УДК 351:004.056.5:004.738.5(477)

В. І. Саричев, О. О. Поплавський, О. В. Черкаський

СИСТЕМА КІБЕРБЕЗПЕКИ ПУБЛІЧНОГО СЕКТОРУ УКРАЇНИ: СТРУКТУРНІ ПРОБЛЕМИ, УПРАВЛІНСЬКІ МОДЕЛІ ТА СТРАТЕГІЧНІ НАПРЯМКИ МОДЕРНІЗАЦІЇ

У статті обґрунтовано стратегічні засади розвитку системи кібербезпеки публічного сектору України в умовах цифрової трансформації, євроінтеграції та воєнних загроз. На основі аналізу національних стратегічних документів і міжнародних підходів: Директиви NIS 2 (Network and Information Security Directive 2, нормативно-правовий акт ЄС щодо заходів із забезпечення високого спільного рівня кібербезпеки в державах-членах), NIST CSF 2.0 (Cybersecurity Framework – рамкова модель управління кібербезпекою), Zero Trust (архітектурний підхід щодо кібербезпеки, який базується на принципі «нікому не довіряй, усе перевіряй»), – систематизовано управлінські інструменти кіберзахисту публічних інституцій. Виявлено структурні проблеми: фрагментарність регулювання, нерівномірність кіберзрілості, кадровий дефіцит, недостатня інтеграція управлінських і технологічних рішень, слабкість ризик-орієнтованого управління та культури безпеки. Запропоновано стратегічні цілі й принципи, концептуальну модель розвитку та інструменти її реалізації, моніторингу й оцінювання ефективності для органів державного управління.

Ключові слова: *кібербезпека, публічний сектор, державне* управління, NIS 2, NIST CSF 2.0, Zero Trust, кіберзрілість, кіберстійкість.

Постановка проблеми. Стрімка цифровізація публічного сектору України (електронні послуги, реєстри, міжвідомчі платформи) розширює поверхню атаки та підвищує залежність державного управління від цифрових компонентів, що є типовим викликом для цифровізованих систем публічного адміністрування й критичної інфраструктури [4, 7, 11]. В умовах воєнного часу ці ризики посилюються гібридним характером загроз, коли кібервплив поєднується з інформаційно-психологічними операціями та тиском на спроможність держави безперервно надавати публічні послуги [7, 11].

Попри наявність нормативних і організаційних елементів кіберзахисту, у публічному секторі зберігаються системні бар'єри: фрагментарність регулювання, нерівномірна кіберзрілість установ, кадровий дефіцит, слабка інтеграція управлінських і технічних рішень та недостатньо розвинуте партнерство з приватним і громадянським секторами [7, 8, 11]. У такій ситуації модернізація системи кібербезпеки потребує переходу від переважно реактивних практик до ризик-орієнтованої моделі управління, узгодженої з європейським регуляторними рамками стандарту NIS 2, а також із сучасними вимогами технологій управління кіберризиками (NIST CSF 2.0 і Zero Trust) [12].

Аналіз останніх досліджень і публікацій. Проблематика кібербезпеки публічного сектору досліджується на перетині державного управління, цифрової трансформації та національної безпеки. Значний масив робіт присвячений захисту критичної інфраструктури, еволюції загроз і підходам до забезпечення кіберстійкості [7, 11], а також системним наслідкам цифровізації інфраструктури і управлінських контурів [4]. Окремі дослідження пропонують інструментальні підходи до структуризації управлінських знань (наприклад, онтології/Knowledge Graph для критичної інфраструктури) [10], що може бути корисним для стандартизації політик і процесів у публічних органах.

Водночас у науковому дискурсі простежуються прогалини, критичні саме для публічного сектору України: (1) домінування техніко-правового фокусу над управлінським аналізом; (2) недостатня інтеграція кібербезпеки в моделі належного врядування та повний цикл публічної політики; (3) дефіцит цілісних стратегічних моделей, адаптованих до умов повномасштабної війни та євроінтеграційних зобов'язань [3, 7].

