ДЕРЖАВНО-ПРИВАТНЕ ПАРТНЕРСТВО В КІБЕРБЕЗПЕКОВІЙ СФЕРІ: ДОСВІД РЕСПУБЛІКИ ПОЛЬЩА

Наразі кібербезпека (як і національна безпека в цілому) є однією з функцій держави, яка спрямовує зусилля на підтримання громадського порядку та захист національної безпеки (включно з кіберпростором).

Відтак, конкуренція у безпекових сферах діяльності є досить незначною (за винятком участі компаній у державних закупівлях). Така тенденція досі була більшою мірою притаманна ЄС і меншою – США та «просунутим» країнам Азії. Разом з тим, сферу кібербезпеки важко відокремити від сфери кібервійн, яка поки що залишається доменом держави.

Автори колективної монографії Інституту Косцюшка «Безпека через інновації. Сектор кіберпростору як рушій економічного зростання» («*Security through Innovation. The Cyber Security Sector as a Driver of Economic Growth*») пропонують вважати вкладення в кібербезпеку найвигіднішими з економічного погляду.

За їх даними глобальні втрати від нехтування питаннями кібербезпеки, станом 2017 р. становлять близько $ 3 трильйонів. Водночас, глобальний ринок кібербезпеки, на їх думку, склав в 2016 р. $ 120 млрд, а до 2021 р. має подвоїтися й складе $ 240 млрд. Оскільки найбільш активним рушієм кібербезпеки в сфері оборони й надання цивільних послуг є держава, то в загальнонаціональному масштабі неможливо розв'язати питання кібербезпеки без налагодження ефективного державно-приватного партнерства (далі – ДПП[1]). Інвестиції, реалізовані в рамках ДПП, є, на думку аналітиків Інституту Косцюшка, на 15-17 % дешевшими (ефективнішими). Такий висновок вони підкріплюють прикладом Великобританії, Ізраїлю й Сінгапуру, які впродовж останніх 5-ти років

[1] Також в тексті може згадуватись як PPP – Public-Private Partnership

активно нарощують вкладення в сектор кібербезпеки, використовуючи передусім механізми ДПП.

За оцінкою відомої компанії The Gartner, видатки на цілі кібербезпеки вже через 10 років складатимуть до третини всіх інвестицій «передових компаній»[2]. Враховуючи, що ДПП істотно здешевлює ці видатки і що сама природа кіберпростору побудована на засадах «мультистейкхолдеризму» («*multistakeholderism*»), як державні установи так і приватні компанії просто «приречені» на розвиток ДПП.

Для Польщі питання забезпечення кібербезпеки також стає надзвичайно актуальним, зважаючи на те, що польський сектор ІСТ сягнув в 2016 р. економічного ефекту в $8,5 млрд. Щороку польські університети випускають біля 30 000 фахівців з ІТ. За даними цілої низки авторитетних міжнародних організацій, Республіці Польщі (далі – РП) належать передові позиції в сфері кібербезпекового розвитку[3].

Однак польський вимір ДПП в сфері кібербезпеки все ще знаходиться в стані становлення. Як вказують польські аналітики, від 2009 р. до грудня 2016 р. в рамках ДПП в Польщі було укладено 112 договорів на загальну суму брутто 5,6 млрд злотих (PLN). На жаль, серед цих договорів не було жодного, який би стосувався кібербезпеки державного сектору. Щоправда, 34 % угод стосувалися впровадження широкосмугового Інтернету й, напевно, передбачали розв'язання питань кібербезпеки[4].

---

[2] Special Report: Cybersecurity at the Speed of Digital Business - https://www.gartner.com/doc/3426427?srcId=1-3132930191&cm_sp=gi-_-cysec-_-srpage

[3] Gartner, Forecast Analysis: Information Security, Worldwide, 1Q16 Update, 2016, - www.gartner.com/doc/3357452; Visiongain, Cyber Security Market Report 2016-2021, 2016, - https://www.visiongain.com/Report/1583/Cyber-Security-MarketReport-2016-2021; Cybersecurity Ventures, Cybersecurity Market Report Q1 2017, http://cybersecurityventures.com/cybersecurity-market-report/; Markets and Markets, Cyber Security Market by Solutions (IAM, Encryption, DLP, UTM, Antivirus/ Antimalware, Firewall, IDS/IPS, Disaster Recovery), Services, Security Type, Deployment Mode, Organization Size, Vertical & Region – Global Forecast to 2021, 2016, www. marketsandmarkets.com/PressReleases/cyber-security.asp (access: 12/05/2017).

