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/tp.19.04.05**

ОСОБЛИВОСТІ НАЦІОНАЛЬНОЇ ТА РЕГІОНАЛЬНОЇ ПОЛІТИКИ У СФЕРІ КІБЕРБЕЗПЕКИ

Розглянуто організаційний механізм та способи боротьби з кіберзагрозами. Проаналізовано досвід зарубіжних країн щодо залучення суб'єктів публічно-управлінських відносин до кібербезпеки через різні закони та регламенти дій. Визначено переваги та недоліки електронного уряду та його потенціал у протидії кіберзлочинам. Доведено, що більш ефективною відповіддю національної та регіональної політики на виклики кібербезпеки має стати утворення публічно-приватних партнерств. Саме в такому форматі лідери публічного та приватного секторів, а також громадянське суспільство можуть вживати заходів для посилення співпраці в кіберпросторі задля забезпечення відповідного складника національної безпеки України.
Ключові слова: національна та регіональна політика, кіберзагроза, кібербезпека, електронний уряд, публічно-приватне партнерство.

Постановка проблеми. Глобальні проблеми у сфері кібербезпеки поширюються на регіональні, національні та місцевий рівні. Світ має довгу історію боротьби зі злочинністю та війною в режимі офлайн; схоже, що ми стикаємося з тим самим викликом онлайн. Оскільки публічний сектор має бути готовим реагувати на кібератаки, нагальним питанням стає розроблення практичних заходів для протидії їм.

Аналіз останніх досліджень і публікацій. Питанням кібербезпеки та її ролі в забезпеченні національної безпеки присвячено наукові праці І. Діордіци, Є. Живила, З. Коваль, В. Куцаєва, В. Ліпкана, С. Срібного, В. Ткаченка, В. Шеломенцева та ін. Серед іноземних досліджень хотілося б окремо виділити напрацювання К. Андреассона, Е. Камарка, П. Кеніса, К. Прована та ін. Проте в сучасних умовах реформування виникають нові умови та проблемні сфери, що вимагають удосконалених підходів під час визначення особливостей забезпечення дотримання культури кібербезпеки в органах публічного управління, організаційного забезпечення її дотримання. Одночасно у вітчизняній науковій літературі не вистачає комплексного аналізу особливостей національної та регіональної політики у сфері кібербезпеки з урахуванням специфіки публічного управління.

Мета дослідження. У статті за мету обрано обґрунтування проблем та напрямів забезпечення реалізації національної та регіональної політики у сфері кібербезпеки в публічному секторі в сучасному світі.

Виклад основного матеріалу. Для визначення особливостей формування та реалізації національної та регіональної політики у сфері кібербезпеки, необхідним є розгляд основних сучасних підходіви до вирішення проблеми забезпечення кібербезпеки в публічному секторі.

У науковій літературі наводяться пояснення того, чому кібербезпека є складною з організаційної точки зору. Наприклад, Е. Камарк з Гарвардського університету стверджує, що кібербезпека є такою проблемою, яка не схожа на будь-яку іншу, з якою раніше стикався уряд [3, с. 45].

Зарубіжні країни мають доволі різний досвід залучення до кібербезпеки, різні закони та регламенти дій. Міжнародні та національні інциденти в галузі кібербезпеки часто захоплюють заголовки новин, але опиняються осторонь органи місцевого самоврядування, і саме це є ілюстрацією того, що має існувати цілісний підхід як згори донизу, так і знизу догори. І тут потрібно аналізувати перемоги та провали місцевих урядових установ та їхніх заходів, які врівноважують безпеку за допомогою нової політики уряду. Доцільним є визначення та обговорення ролі, яку може відігравати субнаціональна політика безпеки в рамках глобальної.

Консультанти Civic Resource Group, Грегорі Г. Кертін та Черіті Ц. Тран стверджують: що більше органи місцевого самоврядування намагаються задовольнити всі більші очікування уряду (відкриті дані, прозорість, розширений доступ до інформації та доступність, точки взаємодії з громадянами та зворотного зв'язку від них), то більше вони мають вирішувати проблеми забезпечення безпеки онлайн-інформації [2, с. 112].

