УДК 351.86:004.056:35.08:327

Гончарук Ю.В.[1]

[1] Національний лісотехнічний університет України, Львів, Україна,
ORCID 0009-0000-0314-1579

Державна політика у сфері кібербезпеки: міжнародне партнерство як інструмент розвитку кадрового потенціалу держслужби

Анотація. У тезах розглядаються пріоритети державної політики у сфері кібербезпеки в умовах воєнного стану та новітніх загроз 2025–2026 років. Обґрунтовано, що людський фактор є критичною вразливістю, що вимагає трансформації підходів до підготовки держслужбовців — від теорії до практичної кіберстійкості. Висвітлено роль міжнародного партнерства та досвіду ENISA у розвитку кадрового потенціалу, а також впровадження Європейської рамки навичок (ECSF). Проаналізовано вплив штучного інтелекту на кібератаки та захисні механізми, доцільність стратегії Zero Trust та захисту ланцюгів постачання ПЗ. Визначено шляхи вдосконалення публічного управління через гармонізацію законодавства з Директивою NIS2 та впровадження стандартів ISO для зміцнення національної стійкості.

Ключові слова: публічне управління, державна безпека, кібербезпека, державна служба, інформаційна безпека.

В умовах повномасштабної війни та безперервних кібератак на критичну інформаційну інфраструктуру України питання кібербезпеки вийшло за межі суто технічних ІТ-рішень і стало фундаментальною складовою національної стійкості. Найбільш вразливою ланкою в системі захисту державної інформаційної інфраструктури та інформації залишається людський фактор. Фішинг, соціальна інженерія та використання несертифікованого програмного забезпечення є основними векторами атак ворога. Саме тому формування ефективної державної політики щодо безперервного навчання та підвищення кваліфікації державних службовців є критичним завданням сьогодення.

Потрібно здійснювати захист державних реєстрів і баз даних, забезпечити безперервність роботи органів влади, захищати персональні дані громадян і протидіяти кібератакам.

Традиційний підхід до навчання публічних службовців часто обмежується базовими курсами цифрової грамотності, що не відповідає актуальному ландшафту загроз. Сучасна державна політика має бути орієнтована на перехід від теоретичного ознайомлення до набуття практичних навичок кібергігієни та кіберстійкості (cyberresilience). Реалізація такого переходу потребує значних ресурсів, методологічної бази та доступу до сучасних тренінгових платформ.

Основні завдання кібербезпеки наведені на рисунку

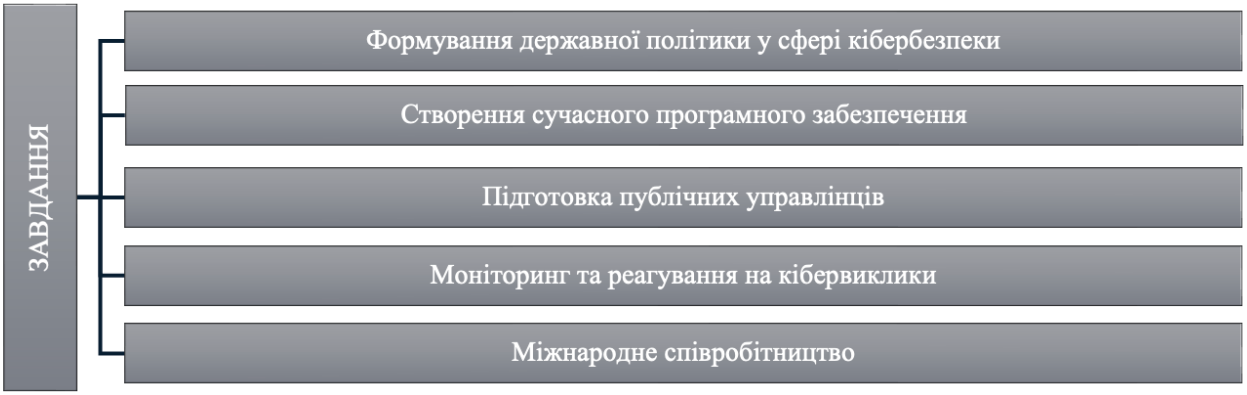

Рис. 1. Основні завдання кібербезпеки
Джерело: [1,2]

