ПУБЛІЧНЕ УПРАВЛІННЯ У СФЕРІ ДЕРЖАВНОЇ БЕЗПЕКИ ТА ОХОРОНИ ГРОМАДСЬКОГО ПОРЯДКУ

УДК 351:004.056
DOI https://doi.org/10.32782/TNU-2663-6468/2026.2/26

Лихач Ю. Ю.
https://orcid.org/0000-0003-0945-0692
Вища школа публічного управління

ФОРМУВАННЯ КУЛЬТУРИ КІБЕРЗАХИСТУ В ОРГАНАХ ДЕРЖАВНОЇ ВЛАДИ ЯК ЧИННИК ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ СТІЙКОСТІ

Забезпечення кібербезпеки є одним із пріоритетів України у системі формування національної стійкості. Реалізація зазначеного пріоритету буде здійснюватися шляхом посилення спроможностей національної системи кібербезпеки для протидії кіберзагрозам у сучасному безпековому середовищі.

У статті досліджено питання формування культури кіберзахисту в органах державної влади як одного з ключових чинників забезпечення національної стійкості України в умовах цифровізації та воєнної агресії. Обґрунтовано, що сучасні кіберзагрози, зокрема кібератаки на державні інформаційні ресурси, об'єкти критичної інфраструктури та інформаційно-психологічні операції, становлять суттєву небезпеку для функціонування держави та потребують комплексного реагування. Проаналізовано стан державної політики у сфері кібербезпеки, нормативно-правове забезпечення та діяльність ключових суб'єктів національної системи кібербезпеки.

Визначено, що важливим елементом протидії кіберзагрозам є не лише технічний захист інформаційних систем, а й підвищення рівня цифрової грамотності та формування відповідної поведінкової моделі державних службовців. Наголошено, що людський фактор залишається одним із найуразливіших елементів системи кібербезпеки, що зумовлює необхідність системного впровадження культури кібергігієни та безпечної роботи з інформаційними ресурсами.

Запропоновано комплекс рекомендацій, спрямованих на формування культури кіберзахисту, зокрема: впровадження системного навчання, розвиток професійних компетентностей, забезпечення функціонування підрозділів кіберзахисту, удосконалення внутрішніх політик безпеки та активізацію інформаційно-роз'яснювальної роботи.

Зроблено висновок, що формування культури кіберзахисту є необхідною умовою підвищення ефективності державного управління, зміцнення інформаційної безпеки та забезпечення стійкості України до сучасних гібридних загроз.

Ключові слова: *кіберзахист, кібербезпека, кіберзагрози, цифрова грамотність, публічні службовці, забезпечення національної стійкості.*

Постановка проблеми. Питання кіберзахисту та кібербезпеки в Україні є надзвичайно актуальними в умовах стрімкого розвитку інформаційних технологій та їх поширення в усі сфери суспільного життя. Особливої гостроти ця проблема набула після початку повномасштабного вторгнення російської федерації в Україну, що супроводжується значним зростанням кількості кібератак на інформаційні системи, ресурси та вебсайти органів державної влади й органів місцевого самоврядування.

Сфера кібербезпеки стала одним із ключових елементів національної безпеки та стійкості України, адже сучасні воєнні дії розгорнулись не лише на полі бою, а й у кіберпросторі та інформаційно-комунікативному середовищі. Одним із най-

більш серйозних викликів є зростання кількості та складності кібератак на органи державної влади, а також на об'єкти критичної інфраструктури, зокрема енергетичні системи, транспортно-логістичні мережі, банківський сектор, телекомунікаційні системи та інформаційні ресурси державних інституцій.

У зв'язку з цим особливої важливості набуває формування ефективної державної політики у сфері кібербезпеки, удосконалення нормативно-правового забезпечення кіберзахисту та формування культури кібербезпеки серед державних службовців.

Аналіз наукових досліджень і публікацій. Проблематика забезпечення кібербезпеки як складової національної безпеки привертає значну увагу як зарубіжних, так і вітчизняних науковців.

Серед зарубіжних фахівців, які проводили наукові дослідження у сфері інформаційної та кібербезпеки, варто відзначити Ліндемалдера Грегга (Lindmulder Gregg), Косінскі Метта (Kosinski Matt), Мішра Неха (Mishra Neha), Петера Вршанського (Peter Vršanský), Даніеля Беднара (Daniel Bednár), Скотт А. Броуна (S.A. Brown), Діба Аламі Харанді (Diba Aalami Harandi) та інших.

