ДОСВІД НІМЕЧЧИНИ У ФУНКЦІОНУВАННІ ПЛАТФОРМ ДЕРЖАВНО-ПРИВАТНОГО ПАРТНЕРСТВА В СФЕРІ КІБЕРБЕЗПЕКИ

Актуальні дискусії щодо державно-приватного партнерства в кіберсфері переважно обертаються довкола, з одного боку, необхідності створення простору безпеки та зменшення ризиків, а з іншого – необхідності збалансування безпеки із потребою інтернет-свободи та права на втручання держави у децентралізований кіберпростір[1].

Втім, від моменту сприйняття кіберпростору як саморегульованого, стійкого та децентралізованого відбулись граничні зміни з огляду на його структурні вразливості. Подібна зміна порядку денного спричинила трансформацію бачення кіберпростору як ліберального і саморегульованого, та усвідомлення потреби певного рівня контролю над процесами з метою зменшення потенційних та реальних ризиків і загроз. Ситуацію ускладнює і той факт, що цілу низку структурних вразливостей кіберпростору неможливо вирішити за рахунок спроможностей якогось окремого суб'єкта[2].

З одного боку це посилює тенденцію до все більш охоплюючої сек'юритизації кіберсфери. Це, в свою чергу, призводить до домінування на порядку денному США, Німеччини, Великої Британії та низки інших країн питань контролю та ухвалення законодавства, що спрямоване і на традиційно слабко контрольовану сферу – соціальні мережі. Наслідком цього стають

---

[1] Зокрема див.: Radu, Roxana, Jean-Marie Chenou, and Rolf H Weber. 2014. The evolution of global internet governance: principles and policies in the making. Vol. 56: Springer Science & Business Media; Chenou, Jean-Marie. 2014. "From Cyber-Libertarianism to Neoliberalism: Internet Exceptionalism, Multi-stakeholderism, and the Institutionalisation of Internet Governance in the 1990s." Globalizations 11 (2):205-223.; Eriksson, Johan, and Giampiero Giacomello. 2009. "Who controls the internet? Beyond the obstinacy or obsolescence of the State." International Studies Review 11 (1):205-230.

[2] Mueller, Milton, Andreas Schmidt, and Brenden Kuerbis. 2013. "Internet security and networked governance in international relations." International Studies Review 15 (1):86-104.

закони, на кшталт німецького закону проти кримінального контенту в Інтернеті – т. з. NetzDG (*Netzwerkdurchsetzungsgesetz*). З іншого боку – партнерство є запорукою залучення різних акторів у спільний процес формування відповідальності за безпекову ситуацію в кіберпросторі від кібергігієни[3] до боротьби із кіберзлочинністю та попередження атак на об'єкти критичної інфраструктури.

Партнерство між державним та приватним сектором у сфері кібербезпеки має багато інституційних форм. Зокрема значний досвід впровадження та функціонування різних видів ДПП у вигляді платформ, альянсів та ініціатив у сфері кібербезпеки має Німеччина, активно застосовуючи його у повсякденній практиці.

У другій половині квітня 2018 р. Федеральне міністерство інформаційної безпеки Німеччини (BSI) використало[4] свій досвід державно-приватного партнерства з метою попередження в Німеччині атак подібних на ті, які здійснювалися РФ проти США та Великій Британії з ціллю корпоративного шпигунства, вилучення інтелектуальної власності, підтримання постійного доступу до мереж підприємств-жертв. Проаналізувавши шкідливу кіберактивність РФ щодо урядових мереж та мереж приватних компаній в США та Великій Британії[5], BSI ініціювало відповідні захисні заходи через Національний центр кіберзахисту та рекомендувало приватним компаніям, особливо операторам критичної інфраструктури, переглянути свої інформаційні мережі та системи, і вжити

---

[3] Кібер-гігієна стосується практики та превентивних заходів, які реалізують користувачі з метою збереження конфіденційності даних та захищеності від крадіжок, зовнішніх атак. Це практичні кроки націлені на підвищення безпеки в Інтернеті серед широкого кола користувачів.

[4] https://goo.gl/M4zGr5

[5] https://www.ncsc.gov.uk/news/joint-us-uk-statement-malicious-cyber-activity-carried-out-russian-government

необхідних заходів безпеки, адаптувавши їх до останніх шкідливої кіберактивності.

