НАЦІОНАЛЬНИЙ ІНСТИТУТ СТРАТЕГІЧНИХ ДОСЛІДЖЕНЬ

ДЕРЖАВНО-ПРИВАТНЕ ПАРТНЕРСТВО У СФЕРІ КІБЕРБЕЗПЕКИ: МІЖНАРОДНИЙ ДОСВІД ТА МОЖЛИВОСТІ ДЛЯ УКРАЇНИ

Аналітична доповідь

Київ 2018

УДК 323.21
Д 36

Електронна версія: http://www.niss.gov.ua

Авторський колектив:
Дубов Д.В., д. політ. н., с. н. с. – вступ, розділ 1, пп. 4.4, 4.5;
Бойко В.О., к. і. н. – пп. 3.1 та 3.2;
Гнатюк С.Л., к. і. н. – пп. 4.1, 4.2 та 4.3;
Ісакова Т.О. – розділ 2;
Ожеван М.А., д. філос. н., проф. – п. 3.4;
Покровська А.В. – п. 3.3.

Державно-приватне партнерство у сфері кібербезпеки: міжнародний досвід та можливості для України : аналіт. доп. / за заг. ред. Д. Дубова. – К. : НІСД, 2018. – 84 с.
Д 36
ISBN 978-966-554-296-7

Аналітична доповідь присвячена питанням формування ефективного державно-приватного партнерства з питань кібербезпеки. Проаналізовано теоретичні підходи до державно-приватного партнерства та їх особливості в питаннях кібербезпекової сфери. Досліджено світовий досвід (США, ЄС, Німеччини, Великої Британії, Польщі) із розбудови довіри між державним та приватним сектором з питань безпеки кіберпростору. Розглянуто нормативно-правові та організаційні основи державно-приватного партнерства в Україні, наведено ефективні приклади такого партнерства. Окреслено перспективні напрямки розвитку кібербезпекового державно-приватного партнерства в Україні та можливі шляхи їх імплементації.

УДК 323.21

ISBN 978-966-554-296-7

ЗМІСТ

ВСТУП

Сьогодні державно-приватне партнерство (далі – ДПП) визнається як державами, так і недержавними суб'єктами ключовим елементом побудови дійсно ефективної системи кібербезпеки держави. Майже кожна стратегія кібербезпеки (національного чи наднаціонального рівня) або ж відомчий візійний документ (який стосується кібербезпеки) містить згадки про бажання розвивати ДПП.

Водночас, незважаючи на таку єдність поглядів, практика реалізації кібербезпекового ДПП (далі – КДПП) все ще є вкрай неоднозначною та суперечливою (наприклад, рейтинг Міжнародного союзу електрозв'язку «Глобальний індекс кібербезпеки 2017» хоча й має графу «державно-приватне партнерство», але вимірює його досить обережно – зеленим, жовтим та червоним кольорами і не надаючи змістовної методології вимірювання[1]).

Запропоноване дослідження – спроба розпочати в Україні більш широку дискусію з цього питання, висвітлюючи, з одного боку, вже наявний досвід окремих західних держав у сфері побудови ДПП, а з іншого – ключові українські проблеми в контексті створення КДПП. Результатом дослідження є рекомендації, які, на нашу думку, допоможуть і державним органам, і недержавним суб'єктам (передусім бізнесу, але так само і неурядовим організаціям та науковцям/експертам) ліпше зрозуміти, якими є можливі шляхи вирішення проблеми розбудови КДПП в Україні.

Перший розділ доповіді присвячений загальнотеоретичним підходам до ДПП як такого та осмисленню самої можливості реалізації КДПП.

У другому та третьому розділах роботи описані проблеми побудови КДПП у економічно та технологічно розвинених державах, які мають значну історію з формування механізмів КДПП та власне мають потужних бізнес-учасників, з якими і вибудовуються ці відносини, або в тих країнах, які лише приступили до формування КДПП, але здійснюють це в межах загальноєвропейського нормативного простору. Таким чином для аналізу були обрані США, Велика Британія, Німеччина та Польща.

Четвертий розділ повністю присвячено проблемам у цій царині в Україні, де ситуація додатково ускладнюється низкою специфічних обставин, характерних здебільшого саме для нашої держави. Передусім це:

- неоднозначна нормативно-правова база, яка регулює КДПП (у т. ч. в питанні, що стосується хактивістської діяльності);
- наявність низки питань (зокрема у сфері впровадження стандартів кібербезпеки), які більшою мірою вже вирішені в західних державах;
- істотно більша активність громадського сектору, який хоче брати більшу участь у забезпечення кібербезпеки держави (особливо в ситуації після 2014 р., коли з'явилася значна кількість хактивістських угруповань).

[1] Global Cybersecurity Index 2017 [Електронний ресурс]. – Режим доступу : https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01–2017-PDF-E.pdf

Усе це доповнюється більш традиційними проблемами, з одного боку, надмірної закритості безпекових структур та виразного тренду до дедалі зростаючого контролю, а з іншого – часто завищених очікувань та «максималізму» від приватного та неурядового секторів, які не завжди спроможні виробити конструктивний порядок денний для обговорення з державою, не мають належних знань про реальні можливості та обмеження державних установ у цій сфері, часто не дуже обізнані із особливостями українського законодавства, а також їм відчутно бракує єдності у поглядах на те, якою взагалі може і має бути КДПП.

Автори доповіді не ставили собі за мету дати вичерпні відповіді на всі питання у цій сфері, але намагались узагальнити світовий досвід у розбудові КДПП, зрозуміти об'єктивні межі КДПП та визначити ключові проблеми, пов'язані із розвитком КДПП в Україні. За результатами цього огляду запропоновані й окремі рекомендації, які, на думку авторів, дозволять перетворити діалог між державними та приватними структурами щодо КДПП на більш результативний та надати йому певних інституційних форм.

Розділ 1. ДПП У СФЕРІ КІБЕРБЕЗПЕКИ: МОЖЛИВОСТІ ТА ОБМЕЖЕННЯ

Історичний тренд до більшої участі приватного сектору в житті держави виник у кінці 70-х років XX ст. у країнах Заходу, що було пов'язано із глобальною економічною кризою того часу[2]. Одним із шляхів виходу з неї неоліберальні теоретики вбачали у необхідності масштабної дебюрократизації та передачі частини повноважень державі приватним суб'єктам або, принаймні, встановлення партнерських відносин між державою та бізнесом. І якщо перші проекти ДПП стосувалися передусім розвитку інфраструктури міст, екологічних проектів, охорони здоров'я та освіти, то в подальшому кількість сфер, до яких застосовується поняття ДПП розширилось настільки, що це вже змушує окремих дослідників казати про вихолощення поняття та перетворення його на «ярлик, для всіх нових або невідомих форм співробітництва між державою та приватним сектором»[3].

Найбільш неоднозначним стало проникнення ДПП до сфери забезпечення державної безпеки, тобто туди, де держава традиційно зберігала свою монополію. Щоправда така монополія завжди була досить умовною: майже в усі періоди історії людства існували приклади специфічних державно-приватних відносин у сфері національної безпеки. Особливо яскраво вони проявлялись у питанні військових операцій на морі, де довгий час були поширені «каперські свідоцтва» для приватних кораблів. Сьогодні така практика продовжується (і багато в чому набуває дедалі нових вимірів) у контексті розвитку «приватних воєнних компаній».

Одним з найбільш складних теоретичних питань, пов'язаних із ДПП, є визначення того, що є «справжнім» ДПП, а що ні. Ключове розуміння ДПП концентрується навколо двох ідей, які дозволяють охарактеризувати необхідні причини для виникнення ДПП:

- жоден із партнерів не може досягти бажаної цілі одноособово (без партнера);
- має бути фінансова домовленість, яка робить партнерство привабливим для обох сторін.

Стівен Ліндер (*Stephen Linder*) характеризує це таким чином: «метою ДПП є використання синергії у спільному інноваційному використанні ресурсів та застосуванні управлінських знань задля оптимального досягнення цілей усіх залучених сторін, якщо ці цілі не могли бути досягнуті без залучення цих сторін»[4]. Крім того, він слушно зазначає, що в межах ДПП обидві сторони, для забезпечення успішності партнерства, мають змінювати характер свого мислення – суб'єкти ДПП змушені думати та діяти як їх партнери, тобто державні учасники мають думати та діяти як підприємці, в т. ч. як бізнес має

[2] Cavelty Myriam Dunn, Suter Manuel. Public–Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection // International Journal of Critical Infrastructure Protection. – December, 2009. – Vol. 2, Is. 4,, – P. 179–187.

[3] Linder S., Coming to terms with the Public-Private Partnership – A grammar of multiple meanings. // Public-Private Policy Partnerships / P. Vaillancourt Rosenau (Ed.). – The MIT Press, Cambridge MA, 2000. – P. 19–36.

[4] Linder S., Vaillancourt P. Rosenau, Mapping the terrain of the Public–Private Policy Partnership // Public–Private Policy Partnerships / P. Vaillancourt Rosenau (Ed.). – The MIT Press, Cambridge, MA, 2000. – P. 1–19.

враховувати суспільний інтерес, і очікувати, що їм доведеться бути більш підзвітними громадськості[5].

Вінсент Коувенховен (*Vincent Kouwenhoven*) конкретизує[6], що ДПП є неможливим без:

- взаємної довіри та встановлення обмежень, спрямованих на недопущення зловживань;
- наявності чітких, недвозначних цілей та стратегії, яка зафіксована у документальному вигляді;
- чіткого розподілу ризиків;
- відповідальності, повноважень, а також функцій забезпечення партнерських бізнес-інтересів.

Арнав Ягасія (*Arnav Jagasia*) багато в чому доповнює цей підхід такими тезами[7]:

- партнери мають ідентифікувати та визначити (*detect*) поведінку, яка викликає занепокоєння;
- учасники партнерства мають переконатися, що учасники – як від державного, так і приватного сектору – повністю погоджуються із засадами (*standards*) партнерства;
- ДПП має запропонувати механізм відповіді на ситуації після кіберзагроз (це включає аналіз атаки та виявлення рішень для обов'язкового вирішення уразливостей в атакованих системах).

Дискусійним залишається і питання того, в яких конкретно формах може реалізовуватись «справжнє» ДПП – тут так само відчувається брак методологічних напрацювань. Фінська дослідниця Марія Костаінен (*Mariia Kostiainen*) пропонує відштовхуватись від того, що загалом усе ДПП може бути поділено на три великі групи взаємодій (щоправда, зважаючи на більш вузьку проблему забезпечення безпеки дітей у мережі Інтернет)[8]:

- дискусії (формування постійних майданчиків для обговорення складних питань ДПП між його учасниками, активне проведення як академічних, так і практичних круглих столів/семінарів на цю тему, розвиток будь-яких форм формальних та неформальних взаємодій між державою, приватним сектором, неурядовими організаціями та науковцями);
- спільні дії (здійснення спільних зусиль державного та приватного секторів на досягнення спільних цілей. Найбільш традиційною є форма такого співробітництва для цілей освіти у сфері кібербезпеки, у т. ч. через залучення співробітників суб'єктів системи кібербезпеки до освітніх акцій, що здійснюються неурядовими структурами);
- пряме та непряме фінансування (мається на увазі пошук механізмів спільного державного та недержавного фінансування проектів, які можуть бути трактовані як ДПП у кіберсфері. Це включає видатки як прямі з держбюджету, так і опосередковані через різноманітні квазідержавні програми фінансування, в т. ч. – через грантування).

Роджер Веттенхал (*Roger Wettenhall*)[9], аналізуючи різні підходи до самої ідеї ДПП, приходить до думки, що загалом є дві великі категорії того, що традиційно відносять до ДПП:

- перша – горизонтальні, не ієрархічні зв'язки, що характеризуються консенсусною моделлю прийняття рішень;

---

[5] Linder, S.H. Coming to Terms With the Public-Private Partnership: A Grammar of Multiple Meanings // American Behavioral Scientist. – 1999. –№ 43(1). – P. 35–51. DOI: 10.1177/00027649921955146

[6] Kouwenhoven V., Public-Private Partnership: A model for the management of Public-Private cooperation // Modern Governance / J. Kooiman (Ed.). – New Government–Society Interactions, Sage, London, 1993. – P. 119–130.

[7] A Look into Public Private Partnerships for Cybersecurity [Електронний ресурс]. – Режим доступу : https://publicpolicy.wharton.upenn.edu/live/news/1815-a-look-into-public-private-partnerships-for

[8] Internet safety for children (Finnish practices and stakeholders) [Електронний ресурс]. – Режим доступу : http://tampub.uta.fi/bitstream/handle/10024/99386/GRADU-1466515272.pdf?sequence=1&isAllowed=y

[9] Wettenhall R. The Rhetoric and Reality of Public-Private Partnerships // Public Organization Review. – March, 2003. – Vol. 3, Is. 1. – P. 77–107.

- друга – ієрархічно організовані відносини, де одна зі сторін має домінуючу позицію.

На його думку лише ті взаємодії, які можуть бути віднесені до першої категорії, можна дійсно називати ДПП.

Водночас кібербезпекова сфера має певні унікальні проблеми, які все ще слабко досліджені та не мають універсальних «рецептів» рішень (більше того, можливо, вони взагалі їх не мають). Американська дослідниця М. Карр (*Madeline Carr*) звертає увагу[10], що навіть у США, де майже 15 років ДПП визначалось як ядро (*cornerstone*) національної системи кібербезпеки, сторонам так і не вдалось визначити параметри, характер та масштаби такого співробітництва (більше того, звіт Рахункової палати США «Доповідь про захист критичної інфраструктури: Поточний підхід до планування в секторі кібербезпеки потребує переоцінки» (*Current Cyber Sector Specific Planning Approach Needs Reassessment*) за 2009 р. виявив значну кількість проблем у тих зусиллях, які здійснювались американським урядом для створенні ДПП у сфері кібербезпеки).

Ефективність КДПП багато в чому пов'язана з тим, як взагалі визначена кібербезпека та якою мірою співвідносяться кібербезпека держави та кібербезпека людини. В багатьох випадках правило «що добре для безпеки держави, то добре і для безпеки індивіда» не працює і особливо часто – в кібербезпекових питаннях. Крім того, майже завжди в цих відносинах присутній брак координації, що впливає на сам характер ДПП. З цього приводу Ларрі Клінтон (*Larry Clinton*)[11] влучно відзначає, що «партнерство між громадянами, чи бізнесом, чи урядом може виявитись значно складнішим, ніж це очікується. Брак координації щодо ролі партнерів, їх відповідальності та очікувань може призвести до проблем, навіть якщо у партнерів начебто спільні цілі. Комунікування ж щодо потенційних відмінностей також може бути проблематичним навіть у тому випадку, якщо партнери щиро хочуть досягти успіху». Тому, на його думку, для ефективного ДПП раціональне та змістовне управління цими відносинами може мати навіть більше значення, ніж сутність цих відносин (чи охопленість ними усієї множини сфер кібербезпеки).

Усе ще дискусійним є, в яких саме сферах кібербезпеки може взагалі застосовуватись ДПП. Тейлор Мур (*Tyler Moore*)[12] пропонує поділити їх на чотири ключові сфери:

- крадіжка даних у мережі (*online identity theft*);
- індустріальне кібершпигунство;
- захист критичної інфраструктури;
- ботнети.

На думку Т. Мура, і державні, і приватні суб'єкти опиняються уразливими та залежними від цих сфер, тож саме навколо них і можуть зосереджуватись ініціативи ДПП.

Однак такий поділ (власне, як і більшість інших), з одного боку, спрощують пошук сфер для можливого ДПП, але, так само, і ускладнюють, адже обмежують коло сфер для перемовин. На нашу думку, говорячи про КДПП, частіше за все мають на увазі дві макросфери:

- економіку в цілому (від якої залежить процвітання держави та її громадян) та
- критичну інфраструктуру (від роботи якої часто залежить безпека і держави, й її громадян).

І перша, і друга сфери абсолютно переважно перебувають у руках приватних власників, але якщо кібератака на економічну міць держави матиме переважно фінансові наслідки, то кібератака на критичну інфраструктуру може привести до людських жертв. Тож

[10] Madeline Carr. Public–private partnerships in national cyber-security strategies [Електронний ресурс]. – Режим доступу : https://www.chathamhouse.org/sites/files/chathamhouse/publications/ia/INTA92_1_03_Carr.pdf

[11] Clinton Larry. A Relationship on the Rocks: Industry-Government Partnership for Cyber Defense.// Journal of Strategic Security. – 2011. Vol. 4, no. 2. – P. 97–112.

[12] Moore T. Introducing the Economics of Cybersecurity: Principles and Policy Options. Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy [Електронний ресурс]. – Режим доступу : https://www.nap.edu/read/12997/chapter/3

природно, що, незважаючи на характер власності, держава визнає за собою певні зобов'язання та відповідальність із контролю за безпекою об'єктів критичної інфраструктури, тим самим невідворотно формуючи базу для ДПП (до речі, про об'єктивну обмеженість можливостей створення реального ДПП саме у сфері захисту критичної інфраструктури говорить багато дослідників цього питання, зокрема Д. Ассаф[13], Л. Клінтон[14] та М. Карр).

Загалом мету впровадження КДПП Остін Гівенс (*Austen D. Givens*) окреслює таким чином (із акцентом на питання захисту об'єктів критичної інфраструктури): «зменшення дублювання зусиль, покращення міжсекторних взаємозв'язків, підвищення ефективності та досягнення захисту ліпше, ніж уряд чи бізнес могли б це зробити незалежно один від одного»[15].

С. Ліндер пропонує визначати сутність будь-яких кібербезпекових проектів у сфері ДПП крізь два великі напрями:

- партнерство як реформа управління та
- партнерство як розподіл (*sharing*) влади.

Перший підхід бере до уваги те, що керівники із сфери державного управління (в т. ч. – у сфері кібербезпеки) мають переймати навички, уміння та підходи своїх колег з приватного сектору, запозичуючи найкращі практики бізнесу з управління своїми сферами. Цей підхід іманентно відштовхується від того, що ринок є більш ефективним за своєю суттю, ніж держава, тож менеджери у приватному секторі є більш кваліфікованими, ніж державні фахівці. Але це припущення веде до більш глобальних узагальнень, які логічно приводять до висновку, що саме приватний сектор, а не держава має перейматися захистом приватних мереж (що, до речі, відображено і в українському профільному законодавстві). Однак у випадку з критичною інфраструктурою це вступає в очевидну суперечність із концепцією суспільного блага, що меншою мірою турбує приватний сектор (який керується власною бізнес-моделлю), але в чому зацікавлений уряд та громадяни. Ця ситуація (однак у більш широкому контексті) дозволила Т. Муру вийти у своїх дослідженнях на феномен «незбалансованих стимулів» (*misaligned incentives*), які виникають у випадку компромісу між безпекою та ефективністю. Під ними мається на увазі часто інтуїтивно зрозуміла та знайома з практики проблема, коли збільшення шарів секретності (безпеки) негативно впливає на ефективність організації. Т. Мур демонструє це на прикладі банків: якщо банки перестануть надавати послуги онлайн-банкінгу, вони дійсно стануть менш уразливими до кібератак. Але так само й їх клієнти були б обмежені у доступі до своїх коштів, а витрати на підтримку роботи філій банків (для забезпечення такого ж рівня обслуговування) були б надзвичайно високими для банків. Ця ж логіка спрацьовує і в протилежному напрямі.

Другий підхід – партнерство як розподіл влади – найбільш вдало характеризується ідеєю «обміну інформацією». Партнерство як розподіл влади базується на ідеї співпраці, в якій довіра у відносинах між партнерами заміщує ідею жорсткої командної системи (тож багато в чому цей підхід підтверджує концепцію неієрархічних відносин як основи для справжнього ДПП). Однак ця ж ідея «обміну інформацією» часто виявляється і найбільш дискусійною. З одного боку, і приватний сектор, і урядові структури вважають цей напрям одним із ключових. З іншого – обидві сторони мають перманентні застереження для цього напряму партнерства. Для приватних компаній це, передусім, можливі витоки інформації про атаку. Причому небезпекою є витоки як публічні, так

[13] Assaf D., Conceptualizing the use of Public–Private Partnerships as a regulatory arrangement in critical information infrastructure protection // Non'State Actors as Standard Setters / A.O. Peters, L. Koechlin, T. Förster, G.F. Zinkernagel (Eds.). – Cambridge University Press, October, 2009.

[14] Clinton Larry. A Relationship on the Rocks: Industry-Government Partnership for Cyber Defense. – Journal of Strategic Security. – 2011. – Vol. 4, no. 2. – P. 97–112.

[15] Наводиться за: John O Halloran. Challenges of public-private partnerships in cybersecurity [Електронний ресурс]. – Режим доступу : https://search.proquest.com/openview/0f178ab71ad4af902baf8e3528f9a473/1?pq-origsite=gscholar&cbl=18750&diss=y

і виключно для конкурентів. Для держави ця проблема здебільшого пов'язана із тим, що значна частина інформації, яка може бути цікава приватному сектору (та важлива для його кібербезпеки) може мати гриф обмеження на поширення. Не слід ігнорувати і загальний тренд державних безпекових структур на втаємничення інформації та швидше її накопичення, ніж поширення.

А. Ягасія звертає увагу на низку причин, чому приватний сектор досить неохоче йде на співпрацю з державою (особливо в частині розслідування інцидентів). Зокрема, на його думку, компанії часто мають сумніви щодо залучення державних структур для розслідування кіберінцидентів і тому, що в такому разі держава отримає доступ до внутрішньої інформації компанії. Крім того, сам факт залучення державних структур може призвести до ескалації серйозності ситуації (ситуація буде сприйматись суспільством як більш серйозна, ніж вона є, а самі компанії матимуть більше бюрократичних проблем через залучення державних структур). До того ж компанії відчувають, що в разі долучення держави вони фактично втратять автономність у розслідуванні кіберінциденту.

Зазначені дискусії істотно вплинули і на ті підходи до КДПП, що істотно впливають і на позиції ключових суб'єктів цієї сфери, зокрема, – Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (*European Union Agency for Network and Information Security, ENISA*). Експерти ENISA ще в 2010 р. у своєму дослідженні «Збірник найкращих практик для кооперативної моделі ефективного ДПП» (де ДПП визначено як «організовані відносини між державними та приватними організаціями, які встановлюються заради загальносуспільних інтересів та перспектив (розвитку). У цих відносин спільні цілі, що досягаються за допомогою розподілу функцій (ролей) та визначення методів роботи»)[16] запропонували своєрідну матрицю ДПП, що дає відповіді на ключові питання:

- навіщо ДПП потрібне;
- хто є учасниками та залучений до процесу;
- хто цим керуватиме;
- які сервіси чи стимули з'являться внаслідок реалізації;
- коли і як така співпраця має розвиватись (табл. 1).

Незважаючи на те, що всі положення цього підходу є важливими для розуміння проблематики КДПП, у контексті теоретичних засад розвитку важливо відзначити, що автори доповіді чітко зазначають, що «для успішного партнерства обидві сторони мають чітко розуміти його важливість для своїх організацій. Це стосується і тих форм, де членство у КДПП є обов'язковим, оскільки визначає ступінь участі». Більше того – чітке розуміння цінності партнерства має бути і у державних структур, і у приватних. У роботі наводяться три переліки причин, чому партнерство може мати сенс для державних структур, для приватних та якими можуть бути спільні (і для держави, і для бізнесу) аргументи на користь КДПП.

Для державних структур основними причинами є такі:

- національна стратегія є, але інструменти її реалізації обмежені, тому КДПП може бути таким механізмом;
- уряд усвідомлює необхідність залучення недержавного сектору (*industry)* до подолання загроз (*help respond to a crisis*);
- у стратегії національної безпеки має бути передбачена участь (представництво) недержавних компаній (*share with industry representatives*);
- уряд має відповідальність щодо захисту критичної інфраструктури, але не має механізмів залучення до цього процесу індустрії;

[16] Good Practice Guide on Cooperatve Models for Effective PPPs [Електронний ресурс]. – Режим доступу : https://www.enisa.europa.eu/publications/good-practice-guide-on-cooperatve-models-for-effective-ppps/at_download/fullReport

Таблиця 1. **Матриця ДПП (версія ENISA)**

ЧОМУ	ХТО	ЯК	ЩО	КОЛИ
ЦІЛІ[I] • Стримування • Захист • Виявлення • Відповідь • Відновлення **ЗАГРОЗИ** • Всі види • Природні катастрофи • Помилки в роботі телеком-систем • Кіберзлочини • Тероризм	**ПОШИРЕННЯ** Географічно • Національний • Європейський • Міжнародний Фокус • Географічний • Сектор • Кроссекторний • Тематичний **ЗВ'ЯЗОК**[IV] • Через національні кордони • Усередині національних кордонів • CERTS чи CSIRTS • Регулятор • Урядові структури • Правоохоронні структури	**УПРАВЛІННЯ** Типи активностей • Довгострокові об'єднання • Робочі групи • Миттєві групи[II] • Комбінована активність • Базова стратегія чи група радників Лідерство[III] • Один з учасників • Координаційна структура • Демократичне партнерство Фінансування • Обов'язкове членство • Стягнення оплати • Держава оплачує все або частину • Оплачується неробочий час та відрядження членів Комунікаційний стиль[V] • Зустрічі віч-на-віч • Віртуальні зв'язки[VI] • Автоматизована система поширення • Автоматизована система двостороннього обміну Норми (правила) • Правила набуття членства • Угоди використання отриманої інформації • Політика розбудови довіри • Безпекові вимоги до членства	**СЕРВІСИ** • Дослідження / аналіз • Збірки найкращих практик • Раннє попередження • Навчання • Підвищення обізнаності • Тощо **СТИМУЛИ** • Зменшення вразливостей • Економія на витратах • Доступ до цінних знань • Вплив на регулювання або національну політику • Тощо	**МОДЕЛІ РОЗВИТКУ** • Зверху вниз • Знизу вгору • Зверху вниз, згодом зростання знизу вгору • Знизу вгору, згодом зростання зверху вниз • «Вистрелив та забув» (разові курси та тренінги) • «Зійшлися – розійшлися» (миттєві групи)

Джерело: European Union Agency for Network and Information Security.

[I] У дослідженні ці етапи подаються як «життєвий цикл безпеки».

[II] Можуть створюватись на декілька днів чи навіть годин для оперативної відповіді на раптову загрозу.

[III] Питання обрання структури, яка безпосередньо координуватиме і очолюватиме ДПП. У більшості випадків нею стає одна з організацій, яка в цілому відповідає за ДПП, або ж для цього створюють окрему структуру.

[IV] Мається на увазі зв'язок учасників ДПП зі структурами, які не є безпосередньо учасниками ДПП. Наприклад, деякі структури ДПП можуть мати тісні зв'язки з аналогічними структурами, які перебувають у інших країнах, або мати зв'язок з такими ж структурами в межах країни.

[V] Серед членів ДПП.

[VI] Мають на увазі е-мейли, телефонні конференції тощо.

- в уряду відсутні достатні кошти для залучення всіх малих стейкхолдерів до захисту критичної інфраструктури/кризових ситуацій.

Для приватних компаній такими причинами є:

- представники індустрії мають проблему і визнають, що її вирішення чи вплив істотно виходять за межі їх організаційних кордонів;
- спостерігається брак залученості вищих керівників (*Senior Management*) до дій, що спрямовані на питання безпеки;
- стратегія/політика національної безпеки не реалістична або не є придатною для реалізації (*fit for purpose*);
- індустрія хоче мати можливість впливати на майбутні редакції стратегії/політику національної безпеки чи регулювання;
- правила регулювання вимагають від організації певної індустрії бути членом КДПП;
- приватні компанії (індустрія) зацікавлена у дієвих механізмах нейтралізації неадекватного державного регулювання.

При цьому є низка факторів, які є спільними для структур обох секторів, які можуть стати аргументом для формування КДПП:

- організації мають негативний досвід бути атакованими і тепер хочуть усунути вразливості;
- організації розуміють, що вони дублюють зусилля;
- організації визнають, що існує недостатня координація чи/та обмін інформацією в певних секторах;
- організації визнають наявність провалів у забезпеченні всіх етапів життєвого циклу безпеки;
- організації визнають, що загрози розвиваються разом із подальшим злиттям комунікацій та інформаційних технологій, а отже, потребують спільної відповіді, а не розподіленої по окремих секторах;
- організації визнають злиття загроз від тероризму та кібератак;
- організації визнають, що загрози еволюціонують та зміщуються з національного/секторального рівня на міжнародний;
- спостерігається брак довіри між конкурентами в межах географічних, секторальних або тематичних сфер, а отже, існує потреба у створенні довіреної структури для вирішення цієї проблеми.

Загалом *ENISA*, користуючись підходом з п'яти елементів «життєвого циклу» пропонує три базові моделі КДПП:

1) **КДПП, сфокусоване на реагування** (розвиток елементів «відповідь» та «відновлення»). Переважно оперативні та тактичні групи, які безпосередньо працюють із наслідками атак (наприклад, *CERT-Polska,* який ще буде розглянутий у цьому дослідженні). Формуються найбільш просто, бо учасникам зрозумілий зиск від діяльності та їх цінність;

2) **КДПП, сфокусоване на попередження** (розвиток елементів «стримування» та «захист»). Основна мета – профілактика та **недопущення** атак. Більшою мірою **стратегічні** групи, які мають значну взаємну довіру, що сформована багаторічним досвідом. Приклад такого ДПП (із тих, що розглянуті у дослідженні) – американська *ISAC*;

3) **«парасолькове» КДПП**. Структури, які намагаються охопити всі елементи, починаючи від профілактичних заходів і закінчуючи допомогою в умовах кризи. **Вимагають** високого рівня готовності партнерів до співпраці. В роботі одна з таких структур розглянута більш докладно – німецька *UPKRITIS*.

У своєму новому дослідженні «Державно-приватне партнерство (ДПП). Кооперативні моделі» (*Public Private Partnerships (PPP). Cooperative models*) від 2018 р.,

ENISA пропонує[17] змінити цю градацію на іншу, яка складається з чотирьох базових моделей КДПП:

1) **інституційне ДПП.** У цьому виді ДПП всі інституції працюють у межах загальних правил ДПП. Зазвичай такий тип ДПП є джерелом числених сервісів та послуг, зокрема, дослідження, аналіз, розвиток найкращих практик, розробка настанов, проведення безпекових аудитів тощо. Цей вид ДПП частіше за все пов'язаний із захистом критичної інфраструктури. Співпраця між учасниками ДПП за такої моделі організовується як робочі групи, групи швидкого реагування та довгострокові об'єднання. Основна мета – убезпечення критичної інфраструктури загалом, але з акцентом на захисті від кіберзагроз;

2) **цілеорієнтоване ДПП** (*Goal-oriented PPP*). Цей тип ДПП орієнтований на розвиток кібербезпекової культури у державах – членах ЄС. Зазвичай це платформа чи рада, які створені для того, щоб поєднати у співпраці державний та приватний сектор для обміну знаннями та найкращими практиками.

3) **аутсорсингові служби кібербезпеки** (*Service outsourcing PPP*). Створення ДПП цього типу ініціюється урядом чи приватним сектором, коли ними визнаються проблеми у певній галузі, але у жодної зі сторін немає ресурсів чи можливостей для їх вирішення. Тому основне завдання таких новостворених структур – підвищення кібер-обізнаності та рівня кібербезпеки серед усіх стейкхолдерів. Такі структури ДПП, з одного боку, задовольняють потребу конкретного сектору в кібербезпекових рішеннях, а з іншого – можуть допомагати уряду в імплементації певних кібербезпекових стандартів чи у підготовці національних стратегій кібербезпеки. Прикладом такої є *UP KRITIS* у Німеччині.

4) **гібридне ДПП.** Загалом мається на увазі поєднання між собою інституційного та аутсорсингового ДПП. Виникає у тих випадках, коли уряду не вистачає ресурсів, необхідних для забезпечення певних рішень на національному рівні, тож є потреба у налагоджені співробітництва із приватною структурою, що має відповідний досвід та ресурси. Частіше за все така діяльність пов'язана із функціонуванням *CSIRT.*

Вочевидь цей підхід (так само, як і запропонована в 2010 р. матриця ДПП) не є єдино можливим, але на нинішньому етапі він пропонує досить цілісне та практично-значиме пояснення формування та реалізації ДПП у сфері кібербезпеки.

Підсумовуючи огляд теоретико-методологічних поглядів на КДПП, слід зазначити, що ключовою системною проблемою цієї сфери залишаються різні очікування потенційних партнерів щодо КДПП, які призводять до цілком конкретних проблем у практичному впровадженні КДПП. Вочевидь бажання держави, щоб бізнес вкладав якомога більше коштів у власну кібербезпеку (навіть якщо це не відповідає бізнес-моделі) заради «суспільного блага», стикається зі зрозумілим небажанням приватних структур нести додаткове фінансове навантаження в питаннях, які вони вважають зоною відповідальності держави (наприклад, відбиття масштабних кібератак на об'єкти критичної інфраструктури). На думку М. Карр, ця ситуація має настільки системний характер, що, можливо, доречніше говорити не стільки про партнерство, скільки про відносини між державою та приватним сектором. Ця дилема між партнерством та відносинами має принаймні ще один вимір – вона загострюється і набуває нової сутності, якщо спостерігається проблема «пробуксовування» у побудові ефективного ДПП (особливо якщо держава вважає, що це відбувається з вини бізнесу). Часто це призводить до того, що у державних структур виникає бажання піти шляхом жорсткого унормування, перетворивши певну сферу на традиційну ієрархічно-патерналістську, коли бізнес буде зобов'язаний брати на себе більше відповідальності за національну безпеку, в той час як уряд

[17] Public Private Partnerships (PPP) Cooperative models [Електронний ресурс]. – Режим доступу : https://www.enisa.europa.eu/publications/public-private-partnerships-ppp-cooperative-models/at_download/fullReport

виконуватиме роль судді. Звісно, в такій моделі щодо відносин про «партнерство» вже не йдеться. Все це породжує і значну варіативність моделей ДПП у різних демократичних країнах, що часто залежить як від нормативно-правового простору країн, так і від традицій ДПП, які в них склались історично.