Вагомий внесок у дослідження проблем інформаційної та кібербезпеки зробили українські науковці, зокрема І. Арістов, Д. Безуглий, І. Бондаренко, І. Березовська, О. Дзьобань, Р. Калюжний, Б. Кормич, В. Котутенков, В. Ліпкан, А. Марущак, М. Падалка, В. Панасевич, В. Потій, І. Трегубенко, В. Цимбалюк, О. Юдін та інші.

Питання формування ефективного нормативно-правового механізму протидії загрозам у сфері кібербезпеки досліджували І. Сопілко, В. Куцаєв, Є. Живило, Д. Мінін, В. Шеломенцев, В. Бурячок, С. Гнатюк та інші.

Разом з тим, у сучасних умовах розвитку цифрового середовища та посилення кіберзагроз, зумовлених воєнною агресією проти України, питання формування культури кіберзахисту в органах державної влади потребують подальших наукових досліджень.

Постановка завдання. Метою статті є аналіз сучасної державної політики України у сфері кібербезпеки та підготовка рекомендації щодо запровадження культури кіберзахисту в органах державної влади як чинника забезпечення національної стійкості.

Виклад основного матеріалу. Забезпечення кібербезпеки є одним із пріоритетних напрямів державної політики України у сфері формування національної стійкості. Реалізація цього пріоритету передбачає посилення спроможностей суб'єктів національної системи кібербезпеки щодо протидії сучасним кіберзагрозам.

З розвитком інформаційних технологій та цифровізації суспільства зростає і рівень кіберзагроз, що безпосередньо впливає на функціонування органів державної влади, підприємств та установ. Крім того, кіберпростір дедалі більше визнається одним із ключових театрів воєнних дій поряд із суходолом, морем, повітряним і космічним простором.

В Україні це проявляється у численних спробах несанкціонованого доступу до державних інформаційних ресурсів, атаках на вебсайти органів державної влади, поширенні шкідливого програмного забезпечення, а також проведенні інформаційно-психологічних операцій у соціальних мережах.

За даними Національної команди реагування на кіберінциденти CERT-UA, яка функціонує при Державній службі спеціального зв'язку та захисту інформації України, у 2025 році було опрацьовано 5927 кіберінцидентів, що на 37,4 % більше порівняно з 2024 роком, коли було зафіксовано 4315 інцидентів [1].

Зростання загальної кількості кіберінцидентів пов'язано не лише зі зростанням інтенсивності атак, а й зі збільшенням можливостей кіберзахисників до їх виявлення та підвищення кіберобізнаності населення. Найчастіше зловмисники атакують місцеві органи влади, уряд та урядові організації, сектор безпеки та оборони, енергетичний сектор, комерційні організації, телекомунікації.

Найбільшу кількість атак у 2025 році було спрямовано на:

– місцеві органи влади – 2115 інцидентів;
– урядові організації – 1170 інцидентів;
– сектор безпеки та оборони – 1039 інцидентів;
– енергетичний сектор – 279 інцидентів;
– медична галузь – 95 інцидентів;
– IT-сектор – 75 інцидентів.

Аналіз типів інцидентів свідчить про масове розповсюдження шкідливого програмного забезпечення (далі – ШПЗ) та соціальної інженерії. Найпоширенішими методами стали:

– розповсюдження ШПЗ – 2058 випадків;
– фішинг – 1727 випадків;
– зараження ШПЗ – 988 випадків;
– компрометація облікових записів – 425 випадків [1].

Подібного роду атаки часто є складовою спланованих гібридних операцій, спрямованих на дестабілізацію держави зсередини та отримання

стратегічно важливої інформації. Під час війни найціннішою для ворога є інформація про плани Сил оборони України, дані підприємств оборонно-промислового комплексу, а також логістичні та фінансові ресурси органів державної влади. Такі типи атак разом з фішингом залишаються наймасовішими інструментами агресора.

Актуальним викликом є також інформаційно-психологічні атаки, що реалізовуються через неправдиві новини та маніпулятивний контент. Такі дії мають на меті посіяти паніку, підірвати довіру до держави та діяльності органів державної влади, зруйнувати національну єдність. Масштабні атаки цього типу можливі, зокрема, з огляду на сучасний рівень цифровізації суспільства. Окрім того, слід враховувати ризики, пов'язані з наявністю ворожих ІТ-продуктів на ринку, які можуть містити приховані механізми збору даних або саботування. В умовах війни це питання набуває особливої ваги, оскільки стосується безпеки як держави, так і кожного громадянина.