Базова складова державно-приватного партнерства німецької системи захисту від кіберзагроз регулюється UP KRITIS[6]. Платформа державно-приватного партнерства UP KRITIS регулярно інформує національних партнерів про відповідні європейські заходи щодо захисту критичної інфраструктури.

Координація партнерів у німецьких структурах державно-приватного партнерства на прикладі UP KRITIS

ДПП у німецькому випадку представляє собою кілька майданчиків партнерства кожен зі своєю специфікою. І хоча UP KRITIS, як приклад такої структури є не єдиною формою ДПП в Німеччині, однак його роль є однією з ключових. Платформа задовольняє потребу конкретного сектору індустрії/бізнесу у кібербезпекових рішеннях, надаючи платформу для досягнення домовленостей, а з іншого – допомагає уряду у імплементації певних кібербезпекових стандартів та у підготовці національних стратегій кібербезпеки. Все це стало особливо актуальним після того, як в 2017 році низка німецьких підприємств стала жертвами масових атак WannaCry та Petya/NotPetya. Відтак німецька бізнес спільнота своїм пріоритетом бачить розвиток механізмів попередження, швидкого реагування задовго до інциденту, що може зменшити тиск на бізнес, може знизити витрати[7]. Це набуває додаткового значення ще і з огляду на те, що дедалі більше німецьких компаній стають об’єктом кіберкорпоративного шпигунства як державних так і недержавних акторів. Водночас дуже часто вони не усвідомлюють, що стали жертвами такого шпигунства. Іноді розуміння, що

[6] Umsetzungsplan KRITIS des Nationalen Plans zum Schutz derInformationsinfrastrukturen 2014 p.

[7] https://goo.gl/uuTfkK

компанія зазнала кіберінциденту, приходить через кілька місяців чи навіть півроку, коли іноземна компанія-конкурент виводить на ринок ідентичний продукт[8].

Унікальність UP KRITIS полягає у пріоритетності роботи з об’єктами критичної інфраструктури. Основними сторонами цього формату ДПП є:

- Федеральне міністерство внутрішніх справ (*BMI*), відповідальне за внутрішню безпеку в Німеччині, що координує та контролює всю діяльність своїх підпорядкованих органів, включаючи Федеральне відомство з питань цивільного захисту та допомоги в катастрофах (*Bundesamt für Bevölkerungsschutz und Katastrophenhilfe*) та Федеральне відомство з безпеки інформаційних технологій (*BSI*);
- оператори критичної інфраструктури – близько 2000 операторів критичної інфраструктури у семи регульованих секторах[9];
- федеральні землі Німеччини, що створює більш тісні зв'язки з відповідними локальними об’єктами критичної інфраструктурами;
- муніципалітети (не лише міста, але також підрозділи та об'єкти, такі як, наприклад, пожежні бригади, рятувальні служби, агентство технічної допомоги (*Bundesanstalt Technisches Hilfswerk*) з відповідними компетенціями, що мають вирішальне значення для цивільного захисту).

Серед поточних проектів UP KRITIS найбільш пріоритетними є ініціативи кібербезпеки в наступних секторах:

- в медичних закладах, виробництва лікарських засобів, у сфері страхування життя, де щорічні фінансові транзакції становлять близько 90,6 мільйонів євро;

---

[8] https://goo.gl/6GU6K1

[9] https://www.kritis.bund.de/SubSites/Kritis/DE/Aktivitaeten/Nationales/UPK/upk_node.html

- сектор транспорту, контролю повітряного руху та управління повітряним рухом (від 17 500 перевезень літаків на рік), вантажних станцій та вокзалів (23 000 поїздів на рік), залізничних мереж, центрів управління (125 млн перевезень пасажирів на рік).