Водночас маємо зазначити, що, попри надзвичайно стриманий погляд багатьох дослідників на простір можливого існування КДПП, навіть найбільші скептики не заперечують, що ДПП потрібне і важливе. В цьому сенсі Стівен Голдсміт (*Stephen Goldsmith*) та Вільям Еггерс (*William D. Eggers*)[18] слушно зауважують, що «важливо аналізувати не те, чи потрібне державно-приватне партнерство взагалі, а те, у яких формах воно має відбуватись»[19].

[18] Goldsmith S., Eggers W.D. Governing by Network: The New Shape of the Public Sector [Електронний ресурс]. Washington, DC : BrookingsInstitution Press, 2009. – Режим доступу : https://www.brookings.edu/wp-content/uploads/2016/07/governingbynetwork_chapter.pdf

[19] Наведено за: Greiman, V.A. Public/Private Partnerships in Cyberspace: Building a Sustainable Collaboration // Journal of Information Warfare; Yorktown. – 2015. – Vol. 14 (3). – P. 30–42.

Розділ 2. НОРМАТИВНО-ПРАВОВІ ТА ІНСТИТУЦІЙНО-ОРГАНІЗАЦІЙНІ ЗАСАДИ КДПП: ДОСВІД США

Сьогодні інтегрованість мереж державного та приватного секторів стає дедалі більш важливою для національної безпеки. Останні чотири адміністрації наголошували на важливості кібербезпеки як у державному, так і в приватному секторах. Адміністративні та законодавчі кроки продемонстрували важливість партнерських відносин між приватним сектором та урядом у захисті критичної інфраструктури, сприянні ініціативам у галузі освіти та кібербезпеки і забезпеченні цілісності мережевої інфраструктури.

Президент Барак Обама з самого початку роботи своєї адміністрації визнавав, що «кіберзагрози – один із найсерйозніших національних і економічних викликів, з якими ми стикаємося як країна». За оцінками фахівців, кібератаки вартують США 300 млрд дол. США на рік (або близько 1 % ВВП) у вигляді втрат інтелектуальної власності, а безпосередні втрати для населення становлять майже 15 млн дол. США на рік[20]. Крім того, стурбованість споживачів питаннями кібербезпеки створює дедалі більше проблем для потенціалу розвитку цифрової економіки. Занепокоєність питаннями безпеки і приватності призвела до того, що приблизно половина користувачів мережі Інтернет в США утримуються від здійснення фінансових трансакцій, участі в операціях *e*-торгівлі або участі в соціальних мережах.

Користь від спільної робити над ініціативами з кібербезпеки взаємна як для державного, так і приватного секторів. Оскільки приватний сектор контролює більшу частину критичної інфраструктури, що часто є привабливою для дій кіберзлочинців, багато приватних компаній уже мають програми з кібербезпеки, володіють спеціальними знаннями та досвідом у вирішенні потенційних загроз. Державний сектор, зі свого боку, має ширші можливості для розслідування кіберзлочинів та переслідування кіберзлочинців.

Уперше питання необхідності спільного з приватним сектором захисту кіберпростору було висвітлено у **Директиві про рішення Президента № 63 «Про захист критичної інфраструктури»** (*Critical Infrastructure Protection, Presidential Decision Directive 63 (PDD-63)*)[21] від 1998 р., де президент Вільям Дж. Клінтон визначив захист критичної інфраструктури та ключових ресурсів (*CIKR*) як національну ціль та закликав до співпраці між урядом та приватним сектором з метою захисту фізичної та кіберсистем. Так, Розділ IV «Державно-приватне партнерство» констатує таке: «Оскільки цілі нападів на нашу критичну інфраструктуру, ймовірно, включатимуть як об'єкти у сфері економіки, так і урядові, зменшення нашої потенційної вразливості вимагає тісно узгоджених

[20] Киберготовность США 2.0 [Електронний ресурс]. – Режим доступу : https://digital.report/kibergotovnost-ssha-2–0-vvedenie/

[21] Presidential Decision Directive/NSC-63 [Електронний ресурс]. – Режим доступу : https://fas.org/irp/offdocs/pdd/pdd-63.htm

зусиль як уряду, так і приватного сектору. Щоб досягти успіху, це партнерство має бути істинним, взаємним і скоординованим. Тому, прагнучи досягти нашої національної мети усунення вразливостей нашої критичної інфраструктури, ми, наскільки це можливо, повинні намагатися уникнути кроків, які підвищують державне регулювання або розширюють нефінансовані урядові повноваження щодо приватного сектору».

Відповідно до Директиви, для кожного з основних секторів економіки, які є вразливими до інфраструктурної атаки, федеральний уряд призначає *Представника сектору* для зв'язків з приватним сектором (*Sector Liaison Official*). Представники сектору після обговорення та узгодження з суб'єктами приватного сектору визначають Координатора сектору (*Sector Coordinator*) для представлення приватного сектору. Разом ці дві особи, а також відомства та корпорації, які вони представляють, сприяють розробленню галузевого плану національної інфраструктури шляхом:

- оцінки вразливості сектору до кібер- або фізичних атак;
- надання рекомендацій щодо усунення вразливості;
- пропозиції щодо системи виявлення та запобігання спробам потужних атак;
- розроблення плану для оповіщення про атаки, з подальшим швидким відновленням мінімально необхідного потенціалу після атаки.

Під час підготовки галузевих планів Національний координатор з питань безпеки, захисту інфраструктури та протидії тероризму (*National Coordinator for Security, Infrastructure Protection and Counter-Terrorism*) разом із представниками провідного федерального агентства галузі та представником Національної економічної ради (*National Economic Council*)[22] забезпечує їх загальну координацію та інтеграцію різних секторальних планів.

Цією ж Директивою в рамках національної системи попередження та обміну інформацією з питань кібербезпеки в межах ФБР був створений **Центр захисту державної інфраструктури** (*National Infrastructure Protection Center, NIPC*). Функцією організації є оцінка загроз, попередження, виявлення вразливостей державної критичної інфраструктури та сприяння правоохоронним органам у розслідуванні та реагуванні. *NIPC* включає елементи, що відповідають за попередження, аналіз, комп'ютерне розслідування, координацію реагування на надзвичайні ситуації, навчання, освітню діяльність, розробку та застосування технічних засобів.

Крім того, Центр захисту державної інфраструктури встановив партнерські відносини безпосередньо з компаніями приватного сектору та зі структурами з обміну та аналізу інформації, створені приватним сектором, на кшталт **Центру з обміну та аналізу інформації** (*Information Sharing and Analysis Center, ISAC, далі* – ЦОАІ). Ці Центри створюються як неприбуткові організації, і являють собою ресурс для збору інформації про кіберзагрози для об'єктів критично важливої інфраструктури та забезпечення двостороннього обміну інформацією між приватним та державним сектором. Фактична структура та функції *ISAC* та його відносини з *NIPC* визначаються приватним сектором за погодженням із Федеральним урядом.

На практиці виявляється, що оскільки далеко не всі критично важливі елементи інфраструктури створили власні ЦОАІ, ті, у яких вони відсутні, отримують зазначені послуги від зовнішніх постачальників. Зокрема, ЦОАІ фінансових інститутів (*FS-ISAC*) надає допомогу у визначенні, запобіганні та реагуванні в разі кіберінцидентів та при спробі кіберфальсифікації. З цією метою ЦОАІ були надані прямі контакти з постачальниками фінансових послуг; комерційними компаніями, що забезпечують безпеку; федеральними, на рівні штатів та місцевими державними органами; правоохоронними органами; а також іншими надійними організаціями з метою надання послуг

[22] Національна економічна рада США – урядове агентство США, що входить до складу Адміністрації Президента США, являє собою головний форум, який використовується Президентом США для розгляду питань економічної політики.

зі своєчасного повідомлення про можливі кіберзагрози та інші загрози у міжнародному масштабі. В рамках своєї співпраці із зазначеними організаціями *FS-ISAC* використовує особливий протокол передачі даних (*Traffic Light Protocol*), щоб кожна з організацій-партнерів одержувала саме ту інформацію, яка їй необхідна. В ході координованих кібератак щодо кількох банків США в 2012–2013 рр. *FS-ISAC* надавав допомогу деяким із банків стосовно оцінки серйозності та захисту від таких атак завдяки обміну інформацією між ними в режимі реального часу. *FS-ISAC* також здійснює кроки в напрямі розповсюдження своєї системи обміну інформацією з участю організацій у Великій Британії та Європі[23].

Відповідно до Директиви № 63 з метою сприяння приватному сектору у досягненні та підтримці безпеки інфраструктури: «Державний координатор та Рада із захисту національної інфраструктури пропонують та розробляють шляхи залучення приватного сектору до періодичної оцінки ризиків критичних процесів, що включають інформаційні та телекомунікаційні системи. Міністерство торгівлі та Міністерство оборони в координації з приватним сектором надають свої знання приватним власникам та операторам критичної інфраструктури для розроблення стандартів найкращої практики у сфері безпеки. Міністерство юстиції та Міністерство фінансів гарантують проведення комплексного дослідження, що містить демографічні показники комп'ютерної злочинності, порівнює державні підходи до комп'ютерної злочинності та розробляє шляхи запобігання та реагування на комп'ютерні злочини неповнолітніми».

Окремо варто наголосити на ініціативах Б. Обами з питань обміну інформацією про кіберзагрози в інтересах посилення захищеності віртуального простору. Так, у 2011 р. з'явилися План з регулювання у сфері кібербезпеки (*Cybersecurity Legislative Proposal*) і Міжнародна стратегія для кіберпростору (*International Strategy for Cyberspace*). План закликає приватний сектор ділитися інформацією про кіберзагрози з Національним центром кібербезпеки та інтегрованих комунікацій (*National Cybersecurity and Communications Integration Center, NCCIC*) при Міністерстві внутрішньої безпеки, який далі оперативно передає цю інформацію відповідним федеральним агентствам і приватним організаціям з обміну та аналізу інформації. План Адміністрації США також покликаний підвищити рівень захисту особистої інформації громадян, зобов'язуючи приватні компанії виконувати визначені правила щодо обмеження її зберігання та використання. План вказує Міністерству внутрішньої безпеки і Генеральній прокуратурі розробити для Федерального уряду інструкції із отримання, зберігання, використання та розкриття персональних даних громадян: «Добровільний обмін інформацією з промисловим сектором, штатами та місцевими органами влади (*Voluntary Information Sharing with Industry, States, and Local Government*). Підприємства, штати та органи місцевого самоврядування іноді виявляють нові види комп'ютерних вірусів або інших кіберзагроз (інцидентів), але вони не знають, чи зможуть вони поділитися цією інформацією з Федеральним урядом. Пропозиція Адміністрації полягає в тому, що ці організації можуть обмінюватися інформацією про комп'ютерні загрози та інциденти з Міністерством внутрішньої безпеки… Водночас пропозиція передбачає надійний контроль за конфіденційністю, щоб гарантувати, що така інформація не зачепить особисту приватність та громадянські свободи»[24].

Таким чином, обов'язки *NIPC* були передані Міністерству внутрішньої безпеки і наразі належать до сфери діяльності *NCCIC*, який є центром координації дій у разі кіберінцидентів на федеральному рівні, рівні штатів, на місцевому, територіальному,

[23] Киберготовность США 2.0: Обмен информацией [Електронний ресурс]. – Режим доступу : https://digital.report/kibergotovnost-ssha-2-0-obmen-informatsiey/

[24] Cybersecurity Legislative Proposal [Електронний ресурс]. – Режим доступу : https://obamawhitehouse.archives.gov/the-press-office/2011/05/12/fact-sheet-cybersecurity-legislative-proposal

міжнародному рівнях і в приватному секторі. *NCCIC* несе відповідальність за інформування та координацію реагування на кіберінциденти, зниження ризиків і відновлювальні заходи в основному щодо федеральних мереж, при співробітництві з приватним сектором, громадянським суспільством, правоохоронними органами, розвідкою, цивільною обороною, а також міжнародними організаціями[25].

NCCIC відповідальний за координацію обміну інформацією та проактивно управляє кіберризиками у країні. Основна діяльність *NCCIC* полягає у:

- активній координації запобігання та пом'якшення наслідків тих типів кібер- і телекомунікаційних загроз, які представляють найбільший ризик для країни;
- операційній вседержавній інтеграції шляхом розширення та поглиблення взаємодії з партнерами шляхом обміну інформацією для управління загрозами, вразливостями та інцидентами;
- руйнуванні технологічних та інституційних бар'єрів, які перешкоджають спільному обміну інформацією, ситуаційній обізнаності (поінформованості) та усвідомленню загроз та їх наслідків;
- підтриманні безперервної готовності негайно та ефективно реагувати на всі випадки загроз національній безпеці у сфері кіберпростору та телекомунікацій;
- для зацікавлених сторін функціонувати як національний центр передового досвіду та експерт з питань кібербезпеки та телекомунікацій;
- захисті приватності та конституційних прав американського народу під час виконання своєї місії[26].

Важливо зазначити, що перелічені ініціативи також були втілені в численних політичних документах і виконавчих указах президентів США, що, зокрема, присвячені питанням обміну інформацією. Серед них, наприклад, Виконавчий указ (*Executive Order*) № 13636 «Про підвищення кібербезпеки у сфері критичної інфраструктури» (*Improving Critical Infrastructure Cybersecurity*)[27], підписаний у лютому 2013 р., Виконавчий указ № 13691 «Про обмін інформацією з кібербезпеки в приватному секторі» (*Private Sector Cybersecurity Information Sharing*)[28], підписаний у лютому 2015 р. Ці документи свідчать про необхідність збільшення обсягів, своєчасність та якість обміну інформацією про кіберзагрози між приватним сектором і урядом, а також наголошують на доцільності більш тісної співпраці у сфері аналізу інформації за участю всіх зацікавлених сторін.

Особливу увагу Указ № 13691 приділив стимулюванню співпраці з організаціями приватного сектора за допомогою створення **організацій з обміну та аналізу інформації** (*Information Sharing and Analysis Organizations, ISAOs*), які повинні служити пунктами обміну інформацією між підприємствами, приватним сектором і урядом. Цей Указ також містив вимогу уточнити повноваження Міністерства внутрішньої безпеки з тим, щоб той міг укладати угоди з організаціями щодо обміну інформацією, тим самим розширюючи співпрацю між організаціями з обміну та аналізу інформації і Федеральним урядом, що дозволило створити механізм, у рамках якого такі ж угоди про обмін інформацією міг би укладати і *NCCIC*. Крім того, Указ передбачає включення Міністерства внутрішньої безпеки у список федеральних агентств, які можуть видавати схвалення і підписувати угоди про обмін секретною інформацією із тим, щоб дозволити

---

[25] National Cybersecurity and Communications Integration Center [Електронний ресурс]. – Режим доступу : https://www.us-cert.gov/nccic

[26] National Cybersecurity and Communications Integration Center [Електронний ресурс]. – Режим доступу : https://www.dhs.gov/national-cybersecurity-and-communications-integration-center

[27] Executive Order – Improving Critical Infrastructure Cybersecurity [Електронний ресурс] / EXECUTIVE ORDER. – Режим доступу : https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

[28] Executive Order 13691—Promoting Private Sector Cybersecurity Information Sharing [Електронний ресурс]. – Режим доступу : https://www.dhs.gov/sites/default/files/publications/2015–03714.pdf

приватним компаніям отримати доступ до секретної інформації про наявні кіберзагрози. Указ № 13691 також містить положення про необхідність створення дієвих механізмів захисту приватності та цивільних свобод на основі спільних стандартів і керівництв, таких як принципи справедливого управління інформацією (*Fair Information Practice Principles*).

Виконавчий указ № 13691, що сприяє обміну інформацією у сфері кібернетики в приватному секторі, уповноважує Міністерство внутрішньої безпеки[29]:

«Розробити більш ефективні засоби для надання допуску до секретної інформації особам приватного сектору, які є членами Організації з обміну та аналізу інформації (*ISAOs*) через визначену програму захисту критичної інфраструктури.

Здійснювати постійну, спільну та всеохоплюючу координацією з *ISAOs* через *NCCIC*, який координує обмін інформацією у сфері кібербезпеки та проводить аналіз у середовищі партнерів приватного сектору і федерального уряду.

Обирати через відкритий та конкурентний процес неурядову організацію, яка стане Організацією стандартів *ISAOs*. Ця Організація стандартів *ISAOs* визначить набір стандартів або керівних принципів для створення і функціонування *ISAOs*».

Стандарти *ISAOs* базуються на принципах:

- добровільності – участь у формуванні *ISAOs* не є обов'язковою. Скоріше вона має бути абсолютно необов'язковою та добровільною;
- прозорості – за допомогою спільної та відкритої співпраці органи державного та приватного секторів матимуть змогу надавати інформацію про розроблені стандарти;
- інклюзивності – учасники з будь-якого сектору – некомерційного чи комерційного, експертного або новачки, повинні мати можливість брати участь у створенні власної *ISAOs*;
- дієвості – учасники отримають корисний та практичний набір стандартів і найкращих практик як керівництво, якщо вони вирішать брати участь у створенні *ISAOs*;
- гнучкості – стандарти не мають перешкоджати формуванню *ISAOs* або завдавати шкоди поточним процесам існуючих організацій, що здійснюють обмін інформацією.

На сьогодні більшість обмінів інформацією приватного сектору проводяться за допомогою **центрів обміну та аналізу інформації** (*ISACs*). *ISACs* працюють за галузевою моделлю, тобто організації в межах певного сектору (наприклад, фінансових послуг, енергетики, авіації тощо) об'єднуються для обміну інформацією про кіберзагрози. Незважаючи на те, що багато з цих груп вже є потужними елементами ефективної співпраці у сфері кібербезпеки, деякі організації не можуть бути долучені до певного сектору або мають унікальні потреби. Ті організації, які не можуть приєднатись до *ISACs*, але мають потребу в інформації про кіберзагрози, надають перевагу участі в *ISAOs*.

Окремим документом, що фіксує процедури співпраці між приватними компаніями та урядовими установами у сфері інформаційної безпеки є Акт про обмін інформацією у сфері кібербезпеки (*Cybersecurity Information Sharing Act, CISA*)[30]**,** затверджений Конгресом наприкінці 2015 р. Відповідно до нього організації, які на добровільній основі обмінювалися інформацією про кіберзагрози між собою і Федеральним урядом, отримали право обмеженої відповідальності. Документ надає додатковий захист компаніям, що добровільно вирішили ділитися даними про кіберзагрози з урядовими установами. Закон покликаний захистити представників бізнесу від можливих судових позовів з боку користувачів, якщо інформація про кіберзагрози, яка передана органам влади, містить персональні дані.

---

[29] Information Sharing and Analysis Organizations (ISAOs) [Електронний ресурс]. – Режим доступу : https://www.dhs.gov/isao#

[30] Cybersecurity Information Sharing Act of 2015 [Електронний ресурс]. – Режим доступу : https://www.congress.gov/bill/114th-congress/senate-bill/754/text

Акт зобов'язує Міністерство внутрішньої безпеки: 1) одержувати інформацію про кіберзагрози та оборонні заходи, що надаються будь-якою організацією; 2) забезпечити отримання всіма федеральними агентствами такої інформації своєчасно, в режимі реального часу і з використанням автоматизованих систем.

У рамках виконання Акта Міністерство внутрішньої безпеки розробило систему автоматичного обміну індикаторами (*Automated Indicator Sharing, AIS*)[31], яка дозволяє отримувати нові індикатори кіберзагроз від підприємств приватного сектору і урядових організацій автоматично, а також стимулює співпрацю підприємств (організацій) приватного сектору з *NCCIC* у питаннях підготовки їх мереж до автоматичного обміну такими індикаторами. Мета програми *AIS* – автоматичне надання інформації організаціям-учасницям, у т. ч. федеральним міністерствам і агентствам, приватним компаніям і центрам обміну і аналізу інформації (*ISACs*).

У рамках реалізації зазначеного Акта, операційна система *AIS* запрацювала з березня 2016 р., а Міністерство підтвердило, що були розроблені рекомендації щодо сприяння неурядовим організаціям в здійсненні обміну показниками про кіберзагрози з Федеральним урядом. Міністерство також розробляє процедури щодо отримання та використання показників про кіберзагрози федеральними органами, а також керівні принципи щодо приватності та громадянських свобод (у рамках обміну цими показниками), та керівництво для федеральних установ щодо обміну інформацією, якою володіє уряд. Серед цих документів, зокрема, такі[32]:

- Заходи із захисту та обміну індикаторами кіберзагроз (*Sharing of Cyber Threat Indicators and Defensive Measures*);
- Керівництво зі сприяння недержавним суб'єктам щодо обміну індикаторами кіберзагроз та захисних заходів з федеральними органами (*Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities*);
- Заключні процедури, пов'язані з отриманням індикаторів кіберзагроз та захисних заходів (*Final Procedures Related to the Receipt of Cyber Threat Indicators and Defensive Measures*);
- Захист конфіденційності та громадянських свобод. Керівництво: Закон про обмін інформацією в галузі кібербезпеки від 2015 року *(Privacy and Civil Liberties Final Guidelines: Cybersecurity Information Sharing Act of 2015*).

Іншим напрямом реалізації проектів ДПП Міністерства внутрішньої безпеки з приватним сектором для обміну інформацією про кіберзагрози стало укладання **Угод про співпрацю у сфері досліджень і розробок** (*Cooperative Research and Development Agreements, CRADA*)[33], які є частиною реалізації більш всеосяжної Програми зі співробітництва та обміну кіберінформацією (*Cyber Information Sharing and Collaboration Program, CISCP*)[34].

Ключовим напрямом діяльності *CISCP* є двосторонній обмін інформацією: партнери *CISCP* надають індикатори зафіксованих кіберзагроз та інформацію про кіберінциденти та виявлені вразливі місця Міністерству внутрішньої безпеки, які воно потім передає іншим партнерам *CISCP* анонімно та у збірному форматі. Після отримання даних аналітики *CISCP* редагують інформацію про власника та персональну інформацію й аналізують дані у співпраці з державними та галузевими партнерами для вироблення точних, актуальних, своєчасних та аналітичних документів. Наразі це такі документи, як:

---

[31] Automated Indicator Sharing (AIS) [Електронний ресурс]. – Режим доступу : https://www.us-cert.gov/ais

[32] Там само.

[33] Cooperative Research and Development Agreements (CRADAs) [Електронний ресурс]. – Режим доступу : https://www.fda.gov/ScienceResearch/CollaborativeOpportunities/CooperativeResearchandDevelopmentAgreementsCRADAs/default.htm

[34] Cyber Information Sharing and Collaboration Program (CISCP) [Електронний ресурс]. – Режим доступу : https://www.dhs.gov/ciscp

«Бюлетні індикаторів», «Аналітичні звіти», «Пріоритетні оповіщення», «Рекомендовані практики».

Крім іншого, Спільна національна оперативна група кіберрозслідувань (*National Cyber Investigative Joint Task Force, NCIJTF*)[35] спільно з іншими федеральними кіберцентрами та органами **вдосконалюють систему кібербезпеки ФБР (***Cyber Guardian system*), з метою підвищення якості процесу створення і використання звітів про кіберзагрози, а також оповіщення компаній, які вже стали цілями шкідливої кібердіяльності. В рамках цієї діяльності різні кіберцентри створили і поширили понад 10 000 звітів про кіберзагрози і розіслали понад 2 000 повідомлень про них станом на липень 2015 р. Нарешті, в лютому 2015 р. Президент США Б. Обама схвалив створення **Національного центру інтеграції розвідки по кіберзагрози** (*The Cyber Threat Intelligence Integration Center, CTIIC*) з метою підвищення ситуаційного інформування урядових органів США про зовнішні кіберзагрози[36]. CTIIC наразі є національним розвідувальним центром, який пов'язує відповідальних посадових осіб в уряді країни і здійснює аналіз інформації з усіх джерел з метою виявлення кіберзагроз національного масштабу.

Інша модель обміну інформацією здійснюється в **Національному альянсі кіберкриміналістики і кіберпідготовки** (*National Cyber-Forensics* & *Training Alliance*[37], *NCFTA*) – некомерційної корпорації, відповідальної за підтримку співпраці між приватним сектором, дослідницькими організаціями та правоохоронними органами з метою визначення, запобігання і нейтралізації комплексних кіберзагроз. Крім правоохоронних органів штатів і місцевого рівня, а також приватного сектору, в цій ініціативі беруть участь міжнародні представники з Канади, Австралії, Великої Британії, Індії, Німеччини, Нідерландів, України і Литви. *NCFTA* забезпечує своєчасний і спрямований обмін інформацією про кіберзагрози між корпораціями та іншими партнерами, а також безпосередньо співпрацює з експертами у сфері охорони порядку, безпеки бізнесу, а також з дослідницьких кіл, з метою запобігання ризикам і протиправній діяльності, а також для збирання інформації, необхідної для переслідування злочинців.

Співпраця з партнерами сприяла відкриттю безлічі кримінальних та цивільних розслідувань, які інакше могли залишитися поза увагою. На сьогодні *NCFTA* надала розвідувальну інформацію, яка допомогла успішному переслідуванню сотень кіберзлочинців по всьому світу. Крім того, протягом останніх трьох років *NCFTA* підготувала понад 800 звітів про розвідку кіберзахисту.

Ще одним прикладом співпраці є діяльність **Розширеного центру кібербезпеки** (*Advanced Cyber Security Center*)[38] у Бостоні, що є регіональною ініціативою, спрямованою на обмін інформацією. Подібно *NCFTA*, він є некомерційним консорціумом, що об'єднує приватні фірми, університети, а також урядові організації з метою запобігти найбільш комплексним кіберзагрозам.

Центр раз на два тижні проводить зустрічі для обміну інформацією про індикатори загроз і обміну думками з питань потенційно шкідливої діяльності в мережі. Він також займається операціоналізацією автоматичного обміну інформацією для того, щоб учасники могли обмінюватися даними про загрози і методи запобігання їм, а також бере активну участь у дослідницькій роботі в цій сфері, співпрацюючи з приватним сектором і університетами.

Незважаючи на значні зусилля, які докладає уряд у сфері досліджень, більшість інновацій та інвестицій тут реалізуються приватним сектором. Інноваційні центри

---

[35] National Cyber Investigative Joint Task Force [Електронний ресурс]. – Режим доступу : https://www.fbi.gov/investigate/cyber/national-cyber-investigative-joint-task-force

[36] The Cyber Threat Intelligence Integration Center [Електронний ресурс]. – Режим доступу : https://www.dni.gov/index.php/ctiic-who-we-are

[37] National Cyber-Forensics & Training Alliance [Електронний ресурс]. – Режим доступу : http://www.ncfta.net/

[38] Advanced Cyber Security Center [Електронний ресурс]. – Режим доступу : https://www.acscenter.org/

в сфері кібербезпеки з'явилися в Атланті, Остіні, Бостоні, Нью-Йорку, Сіетлі та Кремнієвій долині. Ці центри залучають значні обсяги венчурних інвестицій, що спрямовуються на розробку технологій безпеки, в т. ч. таких, як антивіруси, антиспам-програми, і ПО з протидії зломів мереж. Усього інвестиції в ІКТ у США становили 133 млрд дол., або 41 % від загального обсягу інвестицій у дослідження в країні, що становив 323 млрд дол. станом на 2013 р. За оцінками фахівців, того ж року ІКТ-сектор становив лише 4,6 % від всієї економіки США, але ця частка зростає в останні два роки приблизно на 1 % щороку[39]. З урахуванням високої залежності економіки США від ІКТ-сектору (в т. ч. досліджень у сфері безпеки), уряд США робить спроби розвивати співпрацю з приватним сектором і планує поглиблювати взаємодію між урядом і промисловістю. Так, Міністерство оборони нещодавно запустило програму *Defense Innovation Unit-Experimental (DIUx)*. Програма *DIUx* покликана забезпечити більшу відкритість Міністерства щодо нетрадиційних технічних ідей і прийому на роботу нових фахівців, а також сприяти відкриттю офісів Міністерства у Кремнієвій долині та Бостоні.

Практика встановлення КДПП демонструє, що незважаючи на те, що КДПП можуть бути вигідними як для приватного сектору так і для уряду, не всі приватні компанії налагоджують таке партнерство. Одним із ключових стримуючих факторів стають проблеми довіри, контролю та розкриття інформації. Деякі компанії не прагнуть обмінюватися інформацією з урядом, оскільки уряд не зможе надати всі дані про потенційні злочини, пов'язані з кіберзлочинністю через те, що певна інформація може бути засекречена або конфіденційна, а тому багато компаній вважають, що обмін інформацією не повинен бути одностороннім. Крім того, деякі приватні компанії також непокоїть, що передача конфіденційної інформації може зашкодити їхній репутації або що передана інформація не буде повністю конфіденційною.

[39] Киберготовность США 2.0 [Електронний ресурс]. – Режим доступу : https://digital.report/kibergotovnost-ssha-2–0-vvedenie/

Розділ 3. КДПП В ЄВРОПЕЙСЬКИХ КРАЇНАХ

3.1. Спільноєвропейські підходи до КДПП

Сучасний стан *acquis communautaire*[40] у сфері кібербезпеки на загальноєвропейському рівні перебуває в точці свого найінтенсивнішого розвитку. З огляду на системність характеру загроз для кібербезпеки у поєднанні із постійним зростанням кіберзлочинності в останні роки, Європейська Комісія у співпраці з країнами – членами ЄС, іншими інституціями Європейського Союзу та відповідними зацікавленими сторонами розробила узгоджену політику дій, що має регулювати цей сектор.

Згідно з проведеним у 2017 р. *PricewaterhouseCoopers* опитуванням[41], щонайменше 80 % європейських компаній засвідчили принаймні про один інцидент протягом останніх трьох років у сфері кібербезпеки.

У липні 2016 р. Європейська Комісія після низки громадських консультацій з усіма зацікавленими сторонами підписала угоду у сфері індустрії кібербезпеки, тим самим активізувавши зусилля, спрямовані на боротьбу з кіберзагрозами у формі КДПП[42].

План дій, ініційований Європейською Комісією (*Agreement with industry on cybersecurity and steps up efforts to tackle cyber-threats*)[43], окреслив рамки КДПП, що надалі регулюватимуть цю сферу, її правові та економічні відносини. На реалізацію цієї стратегії було виділено 450 млн євро, основним джерелом перерозподілу коштів є програма досліджень та інновацій «Горизонт 2020». Також учасники ринку кібербезпеки, представлені Європейською організацією з кібербезпеки (*ECSO*), задекларували намір щодо реалізації своїх інвестицій у рамках цієї ініціативи.

Метою партнерства є створення платформи для кібербезпеки різних секторів (таких як енергетика, охорона здоров'я, транспорт та фінанси, а також включення у цей процес органів влади, науково-дослідних центрів та інших зацікавлених сторін), яка розвивала б дослідницький та інноваційний потенціал сектору. Така співпраця покликана зменшити негативний ефект роздробленості ринку кібербезпеки ЄС, його неповної врегульованості, що демонструє різниця у процедурах сертифікації, з тим, щоб кожен

---

[40] *Acquis communautaire* (з фр. – *доробок спільноти*) сукупність спільних прав і зобов'язань, обов'язкових до виконання для усіх країн – членів ЄС. Доробок постійно змінюється і узагальнюється. Правова система Європейського Союзу включає акти законодавства Європейського Союзу (але не обмежується ними), прийняті в рамках Європейського співтовариства, Спільної зовнішньої політики та політики безпеки і Співпраці у сфері юстиції та внутрішніх справ.

[41] Огляд глобального стану інформаційної безпеки 2017 [Електронний ресурс]. – Режим доступу : http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html

[42] Комісія підписує угоду з галуззю про кібербезпеку та активізує зусилля, спрямовані на боротьбу з кіберзагрозами [Електронний ресурс]. – Режим доступу : http://europa.eu/rapid/press-release_IP-16–2321_en.htm

[43] Ibidem [Електронний ресурс]. – Режим доступу : http://europa.eu/rapid/press-release_IP-16–2321_en.htm

постачальник послуги у сфері кібербезпеки міг реалізувати свою діяльність у кожній країні – члені ЄС, однаково легко уникаючи політики протекціонізму.

Ці рамки співпраці підкреслюють особливу важливість інновацій, що з'являються на перетині інтересів згаданих вище учасників ринку – від нішевих ринків на кшталт криптографії, з одного боку, до добре розвинених ринків з новими бізнес-моделями (наприклад, ринку антивірусного програмного забезпечення). Цією ініціативою Європейська Комісія намагалась полегшити доступ до виходу на нові ринки підприємствам малого та середнього бізнесу, що працюють у сфері кібербезпеки.

Основою загального плану дій слугують Стратегія єдиного цифрового ринку 2015 р. (*Digital Single Market Strategy for Europe*)[44], Кіберстратегія Європейського Союзу 2013 р. (*Cyber Security Strategy of the European Union: An Open, Safe and Secure Cyberspace*)[45] та Директива ЄС щодо мережевої та інформаційної безпеки (*NIS Directive on security of network and information systems*) (має бути включена в національне законодавство країн – членів ЄС до 9 травня 2018 р. та у внутрішні статутні документи основних підприємств до 9 листопада 2018 р.)[46].

Ухвалена у 2013 р. Європейська стратегія кібербезпеки[47] визначила спільне бачення Європейської Комісії та Високого представника Європейського Союзу із закордонних справ та політики безпеки щодо відкритого та безпечного кіберпростору.

Стратегія визначає основні пріоритети, що регулюють проблеми як внутрішньоєвропейського, так і міжнародного законодавства. Пріоритети цієї ініціативи стосуються підвищення рівня захисту та стійкості європейських мереж та розвитку промислових і технологічних ресурсів для забезпечення кібербезпеки.

Відповідно до Стратегії у 2013 р. Європейська Комісія запропонувала перший всеосяжний елемент законодавства ЄС щодо кібербезпеки – Директиву ЄС щодо мережевої та інформаційної безпеки (*NIS Directive on security of network and information systems*), ухвалену Європейським Парламентом 6 липня 2016 р. і яка набрала чинності в серпні 2016 р.[48]. Після трьох років переговорів цей документ був ухвалений із поправками, далі відбулася його імплементація на національному рівні.