[4] Wiesław Goździewicz, Cyprian Gutkowski, Lior Tabansky, Robert Siudak. Bezpieczeństwo poprzez innowacje. Sektor cyberbezpieczeństwa jako siła napędowa wzrostu gospodarczego. Instytut Kościuszki 2017. – http://www.ik.org.pl/wp-content/themes/ik/report-img/bezpieczenstwo-poprzez-innowacje.pdf

1. Концептуальні підходи до ДПП в Польщі

ДПП часто трактується в Польщі як співпраця між органами державного управління й органами місцевого самоврядування (польською – «*administracji rządowe*»; «*administracji samorządowe*»; «*administracji publiczne*») й приватними організаціями у сфері надання публічних послуг. Принципово важливим для адекватного розуміння ДПП є функціональне в РП поняття «суспільних благ» («*dobra publiczne*»; «*the general welfare*»)[5], яке поки що не увійшло належним чином в український громадсько-політичний та інституційно-правовий обіг, а тому може бути вельми неточно перекладене як «громадські товари» або «товари народного споживання».

У випадку «суспільних благ» йдеться про найрізноманітніші товари (речі, послуги тощо), які неможливо виключити зі споживання пересічного громадянина і які водночас не є в споживанні конкурентоспроможними, тобто ринковими, призначеними для персонального збагачення тощо.

Існує дві необхідні й достатні передумови адекватного розуміння «суспільного блага».

Перша полягає у тому, що хороший постачальник відповідних благ не може юридично перешкоджати постачанню й використанню такого блага іншими постачальниками.

Друга умова полягає в тому, що споживання «суспільного блага» однією людиною не виключає можливості й іншим людям споживати те ж саме благо. Саме тому без будь-яких негативних наслідків чимало людей можуть водночас споживати одне й те ж саме «суспільне благо».

У недемократичному суспільстві «суспільні блага» є контрольовані державою. З відповідної сфери життя зазвичай видаляють недержавних суб’єктів, що унеможливлює ДПП (в більшості випадків - в принципі або ставить ДПП в певні рамки штучних обмежень). У демократичному ж суспільстві «суспільні блага» є результатом спільної дії громадян, волю

[5] Dobra publiczne // Wikipedia - https://pl.wikipedia.org/wiki/Dobra_publiczne. -

яких виражають вибрані ними державні органи та органи місцевого самоврядування. Одні й ті ж самі послуги (наприклад, шкільництво й освіта або охорона здоров'я) можуть бути віднесені демократичним соціумом до публічної або приватної сфери, або ж до тієї й іншої водночас, залежно від волі й особистого вибору громадян.

Одним зі способів отримання «суспільних благ» є публічна (державна) послуга («*usługi publiczne*»; «*public service*»)[6], яка в жодному разі не може бути зведеною до публічної (державної) монополії[7]. Тобто такі послуги держава може надавати не тільки безпосередньо, але й опосередковано, звертаючись до приватних структур й фінансуючи від імені суспільства подібну діяльність з бюджетних засобів.

В сучасних державах демократичного типу особливого поширення надання публічних послуг набуло в таких сферах як: телекомунікації та поширення «ефірного» радіотелевізійного сигналу; освіта та шкільництво; соціальна опіка (особливо для дітей, людей з вадами розвитку, похилого віку тощо); охорона довкілля; охорона здоров'я та санітарія; господарювання відходами та підтримання чистоти й порядку; поліційна справа; пожежна справа; військова справа; енергопостачання (електроенергетика, газифікація, тепломережі тощо); міський транспорт; будівництво соціального житла; просторове планування та міська архітектура; водне господарювання (водопостачання та каналізація); збереження та архівація публічної інформації (наприклад в «паперових» або електронних бібліотеках)[8].

Таким чином предметом ДПП є надання «суспільних благ». Польський Інститут публічно-приватного партнерства виокремлює наступні визначальні ознаки ДПП:

---

[6] Usługi publiczne // Wikipedia https://pl.wikipedia.org/wiki/Us%C5%82ugi_publiczne
[7] Cesar A. Guimarães Pereira, Public-Private Partnerships (PPPs) and Concessions of Public Services in Brazil - www.bricslawjournal.com/jour/article/download/4/5
[8] Usługi publiczne.