Міжнародне партнерство є ключовим інструментом стратегічного розвитку кадрового потенціалу державної служби України. Інтеграція європейських стандартів (зокрема підходів

ENISA) та залучення міжнародної допомоги дозволяють побудувати сучасну систему безперервної підготовки управлінців. Водночас ця співпраця поступово набуває двостороннього характеру: українські державні службовці, отримуючи міжнародну експертизу, водночас діляться з партнерами унікальним практичним досвідом забезпечення стійкості державного апарату в умовах реальної кібервійни. Звіт Європейської комісії за 2025 рік щодо прогресу України на шляху до вступу в ЄС надає інформацію щодо цифрової оборони. Цей офіційний документ, хоч і охоплює широкий спектр реформ, містить конкретні факти та оцінки стану кібербезпеки в країні. Аналіз цих даних дозволяє аналізувати не лише досягнення, але й виклики, що стоять перед Україною [3].

Зі звіту випливає п'ять ключових висновків щодо стану кібербезпеки в Україні, що базуються виключно на офіційних даних звіту Єврокомісії. Вони є об'єктивним аналізом того, як Україна створює цифровий захист, інтегрується в європейський безпековий простір та готується до майбутніх викликів:

1. Створено комплексну національну систему кіберзахисту.
2. Йде поступова інтеграція з ЄС у сфері кіберзахисту.
3. Розвивається співпраця з Агентством Європейського Союзу з кібербезпеки (ENISA).
4. Розширюється співпраця у фінансовому секторі.
5. Розпочалася розбудова мережі 5G, яка, щоправда, наразі виглядає серйозною потенційною вразливістю у критичній інфраструктурі [3].

Звіт ЄС підтверджує, що Україна не просто реагує на загрози, а діє на основі чіткої стратегії. В країні діє стратегія кібербезпеки, а законодавча база постійно посилюється для відповіді на нові виклики. Ключовим кроком стало ухвалення в березні 2025 року змін до законів про інформаційний захист та кіберзахист. Ці зміни формалізували створення єдиної національної системи реагування на кіберінциденти.

Згідно зі звітом, співпраця України з інституціями Європейського Союзу у сфері кібербезпеки за 2025 рік значно поглибилася і стала системною. Це свідчить про те, що Україна розглядає євроінтеграцію не лише як політичну мету, але і як практичний інструмент для посилення власної безпеки [3]. Зокрема, у документі наведено конкретні приклади такої співпраці:

- Співпраця з Агентством Європейського Союзу з кібербезпеки (ENISA), що дозволяє Україні долучатися до найкращих європейських практик та стандартів.
- Проведення регулярного Кібердіалогу Україна-ЄС, який слугує платформою для стратегічної координації та обговорення спільних загроз.
- Підписання меморандуму про співпрацю між Національним координаційним центром кібербезпеки (НКЦК) та Європейським центром компетенцій у сфері кібербезпеки (ECCC) у березні 2025 року, відкрило шлях до спільних проєктів та досліджень.
- Розвиток тристоронньої співпраці з Румунією та Молдовою, яка включає компонент кібербезпеки, що свідчить про розбудову регіонального поясу безпеки.

Така глибока інтеграція має подвійний ефект. По-перше, вона надає Україні доступ до передових технологій, експертизи та розвідувальних даних ЄС, що прямо посилює її обороноздатність. По-друге, вона прискорює гармонізацію українського законодавства з європейським, що є невід'ємною частиною процесу інтеграції до Євросоюзу. Таке стратегічне зближення з ЄС не лише забезпечує безпеку, але й стимулює впровадження найкращих практик для захисту життєво важливих секторів економіки, насамперед фінансової системи та критичної інфраструктури.

Звіт Єврокомісії окремо виділяє зусилля України, спрямовані на захист фінансового сектору, як один із пріоритетів національної кібербезпеки. Стабільність банківської системи є фундаментом економічного виживання країни в умовах війни.