Поширена відповідь на виклик кібербезпеки – утворення публічно-приватних партнерств (ДПП). Але вони діють лише в поодиноких випадках. На прикладі основних положень однієї з наукових робіт [2, с. 112–114] визначимо основні напрями, у яких лідери публічного та приватного секторів, а також громадянське суспільство можуть вживати заходів для посилення співпраці в кіберпросторі.

Діяльність уряду – це, власне, усе, що пов'язано з даними, інформацією та знаннями про публічний сектор, що створюються, змінюються, переміщуються та розгортаються для задоволення потреб суспільства. Електронний уряд оцифровує деякі або всі ці процеси та отримані результати, потенційно змінюючи їх шляхами, що не завжди прогнозовані або бажані, як для внутрішніх потреб публічного сектора, так і для користувачів публічними послугами та можливостями. Ці ненавмисні наслідки можуть бути проблематичними. Наприклад, вони можуть спричинити серйозні проблеми для кібербезпеки в частині несанкціонованого доступу або використання даних та інформації публічного сектору. Керівники публічного сектору мають настільки ж усвідомлювати ці ненавмисні наслідки, як й ті, яких вони очікують від запровадження електронного уряду.

Електронний уряд – це дуже гарна річ, і вона має багато зрозумілих та задокументованих переваг. Для прикладу, існує багато доказів того, що наслідком оцифрування внутрішніх офісних процесів може стати суттєва економія витрат уряду завдяки більш ефективним та раціональним процесам, об'єднанню адміністрацій задля обміну та економії ресурсів, кращому дизайну та персоналізації сервісів, а також більш інтелектуальній розробці більш впливової політики на основі доказів. Але електронний уряд має багато чого запропонувати для подолання фінансово-економічної кризи. Зовнішній, що працює з користувачами, офіс електронного урядування, безперечно, надає їм кращі, зручніші послуги, що заощаджують час та доступні 24/7. Оцифровування сприяє прозорості, відкритості та залученості, надає користувачам інструменти для споживання та залучення до розроблення послуг, що більше відповідають їхнім індивідуальним потребам.

Перехід до більш відкритого уряду створив не тільки можливості, але й загрози теж. Часто такі наслідки не беруться до уваги. Наприклад, багато урядів помиляються, намагаючися встановити системи безпеки на занадто

високому рівні для надаваних функціональних можливостей, що призводять до втрати ресурсів, які могло б бути використано під час роботи більш вразливих систем. Було багато невдалих спроб упровадити складну інфраструктуру відкритих ключів та системи цифрового підпису, у той час коли вистачило б простих паролів чи PIN-кодів. Урок полягає в тому, щоб поставитися до безпеки та захисту даних вкрай серйозно і розглядати це як найнагальнішу технічну проблему, але в той же час підходити до цих питань поступово та пропорційно, беручи до уваги, що завжди має бути компроміс між підвищеною безпекою та придатністю до використанням. Підхід, який потрібно застосувати, полягає у побудові безпеки та захисту даних від самого початку будь-якої ініціативи електронного уряду.

Напрям розвитку Інтернету впливає й на електронний уряд з посиленням уваги до парадигми уряду 2.0 (Government 2.0). Ця парадигма значно більше концентрується на боці попиту, на розширенні прав та можливостей користувачів, на залученні їх, а також на вигодах та впливах на вирішення конкретних суспільних проблем, а не просто на наданні онлайн адміністративних послуг.

Цього слід досягати, підтримуючи реальну трансформацію механізмів управління в напрямі від ізольованості та урядоцентричності до більшої орієнтованості на користувачів та їхні потреби. З цією метою протягом останніх 10–15 років було досягнуто величезного прогресу електронного уряду. Протягом цього часу використання інформаційно-комунікаційних технологій у публічному секторі перейшло до стану, коли ІКТ використовуються для об'єднання міністерств, реінжинірінгу процесів, для пропонування багатьох нових послуг громадянам та бізнесу. Електронний уряд став головним пріоритетом для урядів у всьому світі та основним напрямком інвестицій.

