

## КІБЕРБЕЗПЕКА ДЕРЖАВНИХ ЦИФРОВИХ СИСТЕМ: ПЕНТЕСТИНГ ХМАРНИХ СЕРЕДОВИЩ

**Андрій Жорняк,**

Центральне міжрегіональне управління Державної служби з питань праці

**Анотація.** У статті розглянуто та проаналізовано напрями досліджень у галузі кібербезпеки державних цифрових систем. Підкреслено, що в сучасних умовах цифровізації та активного впровадження цифрового урядування кібербезпека державних цифрових систем набуває особливого значення. Це зумовлено необхідністю підвищення стійкості організаційного середовища до кіберзагроз та зміцнення інформаційного суверенітету держави. Визначено актуальні аспекти щодо перспектив удосконалення законодавства, а також сформовано комплексну систему рекомендацій, яка включає як управлінські рішення, так і технічні заходи кібербезпеки.

Зазначено, що використання хмарних технологій має потенціал для покращення та підвищення ефективності функціонування державних установ. Водночас наголошено на можливих кіберзагрозах та ризиках, пов'язаних із застосуванням хмарних технологій. Розглянуто методологію пентестингу в хмарних середовищах державних цифрових інформаційних ресурсів.

У статті представлено пропозиції та надано рекомендації для вдосконалення кіберзахисту в державних цифрових інформаційних системах.

**Ключові слова:** аудит інформаційної безпеки, безпека державних інформаційних систем, захист інформації, кібербезпека, пентестинг, тестування на проникнення, цифрові інструменти, хмарні середовища.

### ВСТУП

Цифрова трансформація публічного управління в Україні включає впровадження цифрового урядування та активно інтегрує інформаційно-комунікаційні технології, що створює потенціал для підвищення ефективності у сфері державного управління та сприяє соціально-економічному розвитку. Водночас зростає вразливість цифрових державних інформаційних ресурсів до кіберзагроз, що зумовлює необхідність формування цілісної системи кібербезпеки. Забезпечення безпеки та кіберстійкості є важливим чинником, який формує довіру громадян до державних інституцій і визначає здатність держави гарантувати безперервне надання публічних послуг. Належна організація системи захисту електронних інформаційних ресурсів має бути інтегрована в стратегічні напрями державної політики. Заходи реагування, а також превентивні заходи мають

формуватися з урахуванням міжвідомчої взаємодії державних установ, яка має відбуватися із залученням інститутів громадянського суспільства.

Нормативно-правове регулювання у сфері кібербезпеки в Україні ґрунтується на Конституції України, профільних законах та стратегічних документах. Закон «Про основні засади забезпечення кібербезпеки України» визначає повноваження суб'єктів, задіяних у цій сфері. Упровадження задекларованих у законодавстві України норм сприяє посиленню національної спроможності протистояти інформаційним загрозам. У контексті зростання кіберзлочинності особливої уваги потребує кіберзахист критичної інфраструктури, урядових платформ, інформаційно-аналітичних систем та інноваційних технологій, включаючи хмарні сервіси й блокчейн-рішення. Уразливість цих систем зумовлює необхідність постійного оновлення

політик безпеки, законодавства та процедур оцінки ризиків. Формування національної моделі кіберзахисту потребує гармонізації з міжнародними стандартами, а також активної участі України в глобальних ініціативах у сфері кібербезпеки. Принципи відкритості, верховенства права, інституційної відповідальності, безперервності державних заходів та дотримання прав людини мають стати основою політики в галузі кібербезпеки.

**Мета дослідження** — дослідити, сформувати та оптимізувати підходи до забезпечення захисту державних цифрових інформаційних ресурсів, проаналізувати можливі кіберзагрози та вразливості, створити практичні рекомендації щодо їх виявлення та усунення.

#### **Завдання для реалізації мети:**

- провести теоретичний аналіз законодавства України та сучасних підходів до забезпечення кібербезпеки державних цифрових систем у хмарних середовищах;
- дослідити методології та інструменти пентестингу, що застосовуються для оцінки безпеки хмарних сховищ даних та віртуальних серверів;
- визначити типові кіберзагрози та вразливості, характерні для державних цифрових систем, розгорнутих у хмарних середовищах;
- розробити комплекс практичних рекомендацій щодо підвищення рівня кіберзахисту державних цифрових інформаційних ресурсів у хмарних середовищах.

#### **МЕТОДОЛОГІЯ ДОСЛІДЖЕННЯ**

Для дослідження законодавства України та принципів кібербезпеки державних цифрових систем, включаючи пентестинг хмарних середовищ, були застосовані такі методи: діалектичний (досліджено взаємозв'язок між розвитком цифрових технологій та рівнем кіберзагроз); формально-правовий (проаналізовано законодавчу базу та сучасні наукові підходи у сфері кібербезпеки та захисту інформації); порівняльний (порівняно підходи до організації пентестингу та

моніторингу безпеки); системний (досліджено структурні особливості функціонування цифрових захисних інструментів та особливості їх упровадження); аналітичний (оцінено ефективність наявних методів пентестингу в забезпеченні кіберзахисту); узагальнення (досліджено досвід застосування цифрових технологій у сфері інформаційної безпеки); праксеологічний (обґрунтовано практичну значущість результатів дослідження для покращення кіберзахисту, процесів аудиту безпеки та управління кіберризиками).

#### **АНАЛІЗ ПУБЛІКАЦІЙ**

Забезпечення безпеки державних електронних інформаційних ресурсів уже тривалий час перебуває в центрі уваги багатьох науковців, про що свідчить аналіз численних наукових публікацій та досліджень. Значний внесок у вивчення цієї сфери зробили П.Є. Антонюк (Антонюк, б.д.), Т.А. Вакалюк (Вакалюк et al., 2021), В.О. Крайнов, Ю.М. Костів (Крайнов et al., 2020), Ю.Г. Даник, В.В. Охрімчук, Ю. Діогенес, О. Ердаль (Diogenes et al., б.д.), Ю. Попов, К. Погоріла (Олефіренко et al., 2022) та інші.

Дослідники приділяли увагу ефективності функціонування державних органів у контексті захисту інформаційного простору України. Водночас науковцями проведено аналіз ключових нормативно-правових актів України, що становлять основу правового регулювання у сферах національної безпеки та кібербезпеки. До них належать, зокрема, Закони України: «Про інформацію» (від 02.10.1992 № 2657-XII, Верховна Рада України, 1992), «Про захист інформації в інформаційно-телекомунікаційних системах» (від 05.07.1994 № 80/94-ВР (Верховна Рада України, 1994), «Про ратифікацію Конвенції про кіберзлочинність» (від 07.09.2005 № 2824-IV (Верховна Рада України, 2005), «Про Державну службу спеціального зв'язку та захисту інформації» (від 23.02.2006 № 3475-IV, Верховна Рада України, 2006), «Про захист персональних даних» (Верховна Рада України, б.д.), «Про доступ до публічної інформації» (від 13.01.2011 № 2939-VI,

Верховна Рада України, 2011), «Про основні засади забезпечення кібербезпеки України» (від 05.10.2017 № 2163-VIII, Верховна Рада України, 2017) та «Про національну безпеку України» (від 21.06.2018 № 2469-VIII, Верховна Рада України, 2018). Крім того, науковці приділяють значну увагу дослідженню стратегічних документів, які формують напрям державної політики у сфері безпеки, а саме: «Стратегія національної безпеки України» (Указ Президента України № 287/2015, Президент України, 2015), «Стратегія кібербезпеки України» (Указ Президента України № 96/2016 (Президент України, 2016) та «Доктрина інформаційної безпеки» (Указ Президента України № 47/2017, Президент України, 2017). Не менш важливим є аналіз указів Президента України, що стосуються вдосконалення державної політики в інформаційній сфері (від 01.05.2014 № 449, Президент України, 2014), а також функціонування Національного координаційного центру кібербезпеки (від 07.06.2016 № 242/2016, Президент України, 2016). Водночас науковцями досліджуються відповідні нормативно-правові акти Кабінету Міністрів України, зокрема Постанова № 518 від 19.06.2019, якою затверджено Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури (Кабінет Міністрів України, 2019).