Також *NIS* передбачила створення координаційного механізму реагування держав-членів у співпраці з приватним сектором на погрози та власне самі кібератаки, тим самим сприяючи стратегічному співробітництву та обміну інформацією і підтримуючи рівень довіри між учасниками процесу. Комісія також запустила державно-приватну платформу на рівні ЄС – т. зв. Платформу мережевої та інформаційної безпеки *(Network and Information Security (NIS) public private Platform)*[49] для визначення ефективної практики кібербезпеки з метою сприяння подальшому впровадженню Директиви. Результатом діяльності Платформи у III кварталі 2015 р. став Стратегічний порядок денний

---

[44] Цифровий єдиний ринок [Електронний ресурс]. – Режим доступу : https://ec.europa.eu/commission/priorities/digital-single-market_en ; Communication from the Commission to the European Parliament, the Council, the European economic and social committee and the Committee of the regions [Електронний ресурс]. – Режим доступу : http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015DC0192

[45] Повідомлення про стратегію кібербезпеки Європейського Союзу – відкритий та безпечний кіберпростір [Електронний ресурс]. – Режим доступу : https://ec.europa.eu/digital-single-market/en/news/communication-cybersecurity-strategy-european-union-%E2 %80 %93-open-safe-and-secure-cyberspace

[46] Директива про захист мережевих та інформаційних систем (Директива щодо ННД) [Електронний ресурс]. – Режим доступу : https://ec.europa.eu/digital-single-market/en/news/directive-security-network-and-information-systems-nis-directive

[47] Стратегія кібербезпеки Європейського Союзу: відкритий та безпечний кіберпростір [Електронний ресурс]. – Режим доступу : http://eur-lex.europa.eu/procedure/EN/202369

[48] Директива Європейського Парламенту та Ради (ЄС) 2016/1148 від 6 липня 2016 року щодо заходів щодо забезпечення високого загального рівня безпеки мережевих та інформаційних систем у всьому Союзі [Електронний ресурс]. – Режим доступу : http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

[49] NIS Платформа – Перша зустріч робочих груп [Електронний ресурс]. – Режим доступу : https://ec.europa.eu/digital-single-market/en/news/nis-platform-kick-meeting-working-groups

дослідження кібербезпеки (*SRA – Cybersecurity Strategic Research Agenda*) на базі Платформи мережевої та інформаційної безпеки[50].

Окрім перелічених вище ініціатив, Європейська Комісія через *FP7* та *CIP* (Сьому Рамкову програму та Програму з конкурентоспроможності та інновацій) фінансує ще низку проектів з кібербезпеки.

Відповідно до Постанови (ЄС) № 460/2004 Європейське співтовариство в 2004 р. заснувало *ENISA*[51] з метою сприяння забезпеченню високого рівня розвитку культури інформаційної безпеки в межах ЄС. Пропозиція щодо модернізації мандата *ENISA* була прийнята 30 вересня 2010 р.[52]. Нормативно-правова база електронних засобів зв'язку, що діяла з листопада 2009 р., передбачала зобов'язання щодо безпеки постачальників електронних засобів зв'язку[53], а також зобов'язання країн-членів до травня 2011 р. транспонувати ці положення у законодавство на національному рівні.

Відтак, усі сторони, у віданні яких є персональні дані, – наприклад, банки чи лікарні, відповідно до нормативно-правової бази захисту даних були зобов'язані вжити заходів безпеки для захисту цих персональних даних. Крім того, відповідно до пропозиції Європейської Комісії від 2012 р. щодо Загального регулювання захисту даних[54], т. зв. «контролери даних» повинні повідомляти національні наглядові органи про порушення режиму персональних даних.

Відповідно до Директиви Ради ЄС 2008/114 від 8 грудня 2008 р. про ідентифікацію та проектування європейської критичної інфраструктури та оцінку необхідності покращення її захисту (*Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection* (*Text with EEA relevance*) в Європейській програмі захисту критично важливої інфраструктури[55] визначено загальний «парасольковий» підхід до захисту критично важливої інфраструктури в ЄС. Директива про безпеку мережі та інформаційних систем повинна застосовуватися без шкоди для Директиви 2008/114.

На міжнародному рівні ЄС працює над кібербезпекою як на двосторонньому, так і на багатосторонньому рівнях. На саміті ЄС–США 2010 р.[56] було створено робочу групу з питань кібербезпеки та кіберзлочинності. Також є низка мультилатеральних угод щодо співпраці у цій сфері з Організацією економічного співробітництва та розвитку, Генеральною Асамблеєю Організації Об'єднаних Націй, Міжнародним союзом електрозв'язку, Організацією з безпеки та співробітництва в Європі, Всесвітнім самітом з питань інформаційного суспільства (*WSIS*) та Форумом з питань управління Інтернетом (*IGF*). 6 травня 2015 р. Європейська Комісія прийняла Стратегію єдиного ринку цифрових

---

[50] Resilience and security of communication infrastructure, networks and services [Електронний ресурс]. – Режим доступу : https://goo.gl/mK4irQ

[51] Регламент (ЄС) № 460/2004 Європейського Парламенту та Ради ЄС від 10 березня 2004 р. про створення Агенства ЄС з питань мережевої та інформаційної безпеки [Електронний ресурс]. – Режим доступу : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460: EN: HTML

[52] Регламент Європейського Парламенту та Ради Європи щодо Агенства ЄС з питань мережевої та інформаційної безпеки (ENISA) [Електронний ресурс]. – Режим доступу : http://ec.europa.eu/smart-regulation/impact/ia_carried_out/docs/ia_2010/sec_2010_1126_en.pdf

[53] Статті 13a та 13b Рамкової директиви.

[54] Пропозиція до Регламенту Європейського Парламенту та Ради про захист фізичних осіб стосовно обробки персональних даних та вільного переміщення таких даних (Загальні положення про захист даних) [Електронний ресурс]. – Режим доступу : http://eur-lex.europa.eu/procedure/EN/201286

[55] Директива Ради ЄС 2008/114/ЄС від 8 грудня 2008 р. про визначення європейських критичних інфраструктур та оцінку необхідності покращення їх захисту [Електронний ресурс]. – Режим доступу : http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32008L0114

[56] Саміт ЄС–США, 20 листопада 2010 р., Лісабон – Спільна заява [Електронний ресурс]. – Режим доступу : http://europa.eu/rapid/press-release_MEMO-10-597_en.htm

технологій (*DSM*)[57]. Така політика стала ще одним із аспектів для регулювання КДПП у сфері технологій та рішень для забезпечення мережевої безпеки впродовж 2016 р.

Незважаючи на те, що КДПП є вигідним для обох секторів, деякі приватні компанії зволікають із дотриманням законодавства у цій сфері. Одним із ключових каменів спотикання є питання довіри, контролю та розкриття корпоративної інформації.

Компанії мають сумнів стосовно залучення уряду до розслідування справи після того, як кібератака на їхню компанію вже відбулась, позаяк це передбачає відкриття доступу до приватних даних компанії. Серед представників приватного сектору побутує думка, що участь уряду лише ускладнить ситуацію. Крім того, у момент, коли приватна компанія залучає урядовий орган до розслідування кібератаки, компанія втрачає автономію щодо такого розслідування.

Оскільки певна інформація може бути класифікована як конфіденційна, багато компаній вважають, що обмін інформацією призведе до потенційних втрат позиції на ринку[58]. Крім того, деякі приватні компанії також можуть непокоїтись, що передача конфіденційної інформації може зашкодити їхній репутації, тобто що відкрита для урядового розслідування інформація після завершення такого розслідування не залишиться конфіденційною[59].

Ще однією проблемою є складний регуляторний і правовий ландшафт у сфері кібербезпеки, у випадку порушення якого приватні компанії можуть бути змушені до більшого, ніж реалізація стандартних зобов'язань щодо розкриття інформації, а саме розкривати потенційні ризики уряду, Міністерству юстиції або навіть позивачам, які можуть постраждати від кіберзлочину.

Загалом же приватні компанії відзначили відсутність довіри як ключову причину вагання щодо державно-приватної співпраці у цьому секторі[60].

Для того щоб зміцнити довіру між учасниками процесу, в Нідерландах створили безпечну мережу інформації, до якої Уряд отримує безпосередній доступ лише після того, як компанія висловить щодо цього свою згоду[61].

У такій моделі представники державного та приватного секторів працюють у спільній платформі над побудовою довіри, розвитком співробітництва та діалогу, враховуючи інтереси усіх учасників процесу.

Така співпраця стимулює створення нових послуг і розвиває індустрію власних програмних продуктів, поліпшує взаємодію суспільства і держави, а також підвищує прозорість діяльності та довіру до органів влади. Беручи до уваги цілі, викладені в Угоді[62], Європейська Комісія розглянула такі сценарії, пов'язані зі зміцненням індустрії кіберзахисту в Європі. Запропоновані варіанти були ретельно відібрані після аналізу доказів з різних джерел, включаючи дослідження ринку кібербезпеки, а також аналіз точок зору під час громадських консультацій, у яких взяли участь більш ніж 250 різних організацій, що представляють як попит так і пропозицію у сфері індустрії кібербезпеки.

Ініціатива Європейської Комісії у сфері КДПП поклала початок розвитку довгострокової конкурентоспроможності та інновацій європейської кібербезпеки, втім сама

---

[57] Спільний цифровий ринок [Електронний ресурс]. – Режим доступу : https://ec.europa.eu/commission/priorities/digital-single-market/

[58] Партнерства у сфері кібербезпеки: нова ера державно-приватної співпраці [Електронний ресурс]. – Режим доступу : http://www.lawandsecurity.org/wp-content/uploads/2016/08/Cybersecurity.Partnerships-1.pdf

[59] Партнерство між державним та приватним секторами не є срібною кулею: розширена модель управління критичною інфраструктурою [Електронний ресурс]. – Режим доступу : http://www.sciencedirect.com/science/article/pii/S1874548209000274

[60] Вивчення синергії між цивільним населенням та ринками захисту кібербезпеки [Електронний ресурс]. – Режим доступу : https://goo.gl/uLXE43

[61] Формування державно-приватного партнерства в сфері кібербезпеки [Електронний ресурс]. – Режим доступу : http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1478&context=jss

[62] Комісія підписує угоду з бізнесом про кібербезпеку та активізує зусилля, спрямовані на боротьбу з кіберзагрозами [Електронний ресурс]. – Режим доступу : http://europa.eu/rapid/press-release_IP-16–2321_en.htm

по собі вона ще не є механізмом подолання проблеми розбалансованості внутрішнього ринку у сфері кібербезпеки.

З огляду на це, після ретельного аналізу та консультацій із зацікавленими сторонами, Європейська Комісія продовжує роботу над додатковими заходами, що дозволятимуть європейським громадянам, підприємствам (включаючи малі та середні), органам державної влади отримувати доступ до цифрових технологій безпеки, найкращих практик забезпечення інформаційної інфраструктури.

Одним із інструментів у цій ситуації є розбудова механізму **економічних кластерів**, які можна широко визначити як групу економічних суб'єктів та інституцій, які територіально розташовані неподалік і мають достатні масштаби для розвитку спеціалізованої експертизи, послуг, ресурсів, умінь та навичок. Співпрацюючи разом, малі та середні підприємства можуть бути більш інноваційними, створювати більше робочих місць та реєструвати більше міжнародних товарних марок та патентів, ніж ті, що працюють відокремлено.

Приналежність до кластеру дозволяє компаніям, які беруть участь в ініціативі, підвищити конкурентоспроможність і, таким чином, досягти більшої продуктивності, головним чином, шляхом її підвищення завдяки покращенню доступу до спеціалізованих постачальників, технологій та інформації та більш високому інноваційному потенціалу співпрацюючих компаній. Це пов'язано з передачею знань, генерацією нових ідей та акцентуванням на інноваціях. Кластери – переважно ринкове явище, найуспішніші з них створюються спонтанно внаслідок природних конкурентних переваг на ринку.

Окремим напрямком політики ЄС цей підхід став наприкінці 1990-х років, з того часу бізнес-ініціативи, вищі навчальні заклади та науково-дослідні інститути сприяли розвитку та появі нових типів державної політики, діючи як каталізатор і допомагаючи розкрити економічний та науковий потенціал окремих регіонів. У цьому контексті в Європейському Союзі більшість кластерів, що зосереджують увагу на кібербезпеці, можна знайти в Західній Європі (*G4C* у Німеччині, що успішно заохотив уряд підтримувати розвиток 17 регіональних кластерів кібербезпеки, *Pôle d'Excellence Cyber* – у Франції, Гаазький дельта-кластер – у Нідерландах або *INCIBE* – в Іспанії), нові ініціативи починають з'являтися також у Центральній та Східній Європі, наприклад, у Чехії та Естонії.

З метою вироблення майбутньої стратегії КДПП Європейська Комісія провела ряд громадських консультацій із зацікавленими сторонами. Старт онлайн-консультаціям було дано 18 грудня 2015 р. на 12 тижнів з метою зібрати різні погляди щодо питання функціонування єдиного європейського ринку у сфері кібербезпеки. Це супроводжувалося дорожньою картою[63] кращого регулювання для КДПП.

Водночас провідними європейськими гравцями сфери кібербезпеки була заснована Європейська робоча група лідерів кібербезпеки. Вона працювала над низкою конкретних рекомендацій для європейських громадян, бізнесу та промислової політики щодо питань кібербезпеки. До складу робочої групи входили *Airbus Group*, *Atos*, *BBVA*, *BMW*, *Cybernetica*, *Deutsche Telekom*, *Ericsson*, *F-Secure*, *Infineon* та *Thales*.

Група представила доповідь комісару Етьєнгері у січні 2016 р. на Міжнародному форумі з кібербезпеки у Ліллі. В доповіді[64] висвітлюються рекомендації щодо заходів, спрямованих на підвищення надійності в ЄС, а також рекомендується успішний досвід європейських лідерів з кібербезпеки. Після проведення громадських консультацій вдалося виявити і низку важливих тенденцій:

---

[63] Державно-приватне партнерство з питань кібербезпеки [Електронний ресурс]. – Режим доступу : http://ec.europa.eu/smart-regulation/roadmaps/docs/2015_cnect_004_cybersecurity_en.pdf

[64] Лідери європейської індустрії кібербезпеки [Електронний ресурс]. – Режим доступу : http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=13326

- більшість респондентів позитивно реагували на ініціативу Комісії щодо КДПП, наголошуючи на важливості стратегічної спрямованості такої співпраці;
- критична інфраструктура, фінанси та банківська діяльність, енергетика та охорона здоров'я розглядалися учасниками опитування як такі, що можуть принести найбільше соціально-економічних збитків у випадку великої кібератаки;
- серед респондентів відзначався загальний консенсус щодо пріоритетності захисту критичної інфраструктури. Значна частина респондентів зазначила, що на європейському ринку бракує необхідних товарів та послуг для забезпечення безперервного і цілісного потоку зв'язків у сфері кібербезпеки. Це, зокрема, стосується систем виявлення кібернападів та управління безпекою інформації та подій, достатньої кількості програмного та апаратного забезпечення, криптографічних стандартів і надійних хмарних сервісів;
- багато респондентів висловили думку стосовно слабкої внутрішньоринкової конкурентності, але також зазначили про слабкість конкурентоспроможності іззовні ЄС. Хоча деякі європейські продукти та послуги, на думку респондентів, є конкурентоспроможними із їхніми відповідниками з інших частин світу, постачальники в різних країнах ЄС часто працюють у нішевих ринках, тому не можуть швидко та без значних втрат долати національні кордони, що впливає на їх цінову конкурентоспроможність;
- більшість респондентів, особливо зі сфери малого та середнього бізнесу, наголосили на проблемах, пов'язаних із доступом до ресурсів для фінансування проектів та ініціатив у сфері кібербезпеки. Фонди ЄС, венчурні фонди та банківські кредити розглядаються як найбільш зручні фінансові інструменти для стимулювання зростання бізнесу;
- більшість респондентів виявили, що стандартизація підтримувала інновації, оскільки сприяла сумісності, надаючи перевагу комбінованому підходу до стандартизації – горизонтальним та багатогалузевим зв'язкам. На питання про майбутнє фокусування на сфері стандартизації серед респондентів було досягнуто міцного консенсусу щодо захисту критично важливої інфраструктури;
- учасники опитування поділилися низкою ідей щодо того, як може працювати схема сертифікації, – починаючи з єдиного європейського рівня, відповідального за визначення будь-яких необхідних стандартів або вимог і закінчуючи угодами про взаємне визнання, що залишаються центральними[65]. Водночас значна частка респондентів заявила, що вони не знають, чи взаємовизнаються схеми сертифікації, роблячи припущення, що наразі вони не є взаємно визнаваними в усіх країнах – членах ЄС;
- багато учасників консультацій висловили думку про необхідність інтенсифікувати обмін інформацією між приватними структурами та урядом у сфері розвідувальної інформації в секторі інформаційної безпеки, оскільки питання кібербезпеки є, за своєю сутністю, транскордонною проблемою.

3.2. Досвід Німеччини

Німеччина є однією з ключових країн, форми КДПП якої виконують роль одного з основних інструментів ефективної системи кіберзахисту країни.

За даними цифрової промислової асоціації Німеччини *Bitkom*, 53 % німецьких компаній уже стали жертвами економічного кібершпигунства[66]. Згідно з опитуванням «Захист бізнесу в цифровому світі» (*Business Protection in the Digital World*), щороку втрачається понад 55 млрд євро через шпигунство, саботаж або крадіжку даних у німецькій

[65] Звернення Комісії до Європейського Парламенту, Ради ЄС, Європейського економічного і соціального комітету та Комітету регіонів. Зміцнення європейської системи кібернетичної стійкості та сприяння розвитку конкурентоспроможної та інноваційної кібербезпеки [Електронний ресурс]. – Режим доступу : https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52016DC0410

[66] Захист бізнесу в цифровому світі [Електронний ресурс]. – Режим доступу : https://goo.gl/Rmp5ZP

промисловості. В опитуванні взяли участь 1 069 менеджерів та співробітників служби охорони[67].

Згідно з аналізом *Bitkom* та Німецької внутрішньої розвідувальної служби (*BfV*), після кібератаки за допомогою до уряду звернулися менше третини компаній. Основною мотивацією неповідомлення про кібератаку є небажання завдати шкоди репутації. Промисловість у плані технологічної просунутості набагато випереджає своїх урядових партнерів. А уряд має можливість сприяти адміністративним ресурсам, на які приватний сектор не має законного впливу.

На стратегічному та операційному рівні Федеральний уряд Німеччини, послуговуючись цілісним підходом до захисту критичної інфраструктури, що здійснюється в рамках впровадження Національної стратегії для захисту критичної інфраструктури (стратегія *CIP*), у 2005 р. розробив та почав втілювати План ДПП КРІТІС (*Umsetzungsplan KRITIS*), який уже в 2006 р. почав реалізуватись у співпраці з операторами критичної інфраструктури. З опублікуванням плану імплементації у 2007 р. це державно-приватне співробітництво під назвою «*UP KRITIS*» почало діяти.

Його головною метою є покращення захисту критичної інфраструктури у різних секторах безпеки. У Німеччині підприємства та об'єкти у сфері постачання енергетики, інформаційних технологій та телекомунікації, транспорту та торгівлі, охорони здоров'я, продовольчого та водопостачання, фінансово-страхового сектору, державного та адміністративного управління, а також засобів масової інформації та культури є складовими критичної інфраструктури держави.

Одним із напрямів ДПП, ініційованого Німеччиною, є заохочення співпраці між державними та приватними організаціями на ранніх етапах дослідницького та інноваційного процесу у країні (та в Європейському Союзі загалом) з метою синхронізації доступу до інноваційних та надійних європейських рішень – продуктів, послуг та програмного забезпечення для ІКТ.

З метою впорядкування кібербезпекової складової сфери ДПП у Німеччині було ухвалено ряд нормативно-правових документів – як загального, так і більш спеціального спрямування.

Передусім Німеччина ще в 2009 р. ратифікувала Конвенцію Ради Європи про кіберзлочинність[68] (підписала її в 2001 р.) та активно імплементує її положення. Крім того, Німеччина підписала та ратифікувала додаткові протоколи до Конвенції про кіберзлочинність, які стосуються криміналізації расистських та ксенофобських дій, здійснених через комп'ютерні системи.

Кримінальний кодекс Німеччини регулює сферу кібернетичних злочинів у частині визначення понять, суті злочину та наслідків за вчинений злочин на кшталт комп'ютерного шахрайства, втручання в дані, комп'ютерного саботажу, корпоративного шпіонажу даних, фішингу, а також інших злочинних дій у кіберпросторі[69].

Розділи 93–95 Кримінального кодексу Німеччини пов'язані з визначенням таємниць національної безпеки[70], а § 4 закону 1994 р. «Про необхідність класифікації даних»[71], що вважаються таємними та критичними для захисту суспільних інтересів, окреслює чотирирівневу систему рівнів засекречування. Рівні призначаються відповідно до рівня ризику, пов'язаного із розголошенням секретної інформації.

---

[67] Короткий звіт 2016 р. Звіт про захист Конституції [Електронний ресурс]. – Режим доступу : https://goo.gl/j36SEV

[68] Конвенція про кіберзлочинність [Електронний ресурс]. – Режим доступу : http://zakon0.rada.gov.ua/laws/show/994_575

[69] Федеральне міністерство юстиції та захисту прав споживачів (2015) [Електронний ресурс]. – Режим доступу : https://www.gesetze-im-internet.de/englisch_stgb/

[70] Кримінальний кодекс Німеччини [Електронний ресурс]. – Режим доступу : https://www.gesetze-im-internet.de/englisch_stgb/

[71] Інтернет-законодаство Німеччини [Електронний ресурс]. – Режим доступу : http://www.gesetze-im-internet.de/

Національна стратегія захисту критичної інфраструктури 2009 р. (Стратегія *CIP*)[72] хронологічно була першим стратегічним документом, що містить відповідні визначення «критичної інфраструктури» та «захисту від атак на критичну інфраструктуру»[73].

Наступним кроком у стратегічному плануванні став Національний план захисту інформаційної інфраструктури, який у 2011 р. було перейменовано у Національну стратегію кібербезпеки[74], – це посилило можливості правоохоронних органів, Федеральної агенції та приватного сектору в боротьбі з кіберзлочинністю, а також акцентувало на захисті країни від шпигунства та саботажу. Саме ця стратегія окремим розділом прописує рамку спільних інститутів для бізнесу/приватного сектору та правоохоронних органів, і як це сформульовано в Законі «Про інформаційну безпеку» (*IT-Sicherheitsgesetz*) 2015 р., усі подальші кроки мають узгоджуватися з ним[75]. Додаткового розвитку сфера КДПП отримала у Стратегії кіберзахисту 2016 р. (*Cyber Sicherheits Strategie*)[76].

Безпосередньо сфера КДПП між операторами критично важливої інфраструктури та відповідними державними органами регулюється планом реалізації *Umsetzungsplan KRITIS des Nationalen Plans zum Schutz der Informationsinfrastrukturen* 2014 р.[77]. Однією з пріоритетних цілей КДПП, закріплених у законодавстві під назвою *UP KRITIS,* є «спільна оцінка кібербезпеки та реакція на неї»[78]. Ця національна ініціатива між державою Німеччина та операторами критичної інфраструктури ініційована з метою захисту стратегічної інформаційної інфраструктури.

Ключовим документом, що впливає на реальні форми КДПП, залишається Стратегія кібербезпеки Німеччини, ухвалена в 2011 р. як комплексна стратегія, що включає основоположні принципи, чіткі цілі та план впровадження стратегічних напрямів та завдань, спрямованих на:

- захист критичної інфраструктури та IT-систем;
- зміцнення інформаційної безпеки державного управління шляхом об'єднання у єдину федеральну мережу;
- створення Національного центру кіберреагування;
- створення Національної ради з питань кіберзлочинності для покращення співпраці між державним сектором та приватним сектором;
- сприяння ефективній міжнародній координації кібербезпеки;
- розвиток інновації в IT-індустрії;
- підготовку кваліфікованого персоналу для федеральних органів влади;
- ефективне використання інструментів державного сектору, таких як законодавчі повноваження, для боротьби з насильством у сфері кібератак[79].

Національна стратегія кіберзахисту 2011 р. уповноважила Федеральну агенцію з питань інформаційної безпеки (*BSI*) створити Національний центр кіберреагування (*National CyberAbwehrzentrum, NCAZ BSI*), який би забезпечував кращу координацію дій щодо атак та більш оперативний обмін інформацією між урядом та приватним сектором. *NCAZ BSI* створює умови усім компетентним органам для оперативного реагування

---

[72] National Strategy for Critical Infrastructure Protection (CIP Strategy) [Електронний ресурс]. – Режим доступу : http://ccpic.mai.gov.ro/docs/Germania_cip_stategy.pdf

[73] Там само. П. 7, С. 9.

[74] Стратегія кібербезпеки Німеччини [Електронний ресурс]. – Режим доступу : https://goo.gl/T5XkLn

[75] Закон Німеччини про інформаційну безпеку [Електронний ресурс]. – Режим доступу : https://goo.gl/otKwQi

[76] Стратегія кібербезпеки Німеччини 2016 [Електронний ресурс]. – Режим доступу : https://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf

[77] План впровадження КРИТИС – Національного плану з охорони об'єктів інформаційної інфраструктури [Електронний ресурс]. – Режим доступу : https://goo.gl/TUur3h

[78] План впровадження КРИТИС [Електронний ресурс]. – Режим доступу : https://goo.gl/DJZQgG

[79] Стратегія кібербезпеки Німеччини [Електронний ресурс]. – Режим доступу : https://goo.gl/XHZYSt

на серйозні інциденти, а також проводить аналіз та оцінку небезпек, координує співпрацю з місцевими та галузевими організаціями із врегулювання кризових ситуацій[80].

Окрім прямої участі Федеральної агенції з питань захисту Конституції (*Bundesamt für Verfassungsschutz, BfV*) та Федерального відомства з питань цивільного захисту та ліквідації наслідків стихійних лих (*Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, BBK*), усі інші урядові органи, що займаються питаннями кібербезпеки, у т. ч. Федеральна служба кримінальної поліції (*Bundeskriminalamt, BKA*), Федеральна поліція (*Bundespolizei, BPOL*), Митна кримінологічна служба (*Zollkriminalamt, ZKA*), Федеральна розвідувальна служба (*Bundesnachrichtendienst, BND*), Бундесвер та інші органи, що здійснюють нагляд за критичною інфраструктурою та операторами у рамках центру, активно співпрацюють з приватним сектором.

Німеччина провела кілька національних навчань з питань кібербезпеки для державних установ та окремих операторів критичної інфраструктури. Одне з них – у 2011 р. – стосувалося підготовки до кризових ситуацій і було спрямоване на розуміння урядом механізму реагування на багатосторонні атаки, включаючи розподілені атаки типу «відмова в обслуговуванні» (*DDoS*), напади на критичну інфраструктуру, потрапляння шкідливих програм у банківські системи та втручання в координацію систем управління руху літаків[81]. Німеччина також бере участь у багатонаціональних навчаннях, організованих Європейським Союзом та Організацією Північноатлантичного договору (НАТО). Незважаючи на кількість навчань, проведених в останні роки, план впровадження центру рекомендував провести більше «вправ для перевірки та оновлення існуючих концепцій». Нарешті, внутрішня розвідувальна служба Німеччини *BfV* публікує щорічні звіти про кіберзагрози, до прикладу, в доповіді 2016 р. зазначено, що Росія та Китай є провідними джерелами кібератак на Німеччину.

Інституційна спроможність Німеччини реалізовувати цілі Стратегії забезпечується низкою державних безпекових інституцій: Німецьким національним центром кіберреагування (*Das Nationale Cyber-Abwehrzentrum* (*NCA*) */ German National Cyber Response Centre*)[82], Федеральною агенцією з питань інформаційної безпеки (*BSI*) та Федеральною агенцією кримінальної поліції (*BKA*), які спільно протидіють кіберзлочинності.

Федеральна агенція з питань інформаційної безпеки (*BSI*)[83] вивчає ризики безпеці, пов'язані з використанням ІКТ, та розробляє превентивні заходи безпеки, надає інформацію про ризики та загрози, пов'язані з використанням інформаційних технологій, і пропонує вирішення проблем[84]. Робота цієї агенції включає також тестування ІТ-безпеки та оцінку ІКТ-систем, у т. ч. їх розробку у співпраці з представниками галузі. Навіть у технічно захищених інформаційних та телекомунікаційних системах ризики та збитки можуть виникнути внаслідок неадекватного адміністрування або неналежного використання. Щоб звести до мінімуму ці ризики або уникнути їх, агенція працює з різними цільовими групами, у т. ч. консультує виробників, дистриб'юторів та користувачів інформаційних технологій, а також аналізує розвиток та тенденції розвитку інформаційних технологій. Агенція має п'ять департаментів, один центральний та чотири спеціалізовані

---

[80] Стратегія кібербезпеки Німеччини [Електронний ресурс]. – Режим доступу : https://goo.gl/XHZYSt

[81] Best Practices in Computer Network Defense: Incident Detection and Response [Електронний ресурс] // NATO Science for Peace and Security Series – D: Information and Communication Security. – IOS Press. – February 2014. – Vol. 35. – P. 12. – Режим доступу : https://www.iospress.nl/book/best-practices-in-computer-network-defense-incident-detection-and-response/

[82] Стратегія кібербезпеки Німеччини [Електронний ресурс]. – P. 28. – Режим доступу : https://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf

[83] Федеральне агентство вищого рівня, яке відповідає за управління ІКТ та забезпечення безпеки зв'язку для уряду Німеччини. Сфера його компетенції та відповідальності включає безпеку комп'ютерних систем, захист критичної інфраструктури, безпеку Інтернету, криптографію, контрслужбу, сертифікацію продуктів безпеки та акредитацію лабораторій тестування безпеки. Агенство розташоване у Бонні, у ньому працюють понад 600 співробітників.

[84] Федеральне відомство з безпеки інформаційних технологій [Електронний ресурс]. – Режим доступу : https://www.bsi.bund.de/EN/TheBSI/Functions/functions_node.html

підрозділи. Кожен відділ складається з одного-трьох підрозділів, кожен з яких у свою чергу – з ряду структурних підрозділів[85].

Як національний орган з питань кібербезпеки для Німеччини Агенція формує політику та діяльність інформаційної безпеки через запобігання, виявлення та реагування. Агенція видає попередження про шкідливе програмне забезпечення та вразливі місця в IT-продуктах і сервісах, поширює інформацію як серед зацікавлених сторін, так і широкої громадськості, і рекомендує контрзаходи. Агенція також відповідає за підтримку інформаційного обміну із понад 50 000 приватними установами[86].

Німеччина має мережу комп'ютерних служб кризового реагування (*network of computer emergency response teams – CERTs*) з національною *CERT – CERT-BUND*[87], тісно співпрацюючи з державним органами та неурядовими структурами кризового реагування.

У Німеччині з 1991 р. було створено кілька груп *CERT* та їх еквівалентів. У 1994 р. Агенція створила першу комп'ютерну команду із надзвичайних ситуацій (*BSI–CERT*) для федеральних установ як віртуальну структуру, що зосереджувала свої зусилля на збиранні інформації. У 2001 р. *BSI–CERT* було перейменовано у *CERT-Bund*, який слугував центральною платформою комунікації для здійснення превентивних, реактивних та активних заходів щодо інцидентів у сфері кібербезпеки. Сьогодні *CERT-Bund* тісно співпрацює як із державними, так і з неурядовими *CERT*.

Німецький національний центр кіберреагування (*Nationales Cyber-Abwehrzentrum, NCAZ / German National Cyber Response Centre*), що був створений у 2011 р., об'єднує ресурси з кіберзахисту Федеральної агенції з питань інформаційної безпеки, Федерального відомства із захисту Конституції, Федеральної розвідувальної служби, Федеральної поліції, слідчого управління митниці Німеччини, Бундесверу, Федерального управління цивільного захисту та допомоги при стихійних лихах і Федерального відомства кримінальної поліції, а також співпрацює з наглядовими органами операторів критично важливої інфраструктури в межах своїх статутних обов'язків і повноважень. Основою взаємодії є «угода про співпрацю» відповідних органів і відомств Німеччини.

NCAZ також уповноважений співпрацювати з будь-якими інститутами ЄС безпосередньо, з використанням ресурсів існуючих органів країн ЄС, що займаються питаннями кіберзахисту. Центр співпрацює з Європейським агентством з мережевої та інформаційної безпеки *ENISA*, директор якого Удо Хельмбрехт раніше обіймав пост президента Федеральної агенції з питань інформаційної безпеки, а президент *NCAZ* Міхаель Ханг входить до Наглядової ради *ENISA*.

Як зазначено в Національній стратегії кіберзахисту 2011 р., Німецький національний центр кіберреагування відповідає за координацію реагування на інциденти та обмін інформацією в цілому. Однією з найгостріших потреб було створення ініціативи/платформи, до складу якої входили б представники промисловості та неурядових організацій, які здатні надавати поточну та достовірну інформацію у сфері кібербезпеки на національному рівні та консультувати зацікавлені сторони шодо попередження та пом'якшення кіберінцидентів. У співпраці з Національним центром кіберреагування «Альянс з питань кібербезпеки» (галузевої платформи для співпраці та обміну інформацією, створений у 2012 р.) реалізується форма співпраці між державними органами, академічним та приватним простором, а також підприємствами, що є об'єктом особливого громадського інтересу.

---

[85] Структура Федерального відомства з безпеки інформаційних технологій [Електронний ресурс]. – Режим доступу : https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/BSI/org_chart_IFG_pdf.pdf?__blob=publicationFile&v=7

[86] Security in focus [Електронний ресурс]. – 2017. – № 01. – Режим доступу : https://goo.gl/prNmr6

[87] CERT-Bund [Електронний ресурс]. – Режим доступу : https://goo.gl/5unMMN

Сприяючи національному обміну інформацією, Національний ІТ ситуаційний центр[88] (*Nationales IT-Lagezentrum*[89]), який також є складовою частиною Федеральної агенції з питань кібербезпеки, стежить за національною та глобальною ситуацією у сфері безпеки ІТ, з метою швидкого виявлення та аналізу серйозних інцидентів у сфері інформаційної безпеки та рекомендує захисні заходи. У випадку кризи ця структура має право розширити свої повноваження і трансформуватися в Національний центр кризового ІТ-реагування (*Nationales IT-Krisenreaktionszentrum*[90]). Цей центр концентрує можливості для подолання ІТ-криз, охоплюючи всі національні аспекти, включаючи державні мережі та критичні інфраструктури.

