Котух Євген Володимирович,
к.т.н, доцент кафедри кібербезпеки та інформаційних технологій,
Університет митної справи та фінансів, м. Дніпро
ORCID 0000-0003-4997-620X

УДК 351.865 **doi 10.34213/db.19.02.16**

ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В ПУБЛІЧНОМУ СЕКТОРІ В УМОВАХ ГЛОБАЛІЗАЦІЇ

Розглянуто тенденції та способи боротьби з кіберзагрозами у публічному секторі. На основі досвіду зарубіжних країн обґрунтовано переваги та недоліки електронного уряду та його потенціал у протидії кіберзлочинам. Доведено, що більш ефективною відповіддю на виклики кібербезпеки в умовах глобалізації має стати утворення публічно-приватних та публічно-громадських партнерств. Визначено, що довіра, прозорість та підзвітність стають найбільшими викликами сьогодення, які стоять перед успішним електронним урядом. Сформульовано перелік заходів та коло завдань, які доцільно делегувати нейтральним посередникам між урядами та постачальниками даних з метою забезпечення захисту інтересів та прав суб'єктів публічно-приватних відносин.

Ключові слова: публічний сектор; кіберзагроза; кібербезпека; глобалізація; прозорість діяльності.

Постановка проблеми. В умовах глобалізації так само, як і координація та інтеграція в публічному секторі, зростає тенденція до співпраці з іншими суб'єктами (приватного, публічного секторів, окремими користувачами). Все це взагалі дуже корисно й надає певні переваги для всіх причетних сторін. Хоча приватний сектор уже протягом багатьох років виступає важливим партнером уряду, публічний сектор також починає ставати важливим, новим джерелом ресурсів та досвіду для виконання завдань публічного сектору та надання послуг. Тому актуальним напрямком наукових досліджень останнім часом залишається аналіз сучасних тенденцій та пріоритетних заходів із забезпечення кібербезпеки в публічному секторі.

Аналіз останніх досліджень і публікацій. Розвиток системи публічного управління досліджено у наукових працях Т. Бєльської, В. Гриневич, В. Дзюндзюка, В. Єлагіна, Д. Карамишева та ін. Питанням забезпечення кібербезпеки у механізмі національної безпеки присвячено роботи І. Діордіци, Є. Живила, З. Коваля, В. Куцаєва, В. Ліпкана, С. Срібного, В. Ткаченка,

В. Шеломенцева та ін. Серед зарубіжних дослідників хотілося б окремо виділити напрацювання К. Андреассона, Е. Камарка, П. Кеніса, К. Прована та ін. Проте в сучасних умовах глобалізації виникають нові проблемні питання, які вимагають вдосконалених підходів визначення особливостей формування відповідної культури кібербезпеки в органах публічного управління, організаційного забезпечення її дотримання.

Мета статті – обґрунтувати організаційні проблеми та напрямки забезпечення кібербезпеки в публічному секторі в умовах глобалізації.

Виклад основного матеріалу. Важливість кібербезпеки для публічного сектору, а також для громадян та підприємств полягає в тому, як та ким, ці дані розповсюджуються, передаються та використовуються. З прийняттям інструментів та підходів Web 2.0 багато урядів переходять до парадигми "Управління 2.0", яка дозволяє мати "спільно вироблені" сервіси, в яких користувачі активно співпрацюють з постачальниками послуг, та "само-створені" сервіси, в яких послугу визначають переважно користувачі. Це також може призвести до "краудсорсингового уряду", коли контент та вклади отримуються від широкого кола користувачів та інших суб'єктів, які мають певні знання та інтереси, яких не має уряд.

Також публічний сектор турбує питання не тільки про те, чи знаходяться дані у безпеці, але й чи можуть вони бути збережені та надані для дозволеного використання в довгостроковій перспективі, зважаючи на постійні зміни форматів та стандартів даних. Тут знову очевидна необхідність компромісу між безпекою та використанням. Наприклад, для доступу до даних, що збережені на дискетах 15 років тому, сьогодні потрібне втручання фахівців при використанні музейних артефактів. Можуть допомогти хмарні обчислення, оскільки вони потенційно дозволяють розподіляти дані та інші ресурси на декількох серверах десь в Інтернеті. Але навіть якщо це вирішує проблему "куди", довгострокове збереження все ще вимагає, щоб стандарти та формати були доступними в довгостроковій перспективі.