Незважаючи на зазначені дослідження та наявну нормативно-правову базу, комплексна проблема захисту державних електронних інформаційних ресурсів у контексті стрімких цифрових трансформацій та цифровізації в Україні залишається розкритою в наукових працях лише частково. Недостатньо висвітлено методологічні підходи до розробки класифікатора загроз для таких ресурсів, дослідження не завжди повною мірою розкривають специфіку правового статусу суб'єктів, які безпосередньо відповідають за забезпечення захисту державних електронних інформаційних ресурсів.

## РЕЗУЛЬТАТИ Й ОБГОВОРЕННЯ ДОСЛІДЖЕННЯ

**Дослідження стану забезпечення кібербезпеки державних цифрових інфор-**

**маційних ресурсів.** Застосування хмарних сервісів відкриває нові можливості для цифровізації адміністративних процесів. Їх використання державними установами для зберігання, обробки й передавання інформації дозволяє підвищити ефективність управлінських процесів, скоротити витрати та забезпечити гнучкий доступ до даних. Ці технології забезпечують гнучкість, масштабованість, доступність та раціональне використання обчислювальних ресурсів, мобільність, що створює умови для адаптивного управління інформаційними потоками (Glazunova et al., 2020), але супроводжуються викликами, пов'язаними із залежністю від зовнішніх постачальників. Одночасно виникає необхідність дотримання протоколів кібербезпеки та комплексного аналізу ризиків, пов'язаних з конфіденційністю, цілісністю й доступністю даних. Залежно від функціонального призначення, у публічному управлінні застосовуються моделі SaaS, PaaS і IaaS. SaaS спрощує доступ до програмних засобів, зменшуючи адміністративні витрати. PaaS забезпечує розробникам повноцінне середовище для створення та тестування застосунків. IaaS надає повний контроль над віртуалізованими ресурсами, що особливо важливо під час кризових або пікових навантажень (International Organization for Standardization, 2020). Не менш важливою є характеристика хмарних сховищ даних (типологія даних, рівні доступності, механізми резервного копіювання та захисту інформації), що визначають ефективність роботи цифрових архівів та інформаційних систем. (Верховна Рада України, б.д.). Системне дослідження цих аспектів сприяє вибору безпечних і адаптивних рішень, здатних забезпечити стабільне, безпечне функціонування державних цифрових сервісів. Водночас технічні аспекти функціонування хмарних платформ (архітектура, протоколи обміну даними, криптозахист, підтвердження ідентичності користувачів, служб і програм для доступу до цифрових ресурсів) є визначальними критеріями для їх надійності та ефективності. Інституційна готовність установ до впровадження хмарних рішень

також має ключове значення. Необхідно забезпечити підготовку персоналу, створення внутрішніх регламентів і адаптацію організаційної структури до нових умов функціонування. Особливе значення має поетапна оцінка доцільності впровадження таких технологій у публічному управлінні. Ключовими етапами впровадження цих технологій є: аналіз потреб установи, вибір типу сервісу, розробка політик безпеки, оцінка ефективності й продуктивності (Кабінет Міністрів України, 2006). Ці етапи забезпечують узгодженість стратегічних, технічних та організаційних аспектів. Основними критеріями вибору мають бути: інтеграційна сумісність, підтримка адаптивності, економічна ефективність та рівень безпеки (Верховна Рада України, 2017). Необхідним компонентом є також оцінка вартості впровадження, яка включає витрати на міграцію, оренду обчислювальних ресурсів, зберігання, технічну підтримку, аналіз ефективності до та після впровадження (Diogenes et al., б.д.) (Федченко, 2018). Оцінювання економічної доцільності доповнюється аналізом потенційних переваг (зниження витрат на ІТ-інфраструктуру, підвищення масштабованості та гнучкості, зміцнення кіберзахисту), що дозволяє забезпечити баланс між вкладеними інвестиціями й отриманими перевагами, орієнтуючи управлінські рішення на довгострокову ефективність (Diogenes et al., б.д.) (Федченко, 2018).

Ефективне застосування моделей хмарних обчислень дозволяє модернізувати державні сервіси, підвищити прозорість управлінських процесів і зміцнити довіру громадян до інституцій публічної влади. На ефективність збереження, обробки й захисту інформації прямо впливають характеристики хмарних сервісів (масштабованість, доступність, безпека) (Олефіренко et al., 2022). Їх використання вимагає комплексного підходу, що включає розроблення стратегії передачі інформації, оцінку поточних ІТ-ресурсів, юридичних обмежень та технічних можливостей. Один із перших кроків — це перенесення цифрових ресурсів (даних, програмного забезпечення) у хмарну інфраструктуру, що

потребує оцінки сумісності та безпекових ризиків. Вибір моделі хмарного сервісу (SaaS, PaaS, IaaS) має базуватися на таких критеріях: загальна вартість, функціональність, гнучкість, підтримка масштабування та гарантії кібербезпеки (Олефіренко et al., 2022). Особлива увага приділяється захисту персональних та конфіденційних даних, що вимагає використання механізмів шифрування, багатофакторної автентифікації, безперервного моніторингу та виявлення загроз.

Однак ці переваги супроводжуються низкою викликів у сфері кіберзахисту. Зокрема, централізоване зберігання великих обсягів даних на віддалених серверах підвищує ризики несанкціонованого доступу, витоку або модифікації конфіденційної інформації. Загрози походять як іззовні (кіберзлочинність), так і зсередини (ненавмисні або свідомі дії працівників провайдерів). Додаткові ризики створюють технічні збої та обмеження доступності сервісів (Proceedings of the 8th Workshop on Cloud Technologies in Education (CTE 2020), 2020). Для належного реагування на ці загрози потрібен системний підхід до інформаційної безпеки із застосуванням сучасних криптографічних алгоритмів, багаторівневого моніторингу, систем виявлення загроз, політик контролю доступу, а також актуалізації процедур автентифікації (Glazunova et al., 2020). Застосування багатофакторної автентифікації (поєднання пароля з одноразовим кодом або біометрією) значно підвищує стійкість систем до зовнішнього втручання. Авторизація користувачів після проходження автентифікації повинна реалізовуватися з урахуванням принципу мінімальних повноважень та посадових обов'язків. Розмежування доступу в хмарних середовищах забезпечується інтеграцією засобів управління ідентифікацією, генерацією одноразових ключів та актуальними політиками інформаційної безпеки (Proceedings of the 8th Workshop on Cloud Technologies in Education (CTE 2020), 2020). Динамічне оновлення відповідних механізмів є критично важливим для забезпечення безперервного захисту в умовах постійної зміни кіберзагроз.