Іншим прикладним проектом в рамках UP KRITIS був проект SKRIBT (*Schutz kritischer Brücken und Tunnel im Zuge von Straßen*) із захисту мостів, тунелів та доріг. Проект SKRIBT був частиною програми «Дослідження для цивільної безпеки» та фінансувався Федеральним міністерством освіти і науки (BMBF), діяв впродовж 2008–2011рр. Мости та тунелі як частина інфраструктури для вантажних і пасажирських перевезень є пріоритетом UP KRITIS, позаяк пошкодження однієї інфраструктурної ланки в результаті цільової атаки, великої аварії або природної небезпеки може призвести до серйозного пошкодження чи виведення з ладу більш широкої мережі комунікацій. Для підприємств, що обслуговують ці об'єкти, наслідком є значні витрати на відновлення та тривалий час простою, тобто економічний збиток. Водночас користувачі інфраструктури опиняються у небезпеці під час атаки, тому захист транспортної інфраструктури є одним із основних напрямків діяльності ДПП в Німеччині. Партнерами проекту були Федеральний науково-дослідний інститут шосе (*BASt*) як координатор проекту, Інститут швидкої динаміки Фраунгофера, *HOCHTIEF Solutions AG*, Рурський університет Бохуму, кафедра тунелювання та будівництва ліній (*TLB*), *Siemens AG*, Штутгартський університет, Інститут легкого проектування та проектування (*ILEK*), кафедра психології Університету Юліус-Максиміліанс у Вюрцбурзі.

Втім, проблемою UP KRITIS на думку учасників ринки є неповне визначення об’єкту критичної інфраструктури, а отже не повністю релевантний потребам індустрії формат ДПП. Так, Федеральна асоціація німецької промисловості (BDI) критикувала позицію UP KRITIS про розподіл

галузей на так звану критичну інфраструктуру і некритичну, а також неповноту законодавчої бази, пропонуючи випрацювати окремий порядок включення підприємств, які не підпадають під категорію об'єктів критичної інфраструктури[10].

Також критикується обов'язок одностороннього звітування компаній щодо кіберінцидентів. BDI висунула пропозицію, яка передбачала окрім процедури звітування об’єктів критичної інфраструктури також окрему процедуру звітності державних органів, що є відомчими у цих питаннях, які також повинні були б своєчасно надавати інформацію про загрози компаніям. Німецька торгово-промислова палата (*Deutscher Industrie-und Handelskammertag, DIHK*) також критично висловилась стосовно дефініції терміну «критична інфраструктура», а також інших важливих термінів, які є недостатньо чітко окресленими.

Альтернативні німецькі платформи розвитку ДПП в кіберсфері

Альянс з кібербезпеки

Іншим майданчиком партнерства є Альянс з кібербезпеки (*Allianzfür Cyber-Sicherheit*) - ініціатива Федеральної агенції з безпеки інформаційних технологій (BSI) у співпраці з Німецькою асоціацією інформаційних технологій, телекомунікацій та нових медіа (*Bundesverband Informationswirtschaft, Telekommunikation und neue Mediene.V. (Bitkom)*)[11]. Заснована в 2012 році ініціатива підтримує обмін інформацією та досвідом між більшим колом учасників, не зводячи їх лише до операторів об'єктів критичної інфраструктури.

Альянс з кібербезпеки (далі – Альянс) налічує близько 2500 установ, участь у платформі є безкоштовною. З 2012 року Альянс пропонує своїм

---

10 http://www.zeit.de/digital/datenschutz/2015-04/it-sicherheitsgesetz-bundestag-ccc-bsi

11 https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Home/startseite.html

учасникам безкоштовно експертні висновки та щотижня проводить спільний захід, присвячений різноманітним темам з інформаційної безпеки.

Однією із цілей є посилення діалогу із ще більшою кількістю різноманітних секторів промисловості, зокрема із такими як хімічна промисловість та автомобільна промисловість з метою подальшого розширення мережі компаній та установ, що співдіють. Конкурентною перевагою Альянсу є націленість на малі та середнього розміру компанії, які часто мають власне ноу-хау, що потребує захисту.

Починаючи з 2014 р. Альянс разом із Федеральною агенцією з безпеки інформаційних технологій щороку готує огляд кібербезпеки (*Survey of Cyber Security*) для вивчення ситуації загрози та ризиків для німецької індустрії та бізнесу у зв'язку із кібератаками, а також статусу реалізації відповідних безпекових заходів. Також щороку близько 900 компаній та установ беруть участь у загальнодоступному опитуванні, яке проводить Альянс. Опитування є анонімним, отримані практичні рішення та рекомендації надаються іншим установам, використовуються для створення та постійного ведення звітності про стан кібербезпеки в Німеччині[12].

За минулорічним опитуванням[13,] проведеним Альянсом серед представників бізнесу та індустрії на предмет кіберризиків, близько 70 % респондентів, які постраждали від кібератак, заявили, що вони стали жертвами комп'ютерних атак у 2016 та 2017 роках.