- співпраця публічного (державного) сектору з сектором приватним;
- цивільно-правовий характер подібної співпраці;
- конкретна мета подібної співпраці: побудова інфраструктурних об'єктів, надання певних послуг, що традиційно виконувалося публічним (державним) сектором;
- оптимальний поділ завдань між обома секторами;
- поділ ризиків між обома секторами;
- взаємна користь[9].

Окремі дослідники виокремлюють також наступні форми ДПП[10]:

1. **Спільне підприємство** (*Joint Venture*) - спільне використання ресурсів та поділ ризиків між урядом та приватним сектором включно з використанням спеціальних інструментальних засобів (*Special Purpose Vehicle, SPV*).

2. **Сервісний договір** (*Service Contract*): уряд наймає з метою надання певних послуг приватну компанію на певний період (зазвичай 1-3 роки).

3. **Управлінський договір** (*Management Contract*): «фундаментальні» видатки бере на себе уряд, приватна компанія забезпечує оборотний капітал для реалізації проекту.

4. **Договір оренди** (*Lease contract***)** - приватний сектор бере на себе повністю реалізацію контракту терміном до 10-20 років включно з фінансуванням, експлуатацією, управлінням якістю та ризиками.

5. **Концесії** (*Concessions*) – концесіонер (приватна компанія) - підприємство повного обслуговування контракту включно з капітальними вкладеннями, експлуатацією, управлінням та обслуговуванням. Зазвичай

---

[9] Partnerstwo Publiczno-Prywatne (PPP) // Instytut Partnerstwa Publiczno-Prywatnego. - www.paih.gov.pl/files/?id_plik=16912

[10] Surya Kiran Sharma. Public-Private-Partnership in Cyber Security // Centre for Land Warfare Studies (CLAWS) - http://www.claws.in/1278/public-private-partnership-in-cyber-security-surya-kiran-sharma.html

діє схема: «побудова об’єкту – його експлуатація – передача його державі» (*Build-Operate-Transfer, BOT*), хоча можливі варіації.

Дискусії довкола сутності ДПП стосуються передусім можливості його ототожнення/розрізнення з «концесійною діяльністю» (концесіями). Тут зустрічаються дві крайніх позиції: ототожнення цих форм взаємодії державного (публічного) й приватного партнерів та їх строге розрізнення.

Найоптимальнішим уявляється погляд, відповідно до якого ДПП – більше широке поняття, а концесія – лише один з різновидів ДПП, який стосується переважно реалізації інфраструктурних об’єктів за кошти приватного інвестора з наступною їх передачею державному (публічному) власнику на засадах вищенаведеного принципу «Build-Operate-Transfer (BOT)».

Довідково:

Зазвичай співпраця на засадах ДПП має довготерміновий характер у зв’язку з низькою окупністю проектів у короткотривалій перспективі, з одного боку, й необхідністю надання гарантій якісної послуги, з іншого. У РП такі контракти укладають зазвичай в межах 30-70 років. Власне будь-який проект, який обіцяє приватнику повернення вкладених в нього коштів може бути реалізований на засадах ДПП.

У країнах ЄС ДПП розповсюджене нерівномірно. Найбільш інтенсивно дана форма співпраці держави (місцевого самоврядування) з приватним сектором розвивалася в Великобританії, Іспанії й Португалії. У Великобританії, зокрема, проекти, реалізовані на засадах ДПП, становлять 15 % від усіх інвестицій в державний сектор.

У Великобританії впродовж останнього десятиліття на засадах «формули ДПП» побудовано понад 800 нових шкіл; 44 лікарень (після 1997 року); 13 тюрем (де міститься біля 10 % ув’язнених); дороги; залізниці; відтинки лондонського метра; чимало урядових будівель (серед них – будівлі Амбасади Великобританії в Берліні та Міністерства фінансів в Лондоні). До цього переліку слід додати чисельні проекти, які стосуються охорони довкілля, господарювання відходами та громадського транспорту.