Поза сумнівом, найбільшим операційним викликом електронному уряду є кібербезпека, включаючи загрози ідентифікації, конфіденційності та системам даних.

Адекватна конфіденційність та захист даних та довіра до цієї підтримки мають вирішальне значення для отримання переваг від електронного уряду. Якщо вони там, де і мають бути, та добре працюють, вони можуть забезпечити стабільну, передбачувану та таку, що будує довіру, структуру. Насправді вони є ключовими для будь-якої діяльності, що використовує інформаційно-комунікаційні технології (ІКТ) у суспільстві – у публічному чи приватному секторах, тому їх не слід розглядати ізольовано. Але якщо їх немає, це може мати негативний вплив на використання. Людство знає багато про основні загрози кібербезпеці, але набагато менше про те, як їх подолати. Оскільки головним обов'язком уряду є захист своїх громадян, публічний сектор має будувати високоефективні та інтегровані системи захисту від злочинності, шпигунства, тероризму та війни в кіберпросторі.

Але реакція уряду на проблеми кібербезпеки здебільшого відстає від приватного сектору, незважаючи на те, що він, напевне, є більш важливим, доступність даних про зусилля публічного сектору обмежено. Навіть у країнах, що вже далеко просунулись у напрямі електронного урядування, таких як Норвегія, лише меншість публічних адміністрацій пропонували безпечні способи комунікації зі своїми веб-сайтами, незважаючи на багато опитувань, які показують, що побоювання щодо незахищеності даних користувачі сприймають як найбільший стримуючий для них чинник у використанні

е-уряду. Однак також варто відзначити, що реакція на загрози кібербезпеці дуже мінлива. Наприклад, центральні уряди набагато частіше вживають адекватних заходів, ніж місцеві, що, вочевидь, віддзеркалює відповідну чисельність населення та наявні ресурси. Але багато послуг електронного уряду надаються на місцевому чи регіональному рівнях, і кількість інформації, яку надають ці суб'єкти, швидко збільшується. Одним із викликів кібербезпеки в електронному уряді є те, що публічний сектор характеризується великою операційною незалежністю та "ізоляцією" серед різних його частин, що у приватному секторі такою мірою не спостерігається.

Таким чином, безпека в кіберпросторі уряду є першочерговою турботою, і зрозуміло, що нинішні системи, як організаційні, так і технічні, не завжди відповідають цьому виклику. Майбутнє, імовірно, потребуватиме рішень, дуже відмінних від сучасних систем, що орієнтовані на порівняно стабільні, чітко визначені, послідовні конфігурації, контексти та учасників щодо безпеки. Можливо, потрібна нова парадигма, що відрізнятиметься "відповідною" безпекою, за якої ступінь і характер безпеки, пов'язані з будь-яким конкретним типом дії, змінюватимуться з часом, зі зміною обставин та зміною наявної інформації. Імовірно, що в цьому напрямі публічному сектору доведеться стикатися з викликами у п'яти сферах: приватність, довіра, безпека даних, втрата контролю даних та поведінка людини.

Ініціативи з питань кібербезпеки мають брати до уваги наслідки для конфіденційності, які в багатьох випадках можуть значною мірою загрожувати їхній імовірній дієвості. Наприклад, конфіденційність та захист даних потребуватимуть відповідних систем безпеки, адаптованих до мінливих потреб доступу та ідентифікації людей та організацій. Ці системи також мають діяти через національні кордони, що вимагатиме не лише політичних угод, але й сумісних структур та стандартів даних. Безпеку даних також буде покращено шляхом надання користувачам набагато більшого контролю над їхніми власними даними та над їхньою власною (почасту) множинною ідентифікацією, наприклад через довірених третіх сторін. Для сервісів, які можуть працювати через кордон, життєво важливими будуть добре функціонуючі системи ідентифікації та аутентифікації. Гарантія інформації також необхідна за цілісного підходу, що включає управління ризиками, з урахуванням того, що жодна система не може забезпечити цілковиту безпеку. Довгострокове зберігання даних та доступ до них також важливі, враховуючи швидко мінливі технічні формати та очікуване величезне збільшення генерації даних.