Коли збереження даних передається на аутсорсинг до спеціалізованої

приватної компанії, або коли послуги електронного уряду, наприклад, можуть бути автоматично надані з “публічної хмари”, виникають складні питання контролю та власності, зокрема можливу втрату підзвітності та демократичного нагляду. Практика у Нідерландах демонструє не лише втрату публічного контролю, а й узурпацію всього, що робить уряд, оскільки інші можуть отримати доступ або навіть створити власні дані, релевантні до того, що раніше було публічною функцією. Мається на увазі поєднання інструментів Web 2.0 та побутової електроніки, як-от записувальне обладнання високої роздільної здатності, датчики та камери, які стають все більше вільно доступними для всіх, а не лише для професіоналів. Коли, наприклад, скарги людей, які живуть поблизу аеропорту Schiphol в Амстердамі, щодо рівня шуму літаків були ігноровані публічними органами, мешканці розробляли власну систему вимірювань на основі сенсорної технології з під’єднанням до комп’ютера та Інтернету. Система була встановлена в садках мешканців і реєструвала рівень шуму літаків. Дані записувались в електронному вигляді, збирається, поєднується з іншими даними та додатками та публікувались на їхньому вебсайті. Це ілюструє зростаючу тенденцію, коли професійні обладнання та програмне забезпечення стають товарами, доступними для кожного, щоб розробити та впровадити власні послуги, орієнтовані на інтереси користувачів. Цей випадок показує, як компетенції публічних установ та довіра до них можуть бути підірвані та узурповані. Після деякої боротьби публічні органи влади визнали, що система мешканців була більш точною та надійною, і тепер це стало сервісом де-факто. Можливо, з іншого боку, деяким зиском для уряду тут можна вважати нагоду усвідомити, що це залишається проблемою, яку необхідно обговорити, а саме те, що, втрачаючи контроль, вони також можуть втратити свою спроможність, як політичну, так і фінансову.

Іншим аспектом втрати контролю з боку уряду є вельми невтішне використання порталів електронного уряду та зростання альтернативних інструментів, керованих користувачами. Наприклад, такий портал у Великій Британії є шлюзом для всіх публічних служб і його часто оцінюють як сервіс

світового класу. Подобається це урядам чи ні, доступ до даних у публічному секторі стає розповсюдженим як через зростання кількості сторонніх провайдерів, так і завдяки урядам. Насправді деякі країни зараз переходять від концепції порталу до багатоканальних методів надання послуг, які пропонують громадянам прямий доступ до місцевих послуг, спрощуючи послуги та скорочуючи час, необхідний для здійснення запиту на послуги, та зменшуючи кількість кроків, необхідних для здійснення транзакції. Такий перехід ілюструє підхід "без помилок", що забезпечує прямий доступ до послуг, де б громадянин не знаходився в Інтернеті.

Втрата публічного контролю над даними також, ймовірно, призводить до того, що організації, підприємства та особи все частіше роблять свої дані (контент та функціональні можливості) доступними у хмарі, а не через портал або навіть веб-сайт. Це означає, що користувачі послуг зможуть створювати свій власний контент та послуги на власних платформах, як правило, через аватари або через автоматичних електронних посередників.

Такий розвиток подій означає, що кібербезпека може стати ще більш актуальною, оскільки навіть, якщо значення мережі знижується, збільшення використання ІКТ на різних каналах робить безпеку як більш важливою загально, так і більш складною для електронного уряду. Гучні атаки на урядові веб-сайти (Білий дім, Пентагон, кібератака на Естонію), в свою чергу, можуть відполохати багатьох користувачів. Це ще більше зменшить довіру до використання електронного уряду та може спонукати користувачів до попиту на повернення до більш традиційних послуг віч-на-віч, які, на їхню думку, є більш безпечними. Може бути досить важко переконати у тому, що ця думка є часто помилковою, не зважаючи на те, що паперові записи набагато легше псуються, губляться або знищуються, а інформація у цьому випадку набагато менш доступна при необхідності.

Те, що електронному уряду вдається добре робити, це надання користувачам даних в якості послуг способами, які раніше були не доступні. І є багато хороших прикладів таких вебсайтів (https://www.fixmystreet.com/

(відремонтуйте мою вулицю) у Великій Британії).