Метою статті є теоретичне обґрунтування та розроблення стратегічних засад розвитку системи кібербезпеки у публічному секторі України на основі синтезу управлінських моделей і міжнародних підходів до кіберзахисту та кіберстійкості [7, 11]. Досягнення мети передбачає формування інтегрованого стратегічного бачення (цілей, принципів, пріоритетів), узгодженого з вимогами NIS 2 та логікою управління кіберризиками NIST CSF 2.0 [12], а також орієнтованого на реалізацію в органах влади та місцевого самоврядування.

Виклад основного матеріалу. Логіка дослідження передбачає змістове уточнення таких основних понять, як система кібербезпеки у публічному секторі та механізми державного управління у сфері кібербезпеки, а також визначення його ефективних методологічних підходів.

Систему кібербезпеки у публічному секторі України пропонується розуміти як організовану сукупність суб'єктів публічної влади, норм права, управлінських процесів, інституційних структур, ресурсів і технологій, спрямованих на забезпечення конфіденційності, цілісності, доступності та стійкості інформаційних ресурсів і інформаційно-комунікаційних систем органів державної влади, місцевого самоврядування та підпорядкованих їм організацій. Стратегічні засади розвитку системи кібербезпеки – це сукупність довгострокових цілей, принципів, пріоритетів, управлінських моделей і базових рішень щодо архітектури, інституційного дизайну та ресурсного забезпечення, які визначають бажаний стан системи, траєкторію її еволюції та правила ухвалення управлінських рішень у середньостроковій і довгостроковій перспективі.

Поряд з цим механізми державного управління у сфері кібербезпеки варто сприймати як інституційно закріплені способи впливу суб'єктів публічної влади на об'єкт управління (систему кібербезпеки), що включають правові, організаційні, економічні, інформаційні, технологічні, кадрові та комунікаційні інструменти, а також процедури планування, реалізації, моніторингу та оцінювання політики в цій сфері.

Отже, спираючись на таке змістове уточнення, можна визначити провідні методологічні підходи представленого дослідження, серед яких найбільш продуктивними є такі:

1) системний підхід, який дозволяє розглядати кібербезпеку публічного сектору як багаторівневу систему, де взаємодіють нормативно-правовий, інституційний, технологічний, кадровий, організаційно-процесуальний та культурно-ціннісний рівні;

2) інституційний підхід, що акцентує увагу на формальних і неформальних правилах, організаційних структурах, компетенціях суб'єктів забезпечення кібербезпеки, а також на механізмах міжвідомчої координації та взаємодії держави, бізнесу й громадянського суспільства;

3) процесний підхід, який застосовано для аналізу циклу державної політики у сфері кібербезпеки – від формулювання проблеми та постановки цілей до впровадження, моніторингу, оцінювання та корекції політик і програм;

4) ризик-орієнтований підхід, що забезпечує концентрацію на оцінюванні й управлінні кіберризиками, включно з ризиками ланцюгів постачання, людського фактору та експлуатації вразливостей інформаційних систем публічного сектору. Він корелює з вимогами директиви NIS 2 та сучасними фреймворками управління кіберризиками;

5) порівняльний підхід, який використано для зіставлення національних стратегічних документів та інституційних практик із європейськими та міжнародними стандартами (NIS 2, NIST CSF, Zero Trust Architecture), що дозволяє адаптувати найкращі практики до умов України.

Логіка дослідження побудована таким чином: спочатку уточнюється категоріальний апарат та методологічні засади; далі – аналізуються глобальні тренди та виклики кібербезпеці; після цього – виявляються структурні проблеми вітчизняної системи кібербезпеки у публічному секторі; на цій основі формулюються стратегічні цілі, принципи, пріоритети й пропонується концептуальна модель; завершальний блок присвячено механізмам реалізації, моніторингу та оцінювання ефективності.