Міжнародне співробітництво стало каталізатором розвитку кадрового потенціалу української держслужби у сфері кібербезпеки. Міжнародна технічна допомога та програми підтримки (зокрема, від USAID, CRDF Global, ініціативи в рамках Талліннського механізму) забезпечують Україну необхідною інфраструктурою для проведення практичних навчань. Завдяки донорській підтримці впроваджуються спеціалізовані тренінгові програми для представників різних державних відомств, відбуваються регулярні симуляції кібератак та тестування на вразливість персоналу.

Ключовим напрямком державної політики у сфері підготовки кадрів є синхронізація української системи з європейськими стандартами. Імплементація європейського досвіду, зокрема Директиви NIS2, вимагає від України зміни парадигми відповідальності. Відповідно до стандартів ЄС, сектор державного управління визнається "суттєво важливим" (essential entity), що робить обов'язковим спеціалізоване навчання для керівного складу органів влади та покладає на них персональну відповідальність за управління кіберризиками. Для операційного персоналу нормою стає не лише базова кібергігієна, але й навички забезпечення безперервності роботи (business continuity), кіберстійкості (cyberresilience) та суворе дотримання протоколів звітування про інциденти.

Впровадження Європейської рамки навичок з кібербезпеки (ECSF), розробленої Агентством Європейського Союзу з кібербезпеки (ENISA), дозволяє чітко профілювати вимоги до українських держслужбовців. Використання стандартів ENISA сприяє:

- Уніфікувати вимоги до компетентностей державних службовців відповідно до їхніх посадових обов'язків.
- Створити єдиний стандарт оцінювання знань із кібербезпеки в органах державної влади.
- Інтегрувати європейські навчальні модулі в програми Вищої школи публічного управління України.

У 2026 році штучний інтелект (AI) – це чинник, який змінює структуру кібератак. AI робить атаки швидшими і більш масовими, а захист – більш автоматизованим. Використовуються генеративні моделі для створення фішингових повідомлень і листів. Вони швидко адаптують тексти під конкретну посаду та державну структуру, підбирають стиль комунікації, спонукають до термінових дій. Такі технології, як Deepfake, підсилюють ці схеми. Це можуть бути голосові та відео дезінформації, які використовуються для підроблених погоджень платежів або доступу.

AI-інструменти дозволяють швидше писати шкідливий код та його модифікувати, що дозволить обходити захисні механізми, проводити розвідку тощо. AI підсилює людські можливості, пришвидшує підготовку та масштабування.

В той же час спеціалісти з кіберзахисту також використовують штучний інтелект. AI-інструменти допомагають виявляти аномалії, класифікувати події, виявляти реальні інциденти та прискорювати реагування. AI перевіряє автентичність та поведінкові моделі, які допомагають помітити підміну.

Органи публічного управління не можуть вважати свій інформаційний простір безпечним в непередбачуваному цифровому середовищі. Кожний процес, кожний пристрій і запит до ресурсу мають перевірятися. Потрібно мінімально обмежувати доступ до даних. Сьогодні інформація виходять далеко за межі локальної мережі. У такому середовищі модифікація одного облікового запису може сприяти доступу до критичних систем в тих випадках, якщо немає контекстної перевірки і контролю доступу.

Нещодавно з’явилась стратегія Zero Trust – принцип «нульової довіри». Простими словами, перед тим, як здійснити авторизацію, в системі повинна бути здійснена технічна перевірка. Наприклад, при авторизації в систему, працівник вводить логін та пароль.

У цьому році кібератаки часто спрямовуються атаки open-source компоненти, CI/CD-інфраструктуру тощо. Для органів публічного управління це є дуже небезпечним тому, що компрометація може відбутися не через власні дії, а через чужий компонент, який є критично важливим.

У 2026 році безпека стає частиною інженерного циклу. Органи публічного управління мають перевіряти код, конфігурації, права доступу, секрети та інше. Крім того програмне забезпечення має бути прозорим, постійно оновлюватися і контролюватися у продукті, і як це оновлюється.

Потрібно весь час вдосконалювати інформаційну безпеку для захисту публічного управління.

Основні напрями вдосконалення інформаційної безпеки публічних управлінців охоплюють комплекс організаційних, технічних, правових і кадрових заходів.