Ще один приклад, також з Великобританії, – це наявність на веб-сайті для обслуговування громадян статистики злочинів на локальних картах. За повідомленням британської газети Guardian, виникали проблеми, яких ніхто не передбачав [1]. По-перше, були побоювання, що ціни на житло в районах з високою злочинністю можуть знизитися, а деякі власники будинків можуть подати позови до відповідного агентства за їх збитки. По-друге, багато даних були помилковими, погано обчисленими, або неправильно розміщеними, почасту даючи абсолютно неправильне уявлення. Масштаб дуже важливий не лише для представлення даних на карті, але навіть для збору даних та визначення місця. Проблеми виникали з приводу того, як збиралися дані, хто робив збір даних, як, та де, вони були зареєстровані. Беззаперечна об'єктивність представлених даних знову виявилася підданою махінаціям з боку далекої від досконалості поведінки людини, яка була посилена через ІКТ. Це також дає зрозуміти, що такі проблеми існували завжди, і однією з переваг оцифрування є те, що інформація стає доступною і прозорою.

Отже, позитивний ефект у вирішенні багатьох питань з даними дають публічно-приватні иа публічно-громадські партнерства. Наприклад, волонтерський сектор та соціальні підприємці, особливо коли вони виступають посередниками між публічним постачальником та відповідним користувачем, можуть додавати низові ресурси, знання, інновації та навіть корисну конкуренцію. Таким чином, уряд стає відкритим та доступним для співпраці шляхом, якого немає в інших секторах, і це може привести до корисних змін поточного способу функціонування публічного сектору та його обов'язків.

Все це загалом приносить багато користі, але є також небезпеки або, принаймні, виклики, які повинні змусити нас зупинитися і замислитися. Коли влада є лише одним із численних гравців у публічній сфері, яка тепер також легітимно складається з суб'єктів приватного та публічного секторів, потрібно знайти нові форми підзвітності. Вона необхідна, коли урядам доводиться обмінюватися даними, владою та відповідальністю, наприклад, через процеси

горизонталізації, детериторіалізації та масштабованості. Горизонталізація дозволяє частково перенести розробку загальнообов'язкових правил від традиційної законодавчої влади до інших регуляторних органів, які можуть не мати демократичної легітимності, таких як незалежні адміністративні органи (наприклад, "парасолькові" організації та "інтерактивні партнери з політики").

Детериторіалізація означає, що численні виклики та проблеми, з якими стикається уряд через кордони (наприклад, торгівля, забруднення, міграція, злочинність), можуть представити національному законодавчому органу факти про події, що вже здійснилися, але над якими він не має безпосереднього контролю. Як для горизонталізації, так і для детериторіалізації, кібербезпека має не тільки впоратись з системами даних та їх розповсюдженням, але й з глобальними загрозами, що все більшають в реальному часі. Мається на увазі не лише технологічна складність, але й політична, організаційна, культурна та поведінкова складність у масових масштабах.

Обмеженість можливостей уряду щодалі помітніше. Складні політичні виклики починаючи від міжнародного рівня до рівнів осіб – у таких різноманітних сферах, як зміна клімату, старіння населення та захворювання – не можуть бути вирішені лише діями уряду. Їх ефективне вирішення вимагатиме узгоджених зусиль усіх суб'єктів суспільства, включаючи окремих громадян. Уряди скрізь знаходяться під тиском, щоб зробити більше з набагато меншими витратами. Більшість наполегливо працюють над тим, щоб забезпечити ефективну політику та послуги принаймні компенсуючи собівартість у публічний гаманець. Багато хто намагається використовувати ресурси поза публічним сектором. І останнє, але не найменш важливе, уряди прагнуть забезпечити та підтримувати високий рівень довіри населення, без якого дії уряду, в кращому випадку, будуть неефективними, або в гіршому випадку – контр-продуктивними. У той же час, більш освічені, добре інформовані та менш покірні громадяни судять свої уряди з точки зору їх демократичності, політики та ефективності надання послуг.

Роль публічного сектора може полягати у збереженні компетенції та

контролю над цими питаннями високого рівня в інтересах суспільства маючи на увазі суспільне благо та суспільну цінність. За такого сценарію захистити публічний сектор від кіберзагроз буде ще важче, оскільки дані будуть розповсюджені. Це також може означати, що насправді захищати дані публічного сектору доведеться суб'єктам приватного сектору. І ще раз: зрозуміло, що основна проблема кібербезпеки не є технічною (яка, проте, важлива та пов'язана з цим), а полягає в необхідності збалансувати кібербезпеку та використання системи в контексті непередбачуваних поведінок і потреб організацій та індивідуумів.