На рис. 1 продемонстровано ці ключові методологічні підходи, що разом формують цілісну логіку дослідження.

Рис. 1 – Ключові методологічні підходи дослідження

У центрі знаходиться вузол методологічних підходів, від якого розходяться основні аналітичні напрямки: системний підхід зосереджується на аналізі взаємозв'язків між елементами системи й дозволяє розглядати об'єкт як цілісну структуру з інтегрованими компонентами; інституційний підхід, спрямований на оцінку організаційної структури, ролі інституцій, формальних і неформальних правил та механізмів функціонування; процесний підхід акцентує увагу на потоках і операціях, що дає змогу досліджувати послідовність дій, управлінські цикли та логіку реалізації політик; ризик-орієнтований підхід зосереджується на ідентифікації та оцінці загроз, визначенні вразливостей і прогнозуванні ризиків, що дозволяє визначати критичні точки та формувати превентивні механізми; порівняльний підхід забезпечує можливість аналізу альтернатив, зіставлення різних моделей і стратегій, що допомагає обрати найбільш ефективне рішення. У сукупності ці підходи забезпечують багатовимірне бачення об'єкта дослідження та дозволяють отримати комплексні збалансовані висновки.

Важливим чинником представленого дослідження є також врахування того, що сучасне середовище кібербезпеки характеризується низкою таких потужних тенденцій, критично важливих для публічного сектору:

– гібридизація загроз, поєднання кібератак з інформаційно-психологічними операціями, фізичним впливом на інфраструктуру та економічним тиском;

– зростання ролі держав та недержавних акторів, які здійснюють цілеспрямовані кібератаки на публічні інституції, виборчу систему, органи управління критичною інфраструктурою;

– розширення цифрового сліду держави через е-послуги, реєстри, системи «єдиного вікна», open data-платформи, що збільшує площину атаки;

– швидке впровадження хмарних сервісів, мобільних рішень, IoT-інфраструктури та інтелектуальних систем аналізу даних у публічному секторі;

– зростання залежності публічного управління від цифрових платформ, керованих приватним сектором (хмарні провайдери, телеком-оператори, постачальники IT-рішень).

Паралельно Україна орієнтується на гармонізацію власної системи кібербезпеки з європейськими підходами, насамперед доктриною NIS 2, яка встановлює єдине тлумачення правового стандарту для забезпечення високого рівня кібербезпеки в критичних секторах, включно з публічною адміністрацією, та вимагає від держав-членів формувати національні стратегії, системи координації й моніторингу (табл. 1).

Таблиця 1 – Структурні проблеми національної системи кібербезпеки у публічному секторі

№	**Ключова структурна проблема**
1	Фрагментарність регулювання: підзаконні акти і відомчі документи неузгоджені, відсутня єдина методична рамка для мінімальних стандартів, політик та процедур
2	Нерівномірна кіберзрілість: частина органів влади має стандарти і SOC/CSIRT-функції, але багато установ, особливо місцевих, працюють на застарілій інфраструктурі та з неформалізованими процедурами
3	Обмежений кадровий потенціал: дефіцит фахівців, конкуренція з приватним сектором, слабка система підготовки та мотивації, що знижує спроможність підтримувати потрібний рівень кіберзахисту
4	Недостатня інтеграція рішень: технічні засоби впроваджуються без змін у процесах, повноваженнях і регламентах, що знижує ефективність інвестицій у кібербезпеку
5	Слабкий розвиток ризик-орієнтованого управління: оцінювання ризиків проводиться епізодично, формально і без єдиної методології, що суперечить сучасним стандартам
6	Недостатня взаємодія з бізнесом і громадянським сектором: механізми обміну інформацією, спільних навчань та інцидент-репортингу працюють фрагментарно
7	Низька культура безпеки: людський фактор є головним джерелом вразливостей, а програми підвищення обізнаності персоналу не є системними.