Напрями вдосконалення кіберзахисту публічних управлінців наведені на рисунку

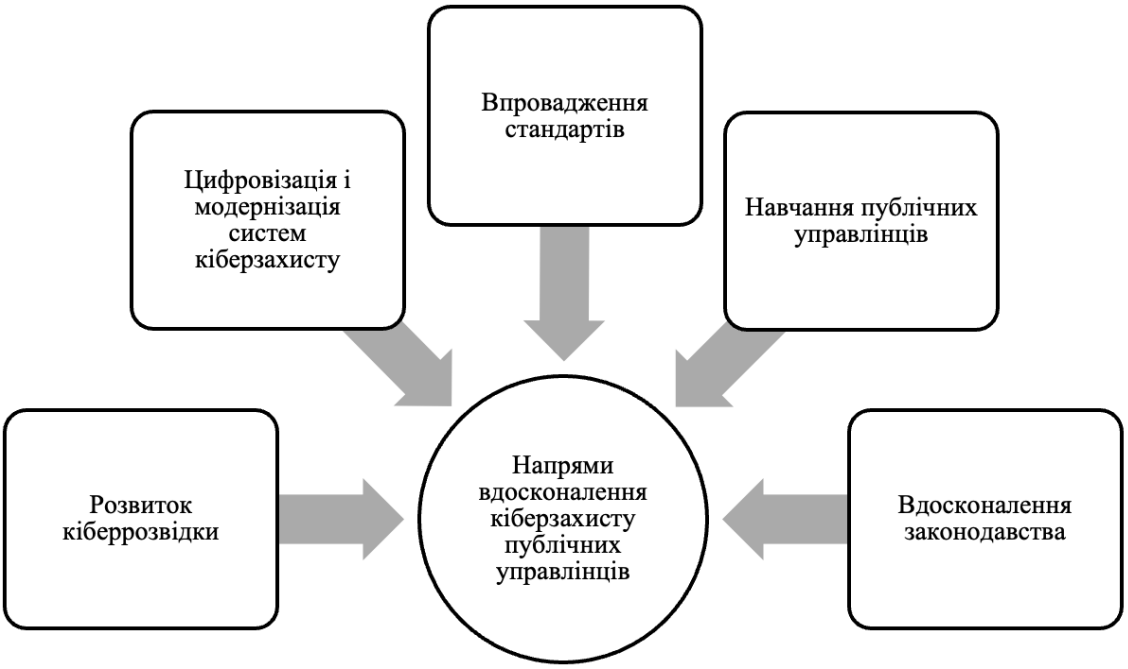

Рис. 2. Напрями вдосконалення кіберзахисту публічних управлінців
Джерело: [1,2]

Потрібно на основі стандартів, наприклад ISO 27001 створювати системи управління інформаційною безпекою і впроваджувати системи внутрішнього контролю. Одним з найважливіших елементів цих систем має бути підвищення рівня обізнаності персоналу шляхом навчання і тренінгів, забезпечення контролю доступу до інформації відповідно до посадових обов'язків, перевіряти персонал при прийомі на роботу тощо.

Українське законодавство у сфері інформаційної та кібербезпеки потребує постійного оновлення та гармонізації з міжнародними стандартами й нормативами, з урахуванням динамічного розвитку інформаційних технологій, актуальних викликів часу та змін, що відбуваються у відповідному регуляторному полі Європейського Союзу.

Список використаних джерел:

1. *Положення про Міністерство цифрової трансформації України: постанова Кабінету Міністрів України від 18 верес. 2019 р. № 856. Офіційний вісник України. 2019. № 80. Ст. 2736.*
2. *Про захист інформації в інформаційно-комунікаційних системах: Закон України від 05 лип. 1994 р. № 80/94-ВР : із змінами, внесеними згідно із Законом № 1089-IX від 16 груд. 2020 р. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80 (дата звернення: 28.04.2026).*
3. *Цифровий щит України: 5 ключових висновків про кіберстійкість. CyberSec.net.ua. URL: https://cybersec.net.ua/statti/932-tsyfrovyi-shchyt-ukrainy-5-kliuchovykh-vysnovkiv-pro-kiberstiikist (дата звернення: 28.04.2026).*