Приблизно в половині випадків зловмисники були успішними у отриманні доступу до IT-систем компаній, та негативно вплинули на їх функціонування, маніпулюючи інформацією, що знаходилась на корпоративних веб-сайтах тощо. Решта респондентів відмітила, що вони успішно відвернули всі атаки.

---

12 https://goo.gl/Ra8PBg

13 https://goo.gl/m9Wh4Y

Щодо *типу кібератак*, з різних видів атак найбільш поширеними були т.з. malware - шкідливі інфекції. Близько 57 % учасників опитування повідомили, що шкідливе програмне забезпечення вторглося в операційні IT-системи для здійснення шкідливих операцій. Хакерські атаки, такі як саботаж промислових систем управління, крадіжки даних або інтернет-маніпулювання склали 19 %, атаки DDos, що призвели до втрати веб-сайтів та інших мережевих інфраструктур через перевантаженість, становили 18% усіх атак.

Стосовно *типів втрат та наслідків від кібератак для компаній — кожна друга компанія* повідомила, що внаслідок кібератак в 2016/2017 роках виникали виробничі чи операційні збої (більше 51 %), що тягло за собою значні фінансові витрати внаслідок необхідності публічного роз'яснення інцидентів та відновлення IT-систем (близько 23 % опитаних), а також репутаційних збитків (16,5 % респондентів).

Згідно критерію оцінки *сприйняття майбутніх ризиків* два з трьох респондентів вважають, що ризики кібер-атак зростатимуть у майбутньому, відтак відчувають потребу у співпраці з державою. Малі та середні підприємства оцінили ситуацію менш критично, ніж великі корпорації. Приблизно 73 % великих корпорацій очікують збільшення кібер-загроз, тоді як серед малих та середніх підприємств лише 62 % так вважають[14].

Щодо *необхідних заходів з кібер безпеки* 89 % респондентів зазначили, що заходи, такі як сегментація або мінімізація шлюзів, були прийняті для забезпечення мереж. Антивірусні заходи також часто використовувались (86 %). Були застосовані заходи для централізованого виявлення, такі як сканування безпекових мережевих шлюзів, поштових серверів тощо, а також

[14] https://goo.gl/ZptH9F

децентралізовані заходи, такі як сканування на клієнтських / серверних системах [15].

Згідно опитування багато компаній планують вдосконалення заходів з кіберзахисту (71 %). Серед них близько 13 % повідомили, що навіть у короткостроковій перспективі планується нагальне вдосконалення критичних областей. Кожен п'ятий респондент оцінив міри кібернетичної безпеки у своєму бізнесі як достатні (20 %), тому немає потреби у подальшому вдосконаленні[16].

Низка компаній визначили для себе пріоритетом підвищення рівня кваліфікації своїх співробітників. Більше половини опитаних компаній повідомили, що регулярне навчання в галузі кібербезпеки є одним із основних пріоритетів (52 %). Ще 20% опитаних компаній повідомили про заплановані регулярні навчальні заходи. Проте майже 30 % респондентів заявили, що тренінг з безпеки інформаційної безпеки не відбувається та не планується.

Стосовно раннього виявлення кібер-атак - чверть опитаних компаній актуально мають моніторинг кібербезпеки. 29 % великих компаній та 23 % малих та середніх підприємств регулярно працюють у цьому напрямку.

Німеччина безпечна в мережі

Ще однією ініціативою німецького ДПП є *Німеччина безпечна в мережі* (*Deutschland sicher im Netze.V.*)[17]. У 2005 році низка великих компаній, організацій та торгових спілок об'єдналися в цю ініціативу з метою активно сприяти підвищенню безпеки ІТ в Німеччині. У грудні 2006 р. ініціатива стала об'єднаною асоціацією, а в червні 2007 р. почала координувати свої