У сукупності наведені у табл. 1 результати демонструють комплексний характер структурних проблем і потребу в системному стратегічному оновленні моделі кібербезпеки публічного сектору – від нормативно-правового забезпечення та кадрової політики до управлінських процесів, партнерства і розвитку ризик-орієнтованих підходів. Необхідність такого підходу обґрунтовується тим, що, як показано у табл. 1, наявні проблеми мають комплексний характер і одночасно охоплюють нормативно-правовий, організаційно-управлінський, кадровий, технологічний та культурний виміри.

Отже, першою стратегічною ціллю є забезпечення стійкості та безперервності функціонування органів публічної влади та електронних публічних послуг в умовах деструктивного впливу у кіберпросторі. Актуальність цієї цілі випливає з нерівномірності кіберзрілості та наявності застарілої інфраструктури і підтверджується зростанням гібридних загроз, ескалацією кібератак і посиленням залежності державного управління від цифрових платформ [1, 7, 11].

Друга стратегічна ціль полягає у формуванні єдиних інтегрованих управлінських та нормативно-методичних рамок стандарту кібербезпеки публічного сектору, узгоджених з їх європейськими аналогами та національними безпековими пріоритетами.

Третьою стратегічною ціллю є підвищення кіберзрілості органів влади на основі стандартизованих моделей оцінювання та розвитку спроможностей, що відповідає міжнародним підходам, викладеним у NIST CSF 2.0, ISO/IEC 27001 та відповідних європейських практиках [6, 12].

Четверта стратегічна ціль передбачає створення сталого кадрового, освітнього та науково-аналітичного потенціалу кібербезпеки публічного сектору. Необхідність цієї цілі зумовлена дефіцитом кваліфікованих фахівців та слабкістю системної підготовки кадрів, що відображено у табл. 1, а також підтверджується національними й міжнародними аналітичними даними [8, 9].

П’ята стратегічна ціль пов’язана з інституціоналізацією партнерства держави, бізнесу та громадянського суспільства у сфері кібербезпеки. Як показано у табл. 1, взаємодія з бізнесом і громадянським суспільством залишається обмеженою та фрагментарною, що ускладнює обмін інформацією про загрози, проведення спільних навчань і розвиток інцидент-репортингу. Механізми такого партнерства передбачаються як у NIS 2, так і в національних стратегічних документах та міжнародних рекомендаціях ENISA, NIST [6, 12].

На підставі визначених даних є можливим формування концептуальної моделі стратегічного розвитку системи кібербезпеки у публічному секторі.