Слід зазначити, що довіра, прозорість та підзвітність – це, мабуть, три найбільші виклики, що стоять перед успішним електронним урядом, і всі вони нерозривно взаємопов'язані. Без довіри до публічного сектору електронний уряд зазнає невдачі. Це загальновизнана істина, що довіру важко отримати і легко зіпсувати, тому вкрай важливо знайти способи повернути цю тенденцію. Довіра зменшує транзакційні витрати, але здорова недовіра заохочує конструктивну критику та обговорення. Уряди можуть сприяти в цьому, досягнувши максимальної прозорості та відкритості, щоб громадяни могли бачити, як приймаються рішення, хто їх приймає та чому. Відповідні можливості для оскарження процесу прийняття рішень також необхідні в рамках чітких правил.

Як зазначає Hansard Society – некомерційна організація у Великобританії, хоча ІКТ може бути дуже важливою для збільшення участі, важливо мати чітку, прозору та засновану на певних правилах відповідальність за всі форми участі, щоб відновити зв'язок між незадоволеними виборцями та політиками [1, с. 22]. Окрім того, ІКТ може підтримувати просування до набагато ширшої прозорості як частини концепції відкритого уряду. Наприклад, дозволяючи користувачам простежувати кожну взаємодію в рамках публічної адміністрації аж до імені публічного службовця, який займається їх запитом у режимі реального часу.

Прозорість системи та даних може дати можливість користувачам та публічним службовцям супроводжувати та відслідковувати запити і справи у

публічному секторі, щоб слідкувати за їх просуванням, знати, яка частина системи зараз несе відповідальність, а також краще передбачати та обходити вузькі місця чи корки. Покладання відповідальності (та прав інтелектуальної власності, коли це є відповідним) може бути вирішальним, особливо щодо користувачів, які за своїм статусом чи станом можуть не мати можливості здійснювати власні права/обов'язки, як от діти, літні люди, інваліди тощо. Це також дозволить користувачам долучитися, бути більш поінформованими та мати більшу можливість контролю задля власної користі.

Як зазначає Європейська ініціатива щодо прозорості (2005 р.), прозорість часто є основою довіри [2]. Прозорість у публічному секторі фактично означає можливість справді "бачити і отримувати те, за що ми платимо" та зробити це видимим для всіх. Також прозорість може заощаджувати час та гроші за рахунок зменшення помилок, об'єднання ресурсів та знань, зменшення дублювання та сприяння співпраці. Прозорість також зменшує корупцію. Важливо підкреслити, що хоча існує постійна потреба у підвищенні довіри користувачів до уряду щодо всіх завдань публічного сектору, урядам також необхідно збільшити свою довіру до користувачів, щоб вони, за підтримки та в рамках чітких рекомендацій, могли брати участь відповідально.

Хоча очевидно, що широке оприлюднення даних публічного сектору може принести величезні переваги, майже напевно існують законні інтереси, які слід захистити від повної прозорості та відкритості. Наприклад, існують, безперечно, законні потреби та інтереси приватності громадян та підприємств, коли їхні дані використовуються урядом. Однак настільки ж важливими є й інтереси публічних службовців та політиків, особливо під час процесу прийняття рішень та політичної діяльності, наприклад, у захисті від настирливого впливу та моніторингу, які можуть стати наслідком того, що всі їх дії та рішення стають абсолютно прозорими. Це може спричинити стрес та надлишкову зосередженість на вимірюванні та виконанні обов'язків на особистому рівні, та призвести до надто бюрократичної позиції, роботи суворо за правилами замість того, щоб бути гнучкими та готовими сприймати

вимірний ризик політичних ідей. Це також може спровокувати небажання приймати рішення або брати на себе відповідальність за них.

Підзвітність випливає як з відповідальності, так і з відкритості та прозорості. Це також пов'язане з етичними міркуваннями, які мають велике значення в суспільній сфері. Існують різні види підзвітності:

1) політична – мають виконувати політики та обрані представники;

2) адміністративна – покладається на публічних службовців, а також на публічний сектор як інститут;

3) підзвітність користувача щодо неправильного користування та зловживання послугами чи можливостями публічного сектору, а також щодо участі законними та відповідальними способами;

4) загальна етична та моральна підзвітність усіх суб'єктів, включаючи громадян, підприємства, громади та публічний сектор.

Підзвітність повинна бути чіткою і простежуваною, щоб, якщо щось пішло не так, було чітко зрозуміло, хто несе відповідальність і як можна вирішити ситуацію. Простота допомагає усім цим питанням, підвищуючи розуміння та усвідомлення демократичного процесу. Однак, на жаль, електронний уряд часто призводить до підвищення складності та масового розмивання між ролями та завданнями, коли задіяно так багато суб'єктів й так багато голосів вимагають, щоб їх почули.