Національна система кібербезпеки являє собою комплексну систему взаємодії між Державною службою спеціального зв'язку та захисту інформації України, Національною поліцією України, Службою безпеки України, Міністерством оборони України та Генеральним штабом Збройних Сил України, розвідувальними органами. Їхня діяльність має на меті забезпечити кібербезпеку та взаємопов'язані заходи політичного, науково-технічного, інформаційного, освітнього характеру, а також кіберзахист об'єктів критичної інформаційної інфраструктури.

Основним суб'єктом національної системи кібербезпеки є Державна служба спеціального зв'язку та захисту інформації України, яка здійснює забезпечення функціонування і розвитку державної системи урядового зв'язку, Національної системи конфіденційного зв'язку, формування та реалізації державної політики у сферах криптографічного та технічного захисту інформації, кіберзахисту, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку, активної протидії агресії у кіберпросторі. Крім того, вона спрямовує свою діяльність на забезпечення національної безпеки України від зовнішніх і внутрішніх загроз та є складовою сектору безпеки і оборони України.

Кібербезпека є ключовим елементом національної безпеки України. Законодавче забезпечення кібербезпеки включає низку нормативно-правових актів, стратегій та програм, спрямованих на захист інформаційного простору країни. Ще 2005 року Україна ратифікувала Будапештську конвенцію –міжнародний документ з кібербезпеки, який визначає спільну кримінальну політику щодо захисту від кіберзлочинності шляхом прийняття відповідного внутрішнього законодавства та сприяння міжнародному співробітництву.

Законодавче забезпечення державної політики кібербезпеки та кіберзахисту складається з відповідних нормативно-правових актів. До основних з них слід віднести Закони України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII [2], «Про Державну службу спеціального зв'язку та захисту інформації України» від 23 лютого 2006 року № 3475-IV [3], «Про електронні комунікації» від 16 грудня 2020 року № 1089-IX [4].

Крім того, Указом Президента України «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» передбачено формування нової якості національної системи кібербезпеки [5]. Реалізація даної стратегії має забезпечити:

– стійкість до кіберзагроз, підвищивши здатність державних органів, бізнесу і громадян захищати себе та реагувати на кіберзагрози;

– спроможність до ефективної протидії недружнім діям у кіберпросторі, забезпечивши їх швидке виявлення та розслідування,

– створення ефективної системи превентивних заходів щодо недопущення таких дій, а також можливість проведення наступальних операцій у кіберпросторі;

– розвиток кадрового потенціалу та інноваційного ринку кібербезпеки, що сприятиме створенню національних розробок для забезпечення можливості протидіяти майбутнім кіберзагрозам.

Окрім цього, реформа кіберзахисту є однією з умов Ukraine Facility Plan, яка передбачає наближення законодавства в сфері кібербезпеки до Директиви NIS2, що встановлює єдині для ЄС правила щодо кібербезпеки. Оскільки Україна не входить до ЄС, Директива NIS2 не є зобов'язуючою, однак вона служить настановою з питань належної практики.

З метою реалізації реформи кібербезпеки 27 березня 2025 року було ухвалено Закон України №4336-IX «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури» [6]. Він містить положення, які забезпечують імплементацію норм європейських директив з кібербезпеки до національного законодавства та дає мож-

ливість протистояти новим викликам і загрозам у кіберпросторі. Документ передбачає створення та забезпечення функціонування національної системи реагування на інциденти кібербезпеки, кібератаки, кіберзагрози щодо інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, об'єктів критичної інформаційної інфраструктури. Також пропонується створити в органах державної влади і на об'єктах критичної інфраструктури підрозділи з кіберзахисту та ввести штатні посади керівників та фахівців з кібербезпеки.

Цифрова грамотність, компетентності щодо основ кіберзахисту та кібергігієни на сьогодні є однією із вимог для ефективної роботи державних службовців. Це, перш за все, здатність ефективно та безпечно використовувати сучасні цифрові технології в роботі, навчанні, професійному та особистісному розвитку.