Концесійні контракти з кінця 60-х років успішно реалізовуються в Іспанії, Франції та Італії. ДПП здобуває популярність в Німеччині.

Активно випробовують модель ДПП на рівні місцевого самоврядування в східних країнах ЄС: Чехії, Словаччині, Румунії, Угорщині, Польщі.

Зокрема, польські дослідження вказують на те, що зацікавленість у даній моделі співпраці з приватним сектором найнижча «нагорі» (на рівні центральних органів державної влади) й зростає мірою руху «вниз» - до владних органів воєводств, повітів та гмін. Найвищою була подібна активність на рівні міст на правах повітів[11].

[11] Raport o partnerstwie publiczno-prywatnym w Polsce. Praca zbiorowa pod redakcją prof. dr hab. Jerzego Hausnera. Autorzy: dr Irena Herbst. dr Aleksandra Jadach-Sepioło. Tomasz Korczyński. Współpraca: Tomasz

2. **Правове регулювання державно-приватного партнерства в Республіці Польща**

У РП «постсоціалістичного періоду» правове регулювання ДПП тривалий час було відсутнє й лише у 2008-2009 рр. набули чинності два принципово важливих закони, які врегулювали ДПП й концесійну діяльність[12]

Польський закон, що врегулював ДПП, ухвалений наприкінці лютого 2009 р. згодом зазнав змін із врахуванням спільноєвропейської практики заохочення ДПП (в тому числі - за рахунок можливостей використання відповідних спільноєвропейських фондів; ресурсів ЄБРР тощо).

Істотно важливим в РП було визначено створення нових інституцій та інструментів. спроможних позитивно впливати на пришвидшення ринку ДПП. В рекомендаціях польського Центру ДПП йшлося зокрема про:

- створення при Міністерстві економіки (*Ministerstwo Gospodarki*) центрального органу, відповідального за організацію та імплементацію в РП ДПП, координацію в цьому напрямі діяльності інших урядових установ;
- впровадження посади Уповноваженого уряду у справі ДПП (*pełnomocnika rządu do spraw PPP*).

До найважливіших завдань подібних інституцій віднесено:

- ***програмні:*** включно із напрацюванням стратегії використання формули ДПП (PPP) для реалізації урядової соціально-економічної політики й стратегії імплементації формули ДПП у практику надання публічних послуг;

Jagusztyn-Krynicki. Bartosz Mysiorski. Przemysław Zaremba. Warszawa, lipiec 2013 (Publikacja sfinansowana z grantu Fundacji S. Batorego przyznanego na realizację projektu upowszechniania PPP w Polsce).

[12] Ustawa z dnia 19 grudnia 2008 r. o partnerstwie publiczno-prywatnym (Dz. U. z 2009 r. Nr 19, poz. 100 z późn. zm.); Ustawą o PPP.

·Ustawa z dnia 9 stycznia 2009 r. o koncesji na roboty budowlane lub usługi (Dz. U. z 2009 r. Nr 19, poz. 101, Nr 157 poz. 1241 z późn. zm.); Ustawą o Koncesjach.

- ***координаційні:*** забезпечення погодженої діяльності державних органів, відповідальних за ДПП;
- ***моніторингові:*** ідентифікація кількості й структури підприємницької активності на засадах ДПП;
- ***аналітичні:*** оцінка впливу правових та інституційних регулятивів на перебіг реалізації ДПП, а також цінність та ефективність проектів у контексті завдань урядової стратегії;
- ***організаційно-юридичні:*** підготовка необхідних правничо-інституційних коректив та подача пропозицій щодо їх прийняття.

26 липня 2017 р. Рада міністрів Республіки Польща ухвалила важливий документ «Політика Уряду у сфері розвитку публічно-приватного партнерства» («*Polityka PPP*»)[13]. У цьому документі перспективи розвитку ДПП подаються з позицій аналітичних оцінок конкретних можливостей польського ринку. Даний документ доповнює й конкретизує більш широкий документ – «Стратегію задля відповідального розвитку»[14] й увійшов до т.зв. «пакету Моравєцького» (Матеуш Моравецький, який згодом очолив польський уряд, на той час був міністром інвестицій та розвитку РП).[15]

У загальнопольському масштабі в умовах максимальної інформаційної прозорості політику ДПП координує Міністерство інвестицій та розвитку (*Ministerstwa Inwestycji i Rozwoju*). Зокрема таку активність легко відстежувати через один з порталів даного міністерства, присвячений поточним питанням ДПП[16].

