov.ua/ua/docs/nakaz-pro-zatverdzhennya-bazovogo-profilyu-bezpeki-sistemi-de-obroblyayetsya-vidkrita-abo-konfidenciina-informaciya
23. Administration of the State Service of Special Communications and Information Protection of Ukraine. (2025). Pro zatverdzhennia bazovoho profiliu bezpeky systemy, de obrobliaietsia sluzhbova informatsiia [On approval of the basic security profile for a system processing official information] (Order No. 419, July 2, 2025). https://cip.gov.ua/ua/docs/nakaz-administraciyi-derzhspeczv-yazku-vid-02-07-2025-419-pro-zatverdzhennya-bazovogo-profilyu-bezpeki-sistemi-de-obroblyayetsya-sluzhbova-informaciya
24. Palamarchuk, N. A., Palamarchuk, S. A., Poberezhets, T. V., & Martyniuk, V. V. (2026). Information protection and cybersecurity of information and communication systems in the defense sector: Trends of changes and issues. In Proceedings of the IV International Scientific and Practical Conference “Security and Defense Sector of Ukraine in Protection of National Interests: Current Problems and Tasks under Martial Law” (pp. 1131–1134). NADPSU Publishing House. https://dspace.nadpsu.edu.ua/handle/123456789/5873
25. Department of Special Telecommunication Systems and Information Protection of the Security Service of Ukraine. (1999). Klasyfikatsiia avtomatyzovanykh system i standartni funktsionalni profili zakhyshchenosti obrobliuvanoi informatsii vid nesanktsionovanoho dostupu [Classification of automated systems and standard functional security profiles for processed information against unauthorized access] (ND TZI 2.5-005-99; Order No. 22, April 28, 1999).
26. Cabinet of Ministers of Ukraine. (2020). Deiaki pytannia funktsionuvannia Natsionalnoi elektronnoi komunikatsiinoi merezhi [Certain issues concerning the functioning of the National Electronic Communication Network] (Resolution No. 1358, December 16, 2020). https://zakon.rada.gov.ua/laws/show/1358-2020-%D0%BF#Text
27. Administration of the State Service of Special Communications and Information Protection of Ukraine. (2023). Pro zatverdzhennia Polozhennia pro systemu zakhyshchenoho dostupu derzhavnykh orhaniv do merezhi Internet [On approval of the regulation on the system of secure Internet access for state authorities] (Order No. 771, August 30, 2023). https://zakon.rada.gov.ua/laws/show/z1624-23#Text
28. Cabinet of Ministers of Ukraine. (2023). Pro zatverdzhennia Polozhennia pro intehrovanu systemu elektronnoi identyfikatsii [On approval of the regulation on the integrated electronic identification

system] (Resolution No. 1150, November 3, 2023). https://zakon.rada.gov.ua/laws/show/1150-2023-%D0%BF#Text

29. Radchenko, M. M., Dykyi, O. V., Palamarchuk, N. A., Palamarchuk, S. A., & Bondarenko, O. Ye. (2021). Approaches to information protection in information and telecommunication systems built using cloud technologies. Visnyk VITI. Communication and Information Systems, (2), 82–95. https://www.viti.edu.ua/files/zbk/2021/2021-2.pdf
30. Zhylin, A., Divitskyi, A., & Kozachok, A. (2019). Problems of information resources protection when using cloud technologies. Information Technology and Security, 7(2), 171–182. https://ela.kpi.ua/handle/123456789/33886

Отримано редакцією журналу / Received: 27.02.26
Прорецензовано / Revised: 07.03.26
Схвалено до друку / Accepted: 24.09.26