Недостатня обізнаність співробітників, порушення правил цифрової гігієни, використання застарілих програмних продуктів можуть поглибити цю проблему. Крім того, в умовах воєнного стану серед фахівців органів державної влади виріс запит на посилення знань та навичок з використання цифрових інструментів для дистанційної роботи (проведення нарад, роботи з інформацією, електронного документообігу, електронної пошти, тощо).

У зв'язку з цим та на виконання постанов КМУ від 8 жовтня 2025 року № 1281 та від 19 червня 2019 року № 518, а також наказу Адміністрації Держспецзв'язку від 3 грудня 2025 року №798 керівники органів державної влади організовують та забезпечують регулярне навчання своїх співробітників з питань кіберзахисту, яке проводиться диференційовано залежно від функціональних обов'язків та з урахуванням професійної кваліфікації співробітників.

Успіх органів державної влади в забезпеченні кібербезпеки значною мірою залежить від поінформованості співробітників. Як показує практика, навіть найсучасніші системи безпеки можуть постраждати від людської помилки. Державні службовці не завжди дотримуються базових правил кібербезпеки: не змінюють на регулярній основі паролі, не стежать за антивірусним захистом комп'ютерів, відвідують шкідливі сайти тощо.

Тож важливо сформувати культуру кіберзахисту в органах державної влади, яка передбачає вироблення у державних службовців звичок та моделей поведінки, що захищають дані, включаючи регулярне навчання, впровадження кібергігієни (паролі, оновлення) та підвищення обізнаності про загрози. Така діяльність передбачає низку організаційних та технічних заходів, спрямованих на запобігання витокам даних та атакам, а також своєчасне виявлення, запобігання і нейтралізацію реальних і потенційних загроз, що у контексті забезпечення національної стійкості набуває особливого значення.

Висновки. З урахуванням викладеного доцільно сформувати рекомендації щодо запровадження культури кібербезпеки в органах державної влади:

1. Запровадження культури кібербезпеки, яка передбачає обізнаність співробітників щодо потенційних ризиків, їх ідентифікацію та реагування на них або повідомлення про них. Формування такої культури передбачає ряд заходів. Зокрема в частині:

– використання складних, унікальних паролів та багатофакторної автентифікації для запобігання несанкціонованому доступу;

– обмеження доступу користувачів лише до ресурсів, необхідних для виконання їхніх посадових обов'язків;

– організації систематичного навчання з питань кіберзагроз, правил безпечного використання технологій;

– створення та безпечне зберігання копій важливих даних для можливості відновлення у разі втрати даних або кібератаки;

– регулярних оновлень програмного забезпечення та встановлення виправлень (патчів);

– використання захисту від шкідливих програм;

– безпечної конфігурації систем та пристроїв: посилення стандартних налаштувань та виділення непотрібних служб;

– наявності розробленого плану для реагування на інциденти кібербезпеки та відновлення після них.

2. Здійснення на постійній основі внутрішнього аналізу навчальних потреб державних службовців з питань цифрової грамотності та кібербезпеки.

3. Включення до індивідуальних програм професійного розвитку державних службовців питань цифрової грамотності, штучного інтелекту, кібербезпеки та кібергігієни. Навчання має бути безперервним процесом, який формує звички безпечної поведінки. Такі навчальні заходи мають буди побудовані з дотриманням базових засад:

– навчання має відображати специфіку діяльності органу державної влади;

– матеріали навчання мають бути адаптовані під специфіку діяльності, посадові обов'язки та рівень посади кожного співробітника;

– зміст навчальних програм необхідно регулярно оновлювати з урахуванням нових типів атак і загроз та змін в законодавстві;

– за результатами навчання важливо здійснювати оцінку ефективності, яка допомагає зрозуміти, як змінюється поведінка працівників і які аспекти потребують додаткової уваги.

4. Сприяння у проходженні державними службовцями онлайн-курсів з питань кібербезпеки та кібергігієни на відповідних освітніх платформах (Дія. Цифрова освіта, StudyiЯ, Prometheus тощо).

5. Забезпечення функціонування в структурі міністерств та інших центральних органів виконавчої влади підрозділів з кіберзахисту та введення штатних посад керівників та фахівців з кібербезпеки.

6. Організація спеціалізованих навчань для фахівців з кібербезпеки за програмами Вищої школи публічного управління.

7. Сприяння залученню фахівців з кібербезпеки до проведення тренінгів з питань кібербезпеки та кібергігієни в рамках організації внутрішніх навчань міністерства та інших центральних органів виконавчої влади.