Новий важливий етап у сфері КДПП розпочався у липні 2015 р., коли у Німеччині було ухвалено Закон «Про інформаційну безпеку»[91] з метою запобігання атакам на важливі інформаційні системи. Закон визначає мінімальні стандарти кібербезпеки для понад 2 тис. компаній – операторів критичної інфраструктури. Відповідно до закону ці мінімальні вимоги до безпеки мають забезпечуватися через доступність, автентичність, конфіденційність та цілісність ІТ-безпеки по всій Німеччині; підвищення безпеки Інтернету для громадян; кращий захист критично важливої інфраструктури національного значення[92].

Згідно із законом оператори критичної інфраструктури зобов'язані встановити належні системи інформаційної безпеки на власних підприємствах під час надання ними послуг та зобов'язані оновлювати цю систему кожні два роки. Оператори також мають повідомляти про серйозні кіберінциденти *BSI* – зобов'язання повідомляти про кібератаки мають оператори атомних електростанцій, телекомунікаційних компаній, а також починаючи із травня 2016 р., згідно із оновленою стратегією кібербезпеки, оператори критичної інфраструктури у секторах енергетики, інформаційних та телекомунікаційних технологій, продуктів харчування та водного. Обов'язкова звітність операторів критичної інфраструктури в галузі фінансів, страхування та транспортних секторів, а також охорони здоров'я про інциденти існували з моменту набрання чинності постановою про зміну до чинного положення про KPITIC 30 червня 2017 р.[93].

Закон[94] вимагає від *BSI* проводити аудит безпеки організацій, що займаються критичною інфраструктурою, один раз на два роки. Цей закон також розширив повноваження Федеральної служби кримінальної поліції для розслідування злочинів, пов'язаних із хакерськими атаками на федеральні ІТ-системи[95]. Закон також вимагає обов'язкової звітності від федеральних органів влади щодо інцидентів у сфері кібербезпеки перед Федеральною агенцією з питань інформаційної безпеки. Не німецькі компанії,

---

[88] Ситуаційний центр надає Центру кіберзахисту звіти про ситуацію, довідкову інформацію про інциденти, пов'язані з інформаційною безпекою, та інформацію/попередження щодо вразливості. Щоб отримати додаткову інформацію для оцінки ситуації та захисту, запитання ставляться цілеспрямовано. Центр кіберзахисту надає рейтинги, додаткові відомості та довгостроковий ситуаційний аналіз у більш широкій міжвідомчій перспективи та зважаючи на відповіді на запитання.

[89] Федеральне відомство з безпеки інформаційних технологій. Раннє попередження [Електронний ресурс]. – Режим доступу : https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Aktivitaeten/IT-Lagezentrum/Fruehwarnung/fruehwarnung_node.html

[90] Центр кризового реагування ІТ [Електронний ресурс]. – Режим доступу : https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Aktivitaeten/IT-Krisenreaktionszentrum/itkrisenreaktionszentrum_node.html

[91] Федеральний закон про захист даних [Електронний ресурс]. – Режим доступу : https://www.gesetze-im-internet.de/englisch_bdsg/

[92] Watson Farley & Williams. Briefing «The New German it Security Act» [Електронний ресурс]. – February 2016. – Режим доступу : http://www.wfw.com/wp-content/uploads/2016/02/WFW-Briefing-GermanyIT-Security-Feb-2016-EN-15-Feb.pdf

[93] Schutz Kritischer Infrastrukturen ITSig u UP-KRITIS [Електронний ресурс]. – Режим доступу : https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Schutz-Kritischer-Infrastrukturen-ITSig-u-UP-KRITIS.pdf?__blob=publicationFile&v=7

[94] Закон про підвищення безпеки інформаційних систем (Закон про захист інформаційних систем) [Електронний ресурс]. – Режим доступу : https://goo.gl/Hft42E

[95] Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) [Електронний ресурс]. – Режим доступу : https://goo.gl/pUw5UG

що є операторами критичної інфраструктури в Німеччині, також потрапляють у сферу дії закону.

Стосовно приватного сектору закон регулює діяльність операторів онлайн-ресурсів та інших постачальників послуг щодо захисту використовуваних ними ІТ-систем та рівня захищеності цих систем від несанкціонованого доступу до персональних (клієнтських) даних. З цією метою повинні використовуватись найсучасніші технічні та організаційні процедури шифрування. Також телекомунікаційні компанії тепер повинні повідомляти своїх клієнтів про будь-які порушення та зловживання у їх мережах. Оператори критичної інфраструктури та їх промислові асоціації можуть запропонувати галузеві стандарти безпеки, які можуть бути визнані *BSI*, якщо ці стандарти дійсно запобігають перебоям і гарантують цілісність, автентичність та конфіденційність відповідної інфраструктури[96].

Протягом двох років після ухвалення закону всі оператори зобов'язані були здійснити належні організаційні та технічні заходи безпеки для захисту ІТ-систем, їх компонентів або процесів, що стосуються функціонування критичної інфраструктури. Крім того, оператори об'єктів критичної інфраструктури зобов'язані проходити аудит або сертифікацію безпеки ІТ щонайменше кожні два роки.

Цей закон мав на меті врегулювати низку попередніх недопрацювань правових положень, утім для бізнесу та підприємств галузі залишається під питанням, хто є частиною *KRITIS* і якими є наслідки закону про ІТ-безпеку. Проте, за відгуками індустрії та бізнес-спільноти, не є достатньо прозорим визначення оператора критичної інфраструктури, зокрема, через те, що у законі 2015 р. для компаній малого і середнього бізнесу сфера застосування закону не розмежовувалася. За опитуванням *PwC*[97], близько 18 % компаній, зареєстрованих у Німеччині, юридично можуть підпадати під поняття оператора, визначеного у законодавстві. Згідно з аналізом *KPMG*[98] кількість «непевних» компаній іще більша.

У лютому 2016 р. був опублікований проект урядової постанови, який частково вирішував це питання, втім низка асоціацій інформаційної безпеки, таких як *VDE* (Асоціація електричних, електронних та інформаційних технологій *E.B.*), *VKU* Асоціація житлово-комунального господарства (*Verband Kommunaler Unternehmen*) або *DVGW* (Німецька асоціація для газу і води) вбачають необхідність у подальшій специфікації[99]. Так, усе ще невирішеним залишається питання членства в *UP KRITIS*: за визначенням Федеральної агенції державно-приватного співробітництва, таке членство є добровільним, але у випадку, коли організація не є членом *UP KRITIS*, вона можете підпадати під санкції згідно із законом 2015 р.

UP KRITIS фінансується операторами критичної інфраструктури та відповідними державними органами. Однією з явних цілей *UP KRITIS* є спільна оцінка стану кібербезпеки та вироблення механізму реагування на кіберінциденти. Як форма державно-приватної співпраці між операторами критичної інфраструктури, їх асоціаціями та відповідними державними органами KPITIC сконцентрований на декількох напрямах діяльності.

Передусім – на підготовці та реалізації спільних рекомендацій для держави та приватного сектору у сфері кіберзахисту. Робоча група *UP KRITIS* виробила два основні підходи, які стали наслідком серії навчань *LÜKEX*. Перший підхід напрацьовувався

---

[96] Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) [Електронний ресурс]. – Режим доступу : https://goo.gl/pUw5UG

[97] Infrastruktur unter besonderem schutz [Електронний ресурс]. – Режим доступу : https://next.pwc.de/wikri-2016/infrastruktur-unter-besonderem-schutz.html

[98] IT-Sicherheitsgesetz [Електронний ресурс]. – Режим доступу : https://goo.gl/MNCQNG

[99] Was KRITIS Fuer Unternehmen Bedeutet [Електронний ресурс]. – Режим доступу : https://www.security-insider.de/was-kritis-fuer-unternehmen-bedeutet-a-536376/

як частина навчань «Раннє виявлення та пом'якшення наслідків кіберзагроз». Другий – як блок навчань «Надзвичайні та кризові дії щодо критичних інфраструктур у випадку кіберзагроз». Зокрема, у рамках навчань «*Bundessonderlage IT 2009*» («Німецька федеральна спеціальна ІТ-ситуація 2009») та «*Eltville 13*» члени *UP KRITIS* змогли інтенсивно відпрацювати критичні сценарії кіберзагроз, визначити потенціал поліпшення, а також розробити рішення для подолання криз у критичних процесах[100].

Наступний напрям – кризовий менеджмент, з якого було проведено дводенні тренінги в Академії управління кризовими ситуаціями, на яких відпрацьовувалася реакція в надзвичайних ситуаціях та заходи цивільного захисту у Федеральній агенції з питань цивільного захисту та ліквідації наслідків стихійних лих (*AKNZ* (*Academy for Crisis Management, Emergency Planning and Civil Protection of the Federal Office of Civil Protection and Disaster Assistance* (*BBK*)) з метою посилення та поглиблення співпраці між державним та приватним секторами у конкретних кризових ситуаціях. Дослідження потенційних кризових сценаріїв сприяло тому, що задіяні організації змогли розробити спільну думку про можливі ІТ-кризи та відповідні схеми скоординованої діяльності.

З метою забезпечення кращого національного та міжнародного співробітництва *UP KRITIS* регулярно інформує національних партнерів про відповідні європейські заходи щодо захисту критичної інфраструктури. Ухвалені членами *UP KRITIS* ініціативи були представлені на європейському рівні, і таким чином отримали можливість впливати на рішення, прийняті в європейських структурах на ранніх стадіях, у напрямі посилення інтересів *UP KRITIS* та Німеччини в цілому.

UP KRITIS об'єднує різні структури кризового менеджменту між секторами, а також продовжує розширювати спільні структури та процеси кризових комунікацій. За необхідності створюються додаткові форми комунікації в окремих галузях.

Усі організації, що діють у сфері критичної інфраструктури і мають свої представництва в Німеччині, можуть подати заявку на участь у *UP KRITIS*. Учасники призначають представників своєї організації, яким надається доступ до інформаційних продуктів *UP KRITIS*, а також до інформації, наданої Альянсом з питань кібербезпеки, та конфіденційної інформації про ситуацію та попередження кіберзагроз, що надається Національною агенцією з інформаційної безпеки.

Водночас, крім *UP KRITIS,* існують й інші майданчики державно-приватного співробітництва.

Зокрема, Альянс для кібербезпеки – це ініціатива федерального уряду Німеччини, в рамках якої основні інформаційно-технологічні компанії – як державні, так і приватні – обмінюються інформацією, створюють та розширюють базу знань з метою посилення кібербезпеки в Німеччині[101].

Крім Альянсу, існує ряд інших майданчиків для швидкого обміну інформацією та евентуального реагування вже недержавного типу, який об'єднує бізнес-кола в незалежні асоціації. Наприклад, Рада з питань кібербезпеки Німеччини – незалежна асоціація з кібербезпеки, яку становлять члени приватних організацій – операторів критичної інфраструктури[102]. Рада є політично нейтральною, її мета – консультування компаній, державних органів та політиків щодо посилення кібербезпеки у боротьбі з кіберзлочинністю.

Членами асоціації є великі та середні підприємства, оператори критичної інфраструктури, федеральні землі (наприклад, Північний Рейн-Вестфалія, Нижня Саксонія),

---

[100] UP KRITIS. Public-Private Partnership for Critical Infrastructure Protection. – Basis and Goals [Електронний ресурс]. – Режим доступу : https://goo.gl/ZpbG6t

[101] Allianz Fuer Cybersicherheit [Електронний ресурс]. – Режим доступу : https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Home/startseite.html

[102] Cyber-Security Council Germany [Електронний ресурс]. – Режим доступу : http://www.cybersicherheitsrat.de/english/about-us/

муніципалітети (наприклад, місто Франкфурт-на-Майні), а також експерти та політичні особи, які приймають рішення щодо кібербезпеки. Асоціація налічує близько 3 млн працівників бізнесу та 1,8 млн членів інших об'єднань та асоціацій.

Серед основних цілей діяльності – посилення співпраці між розробниками політики, урядовими структурами, бізнесом та науковими установами для покращення кіберзахисту, впровадження ініціатив та проектів, спрямованих на популяризацію кібербезпеки, створення німецької мережі кібербезпеки в європейському та міжнародному контекстах.

3.3. Досвід Великої Британії

Велика Британія характеризується високим рівнем розвитку національної системи кібербезпеки, який забезпечується потужною стратегічною та законодавчою базою, а також низкою практичних заходів, спрямованих на розбудову широкого партнерства між державними структурами, приватним сектором, науковими установами та громадянським суспільством. Хоча обсяг ресурсів, які виділяються у Великій Британії на кібербезпеку, не можна порівнювати з можливостями нашої держави, аналіз британського досвіду КДПП є актуальним для України з точки зору підходів та механізмів співпраці, особливо зважаючи на те, що Стратегією кібербезпеки України, що ухвалена 2016 р., КДПП було визначено як один із головних принципів забезпечення кібербезпеки.

На законодавчому рівні поняття ДПП у Великій Британії унормоване в Акті про державні ресурси та рахунки 2000 р. (*Government Resources and Accounts Act*), де зазначено, що ДПП – це «проекти та ініціативи, ресурси на які виділяються частково державними установами, частково – приватним структурами»; під ресурсами розуміються «кошти, активи, професійні навички та будь-які інші види комерційних ресурсів»[103]. Відповідальним за механізм ДПП є британське Міністерство фінансів (Королівська Скарбниця – *HM Treasury*), яке забезпечує реалізацію цього механізму, інвестуючи фінансові та інші ресурси та надаючи консультації, а також підзвітна міністерству Служба з питань інфраструктури та проектів (*Infrastructure and Projects Authority*).

У 1990-х роках Велика Британія була однією з перших країн, яка поряд із програмами приватизації почала впроваджувати механізм ДПП. Так, у 1992 р. Міністерством фінансів була запущена схема *Private Finance Initiative* (*PFI*), за якою приватні компанії підписують довгострокові контракти з державними установами, відповідно до вимог установи розробляють, фінансують та управляють певними (переважно інфраструктурними) проектами; після виконання проекту держава впродовж кількох десятиліть сплачує постачальнику за використання реалізованого об'єкта[104]. У 2012 р. *PFI* була оновлена та замінена на *Private Finance* 2; згідно з *PF*2 держава стає міноритарним інвестором проектів, встановлюється обмеження у 18 місяців на тендерні процедури, а невиробничі послуги (*soft services*, наприклад, прибирання чи громадське харчування) перестають бути предметом ДПП[105]. Станом на березень 2016 р. налічувалося 716 проектів *PFI* та *PF*2, з яких 686 були виконані та за які держава почала виплачувати кошти; загальна вартість проектів становила 59,4 млрд фунтів стерлінгів (проекти з найбільшою сукупною вартістю реалізовувались на замовлення Департаменту охорони здоров'я (майже

[103] Government Resources and Accounts Act 2000 [Електронний ресурс]. – Режим доступу : https://www.legislation.gov.uk/ukpga/2000/20/pdfs/ukpga_20000020_en.pdf

[104] A new approach to public private partnerships [Електронний ресурс]. – Режим доступу : https://goo.gl/fBj8mF

[105] Private Finance Initiative and Private Finance 2 projects: 2016 summary data [Електронний ресурс]. – Режим доступу : https://goo.gl/m6qKLd

13 млрд фунтів), Міністерства оборони (9,5 млрд фунтів), Департаменту освіти (близько 8,6 млрд фунтів) та Департаменту транспорту (7,8 млрд фунтів)[106]. Серед цих, діючих у 2016 р., проектів у сфері ІТ-інфраструктури та комунікацій були, зокрема: проект *Defence Fixed Telecommunications Service*, який у 1997 р. на замовлення Міністерства оборони Великої Британії почала реалізовувати *British Telecom*, його загальна вартість становила 312,2 млн фунтів стерлінгів; проект запуску у 2008 р. супутника *Skynet* 5 від *Airbus Defence & Space* на замовлення Міноборони, загальна вартість – понад 1,3 млрд фунтів стерлінгів; розпочатий у 2002 р. проект впровадження автоматизованої системи управління справами *Compass CMS* від *CGI Group* у Королівській прокурорській службі, загальна вартість – 2,9 млн фунтів стерлінгів[107].

Поряд зі схемами КДПП у Великій Британії успішно діють урядові рамкові програми закупівель у різних сферах, зокрема, у сфері кібербезпеки. Однією з таких програм є запущена Урядовою цифровою службою (*Government Digital Service*) та Королівською комерційною службою (*Crown Commercial Service*) у 2013 р. ініціатива «*G-Cloud*», у рамках якої державні структури можуть закуповувати послуги у провайдерів хмарних сервісів. Компанії різних розмірів можуть раз на рік подавати заявки та бути обраними як постачальники одного з трьох видів хмарних сервісів – хостингу, програмного забезпечення та послуг підтримки[108]. Державні структури отримують доступ до онлайн-магазину *Digital Marketplace*, де можуть придбати необхідні хмарні сервіси від обраних компаній. Крім того, на *Digital Marketplace* державні органи можуть отримати послуги експертів у сфері цифрових технологій у рамках програми «*Digital Outcomes and Specialists*», а також отримати фізичний обсяг місця у дата-центрі в рамках програми «*Crown Hosting Data Centres*» (спільного підприємства, створеного урядом та компанією *Ark Data Centres Limited*)[109]. У 2015 р. Королівська комерційна служба запустила програму закупівлі консалтингових послуг у сфері кібербезпеки «*Cyber Security Services*» – державні структури отримали змогу обирати визначених приватних постачальників послуг з розроблення політики безпеки даних, оцінки та управління ризиками, управління інцидентами, розроблення безпекової архітектури установи тощо[110].

На стратегічному рівні КДПП (у його широкому розумінні) визначено однією з основ сталого функціонування безпекової системи держави. Стратегія кібербезпеки Великої Британії, ухвалена на період 2011–2015 рр., визначала ключову роль приватного сектору для кібербезпеки, оскільки потужності та технології переважно перебувають у власності приватних компаній. У рамках встановлення партнерства з приватним сектором держава вживала заходів щодо обміну інформацією про кіберзагрози, управлінням кіберінцидентами, розбудови спроможностей кібербезпеки, розроблення галузевих стандартів кібербезпеки[111]. За результатами оцінки урядом виконання Стратегії 2011–2015 рр.[112] можна стверджувати, що у напрямі розбудови партнерства з приватним сектором було зроблено чимало кроків. Із загального п'ятирічного обсягу фінансування, виділеного урядом на реалізацію Стратегії (близько 860 млн фунтів стерлінгів), близько 61,1 млн фунтів стерлінгів було витрачено лише на залучення бізнесу до співпраці

[106] Private Finance Initiative and Private Finance 2 projects: 2016 summary data [Електронний ресурс]. – Режим доступу : https://goo.gl/m6qKLd

[107] Current projects as at 31 March 2016 [Електронний ресурс]. – Режим доступу : https://goo.gl/yPsZVh

[108] The G-Cloud framework on the Digital Marketplace [Електронний ресурс]. – Режим доступу : https://goo.gl/sEg3sp

[109] The Crown Hosting Data Centres framework on the Digital Marketplace [Електронний ресурс]. – Режим доступу : https://goo.gl/xb17Sj

[110] Cyber Security Consultancy Framework for UK Public Sector [Електронний ресурс]. – Режим доступу : https://goo.gl/Ae3Rjw

[111] The UK Cyber Security StrategyProtecting and promoting the UK in a digital world [Електронний ресурс]. – Режим доступу : https://goo.gl/XWskxu

[112] The UK Cyber Security Strategy 2011–2016: Annual ReportApril 2016 [Електронний ресурс]. – Режим доступу : https://goo.gl/ojjk6K.

та підвищення його обізнаності у питаннях кібербезпеки; найбільше коштів було виділено на підвищення спроможності держави виявляти та ліквідовувати найнебезпечніші загрози – 441,8 млн фунтів стерлінгів[113].

Чинна Стратегія кібербезпеки на 2016–2021 рр. наголошує, що «бізнес зменшить потенційні кіберзагрози, лише якщо оцінюватиме та мінімізовуватиме ризики для своїх критичних систем та конфіденційних даних, інвестуючи у людський капітал, технології та управління»[114]. Держава проголошує намір брати на себе ще більшу відповідальність за впровадження заходів з кібербезпеки, але водночас наголошує на тому, що приватний сектор має бути не менш відповідальним за захист даних, якими він володіє, має сприяти забезпеченню стійкості систем, розв'язанню кіберінцидентів та нести юридичну відповідальність за наслідки можливих кібератак. Нова Стратегія передбачає збільшене у понад двічі фінансування – 1,9 млрд фунтів стерлінгів, а головною метою держави проголошує «зробити Сполучене Королівство найбільш безпечним місцем для життя та ведення бізнесу онлайн»[115].

Слід зазначити, що одним із найпомітніших результатів виконання попередньої п'ятирічної Стратегії стало об'єднання у жовтні 2016 р. зусиль різних державних суб'єктів забезпечення кібербезпеки у рамках єдиної структури – Національного центру кібербезпеки (*National Cyber Security Centre, NCSC*) у складі Центру урядового зв'язку (*Government Communications Headquarters, GCHQ*)[116]. *NCSC* активно та публічно взаємодіє з приватним сектором, науковим середовищем, громадськістю та міжнародними партнерами і слугує єдиним майданчиком для формування спільного бачення та засад безпечної та ефективної діяльності держави у кіберпросторі.

У 2017 р. зусилля Королівської комерційної служби у напрямі закупівель консалтингових послуг були об'єднані із зусиллями Національного центру кібербезпеки, результатом чого стало впровадження рамкової програми «*Cyber Security Services 2*». Зокрема, програма була значно розширена – до постачальників консалтингових послуг додалися провайдери тестів на виявлення вразливостей інформаційних систем (*Penertation Testing CHECK*), розроблені дві схеми реагування на кіберінциденти та додані відповідні групи компаній-постачальників (*Cyber Incident Response* для державних структур та *Cyber Security Incident Response* для приватних компаній та академічних установ), а також додані провайдери оцінки відповідності інформаційних систем компаній та установ вимогам Національного центру кібербезпеки[117].

Іншою структурою, що тісно співпрацює з *NCSC*, є Центр захисту національної інфраструктури (*Centre for the Protection of National Infrastructure, CPNI,* підзвітний *MI5*). Центр забезпечує обмін інформацією між державою та 13 ключовими секторами критичної інфраструктури (хімічна промисловість, ядерні об'єкти цивільного призначення, оборона, аварійно-рятувальні служби, енергетика, фінанси, продовольство, уряд, охорона здоров'я, космічна галузь, транспорт, водопостачання[118]), підтримує співробітництво у питаннях виявлення ризиків та зменшення вразливості об'єктів критичної інфраструктури, а також розробляє відповідні рекомендації, наприклад, щодо впровадження кращих практик зменшення кібернетичних ризиків в управлінні ланцюгом поставок на різних підприємствах[119].

---

[113] The UK Cyber Security StrategyProtecting and promoting the UK in a digital world [Електронний ресурс]. – Режим доступу : https://goo.gl/XWskxu

[114] NATIONAL CYBER SECURITY STRATEGY 2016–2021 [Електронний ресурс]. – Режим доступу : https://goo.gl/QEQs11

[115] Там само.

[116] About the NCSC [Електронний ресурс]. – Режим доступу : https://www.ncsc.gov.uk/information/about-ncsc

[117] NCSC Scheme benefits [Електронний ресурс]. – Режим доступу : http://ccs-agreements.cabinetoffice.gov.uk/DF_NCSC_Certs

[118] About the NCSC [Електронний ресурс]. – Режим доступу : https://www.ncsc.gov.uk/information/about-ncsc.

[119] Critical National Infrastructure [Електронний ресурс]. – Режим доступу : https://www.cpni.gov.uk/critical-national-infrastructure-0

Розглядаючи законодавчий аспект КДПП, варто звернути увагу на питання регулювання порушень з боку приватних компаній. Нині законодавчо не встановлена обов'язкова необхідність компаній звітувати про кіберінциденти та порушення безпеки чи проходити спеціальну сертифікацію (у випадках критичної інфраструктури – питання регулюється шляхом обов'язкового ліцензування згідно з Актом про непередбачувані ситуації 2004 року (*Civil Contingencies Act*[120]). Компанії, що працюють з персональними даними, підпадають під дію Акта про захист даних (*Data Protection Act*) 1998 р. та Положення про конфіденційність та електронні комунікації (*Privacy and Electronic Communications (EC Directive) Regulations*) 2003 р. (британський законодавчий акт, яким була імплементована відповідна Директива ЄС 2002/58/ЕС про оброблення персональних даних та захист приватності), якими визначаються вимоги до цільового та законного використання даних, забезпечення захищених каналів комунікацій, використання *cookies* на веб-сайтах, збереження приватності даних клієнтів (дані про трафік, місцезнаходження, ідентифікація, розрахунки онлайн тощо)[121].

У випадку кібератаки, що призвела до знищення чи крадіжки персональних даних, компанії мають повідомити Офіс інформаційного комісара (*Information Commissioner's Office, ICO*) – структуру, підзвітну безпосередньо парламенту, що фінансується Департаментом цифрового розвитку, культури, медіа та спорту. *ICO* розглядає кожну конкретну ситуацію та визначає, чи призначати штраф (максимальний розмір – до 500 тис. фунтів стерлінгів[122]). Серед найрезонансніших випадків накладання на компанії Великої Британії штрафів за кіберінциденти можна згадати справу інтернет-провайдера *TalkTalk*. Так, у жовтні 2015 р. компанія зазнала нескладної за принципом кібератаки на свою базу даних (*SQL*-ін'єкція), внаслідок якої зловмисники отримали доступ до чутливих персональних, зокрема платіжних, даних понад 15 тис. осіб. Хоча компанія і повідомила *ICO* про інцидент, регулятор стягнув з неї 400 тис. фунтів стерлінгів штрафу за недотримання базових вимог щодо захисту даних користувачів[123]. Дещо іншою ситуація була щодо інциденту в компанії *Uber*; у жовтні 2016 р. хакери вкрали персональні дані (імена, телефони, електронні адреси тощо) 57 млн користувачів та водіїв, з них 2,7 млн – з Великої Британії; компанія вирішила це приховати і заплатила хакерам 75 тис. фунтів стерлінгів за видалення даних[124]. Станом на середину грудня 2017 р. ситуація розслідується *ICO* та *NCSC*; хоча викрадені дані не були чутливими (*sensitive*), до *Uber* може бути застосовано штраф за порушення вимог до безпеки даних користувачів.

З 9 травня 2018 р. процедура повідомлення про кіберінциденти у Великій Британії має стати обов'язковою через набуття чинності новим законодавством ЄС, зокрема Директиви ЄС щодо мережевої та інформаційної безпеки (*The Network and Information Security Directive, NIS*) 2016 р. Крім того, держави – члени ЄС мають створити групи реагування на кіберінциденти, визначити ключових операторів критичної інфраструктури (*essential services*) та провайдерів цифрових послуг, забезпечити виконання ними заходів щодо управління ризиками, мінімізації наслідків кіберінцидентів; приватні компанії, які не відносяться до критичної інфраструктури та провайдерів цифрових послуг, мають право добровільно повідомляти про кіберінциденти[125].

---

[120] The UK's Cybersecurity Regulatory Landscape: An Overview [Електронний ресурс]. – Режим доступу : https://goo.gl/XnsWAF

[121] Guide to Privacy and Electronic Communications Regulations [Електронний ресурс]. – Режим доступу : https://ico.org.uk/for-organisations/guide-to-pecr/

[122] Government to strengthen UK data protection law [Електронний ресурс]. – Режим доступу : https://goo.gl/Ur9KXs

[123] TalkTalk hit with record £400k fine over cyber-attack [Електронний ресурс]. – Режим доступу : https://goo.gl/HGEfRh

[124] Uber failed to tell UK authorities of mass data breach, says No 10 [Електронний ресурс]. – Режим доступу : https://goo.gl/7PnUyb

[125] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [Електронний ресурс]. – Режим доступу : https://goo.gl/bxKxJW

Загальний регламент захисту даних (*General Data Protection Regulation, GDPR*) 2016 р. (який не має зобов'язуючого характеру), також передбачає ініціювання державою норм щодо зобов'язання компаній, які зберігають та обробляють персональні дані, повідомляти про кіберінциденти та порушення *ICO* та клієнтів, проводити регулярні оцінки стану захищеності даних. Крім того, *GDPR* визначає необхідність надавати користувачам більший контроль над своїми персональними даними, видаляти їх за вимогою на законних підставах. За порушення компанією норм держава може застосувати адміністративний штраф у розмірі до 20 млн євро або до 4 % загального прибутку компанії[126], що залежатиме від серйозності порушення.

Зважаючи на те, що процедура виходу Великої Британії з ЄС триває, питання подальшої дії вже імплементованих директив ЄС та імплементації нещодавно прийнятих залишається вкрай важливим. Так, у січні 2017 р. Європейська Комісія представила новий Регламент про конфіденційність та електронні комунікації, що має прийти на заміну Директиві 2002/58/ЕС (регламент, на відміну від директиви, має обов'язково стати частиною національного законодавства). У жовтні 2017 р. Європарламент проголосував за зміни, а станом на початок січня 2018 р. пропозиція нового положення проходить процедуру обговорення державами – членами ЄС[127]. Серед ключових змін, передбачених Регламентом: включення до переліку провайдерів електронних телекомунікаційних сервісів суб'єктів, що надають послуги *Over-the-Top* (*IP*-телефонія, месенджери, електронна пошта на основі веб-технологій); поширення дії норм на провайдерів, які територіально базуються поза межами ЄС і надають послуги користувачам на території ЄС; спрощення правил використання *cookies* та інших технологій ідентифікації користувачів[128]. Парламент Великої Британії проаналізував пропозиції та закликав уряд забезпечити впровадження оновлених норм у національне законодавство, оскільки, якщо Велика Британія хоче продовжувати будь-яку діяльність, що передбачає обмін електронними комунікаціями та персональними даними користувачів на території ЄС після виходу з нього, то необхідним є узгодження британських норм та норм ЄС[129]. Питання того, яким саме чином ці норми будуть впроваджені – шляхом включення Регламенту до національного законодавства, адаптації, чи укладання Великою Британією окремих угод з ЄС – залишається відкритим.

У випадку з Директивою ЄС щодо мережевої та інформаційної безпеки, то ймовірність її впровадження у британське законодавство є високою. В урядовій доповіді «Огляд законодавчого регулювання та ініціатив у сфері кібербезпеки» за 2016 рік зазначається, що Директива *NIS* «повинна бути впроваджена у 2018 році», а «детальний опис та вимоги щодо імплементації Директиви будуть визначені урядом впродовж 2017 року»[130]. Станом на осінь 2017 року Департамент цифрового розвитку, культури, медіа та спорту провів консультації з представниками бізнесу, регуляторних органів та інших зацікавлених сторін щодо планів уряду імплементувати норми Директиви у британське законодавство. У звіті за результатами консультації зазначається, що доки триває переговорний процес щодо виходу Сполученого Королівства з ЄС, уряд «обговорюватиме, впроваджуватиме та застосовуватиме законодавство ЄС»[131], а після виходу з ЄС це законодавство діятиме і надалі. Подібна ситуація найбільш ймовірно складеться і з імплементацією *GDPR*. Уряд неодноразово проголошував намір впровадити *GDPR* у повному

[126] Data protection: Rules for the protection of personal data inside and outside the EU [Електронний ресурс]. – Режим доступу : http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

[127] Proposal for a Regulation on Privacy and Electronic Communications [Електронний ресурс]. – Режим доступу : https://goo.gl/vvKE1Y

[128] Там само.

[129] Proposed Regulation on Privacy and Electronic Communications repealing Directive 2002/58/EC [Електронний ресурс]. – Режим доступу : https://publications.parliament.uk/pa/cm201617/cmselect/cmeuleg/71-xxix/7109.htm.

[130] Cyber Security Regulation and Incentives Review [Електронний ресурс]. – Режим доступу : https://goo.gl/m529Zv

[131] Security of Network and Information Systems [Електронний ресурс]. – Режим доступу : https://goo.gl/G4mWso

обсязі до 25 травня 2018 р.[132]. Регламент має бути імплементований у британське законодавство новим Актом про захист даних, який нині проходить слухання у парламенті.

Велика Британія – держава з одним із найдинамічніших, інноваційних та потужних ринків кібербезпеки у Європі та світі. За останні сім років загальний обсяг британського ринку кібербезпеки зріс на майже півтора мільярди доларів – з 2,4 млрд фунтів стерлінгів у 2010 р. до майже 3,5 млрд фунтів стерлінгів у 2017 р.[133]. Збільшується також частка експорту продукції та послуг кібербезпеки у загальному безпековому експорті Великої Британії. Так, у 2016 р. кібербезпека становила 34 % усього обсягу безпекового експорту, або понад 1,5 млрд фунтів стерлінгів[134].

Разом зі зростанням ринку кібербезпеки змінюється і кількість та характер загроз, що постають як перед учасниками ринку, так і перед більш широким колом зацікавлених осіб у різних секторах економіки. Зважаючи на це, держава прагне забезпечувати ефективне регулювання сфери кібербезпеки, впроваджуючи стандарти, розробляючи спільно з представниками бізнесу, науки та громадськості рекомендації, а також забезпечуючи необхідний рівень відповідальності за дотримання приватним сектором базових вимог та підтримку належного рівня захищеності даних та потужностей, особливо якщо йдеться про провайдерів критичної інфраструктури.