Отже, можна зробити такі висновки.

1. Публічному сектору властива велика ступінь оперативної незалежності та ізольованості між різними його частинами, що робить для нього вирішення питань кібербезпеки надзвичайно складним та, можливо, більш складним, ніж для приватного.

2. Наразі важливі загальнодоступні дані створюються, зберігаються та застосовуються суб'єктами та особами поза урядом, тому визначення безпеки публічного сектора має бути розширене та переосмислене.

3. Поведінка людини є стрижнем кібербезпеки.

4. Існує зворотна залежність між використанням систем і безпекою цих

систем, але ми ще не достатньо знаємо про те, як досягти певної рівноваги.

5. Користувачі електронного уряду потребують такого ж захисту кібербезпеки від уряду, як уряд потребує захисту від третіх сторін, зокрема, коли органи управління некомпетентні або корумповані.

Наслідки цих викликів полягають у тому, що координація та контроль стають все складнішими, а спектр загроз кібербезпеці збільшився в обсязі та масштабах для всіх суб'єктів суспільної сфери. Як показує практика, високий відсоток порушень безпеки відбувається з причин недбалості внутрішніх користувачів або недотримання процедур. Місцеві органи влади, можливо, знаходяться під загрозою навіть більшою мірою, ніж центральні адміністрації через їх відносну нестачу ресурсів та досвіду. Але питання кібезбезпеки для них є найактуальнішими, в зв'язку з чим необхідно організаційно забезпечити відповідний захист, що стосується таких заходів: актуалізація та усвідомлення проблеми; призначення відповідальності; захист основного обладнання, програмного забезпечення та інформації; контроль доступу; забезпечення безпечної утилізації; поліпшення навчання та обізнаності.

Для подолання опору відповідним змінам у роботі службовців може знадобитися поступова зміна образу мислення та поступовість у діях. Однак, як на це вказував зарубіжні автори [3; 4], зараз багато свідчень вказують на переваги створення нейтральних довірених третіх сторін між урядами та постачальниками даних, з одного боку, та громадянами з іншого. Також при цьому є необхідність забезпечення справедливого захисту інтересів та прав усіх зацікавлених сторін. Такі треті сторони можуть бути приватними, громадськими або навіть публічними органами, але вони мають бути юридично та операційно незалежними та сприйматися саме такими. Вони можуть з перевагами виконувати деякі з наступних завдань:

– виступати як "чемпіон" та "сторожовий собака" для користувачів щодо використання даних та участі у політиці та прийнятті рішень, таким чином, виступати як "омбудсмен" для користувачів у відносинах з урядом;

– погодити та оприлюднити громадянську хартію прав та обов'язків

користувачів щодо використання публічних даних та громадської участі, покладаючись на те, що вже є у законі чи нормативно-правових актах, та відкрити це для обговорення користувачами та внесення змін;

– визначити та впровадити рамки для реальної мотивації, стимулювання та винагороди користувачів за залучення до розробки послуг та участі у політиці;

– постійно контролювати потенційні ризики та інформувати користувачів про них, а також пропонувати можливі рішення та допомогу;

– за запитом, та якщо доцільно, забезпечувати як проактивну, так і пасивну модерацію Web 2.0 медіа, а також нейтрально і врівноважено допомагати у проведенні рамкових дебатів;

– відстежувати та підтримувати права користувачів на конфіденційність та захист даних у відносинах з урядом та інших їхніх інтересів;

– забезпечувати, щоб всі публічні послуги ідентифікувались за походженням даних та інших використаних джерел, водночас дотримуючись вимог до відкритого джерела щодо відповідної власності та відповідальності. Це має також включати функції моніторингу та перенаправлення для забезпечення того, щоб будь-яка служба, розроблена для громадського використання, відповідала узгодженим стандартам точності та якості;

– незважаючи на величезні потенційні вигоди від звільнення всіх типів публічних даних, існує небезпека перевантаження даних та нецільового використання даних. Дані, як і статистика, можуть бути серйозно зіпсовані з метою, щоб вони означали будь-що, чого бажає будь-хто. Довірена третя сторона має відстежувати це та надавати нейтральні та прозорі настанови, а також втручатися в такі питання.