8. Забезпечення систематичного нагадування державним службовцям про важливість та основні практики кібергігієни, які є критичними для зниження ризиків кібербезпеки та забезпечення стійкості органів державної влади в цифровому просторі через внутрішні інформаційні канали.

9. Організація спеціалізованих тренінгів з питань кібербезпеки та кібергігієни для керівного складу органів державної влади (керівників та заступників керівників, державних секретарів, заступників з питань цифровізації) на базі Вищої школи публічного управління та CDTO Campus за участі фахівців Держспецзв'язку.

10. Проведення фахівцями з кібербезпеки інструктажів, внутрішніх навчань та систематичних тренінгів щодо кібергігієни з метою підвищення рівня обізнаності та формування практичних навичок безпечного користування засобами інформатизації та Інтернетом для запобігання, своєчасного виявлення та реагування на кіберінциденти, кібератаки, забезпечення захисту персональних даних, а також дотримання вимог законодавства у сфері кібербезпеки та відповідних стандартів, політик безпеки та особливостей у відповідній сфері або галузі.

11. Розробка та затвердження внутрішніх нормативних документів, що регламентують проведення інструктажів, брифінгів і систематичних навчань з питань кібергігієни та кібербезпеки в органах держаної влади.

Список літератури:

1. CERT-UA у 2025 році опрацювала майже 6000 кіберінцидентів: кількість ворожих атак зросла на 37%. URL: https://cip.gov.ua/ua/news/cert-ua-u-2025-roci-opracyuvala-maizhe-6000-kiberincidentiv-kilkist-vorozhikh-atak-zrosla-na-37 (дата звернення: 25.03.2026).

2. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII : станом на 19 жовт. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 25.03.2026).

3. Про Державну службу спеціального зв'язку та захисту інформації України : Закон України від 23.02.2006 № 3475-IV : станом на 20 квіт. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/3475-15#Text (дата звернення: 25.03.2026).

4. Про електронні комунікації : Закон України від 16.12.2020 № 1089-IX : станом на 27 лют. 2026 р. URL: https://zakon.rada.gov.ua/laws/show/1089-20#Text (дата звернення: 25.03.2026).

5. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України від 26.08.2021 № 447/2021 URL: https://www.president.gov.ua/documents/4472021-40013 (дата звернення: 25.03.2026).

6. Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури : Закон України від 27.03.2025 № 4336-IX. URL: https://zakon.rada.gov.ua/laws/show/4336-20#Text (дата звернення: 25.03.2026).

Lykhach Yu. Yu. FOSTERING CYBERSECURITY CULTURE IN PUBLIC AUTHORITIES AS A FACTOR IN ENSURING NATIONAL RESILIENCE

Ensuring cybersecurity is one of Ukraine's key priorities within the system of building national resilience. The implementation of this priority will be carried out by strengthening the capacity of the national cybersecurity system to counter cyber threats in the modern security environment.

The article examines the issue of developing a cybersecurity culture in public authorities as one of the key factors in ensuring Ukraine's national resilience in the context of digitalization and military aggression. It is substantiated that modern cyber threats, including cyberattacks on state information resources, critical infrastructure, and information and psychological operations, pose a significant risk to the functioning of the state and require a comprehensive response. The study analyzes the current state policy in the field of cybersecurity, the regulatory and legal framework, and the activities of key actors within the national cybersecurity system.

It is determined that an important element of countering cyber threats is not only the technical protection of information systems but also the improvement of digital literacy and the formation of appropriate behavioral patterns among civil servants. It is emphasized that the human factor remains one of the most vulnerable elements of the cybersecurity system, which necessitates the systematic implementation of cybersecurity hygiene and safe practices in handling information resources.

A set of recommendations aimed at developing a cybersecurity culture is proposed, including the introduction of systematic training, the development of professional competencies, ensuring the functioning of cybersecurity units, improving internal security policies, and enhancing information and awareness activities.

It is concluded that the development of a cybersecurity culture is a necessary condition for improving the effectiveness of public administration, strengthening information security, and ensuring Ukraine's resilience to modern hybrid threats.

Keywords: *cyber defense, cybersecurity, cyber threats, digital literacy, public servants, ensuring national resilience.*

Дата першого надходження статті до видання: 26.03.2026
Дата прийняття статті до друку після рецензування: 30.04.2026
Дата публікації (оприлюднення) статті: 29.05.2026