Ще одним важливим елементом кібербезпеки в хмарних середовищах є шифрування даних. Використання цього інструменту забезпечує цілісність і конфіденційність як у площині зберігання даних на серверах провайдера, так і під час їх передавання через мережу. Надійність шифрування обумовлюється вибором сучасних криптографічних алгоритмів та ефективним управлінням ключами, що унеможлиблює доступ до інформації без відповідної автентифікації (Маслова et al., 2020). Так, фундаментальну роль у забезпеченні стійкості до кіберзагроз відіграють моніторинг та аудит безпеки. Системи моніторингу дозволяють своєчасно виявляти аномальну активність, що може свідчити про спроби несанкціонованого втручання. Аудит спрямований на верифікацію дотримання політик безпеки, виявлення вразливостей та вдосконалення захисних механізмів. Доцільним є впровадження SIEM-рішень (програмний продукт для виявлення, моніторингу, аналізу кіберзагроз), які автоматизують виявлення та аналіз інцидентів. Одним із викликів кібербезпеки для хмарних середовищ є також протидія DDoS-атакам. Надмірне навантаження на сервіси може призводити до втрати доступності до інформаційних ресурсів. Ефективна стратегія включає розгортання систем раннього виявлення атак, балансування навантаження за допомогою CDN (мережа серверів, які розміщені по всьому світу й служать для кешування та швидкої доставки контенту сайтів) і використання розподілених ресурсів для мінімізації наслідків порушення сервісної доступності (Київський центр безпеки, б.д.). Усередині організацій потенційною загрозою залишаються дії внутрішніх осіб. Для нейтралізації таких дій запроваджуються принципи мінімального доступу, сегментація прав, аудит дій персоналу та двофакторна автентифікація. Водночас важливим елементом є формування культури кібергігієни через реалізацію заходів, передбачених навчальними програмами для працівників. Безперервність функціонування інформаційних систем державного сектору забезпечується механізмами резервного

копіювання та відновлення даних. Своєчасне створення копій, зберігання їх на віддалених серверах, а також тестування відновлювальних процедур дозволяють мінімізувати ризики втрати інформації внаслідок технічних або кіберінцидентів. Забезпечення актуальності програмного забезпечення та впровадження індикаторів безпеки є завершальним елементом у системі захисту хмарних середовищ. Оперативне оновлення компонентів IT-інфраструктури дозволяє ліквідувати вразливості, запобігаючи можливому їх використанню зловмисниками. Упровадження автоматизації оновлень підвищує ефективність реагування на нові загрози.

Одним із ключових напрямів забезпечення безпеки у віртуалізованих середовищах є мережна сегментація. Віртуальні сервери дозволяють формувати ізольовані мережеві простори з окремими політиками доступу, що забезпечує незалежність сегментів, навіть у межах одного фізичного сервера. Така архітектура уможлиблює обмеження поширення загроз та підвищення рівня контролю за доступом до критичних ресурсів. У сфері публічного управління це забезпечує персоналізований доступ до інформаційних систем відповідно до ролей, функціональних завдань або структурної належності користувачів, що мінімізує ймовірність витоку конфіденційних відомостей (Антонюк, б.д.). Інтеграція технологій віртуалізації в інформаційну інфраструктуру органів державної влади сприяє впровадженню сучасних стандартів безпеки через ізоляцію середовищ і гнучке управління доступом. Це створює підґрунтя для побудови адаптивної та захищеної цифрової системи управління, що відповідає вимогам сучасного етапу цифровізації. Значною перевагою віртуалізації є оптимізація процесів резервного копіювання та відновлення даних. Архітектура віртуальних машин дозволяє здійснювати копіювання лише критично важливих компонентів, що знижує навантаження на ресурси, обсяг трафіку та витрати на зберігання (Glazunova et al., 2020). Додатково функція створення знімків (snapshot) забезпечує збереження контрольних точок

перед оновленнями чи конфігураційними змінами, що дає змогу швидко відновити працездатність системи в разі збоїв. Це підвищує готовність інформаційних систем до надзвичайних ситуацій і сприяє збереженню функціональної безперервності.

Впровадження цифрових технологій у державному секторі вимагає системного підходу до кібербезпеки, орієнтованого на забезпечення конфіденційності, цілісності та доступності інформаційних ресурсів, включаючи дані з обмеженим доступом. Ключовими елементами такої моделі є шифрування даних у процесі зберігання й передавання, багаторівневий контроль доступу, постійний моніторинг систем на предмет виявлення аномальної активності, а також упровадження ефективних механізмів резервного копіювання й відновлення. Захист інформації має ґрунтуватися не лише на технічних засобах, зокрема сучасних криптографічних алгоритмах, системах моніторингу та протидії DDoS-атакам, але й на організаційних заходах — таких як навчання персоналу, формування політик доступу та регулярний аудит. Визначальним є поєднання технічних і адміністративних механізмів у межах цілісної системи управління безпекою цифрових ресурсів. На організаційному рівні забезпечення кібербезпеки в хмарних середовищах передбачає формалізацію політик доступу, упровадження процедур реагування та відновлення після кібератак. Окреме значення має розвиток кіберкультури серед працівників через регулярну підготовку та підвищення обізнаності щодо кіберзагроз і безпечної поведінки в цифровому середовищі. У сучасних умовах ефективний захист хмарної інфраструктури вимагає постійного вдосконалення внутрішніх регламентів безпеки, а також автоматизації ключових процесів. Узгоджене застосування цих заходів забезпечує надійність та стійкість до новітніх кіберзагроз (Тарасов et al., 2021).

**Методологія пентестингу в хмарних середовищах державних цифрових інформаційних ресурсів.** Історичні засади тестування на проникнення (пентестингу) сфор-

мувалися в США у 1970–1980-х роках, коли термін «хакер» позначав висококваліфікованого програміста, що вдосконалює програмний код та перевіряє електронно-обчислювальні машини на наявність помилок. Така діяльність не мала негативного забарвлення й асоціювалася з академічними центрами — Массачусетським технологічним інститутом і Стенфордським університетом, випускники яких здійснили вагомий внесок у розвиток обчислювальних технологій. Значущу роль у цьому контексті відіграла й ІТ-спільнота Homebrew Computer Club (Yevseiev et al., 2021). Однак із часом значення поняття «хакер» змінилося. Зокрема, після інциденту з поширенням «черв'яка Морріса» у 1988 році, створеного аспірантом Робертом Моррісом (Cornell University), діяльність хакерів почала асоціюватися з кіберзагрозами. Вірус спричинив параліч мережі ARPANET і, за різними оцінками, завдав збитків на понад 96 млн доларів США (Yevseiev et al., 2021).

Пентестинг є ефективним інструментом оцінки рівня кіберзахисту цифрових інформаційних систем. Його метою є виявлення потенційних вразливостей та підготовка рекомендацій щодо їх усунення. Застосовуються різні методи тестування — від імітації зовнішніх атак до аналізу людського чинника через методи соціальної інженерії. Одним із ключових підходів виступає тестування типу «чорний ящик» (Black Box Testing): пентестери не мають попередньої інформації про систему й оперують лише доступними зовнішніми інтерфейсами. Такий метод дозволяє змоделювати дії зовнішнього зловмисника, але має обмеження у виявленні внутрішніх вразливостей. Іншим є підхід «білий ящик» (White Box Testing), що передбачає надання повного доступу до внутрішньої інформації, вихідного коду, схем мережі тощо. Це забезпечує глибокий аналіз безпеки, проте його використання часто обмежується правовими або організаційними чинниками. Компромисом між двома зазначеними стратегіями є «сірий ящик» (Grey Box Testing), який передбачає часткове розкриття інформації. Цей метод поєднує переваги обох підходів, збері-

гаючи баланс між реалістичністю атак і точністю аналізу, що робить його ефективним для державного сектору, де необхідно враховувати як прозорість, так і захист критичних ресурсів.