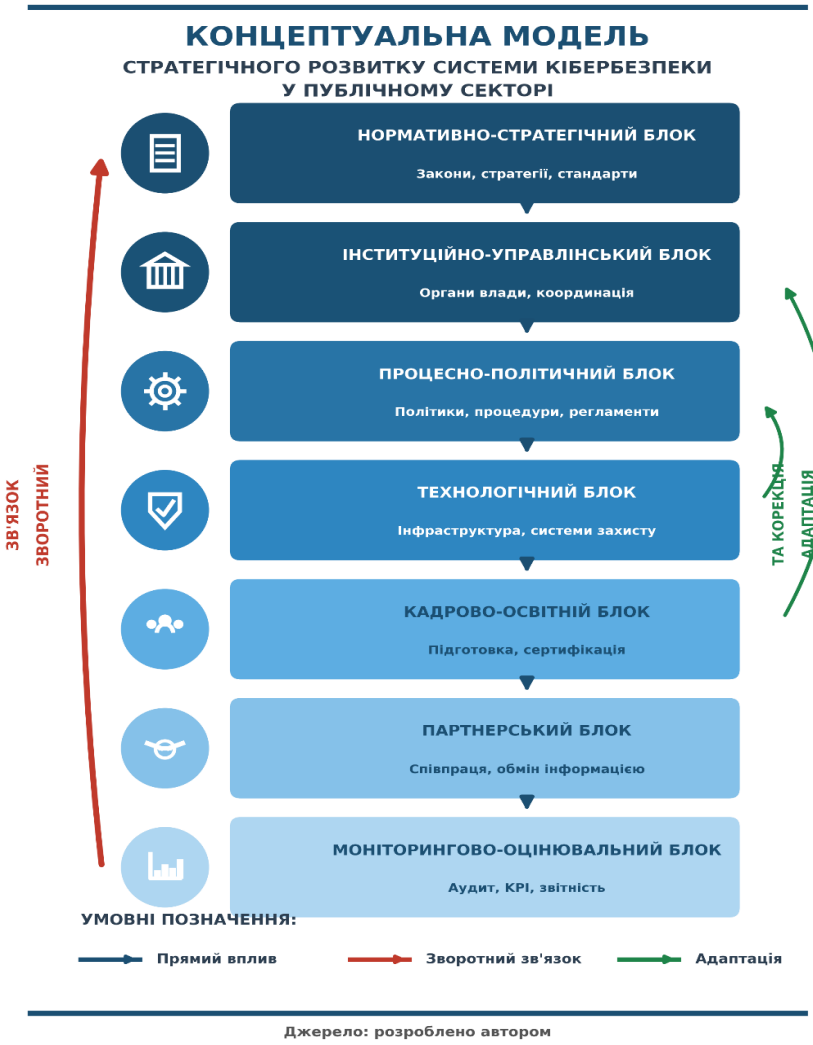

Рис. 2 – Структурні блоки концептуальної моделі

Представлена модель демонструє послідовну взаємодію семи структурних блоків, які разом формують стратегічну архітектуру розвитку системи кібербезпеки у публічному секторі. Її верхній нормативно-стратегічний блок задає правову, концептуальну і методичну основу; наступний – інституційно-управлінський блок забезпечує розподіл ролей між центральними й місцевими органами влади, визначає механізми координації та формує інституційну інфраструктуру (SOC, CERT, міжвідомчі центри); процесно-політичний блок регулює цикл формування та реалізації державної політики: від аналізу проблем і розроблення рішень до впровадження, моніторингу та корекції.

На нього спирається технологічний блок, який охоплює інфраструктурні компоненти, системи захисту, інструменти моніторингу, застосування моделей Zero Trust та міжнародних стандартів кіберзахисту. Далі модель переходить до кадрово-освітнього блоку, що формує компетентності персоналу, систему підготовки, сертифікації та культуру безпеки. Поруч розташовано партнерський блок, який забезпечує взаємодію держави з бізнесом, науковими установами, громадянським суспільством і міжнародними партнерами, створюючи спільне середовище кіберстійкості. Завершальним є моніторингово-оцінювальний блок, відповідальний за аудит, оцінювання зрілості, KPI (ключові показники ефективності), звітність та формування зворотного зв’язку, що сприяє оновленню політик і адаптації системи до нових загроз. Прямий, зворотний і адаптивний зв’язки між блоками забезпечують циклічність розвитку, безперервність удосконалення та узгодженість усіх компонентів моделі.

Проте розвиток системи кібербезпеки у публічному секторі України вимагає не лише стратегічно сформульованих цілей, але й ефективних інструментів їх практичної реалізації. В умовах цифрової трансформації, поглибленої євроінтеграції та зростання гібридних загроз органи державної влади потребують комплексної, взаємопов'язаної та адаптивної системи управлінських, нормативних, технологічних та комунікаційних рішень. Визначені у дослідженні стратегічні засади розвитку кібербезпеки публічного сектору спрямовані на підвищення кіберзрілості інституцій, забезпечення безперервності публічних сервісів, зміцнення кадрового потенціалу та формування сталих партнерських взаємодій між державою, бізнесом і громадянським суспільством. У цьому контексті важливою складовою є систематизація інструментів державного управління, які забезпечують практичну реалізацію стратегічних орієнтирів.