Конфіденційність має захищатися, наприклад, шляхом регламентації та міжнародних угод, таких як Європейський закон про захист даних, включаючи відповідних омбудсменів, хранителів даних або довірених третіх осіб. Слід обережно уникати "сповзання місії", коли дані використовуються для цілей, на які не були призначені спочатку, або "гонки донизу" в міжвідомчому чи транскордонному обміні даними шляхом повернення до стандартів самого слабкого члена. Потреби та довіра користувачів повинні будуватися на розумінні реальної поведінки людини під час використання даних, а також на технічних вимогах.

Технічний аспект кібербезпеки може виявитися легкою частиною. Певно, що розуміння та обслуговування того, що деякі називають ірраціональним, – поведінки людини – може бути справжнім викликом для кібербезпеки.

Довіра є критичною проблемою, і вона будується за допомогою мінімізації інформації (тобто з використанням якомога меншої кількості даних, тільки тих, що необхідні для виконання завдання) та інформування користувачів або отримання згоди користувачів під час доступу та оброблення їхніх даних, сприяючи користувачам відстежувати, володіти, або контролювати їхні власні дані. Довіра також будується шляхом належного управління, роз'яснення та мінімізації ризиків втрати або витоку даних. Загальновідомо, що довіру важко побудувати, але її можна дуже швидко та руйнівно знищити одним-єдиним порушенням. Це підкреслює необхідність вважати довіру багатовимірною. Очевидно, що для максимальної вигоди користувачі мають довіряти своєму уряду чи постачальнику послуг, але для урядів стає все більш важливим довіряти користувачам, наприклад, дозволяючи їм розгортати дані публічного сектору та залучаючи їх до розроблення політики та прийняття рішень. Електронний уряд потребуватиме також персоналізованих та контекстно-релевантних інформаційно-комунікаційних технологій, систем управління відносинами з клієнтами (або громадянами) та систем підтримки прийняття рішень та прогнозування на основі інтелектуального управління знаннями та архівування. В електронному управлінні, мабуть, стануть важливими особисті модулі/простори, що чутливі до контексту, розвинені та персоналізовані. Також вони важливі для супроводу, та розвитку обслуговування супроводу.

Хоча багато дискусій щодо кібербезпеки далекі від раціональності, поінформованості чи точності, але також дуже важко бути безпристрасним. З одного боку, існує думка, яку підтримують багато урядів, що, чим більше доступно даних про громадян, тим краще громадянам можна допомогти та захистити їх. Порівняйте це з протилежним поглядом, якого дотримуються багато громадян, страхаючись стану спостереження/нагляду, від якого нема де сховатися. Якщо уряди володіють занадто багатьма даними, це втручається у приватне життя громадян. Більше того, уряди мають поганий послужний список щодо збереження даних, є чимало прикладів, коли уряди зловживали даними, свідомо чи несвідомо. Водночас ті самі громадяни, які занепокоєні поведінкою уряду, охоче надають приватним компаніям (які, як їм добре відомо, займаються лише зароблянням на них грошей), набагато більше особистих даних, ніж вони будь-коли надають урядам. Багато людей також розкидають ще більше своїх особистих та подекуди інтимних подробиць про себе на сайтах соціальних мереж. Можливо, громадяни сприймають уряди настільки великими, монолітними та всепроникними, що будь-яке неналежне використання даних матиме дуже великі наслідки, тоді як приватний сектор чи сайти соціальних мереж настільки порівняно розрізнені та строкаті, що неналежне використання даних не може бути надто важливим. Професіонали знають, що це дуже далеко від того, що насправді відбувається.