За останній рік кількість кіберінцидентів у державних та приватних структурах Великої Британії збільшилася. Так, за даними оцінки рівня злочинності, проведеної Службою національної статистики Великої Британії, у 2016 р. було зафіксовано 3,6 млн випадків онлайн-шахрайства та 2 млн випадків неправомірного використання комп'ютерів, що загалом на 8 % більше, ніж минулого року[135]. За результатами оцінки порушень кібербезпеки у період з жовтня 2016 р. по січень 2017 р., проведеної урядовим Департаментом культури, медіа та спорту, 46 % опитаних з 1 523 компаній зазнали хоча б однієї кібератаки або порушення безпеки за останній рік; одна компанія у середньому втрачає 1 570 фунтів стерлінгів на одній атаці (для великої компанії ця цифра становить 19 тис. фунтів стерлінгів, для середнього бізнесу – 3 070, для малого – 1 380 фунтів стерлінгів)[136]. Переважна кількість порушень пов'язана з відкриттям шахрайських електронних повідомлень, вірусами, шкідливим ПЗ та програмами-вимагачами, що свідчить про значний вплив людського фактора та можливе недотримання простих правил поводження з підозрілими додатками. Крім того, дослідження виявило, що хоча 74 % компаній визначає кібербезпеку ключовим пріоритетом, а 67 % компаній витрачає гроші на кібербезпеку (переважно з метою захисту даних клієнтів та активів компанії), лише 20 % компаній приділяють увагу навчанню співробітників основам кіберзахисту, і тільки 11 % фірм мають розроблений план управління кіберінцидентами[137]. Такі факти порушень на низовому рівні можуть призводити до суттєвих збитків на рівні національної економіки, тому одним із важливих напрямів державно-приватного співробітництва стає впровадження базових рекомендацій з кібербезпеки у різних компаніях.

Одним із найпомітніших та найефективніших проектів КДПП можна назвати започатковане у 2013 р. Партнерство з обміну інформацією у сфері кібербезпеки (*Cyber Security Information Sharing Partnership, CISP*). Ця ініціатива покликана забезпечити «обмін інформацією про кіберзагрози у режимі реального часу, в безпечному, конфіденційному

---

[132] International Strategy 2017–2021 [Електронний ресурс]. – Режим доступу : https://ico.org.uk/media/about-the-ico/documents/2014356/international-strategy-03.pdf

[133] Cyber security market size in the United Kingdom (UK) from 2010 to 2017 (in million GBP) [Електронний ресурс]. – Режим доступу : https://www.statista.com/statistics/289173/uk-cyber-security-private-enterprises-segment-size/

[134] UK defence and security export statistics for 2016 [Електронний ресурс]. – Режим доступу : https://goo.gl/gTVphZ

[135] Cybercrime and fraud scale revealed in annual figures [Електронний ресурс]. – Режим доступу : http://www.bbc.com/news/uk-38675683

[136] Cyber security breaches survey 2017: Mainreport [Електронний ресурс]. – Режим доступу : https://goo.gl/SVHkS8

[137] Там само.

та динамічному середовищі, посилюючи ситуаційну обізнаність та зменшуючи вплив на бізнес у Сполученому Королівстві»[138]. У рамках цього партнерства можливим став обмін інформацією між бізнесом та спецслужбами щодо реальних і потенційних кіберзагроз; така інформація готується координаційною аналітичною групою у складі представників індустрії та держави (зокрема, Служби безпеки *MI5*, *GCHQ* та Національного агентства із боротьби зі злочинністю). Отримуючи інформацію про порушення безпеки в інформаційних системах компаній, фахівці спецслужб мають можливість запобігти поширенню шкідливого ПЗ за межами компанії. Компанії, своєю чергою, можуть попередити кіберінцидент, володіючи необхідною інформацією, доступною лише спецслужбам. Станом на кінець 2016 р. членами *CISP* були понад 2 800 організацій та 8 000 осіб[139], за рік роботи рівень залучення до партнерства збільшився на 43 %[140].

Уряд також доклав зусиль до того, аби бізнес-структури приділяли більшу увагу питанням кібербезпеки. Зокрема, було започатковано низку інформаційних кампаній та програм, орієнтованих на малий та середній бізнес. Так, у 2014 р. урядовий Департамент у справах бізнесу, енергетики та промислової стратегії розробив кампанію *Cyber Streetwise*, яка шляхом поширення інформації через соціальні мережі та рекламу закликала малий і середній бізнес дотримуватися п'яти дуже простих правил убезпечення від кібератак та кіберінцидентів: завжди встановлювати та періодично оновлювати антивірусне ПЗ, використовувати складні паролі, не завантажувати додатки та розширення невідомого походження, видаляти підозрілі електронні листи та періодично перевіряти *захищеність інформації, яку зберігає компанія*[141]. Згодом у 2016 р. *Cyber Streetwise* була перейменована на *Cyber Aware*[142], яку на сьогодні підтримують 128 партнерів, серед яких поліція та компанії у різних сферах бізнесу; за результатами кампанії понад 1 млн бізнес-структур висловили готовність дотримуватися базових правил кібербезпеки[143].

У 2014 р. також було розроблено та впроваджено схему сертифікації компаній на предмет відповідності базовим вимогам до кібербезпеки *Cyber Essentials*. Серед таких вимог: наявність на комп'ютерах мережевого екрану, безпечна конфігурація, контроль доступу користувачів, захист від шкідливого ПЗ, постійне контрольоване оновлення встановленого ПЗ. Компанія може звернутися до однієї з п'яти визначених урядом компаній, які проводять сертифікацію; сертифікація є обов'язковою, якщо фірма планує взаємодіяти з державними органами в рамках процесів, що передбачають обмін чутливою та конфіденційною інформацією, зокрема під час здійснення державних закупівель[144]. У період з 2014 по 2016 рр. було видано понад 2 тис. сертифікатів *Cyber Essentials*, а рекомендації з дотримання базових вимог до кібербезпеки були завантажені понад 50 тис. разів[145]. Серед інших прикладів рекомендаційних матеріалів для бізнесу слід також назвати «10 кроків до кібербезпеки», розроблені *GCHQ* у 2015 р.[146].

---

[138] The cyber threat to UK business 2016/2017: Report [Електронний ресурс]. – Режим доступу : https://goo.gl/uaQiSs

[139] The UK Cyber Security Strategy 2011–2016: Annual Report [Електронний ресурс]. – Режим доступу : https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/516331/UK_Cyber_Security_Strategy_Annual_Report_2016.pdf

[140] UK National Cyber Security Centre looks to future in annual review [Електронний ресурс]. – Режим доступу : https://goo.gl/9ixfGY

[141] Cyber streetwise: Open for Business [Електронний ресурс]. – Режим доступу : https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/273330/cyber_streetwise_open_for_business.pdf

[142] Cyber Aware [Електронний ресурс]. – Режим доступу : https://www.cyberaware.gov.uk/

[143] The cyber threat to UK business 2016/2017: Report [Електронний ресурс]. – Режим доступу : https://www.ncsc.gov.uk/content/files/protected_files/news_files/The%20Cyber%20Threat%20to%20UK%20Business%20 %28b%29.pdf

[144] How can Cyber Essentials help you? [Електронний ресурс]. – Режим доступу : https://www.cyberessentials.ncsc.gov.uk/about.html

[145] The UK Cyber Security Strategy 2011–2016: Annual Report [Електронний ресурс]. – Режим доступу : https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/516331/UK_Cyber_Security_Strategy_Annual_Report_2016.pdf

[146] 10 Steps to Cyber Security [Електронний ресурс]. – Режим доступу : https://www.ncsc.gov.uk/guidance/10-steps-cyber-security

З 2015 р. співпраця уряду та приватного сектору активно здійснюється в рамках програми *Cyber Growth Partnership* – майданчика для обміну досвідом між представниками бізнесу, науки та держави, пошуку ресурсів, тематичних заходів, рекомендацій, програм менторства. Однією з нещодавніх ініціатив в рамках цього партнерства було відкриття Центру кібердемонстрації (*Cyber Demonstration Centre*) у Лондоні. Урядовий Департамент цифрового розвитку, культури, медіа та спорту спільно з Департаментом міжнародної торгівлі встановили домовленість з бізнес-простором *Level*39, надавши малому і середньому бізнесу та стартапам можливість демонструвати свої пропозиції потенційним клієнтам та інвесторам у спеціально обладнаних приміщеннях[147]. Станом на жовтень 2017 р. до *Cyber Growth Partnership* входять 570 компаній та організацій, серед яких *Cisco*, *KPMG*, *Barclays*, платформа технологічних компаній *techUK* та багато інших[148]. Ця програма сприяє функціонуванню потужного хабу представників сектору кібербезпеки Великої Британії.

Прогресивним напрямом КДПП є безпосереднє залучення представників бізнесу до роботи у Національному центрі кібербезпеки. Запущена у лютому 2017 р. програма «*Industry* 100» передбачає залучення співробітників компаній у сфері кібербезпеки до різних структурних підрозділів *NCSC* (програма не передбачає постійного працевлаштування, оскільки співробітники *NCSC* є державними службовцями)[149]. Впродовж 2017–2018 рр. планується залучити 100 фахівців з приватних компаній. Нині *NCSC* не має оцінки проміжних результатів реалізації програми, однак відгуки перших залучених до роботи Центру фахівців у цілому можна назвати позитивними; доступними нині є понад 20 позицій, що може свідчити про відносно позитивну динаміку набору людей.

Поряд із програмами загального спрямування, які координуються з єдиного Національного центру кібербезпеки, різні урядові департаменти розробляють рекомендації щодо дотримання базових правил кібербезпеки у своїх сферах. Так, наприклад, Департамент транспорту у 2016 р. підготував рекомендації з кібербезпеки для залізничних перевізників[150]. Департамент у справах бізнесу, енергетики та промислової стратегії на початку 2017 р. розробив окрему Стратегію кібербезпеки для цивільного ядерного сектору, який на сьогодні забезпечує близько 18 % потреб Великої Британії в електроенергії[151]. Пізніше, цього ж року, Департамент транспорту, Центр захисту національної інфраструктури та Центр об'єднаних та автономних транспортних засобів випустили рекомендації із забезпечення необхідного рівня кібербезпеки при виробництві автомобілів та інших транспортних засобів[152]. Департамент охорони здоров'я підготував вимоги до забезпечення безпеки даних провайдерами послуг у сфері охорони здоров'я[153]. Хоча галузеві рекомендації і не є документами зобов'язуючого характеру та в цілому повторюють принципи, які впроваджує *NCSC*, однак вони забезпечують вищий рівень обізнаності суб'єктів різних галузей та акцентують увагу лише на необхідних для певної галузі заходів кібербезпеки.

Окремо слід відзначити, що держава приділяє значну увагу розвитку стартапів у сфері кібербезпеки. У межах державного бюджету передбачено створення спеціального фонду на підтримку інновацій у сфері оборони та кібербезпеки, в який спрямовуватимуться 165 млн фунтів стерлінгів щороку, з яких 10 млн фунтів стерлінгів призначатимуться

[147] The UK Cyber Demonstration Centre [Електронний ресурс]. – Режим доступу : https://cyberexchange.uk.net/#/cdc

[148] Cyber Exchange: Newsletter – October 2017 [Електронний ресурс]. – Режим доступу : https://cyberexchange.uk.net/media/admin/resources/Cyber%20Exchange%20Newsletter%20Oct%2017 %20FINAL.pdf

[149] Introduction to Industry 100 [Електронний ресурс]. – Режим доступу : https://www.ncsc.gov.uk/information/industry-100

[150] Rail Cyber Security: Guidance to Industry [Електронний ресурс]. – Режим доступу : https://goo.gl/X5HGwa

[151] Civil Nuclear Cyber Security Strategy [Електронний ресурс]. – Режим доступу : https://goo.gl/aGLjsC

[152] The key principles of vehicle cyber security for connected and automated vehicles [Електронний ресурс]. – Режим доступу : https://goo.gl/RTezf5

[153] 2017/18 Data Security and Protection Requirements [Електронний ресурс]. – Режим доступу : https://goo.gl/DyhmAV

на підтримку стартапів[154]. У січні 2016 р. Департамент цифрового розвитку, культури, медіа та спорту запустив спільно з акселератором *Cyber London* та Центром безпеки інформаційних технологій при Королівському університеті Белфаста програму ранньої підтримки стартапів, бюджет якої становив 250 тис. фунтів стерлінгів[155]. Програма згодом отримала назву «*HutZero*» та передбачає шестимісячний інтенсивний курс для 20 майбутніх підприємців[156]. У березні 2016 р. Департамент цифрового розвитку, культури, медіа та спорту, *GCHQ* та Національний центр кібербезпеки спільно з акселератором *Wayra UK*, який входить до міжнародної групи телекомунікаційних компаній *Telefónica Group* (у Великій Британії представлена дочірньою компанією *O*2 – другим за величиною ІКТ-провайдером у країні), започаткували програму *Cyber Accelerator*, метою якої є надання допомоги на розвиток найкращим стартапам у сфері кібербезпеки, які мають інноваційні розробки в актуальних для держави напрямах. Зокрема, після відбору спеціальною комісією у складі представників держави, *Wayra UK*, *Telefónica Group* та інвесторів, компанія матиме змогу отримати грант на 25 тис. фунтів стерлінгів, доступ до широкої мережі ресурсів та експертів, а також приміщення для початкового ведення діяльності[157]. За результатами першого набору програми, що тривав дев'ять місяців, сім стартапів загалом зібрали понад 2,7 млн фунтів стерлінгів[158].

На сьогоднішній день Велика Британія не обмежується лише інвестуванням у перспективний бізнес, але й заохочує бізнес інвестувати у передові дослідження у сфері кібербезпеки. У рамках інвестиційної програми «*CyberInvest*» уряд спільно з Радою досліджень у сфері фізики та інженерних наук забезпечують залучення приватного сектору до фінансової допомоги університетам, при яких створюються центри вивчення передового досвіду у сфері кібербезпеки (на 2017 р. такі центри діяли у 14 британських університетах[159]). Обсяг інвестицій варіюється від 10 тис. фунтів стерлінгів для малого бізнесу (до 10 співробітників) до 500 тис. фунтів стерлінгів для великих компаній (понад 250 співробітників), або ж компанії можуть допомагати обладнанням та іншими ресурсами. Впродовж наступних п'яти років 24 компанії, серед яких *IBM*, *Cisco*, *Airbus*, *Hewllett Packard* та інші, інвестують у дослідження понад 8 млн фунтів стерлінгів[160].

Окремим, але не менш важливим напрямом державно-приватного співробітництва варто визначити підтримку освітніх та професійних програм у сфері кібербезпеки. У чинній Стратегії кібербезпеки держави зазначається, що динамічне зростання сектору спричиняє розрив між попитом та пропозицією на ринку професіоналів з кібербезпеки, а отже, державна підтримка програм освітньої та професійної підготовки стає однією з необхідних умов забезпечення сталого функціонування держави у кіберпросторі[161]. Серед ключових проектів у цьому напрямі можна назвати програму «*CyberFirst*», що організовується Національним центром кібербезпеки у партнерстві з представниками індустрії та в рамках якої проводяться як короткострокові курси для дітей та молоді на тему кібербезпеки, так і надаються стипендії у розмірі 4 тис. фунтів стерлінгів для

---

[154] GCHQ Cyber Accelerator doubles down for second intake [Електронний ресурс]. – Режим доступу : https://techcrunch.com/2017/10/18/gchq-cyber-accelerator-doubles-down-for-second-intake/

[155] Making Cyberspace «Cyber Safe» – New Government initiative for Cyber startups will drive innovation [Електронний ресурс]. – Режим доступу : https://goo.gl/P1K8ne

[156] HutZer [Електронний ресурс]. – Режим доступу : http://www.hutzero.co.uk/

[157] Developing the UK's cyber security ecosystem through accelerating innovative start-ups [Електронний ресурс]. – Режим доступу : https://wayra.co.uk/gchq/

[158] Firms urged to apply for groundbreaking GCHQ cyber start-up scheme [Електронний ресурс]. – Режим доступу : https://www.ncsc.gov.uk/news/firms-urged-apply-groundbreaking-gchq-cyber-start-scheme

[159] Academic Centres of Excellence in Cyber Security Research [Електронний ресурс]. – Режим доступу : https://www.ncsc.gov.uk/articles/academic-centres-excellence-cyber-security-research

[160] CyberInvest [Електронний ресурс]. – Режим доступу : https://www.ncsc.gov.uk/articles/cyber-invest

[161] NATIONAL CYBER SECURITY STRATEGY 2016–2021 [Електронний ресурс]. – Режим доступу : https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

першокурсників, які планують будувати кар'єру у цій сфері; для талановитих студентів також є можливість пройти трирічну програму професійної підготовки «*Cyber First Degree Apprenticeship*»[162].

Більше того, *NCSC* станом на 2017 р. встановив партнерство з 25 університетами, завдяки чому студенти мають змогу отримувати сертифіковані *NCSC* бакалаврські та магістерські ступені з кібернетичної/інформаційної безпеки. Також *NCSC* підтримує чотири віртуальних дослідницьких інститути у сфері кібербезпеки[163]. У планах Великої Британії до 2020 р.: підготовка 6 000 підлітків у рамках програми *Cyber Schools Programme*, розширення програм стажування на різних підприємствах критичної інфраструктури та створення Академії кібернетичної оборони як центру передового досвіду Міністерства оборони та уряду в цілому[164]. Для представників бізнесу наразі є чимало безкоштовних онлайн-курсів[165].

3.4. Досвід Польщі

ДПП у Польщі часто трактується як співпраця між органами державного управління, органами місцевого самоврядування (польською – *administracji rządowe*; *administracji samorządowe*; *administracji publiczne*) й приватними організаціями у сфері надання публічних послуг. Принципово важливим для адекватного розуміння польського ДПП є функціональне в Республіці Польща (далі – РП) поняття «суспільні блага» (*dobra publiczne*; *the general welfare*)[166], яке поки що належним чином не увійшло 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 ідеться 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 споживати його й іншими людьми. Саме тому без будь-яких негативних наслідків чимало людей можуть водночас споживати одне й те ж саме суспільне благо.

У недемократичному суспільстві суспільні блага контролюються державою. З відповідної сфери життя зазвичай видаляють недержавних суб'єктів, що унеможливлює ДПП (в більшості випадків – в принципі, або уводить його в певні рамки штучних обмежень). У демократичному ж суспільстві суспільні блага є результатом спільної дії громадян, волю 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.

---

[162] CyberFirst Bursary and Degree Apprenticeship [Електронний ресурс]. – Режим доступу : https://www.ncsc.gov.uk/articles/cyber-first-bursary-scheme

[163] Academics and researchers [Електронний ресурс]. – Режим доступу : https://www.ncsc.gov.uk/Academics-and-researchers

[164] NATIONAL CYBER SECURITY STRATEGY 2016–2021 [Електронний ресурс]. – Режим доступу : https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

[165] Cyber security training for business [Електронний ресурс]. – Режим доступу : https://www.gov.uk/government/collections/cyber-security-training-for-business

[166] Dobra publiczne [Електронний ресурс] / Wikipedia. – Режим доступу : https://pl.wikipedia.org/wiki/Dobra_publiczne

Одним зі способів отримання суспільних благ є публічна (державна) послуга (*usługi publiczne*; *public service*)[167], яка в жодному разі не може бути зведеною до публічної (державної) монополії[168]. Тобто такі послуги держава може надавати не тільки безпосередньо, але й опосередковано, звертаючись до приватних структур та фінансуючи від імені суспільства подібну діяльність з бюджетних засобів.

У 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; поводження з 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, у традиційних або електронних бібліотеках)[169].

Таким чином, предметом ДПП є надання суспільних благ. Польський Інститут публічно-приватного партнерства виокремлює такі визначальні ознаки ДПП:

- співпраця публічного (державного) сектору з 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[170].

Окремі дослідники виокремлюють також такі форми ДПП[171]:

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 на 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 повністю бере на себе реалізацію контракту строком 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 діє схема: «побудова об'єкта – його експлуатація – передача об'єкта 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 крайні позиції: ототожнення цих форм взаємодії державного (публічного) та приватного партнерів та їх розмежування.

---

[167] Usługi publiczne [Електронний ресурс]. – Режим доступу : Wikipedia https://pl.wikipedia.org/wiki/Us%C5 %82ugi_publiczne

[168] Cesar A. Guimarães Pereira, Public-Private Partnerships (PPPs) and Concessions of Public Services in Brazil [Електронний ресурс]. – Режим доступу : www.bricslawjournal.com/jour/article/download/4/5

[169] Usługi publiczne.

[170] Partnerstwo Publiczno-Prywatne (PPP) [Електронний ресурс] / Instytut Partnerstwa Publiczno-Prywatnego. – Режим доступу : www.paih.gov.pl/files/?id_plik=16912

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

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 їх наступною передачею державному (публічному) власнику на засадах наведеного вище принципу «*Build-Operate-Transfer (BOT)*».

Зазвичай співпраця на засадах ДПП має довготерміновий характер через низьку окупність проектів у короткотривалій перспективі, з одного боку, та необхідністю надання гарантій якісної послуги – з іншого. У РП такі контракти укладають у межах 30–70 років. Власне будь-який проект, який обіцяє приватнику повернення вкладених у нього коштів, може бути реалізований на засадах ДПП.

У країнах ЄС ДПП розповсюджене нерівномірно. Найбільш інтенсивно така форма співпраці держави (місцевого самоврядування) з приватним сектором розвивалася в Великій Британії[172], Іспанії й Португалії. Зокрема, у Великій Британії, проекти, реалізовані на засадах ДПП, становлять 15 % від усіх інвестицій в державний сектор.

Польські дослідження свідчать про те, що зацікавленість у цій моделі співпраці з приватним сектором найнижча нагорі (на рівні центральних органів державної влади) і зростає у міру руху вниз – до владних органів воєводств, повітів та гмін. Найвищою була подібна активність на рівні міст на правах повітів[173].

Правове регулювання ДПП у РП тривалий час було відсутнє і лише у 2008–2009 рр. набули чинності два принципово важливі закони, які врегулювали ДПП та концесійну діяльність[174].

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

Істотно важливим у РП стало створення нових інституцій та інструментів, спроможних позитивно впливати на пришвидшення ринку ДПП. У 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 для реалізації урядової соціально-економічної політики й стратегії імплементації формули ДПП у практику надання публічних послуг;
- ***координаційні*** – забезпечення погодженої діяльності державних органів, відповідальних за ДПП;
- ***моніторингові*** – ідентифікація кількості та структури підприємницької активності на засадах ДПП;

---

[172] У Великій Британії впродовж останнього десятиліття на засадах «формули ДПП» побудовано понад 800 нових шкіл; 44 лікарні (після 1997 р.); 13 тюрем (де перебувають близько 10 % ув'язнених); дороги; залізниці; лінії лондонського метро; чимало урядових будівель (серед них – будівлі Амбасади Великої Британії у Берліні та Міністерства фінансів в Лондоні). До цього переліку слід додати численні проекти щодо охорони довкілля, поводження з відходами та громадського транспорту.

[173] Herbst Irena, Jadach-Sepioło Aleksandra, Korczyński Tomasz. Współpraca: Jagusztyn-Krynicki Tomasz, Mysiorski Bartosz, Zaremba Przemysław. Raport o partnerstwie publiczno-prywatnym w Polsce / Praca zbiorowa pod redakcją prof. dr hab. Jerzego Hausnera. – Warszawa, lipiec 2013. (Publikacja sfinansowana z grantu Fundacji S. Batorego przyznanego na realizację projektu upowszechniania PPP w Polsce).

[174] 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.

- ***аналітичні*** – оцінку 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 ухвалення.

26 липня 2017 р. Рада міністрів Республіки Польща ухвалила важливий документ «Політика Уряду у сфері розвитку публічно-приватного партнерства» («*Polityka PPP*»)[175]. У цьому документі перспективи розвитку ДПП подаються з позицій аналітичних оцінок конкретних можливостей польського ринку. Цей документ доповнює й конкретизує більш широкий документ – «Стратегію задля відповідального розвитку»[176] й увійшов до т. зв. «пакета Моравецького» (Матеуш Моравецький, який згодом очолив польський уряд, на той час був міністром інвестицій та розвитку РП)[177].

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 цього міністерства, присвячений поточним питанням ДПП[178].

Неоднозначним залишається питання вимірювання якості КДПП у Польщі. У 2015 р. організація, що репрезентує інтереси найбільших софтверних компаній світу *BSA – Software Alliance* (штаб-квартина – у Вашингтоні) проаналізувала стан кібербезпеки в усіх 28 країнах – членах ЄС й розробила відповідні рекомендації європейського представництва міжнародної організації[179].

Оцінювання проводилося 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 КДПП *BSA – Software Alliance* визнано п'ять країн ЄС: Австрію, Німеччину, Нідерланди, Іспанію й Велику Британію. Щодо інших країн ЄС, то стан КДПП у них визнано «або неіснуючим, або вельми обмеженим, або на найнижчому щаблі розвитку».

РП за всіма запропонованими критеріями посіла позицію «твердого середняка» й, згідно із запропонованою доповіддю *BSA – Software Alliance*, «мала комплексну стратегію з чітко сформульованими цілями». Йшлося про такий документ, як «Політика захисту кіберпростору Республіки Польща» від 25 червня 2013 р.[180], ухвалений Постійним комітетом Ради міністрів РП (*Komitet Stały Rady Ministrów*).

---

[175] Politykę Rządu w zakresie rozwoju partnerstwa publiczno-prywatnego [Електронний ресурс]. – Режим доступу : https://www.ppp.gov.pl/Aktualnosci/Documents/POLITYKA_PPP_0717.pdf

[176] Strategia na rzecz Odpowiedzialnego Rozwoju [Електронний ресурс]. – Режим доступу : https://www.mr.gov.pl/media/36848/SOR_2017_maly_internet_03_2017_aa.pdf

[177] SOR: administracja będzie zorientowana na usługi cyfrowe [Електронний ресурс]. – Режим доступу : https://www.onet.pl/?utm_source=biznes_viasg&utm_medium=nitro&utm_campaign=allonet_nitro_new&srcc=ust

[178] Departament Partnerstwa Publiczno-Prywatnego [Електронний ресурс]. – Режим доступу : https://www.ppp.gov.pl

[179] BSA – Software Alliance [Електронний ресурс]. – Режим доступу : http://www.bsa.org/about-bsa

На момент опублікування цієї доповіді *BSA – Software Alliance* серед 28 тодішніх членів ЄС лише 19 розробили стратегії кібербезпеки. Відповідних стратегій на той 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 за всіх (у 2008 р.) – Словаччина.

[180] Polityka ochrony cyberprzestrzeni Rzeczypospolitej Polskiej [Електронний ресурс]. – Режим доступу : https://goo.gl/VCXSTW

Більш критично поставилися до зазначеного документа польські контролери з «Найвищої контрольної палати»[181], які зауважили, що він є «результатом поганого компромісу», а тому не є дієздатним, позбавлений належної конкретики тощо. У документі навіть було виявлено «істотні помилки» (*błędy merytoryczne*).

На момент опублікування зазначеної 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[182].

Метою ***CERT.GOV.PL*** є забезпечення та розвиток потенціалу організаційних підрозділів державного управління РП для захисту від кіберзагроз, із 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*)»[183], ухваленої 9 березня 2009 р. Постійним комітетом Ради міністрів РП.

CERT Polska[184] діє від 1996 р. (до кінця 2000 р. – 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 у рамках *FIRST*;
- 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;
- розроблення 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 у сфері інформаційної безпеки, в т. ч. через публікацію інформації про безпеку в блозі *cert.pl* та у соціальних мережах *Facebook* і *Twitter*; організацію конференцій *SECURE*[185];
- незалежні аналізи та тести рішень у сфері IT-безпеки.

Серед проектів, які впродовж останнього періоду успішно реалізує NASK, слід виокремити такі[186]:

- ***ARAKIS-GOV*** – систему раннього попередження про інтернет-загрози, яка є результатом співпраці Департаменту телеінформаційної безпеки Агенції внутрішньої безпеки та команди *CERT Polska*, що діє в рамках *NASK*. *ARAKIS-GOV* був початково створений для підтримки та захисту ресурсів ІКТ державних адміністрацій, але завдяки співпраці з *CERT Polska* набуде додаткової функціональності.

---

[181] Realizacja przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni RP, Informacja o wynikach kontroli, KPB4101–002–00/2014 – nr ewid. 42/2015/P/14/043/KPB. / Departament Porządku i Bezpieczeństwa Wewnętrznego, Najwyższa Izba Kontroli. – Warszawa, 2015. – S. 12.

[182] Młotek Michał, Siedlarz Marcin. Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL

[183] Rządowy Program Ochrony Cyberprzestrzeni RP na lata 2009–2011 (RPOC).

[184] CERT Polska [Електронний ресурс]. – Режим доступу : https://www.cert.pl/

[185] SECURE 2018–22. KONFERENCJA NA TEMAT BEZPIECZEŃSTWA TELEINFORMATYCZNEGO [Електронний ресурс]. – Режим доступу : https://www.secure.edu.pl/pl/site.html

[186] PROJEKTY STRATEGICZNE [Електронний ресурс]. – Режим доступу : https://www.nask.pl/pl/dzialalnosc/projekty-strategiczne/145, Projekty-strategiczne.html

- ***ACADEMICA*** – проект оцифрування бібліотечних фондів, який реалізує Національна бібліотека та *NASK*, заснований під егідою Фонду польської науки (*Fundacja na Rzecz Nauki Polskiej*) та який фінансується з «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 унаслідок використання інтернет-комунікацій. Серед заходів пріоритетом є боротьба з незаконним і шкідливим вмістом Мережі.

Важливим кроком уперед у справі налагодження КДПП між Міністерством оцифрування й польським бізнесом став офіційний початок роботи 5 липня 2016 р. Національного центру кібербезпеки (*Narodowe Centrum Cyberbezpieczeństwa, NCC*), створеного на базі *CERT NASK*. 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 (*Włodzimierz Nowak*)[187].

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

Окрім «Політики захисту кіберпростору Республіки Польща», питання КДПП обговорюються передусім у таких документах РП:

- Доктрині кібербезпеки РП 2015 р.[188];
- Стратегії кібербезпеки РП на 2017–2022 рр.[189].

Доктрина кібербезпеки РП 2015 р. у четвертому розділі («Концепція підготовчих завдань у сфері кібербезпеки (підтримання й розвитку кібербезпекової сфери Польської Республіки)») пропонує підрозділ з ДПП (4.3.), де такі зусилля мають бути вжиті для того, щоб[190]:

- створити умови, що сприяють зростанню відповідальності 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 у сфері кібербезпеки.

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

---

[187] NCC – na straży cyberbezpieczeństwa [Електронний ресурс]. – Режим доступу : https://www.gov.pl/cyfryzacja/ncc-na-strazy-cyberbezpieczenstwa

[188] 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 [Електронний ресурс]. – Режим доступу : http://en.bbn.gov.pl/ftp/dok/01/DCB.pdf

[189] Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022 [Електронний ресурс]. – Режим доступу : https://www.gov.pl/documents/31305/0/strategia_cyberbezpieczenstwa_rzeczypospolitej_polskiej_na_lata_2017_-_2022.pdf/f249b627-4050-a6f4-5cd3-351aa025be09

[190] 4.3. PUBLICZNE I PRYWATNE OGNIWA WSPARCIA [Електронний ресурс]. – Режим доступу : http://en.bbn.gov.pl/ftp/dok/01/DCB.pdf

- 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 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 у сфері кібербезпеки.

У цьому ж документі підкреслюється: «Важливо створити систему підтримки досліджень та розробок у сфері кібербезпеки та освіти включно з проектами, реалізованими у співпраці зі світом науки і комерційних підприємств. Пріоритетним у цьому сенсі є створення системи сертифікації національних рішень, які можуть посприяти національній незалежності в технічному, програмному та криптологічному вимірах». У розвиток цієї 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 сфері управління ризиками в кібербезпеці.

Питання КДПП деталізує розділ 7 «Стратегії кібербезпеки РП на 2017–2022 рр.», ухваленої під егідою Міністерства оцифрування РП у 2017 р. Цей 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 структурі у цій групі опосередковано представляв Національний кібербезпековий центр *NASK*.

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

Розділ 4. АКТУАЛЬНІ ПИТАННЯ РОЗВИТКУ КДПП В УКРАЇНІ

Як і в усіх інших країнах, орієнтованих на демократичну модель розвитку, під безпосереднім (за формою власності і можливостями адміністративно-правового впливу) контролем держави в Україні перебуває лише частина національної критичної інформаційної інфраструктури (НКІІ). Значний її сегмент – у галузях енергетики, хімічної промисловості, транспорту, ІКТ, банківському секторі, комунальному господарстві тощо – перебуває у приватній та інших формах власності. Поряд із цим як український так і міжнародний досвід свідчить про те, що: 1) саме недержавні об'єкти кібербезпеки зазвичай є найбільш вразливими для кібератак[191]; 2) повноцінний захист таких об'єктів вимагає об'єднання зусиль приватного та державного секторів і системної взаємодії між ними; 3) широке, тобто не обмежене лише об'єктами НКІІ, КДПП є взаємовигідним і сприяє оптимізації галузевої державної політики та зміцненню національної безпеки (звісно, за умови адекватного інституційно-правового регулювання).

Критична потреба в розвитку КДПП обумовлена в сучасному світі низкою причин, серед яких експерти називають насамперед такі:

- активна приватизація деяких секторів критичної інфраструктури (що є не лише українським, але й глобальним трендом), унаслідок якої державні органи не можуть самостійно гарантувати повноту захисту критичної інформаційної інфраструктури;
- накопичення великої кількості електронних інформаційних ресурсів, які мають важливе значення для діяльності як приватних власників так і органів державного управління;
- залежність інфраструктури від інформаційно-телекомунікаційних систем та їхньої уразливості;
- зростаюча конвергенція комп'ютерних мереж, унаслідок чого ураження однієї з інформаційно-комунікаційних систем може суттєво позначитися на функціонуванні інших;
- у підприємств малого та середнього бізнеса зазвичай бракує повноважень і ресурсів для повноцінного захисту власної інформаційної інфраструктури, тому вони зацікавлені в отриманні відповідних послуг від державних органів та/або від крупних корпорацій[192].

Саме тому різні форми КДПП розглядаються нині як один з основних інструментів побудови ефективних систем кіберзахисту і широко застосовуються в міжнародній практиці. В ідеалі це дозволяє поєднати у формуванні національної системи кібербезпеки

[191] В Україні це добре продемонструвала, зокрема, атака вірусу NotPetya влітку 2017 р., причому з'ясувалося, що, крім суто технічних чинників (недосконалих, або просто відсутніх систем ТЗІ), основною причиною уражень у приватному секторі став т. зв. людський фактор, тобто неграмотність користувачів і недбалість та непрофесіоналізм ІТ-працівників.