Представлена схема (рис. 3) демонструє логічно впорядковану архітектуру інструментів – від нормативної основи до технологічних рішень. Вона ілюструє комплексну структуру інструментів державного управління, які забезпечують практичну реалізацію стратегічних засад розвитку кібербезпеки публічного сектору. Схема побудована за принципом вертикальної послідовності: кожен наступний інструментальний блок спирається на попередній та доповнює його.

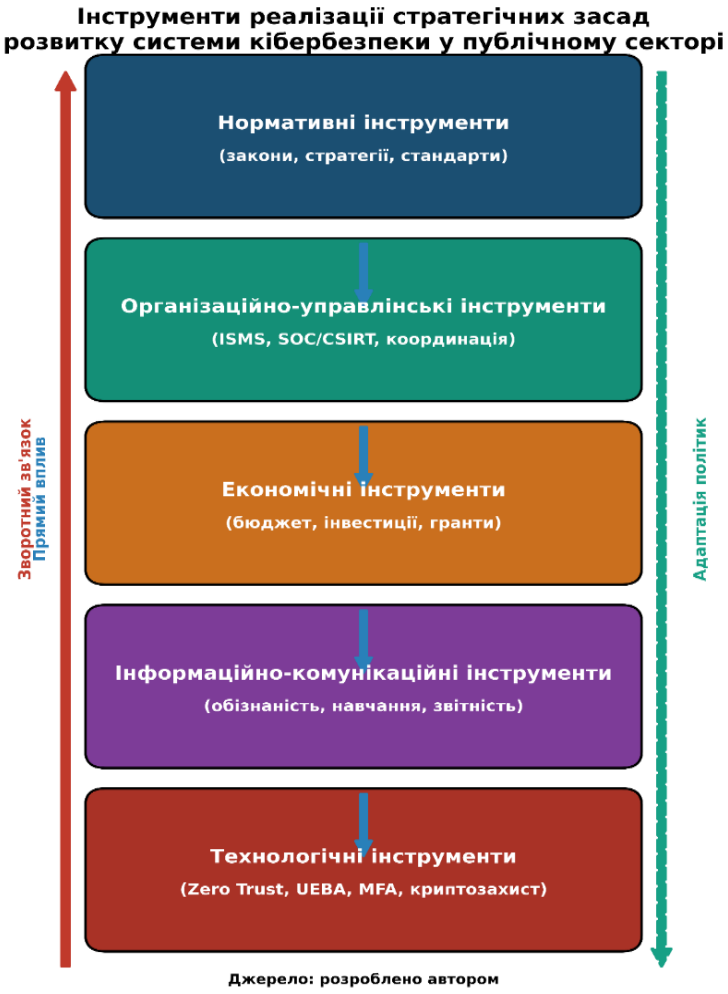

Рис. 3 – Інструменти реалізації стратегічних засад розвитку системи кібербезпеки у публічному секторі

Схема також містить дві ключові системні петлі. Зворотний зв'язок (червоний контур) іде від технологічного блоку до нормативного та забезпечує перегляд політик, оновлення стандартів і удосконалення вимог на основі отриманих результатів, аудитів і виявлених інцидентів. Адаптивний зв'язок (зелений контур) відображає можливість динамічного коригування управлінських рішень і нормативних положень на основі нових загроз, розвитку технологій та оновлення міжнародних вимог. У сукупності схема демонструє, що система кібербезпеки публічного сектору є циклічною та

самопідсилюваною: результати практичної діяльності постійно повертаються у стратегічний контур і забезпечують безперервне вдосконалення моделей, стандартів і процедур.

Висновки

У дослідженні визначені ключові проблеми розвитку кібербезпеки публічного сектору, що мають системний характер: фрагментарність регулювання і практик, нерівномірність кіберзрілості установ, дефіцит компетентних кадрів, недостатня інтеграція управлінських рішень з технологічними, а також обмежена інституціоналізація партнерства і обміну інформацією про інциденти. Це формує потребу у переході від переважно реактивної моделі захисту до ризик-орієнтованого управління, де пріоритети визначаються критичністю послуг і процесів, а заходи безпеки інтегруються у цикл планування, бюджетування, контролю та аудиту.