---

[13] Politykę Rządu w zakresie rozwoju partnerstwa publiczno-prywatnego". - https://www.ppp.gov.pl/Aktualnosci/Documents/POLITYKA_PPP_0717.pdf

[14] Strategia na rzecz Odpowiedzialnego Rozwoju - https://www.mr.gov.pl/media/36848/SOR_2017_maly_internet_03_2017_aa.pdf

[15] SOR: administracja będzie zorientowana na usługi cyfrowe - https://www.onet.pl/?utm_source=biznes_viasg&utm_medium=nitro&utm_campaign=allonet_nitro_new&srcc=ust

[16] https://www.ppp.gov.pl

3. **Питання публічно-приватного партнерства в стратегічних документах та діяльності CERTs Республіки Польща**

У 2015 році організація, яка репрезентує інтереси найбільших «софтверних» компаній світу BSA - Software Alliance (штаб-квартина – у Вашингтоні) проаналізувала стан кібербезпеки у всіх 28 країнах-членах ЄС й розробила відповідні рекомендації європейського представництва міжнародної організації[17].

Оцінювання провадилося за 25 критеріями, згрупованими довкола п’яти засадничих тематик:

- правових підстав функціонування кіберпростору;
- організаційних інституцій та механізмів;
- публічно-приватного партнерства;
- секторальної кібербезпеки;
- кібербезпекового просвітництва.

Лідерами у сфері кібербезпекової ДПП BSA - Software Alliance визнано п’ять країн ЄС: Австрію, Німеччину, Нідерланди. Іспанію й Великобританію. Щодо інших країн ЄС, то стан кібербезпекової ДПП в них визнано «або неіснуючим, або вельми обмеженим, або на найнижчому щаблі розвитку».

РП за всіма запропонованими критеріями посіла позицію «твердого середняка» й, згідно запропонованої доповіді BSA - Software Alliance, «мала комплексну стратегію з чітко сформульованими цілями». Йшлося про такий документ як «Політика захисту кіберпростору Республіки Польща» від 25 червня 2013 року[18], ухвалений Постійним комітетом Ради міністрів РП (*Komitet Stały Rady Ministrów*).

---

[17] http://www.bsa.org/about-bsa. На момент опублікування даної доповіді BSA - Software Alliance серед 28-и тодішніх членів ЄС лише 19 розробили стратегії кібербезпеки. Відповідних стратегій на то й момент не розробили: Болгарія; Хорватія; Данія; Греція; Ірландія; Мальта; Словенія; Швеція.
У Португалії така стратегія перебувала в стадії розроблення. Найпізніше (у 2014 р.) такі стратегії розробили Литва, Естонія й Італія, а раніше всіх (у 2008 р.) – Словаччина.

[18] Polityka ochrony cyberprzestrzeni Rzeczypospolitej Polskiej. https://www.cert.gov.pl/cer/publikacje/polityka-ochrony-cyber/639,Polityka-Ochrony-Cyberprzestrzeni-Rzeczypospolitej-Polskiej.html

Більш критично поставилися до зазначеного документу польські контролери з «Найвищої контрольної палати»[19], які зауважили що даний документ є «результатом поганого компромісу», а тому не є дієздатним, позбавлений належної конкретики тощо. У документові навіть було виявлено «істотні помилки» (*błędy merytoryczne*).

На момент опублікування вищевказаної доповіді BSA - Software Alliance, РП мала декілька «комп'ютерних груп з реагування на надзвичайні ситуації – CERTs» включно з CERT.GOV.PL, який забезпечував безпеку всієї урядової та критичної інфраструктури[20].

Метою **CERT.GOV.PL** є забезпечення та розвиток потенціалу організаційних підрозділів державного управління РП для захисту від кіберзагроз, з особливим акцентом на напади, орієнтовані на критичну інфраструктуру. CERT.GOV.PL функціонує відповідно до приписів «Програми охорони державного кіберпростору Республіки Польща на 2009 - 2011 роки (*RPOC*)[21], ухваленої 9 березня 2009 року Постійним комітетом Ради міністрів РП.