[192] Марушак А., Панченко В. Взаємодія державного та приватного секторів у сфері кібернетичної безпеки: іноземний досвід та перспективи для України // Інформаційна безпека, людина суспільство держава. – 2014. – № 3 (16). – С. 56–63.

розмаїття ресурсів приватного (суспільного) сектору із системністю методичного державного регулювання кібербезпеки.

4.1. Нормативно-правове та інституційно-організаційне забезпечення КДПП в Україні

Ухвалення Верховною Радою 5 жовтня та підписання Президентом України 7 листопада 2017 р. Закону України «Про основні засади забезпечення кібербезпеки України», а також затвердження Указом Президента України (від 15 березня 2016 р. № 96/2016) національної Стратегії кібербезпеки заклали основи національного галузевого законодавства і визначили ключові вектори його подальшого розвитку відповідно до європейських демократичних практик. В обох документах значущу увагу приділено питанню правового регулювання КДПП (у зазначеному Законі застосовується форма «державно-приватна взаємодія» – ДПВ[193]).

І в Законі, і в Стратегії затверджується, що державно-приватна взаємодія є одним з принципів забезпечення кібербезпеки в Україні, а також одним із шляхів функціонування національної системи кібербезпеки, зокрема за допомогою «обміну інформацією про інциденти кібербезпеки, реалізації спільних наукових та дослідницьких проектів, навчання та підвищення кваліфікації кадрів у цій сфері». Стаття 10 «Державно-приватна взаємодія у сфері кібербезпеки» визначає основні напрями та види діяльності, де доцільно вдаватися до ДПВ у сфері кібербезпеки[194].

Як у цих базових документах, так і у відповідних підзаконних актах держава незмінно декларує готовність до системної роботи щодо розвитку ДПВ у сфері забезпечення кібербезпеки. Так, у розпорядженні Кабінету Міністрів України від 10 березня 2017 р. № 155-р «Про затвердження плану заходів на 2017 рік з реалізації Стратегії кібербезпеки України» як один з пріоритетних напрямів дій також визначене «формування стратегічних напрямів державно-приватної взаємодії у сфері кібербезпеки та пріоритетів, на які спрямовуються спільні зусилля для протидії кіберзагрозам»[195].

Заувага щодо необхідності «розробити та запровадити механізми ДПП для управління кіберзахистом критичної інформаційної інфраструктури у запобіганні кіберзагрозам та в умовах кризових ситуацій, надзвичайного стану, в особливий період» міститься також в рекомендаціях парламентських слухань «Реформи галузі інформаційно-комунікаційних технологій та розвиток інформаційного простору України», що відбулися у лютому 2016 р.[196].

Здійснення ДПП в Україні регулюється Законом «Про державно-приватне партнерство» (від 1 липня 2010 р. № 2404-VI з останніми змінами та доповненнями від 24.11.2015 р.). Згідно зі змістом проекти ДПП повинні відповідати таким основним критеріям: 1) мати довготривалий характер (понад п'ять років); 2) передбачати передання приватному партнеру частини ризиків у процесі реалізації проектів; 3) мати вищі техніко-економічні показники ефективності, ніж у разі реалізації без участі приватного партнера.

---

[193] У цьому дослідженні ми будемо використовувати поняття «державно-приватне партнерство» для всіх форм співробітництва крім випадків, де це стосується прямого посилання на норми Закону України «Про основи кібербезпеки України». Фактично обидва терміни («державно-приватна взаємодія» та «державно-приватне партнерство») використовуватимуться як рівнозначні, хоча вони і мають відмінне змістовне наповнення.

[194] Закон України «Про основні засади забезпечення кібербезпеки України» [Електронний ресурс]. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/2163–19

[195] Розпорядження КМУ «Про затвердження плану заходів на 2017 рік з реалізації Стратегії кібербезпеки України» [Електронний ресурс]. – Режим доступу : http://www.kmu.gov.ua/control/uk/cardnpd?docid=249807504

[196] Постанова Верховної Ради України «Про Рекомендації парламентських слухань на тему: «Реформи галузі інформаційно-комунікаційних технологій та розвиток інформаційного простору України»» [Електронний ресурс]. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/1073–19

Водночас, хоча базові положення Закону відповідають сучасним європейським правовим нормам та практикам, він, за оцінками експертів, має й певні недоліки. По перше, не встановлено мінімальну частку участі у проекті приватного партнера (зокрема, у розвинених країнах мінімальна частка приватного фінансування становить 25 %). Через це навіть мінімальна частка приватного фінансування у спільному проекті дозволяє відносити його до категорії ДПП, перекладаючи більшу частину відповідальності на державу. По-друге, відсутні чітко визначені механізми практичної реалізації (визначення етапів реалізації проектів ДПП, створення мотивації для іноземних інвесторів тощо). По-третє, залишається невизначеною роль Державного фонду регіонального розвитку у фінансуванні проектів ДПП[197].

Насамкінець, сфера забезпечення кібербезпеки у зазначеному законі не фігурує в переліку сфер застосування ДПП (стаття 4). З іншого боку, в Законі «Про основні засади забезпечення кібербезпеки України» вживається виключно термін «державно-приватна взаємодія», причому зі змісту Закону (включаючи перехідні положення) не зрозуміло, чи є така взаємодія різновидом ДПП згідно з визначеннями та нормами чинного законодавства щодо ДПП і, відтак, чи потрапляє вона під його дію. Враховуючи це, а також те, що (а) в ухваленій Верховною Радою редакції Закону «Про основні засади забезпечення кібербезпеки України» формулювання щодо ДПВ мають здебільшого описовий та абстрактний характер, і (б) зважаючи на відсутність пов'язаних підзаконних актів, можна констатувати, що здійснення ДПВ у сфері кібербезпеки поки не має в Україні адекватного нормативно-правового фундаменту.

Багато в чому питання про ДПП чи ДПВ є наслідком уже згаданих у першій частині цієї доповіді дискусій про можливість взагалі існування саме КДПП у певних сферах (зокрема – щодо захисту критичної інфраструктури). З метою уточнення цього пункту нами було спрямовано відповідні запити як до суб'єктів національної системи кібербезпеки України, так і неурядових структур, що опікуються кібербезпековою проблематикою.

Відповідно Міністерство оборони України пропонує[198] розглядати ці два поняття окремо, використовуючи обидва. Зокрема, під КДПП пропонується розуміти «комплекс заходів, що здійснюється державними органами влади з метою створення довірчих суспільних відносин з приватним сектором за визначеною законом домовленістю для створення сприятливих умов щодо забезпечення безпеки людини, суспільства та держави в кіберпросторі», в т. ч. як під ДПВ у сфері кібербезпеки – «діяльність, що здійснюється державними органами влади з метою задоволення суспільних потреб державного та приватного секторів у кіберпросторі». Відповідно перша діяльність більшою мірою спрямована на формування довірчих відносин, тоді як друга – на вирішення конкретних проблем державного та приватного секторів.

Національний банк України також звертає увагу на різницю в цих поняттях, акцентуючи увагу на тому, що спроба змінити/замінити поняття ДПВ на ДПП «призведе до звуження поняття державно-приватної взаємодії у сфері кібербезпеки та змінить концептуальні підходи і принципи такої взаємодії»[199].

Служба безпеки України в цьому питанні відштовхується від того, що «поняття «взаємодія» є найбільш близьким до взаємовідносин, які необхідно збудувати між органами державної влади та суспільством для налагодження взаєморозуміння, довіри та організації ефективної роботи у напрямку захисту життєво важливих інтересів людини і громадянина, суспільства і держави, національних інтересів України у кіберпросторі

[197] Особливості застосування державно-приватного партнерства як механізму реалізації нової регіональної політики [Електронний ресурс]. – Режим доступу : http://www.niss.gov.ua/articles/1239/

[198] Лист Міністерства оборони України № 123/2/171 від 03.03.2018 на запит НІСД № 293/54 від 31.01.2018.

[199] Лист Національного банку України № 56–0007/13334 від 06.03.2018 на запит НІСД № 293/54 від 31.01.2018.

в умовах ведення потужної кібервійни, яку здійснює РФ»[200]. Це зумовлено тим, що «ДПВ є одним з головних принципів забезпечення кібербезпеки держави, який передбачає широку співпрацю з громадянським суспільством у сфері кібербезпеки і кіберзахисту… вказаний принцип ґрунтується на спільній відповідальності держави та приватного сектору за стан забезпечення кібербезпеки, що передбачає передачу приватному партнеру частини ризиків, а також внесення останнім відповідних інвестицій у сферу забезпечення кібербезпеки держави. Принцип державно-приватної взаємодії, в першу чергу, спрямований на підвищення ефективності діяльності як державних, так і недержавних суб'єктів у сфері забезпечення кібербезпеки за умов їх належної співпраці, а також посилення спроможностей національної системи кібербезпеки України».

Крім того, СБУ визначає у своїй відповіді й перелік ключових напрямів у сфері ДПВ відповідно до компетенції СБУ (водночас цей перелік багато в чому можна екстраполювати і на більш широке коло завдань ДПВ в Україні у сфері кібербезпеки):

- надання власникам та операторам критичної інфраструктури інформації щодо виявлення кібератак та/або кіберінцидентів, вразливостей власних систем кіберзахисту;
- розроблення організаційно-правових засад та безпосереднє залучення фахівців приватного сектору (в т. ч. хактивістів) до проведення негласних перевірок готовності об'єктів критичної інфраструктури до кібератак та кіберінцидентів;
- організація на базі провідних ІТ-компаній тренінгів та навчальних програм з підвищення кваліфікації для фахівців СБ України;
- забезпечення виконання операторами та провайдерами телекомунікацій положень Конвенції РЄ про кіберзлочинність у частині термінового збереження та надання на вимогу компетентного правоохоронного органу даних, необхідних для протидії кіберзлочинності.

Водночас питання узгодження понять ДПП та ДПВ усе ще залишається актуальним як для нормативно-правового поля, так і для самої державної управлінської системи. Наразі функцію спеціально уповноваженого органу з питань ДПП в Україні виконує Міністерство економічного розвитку і торгівлі України (МЕРТ). Згідно з його даними, протягом 2016 р. в Україні ДПВ у сфері забезпечення кібербезпеки практично була відсутня (укладені тут договори могли відноситися хіба що до тих нерубрикованих 2,9 % угод, що фігурують у таблиці у стовпчику «Інше»)[201]. Дані з інших джерел переконливо свідчать, що у 2017 р. ситуація принципово не змінилася, що є закономірним, враховуючи крайню нерозвиненість нормативної бази, а також відсутність відповідної державної галузевої та комунікативної політики. Нині не лише в українських експертних, бізнесових та управлінських колах, але і в суспільстві широко представлені наративи та рішення щодо інформаційної та кібернетичної безпеки, але вони майже ніколи не асоціюються з КДПП. При цьому жоден з державних органів на сьогоднішній день не виконує функції координатора з питань ДПВ як загалом, так і у сфері кібербезпеки зокрема.

Таким чином, на нинішньому етапі для створення платформи державно-приватної взаємодії у сфері кібербезпеки державою ухвалені лише базові рамкові нормативні акти, проте не налагоджено діалог з експертними колами та суспільством і не створено жодних інституційно-правових інструментів такої взаємодії.

Поряд із цим чинне профільне законодавство має низку суттєвих вад. У контексті проблематики ДПП основними з них є такі:

- Відповідні нормативні положення сформульовані дуже широко, при цьому спостерігається гострий дефіцит пов'язаних підзаконних актів, спрямованих на розвиток

[200] Лист Служби безпеки України № 30/5/2–3288 від 05.03.2018 на запит НІСД № 293/54 від 31.01.2018

[201] Довідка щодо результатів здійснення ДПП (2017 рік) [Електронний ресурс]. – Режим доступу : http://www.me.gov.ua/Documents/Detail?lang=uk-UA&id=ed00a2ba-480a-4979–84eb-d610a0827a8c&title=ZagalniiOgliad

і конкретизацію цих положень[202]. Насамперед це стосується галузевого регулювання захисту об'єктів кібербезпеки (з урахуванням специфіки різних секторів економіки), унормування інституту незалежних аудиторів і, зрештою, визначення правового змісту самого поняття «державно-приватна взаємодія».

- Суперечливими є норми, що визначають порядок впровадження аудиту інформаційної безпеки на об'єктах НКІІ, встановлюють вимоги до аудиторів інформаційної безпеки і визначають порядок їх атестації[203]. Це створює потенційний простір для зловживань, тиску на недержавний сектор (передусім бізнес) і створення корупційних схем.
- Законом «Про основні засади забезпечення кібербезпеки України» встановлено, що порядок та методика здійснення аудиту кібербезпеки здійснюється на основі міжнародних стандартів, проте в його прикінцевих та перехідних положеннях немає жодної згадки про чинний Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», згідно зі статтею 7 якого «державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинні оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю». Очевидно, що під дію цієї норми потрапляють практично всі об'єкти критичної інформаційної інфраструктури, значна кількість яких перебуває в недержавному секторі (наприклад, в енергетиці, транспортній системі, телеком-індустрії, фармацевтиці тощо). Поряд із цим і сама Комплексна система захисту інформації (КСЗІ), базована на українському стандарті КСЗІ НД ТЗІ 2.5–004–99, і вимога її обов'язкового застосування на об'єктах НКІІ здебільшого піддається гострій критиці у вітчизняних експертних та бізнесових колах[204].

4.2. Стандартизація та сертифікація у кібербезпеці: джерело суперечностей чи підстава для реалізації КДПП

Питання стандартизації у сфері кібербезпеки та захисту інформації є предметом постійних дискусій між вітчизняною професійною спільнотою і профільними державними органами. Наразі в Україні як єдиний (крім банківського сектору) державний стандарт технічного захисту інформації діє серія нормативних документів, центральним з яких є НД ТЗІ 2.5–004–99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу»[205]. Стандарт розроблений на основі т. зв. Канадських критеріїв безпеки комп'ютерних систем (*Canadian Trusted Computer Product Evaluation Criteria* (*CTCPEC*))[206], а також з урахуванням прийнятих в 2005 р. міжнародних «Загальних критеріїв» (*Common Criteria for Information Technology Security Evaluation*

---

[202] Станом на жовтень 2017 р.

[203] Див. статті 5, 6, 8 Закону України «Про основні засади забезпечення кібербезпеки України».

[204] Закон про кібербезпеку та стратегія кібербезпеки України [Електронний ресурс]. – Режим доступу : http://uz.ligazakon.ua/ua/magazine_article/EA010553 ; Що не так із законопроектом про кібербезпеку та як його вдосконалити [Електронний ресурс]. – Режим доступу : https://ain.ua/2017/06/10/kiberbezpeka-v-nebezpeci ; Комплексні системи захисту інформації: бути чи не бути? [Електронний ресурс]. – Режим доступу : http://infosafe.ua/article-6 ; Кибербезопасность в Украине. Дискуссия [Електронний ресурс]. – Режим доступу : http://ko.com.ua/kiberbezopasnost_v_ukraine_diskussiya_121089

[205] НД ТЗІ 2.5–004–99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» [Електронний ресурс]. – Режим доступу : http://web.archive.org/web/20121202025850/http://am-soft.ua/files/KSZI/2.5-004-99.pdf ; Інформаційний перелік документів Фонду нормативних документів у сфері технічного та криптографічного захисту інформації [Електронний ресурс]. – Режим доступу : http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=89740&cat_id=89734

[206] Національний стандарт інформаційної безпеки, розроблений Центром безпеки відомства безпеки зв'язку Канади (*Canadian System Security Centre Communication Security Establishment*) у 90-х роках XX ст. Докладніше див.: https://en.wikipedia.org/wiki/Canadian_Trusted_Computer_Product_Evaluation_Criteria

(*ISO* 15408))[207]. На відміну від найпоширенішої у світі серії *ISO/IEC*27000, яка сфокусована на менеджменті інформаційної безпеки, критерієм захищеності інформації в НД ТЗІ 2.5–004–99 є відповідність архітектури та параметрів програмно-апаратних засобів об'єкта чіткому регламенту – комплексній системі захисту інформації (КСЗІ). З точки зору фахівців, сама ідея, внутрішня структура і модель впровадження КСЗІ здебільшого не відповідає вимогам сучасного кіберзахисту, особливо в недержавному секторі. Зазвичай експерти вказують на такі її недоліки, як:

- **недостатня гнучкість**. Концепція КСЗІ вимагає ретельного документування архітектури та всіх налаштувань системи захисту інформації, а при внесенні будь-яких змін – складного й бюрократизованого процесу переатестації (до кількох місяців). Досить очевидно, що така статична модель захисту мало корелює з динамікою та розмаїттям бізнес-процесів, та й взагалі є не зовсім неадекватною викликам сучасного кіберпростору;
- **громіздкість**. Підходи НДТЗІ, що вимагають створення великої кількості документації, є занадто громіздкими для приватного бізнесу;
- **обмежені можливості масштабування**. КСЗІ/НДТЗІ не підходять для великих організацій/підприємств, приміром для заводів, де можуть використовуватися великі розподілені системи спостереження та керування промисловими процесами (наприклад, *SCADA/ACK ТІТ*[208])[209];
- **застаріла концепція захисту/захищеності**. Модель КСЗІ/НДТЗІ орієнтована на захист інформації в інформаційно-комунікаційній (комп'ютерній) системі як такій, без урахування конкретних безпекових потреб об'єкта кіберзахисту загалом. Як свідчить міжнародний досвід, у сучасних умовах значно більший ефект дає проактивний, т. зв. ризик-орієнтований підхід, який передбачає моніторинг, імовірнісний аналіз та оцінювання ризиків (за шкалою – від прийнятних до неприпустимих) суб'єкта господарювання у певній екосистемі з метою дотримання кібербезпеки шляхом управління цими ризиками.

Нині у світі існує ціла низка відкритих для використання міжнародних стандартів кібербезпеки, але насамперед варто згадати про два їх різновиди, оскільки (а) саме вони задають нині у світі певну концептуально-технологічну рамку і широко застосовуються в багатьох країнах, а до того ж (б) у них враховані найсучасніші тренди розвитку і відсутні вади, властиві українському НД ТЗІ 2.5–004–99.

По-перше, це серія міжнародних стандартів *ISO/IEC*27000[210], розроблена Міжнародною організацією з стандартизації (*ISO*) спільно з Міжнародною електротехнічною комісією (*IEC*), яка постійно доповнюється новими документами. Серія, по суті, являє собою модель (фреймворк) для розробки, впровадження, функціонування, моніторингу, аналізу, підтримки та поліпшення системи менеджменту інформаційної безпеки як на загальному рівні (27001), так і в окремих секторах та галузях, – таких як фінанси, транспорт, енергетика, охорона здоров'я, оператори зв'язку, хмарні обчислення, інфраструктурні проекти, аудит і сертифікація тощо.

Впровадження системи управління інформаційною безпекою (СУІБ) відповідно до *ISO/IEC*27000 дозволяє оптимізувати процес захисту інформаційних ресурсів і управління ризиками для цих ресурсів. У нашій країні статус державного стандарту отримала

---

[207] *Common Criteria* є методологічною базою для визначення вимог захисту комп'ютерних систем від несанкціонованого доступу, створення захисних систем та оцінки ступені захищеності. З допомогою критеріїв *Common Criteria* можливо порівняти різні механізми захисту інформації та визначити необхідну функціональність таких механізмів у розробці захищених комп'ютерних систем.

[208] Автоматизована система керування технологічним процесом [Електронний ресурс]. – Режим доступу : https://goo.gl/p1V2tU

[209] Що не так із законопроектом про кібербезпеку та як його вдосконалити [Електронний ресурс]. – Режим доступу : https://ain.ua/2017/06/10/kiberbezpeka-v-nebezpeci

[210] ISO/IEC27000 family – Information security management systems [Електронний ресурс]. – Режим доступу : https://www.iso.org/isoiec-27001-information-security.html

перша версія *ISO/IEC*27001 (найновішою є *ISO/IEC*27001:2013), проте де-факто імплементований він лише в банківській сфері – у вигляді вимог СОУ Н НБУ 65.1 СУІБ 1.0: 2010[211] (згідно із Законом «Про основні засади забезпечення кібербезпеки України» Національний банк України є одним з суб'єктів національної системи кібербезпеки). Практичне застосування *ISO/IEC*27001 в інших галузях української економіки та бізнесу поки залишається відкритим через нормативно-правову неврегульованість.

Одним із найбільш авторитетних і відомих у світі є також *National Institute of Standarts and Technology Cybersecurity Framework* (*NIST CSF*)[212] – розроблений американським Інститутом стандартів і технологій для організацій приватного сектору США комплекс методологій та рекомендацій щодо зниження IT-ризиків, запобігання, моніторингу і реагування на кібератаки. Фреймворк є відкритим, призначений виключно для добровільного використання і достатньо «гнучкий» для адаптації в різних умовах/країнах, що зумовило його поширеність у світі. Уперше *NIST CSF* був випущений у 2014 р., в поточному році винесений на обговорення проект (*draft version*) версії 1.1[213].

Треба відзначити, що нормальною світовою практикою є розробка і застосування у разі необхідності альтернативних або призначених для тих чи інших секторів недержавного сектору стандартів та фреймворків з кібербезпеки. Серед іншого, це дозволяє уникати надмірної регуляторної монополізації, недоброчесної конкуренції й корупції, що нині особливо актуальне для України. Наприклад, хоча близько 70 % приватних організацій у США сьогодні віддають перевагу *NIST Cybersecurity Framework*[214], в американському енергетичному секторі діють стандарти *NERC CIP*[215], розроблені Північноамериканською корпорацією із забезпечення надійності електросистем (*North American Electric Reliability Corporation*), яка, до речі, є неприбутковою недержавною організацією. Варто наголосити, що саме ці стандарти рекомендують запровадити в українському ПЕК експерти київського відділення *ISACA*.

Довідково. ***ISACA*** – міжнародна професійна неприбуткова асоціація, орієнтована на IT-менеджмент. Об'єднує фахівців у сфері IT-аудиту, IT-консалтингу, управління IT-ризиками та інформаційною безпекою. Основним завданням асоціації є розробка і формалізація єдиних ефективних підходів до оцінки та управління IT-процесами та IT-системами (докладніше див. http://www.isaca.org.ua/). У листопаді 2014 р. Адміністрація Державної служби спеціального зв'язку та захисту інформації України та київське відділення *ISACA* уклали меморандум про співробітництво у сфері кібербезпеки та інформаційних технологій. У сфері аудиту і стандартизації IT-організація має низку напрацювань і розробок, які становлять безсумнівний інтерес з точки зору зміцнення національної системи кібернетичної безпеки. Зокрема:
CobiT (акронім англ. *Control Objectives for Information and Related Technology* («Контрольні цілі для інформаційних та суміжних технологій») – відкритий міжнародний IT-стандарт, який в свою чергу містить низку документів зі стандартами щодо оптимізації управління IT: аудитом IT та IT-безпекою. Створено Асоціацією з аудиту та контролю інформаційних система (*ISACA*) спільно із Інститутом управлінням IT (*IT Governance Institute – ITGI*). Перше видання – 1996 р. У 2012 р. відбувся реліз поточної версії – *CobiT* 5[216].
ITAF – (*Information Technology Assurance Framework*) – еталонна модель використання кращих практик, до якої можуть звертатися фахівці з аудиту та підтвердження довіри до інформаційних систем (ІС) за настановами, для дослідження політики і процедур, отримання програм аудиту та підтвердження довіри, а також формування ефективних звітів[217].

---

[211] Методи захисту в банківській діяльності. Система управління інформаційною безпекою: Вимоги [Електронний ресурс]. – Режим доступу : https://kyianyn.files.wordpress.com/2010/12/nbu-27001.pdf

[212] Cybersecurity Framework [Електронний ресурс]. – Режим доступу : https://www.nist.gov/cyberframework

[213] Draft Version 1.1 [Електронний ресурс]. – Режим доступу : https://www.nist.gov/cyberframework/draft-version-11

[214] NIST Cybersecurity Framework Adoption Hampered By Costs, Survey Finds». Information Week Dark Reading. Retrieved 2016–08–02.

[215] (CIP) Critical Infrastructure Protection [Електронний ресурс]. – Режим доступу : http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

[216] Громадська організація «ISACA Київ» [Електронний ресурс]. – Режим доступу : http://www.isaca.org.ua/index.php/standards

[217] Там само.

Такі рекомендації зустрічають розуміння в українському бізнесі. Так, саме згідно з *NERC CIP* (у комплексі зі стандартами *NIST 800-SERIES, IEC62443* та *ISO 27000*) побудований та сертифікований захист критичної ІТ-інфраструктури в ТОВ ДТЕК Енерго. Крім того, самим Міністерством енергетики та вугільної промисловості України зміцнення кібербезпеки українського паливно-енергетичного комплексу також мислиться як створення комплексної галузевої системи кібербезпеки, причому з орієнтацією саме на кращі міжнародні норми та практики[218]. У «Типовому положенні про інформаційну безпеку підприємств ПЕК», розміщеному на офіційному веб-порталі міністерства, є положення щодо «реалізації вимог міжнародних стандартів з інформаційної безпеки *ISO 27000-series, ISA 099-series* та *IEC 62443*»[219]. Останні два – спеціалізовані відкриті стандарти, оптимізовані в тому числі для застосування на об'єктах критичної інфраструктури приватної форми власності. Таким чином, можна говорити про те, що в українському ПЕК уже зараз триває формування єдиного пакета галузевих стандартів з інформаційної безпеки.

На отримання міжнародної сертифікації у сфері інформаційної безпеки в Україні орієнтовані також й інші приватні гравці, у т. ч. великі. Наприклад, компанія *De Novo* – найбільший в Україні провайдер хмарових сервісів, яка має сертифікат відповідності вимогам українським стандартам КСЗІ для свого сервісу *G-Cloud* (хмара для органів державної влади), водночас впровадила у середині 2017 р. систему управління інформаційною безпекою (СУІБ) і отримала сертифікат відповідності згідно з міжнародним стандартом *ISO 27001*[220].

Але з урахуванням викладеного вище, незрозуміло, наскільки такі дії Міненерго і *De Novo* корелюють із чинним законодавством у частині стандартизації та сертифікації інформаційної та кібернетичної безпеки.

4.3. Досвід релізації КДПП в Україні

Поряд із викладеним вище і недержавний сектор в Україні, і державні відомства (поки що – деякі з них) демонструють значний потенціал для формування повноцінної платформи КДПП у загальнонаціональних масштабах. Наприклад, саме на засадах ДПП триває робота над створенням в Україні потужного центру з кібербезпеки на базі ДК «Укроборонпром». Крім представників РНБОУ, Міністерства оборони, СБУ, ДССЗЗІ, Департаменту кіберполіції, фахівців НАТО, консультантів турецької державної компанії *HAVELSAN* та спеціалістів НТУУ «КПІ», у проекті беруть участь громадська неприбуткова організація «Українська академія кібербезпеки»[221] і українська команда «білих» хакерів *DCUA* (одна з найсильніших у світі)[222]. Проект державного концерну «Укроборонпром» *Cyber Guard* був реалізований у партнерстві з приватними компаніями для захисту від кібератак приватних і державних установ України[223].

---

[218] Створення комплексної системи кібербезпеки – пріоритетне завдання [Електронний ресурс]. – Режим доступу : http://mpe.kmu.gov.ua/minugol/control/publish/article?art_id=245224502

[219] Типове положення про інформаційну безпеку підприємств ПЕК [Електронний ресурс]. – Режим доступу : http://195.78.68.67/minugol/doccatalog/document?id=245167627

[220] Безпека хмарних сервісів De Novo підтверджена сертифікатом ISO 27001 [Електронний ресурс]. – Режим доступу : https://goo.gl/MAoW8k

[221] Ukrainian Academy of Cyber Security [Електронний ресурс]. – Режим доступу : http://www.uacs.kiev.ua/

[222] В Україні за підтримки НАТО створять єдиний центр з кібербезпеки [Електронний ресурс]. – Режим доступу : https://goo.gl/4NL8TX;

[223] Проект державного концерну «Укроборонпром» у партнерстві з приватними компаніями [Електронний ресурс]. – Режим доступу : https://cyberguard.com.ua/

З кінця 2015 р. в Україні, крім державного *CERT-UA*, діє офіційно акредитований міжнародною мережею *FIRST*[224] приватний центр реагування та боротьби з кіберінцидентами (*computer emergency response team*, або *CERT*). Ідеться про вітчизняну компанію *CyS-Centrum*, яка спеціалізується на моніторингу й нейтралізації ІБ-загроз з використанням апаратно-програмних рішень власної розробки, а також на консалтингу у сфері інформаційної безпеки[225].

Ще у квітні 2015 р. МВС України та корпорація «Майкрософт» підписали Меморандум про взаєморозуміння, який засвідчив взаємну зацікавленість у співпраці у сфері захисту даних, інформаційної та кібербезпеки. У листопаді 2017 р. подібний же меморандум, спрямований на організацію взаємодії в побудові комплексних рішень технічного забезпечення відомчої діяльності у масштабах держави, застосування інновацій у сфері держуправління, а також оптимізації наявного ресурсу, був підписаний представниками Національної поліції України та компанії «Майкрософт Україна»[226].

Особливо високу динаміку розвитку КДПП демонструє Департамент кіберполіції Національної поліції України. Зокрема, з 2016 р. налагоджена системна співпраця між відомством і українськими профільними компаніями *ProtectMaster* (*protectmaster.org*) і *Berezha Security* (*berezhasecurity.com*), а також з громадською організацією «Експертів кібербезпеки» (залучення фахівців, обмін даними, проведення спільних конференцій, тренінгів для держслужбовців). Департаментом також організовано регулярний обмін інформацією та досвідом з фахівцями з Харківського національного університету радіоелектроніки (ХНУРЕ) і Національного аерокосмічного університету ім. М.Є. Жуковського «ХАІ». Крім того, за підрахунками спеціалістів кіберполіції, збільшити ефективність реагування на кіберзагрози в декілька разів дозволило розміщення онлайн-форми зворотного зв'язку на її сайті[227].

У вересні 2017 р. за сприяння Української асоціації операторів зв'язку «Телас» було підписано меморандум про співпрацю між Департаментом кіберполіції й дата-оператором *lifecell*, за умовами якого останній на безоплатній основі передав Департаменту систему власної розробки для екстреного інформування в умовах надзвичайних ситуацій *Emergency Notification System (ENS)*. Серед іншого, система дає змогу локалізувати кіберзагрозу й уникнути її розповсюдження за допомогою оперативного інформування про небезпеки завчасно визначених груп отримувачів через голосові виклики, *SMS* та електронні листи. За повідомленнями керівництва, *ENS* вже успішно пройшла тестування й її абонентами можуть стати як державні, так і приватні компанії, включаючи об'єкти критичної інфраструктури[228].

Водночас цей потенціал співробітництва міг би бути більшим і заінтересованість в цьому засвідчують і державні органи. Наприклад за даними Міністерства оборони України[229], протягом 2014–2017 рр. ним уже отримано позитивний досвід

---

[224] ***FIRST*** (акронім від англ. – *Forum for Incident Response and Security Teams* – Форум команд реагування на інциденти інформаційної безпеки) – є міжнародною добровільною мережною спільнотою окремих команд спеціалістів у сфері інформаційної та кібернетичної безпеки (*CERT teams*), створеною передусім з метою вивчення кіберзагроз та протидії їм у глобальному вимірі. У межах *FIRST* можуть працювати представники урядових, правоохоронних, наукових, бізнесових та інших кіл, але їхня діяльність регулюється Координаційним Комітетом організації. Варто наголосити, що членство команди у *FIRST* означає її міжнародне визнання, а крім того, це надає можливість системно та оперативно взаємодіяти з 326 іншими командами *CERT* із 73 країн світу, що робить їхню роботу значно ефективнішою (докладніше див.: https://www.first.org/).

[225] Сайбер Секьюрити Центрум [Електронний ресурс]. – Режим доступу : https://cys-centrum.com/ru

[226] МВС та «Майкрософт» підписали Меморандум про співпрацю в галузі кібербезпеки [Електронний ресурс]. – Режим доступу : https://www.npu.gov.ua/uk/publish/article/1422098

[227] Кіберполіція взаємодіє з приватними компаніями з кібербезпеки з метою підвищення ефективності розкриття злочинів [Електронний ресурс]. – Режим доступу : https://goo.gl/GnQ1e6 ; Компания ProtectMaster активно взаимодействует с государством [Електронний ресурс]. – Режим доступу : https://goo.gl/6HsXhK

[228] Сергій Демедюк: Кіберполіція використовуватиме систему екстреного сповіщення у випадках кіберзагроз [Електронний ресурс]. – Режим доступу : https://goo.gl/Ef2ZNH ; Кіберполіція запроваджує в Україні глобальну систему сповіщення про загрози [Електронний ресурс]. – Режим доступу : https://goo.gl/snoAGA ; Кіберполіція зможе терміново інформувати про кіберзагрози [Електронний ресурс]. – Режим доступу : https://goo.gl/N9aBLg

[229] За матеріалами листа Міністерства оборони України № 123/2/171 від 03.03.2018 на запит НІСД № 293/54 від 31.01.2018.

реалізації низки проектів забезпечення кібербезпеки у форматі КДПП, у першу чергу в контексті відбиття російської інформаційної агресії та проведення АТО на території Донецької та Луганської областей. При цьому МО зацікавлене в розширенні спроможностей Збройних Сил України щодо підготовки та здійснення кібероборони та планує організацію державно-приватного партнерства за основними напрямами щодо:

- створення кіберрезерву;
- використання інфраструктури та обчислювальних спроможностей;
- отримання консультаційної та матеріальної допомоги.

Зазначену діяльність на цей час розпочато у взаємодії з Громадською радою при Міністерстві оборони України та провідними ІТ-компаніями України.