Сформульовані стратегічні засади розвитку системи кібербезпеки доцільно реалізовувати як комплекс взаємопов'язаних напрямів: удосконалення нормативної та організаційної архітектури, упровадження єдиних вимог і процедур управління ризиками, підвищення стійкості та відновлюваності цифрових сервісів, розвиток спроможностей моніторингу й реагування, підсилення захисту ланцюгів постачання та системної роботи з людським фактором. Практичний акцент має бути зроблений на стандартизації процесів (політики, регламенти, ролі відповідальності), розгортанні показників результативності та відповідності, забезпеченні навчання персоналу і керівного складу, а також на створенні сталих механізмів міжвідомчої координації. У підсумку, стратегічний підхід дозволяє перевести кібербезпеку з режиму переважного реагування на актуальні інциденти у режим керованої системи, де інциденти не стають нормою управління.

Отримані результати мають прикладне значення для формування та актуалізації державних і відомчих програм кіберзахисту, підготовки управлінських рішень щодо ресурсного забезпечення, проєктування організаційних моделей (функції, повноваження, відповідальність), а також для модернізації освітніх і підвищувальних програм, орієнтованих на кіберзрілість публічних інституцій. Водночас слід враховувати, що запропоновані підходи потребують подальшої емпіричної перевірки та деталізації на рівні конкретних інституційних кейсів і типів цифрових сервісів.

Напрямами подальших досліджень можуть стати: емпірична валідація запропонованих стратегічних засад на прикладах органів влади різних рівнів із порівнянням профілів ризиків, кіберзрілості та організаційних моделей; розроблення формалізованої методики оцінювання кіберзрілості публічних інституцій із чіткими рівнями, вимірюваними критеріями та профілями відповідності, а також побудова системи KPI і метрик ефективності, зокрема для виявлення, реагування, відновлення, а також для управління вразливостями та ризиками ланцюгів постачання.

Перелік джерел посилання

1. Angyalos Z., & Szilágyi R. Cybersecurity risks in critical infrastructures: Insights from CISA and ENISA data. *Journal of Agricultural Informatics*. October 2025. No. 16(2), P. 1–11. DOI: https://doi.org/10.17700/jai.2025.16.2.759.
2. Potapovs M., & Kanasta K. E. (Eds.). Cybersecurity in Latvia: Forging Resilience amidst Emerging Threats. Routledge. 2025. DOI: https://doi.org/10.4324/9781003638858.
3. Frey C. Future-proofing cybersecurity: Leveraging strategic foresight to enhance resilience. *International Journal of Cyber Diplomacy.* 2024. No. 5, P. 23–40. DOI: https://doi.org/10.54852/ijcd.v5y202402.
4. Vevera A. V. The digitalization of critical infrastructures – Systemic considerations, evolutions of governance and elements of a national research agenda. *Romanian Military Thinking.* December 2024 (3), P. 104–125.
5. Ahokangas P., & Aagaard A. (Eds.). The changing world of mobile communications: 5G, 6G and the future of digital services. Palgrave Macmillan. 2024. DOI: https://doi.org/10.1007/978-3-031-33191-6.
6. Crowther A., Foulds C., Robison R., & Gladkykh G. (Eds.). Strengthening European energy policy: Governance recommendations from innovative interdisciplinary collaborations. Palgrave Macmillan. 2024. DOI: https://doi.org/10.1007/978-3-031-66481-6.

7. Daniel S. A., & Victor S. S. Emerging trends in cybersecurity for critical infrastructure protection: A comprehensive review. *Computer Science & IT Research Journal.* 2024. No. 5(3), P. 576–593. DOI: https://doi.org/10.51594/csitrj.v5i3.872.