CERT Polska[22] діє від 1996 р. (до кінця 2000 р. діяв під назвою CERT NASK). Від 1997 р. CERT Polska є членом FIRST (*Forum of Incidents Response and Security Teams*), співпрацюючи в рамках цієї організації з подібними структурами по всьому світі.

До головних завдань CERT Polska належать:

- запис та обробка подій, які порушують безпеку мережі;
- повідомлення користувачів про настання загроз й активна відповідь у разі безпосередньої загрози користувачам;
- співпраця з іншими командами IRT (*Incidents Response Team*), які діють в рамках FIRST;

[19] Realizacja przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni RP, Informacja o wynikach kontroli, KPB 4101–002–00/2014 – nr ewid. 42/2015/P/14/043/KPB, Departament Porządku i Bezpieczeństwa Wewnętrznego, Najwyższa Izba Kontroli, Warszawa 2015, s. 12.
[20] Michał Młotek. Marcin Siedlarz. Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL
[21] Rządowy Program Ochrony Cyberprzestrzeni RP na lata 2009 - 2011 (RPOC).
[22] https://www.cert.pl/

- участь у національних та міжнародних проектах, пов'язаних з тематикою інформаційної безпеки;
- науково-дослідна діяльність щодо методів виявлення інцидентів безпеки;
- аналіз шкідницького програмного забезпечення та системи обміну інформацією про загрозу;
- розробка власних інструментів для виявлення, моніторингу, аналізу та співвіднесення загроз;
- регулярна публікація звіту CERT Polska про безпеку інтернет-ресурсів Польщі;
- інформаційно-просвітницькі заходи, спрямовані на підвищення обізнаності в галузі інформаційної безпеки, в тому числі через:
- публікацію інформації про безпеку в блозі cert.pl та у соціальних мережах Facebook і Twitter;
- організація конференцій SECURE[23];
- незалежні аналізи та тести рішень в сфері IT-безпеки.

Серед проектів, які впродовж останнього періоду успішно реалізує NASK слід виокремити[24]:

- **ARAKIS-GOV** - система раннього попередження про Інтернет-загрози, яка є результатом співпраці Департаменту телеінформаційної безпеки Агенції внутрішньої безпеки та команди CERT Polska, що діє в рамках NASK. ARAIKIS-GOV був початково створений для підтримки й захисту ресурсів ІКТ державних адміністрацій, але завдяки співпраці з CERT Polska набуде додаткової функціональності.
- **ACADEMICA** – проект оцифрування бібліотечних фондів, який реалізує Національна бібліотека та NASK, заснований під егідою Фонду польської науки (*Fundacja na Rzecz Nauki Polskiej*) й який фінансується з

[23] https://www.secure.edu.pl/pl/site.html. SECURE 2018 - 22. KONFERENCJA NA TEMAT BEZPIECZEŃSTWA TELEINFORMATYCZNEGO

[24] PROJEKTY STRATEGICZNE - https://www.nask.pl/pl/dzialalnosc/projekty-strategiczne/145,Projekty-strategiczne.html

«Операційної програми інноваційної економіки (*Programa Operacyjna Innowacyjna Gospodarka, Działanie*).

«Безпечний Інтернет» - реалізується Польським програмним центром безпечного Інтернету (*PCPSI*) спочатку в рамках програми ЄС «Безпечний Інтернет» (2005-2014 рр.), а надалі в рамках програми ЄС «Connecting Europe Facility» (*CEF*). Метою проекту є підвищення обізнаності громадськості щодо загроз, які виникають внаслідок використання Інтернет-комунікацій. Серед заходів пріоритетом є боротьба з незаконним і шкідливим вмістом Мережі.

Важливим кроком уперед в справі налагодження ДПП між Міністерством оцифрування й польським бізнесом стала офіційна «інавгурація» 5 липня 2016 р. створеного на базі CERT NASK Національного центру кібербезпеки (*Narodowe Centrum Cyberbezpieczeństwa - NCC*). Для цього було укладено відповідну угоду між Міністерством оцифрування та Спілкою польських банків (*Związek Banków Polskich*). До списку підписантів угоди увійшли: Citi Handlowy, Credit Agricole, mBank, PKO BP, Raiffeisen Polbank, BZW BK, Orange, T-Mobile, Polkomtel, Energa, PSE S.A., Gas-System S.A., PERN S.A. й PKP Informatyka.