Хто є володарем даних – це може бути глибоко філософським питанням, але це є реальне важливим на практиці, коли йдеться про кібербезпеку, оскільки це визначає, хто може (або має) їх захистити. Наприклад, хто є володарем тих даних, що приватні особи чи організації надають урядам, або уряди збирають – вони самі, чи уряд, з моменту, коли він їх отримав? Можливо, важливіше значення має право на використання даних незалежно від володіння, особливо якщо вони мають економічну або іншу цінність. Наприклад, у Великобританії більшість публічних установ відкривають інформацію PSI

у машиночитабельному та легкодоступному форматах для безкоштовного користування будь-ким. Основним аргументом є те, що тим самим створюється ще більша економічна цінність для суспільства в цілому, коли підприємці всіх типів можуть розробляти нові офлайн-продукти (наприклад, бізнес-послуги щодо економічних даних), а також нові онлайн-смарт-сервіси (або "додатки"), до яких, на власний розсуд підприємців, може надаватися вільний доступ. Звільнення даних у такий спосіб є частиною зростаючого руху "за відкритий уряд", ініціатива прозорості та підзвітності, хоча цей рух поки що став вагомим лише у кількох країнах.

Існує думка, що безпеку даних буде покращено шляхом надання користувачам набагато більшого контролю над їхніми власними даними та над їхньою власною (почасту) множинною ідентифікацією, оскільки так вони будуть безпосередньо зацікавлені в забезпеченні безпеки та точності таких даних. Наприклад, в Естонії ще у 2003 р. було прийнято Закон про захист персональних даних. На запит фізична особа має законне право на доступ до всіх персональних даних, що стосуються її, – цілей, призначення цих даних, їхніх категорій та джерел, а також третіх осіб чи категорій, яким передачу цих даних дозволено. Також особа має подальше право вимагати припинення обробляння своїх персональних даних, виправлення у випадку помилок, та блокування чи видалення їхніх даних через Інспекцію захисту даних або суди. Проте дуже мало країн мають настільки ж добре розвинене забезпечення власності та прав на дані, як Естонія, і це, ймовірно, дає уявлення про відхилення підходу урядів до упровадження кібербезпеки від ставлення громадян до цього питання.

Вже з'являються дуже корисні приклади аутсорсингу, коли кібербезпека, як виглядає, не була під загрозою, але сам факт поширення даних, уже не під прямим контролем уряду, та їхнього розповсюдження збільшує ризики. Вони виникають за обставин технічної несумісності та через почасту різні організаційні та робочі культури і наміри залучених учасників, коли стає все складніше забезпечувати загальний контроль та контролювати стандарти.

Упровадження електронного уряду передбачає необхідність повністю переробити як організаційні структури (по суті, зламати ізольованість), так і архітектуру даних, щоб забезпечити обмін послугами та ресурсами всередені публічних адміністрацій та між ними [1]. Це все частіше відбувається в центрах спільного обслуговування, структурних частин, інформації та даних електронного уряду, а також загальних бізнес-процесів. Це також може сприяти аутсорсингу до інших суб'єктів, у тому числі поза публічним сектором, якщо витрати можуть бути скорочені. Проте основна критика полягає в тому, що у довгостроковій перспективі витрати можуть бути й не зекономлені, якість може зменшитися, і поза сумнівом, це призводить до втрати контролю з боку урядів, які, в решті решт, є демократично відповідальними на відміну від приватних підрядників.

Висновки з цього дослідження і перспективи подальших розвідок у цьому напрямі. Для України важливою відправною токою є визначення золотої середини між контролем, відкритістю та безпекою. Зрозуміло, що відбуваються значні збої. Тому створення технічної стійкості щодо кібератаки та забезпечення швидкого відновлення життєво важливих функцій є ключовими з технічного боку. Проте головне відоме-невідоме кібербезпеки виявляється важливішим, ніж суто технічне питання, – це поведінка людини. Більшість

приймає, що безпека ніколи не може бути ідеальною, але причини цього мають бути вивчені більш уважно, а надто, коли також стає зрозумілим, що між використанням систем та безпекою цих систем існує зворотна залежність.