Національний банк України як один із ключових проектів у сфері ДПВ розглядає створений ним Центр кіберзахисту (*CSIRT-NBU*), у межах якого «організована взаємодія і співробітництво Центру кіберзахисту з банками України, більшість з яких є приватними, і стане основою державно-приватної взаємодії в банківській системі України у сфері кібербезпеки»[230].

Служба безпеки України також напрацювала[231] значний досвід у сфері ДПВ. Зокрема, за результатом аналізу світового досвіду (в т. ч. у країнах НАТО) використання систем на кшталт «*Malware Information Sharing Platform*»[232] (*MISP*) фахівцями Департаменту контррозвідувального захисту інтересів держави у сфері інформаційної безпеки СБУ створено адаптивний програмний продукт *Malware Information Sharing Platform and Threat Sharing* «*Ukrainian Advantage*» (*MISP-UA*), який враховує особливості інформаційного обміну між різними групами користувачів (суб'єктами та об'єктами кібербезпеки та кіберзахисту): забезпечено розподіл прав доступу, розширено функціонал з аналітичної обробки інформації та впроваджено розширену політику безпеки. Крім того, з розпорядниками окремих об'єктів критичної інфраструктури досягнуто попередніх домовленостей щодо надання доступу до інформаційної системи *MISP-UA* з метою обміну ідентифікаторами компрометації, що використовувались у цільових кібератаках. Розроблено проект Меморандуму про обмін інформацією з використанням інформаційної системи *MISP-UA*.

Також з ініціативи СБУ започатковано спільний з Радою Європи проект *Cybercrime@EAPIII*, спрямований на зміцнення співробітництва державних, у т. ч. правоохоронних і спеціальних органів країн – членів Східного партнерства, з приватним ІТ-сектором у сфері протидії кіберзагрозам, а також використання електронних доказів у досудових розслідуваннях. У межах цього проекту незалежними експертами вже розроблено проект Меморандуму про порозуміння з питань співпраці в боротьбі з кіберзлочинністю та злочинами, під час доведення яких використовуються електронні докази. Крім зазначеного вище протягом 2016–2017 рр. СБУ проводила різноманітні заходи (круглі столи, семінари тощо) за участю представників зацікавлених органів державної влади, спеціальних та правоохоронних органів та провайдерів України з питань стану імплементації положень Конвенції РЄ про кіберзлочинність.

Одним з найбільш важливих та перспективних напрямів КДПП є освітній напрям – підготовка кваліфікованих кадрів і поширення серед працівників компаній та пересічних користувачів культури інформаційної та кібернетичної безпеки (запуск загальнонаціональної програми «комп'ютерного лікнепу»).

---

[230] Лист Національного банку України № 56–0007/13334 від 06.03.2018 на запит НІСД № 293/54 від 31.01.2018.

[231] Лист Служби безпеки України № 30/5/2–3288 від 05.03.2018 на запит НІСД № 293/54 від 31.01.2018.

[232] Платформа для збирання, обробки та обміну інформацією про інциденти кібернетичної безпеки, а також технічними даними про ідентифікатори компрометації інформаційних систем об'єктів критичної інфраструктури в режимі реального часу між суб'єктами сектору безпеки.

Відомо, що Україна має значний потенціал у цій сфері. Бакалаврів та магістрів за спеціальністю «Кібербезпека» готують 44 вітчизняних ВНЗ (у тому числі при профільних відомствах – ДССЗЗІ, СБУ, МВС, МО України, розвідувальних органах) і обсяги державного замовлення на цих фахівців останніми роками постійно зростають[233]. Діють та розвиваються також спеціалізовані державні та комерційні центри підвищення кваліфікації та тренінгу. Разом із цим як експерти-освітяни, так і професійна ІТ-спільнота констатують наявність системних проблем у цій сфері. Наприклад, у річному звіті VIII Українського форуму з управління Інтернетом *IGF-UA* (жовтень 2017 р.) зазначається:

- відсутність належного рівня кваліфікації в підготовці сучасних фахівців з питань кібербезпеки та інформаційної безпеки в закладах освіти;
- низькій рівень зарплати професорсько-викладацького складу в інститутах та фінансування фахівців у державних компаніях;
- застарілу навчальну програму з підготовки фахівців з питань кібербезпеки та інформаційної безпеки;
- відсутність координації в системі освіти між замовниками кадрів та закладами освіти;
- відірваність фахівців з інформаційної та кібербезпеки від міжнародної системи стандартизації;
- брак наукових досліджень з проблем кібербезпеки[234].

Експертні дослідження свідчать, що в сучасному світі підготовка кадрів із кібербезпеки не може обмежуватися лише отриманням вищої освіти у ВНЗ за відповідною спеціальністю. Для збереження належної конкурентоспроможності та професійного рівня цим фахівцям необхідно перманентно підвищувати свою кваліфікацію на засадах т. зв. концепції безперервної освіти (або «освіти протягом життя»), множинність форм та методів якої відкриває ще один широкий та перспективний напрям для галузевої КДПП. Можливі декілька варіантів роботи в цьому напрямі, серед яких перепідготовка в рамках післядипломної освіти фахівців у споріднених з кібернетичною безпекою спеціальностей, застосування нелінійної схеми підготовки фахівців, використання потенційних можливостей неформальної освіти для підвищення кваліфікації діючих фахівців через проведення тренінгів, семінарів, міжнародних стажувань тощо[235].

Критично важливим є також забезпечення належного рівня обізнаності персоналу компаній та установ в питаннях кібернетичної та інформаційної безпеки, – знову ж таки спільними зусиллями приватних та державних суб'єктів. Форми КДПП тут можуть бути різноманітними: спільні семінари, тренінги, онлайн-курси, залучення науково-аналітичних та консалтингових компаній всіх форм власності і багато іншого. Крім того, необхідними є регулярні тестування (навчання) на проникнення, моделювання загроз, грамотність поведінки працівників/користувачів у мережі (дотримання елементарних правил онлайн-безпеки, стійкість до спроб фішингу тощо).

Статтею 10 чинного Закону «Про основні засади забезпечення кібербезпеки України» «створення системи підготовки кадрів» та «підвищення цифрової грамотності громадян» визначені як одні з напрямів КДПП. Поряд із цим значною мірою невирішеним залишається питання інституційно-правового забезпечення повноцінної реалізації цієї норми.

---

[233] Довідник ВНЗ [Електронний ресурс]. – Режим доступу : https://osvita.ua/vnz/guide/search-17-0-0-42-43-0.html

[234] VIII Український форум з управління Інтернетом IGF-UA [Електронний ресурс]. – Режим доступу : https://goo.gl/FQxQjx

[235] Напрями підготовки та підвищення кваліфікації фахівців із кібербезпеки [Електронний ресурс]. – Режим доступу : http://pgp-journal.kiev.ua/archive/2017/3/45.pdf ; Проблемні питання та актуальні завдання підготовки фахівців з кібернетичної безпеки галузі знань «інформаційні технології» [Електронний ресурс]. – Режим доступу : http://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe? C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/szi_2016_2_3.pdf ; Корнейко Олександр. Безпека кіберпростору України: сучасні виклики та підготовка фахівців [Електронний ресурс]. – Режим доступу : http://inau.ua/doc/6/all

Украй важливим є постійний та системний обмін даними щодо актуальних кіберзагроз і можливостей (інструментів) боротьби з ними. Для цього оптимальним було би створення та підтримка на основі широкої КДПП національної системи обміну даними про кіберінциденти та їх реєстр. Це дозволило б підрозділам з ІТ-безпеки компаній та установ перевіряти маркери компрометації, відслідковувати, кому ще розсилалися аналогічні зразки шкідливого програмного забезпечення, обмінюватися індикаторами атак, убезпечуючи таким чином свої об'єкти від кіберзлочинців[236].

В Україні поки не існує такої системи, однак необхідно наголосити, що її створення є складною проблемою у більшості країн світу, причому в зв'язку з позицією саме недержавних (передусім бізнесових), а не державних акторів. Керівництво таких підприємств та компаній зазвичай вважає ДПВ у цій сфері занадто ризикованим через небезпеку розкриття комерційної таємниці та іміджевих втрат, пов'язаних з оприлюдненням даних про кіберінциденти в межах компанії. Понад це свою вагому роль відіграють такі чинники, як різна динаміка роботи і прийняття рішень у державних (бюрократичних) та комерційних організаціях, а також недостатня інтероперабельність їх інформаційних інфраструктур[237].

З іншого боку, в міжнародній практиці для обміну інформацією про атаки та загрози, розслідувань кібератак, експертної підтримки і т. ін. широко та успішно практикується ДПВ з галузевими асоціаціями і приватними компаніями, що спеціалізуються на ІБ-рішеннях[238]. Вітчизняний потенціал і чинне законодавство (статті 7 та 10 Закону «Про основні засади забезпечення кібербезпеки України») цілком дозволяють налагодити в Україні КДПП такого напряму, навіть більше – існують окремі приклади її успішної реалізації (див. вище). Водночас, для того щоб така взаємодія в нашій країні набула системного загальнонаціонального характеру, потрібні інституційні важелі (наприклад, у вигляді організованих державою постійно діючих платформ для комунікації й налагодження співробітництва) та відповідний нормативно-правовий інструментарій для її стимулювання/регулювання і юридичного оформлення. Нині все це повноцінно не реалізоване.

З точки зору українських фахівців[239], які спеціально досліджували світовий досвід КДПП, найдоцільніше організовувати її на таких принципах і засадах:

- формування відносин довіри між державними суб'єктами (регуляторами) кібербезпеки і керівництвом приватних підприємств;
- створення умов, за яких приватні об'єкти кіберзахисту добровільно приводитимуть свої програми управління ризиками у відповідність до вимог регулятора (галузевих регуляторів) та надаватимуть всю необхідну інформацію в інтересах захисту критичної інфраструктури;
- постійне врахування галузевої специфіки процесів інформатизації та дотримання кібербезпеки у різних секторах економіки, запровадження інституту галузевих регуляторів;
- основними контактними (координуючими) суб'єктами захисту критичної інфраструктури повинні бути тільки державні установи;
- діяльність державних структур унормована (суворо регламентована) у стосунках з приватним сектором – у розвитку ДПВ належить використовувати інструментарій пільг і привілеїв;

---

[236] Cybercrime: системи захисту «нарощують м'язи» [Електронний ресурс]. – Режим доступу : https://goo.gl/YwcRei

[237] Марушак А., Панченко В. Взаємодія державного та приватного секторів у сфері кібернетичної безпеки: іноземний досвід та перспективи для України // Інформаційна безпека людини, суспільства, держави. – 2014. – № 3(16). – С. 56–63.

[238] Попередні пропозиції ГО «ІСАКА Київ» щодо покращення Закону «Про основні засади забезпечення кібербезпеки України» [Електронний ресурс]. – Режим доступу : https://goo.gl/ve38K8

[239] Марушак А., Панченко В. Взаємодія державного та приватного секторів у сфері кібернетичної безпеки: іноземний досвід та перспективи для України // Інформаційна безпека людини, суспільства, держави. – 2014. – № 3(16). – С. 56–63.

- створення співтовариств для обміну інформацією (наприклад, на основі концепції *Information Exchange Model*, як це реалізовано у Великій Британії[240]);
- організація *CERT* у різних галузях і на різних рівнях;
- розробка та розвиток у рамках ДПВ спільних автоматизованих систем моніторингу кібератак (на кшталт польської системи *ARAKIS-GOV*[241]).

Із порівняльного аналізу цього переліку і викладених вище фактів випливає, що станом на осінь 2017 р. в Україні триває формування окремих елементів загальнонаціональної системи державно-приватної взаємодії у сфері кібербезпеки, проте сама система як така поки відсутня.

4.4. Хактивізм та державно-приватне партнерство: від протиправної діяльності до легального співробітництва з державою

Протягом останніх чотирьох років спостерігалося помітне зростання ролі волонтерських та громадських структур, які допомагали державі в різних аспектах національної безпеки. Ця допомога набула особливого значення в перші роки конфлікту на сході України із російсько-терористичними силами.

Не стала винятком і кіберсфера. Проукраїнські хактивісти (зокрема, «Українські кібервійська», «Кіберсотня», «*FalconsFlame*», «*Trinity*», «*RUH*8» та інші) здійснювали:

- злами комп'ютерних систем – як терористів, так і їх російських кураторів;
- отримували доступ до поштових скриньок осіб, які задіяні в організації та реалізації російської агресії проти України;
- відслідковували аккаунти в соціальних мережах та мережі Інтернет, через які терористичні угруповання вели свою агітацію та збирали кошти;
- блокували окремі електронні гаманці фінансистів терористів;
- допомагали у ідентифікації осіб, які беруть участь у збройному протистоянні на сході України проти сил АТО та багато іншого.

Вочевидь для класифікації їх діяльності найбільш доцільно використовувати концепцію «кольорових капелюхів» (*hats*)[242], що вже стала звичною при характеристиці дій хакерських (чи просто ІТ-експертних) угруповань. «Білі капелюхи» (*White hat*) зазвичай є повністю легальними ІТ-фахівцями, що здійснюють свою діяльність законно і частіше за все – на комерційній основі. Основна їх мета – вдосконалення систем кібербезпеки тих чи інших структур (державних чи приватних), у т. ч. через пошук недоліків коду тих інформаційних систем, які використовують ці структури. Основний інструмент – пентест[243]. Важливим є те, що ці дії вони застосовують на запит самої організації та за чіткою попередньою домовленістю з нею.

Іншим полюсом є «чорні капелюхи» (*Black hat*), які більшою мірою є традиційними кіберзлочинцями, що здійснюють свою діяльність заради особистого зиску, використовуючи будь-які методи зламу. Водночас послугами таких груп дедалі частіше користуються військові та розвідувальні структури задля досягнення своїх військово-політичних цілей, але мінімізуючи при цьому юридичні наслідки від такого втручання

---

[240] Марушак А., Панченко В. Взаємодія державного та приватного секторів у сфері кібернетичної безпеки: іноземний досвід та перспективи для України // Інформаційна безпека людини, суспільства, держави. – 2014. – № 3(16). – С. 58–59.

[241] ARAKIS-GOV [Електронний ресурс]. – Режим доступу : http://www.cert.gov.pl/cee/arakis-gov-system/78, ARAKIS-GOV-system.html

[242] Традиція поділяти хакерів за капелюхами бере початок з американського кіновестерну, де позитивні герої традиційно носили білі капелюхи, тоді як злодії та негативні персонажі – чорні.

[243] Пентест (penetration test, pentest) – оцінювання захищеності комп'ютерної системи чи мережі шляхом часткового моделювання дій зовнішніх зловмисників з проникнення у неї.

(неможливість визнання відповідальності держав за такі атаки). В таких випадках «чорні капелюхи» виступають як своєрідні «проксі-групи», аналогічні за своєю суттю до різноманітних форм найманців, які здійснюють свою діяльність проти України з територій «ДНР/ЛНР».

Водночас українські хактивісти швидше підпадають під третю класифікаційну групу – «сірих капелюхів» (*Grey hat*). До них відносяться хакери чи фахівці з комп'ютерної безпеки, які почасти порушують законодавство чи типові етичні норми, але не здійснюють деструктивного впливу на зламану систему, що є типовим для «чорних капелюхів». Така характеристика проукраїнських хакерських груп меншою мірою стосується їх діяльності проти інформаційних ресурсів «ДНР» та «ЛНР», а також російських інформаційних ресурсів, щодо яких вони діють саме як «чорні капелюхи».

Останнім часом їх безпосередня активність дедалі частіше спрямовується на внутрішні інформаційні системи (передусім – державні органи та об'єкти критичної інфраструктури), щодо яких вони проводять несанкціоновані пентести, скачуючи при цьому окремі документи (які не мають грифів обмеження доступу) для підтвердження наявності уразливості. Незважаючи на те, що ці дії здійснюються ними в інтересах забезпечення більшої кібербезпеки держави в умовах агресії (принаймні така мета ними публічно декларується), але відповідно до чинного українського законодавства, частіше за все вони його порушують.

Показовим у цьому сенсі був випадок із українським програмістом О. Моховим, який у 2013 р. помітив уразливість у системі «Приват-24»[244] та, здійснивши декілька тестів уразливості, звернувся до Служби безпеки ПриватБанку. Однак фактично експлуатацію цієї уразливості можна було кваліфікувати як порушення законодавства (про що і заявила тоді прес-служба банку[245]), у т. ч. – статті 361 КК України. Надалі ситуацію урегулювали, однак при цьому принципова проблема не зникла.

Ще більш виразно проблема своєрідної «негнучкості» українського законодавства щодо діяльності у кіберпросторі проявилась у історії навколо акції[246] (флешмобу) «*Ukrainian Cyber Alliance*» під загальним хештегом *#F*ckResponsibleDisclosure*[247], який розпочався у листопаді 2017 р. За словами організаторів, його мета – «*громадська акція для підвищеня рівня IT-гігієни*» (по суті акція є формою краудсорсингового пентесту державних інформаційних систем). У межах флешмобу були знайдені уразливості в комп'ютерних системах щонайменше 10-ти ЦОВВ (у т. ч. – правоохоронних органів), декількох облрад, мінімум п'яти об'єктів, які можна віднести до критичної інфраструктури держави, низки наукових та комунальних закладів.

Щонайменше одна з атакованих структур звернулась до поліції[248] із заявою щодо незаконного вторгнення в локальну комп'ютерну мережу облради.

Слід визнати, що з погляду чинного законодавства дії «*Ukrainian Cyber Alliance*» тією чи іншою мірою дійсно порушують статтю 361 Кримінального кодексу України[249]: «несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів),

---

[244] Как КПИшник Алексей Мохов взломал ПриватБанк [Електронний ресурс]. – Режим доступу : http://kpishnik.com/mohov-privat24/

[245] ПриватБанк обвинил украинского программиста во взломе своего Android-приложения [Електронний ресурс]. – Режим доступу : https://habrahabr.ru/post/193204/

[246] F*ck responsible disclosure. Привет от очень злых хакеров [Електронний ресурс]. – Режим доступу : https://petrimazepa.com/disclosure.html

[247] Responsible Disclosure – форма пошуку уразливостей інформаційних систем, за якою першим про її наявність повідомляється власник системи (для того, щоб він міг її виправити) і лише з певним часовим проміжком про цю уразливість повідомляють громадськість. Концепція «Full disclosure» не передбачає паузи для інформування власника системи. Більш докладно про сутність поняття «Responsible Disclosure» та небажання авторів флешмобу його дотримуватись – у матеріалі за посиланням: https://www.facebook.com/vstyran/posts/10155958884177372

[248] За даними офіційного повідомлення на сайті установи.

[249] Аналогічна оцінка діяльності «*Ukrainian Cyber Alliance*» міститься і в листах окремих суб'єктів національної системи кібербезпеки України.

автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку»[250]. Фактично згадана стаття розглядає будь-яке втручання (в т. ч. те, яке не нанесло безпосередньої шкоди) до автоматизованої системи чи комп'ютерної мережі як злочин, адже внаслідок дій «*Ukrainian Cyber Alliance*» відбувся витік інформації. Формулювання зазначеної статті КК фактично унеможливлює діяльність некомерційних пентестерів, якщо ці тести заздалегідь не погоджені із об'єктами атаки.

Вочевидь діяльність груп на кшталт «*Ukrainian Cyber Alliance*» із виявлення вразливостей в інформаційних системах (у т. ч. – органів державної влади) є важливою і цілком підпадає під сутнісні ознаки державно-приватного партнерства, однак потребує свого повноцінного законодавчого вирішення. Передусім – задля виведення таких хактивістів з-під дії статей КК України та організації їх діяльності у легальний спосіб, який би не наносив шкоди державним ресурсам і не створював передумови для застосування правоохоронними органами статті 361.

Одним із варіантів вирішення проблеми є уточнення статті 361 додатковим пунктом 3, таким чином, як сформульовано у статті 111 КК «Державна зрада», де зазначено, що «звільняється від кримінальної відповідальності громадянин України, якщо він на виконання злочинного завдання іноземної держави, іноземної організації або їх представників ніяких дій не вчинив і добровільно заявив органам державної влади про свій зв'язок з ними та про отримане завдання». Таким чином йдеться про форму попередження відповідальних органів державної влади про дії, які можуть бути трактовані як злочин відповідно до положень статті КК.

Крім того, слід визнати, що діяльність «*Ukrainian Cyber Alliance*» та схожих на них хактивістів (які відрізняються від комерційних пентестерів, які узгоджують свої дії зі структурою, щодо якої проводиться пентест) вочевидь частково підпадає під формулювання «негласна перевірка готовності об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів», що відповідно до Закону України «Про основні засади забезпечення кібербезпеки України»[251] покладено на Службу безпеки України. Водночас може виникнути певна юридична проблема через те, що стаття 361 КК України підвідомча Національній поліції України, дії таких активістів, можливо, мають узгоджуватися не лише зі Службою безпеки України, а й з Національною поліцією (профільним департаментом).

Важливо відзначити, що «негласна перевірка» є складовою оперативно-розшукової діяльності, яка у Законі України «Про оперативно-розшукову діяльність» визначена як «система гласних і негласних пошукових, розвідувальних та контррозвідувальних заходів, що здійснюються із застосуванням оперативних та оперативно-технічних засобів», а, відповідно до українського законодавства, і Служба безпеки України, і Національна поліція України є суб'єктами проведення оперативно-розшукової діяльності.

Неоднозначним видається і пошук практичного механізму співпраці – швидше за все це актуалізує принаймні ще дві проблеми, які стануть тлом для дискусії з цього приводу.

По-перше, сам механізм та необхідність активістів узгоджувати свої дії із правоохоронними/контррозвідувальними структурами можуть стати питанням складних перемовин. Не в усіх випадках неурядові структури бажають узгоджувати свої дії із правоохоронними/контррозвідувальними органами, часто вбачаючи в цьому обмеження своїх прав та можливостей, а також незалежності дій. Крім того, публічне артикулювання фактів такого співробітництва може мати негативні іміджеві наслідки для таких структур. Тому пошук практичного механізму співпраці має базуватися на гарантуванні

[250] Кримінальний кодекс України [Електронний ресурс]. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/2341-14/print

[251] Закон України «Про основні засади забезпечення кібербезпеки України» [Електронний ресурс]. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/2163-19/

нерозголошення інформації про таку співпрацю та мінімально необхідних бюрократичних процедурах для ініціювання перевірки.

По-друге, вирішення проблеми з урахуванням результатів такого тестування для безпосереднього поліпшення кібербезпеки протестованих структур. Останнє особливо важливо для хактивістів, оскільки одна з основних їх претензій та обґрунтувань формату проведення флешмобу полягала у системному ігноруванні установами інформації про уразливості в інформаційній системі тієї чи іншої державної структури, які надавались хактивістами.

Важливо відзначити ще один аспект: відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» суб'єкти кібербезпеки реалізують свої повноваження передусім щодо об'єктів критичної інфраструктури. Сайти ж органів державної влади, їх внутрішні комп'ютерні мережі швидше за все не підпадуть під ознаки об'єктів критичної інфраструктури. Тож потрібно або уточнити положення зазначеного Закону, або ж передбачити можливість використання механізму співпраці з активістами і для цієї сфери в інших законах України.

Незважаючи на те, що вирішення зазначеної (можливо – суто тактичної) проблеми може видатися неістотним на тлі більш значущих проблем, однак пошук рішення варто розглядати у більш широкому контексті. Зокрема, напрацювання механізму роботи таких ІТ-експертів у взаємодії із органами сектору безпеки та оборони можуть напрацювати ефективні моделі і для інших сфер, де досягнення консенсусу все ще є далекою перспективою. Фактично, забезпечення ефективної співпраці буде важливим елементом у формуванні атмосфери довіри між учасниками КДПП, а отже – сприяти реалізації більш масштабних проектів.

4.5. Розвиток КДПП в Україні: від політики «великих надій» до «малих кроків»

Як і більшість світових держав, які або вже сформували стратегічні пріоритети своєї кібербезпекової політики, або лише формують їх, Україна ставить питання про розвиток державно-приватного партнерства. Водночас у цьому питанні спостерігаються дві помітні тенденції.

З одного боку, в офіційних заявах та коментарях потенційних учасників ДПП визнається як ключовий елемент кібербезпекової системи держави, що потрібно максимально розвивати. Більше того, часто таке КДПП представляється як своєрідна «панацея» від усіх проблем у сфері кібербезпеки, а отже, на його розвиток покладають великі надії як експерти, так і громадськість.

З іншого боку, особливих практичних кроків у цьому напрямі не відбувається, а сторони, які декларують бажання розвивати КДПП, частіше за все обмежуються заявами, не бажаючи змінювати реальний статус-кво. І проблема виходить не лише з державних установ (як це часто сприймається суспільною думкою) – недержавні учасники також почасти використовують дискусію щодо КДПП з популістською метою і не мають на увазі перехід до реального співробітництва.

У цьому сенсі показовим є і досвід авторів цієї доповіді при збиранні відповідних матеріалів: для отримання позицій та поглядів державних та недержавних суб'єктів у сфері кібербезпеки (або пов'язаних із нею) було спрямовано запити п'ятьом ключовим суб'єктам національної системи кібербезпеки України та п'ятьом неурядовии структурам (з яких дві асоціації, одна міжнародна та дві українські НУО). Відповідь було отримано лише від трьох державних установ – **жодна** з неурядових структур так і не відповіла.

Водночас це не відміняє наявності макропроблеми – майже цілковитої закритості даних про стан українського кібербезпекового сектору загалом, що ускладнює

формування довіри до державних суб'єктів. Навіть із урахуванням особливостей утаємничення процесів планування в секторі безпеки та оборони, ступінь закритості в кібербезпековій сфері залишається надзвичайно високим.

Понад те, закритість спостерігається не лише щодо інформування суспільства та фахівців, але й часто щодо самих суб'єктів забезпечення кібербезпеки держави. Держава почасти опиняється в ситуації, коли достеменно не знає, яким ресурсом володіє і які можливості мають її органи. Це унеможливлює побудову дійсно цілісної та ефективної системи кібербезпеки держави, що складається як із захисних, так і з наступальних систем та засобів. Окремі дані щодо стану кібербезпеки держави оприлюднюються лише *CERT-UA*, а в деяких випадках – СБУ та МВС (у вигляді повідомлень про затримання тих чи інших зловмисників). Інша статистична інформація майже відсутня або надається за окремими запитами.

Це призводить до того, що проблеми сфери кібербезпеки, а також пошук шляхів їх вирішення більшою мірою базуються на суб'єктивному сприйнятті її стану окремими фахівцями сектору кібербезпеки України.

У багатьох випадках обидві сторони КДПП виявляються неспроможними знайти для себе аргументи в межах тих ключових драйверів, які й обумовлюють появу проектів КДПП.

Слід констатувати, що в багатьох випадках КДПП потребує не стільки риторики «завищених очікувань», скільки дуже практичної політики «малих кроків», яка реалізується через конкретні проекти з низьким рівнем конфліктності чи суперечності інтересів. Саме вони мають вирішувати ключову проблему, яка уповільнює будь-який прогрес на шляху КДПП, – **брак довіри** у суб'єктів КДПП один до одного, а відтак – і до співпраці. Формування довіри має стати одним із ключових пріоритетів найближчого часу. Більшою мірою на це має бути спрямовано створення різноманітних дискусійних майданчиків, експертних обговорень, запуск нескладних спільних проектів у форматі КДПП.

Саме щодо останнього спостерігається помітна проблема – в Україні відчувається нестача проектів, які б могли стати дійсно ініціюючими для більш широкого обговорення щодо сутності КДПП та, з одного боку, могли б визначити напрями такої співпраці, а з іншого – сама їх реалізація могли б стати прикладом КДПП.

Одним із таких спільних проектів може стати підготовка спільного документа щодо стану сектору кібербезпеки України. Вимога проведення такого огляду закріплена і в Стратегії кібербезпеки України. Зокрема, у п. 4.4 (п. п. 2) зазначається про необхідність «періодичного проведення огляду національної системи кібербезпеки, розроблення галузевих індикаторів стану кібербезпеки». Тож для цього є, принаймні, нормативна вимога, що вже формує базу для діалогу у форматі КДПП. Зазначений огляд, підготовлений із залученням усіх зацікавлених сторін, мав би дати відповіді на питання про стан кібербезпекової сфери України, її реального ресурсного потенціалу, а також щодо шляхів оптимізації кібербезпекового сектору.

Сам процес створення такого огляду міг би стати прикладом ефективної співпраці суб'єктів національної системи кібербезпеки та недержавних структур. Зважаючи на те, що, вочевидь, переважна частина документа має бути відкритою (не виключаючи при цьому наявність закритої частини), майже на всіх етапах підготовки документа до цього процесу доцільно залучати представників ключових індустрій (що є операторами критичної інфраструктури), наукові установи, неурядові організації профільного спрямування а також експертів з недержавного сектору.

Ідейно цей огляд міг би взяти за основу традиційний оборонний огляд ЗС України, в межах якого формується стратегія розвитку ЗС України на довгострокову перспективу, її гармонізація з наявними ризиками, можливостями та ресурсами, що є однією з цілей проведення оборонного огляду. Цей же огляд є підставою для здійснення ефективного оборонного планування.

Структурно Огляд міг би включати в себе такі елементи.

1. **Ступінь розвитку та основні загрози у сфері кібербезпеки**	Це аналіз загроз не лише на національному, а й на міжнародному рівні. Фактично цей розділ – це принципове бачення авторів Огляду того кібербезпекового середовища, в якому держава має вирішувати свої завдання із захисту національних інтересів. Він же визначає ті ключові параметри, що впливають на завдання, які стоять перед Україною у сфері оптимізації власної кібербезпекової системи.
2. **Визначення сил, які потрібно залучити для вирішення завдань протидії виявленим загрозам та негативним сценаріям розвитку**	Принаймні загальна (теоретична) оцінка тих сил, які знадобляться державі для ефективної протидії ключовим викликам, виявленим у першому розділі. Цей розділ може бути частково «закритим» (у частині, що стосується кількісних показників), однак відповідні дані повинні стати доступними тим фахівцям з кібербезпекових питань, які мають необхідний рівень допуску до державної таємниці.
3. **Оцінка наявних можливостей сектору безпеки щодо протидії виявленим загрозам та негативним сценаріям розвитку**	Важлива складова, що може мати як відкриту, так і закриту частини. Відкрита частина більшою мірою може зазначати ті публічні відомості про стан органів сектору безпеки і оборони, що задіяні у процесі захисту кібернетичного простору держави. Водночас закрита частина має містити цілісну інформацію про структуру цих органів, їх склад, дані аудиту їх потенціалу, основні проблеми[258].
4. **Аналіз стану кадрового, фінансового, матеріально-технічного та інших видів забезпечення органів сектору безпеки**	Критично важливий розділ. Однак, якщо оцінка наявних можливостей переважно зосереджена на організаційних та інституційних можливостях, то в цьому розділі йтиметься про технічні та фінансові ресурси, завдяки яким органи сектору кібербезпеки можуть виконувати покладені на них завдання. Крім того, цей же розділ має дати відповіді на питання, якими є відносини державних суб'єктів сектору кібербезпеки із недержавним сектором.
5. **Формування оптимальної моделі забезпечення завдань убезпечення кіберпростору з урахуванням реальних можливостей та ресурсів**	На основі аналізу попередніх пунктів доцільно сформувати найбільш функціональні моделі забезпечення кібербезпеки держави, ключові пріоритети та завдання розвитку.
6. **Визначення найбільш перспективних альтернативних стратегій досягнення поставлених завдань**	Розуміючи, що суспільно-економічне середовище надзвичайно динамічне, мають бути запропоновані й альтернативні стратегії досягнення ключових цілей. У т. ч. як за умов збільшення фінансування та ресурсів, так і при їх зменшенні чи взагалі в умовах воєнного часу.

Організаційно проведення огляду доцільно здійснювати на двох основних майданчиках – Апарату РНБО України (Національного координаційного центру кібербезпеки) та НІСД. Перший має необхідні можливості збирання та узагальнення даних з основних органів державної влади та ключових суб'єктів кібербезпеки держави. НІСД може виступити майданчиком для обговорень зазначених питань науковцями, громадськими організаціями та приватними структурами.

Ще одним напрямом може і має стати спільна підготовка загальної Концепції (Плану дій) КДПП, яка б конкретизувала як положення Стратегії кібербезпеки в цій частині, так і Закону України «Про основні засади забезпечення кібербезпеки України». Створення такого Плану дій є і однією з важливих рекомендацій *ENISA* в частині розвитку ДПП: «Дуже важливим для державних структур є чітке та відверте комунікування своїх потреб та обмежень для бізнес-сектору. Створення контактної точки (*point of contact*), можливо, є найбільш видимим аспектом цього айсбергу. Але значно більш важливим є те, щоб державні органи, які хочуть розвивати КДПП, до того, як запросять

[252] Показово, що за результатами відповідей суб'єктів національної системи кібербезпеки України на запит НІСД в жодному з них поки що не було проведено оцінки необхідних ресурсів для реалізації ДПП у сфері кібербезпеки, що також стане одним із важливих завдань такого Огляду.

приватний сектор долучитись до процесу, дуже добре розуміли, чого вони дійсно хочуть досягти, яким буде їхній внесок та що має внести приватний сектор у таке співробітництво. Якщо бути максимально лаконічними: майте стратегію до того, як приєднаєтесь до ДПП»[253].

Крім зазначеного, сторони мають шукати ширшого діалогу з метою реалізації тих проектів, які при мінімальних зусиллях можуть встановлювати формати спочатку короткострокової, а потім і довгострокової співпраці. На першому етапі це можуть бути проекти, спрямовані на:

- дослідження та аналіз (передусім спільні дослідження загроз та можливих нових технологій);
- розвиток керівництв із «найкращих практик»;
- спільні навчання (на першому етапі це можуть бути суто командно-штабні навчання);
- підвищення обізнаності (спільні інформаційні кампанії);
- визначення стандартів (на першому етапі – формування постійної групи для дискусій навколо ключових стандартів у сфері кібербезпеки);
- обмін статистичними даними.