В організації Національного центру кібербезпеки польські медіа відповідного фахового спрямування підкреслюють персональну заслугу помічника міністра оцифрування з питань кібербезпеки, генерала Влодзимєжа Новака (*Gen. Włodzimierz Nowak*)[25].

Ідея Національного центру кібербезпеки полягає передусім у цілодобовому стеженні за кіберзагрозами й кібервикликами, які приходять звідусіль до кордонів польської Мережі або виникають всередині даної Мережі. В.Новак навіть висловлювався неодноразово на користь організації національних вхідних «екранів» типу firewalls.

[25] NCC - na straży cyberbezpieczeństwa - https://www.gov.pl/cyfryzacja/ncc-na-strazy-cyberbezpieczenstwa

Окрім «Політики захисту кіберпростору Республіки Польща», питання ДПП в кібербезпековій сфері обговорюються передусім в наступних документах РП:

- Доктрині кібербезпеки РП 2015 р.[26];
- Стратегії кібербезпеки РП на 2017-2022 рр.[27].

Доктрина кібербезпеки РП 2015 р. пропонує у четвертому розділі – («Концепція підготовчих завдань у сфері кібербезпеки (підтримання та розвиток кібербезпекової сфери Польської Республіки)» підрозділ з ДПП (4.3.), де такі зусилля мають бути вжиті для того щоб[28]:

- створити умови, що сприяють впливу приватних підприємств і громадян за публічні дії у сфері кібербезпеки. що має забезпечити синергію державно-приватного партнерства у сфері кібербезпеки РП;
- забезпечити відповідні механізми співробітництва та партнерства між державним та приватним секторами галузі кібербезпеки.

При цьому наголошується на особливій увазі до кібербезпеки держави, для чого пропонується використовувати:

- публічно-приватний діалог у сфері підготовки законопроектів, які сприятимуть створенню ефективних правил та процедур діяльності у сфері кібербезпеки;
- угоди у сфері цілей та завдань кібербезпеки через діалог на теоретичному та практичному рівнях;
- просування польських рішень та продуктів у сфері кібербезпеки на національному та міжнародному рівнях;
- ефективну співпрацю та державну підтримку у сфері кібербезпеки для приватних операторів компонентів інфраструктури

[26] Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej. (Warszawa 2015) - 4. KONCEPCJA ZADAŃ PREPARACYJNYCH (PRZYGOTOWAWCZYCH) W DZIEDZINIE CYBERBEZPIECZEŃSTWA (UTRZYMANIA I ROZWOJU SYSTEMU CYBERBEZPIECZEŃSTWA RP) - 4.3. Publiczne i prywatne ogniwa wsparcia . - http://en.bbn.gov.pl/ftp/dok/01/DCB.pdf
[27] Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017 – 2022
[28] 4.3. PUBLICZNE I PRYWATNE OGNIWA WSPARCIA - http://en.bbn.gov.pl/ftp/dok/01/DCB.pdf

критичних систем управління з використанням телеінформаційних систем і операторів та провайдерів телеінформаційних послуг;

- залучення представників державного, приватного та державного секторів, громадян у процесі безперервної освіти та підвищення рівня обізнаності щодо загроз в галузі кібербезпеки.

У цьому ж документі підкреслюється: «Важливо створити систему підтримки досліджень та розробок в галузі кібербезпеки та освіти включно з проектами, реалізованими у співпраці з світом науки і комерційних підприємств. Пріоритетним у цьому відношенні є створення системи сертифікації національних рішень, які можуть посприяти національній незалежності в технічному, програмному та криптологічному вимірах». У розвиток даної ідеї зазначено, що для довгострокової оптимізації кібербезпеки РП важливо створити відповідні галузеві стандарти та належні практики підтримки приватних та недержавних організацій (НДО, наукових установ тощо), підтримання на урядовому рівні досліджень у галузі управління ризиками в сфері кібербезпеки.

Питання ДПП у кібербезпековій сфері деталізує 7-ий розділ «Стратегії кібербезпеки РП на 2017-2022 рр», ухваленої під егідою Міністерства оцифрування РП у 2017 році. Даний документ є продуктом діяльності міжвідомчої групи, до складу якої увійшли представники міністерств: оцифрування, національної оборони, внутрішніх справ та адміністрації, а також низки безпекових структур: Агенції внутрішньої безпеки, Урядового центру безпеки, Бюро національної безпеки. Приватні структури у даній групі опосередковано представляв Національний кібербезпековий центр NASK.