Поведінка людини, раціональна чи ні, є стрижнем кібербезпеки – що люди думають про свою ідентифікацію, про дані своєї ідентифікації, хто володіє ними, має до них доступ та як їх використовує. Врахування вказаних аспектів має лягти в основі утворення публічно-приватних партнерств та бути спрямованим на підвищення ефективності національної та регіональної політики у відповіді на виклики кібербезпеки. Слід наголосити, що головним викликом є краще розуміння співвідношення ризиків, що пов'язані з кібернебезпекою, та переваг використання системи, але ми ще недостатньо знаємо про те, як досягти певної рівноваги. Зокрема, це стосується публічного сектору (порівняно з приватним), де неможливо або небажано застосовувати ринкові рішення, щоб знайти баланс. Натомість її потрібно досліджувати шляхом спроб та помилок, збирання доказів, а також свідомим застосуванням етичних та демократичних принципів.

Список використаних джерел

1. Прудкий В. В., Сидорчук В. В., Лободзинська Т. П. Інновації в IT-менеджменті: допуски та обмеження в процесі впровадження електронного уряду в Україні. *Економічний вісник НТУУ "КПІ"*. URL: http://doi.org/10.20535/2307-5651.15.2018.135689.

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

3. Kamarck E., Nye J. Vision of Governance in the 21st Century (Program) Governance.com: democracy in the information age. Brookings Institution Press, 2002. 192 p.

References

1. Prudkui, V.V., Sydorchuk, V.V., Lobodzynska, T.P. Innovacii v IT-menedzhmenti: dopusky ta obmezhennia v procesi vprovadzhennia elektronnogo uriadu v Ukraini [Innovation in IT-management: admittances and limitations in the process of introduction of electronic government in Ukraine]. *Ekonomichnyi visnyk NTU "KPI"*. URL: http://doi.org/10.20535/2307-5651.15.2018.135689 [in Ukrainian].

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

3. Kamarck, E., Nye, J. (2002). Vision of Governance in the 21st Century (Program) Governance.com: democracy in the information age. Brookings Institution Press.

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

SPECIFIC FEATURES OF NATIONAL AND REGIONAL POLICIES IN CYBER SECURITY

The world has a long history of counteracting crime, on-line wars and challenges. Since the public sector has to be ready to respond to cyberattacks, elaboration of practical counteraction measures becomes an urgent task.

The paper considers an organizational mechanism and ways to counteract cyber threats. The international practices of getting public-administrative subjects involved in cyber security activities through a variety of legal acts and operating procedures have been analyzed. The above-mentioned measures are quite varied, which is stipulated by the extent of open access to public information, e-government sophistication, cybercrime incidence, previous experience of fighting cyber threats, as well as public opinion and public involvement.

Information and knowledge about the public sector are created, changed, transferred and expanded to meet the social needs. E-government digitizes certain processes and results, changing

them potentially in the ways which are not always predictable or appropriate for either the internal needs of the public sector or public service consumers. Thus, the consequences may be precarious. Therefore, it is expedient to identify the advantages and flaws of e-government and its capacity for counteracting cybercrime in each specific country.

It has been proved that creation of public-private partnerships can become a more effective response of the national and regional policies to cyber security challenges. It is in this format that measures for enhancement of cyberspace cooperation can be used in order to provide a proper component of the national security of Ukraine.

For Ukraine, finding the middle ground among control, openness and security is topical. Under these conditions, both the technicality of the issue and human behaviour should be given an increased attention to. Consideration of the said aspects should lay the basis for creation of public-private partnerships and raise the effectiveness of the national and regional policies in their response to cyber security challenges. It is also important to fully understand the ratio between the cyberthreat-related risks and benefits of using the system chosen to counteract them.

Key words: national and regional policies, cyber threat, cyber security, e-government, public-private partnership.

Надійшла до редколегії 20.11.2019 р.