У забезпеченні кібербезпеки державних цифрових ресурсів важливу роль відіграють два ключові підходи до проведення тестування на проникнення — внутрішнє та зовнішнє. Обидва методи імітують різні сценарії потенційних атак, дозволяючи здійснити комплексну оцінку рівня вразливості систем публічного сектору. Внутрішнє тестування моделює дії зловмисника, який уже має певний рівень доступу до внутрішнього середовища інформаційної системи. Такий підхід відображає ризики, пов'язані з інсайдерськими загрозами, включаючи фізичний доступ або соціальну інженерію (зокрема фішинг). У процесі аналізуються механізми контролю доступу, мережеві конфігурації та слабкі місця, які можуть бути використані для небажаної ескалації привілеїв або витоку даних (Hewlett Packard Enterprise, 2016). Зовнішнє тестування орієнтоване на симуляцію дій стороннього атакувальника, що здійснює спроби проникнення без попереднього доступу. У фокусі дослідження — мережеві межі, відкриті порти, налаштування міжмережевих екранів, а також вразливості вебдодатків. Метою є виявлення точок входу до інформаційної інфраструктури через відкриті або недостатньо захищені сервіси (Hewlett Packard Enterprise, 2016). Вибір між цими підходами залежить від пріоритетів організації, актуальних для її інформаційного середовища.

Тестування на проникнення (пентестинг) зазвичай реалізується в кілька етапів, що формують методологічну основу аналізу, а саме:

- розвідка (Reconnaissance) — збір відкритої інформації про цільову систему, включно з мережевою структурою, доменними іменами, вебсайтами, персоналом тощо;
- сканування (Scanning) — застосування автоматизованих засобів для виявлення відкритих портів, сервісів, версій про-

грамного забезпечення та потенційних вразливостей;

- експлуатація (Exploitation) — використання знайдених вразливих компонентів для підтвердження можливості отримання несанкціонованого доступу або порушення конфіденційності, цілісності чи доступності системи;
- звітність (Reporting) — документування отриманих результатів, класифікація загроз і формулювання конкретних заходів для усунення вразливостей. Звіт стає підґрунтям для подальших управлінських рішень щодо покращення систем захисту (Президент України, 2021).

У межах забезпечення кіберзахисту державних інформаційних систем також доцільно розрізняти два підходи до ідентифікації вразливостей: ручний та автоматизований. Ручний аналіз передбачає участь фахівців, які задіюють професійний досвід і контекстуальне мислення для виявлення специфічних, логічно складних недоліків, що можуть не фіксуватись технічними засобами (Тарасов et al., 2021). Автоматизовані засоби, у свою чергу, забезпечують швидке виявлення типових вразливостей, зокрема уразливих конфігурацій і програмних компонентів. Однак такі інструменти часто не фіксують складні логічні помилки, що вимагає подальшого «ручного» аналізу (Тарасов et al., 2021). Найефективнішим підходом визнається комбінування обох методів: автоматизоване сканування застосовується на початкових етапах, а ручна перевірка — для глибокої експертизи.

Структурований і системний підхід до планування та реалізації тестування на проникнення є важливою складовою підвищення захисту державних цифрових ресурсів, бо він сприяє зміцненню довіри суспільства до електронних сервісів. Контрольований процес активного виявлення вразливостей в інформаційних системах (пентестинг) зумовлений потребою у забезпечення даних у сучасному кіберпросторі (Національний банк України, 2017). Розробка пентест-плану передбачає визначення цілей перевірки, вибір відповідної методології, окреслення обсягів

дослідження, а також ресурсне й організаційне планування. Під час реалізації тестування спеціалісти застосовують технічні засоби, що імітують загрози, моделюючи можливі сценарії атак. Після завершення тестування проводиться аналіз зібраних даних, на основі яких формуються рекомендації з посилення кіберзахисту. Результати такого тестування використовуються, зокрема, для підвищення безпеки хмарних платформ і раннього виявлення кіберзагроз.

Пентестинг є циклічним процесом, що потребує періодичного оновлення відповідно до динаміки розвитку технологій. Ефективне проведення пентесту вимагає розробки комплексного плану, що структурує процес за такими основними етапами:

- визначення цілей (постановка завдань, пов'язаних із виявленням технічних недоліків, перевіркою стійкості до атак або аудитом відповідності політикам безпеки) (Кабінет Міністрів України, 2006);
- обрання методології (застосування відповідного підходу (black-box, white-box або grey-box), який визначає рівень обізнаності тестувальників щодо внутрішньої архітектури системи та обсягу доступу до неї);
- окреслення меж тестування (ідентифікація об'єктів перевірки — мереж, програмних продуктів, пристроїв тощо);
- планування ресурсів (розрахунок необхідного кадрового потенціалу, технічних засобів і фінансування для реалізації робіт (Кабінет Міністрів України, 2006));
- одержання згоди (юридичне погодження процедур тестування з власниками систем і повідомлення відповідальних осіб, щоб уникнути правових та комунікаційних ризиків (Верховна Рада України, 2017));
- реалізація тестування (практичне виконання перевірки з використанням обраного підходу, моделювання загроз і спроб експлуатації виявлених вразливостей (Київський центр безпеки, б.д.));
- оцінка результатів (систематизація виявлених проблем, формулювання висновків щодо ймовірних ризиків і вразливих сегментів);
- підготовка звіту (створення документа з детальним описом загроз, рівнів критичності та рекомендацій щодо посилення безпеки);
- впровадження змін (ініціація коригувальних заходів, спрямованих на усунення недоліків і підвищення стійкості системи (DOU, б.д.));
- оцінювання ефективності (аналіз впроваджених змін та контроль за усуненням виявлених вразливостей (Олефіренко et al., 2022)).

У практиці інформаційної безпеки виділяють кілька типів пентесту, орієнтованих на різні середовища та об'єкти дослідження. Серед найбільш поширених — тестування вебресурсів, що охоплює сайти, онлайн-сервіси, бази даних та інші компоненти, які взаємодіють із мережею (Microsoft, б.д.). З огляду на розширення використання хмарних технологій дедалі більшої актуальності набуває тестування хмарної інфраструктури — віртуалізованих середовищ зберігання та обробки інформації. Окремо виділяється тестування мобільних платформ, орієнтоване на перевірку безпеки додатків, ОС та апаратного середовища (Антонюк, б.д.). Особливе значення у сфері державного управління має тестування комп'ютерних мереж, що дозволяє оцінити ризики зовнішнього та внутрішнього втручання (Network Penetration Testing). Також проводиться тестування програмного забезпечення з метою виявлення вразливостей у коді, які можуть вплинути на конфіденційність, цілісність і доступність даних. Доповненням є пентестинг апаратних компонентів, зосереджений на виявленні проблем безпеки, пов'язаних із прошивками, мікроконтролерами чи портами доступу (International Organization for Standardization, 2020). Розширення екосистеми інтернету речей актуалізує потребу в цільовому пентестуванні IoT-пристроїв, орієнтованому на виявлення вразливостей у розумних приладах, автоматизованих системах управління та сенсорних мережах, які функціонують у складному інформаційно-комунікаційному середовищі.

Промислові системи управління (ICS), які входять до складу критичної цифрової інфраструктури, потребують окремого типу аналізу — ICS/SCADA Penetration Testing. Такий підхід дозволяє ідентифікувати потенційні загрози технологічним процесам у галузях енергетики, транспорту та житлово-комунального господарства (Glazunova et al., 2020). Серед новітніх напрямів тестування можна виділити безпековий аудит блокчейн-інфраструктур, що охоплює перевірку смарт-контрактів, децентралізованих застосунків і криптографічних протоколів, які застосовуються для забезпечення функціонування публічних реєстрів і цифрових сервісів е-урядування. Окремо слід відзначити тестування методів соціальної інженерії (Social Engineering Testing), спрямоване на виявлення вразливостей у поведінкових реакціях персоналу. Серед поширених форм можна виділити фішинг, вішинг, смішинг та інші методи впливу з використанням соціотехнічних прийомів.