Висновки. Таким чином, довіра, прозорість та підзвітність стають найбільшими викликами сьогодення, що стоять перед успішним електронним урядом, і всі вони нерозривно взаємопов’язані. В умовах глобалізації ускладнюються не тільки економічні та публічні відносини, певної специфіки набувають і заходи щодо забезпечення кібербезпеки. Вказані запобіжники

стосовно захисту інтересів та прав важливо встановити для того, щоб уряди або будь-які суб'єкти не маніпулювали неналежним чином іншими суб'єктами. Цьому також сприятиме забезпечення відкритості та прозорості публічних даних та процесів, оскільки це врівноважує владу з усіма суб'єктами та зменшує зловживання та корупцію.

Список використаних джерел

1. Гавловський В. Д. До питання використання соціальних мереж у деструктивних цілях. *Актуальні проблеми управління інформаційною безпекою держави* : зб. матеріалів наук.-практ. конф., (Київ, 24 травня 2017 р.). Київ : Нац. акад. СБУ, 2017. С. 21–23.

2. Куюмджиєва А. Міжнародна практика заходів, спрямованих на зміцнення довіри між державою та організаціями громадянського суспільства. Проект на замовлення Координатора проектів ОБСЄ в Україні. Київ, 2010. URL: www.osce.org/ukraine (дата звернення: 22.11.2019).

3. Andreasson K. Cybersecurity: Public Sector Threats and Responses. CRC Press. Taylor & Francis Group, 2012. 392 p.

4. White House. June 2009. Cyberspace Policy Review: Assuring a Trusted and Resiliant Information and Communications Infrastructure. URL: http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf. (дата звернення: 18.10.2019).

References

1. Gavlovsryi, V.D. (2017). Do pytannia vykorystannia socialnykh merezh u destruktyvnykh tsiliakh [To the question of the use of social networks in destructive purposes]. *Aktualni problemy upravlinnia informatsiinoiu bezpekoiu derzhavy* (24 trav. 2017 r.). Kyiv: Nat. acad. SSU, *21–23* [in Ukrainian].

2. Kuiumdzhyeva, A. (2010). Mizhnarodna praktyka zakhodiv, spriamovanykh na zmitsnennia doviry mizh derzhavoiu ta organizatsiiamy gromadianskogo suspilstva. Proekt na zamovlennia Koordynatora proektiv OBSIe v Ukraini [International practice of the measures directed on strengthening of trust between the state and organizations of civil society. Project on the order of Co-ordinator of projects OSCE in Ukraine]. URL: www.osce.org/ukraine [in Ukrainian].

3. Andreasson, K. (2012). Cybersecurity: Public Sector Threats and Responses. CRC Press. Taylor & Francis Group.

4. White House. June 2009. Cyberspace Policy Review: Assuring a Trusted and Resiliant Information and Communications Infrastructure. URL: http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

Kotukh Ye. V.,
PhD in Technical Sciences, Associate Professor of Cyber Security and Information Technologies Department,
University of Customs Service and Finances, Dnipro
ORCID 0000-0003-4997-620X

Specific Features of Ensuring Cyber Security in Public Sector under Globalization

Under the conditions of globalization, alongside with coordination and integration in the public sector, there exists a growing trend of cooperation with other subjects from the private and public sectors, and individual users. Recently an important area of scientific research has been analysis of the modern tendencies and priority measures for ensuring the cyber security of e-government.

The objective of research is substantiation of organizational issues and areas of providing cyber security in the public sector under globalization.

The paper considers trends and methods of counteracting cyber threats in the public sector. Taking foreign countries' experience as an example, the advantages and drawbacks of e-government and its capacity for counteracting cybercrime have been substantiated. Major political challenges – from international to individual ones – in different spheres cannot be coped with through the actions of the government alone. Coordinated efforts of all the subjects of the society are needed, including those of individuals. Governments are always under pressure, since they try to do more at a lower cost. It has been proved that creation of public-private and public-civil partnerships is to become a more effective response to cyber security challenges under the conditions of globalization. Most often the government becomes open and accessible for cooperation by a way that is not available in other sectors, and this can lead to useful changes in the current mode of public sector operation and its duties.

It has been found that nowadays trust, transparency and accoutability turn out to be the most serious challenges which a successful e-government faces. These issues are imperative for Ukraine in today's context. A list of arrangements and tasks has been drawn, which are expedient to be delegated to neutral intermediaries between the government and its data suppliers, with the aim of protecting the interests and rights of subjects of public-private relations. Providing the openness and transparency of public data and processes balances the authorities with all the subjects, eliminating abuse of power and corruption.

Keywords: public sector; cyber threat; cyber security, globalization; transparency of activity.

Надійшла до редколегії 23.11.2019 р.