Саме в цих проектах участь неурядового та наукового секторів може бути критично важливою. Більшою мірою фахівці, які не належать безпосередньо ані до державних, ані до приватних структур, можуть виступити фасілітаторами дискусій між основними гравцями (частково нівелюючи тим самим брак взаємної довіри), передусім при:

- формуванні базового переліку сфер/цілей КДПП (як для держави, так і приватного сектору);
- визначенні критеріїв, за яких КДПП стане привабливим рішенням для обох сторін;
- допомозі обом сторонам КДПП у визначенні цілей партнерства;
- формуванні довгострокових стратегій такого партнерства.

Важливим питанням є створення основи для механізму «обміну інформацією». Видається, що на сьогоднішній день жодна зі сторін КДПП не має об'єктивних можливостей (розуміючи під ними не лише ресурсну, але й психологічну готовність) для реалізації таких проектів, зважаючи на те, що вони потребують високого рівня довіри між учасниками. Тож спроби (з обох сторін) якимось чином штучно інтенсифікувати цей процес будуть, вочевидь, невдалими і лише збільшуватимуть конфліктність відносин між потенційними суб'єктами КДПП.

[253] Public Private Partnerships (PPP) Cooperative models [Електронний ресурс]. – Режим доступу : https://www.enisa.europa.eu/publications/public-private-partnerships-ppp-cooperative-models/at_download/fullReport

ВИСНОВКИ

1. КДПП все ще залишається надзвичайно складним та неоднозначним явищем, яке формується в умовах взаємної недовіри учасників та браку методологічних підходів для розуміння самої сутності ДПП у цій царині. Хоча більшість розвинених країн мають тією чи іншою мірою працюючі форми КДПП, однак майже в кожному випадку вони формуються у режимі *ad-hoc* і під значним впливом історичного досвіду кожної конкретної країни. Крім того, можна відзначити, що фактично жодній країні сьогодні не вдалося створити систему КДПП, яку б можна було назвати взірцевою і яка б повністю вирішувала всі ключові питання, що виникають у сфері кібербезпеки.

2. На загальноєвропейському рівні все ще більшою мірою спостерігається процес візіонерства в царині КДПП, хоча ключові стратегічні документи у сфері кібербезпеки включають і складову ДПП. Зокрема, Європейська Комісія ініціювала план дій, основою якого слугують Стратегія єдиного цифрового ринку від 2015 р., Кіберстратегія Європейського Союзу від 2013 р. та Директива ЄС щодо мережевої та інформаційної безпеки, що має бути включена в національне законодавство країн – членів ЄС до 9 травня 2018 р. та у внутрішні статутні документи основних підприємств до 9 листопада 2018 р.

3. У межах пошуку ефективних форм КДПП Європейська Комісія провела програми консультацій з великим, малим та середнім бізнесом, асоціаціями, дослідницькими інституціями, громадським сектором, органами державної влади та органами регіонального рівня. Тривалість консультацій – 12 тижнів. Вочевидь застосований ЄК механізм консультацій має стати основою і для відповідного процесу, якого потребує й Україна.

4. Незважаючи на те, що КДПП є в цілому вигідним для обох секторів, приватні компанії все ще з пересторогою ставляться до його реалізації. Одними з ключових проблем залишаються проблеми довіри, контролю та розкриття корпоративної інформації.

5. Майже всі проаналізовані країни мали виразні акценти розвитку КДПП лише в одному чи двох аспектах, хоча на нормативно-правовому рівні (передусім – у стратегічних документах щодо забезпечення кібербезпеки) КДПП описувалось як базовий елемент, що потребує всебічного розвитку для всіх компонентів.

6. Зокрема, для США одним із основних напрямів КДПП є взаємний обмін інформацією про кіберзагрози між урядом та приватним сектором, що знайшли своє втілення в законодавчих та інституційних ініціативах. Водночас така співпраця виявила як переваги, так і недоліки КДПП. З одного боку, КДПП допомогло розслідувати кримінальні та цивільні злочини, сприяло попередженню кібератак, а також створенню нових методів попередження та протидії кіберзагрозам. З іншого – така взаємодія викликає дедалі більше занепокоєння з боку представників приватних компаній через односпрямованість інформаційного обміну, надмірну закритість державних органів, що ставить питання про доцільність такої співпраці.

7. У Німеччині КДПП спрямовано передусім на встановлення взаємовигідних правил гри для операторів критично важливої інфраструктури. На нинішньому етапі, незважаючи на значну кількість механізмів, створених в інтересах реалізації КДПП,

відповідна система в Німеччині все ще перебуває на етапі становлення, а значна кількість питань (особливо у сфері КДПП щодо об'єктів критичної інфраструктури) об'єктивно залишається невирішеною.

8. Пошук механізмів співробітництва відбувається в межах реалізації програми *UP KRITIS*, основним завданням якого є підготовка та реалізація спільних рекомендацій для держави та приватного сектору у сфері кіберзахисту. *UP KRITIS* регулярно інформує своїх учасників та партнерські структури з інших країн про відповідні європейські заходи щодо захисту критичної інфраструктури. Рішення, прийняті членами *UP KRITIS*, представляються на розгляд європейських структур, впливаючи на європейський порядок денний на ранніх стадіях, посилюючи інтереси Німеччини в цьому секторі безпеки. Існують також інші майданчики співпраці, що мають змішане приватно-державне фінансування, на кшталт Альянсу для кібербезпеки, ініціативи Федерального уряду Німеччини, в рамках якої основні гравці – як державні, так і приватні, обмінюються інформацією, створюють та розширюють базу даних з метою посилення кібербезпеки в Німеччині.

9. Німецькі урядові структури, зі свого боку (керуючись Національною стратегією кіберзахисту від 2011 р.) також вживають заходів, які можуть бути кваліфіковані як КДПП. Зокрема, німецька Федеральна агенція з питань інформаційної безпеки (*BSI*) має кілька структур (зокрема Національний центр кіберреагування), що покликані забезпечувати кращу координацію дій щодо протидії кібератакам та більш оперативний обмін інформацією між урядом та приватним сектором. Зазначений Центр створює умови всім компетентним органам для оперативного реагування на серйозні інциденти, а також проводить аналіз та оцінку небезпек, координує співпрацю з місцевими та галузевими організаціями з урегулювання кризових ситуацій.

10. КДПП у Великій Британії на нинішньому етапі більшою мірою зосереджене на пошуку суто ринкових форм взаємодії та на заходах посилення взаємної довіри. Зокрема, КДПП розвивається в межах механізму державних закупівель, а також відіграє важливу роль у забезпеченні державних структур якісними послугами, зокрема у сфері цифрових технологій. Цьому сприяє той факт, що ринок кібербезпеки Великої Британії розвивається дуже динамічно, і для забезпечення його захищеності та сталого функціонування держава та приватний сектор мають нести посилену спільну відповідальність, навіть якщо сутнісні цілі держави та бізнесу є різними (для держави головною є безпека громадян, а для бізнесу – одержання прибутків).

11. Роль уряду у питаннях кібербезпеки не обмежується тотальним контролем та наглядом, а полягає у стимулюванні приватного сектору до співпраці, допомозі інноваційним стартапам, координації інструментів забезпечення кібербезпеки, підтримці мереж фахівців з питань кібербезпеки. Попри активність держави у напрямі розбудови партнерства, бізнес не завжди добровільно попереджає державні структури про загрози, з якими стикається і які можна попередити, що зумовлює необхідність більш жорсткого регулювання.

12. Вдалим прикладом консолідації зусиль різних державних структур у сфері кібербезпеки є функціонування Національного центру кібербезпеки (складова *GCHQ*), який у своїй практичній діяльності керується принципами пошуку порозуміння з бізнесом та залучення представників держави, бізнесу, науки та громадськості до процесу розробки кращих практик, рекомендацій та настанов із впровадження високих стандартів кібербезпеки, у т. ч. – галузевих.

13. До засадничих характеристик КДПП згідно з усталеною в Республіці Польща юридичною практикою слід віднести: взаємну корисність; цивільно-правовий характер; конкретну мету (побудову 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. Дискусії в Польщі довкола сутності КДПП стосуються передусім можливості його ототожнення/розрізнення з «концесійною діяльністю» (концесіями). Побутують дві крайні позиції: ототожнення цих форм взаємодії державного (публічного) й приватного партнерів та їх жорстке розмежування.

14. На сьогодні Польща більшою мірою зосереджується на розвитку системи *CERTs,* фактично «вбудовуючи» окремі форми КДПП (у т. ч. – з банківським сектором та науковим співтовариством) у їх діяльність (передусім – *CERT NASK* та *NCC*, створеного на його основі). Важливу роль у інституціюванні КДПП Польщі відіграють урядові структури, передусім – Міністерство оцифрування, а також розроблена нормативно-правова база, яка констатує необхідність впровадження КДПП.

15. Станом на осінь 2017 р. для створення правової платформи КДПП в Україні державою ухвалено лише базові рамкові нормативні акти – Закон України «Про основні засади забезпечення кібербезпеки України», а також затверджена Указом Президента України від 15 березня 2016 р. № 96/2016 Стратегія кібербезпеки України. На нинішньому (початковому) етапі вони не формують адекватного нормативно-правового фундаменту для здійснення галузевої КДПП, оскільки не підкріплені відповідними підзаконними актами (включаючи реєстр НКІІ) і містять низку спірних або занадто абстрактно сформульованих визначень, положень та норм. А саме:

- невизначеним залишається правовий зміст самого поняття «державно-приватна взаємодія», зокрема його кореляція із Законом України «Про державно-приватне партнерство» та іншими нормативними актами;
- недостатньо артикульовані механізми та процедури галузевого регулювання захисту об'єктів кібербезпеки, не враховані можливості ДПВ у цій сфері (зокрема, запровадження недержавних галузевих регуляторів, що довело свою ефективність у міжнародних практиках);
- на засадах збалансованості повноважень та інтересів між усіма стейкхолдерами ДПВ потребує подальшого узгодження порядок впровадження аудиту інформаційної безпеки на об'єктах НКІІ, встановлення вимог до аудиторів інформаційної безпеки і визначення порядку їх атестації;
- на цих же засадах необхідне також унормування самого інституту незалежних аудиторів;
- неврегульованими залишаються питання стандартизації у сфері кіберзахисту та інформаційної безпеки, насамперед у частині порядку та меж застосування відповідних українських та/чи міжнародних стандартів (особливо критично для розвитку ДПВ за участі об'єктів НКІІ).

16. При тому, що як недержавний сектор в Україні, так і державні відомства подекуди демонструють значний потенціал для створення загальнонаціональної системи КДПП, поряд із цим станом на осінь 2017 р. в Україні триває формування лише окремих її елементів, сама ж система як така поки відсутня.

17. Поряд із недосконалістю нормативно-правової бази другою фундаментальною проблемою розвитку ДПВ наразі залишається дефіцит артикульованої та ефективної державної політики, передусім – комунікативної й регуляторної. У цьому контексті особливої актуальності для профільних відомств набуває (а) налагодження належної комунікації/співробітництва держави з недержавним сектором (галузевими бізнес-асоціаціями, професійними неприбутковими організаціями, експертними колами тощо) і (б) створення дієвих інституційно-правових інструментів такої взаємодії.

18. Проблемою у розбудові ефективного КДПП в Україні залишається і те, що кібербезпековий сектор України вкрай закритий, а наявна інформація про нього не дає об'єктивного уявлення про його стан та перспективи. Це зумовлює необхідність проведення огляду кібербезпекового сектору України та напрацювання на його основі відповідного документа, що дозволить створити цілісне уявлення про проблеми у сфері

кібербезпеки, оцінити ресурси для вирішення проблем та окреслити можливі стратегії вирішення існуючих проблем.

19. Політичний хактивізм стає значимим фактором у загальних питаннях кібербезпеки України. Участь волонтерських та неурядових структур у протидії агресії РФ шляхом атак на комп'ютерні системи російсько-терористичних угруповань, а також проти комп'ютерних систем на території РФ дійсно надало важливу допомогу у протидії російській агресії та допомогло надати публічності доказам активної включеності РФ у конфлікт на сході України.

20. Водночас спроби українських хактивістів частково переорієнтувати свою діяльність із зовнішніх майданчиків на внутрішні (вдаючись до несанкціонованих пентестів державних систем) у межах чинного законодавства багато в чому протизаконні і можуть бути кваліфіковані відповідно до ст. 361 КК України. Без юридичного вирішення цієї проблеми ефективне КДПП між державою та активістськими угрупованнями (окремими експертами з питань кібербезпеки) буде істотно ускладнено.

21. Зважаючи на те, що в Україні часто відсутні навіть базові елементи, необхідні для створення ефективного КДПП, ключовими напрямами практичних кроків у цій царині є такі:

- формування базового переліку сфер/цілей КДПП (як для держави, так і приватного сектору), яких вони не можуть досягти один без одного;
- визначення (на базі широкої дискусії та якісних науково-експертних досліджень) критеріїв, за яких КДПП стане привабливим рішенням для обох сторін;
- здійснення системних заходів, спрямованих на посилення довіри учасників КДПП один до одного;
- допомога з боку неурядових структур та науково-експертного співтовариства обом сторонам у визначенні цілей партнерства та у формуванні довгострокових стратегій такого партнерства;
- пошук ефективних підходів до визначення ризиків для кожної із сторін, а також оптимальних форм відповідальності;
- розвиток дискусій між обома сторонами партнерства задля вирішення наявних проблем та створення постійно діючих дискусійних майданчиків;
- обговорення можливих спільних проектів (як на засадах співучасті, так і співфінансування).

РЕКОМЕНДАЦІЇ

1. Україна потребує відкритої та масштабної дискусії з питань КДПП, результати якої могли б бути втілені у чіткому та зрозумілому державному стратегічному документі («Стратегії державно-приватного партнерства у сфері кібербезпеки» чи «Концепції організації державно-приватної взаємодії у сфері забезпечення кібербезпеки»). Зазначений документ має формуватися за активного залучення зацікавлених сторін і більшою мірою бути продуктом недержавного сектору, ніж державних структур. Зважаючи на необхідність вирішення проблеми державно-приватного партнерства у сфері кібербезпеки відповідно до європейських демократичних практик, пропонуються такі кроки, що дозволять оптимізувати зазначену сферу:

- З огляду на значну кількість стейкхолдерів у цьому процесі, він матиме більшою мірою політичний, а не суто юридичний/технічний вимір. Зважаючи на це, ще до етапу проведення консультацій доречно розпочати заходи з підвищення довіри між учасниками ринку (недержавними суб'єктами) та державою в цілому. З цією метою у практиці інституцій ЄС ще до проведення консультацій було *створено платформу (як онлайн, так і офлайн) для обміну дослідженнями та інноваціями, досвідом,* що має на меті формування простору довіри учасників до процесу. Відтак пропонується утворення базової онлайн-платформи «**Кібердіалог**», яка має стати основою для проведення громадських консультацій із зацікавленими сторонами щодо планування майбутньої стратегії державно-приватного партнерства у сфері кібербезпеки.
- З метою запуску платформи на базі Адміністрації Президента України (під головуванням одного із заступників Голови АПУ) пропонується утворення Ініціативної робочої групи, до якої мають увійти основні недержавні учасники ринку у сфері кібербезпеки (в т. ч. – системні інтегратори ПЗ, виробники антивірусного програмного забезпечення), представники профільних ІТ-асоціацій, а також представники наукових установ. Зазначена група проводить підготовчі заходи (семінари та робочі наради) з КДПП, а також з урахуванням пропозицій та зауважень галузевих недержавних суб'єктів готує базові пропозиції, які в подальшому мають стати основою платформи «Кібердіалог».
- Діяльність цієї платформи має забезпечуватись належним комунікуванням всіх державних установ, задіяних у цьому процесі: АПУ, Держспецзв'язку, СБУ, МВС, Нацбанку. Посилання на цю платформу мають бути обов'язково розміщені на сайтах усіх державних установ, на ФБ-акаунтах відомств, а також за можливості згадуватись у виступах представників відомств для ЗМІ чи на профільних публічних заходах.
- Відповідний онлайн проект має бути запущено на строк не менше 12 тижнів (варіант – до 24 тижнів), щоб зібрати різні точки зору щодо питання функціонування українського ринку у сфері кібербезпеки, а також ключові пропозиції та зауваження зацікавлених сторін до чинної системи взаємодії меж державою та приватним сектором у сфері кібербезпеки.
- Апарату РНБО України (в межах виконання Стратегії кібербезпеки України) запропонувати суб'єктам національної системи кібербезпеки підготувати спільну візію

державних органів щодо того, якою може і має бути співпраця між державою та недержавним сектором у сфері кібербезпеки.

- У межах консультацій має бути напрацьовано консенсусний погляд на низку принципових питань, які надалі становитимуть основу для рамкового державного документа у сфері КДПП: галузеві вимоги до здійснення КДПП; стейкхолдерів КДПП (можливо – у вигляді проекту відповідного реєстру); методології оцінки ризиків (на основі міжнародних стандартів та практик); типових моделей-проектів КДПП із визначенням правових, інституційних, інвестиційних та інших механізмів їх реалізації; порядку сертифікації аудиторів та проведення аудиту (із посиланням на відповідні нормативно-правові акти); механізму налагодження безперервного багатостороннього обміну відповідною інформацією між усіма учасниками КДПП; джерел та механізмів стимулювання КДПП; шляхів і механізмів підтримки досліджень та розробок (ДіР), а також підготовки проектів концептуальних документів у сфері кібербезпеки у рамках КДПП; порядку проведення навчань, тренінгів тощо.

2. За результатами консультацій, узагальнення та ухвалення відповідного документа може відбуватись одним із запропонованих шляхів:

- **Варіант 1**. На базі Апарату РНБО України може бути утворено Спільну робочу групу з підготовки проекту «Стратегії державно-приватного партнерства у сфері кібербезпеки», яка має максимально повно враховувати напрацювання Ініціативної групи. До процесу розроблення (консультування) тексту Стратегії доречно залучити представників європейських структур, які або мають досвід створення відповідних стратегії, або задіяні сьогодні у процесах реформування сектору безпеки і оборони України: *EUAM*[254], представників ЄК, які брали участь у розробленні європейського плану дій (*European public private partnership on cybersecurity*). Зазначену Стратегію доцільно ухвалити відповідним рішенням РНБО України в межах розвитку положень Стратегії кібербезпеки України.
- **Варіант 2.** Розроблення проекту відповідного документа може відбуватись на базі Міністерства економічного розвитку і торгівлі (як ключового суб'єкта реалізації форм КДПП в Україні) спільно з суб'єктами забезпечення кібербезпеки в Україні (відповідно до меж їх компетенції) для підготовки «Концепції організації державно-приватної взаємодії у сфері забезпечення кібербезпеки». Означену Концепцію доцільно увести в дію Постановою Кабінету Міністрів України в рамках заходів із реалізації положень Закону України «Про основні засади забезпечення кібербезпеки України», ухваленого Верховною Радою України 05.10.2017 р.

Загальні рекомендації

3. Суб'єктам національної системи кібербезпеки в межах їхніх повноважень підготувати (та подати на розгляд Комітетів Верховної Ради України з питань інформатизації та зв'язку та з питань національної безпеки і оборони) проект змін, спрямований на подальшу гармонізацію Закону України «Про основні засади забезпечення кібербезпеки України» з пов'язаними нормативно-правовими актами (передусім із Законом України «Про захист інформації в інформаційно-телекомунікаційних системах» в частині умов обробки інформації у системі та повноважень державних органів у сфері захисту інформації в системах (стаття 8, 10)).

4. Кабінету Міністрів України, суб'єктам національної системи кібербезпеки (базуючись на результатах експертного обговорення) та відповідно до норм чинного законодавства, розробити:

- єдині критерії та процедури віднесення об'єктів до переліку національної критичної інформаційної інфраструктури;

[254] EUAM Ukraine [Електронний ресурс]. – Режим доступу : http://www.euam-ukraine.eu/ua/our-mission/our-priorities/

- обов'язкові загальні вимоги до інформаційної безпеки об'єктів НКІІ, у т. ч. під час їх створення, уведення в експлуатацію, експлуатації та модернізації з урахуванням міжнародних стандартів.

5. Визначити відповідно до вимог Закону України «Про основні засади забезпечення кібербезпеки України» суб'єктів забезпечення кібербезпеки у галузях та/або окремих об'єктах і зобов'язати їх розробити обов'язкові галузеві вимоги (стандарти) інформаційної безпеки об'єктів НКІІ з урахуванням локальної специфіки.

Щодо вдосконалення термінології

6. Стаття 10 Закону України «Про основні засади забезпечення кібербезпеки України» містить перелік шляхів здійснення «державно-приватної взаємодії» у сфері кібербезпеки, який потребує подальшої конкретизації. Передусім вбачається необхідним напрацювати однозначний понятійний апарат, зокрема надати чітке визначення поняттям «державно-приватна взаємодія», про яке йдеться в Законі та «державно-приватне партнерство», про яке згадується у Стратегії кібербезпеки України.

Щодо стандартів

7. На виконання пп. 3 п. 3 ст. 8 Закону України «Про основні засади забезпечення кібербезпеки України» важливо опрацювати можливість впровадження досвіду Німеччини в частині затвердження суб'єктами національної системи кібербезпеки, які безпосередньо відповідають за питання вироблення та контролю за дотриманням стандартів у цій сфері, для операторів об'єктів критичної інфраструктури тих галузевих стандартів кібербезпеки, що будуть запропоновані самими операторами.

Щодо співпраці з зарубіжними партнерами

8. Службі безпеки України розглянути можливість включення тематики КДПП до програм, що реалізуються у межах Трастового фонду Україна – НАТО з питань кібербезпеки.

9. Міністерству закордонних справ України з метою залучення досвіду міжнародних партнерів в частині розроблення нових механізмів КДПП у сфері кіберзахисту та обміну інформацією про кіберзагрози пропонується спрямувати тематичні запити до Міжнародного секретаріату НАТО, країн – членів НАТО, Європейської Комісії щодо наявних найкращих практик КДПП.

Щодо налагодження обміну інформацією між суб'єктами КДПП

10. ДССЗЗІ ініціювати спільно з представниками бізнес-середовища (передусім – операторами об'єктів критичної інфраструктури) створення «Програми зі співробітництва та обміну кіберінформацією» (взявши за основу принципи програми *CISCP*). З метою більш ефективної реалізації такої програми пропонується залучити як консультантів при її створенні фахівців Міністерства внутрішньої безпеки США, які відповідають за підтримку та реалізацію *CISCP*.

11. Враховувати, що невід'ємною складовою при формуванні та реалізації «Програми зі співробітництва та обміну кіберінформацією» мають стати принципи захисту приватності та громадянських свобод, що можуть бути сформовані на основі спільних стандартів і керівництв на кшталт «Принципів справедливого управління інформацією США» (*Fair Information Practice principles*).

12. Розглянути можливість запровадження подібного британському *CISP* захищеного онлайн-механізму обміну інформацією про кібернетичні загрози між представниками

індустрії кібербезпеки та електронних комунікацій, з одного боку, та суб'єктами національної системи кібербезпеки – з іншого. Розробку подібного механізму доцільно здійснювати під егідою Національного координаційного центру кібербезпеки за участі експертів зі сфер бізнесу, провідних науково-дослідних установ, державних органів та громадського сектору.

Щодо розвитку діалогу та заходів, спрямованих на збільшення взаємної довіри

13. Задіяти механізм регулярного діалогу між приватними компаніями та урядом (семінари, форуми, тренінги) задля просування та реалізації ініціатив КДПП. Одним із механізмів реалізації може стати започаткування щорічного міжнародного/всеукраїнського форуму з питань державно-приватного партнерства у кіберсфері за участі основних суб'єктів національної системи кібербезпеки та всіх зацікавлених сторін з боку недержавних структур.

14. Суб'єктам національної системи кібербезпеки, на виконання п. 6 ст. 10 Закону України «Про основні засади забезпечення кібербезпеки України» спільно з представниками національної інформаційної індустрії сформувати пул експертів, які можуть залучатися до:

- розслідування кіберінцидентів на об'єктах критичної інфраструктури та подолання наслідків;
- для комунікування інцидентів у засобах масової інформації;
- до програм підвищення кваліфікації співробітників структур національної системи кібербезпеки та для співробітників об'єктів критичної інфраструктури.

Пул експертів може бути сформований за галузевим принципом з регулярним щорічним переглядом.

15. Під час процедури формування Планів дій з реалізації Стратегії кібербезпеки України (зокрема тих, які відносяться до пп. 6 п. 4.3 розділу «Пріоритети та напрями забезпечення кібербезпеки України») врахувати необхідність розширення заходів, спрямованих на реалізацію державно-приватного партнерства. Зокрема, передбачити можливість створення українського аналогу КРІТІС, до функцій та завдань якого мають бути віднесені:

- підготовка реалізації спільних рекомендацій для державного і приватного секторів у сфері кібербезпеки;
- проведення тренінгів для сторін КДПП;
- взаємодія з міжнародними партнерами та аналогічними структурами;
- кризові комунікації;
- інформування національних партнерів про відповідні європейські структури щодо захисту критичної інфраструктури;
- визначення порядку долучення учасників до цієї платформи.

16. Спільно з Громадською радою при ДССЗЗІ опрацювати питання підготовки концептуальних пропозицій для всіх суб'єктів національної системи кібербезпеки щодо форм та методів (а також безпосередніх протоколів та процедур) реалізації державно-приватного партнерства в органах державної влади у частині питань, що пов'язані з кібербезпекою.

17. Кабінету Міністрів України спільно з іншими суб'єктами забезпечення кібербезпеки, МЕРТ, МІП, ПАТ НСТУ та із залученням інших національних мовників – розглянути питання налагодження широкого експертного та громадського обговорення створення платформи державно-приватної взаємодії у сфері кібербезпеки (підзаконні акти, єдині та галузеві нормативні вимоги інформаційної безпеки, формування реєстру об'єктів НКІІ, стандартизація, сертифікація, аудит, технічне забезпечення, інтероперабельність систем тощо). Забезпечити належну публічність і достатній медіа-супровід

цього обговорення: онлайн-майданчик(и), веб-трансляції, підготовка відповідних телепрограм та інші форм ТБ-промоушена. Оприлюднити результати обговорення.

Щодо вирішення проблеми діяльності хактивістських угрупувань

18. Важливим є ініціювання дискусії (передусім) щодо модифікації українського законодавства (в т. ч. – Кримінального кодексу України) для легалізації пентестової діяльності хактивстів в інтересах перевірки готовності об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів. З цією метою пропонується уточнити формулювання статті 361 КК України, доповнивши її новим пунктом у такій редакції: «звільняється від кримінальної відповідальності громадянин України, якщо таке втручання здійснювалось за погодженням із суб'єктами національної системи кібербезпеки, що мають право на здійснення оперативно-розшукової діяльності та на яких відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» покладено завдання негласної перевірки готовності об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів».

19. Доцільним є напрацювання реального механізму погодження дій хактивістів, максимально дебюрократизувавши його та гарантуючи нерозголошення інформації про таку співпрацю. Варіантів вирішення зазначеного питання може бути два. Перший – утворення на базі Національного координаційного центру кібербезпеки постійно діючої робочої групи з особливих питань державно-приватного партнерства. Другий – робоча група у складі органу влади, на який покладено завдання негласної перевірки готовності об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів (наразі це СБУ).

20. Для функціонування групи має бути сформовано окреме положення, в якому слід чітко визначити механізм надання дозволу на здійснення пентесту систем, а також його граничні показники, за межами яких дозвіл заявнику більше не надаватиметься. Крім того, це ж положення має чітко регламентувати й вичерпні причини, чому такий дозвіл може не надаватися суб'єктам національної системи кібербезпеки. Розроблення відповідного положення доцільно проводити спільно із представниками українського ІТ-співтовариства, передусім тими, які спеціалізуються на комерційному здійсненні пентестів.

21. Передбачити, що суб'єктом отримання відомостей при роботі таких хактивістських пентестових груп є органи, які надавали дозвіл на пентест. У межах роботи такої Групи передбачити чіткий механізм донесення результатів такої перевірки до тих відомств, які були піддані негласному пентесту (наприклад, у 10-денний термін після отримання даних про уразливість), а також контролю за їх усуненням (повторний контрольний тест системи через 30 днів з моменту повідомлення).

22. Розглянути можливість проведення Національним координаційним центром кібербезпеки щонайменше одного засідання на рік, присвяченого питанням стану реалізації державно-приватного партнерства (можливо – із залученням представників недержавного сектору).

Щодо розвитку взаємодії між суб'єктами КДПП (у т. ч. – обмін досвідом)

23. Кабінету Міністрів України, Верховній Раді України розглянути питання створення координаційної державно-приватної платформи з консультативно-дорадчими повноваженнями (наприклад, у формі тимчасової комісії або комітету) для участі в розробленні нормативно-правових актів із незалежного аудиту інформаційної безпеки на об'єктах НКІІ на основі міжнародних стандартів, у т. ч. Європейського Союзу та НАТО (згідно з вимогами частини 3 статті 6 Закону України «Про основні засади забезпечення кібербезпеки України»).

24. При розробленні плану заходів з реалізації Стратегії кібербезпеки України (на виконання пункту 2 рішення Ради національної безпеки і оборони України від 27.01.2016 р. «Про Стратегію кібербзпеки України») слід враховувати необхідність розроблення практичних механізмів залучення фізичних та юридичних осіб до кіберзахисту державних інформаційних ресурсів у рамках програм державно-приватного партнерства, в т. ч. використовуючи досвід *ISAC* або *ISAO*.

25. Актуальним також вбачається ініціювання суб'єктами національної системи кібербезпеки України консультацій щодо створення відкритого онлайн-майданчика для обміну досвідом у сфері кібербезпеки між державою, наукою, бізнесом та громадським сектором за аналогом британської ініціативи *Cyber Growth Partnership*. Безпосереднє створення онлайн-платформи можливе, зокрема, за рахунок приватних та волонтерських зусиль.

26. З метою запозичення практичного досвіду приватного сектору в питаннях попередження кіберзагроз, реагування на кіберінциденти та захисту інформаційних систем ключових суб'єктів національної системи кібербезпеки доцільно розробити механізм залучення перевірених фахівців з приватного сектору до роботи над проектами в рамках своїх підрозділів чи підрозділів, відповідальних за кібербезпеку, у складі інших державних установ. Фінансування оплати праці таких фахівців можливе за рахунок проектів міжнародної технічної допомоги, а також, за можливості, за рахунок коштів, виділених у рамках Трастового фонду Україна – НАТО з питань кібербезпеки.

27. Для додаткового наукового та інформаційного забезпечення суб'єктів національної системи кібербезпеки вбачається доцільним створення при ключових ЗВО України Центрів вивчення передового досвіду у сфері кібербезпеки. Як пілотні подібні центри доцільно створити у провідних освітніх закладах, зокрема, у рамках Навчально-наукового інституту інформаційної безпеки при Академії СБУ, Інституту спеціального зв'язку та захисту інформації при НТУУ КПІ, Військового інституту телекомунікації та інформатизації, КНУ імені Тараса Шевченка, Державного університету телекомунікацій.

28. ДССЗЗІ та іншим суб'єктам національної системи кібербезпеки розглянути питання інституційного, ресурсного і нормативно-правового забезпечення подальшого розширення КДПП з галузевими асоціаціями та іншими недержавними акторами у сфері обміну інформацією про кіберінциденти, експертного та технічного співробітництва, в запобіганні та розслідуваннях кібератак (у контексті створення загальнонаціональної системи обміну даними про кіберінциденти).

Щодо пріоритетних спільних проектів у межах розвитку КДПП

29. Міністерству освіти та науки України – в рамках налагодження ДПВ у сфері підвищення обізнаності громадян у сфері кібербезпеки та забезпечення належного рівня комп'ютерної грамотності працівників установ, компаній та підприємств – розглянути можливість встановлення системної співпраці з профільними недержавними організаціями для спільного розроблення спеціалізованих навчальних програм для вищої та середньої школи, участі в навчальному процесі на засадах концепції безперервної освіти – післядипломна, дистанційна, неформальна (тренінги, курси) освіта, факультативні програми для студентів непрофільних ЗВО та школярів тощо.

30. Доцільним є ініціювання розроблення ключовими суб'єктами національної системи кібербезпеки, Міністерством інформаційної політики України спільно з представниками приватного сектору низки інформаційних кампаній з метою донесення до державних установ, бізнесу та широкого загалу рекомендацій із дотримання базових правил кібербезпеки. Крім того, необхідним також є розроблення (зусиллями СБУ, Кіберполіції та *CERT-UA*) поглиблених галузевих рекомендацій для підприємств та установ критичної інфраструктури.

31. Важливим пілотним проектом КДПП могла би стати підготовка «Огляду сектору кібербезпеки» із залученням усіх зацікавлених сторін, що має охарактеризувати поточний стан кібербезпекової сфери України, її ресурсного потенціалу та шляхів оптимізації спроможностей кібербезпекового сектору.

32. Одним із форматів проведення зазначеного огляду може бути використання вже наявних процедур проведення комплексних оцінок станів кібербезпеки. Зокрема, виглядає доречним більш ефективне дослідження досвіду проведення таких оглядів міжнародними кібербезпековими організаціями (зокрема *Business Software Alliance*), а сам Огляд може будуватись за такою схемою:

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

ДЛЯ НОТАТОК

ДЛЯ НОТАТОК

Наукове видання

ДЕРЖАВНО-ПРИВАТНЕ ПАРТНЕРСТВО У СФЕРІ КІБЕРБЕЗПЕКИ: МІЖНАРОДНИЙ ДОСВІД ТА МОЖЛИВОСТІ ДЛЯ УКРАЇНИ

Аналітична доповідь

Редагування: *І.І. Бажал*
Коректура: *О.І. Сабадаш, О.М. Романова*
Комп'ютерне верстання: *О.М. Адулов*

Відповідальний за випуск: *О.М. Романова*

Оригінал-макет підготовлено
у Національному інституті стратегічних досліджень:
вул. Пирогова, 7-а, Київ-30, 01030
Тел./факс: (044) 234–50–07
e-mail: info-niss@niss.gov.ua

Формат 60х84/8. Ум. друк. арк. 9,53
Наклад 150 прим. Зам. № ДФ 654

ПП «Видавництво Фенікс»
03067, Київ, вул. Шутова, 13-б
www.fenixprint.com.ua
Свідоцтво суб'єкта видавничої справи
ДК № 271 від 07.12.2000 р.