Зростання цифрових (інформаційних) ризиків у сфері державного управління зумовлює необхідність комплексного та типологічного підходу до організації тестування інформаційних систем. Це передбачає створення спеціалізованих команд (фахівців) із чітко розмежованим функціоналом. Зокрема, «Red Team» (наступальні підрозділи) моделюють сценарії порушення безпеки, включно із соціоінженерними методами, атаками на апаратні компоненти (Hardware Penetration Testing) та нестандартними кіберінцидентами; прикладом може бути випадок розгортання шкідливого коду Stuxnet, що був націлений на інфраструктуру промислових систем керування (Антонюк, б.д.). Ці команди імітують тактики реальних загроз і за певних умов можуть трансформуватись у АРТ-групи (Advanced Persistent Threats), що характеризуються високою організаційною структурою та тривалими цілеспрямованими атаками, іноді з державною підтримкою (International Organization for Standardization, 2020). Функціональним антиподом є «Blue Team» — підрозділи оборонного характеру, які забезпе-

чують превентивну, аналітичну та моніторингову діяльність у сфері інформаційної безпеки. Їхні завдання — виявлення інцидентів, налаштування систем захисту та тестування стійкості цифрових платформ органів влади (Glazunova et al., 2020). Інтегрований підхід, відомий як «Purple Team», об'єднує функції «Red» і «Blue» команд, забезпечуючи взаємодію між симуляцією загроз та їх нейтралізацією. У державному управлінні такий формат сприяє підвищенню адаптивності систем кіберзахисту, що є критичним для збереження стійкості цифрових сервісів. Результативність тестування інформаційної безпеки залежить від обґрунтованого вибору методології, яка має відповідати типу інформаційної системи, управлінським завданням і рівню допустимого ризику (Антонюк, б.д.).

Серед визнаних міжнародних методологій тестування інформаційних систем, що можуть бути адаптовані до потреб публічного управління, виділяються:

- OWASP TOP 10, ASVS, MASVS, Firmware Security Testing — відкриті методичні стандарти, які регламентують безпечну розробку та тестування веб- і мобільних застосунків, а також мікропрограм (International Organization for Standardization, 2020);
- OSSTMM — формалізована методика оцінки безпеки ІТ-систем від ISECOM з урахуванням концептуального аналізу загроз (Glazunova et al., 2020);
- PTES — стандартизована послідовність проведення пентесту, що охоплює як технічні, так і організаційні аспекти (Proceedings of the 8th Workshop on Cloud Technologies in Education (CTE 2020), 2020);
- NIST SP 800–115 — офіційний гайд Національного інституту стандартів США, орієнтований на державні установи (Валюк et al., 2021);
- MITRE ATT&CK — база знань про реальні сценарії атак, яка широко застосовується в системах захисту критичної інфраструктури (Маслова et al., 2020);
- SANS CWE Top 25 — каталог критичних вразливостей, що визначає пріоритет-

ність під час тестування (Крайнов et al., 2020);

- ISSAF — глибоко структурована методологія, адаптована для аудиту інформаційних систем у публічному секторі (Diogenes et al., б.д.);
- PCI-DSS Penetration Test Guidance — специфікація для перевірки систем, що обробляють платіжні дані, включно з публічними сервісами фінансового характеру (Федченко, 2018);
- WASC Threat Classification — система класифікації загроз для вебзастосунків, спрямована на уніфікацію аналізу безпеки (Network Cultures, б.д.);
- PTF — прикладна методологія, орієнтована на практичне застосування спеціалізованих інструментів у пентестах.

Ефективність упровадження вищезазначених методик значною мірою залежить від здатності органів влади адаптувати їх до специфіки нормативно-правового середовища, а також до вимог прозорості та підзвітності цифрових сервісів у публічному управлінні.

Комплексний аналіз ризиків віртуальних середовищ дозволяє виявити критичні напрями загроз, що потенційно впливають як на функціонування органів влади, так і на цілісність, конфіденційність і доступність інформації (International Organization for Standardization, 2020); (Glazunova et al., 2020). До найпоширеніших викликів у хмарних середовищах слід віднести такі: витоки інформації, вразливості мережевого рівня, DDoS-атаки, недосконалість механізмів ідентифікації та доступу, неефективність резервного копіювання, фрагментарність політик з управління інформацією та недостатній рівень реагування на інциденти (Proceedings of the 8th Workshop on Cloud Technologies in Education (CTE 2020), 2020); (Diogenes et al., б.д.).

Інформаційна безпека хмарних середовищ повинна ґрунтуватися на механізмах, основними елементами яких є: шифрування даних, багаторівнева аутентифікація, обмеження доступу за принципом мінімальних прав, систематичний аудит та навчання персоналу збереженню конфіденційної інформа-

ції, що зберігається в хмарних середовищах (Вакалюк et al., 2021). Причини кіберінцидентів часто пов'язані з вразливістю програмного забезпечення, людським фактором або неналежним адмініструванням облікових записів (Glazunova et al., 2020); (Proceedings of the 8th Workshop on Cloud Technologies in Education (CTE 2020), 2020). Успішні кібератаки можуть призводити до крадіжки персональної або службової інформації, маніпуляцій чи репутаційних втрат. Не менш значущим є ризик мережевих атак, включно з атаками типу Man-in-the-Middle або перехопленням трафіку. Для протидії таким загрозам застосовуються протоколи SSL/TLS, сегментація мереж, IDS/IPS-системи, а також упровадження стандартів ISO/IEC 27001 та NIST (Маслова et al., 2020); (Крайнов et al., 2020).

DDoS-атаки залишаються однією з найнебезпечніших форм загроз, що можуть тимчасово виводити з ладу критичні сервіси (Glazunova et al., 2020). Серед превентивних заходів є фільтрація трафіку, використання CDN, мережева сегментація та інтеграція систем IDS/IPS (Proceedings of the 8th Workshop on Cloud Technologies in Education (CTE 2020), 2020); (Вакалюк et al., 2021). Одночасно суттєвий ризик становлять вразливості хмарних додатків (SQL-ін'єкції, переповнення буфера, помилки автентифікації). Для їх нейтралізації застосовуються аудит коду, оновлення компонентів, стандарти безпечного програмування та контроль сесій (Маслова et al., 2020); (Крайнов et al., 2020). Ризик втрати даних, пов'язаний із збоєм обладнання, людським фактором чи кібератаками, потребує реалізації стратегії резервного копіювання, реплікації інформації, криптографічного захисту та моделювання сценаріїв відновлення (Федченко, 2018). Додатково варто акцентувати увагу на нормативній відповідності. Хмарні сервіси, що використовуються в публічному секторі, мають дотримуватись вимог міжнародних регламентів щодо зберігання, обробки й знищення персональної та службової інформації (Верховна Рада України, 2017). Забезпечення правових гарантій інформаційної безпеки є умовою

довіри громадян до цифрових державних сервісів.