Таким чином в РП склалася досить чітко регламентована з правової точки зору та підтримана на рівні громадянського суспільства й бізнесового та банківського секторів система ДПП в кібербезпековій сфері, яка по суті доповнює й розвиває подібні практики ДПП в інших сферах надання «суспільних благ».

ВИСНОВКИ ТА РЕКОМЕНДАЦІЇ:

1. До засадничих характеристик ДПП згідно усталеної в Республіці Польща юридичної практики слід віднести:

- взаємну корисність;
- цивільно-правовий характер;
- конкретну мету (побудова інфраструктурних об’єктів, надання певних послуг, що традиційно виконувалося публічним (державним) сектором тощо);
- оптимальний поділ завдань між державним (публічним) та приватним секторами співпраці;
- поділ ризиків між обома секторами.

На жаль, ці характеристики не знайшли адекватного відображення в українському Законі про ДПП 2010 року, у якому співпраця між державою та приватним сектором хибно зводиться до питання вибору державою «адекватного партнера» серед приватних компаній, що окреслено через призму «ефективності». Таке тлумачення сутності ДПП відкриває простір для різноманітного суб’єктивізму й волюнтаризму, сприяє корупції тощо. До того ж, ігноруються питання підтримки вітчизняного виробника (партнера), створення в Україні додаткових робочих місць тощо.

2. Дискусії довкола сутності ДПП стосуються передусім можливості його ототожнення/розрізнення з «концесійною діяльністю» (концесіями). Зустрічаються дві крайніх позиції: ототожнення цих форм взаємодії державного (публічного) й приватного партнерів та їх строге розрізнення.

Найоптимальнішим уявляється поширений в Україні погляд, відповідно до якого ДПП – більше широке поняття, а концесія – лише один з різновидів ДПП, який стосується переважно реалізації інфраструктурних об’єктів за кошти приватного інвестора з наступною їх передачею державному (публічному) власнику на засадах принципу «Побудуй –

Використай – Передай» («Build-Operate-Transfer (BOT)». На цих засадах в країнах ЄС (включно з РП) будується дедалі більше інфраструктурних об’єктів і цей досвід безумовно заслуговує на екстенсивне й інтенсивне використання в Україні.

3. Побудова ефективного ДПП в сфері кібербезпеки неможлива без проведення об’єктивного та незалежного оцінювання системи кібербезпеки на рівні як державних, так і недержавних інституцій під егідою однієї з авторитетних міжнародних кібербезпекових організацій (імовірно, Business Software Alliance (BSA) за наступними критеріями:

- правові підстави функціонування даного фрагменту кіберпростору;
- організаційні інституції та механізми забезпечення кібербезпеки;
- стан державно-приватного (публічно-приватного) партнерства;
- секторальна кібербезпека;
- кібербезпекове просвітництво.

4. Для довгострокової оптимізації стану кібербезпеки в Україні, за прикладом РП та інших країн ЄС, важливо створити відповідні галузеві стандарти та належні практики підтримки приватних та недержавних організацій (НДО, наукових установ тощо), підтримки на урядовому рівні досліджень у галузі управління ризиками в сфері кібербезпеки.

5. За прикладом РП та інших країн ЄС Україна потребує створення практичних механізми співробітництва та партнерства в сфері кібербезпеки для чого пропонується:

- розвиток публічно-приватного діалогу у сфері підготовки законопроектів, які посприяють створенню ефективних правил та процедур діяльності у сфері кібербезпеки;
- підписання відповідних угод у сфері цілей та завдань кібербезпеки через налагодження діалогу на теоретичному та практичному рівнях;

- просування українських рішень та продуктів у сфері кібербезпеки (стартапів) на національному та міжнародному рівнях;
- залучення представників державного, приватного та державного секторів, громадян до процесу безперервної освіти та підвищення рівня обізнаності щодо загроз в галузі кібербезпеки.

М.А.Ожеван
Відділ інформаційної безпеки та
розвитку інформаційного суспільства
Національний інститут стратегічних досліджень
лютий 2018 р.