8. Simu S. J., & Zaman F. I. Advanced cybersecurity strategies for protecting critical infrastructure: Strengthening the backbone of national security. *International Journal of Scientific Research and Management.* 2023. No. 11 (12), P. 999–1016. DOI: https://doi.org/10.18535/ijsrm/v11i12.ec07.

9. Young D. Protecting critical infrastructure in Nigeria: A framework for integrated cybersecurity approach. *International Journal of Research and Innovation in Social Science.* 2025. No. 9 (7), P. 1151–1167. DOI: https://doi.org/10.47772/IJRISS.2025.90700095.

10. Chen J., Lu Y., Zhang Y., Huang F., & Qin J. A management knowledge graph approach for critical infrastructure protection: Ontology design, information extraction and relation prediction. *International Journal of Critical Infrastructure Protection.* 2023. 43, Article 100634. DOI: https://doi.org/ 10.1016/j.ijcip. 2023.100634.

11. Maglaras L., Janicke H., & Ferrag M. A. Cybersecurity of critical infrastructures: Challenges and solutions. *Sensors.* 2022. No. 22(14), Article 5105. DOI: https://doi.org/10.3390/s22145105.

12. European Commission. NIS2 Directive: Securing network and information systems. *Shaping Europe's Digital Future.* 2025. URL: https://digital-strategy.ec.europa.eu/en/policies/nis2-directiv (accessed: 27.11.2025).

Стаття надійшла до редакції 29.11.2025 р.

УДК 351:004.056.5:004.738.5(477)

V. Sarychev, O. Poplavskyi, O. Cherkaskyi

CYBERSECURITY SYSTEM OF THE PUBLIC SECTOR OF UKRAINE: STRUCTURAL PROBLEMS, GOVERNANCE MODELS, AND STRATEGIC MODERNIZATION DIRECTIONS

The article provides a comprehensive theoretical and methodological justification of the strategic foundations for developing the cybersecurity system in the public sector of Ukraine amid digital transformation, European integration, and full-scale armed aggression. Based on an analysis of current legislation, the Cybersecurity Strategy and the Information Security Strategy of Ukraine, as well as international standards (NIS2, NIST CSF 2.0, Zero Trust Architecture), the study systematizes modern approaches to cybersecurity of public institutions. The content of key public administration categories adapted to the sphere of public-sector cybersecurity is clarified, including "public-sector cybersecurity system", "strategic foundations for cybersecurity system development," and "public-administration mechanisms in the field of cybersecurity."

Key global trends and national challenges are identified, along with structural problems of the national cybersecurity system: fragmented regulatory frameworks, uneven cybersecurity maturity of public authorities, workforce shortages, underdeveloped risk-oriented management and security culture, and limited partnership engagement with business and civil society.

A system of strategic goals and principles for developing public-sector cybersecurity is proposed, oriented toward ensuring the resilience of public services, integration of the governance framework, and institutionalization of multilevel partnerships. A conceptual model of strategic cybersecurity system development is elaborated, comprising normative-strategic, institutional-managerial, process-political, technological, human-resource/educational, partnership, and monitoring-evaluation components. A set of tools for implementation, monitoring, and performance evaluation–suitable for practical use in state and local government bodies—is also outlined.

Keywords: *cybersecurity; public sector; public administration; strategic foundations; NIS2; NIST CSF; Zero Trust; cyber maturity; public policy; digital transformation; cyber resilience.*

Саричев Володимир Іванович – доктор економічних наук, доцент, професор кафедри економіки та економічної безпеки, Університет митної справи та фінансів
http://orcid.org/0000-0002-8544-9901

Поплавський Олег Олександрович – кандідат технічних наук, доцент, завідувач кафедри військової підготовки, Університет митної справи та фінансів
https://orcid.org/0000-0002-9023-9992

Черкаський Олександр Валерійович – аспірант, Державний університет інформаційно-комунікаційних технологій
https://orcid.org/0009-0006-3105-5217