### **Удосконалення механізмів кібербезпеки хмарних середовищ державних цифрових інформаційних ресурсів.**

Під впливом сучасних викликів, що прискорюють цифрову трансформацію, уряди країн зосереджуються на модернізації та адаптації цифрової інфраструктури державного сектору. Це, зі свого боку, зумовлює нагальну потребу в ефективних інструментах кіберзахисту. Тестування на проникнення (пентестинг) є одним із пріоритетних методів виявлення вразливостей інформаційних систем. Цей інструмент базується на моделюванні потенційної атаки для виявлення недоліків у конфігурації систем, програмному забезпеченні або організаційних процесах захисту даних та виконує функцію активного аудиту безпеки критичних цифрових інформаційних ресурсів державного сектору (Антонюк, б.д.). Проведення пентесту дозволяє своєчасно визначати загрози та ухвалювати обґрунтовані управлінські рішення щодо посилення інформаційної безпеки, зокрема шляхом оновлення політик безпеки, модернізації технічної інфраструктури та вдосконалення інструкцій із кібербезпеки та розпорядчої документації (International Organization for Standardization, 2020); (Glazunova et al., 2020). Реалізація повноцінного процесу тестування вимагає створення окремого безпечного середовища. Доцільним є формування спеціалізованої лабораторії, оснащеної високопродуктивними обчислювальними засобами, мережевим обладнанням (комутатори, маршрутизатори), а також платформами віртуалізації або контейнеризації для симуляції типових сценаріїв атак без втручання в діючі системи (Proceedings of the 8th Workshop on Cloud Technologies in Education (CTE 2020), 2020); (Вакалюк et al., 2021). Для забезпечення навчальні та тестові середовища мають бути ізольовані від основної мережі, що дозволяє запобігти несанкціонованому поширенню зловмисного коду, витоку даних або порушенню конфіденційності. Мережева сегментація є базовим елементом архітектури

таких рішень. (Антонюк, б.д.). Управлінський аспект організації пентестингових лабораторій передбачає не лише технічну, але й правову та етичну відповідність: усі перевірки мають здійснюватися з дозволу власника ІТ-інфраструктури із дотриманням принципів законності, об'єктивності та прозорості (Маслова et al., 2020). Важливою складовою залишається підготовка персоналу — регулярні тренування підвищують професійну готовність до інцидентів і стимулюють розвиток адаптивних механізмів реагування. Упровадження лабораторій пентестингу в інформаційних структурах публічного сектору може сприяти не лише підвищенню кіберстійкості органів влади, а й формувати умови для сталого розвитку цифрової безпеки в межах державної політики інформаційної трансформації (Маслова et al., 2020).

Одним із ключових інструментів логічної ізоляції цифрового середовища в публічному секторі є впровадження віртуальних локальних мереж (VLAN), що забезпечують незалежність мережевих сегментів без потреби у фізичному розділенні інфраструктури (International Organization for Standardization, 2020); (Yevseiev et al., 2021). Це критично важливо для функціонування аналітичних, наукових і освітніх підрозділів, що поєднують обслуговування громадськості з цифровізацією. Раціональне проектування ізольованої мережі передбачає використання комутатора, WAP-пристроїв та основного маршрутизатора з підключенням до інтернету. Конфігурація портів — зокрема поділ на trunk- та access-порти — дозволяє функціонально розмежовувати трафік (Glazunova et al., 2020). Це створює два незалежні середовища: для адміністративних завдань і для дослідницьких цілей у сфері кібербезпеки (Proceedings of the 8th Workshop on Cloud Technologies in Education (CTE 2020), 2020). Застосування VLAN знижує ризик поширення шкідливого коду та підтримує реалізацію політики кібергігієни відповідно до стандартів інформаційної безпеки (International Organization for Standardization, 2020). Встановлення PVID, а також робота з tagged- / untagged-трафіком

забезпечує коректне функціонування портів відповідно до архітектури мережі (Антонюк, б.д.). Візуалізація топології демонструє практичну реалізацію безпечного середовища в умовах дослідницької лабораторії з кібербезпеки. Така модель може бути адаптована для використання в академічних або державних ІТ-системах, де важливо дотримуватися принципів розділення функціональних зон. Розміщення окремих WAP без активного DHCP і відключення SSID на боці провайдера дозволяють централізовано керувати адресним простором і запобігти несанкціонованому доступу (Антонюк, б.д.). Для підвищення рівня безпеки доцільною є інтеграція апаратного міжмережевого екрану, що дозволяє реалізувати принцип мінімальних привілеїв в умовах доступу до мережевих ресурсів.

Формування захищеного віртуального середовища в системі цифрового державного управління може передбачати створення лабораторних платформ, що імітують реальні умови функціонування інформаційної інфраструктури держави. Ключовим елементом такого середовища є побудова гнучкої та безпечної мережевої архітектури, яка забезпечує як ізольовану взаємодію між віртуальними машинами, так і контрольований доступ до глобальних мережевих ресурсів (Антонюк, б.д.). Для реалізації зазначених вимог використовується розмежування мережевих інтерфейсів на локальний (LAN) та глобальний (WAN). LAN-інтерфейс відповідає за внутрішню комунікацію між віртуальними інстанціями, дозволяючи моделювати сценарії функціонування ІТ-систем органів влади в середовищі з обмеженим доступом. WAN-інтерфейс забезпечує вихід до інтернету, що необхідно для дослідження міжмережевих запитів, а також для моделювання потенційних загроз, включно з несанкціонованими спробами доступу до державних ресурсів (Антонюк, б.д.). Архітектурне розділення інтерфейсів створює основу для інформаційної гігієни — ключової передумови розробки політик безпеки цифрового урядування. У межах дослідницької моделі всі віртуальні машини, за винятком захис-

ної, приєднуються до локального сегмента, що дозволяє досягти ізоляції, оптимізувати внутрішній трафік і знизити ризики витоку інформації. Централізовану маршрутизацію виконує віртуальний шлюз, який контролює взаємодію між сегментами (Антонюк, б.д.). Зазначена конфігурація дозволяє ефективно тестувати політики кібербезпеки, зокрема у сфері захисту критичної інформаційної інфраструктури, що є важливою складовою цифровізації публічного сектору.

Отже, забезпечення стійкості державних цифрових інформаційних систем до зовнішніх і внутрішніх загроз є ключовим чинником цифрової трансформації публічного сектору. Одним із пріоритетів виступає виявлення вразливостей у програмному забезпеченні, пов'язаних із помилками коду, дефіцитом перевірок даних, порушеннями логіки функціонування або недосконалістю архітектури (Diogenes et al., б.д.). Першим етапом виступає ідентифікація вразливостей, що потенційно загрожують доступності, цілісності або конфіденційності даних. Такий аналіз базується на вивченні архітектури, взаємодії модулів і механізмів автентифікації (Антонюк, б.д.). Наступний крок — моделювання наслідків, серед яких витоки даних, DoS-атаки, маніпуляції, фінансові втрати (International Organization for Standardization, 2020). Оцінка загального рівня загрози здійснюється з урахуванням поширеності вразливості, доступності експлоїтів та ролі системи в інфраструктурі державного управління (Glazunova et al., 2020). Це дозволяє диференціювати рівень ризику та сформувати відповідні сценарії реагування. Фінальним етапом є впровадження захисних заходів, зокрема оновлень, модифікацій коду, змін автентифікаційних процедур і зонування доступу (Proceedings of the 8th Workshop on Cloud Technologies in Education (CTE 2020), 2020). У державному секторі такі дії повинні відповідати правовим нормам, зокрема Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» (Верховна Рада України, 1994). Моніторинг та аудит безпеки є постійними елементами ризик-менеджменту. Вони

включають аналіз журналів подій, перевірку конфігурацій, контроль за доступом і виявлення аномалій. Ці заходи спрямовані на вчасне виявлення нових загроз та підтримку відповідності стандартам. Інтеграція технічного й управлінського підходів до кібербезпеки дозволяє забезпечити цілісність функціонування державних цифрових сервісів, зменшити репутаційні втрати та сформувати довіру громадськості (Президент України, 2021).

**Висновки та рекомендації щодо підвищення ефективності рівня безпеки державних цифрових інформаційних ресурсів.** Забезпечення належного рівня кібербезпеки є одним із ключових завдань органів державної влади. Воно потребує системного підходу до формування державної політики, що охоплює міжвідомчу взаємодію між органами влади, інститутами громадянського суспільства, бізнесу, достатнє ресурсне забезпечення, а також постійне оновлення стратегічних підходів відповідно до змін у цифровому середовищі (Антонюк, б.д.); (International Organization for Standardization, 2020).

Державна політика в галузі кібербезпеки охоплює такі основні напрями:

- міжнародна взаємодія, яка передбачає участь України в глобальних ініціативах, уніфікацію законодавства з міжнародними стандартами, посилення співпраці з міжнародними структурами та організацію спільних заходів (Glazunova et al., 2020);
- національна безпека та внутрішня політика, що включає створення Національної системи кібербезпеки, стандартизацію захисту критичної інфраструктури та вдосконалення нормативного забезпечення правоохоронної діяльності у сфері кіберзлочинності (Proceedings of the 8th Workshop on Cloud Technologies in Education (CTE 2020), 2020);
- безпека та оборона, де акцент робиться на підготовці відповідних державних структур до кібероперацій, захисті військових та державних інформаційних

систем, розвитку фахового кадрового потенціалу (Вакалюк et al., 2021);

- освіта, наука та інновації, що передбачають розвиток освітніх програм із кібербезпеки, популяризацію знань серед молоді, підвищення кваліфікації працівників критичної інфраструктури та формування цифрової культури (Маслова et al., 2020).

Системна реалізація державної політики потребує створення ефективної інституційної архітектури. До суб'єктів національної системи кібербезпеки належать Служба безпеки України, Міністерство внутрішніх справ, Міністерство оборони, Генеральний штаб Збройних Сил України, Державна служба спеціального зв'язку та інші уповноважені органи (Крайнов et al., 2020). Для координації їхньої діяльності доцільним є створення Державного агентства з питань кіберзахисту, функції якого включатимуть аналітику загроз, нормативно-методичне забезпечення, ведення реєстрів об'єктів критичної інфраструктури та надання дозволів на використання засобів захисту (Diogenes et al., б.д.).

Важливим завданням є адаптація чинного законодавства до нових викликів, зокрема внесення змін до законів України «Про основи національної безпеки», «Про кібербезпеку», «Про критичну інфраструктуру», а також до Кримінального кодексу та КУпАП — із метою чіткого визначення відповідальності за кіберзлочини, інтеграції поняття цифрових доказів та вдосконалення процедур реагування на інциденти (Федченко, 2018). Окрему увагу слід приділити гармонізації національного законодавства із стандартами ЄС та НАТО — зокрема у сферах сертифікації, аудитів, ліцензування, кібергігієни, оцінки ризиків та спільного реагування (Верховна Рада України, 2017). У цьому контексті рекомендовано ухвалити Національний план реагування на інциденти інформаційної безпеки, який має передбачати алгоритми дій, строки реагування, канали комунікації та механізми відновлення систем. Також необхідно розвивати кадровий потенціал у сфері публічного управління через оновлення державних освітніх стандартів із включенням

компетентностей з кіберзахисту, створення системи підвищення кваліфікації держслужбовців із використанням сертифікованих платформ. Важливою складовою є розвиток державно-приватного партнерства, зокрема через угоди про спільне реагування на кіберінциденти, обмін інформацією про загрози, участь бізнесу у формуванні політик та залучення ІТ-компаній до аудиту безпеки державних систем. Комплексна реалізація цих заходів забезпечить не лише стійкість публічного управління до цифрових загроз, але й підвищить рівень довіри до органів державної влади, що є критично важливим в умовах воєнного стану та глобальної цифровізації.

Ефективне функціонування цифрового середовища державних установ вимагає впровадження цілісної системи заходів з кібербезпеки, що включає: аудит безпеки, перегляд політик інформаційного захисту, виявлення вразливостей, адаптацію нормативно-правової бази та розробку комплексної стратегії захисту інформації. Значну роль відіграє впровадження антивірусних рішень, систем шифрування, обмеження доступу до об'єктів критичної інфраструктури, а також підвищення цифрової грамотності персоналу. Одночасно важливими є постійний моніторинг загроз, резервне копіювання даних, а також проведення тестування на проникнення (пентестингу) як дієвого інструмента для оцінки ступеня вразливості систем. Пентестинг виконує не лише технічну, а й управлінську функцію — результати випробувань є основою адаптації заходів із кіберзахисту. Вивчення ризиків, пов'язаних із виявленими вразливостями, потребує динамічного підходу до оцінки загроз у цифровому середовищі. Систематичний аналіз потенційних наслідків дозволяє своєчасно реагувати на інциденти й мінімізувати політичні, репутаційні та економічні втрати. Запропоновано модель інтегрованого управління інформаційною безпекою, яка поєднує нормативно-правові, технічні та освітні компоненти. Серед пріоритетних заходів — удосконалення політик контролю доступу, реалізація навчальних

програм з кібергігієни, оновлення стратегій захисту інформації та підвищення цифрової компетентності працівників органів державної влади.

Запропоновані в статті рекомендації з підвищення рівня кіберзахисту державних цифрових систем у хмарних середовищах мають комплексний характер і охоплюють ключові рівні управління кібербезпекою — стратегічний, технічний та організаційний.

Стратегічний рівень включає формування та реалізацію державної політики у сфері кібербезпеки, відповідність законодавства з міжнародними стандартами, участь у глобальних ініціативах, розвиток міжнародного партнерства, створення національної інституційної архітектури та міжвідомчої координації тощо.

Технічний рівень охоплює проведення пентестингу, аудитів безпеки, впровадження сучасних рішень із шифрування та захисту даних, резервне копіювання, постійний моніторинг загроз, використання сертифікованих засобів захисту та адаптацію технічних заходів до нових вразливостей тощо.

Організаційний рівень має включати розвиток кадрового потенціалу, впровадження навчальних програм із кібергігієни та підвищення кваліфікації державних службовців, розширення державно-приватного партнерства, впровадження ефективних політик контролю доступу та процедур реагування на інциденти тощо.

Реалізація запропонованих заходів сприятиме зміцненню кіберстійкості державних цифрових ресурсів, зниженню ризиків витоку або компрометації даних, підвищенню довіри громадян та міжнародних партнерів до цифрової інфраструктури України. Комплексний підхід, що поєднує управлінські, технічні та організаційні інструменти, є критично важливим в умовах воєнного стану та глобальної цифрової трансформації.

Забезпечення цифрового суверенітету України можливе лише за умови цілісного підходу до кібербезпеки, що інтегрує інноваційні технології, управлінські рішення та правове регулювання.

## REFERENCES

1. Антонюк, П. Є. (2009). Класифікація ймовірних способів вчинення атак на інформацію як напрям протидії комп'ютерній злочинності. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*, 19, 231-240. [http://www.nbu.gov.ua/portal/Soc\\_Gum/bozk/19text/g1927.htm](http://www.nbu.gov.ua/portal/Soc_Gum/bozk/19text/g1927.htm)
2. Вакалюк, Т. А., & Мар'єнко, М. В. (2021). Досвід використання хмаро орієнтованих систем відкритої науки в процесі навчання і професійного розвитку вчителів природничо-математичних предметів. *Інформаційні технології і засоби навчання*, 81(1), 340–355. <https://www.doi.org/10.33407/itlt.v81i1.4225>
3. Закон України «Про інформацію» № 2657-XII (1992). <https://zakon.rada.gov.ua/laws/show/2657-12#Text>
4. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» № 80/94-ВР (1994). <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text>
5. Закон України «Про ратифікацію Конвенції про кіберзлочинність № 2824-IV (2005) <https://zakon.rada.gov.ua/laws/show/2824-15#Text>
6. Закон України «Про Державну службу спеціального зв'язку та захисту інформації» № 3475-IV (2006). <https://zakon.rada.gov.ua/laws/show/3475-15#Text>
7. Закон України «Про доступ до публічної інформації» № 2939-VI (2011). <https://zakon.rada.gov.ua/laws/show/2939-17>
8. Закон України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII (2017). <https://zakon.rada.gov.ua/laws/show/2163-19>
9. Закон України «Про національну безпеку України» № 2469-VIII (2018). <https://zakon.rada.gov.ua/laws/show/2469-19>
10. Закон України «Про захист персональних даних» № 2297-VI (2010) <https://zakon.rada.gov.ua/laws/show/2297-17#Text>
11. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» № 80/94-ВР (1994). <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80>
12. Diogenes, Y., & Ozkaya, E. (2018). *Cybersecurity – Attack and Defense Strategies*. <https://www.tsoungui.fr/ebooks/CYBER-Security.pdf>
13. DOU. (2018). Що варто знати про GDPR. <https://dou.ua/lenta/articles/what-gdpr-is/>
14. Glazunova, O., Voloshyna, T., Korolchuk, V., & інші. (2020). Cloud-oriented environment for flipped learning of the future IT specialists. *E3S Web of Conferences*. <https://www.doi.org/10.1051/e3sconf/202016610014>
15. Hewlett Packard Enterprise. (2016). Наукове дослідження Інтернету речей від Hewlett Packard Enterprise. [https://json.tv/tech\\_trend\\_find/nauchnoe-issledovanie-interneta-veschey-ot-hewlett-packard-enterprise-20160503115845](https://json.tv/tech_trend_find/nauchnoe-issledovanie-interneta-veschey-ot-hewlett-packard-enterprise-20160503115845)
16. International Organization for Standardization. (2020). *ISO/IEC 27035-3:2020: Information security incident management – Part 3: Guidelines for ICT incident response operations*. <https://www.iso.org/standard/74033.html>
17. Постанова Кабінету Міністрів України «Про затвердження правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» № 373 (2006). <https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF#Text>
18. Постанова Кабінету Міністрів України «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» № 518 (2019). <https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text>
19. Київський центр безпеки. (б.д.). Украинский ресурс по безопасности. <http://kiev-security.org.ua>
20. Крайнов, В. О., Маланчук, М. Ф., & Грозовський, Р. І. (2020). Методика оцінки ефективності комплексної системи захисту інформації автоматизованих інформаційних систем органів військового управління. *Сучасні інформаційні технології у сфері безпеки та оборони*, 1(37), 103–106. <https://sit.nuou.org.ua/article/view/199608/202809>

21. Маслова, Н. О., & Полуніна, Д. О. (2019). Методи біометричної автентифікації при ідентифікації особи. *Науковий вісник ДонНТУ* (1-2), 12-20. <https://visnyk.donntu.edu.ua/wp-content/uploads/2020/06/Maslova.pdf>
22. Microsoft. (б.д.). Керівництво по GDPR. <https://docs.microsoft.com/en-us/office365/admin/security-and-compliance/gdpr-compliance?view=o365-worldwide>
23. Постанова НБУ «Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України» № 95 (2017). <http://zakon2.rada.gov.ua/laws/show/en/v0095500-17/page>
24. Network Cultures. (б.д.). The Internet of Things: A Critique of Ambient Technology and the AllSeeing Network of RFID. [https://www.networkcultures.org/\\_uploads/notebook2\\_theinternetofthings.pdf](https://www.networkcultures.org/_uploads/notebook2_theinternetofthings.pdf)
25. Указ Президента України «Про заходи щодо вдосконалення державної політики в інформаційній сфері» № 449/2014 (2014). <https://zakon.rada.gov.ua/laws/show/449/2014>
26. Указ Президента України «Про Стратегію національної безпеки України» № 287/2015 (2015). <https://zakon.rada.gov.ua/laws/show/287/2015>
27. Указ Президента України «Питання Національного координаційного центру кібербезпеки» № 242/2016 (2016). <https://zakon.rada.gov.ua/laws/show/242/2016>
28. Указ Президента України «Про Стратегію кібербезпеки України» № 96/2016 (2016). <https://zakon.rada.gov.ua/laws/show/96/2016>
29. Указ Президента України «Про Доктрину інформаційної безпеки» № 47/2017 (2017). <https://zakon.rada.gov.ua/laws/show/47/2017>
30. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» № 447/2021 (2021). <https://zakon.rada.gov.ua/laws/show/447/2021#Text>
31. Proceedings of the 8th Workshop on Cloud Technologies in Education (CTE 2020). (2020). <https://ceur-ws.org/Vol-2879/>
32. Федченко, Д. (2018). Система забезпечення кібербезпеки: проблеми формування та ефективної діяльності. *Молодий вчений. Юридичні науки*, 5(57), 653-658. <https://molodyivchenyi.ua/index.php/journal/article/view/4603>
33. Yevseiev, V., & other. (2021). Development of conception for building a critical infrastructure facilities security system. *Eastern-European Journal of Enterprise Technologies*, 3(9 (111)), 63-83. <https://www.doi.org/10.15587/1729-4061.2021.233533>

## CYBERSECURITY OF GOVERNMENT DIGITAL SYSTEMS: PENTESTING OF CLOUD ENVIRONMENTS

**Abstract.** *The article reviews and analyzes research areas in the field of cybersecurity of state digital systems. It is emphasized that in the context of digitalization and the implementation of digital governance, cybersecurity of state digital systems is of particular importance. This is due to the need to increase the resilience of the organizational environment to cyber threats and strengthen the information sovereignty of the State. Relevant aspects regarding the prospects for improving legislation are identified, and a comprehensive system of recommendations is formed, which includes both management solutions and technical cybersecurity measures.*

*It is noted that the use of cloud technologies has the potential to improve and increase the efficiency of the functioning of state institutions. At the same time, possible cyber threats and risks associated with the use of cloud technologies are emphasized. The methodology of pentesting in cloud environments of state digital information resources is considered.*

*The article presents proposals and provides recommendations for improving cyber protection in state digital information systems.*

**Keywords:** *information security audit, security of government systems, information protection, cybersecurity, pentesting, penetration testing, digital tools, cloud environments.*

#### ІНФОРМАЦІЯ ПРО АВТОРА

**Жорняк Андрій** — PhD, доктор філософії в галузі публічного управління та адміністрування, головний державний інспектор відділу з питань безпеки праці південного напрямку управління інспекційної діяльності у Київській області Центрального міжрегіонального управління Державної служби з питань праці, вул. Вавілових, 10, м. Київ, 04060, Україна; e-mail: dr.andrij.zhorniak@gmail.com; ORCID: 0000-0001-9515-0180

#### INFORMATION ABOUT THE AUTHOR

**Zhorniak Andrii** — PhD, Doctor of Philosophy in Public Administration and Management, Chief State Inspector of the Labour Safety Department of the Southern Division of the Inspection Department in Kyiv Region of the Central Interregional Directorate of the State Labour Service of Ukraine, 10 Vavilovykh Street, Kyiv, 04060, Ukraine; e-mail: dr.andrij.zhorniak@gmail.com; ORCID: 0000-0001-9515-0180