---

15 Ibidem

16 https://goo.gl/57wXNj

17 www.sicher-im-netz.de

зусилля із Федеральним міністерством внутрішніх справ[18]. Цільовим завданням є включення малого та середнього бізнесу у процеси державно-приватного партнерства. Один із проектів ініціативи «Німеччина безпечна в мережі» має в основі міждисциплінарну команду вчених з області інформатики, кримінології, соціології та економіки, зокрема учасниками проекту є науково-дослідний інститут кримінології Нижньої Саксонії, науково-дослідний центр ІТ-безпеки університету Ганновера. Команда всебічно досліджує кібернапади в Німеччині та розробляє рекомендації для подальшого реагування бізнесу/індустрії та державних органів. В рамках проекту було проведено репрезентативне опитування 5000 компаній у Німеччині. Основна увага до цього дослідження полягала в тому, наскільки добре компанії захищають себе від кібератак та наскільки ефективними є ці зусилля. Також буде розглянуто, як компанії реагують на напади та роль державних установ, таких як поліція та Федеральна агенція захисту конституції. Планується проаналізувати, провівши попередні польові дослідження, наскільки існуючі рекомендації можуть бути реалізовані відповідними співробітниками організації та як вчинити з цими інцидентами, щоб правильно виявляти атаки і реагувати в майбутньому.

Результати окремих досліджень будуть використані на другому етапі проекту пропонуючи рішення більш доступні для малих та середніх підприємств. Крім того, буде розроблено онлайнову платформу, яка дозволить компаніям здійснити первинну оцінку потенційних кіберзагроз та отримати додаткову допомогу у випадку необхідності.

Іншим проектом ініціативи «Німеччина безпечна в мережі» є проект Професійна школа для *ІТ-безпеки* (Berufsschule für IT-Sicherheit). Проект створює середовище для заохочення учнів професійно-технічних навчальних закладів поглиблювати вміння в питаннях інформаційної безпеки, аби вони

[18] Ibidem

могли застосовувати основні принципи інформаційної безпеки у своїх навчальних закладах[19].

Проект для малого і середнього підприємництва – «Усвідомлення IT небезпек для малого та переднього бізнесу» *(AWARE – Awareness im Mittelstand)* займається підвищенням обізнаності щодо інформаційної безпеки у галузі малого та середнього бізнесу. Проект з посилення складової інформаційної безпеки в галузі малого та середнього бізнесу націлений на уникнення репутаційних втрат, зниження продажів або втрати роботи у наслідок кібератак. Метою проекту є підвищення рівня довіри малого та середнього бізнесу у Німеччині до держави та заохотити використання IT технологій. Увага проекту зосереджена на трьох темах: виявлення атак соціальної інженерії, використання сильних паролів і використання безпечних параметрів конфіденційності[20].

Технологічний університет Дармштадта та низка інших учасників проекту розробляють практично важливі підходи та рішення, що є необхідними у реалізації цілей індустрії 4.0 та регулювання захисту даних ЄС, питання страхування кіберризиків, які надаються за допомогою онлайн-платформи awareness-im-mittelstand.de.

ВИСНОВКИ

1. Ініціатива Федерального міністерства інформаційної безпеки Німеччини (BSI) та Міністерства оборони Німеччини стосовно посилення залучення приватного сектору та індустрії до оперативної реакції на хакерські атаки та подолання наслідків такої є свідченням важливості цієї складової стратегічного планування щодо забезпечення кібербезпеки країни.

---

19 www.dsin-berufsschulen.de

20 www.awareness-im-mittelstand.de

2. Це також демонструє важливість діючого державно-приватного партнерства як основи кібербезпеки держави та можливості швидкого реагування та співдії державних органів на міждержавному рівні.

3. Окрім основного майданчика ДПП, яким є UP KRITIS, орієнтованого на об’єкти критичної інфраструктури, Німеччина має ще низку ініціатив, націлених на доповнення кластеру критичної інфраструктури, адже низка підприємств і організацій приватного бізнесу та індустрії не підпадають під кваліфікацію об’єктів критичної інфраструктури. Альтернативні майданчики державно-приватного партнерства включають малий та середній бізнес у процеси підтримання інформаційної безпеки.

4. Типові механізми безпеки та цикли, такі як власне тестування та виявлення слабких місць, нагородження іноземних повідомлень про слабкі місця (так звані помилки), оновлення патчів і функціональні можливості безпеки можуть бути значно прискорені та покращені на багатьох підприємствах за умови підвищення кваліфікації співробітників. Багато ІТ-компаній відмовляються проводити самостійно тестування чи опрацьовувати інформацію, що надходить ззовні, щодо їхніх ризиків, показяк вони не належать до критичної інфраструктури, отже не мають обов’язку і відповідні санкції не можуть бути застосованими .

РЕКОМЕНДАЦІЇ:

Суб’єктам національної системи кібербезпеки

1. Розглянути можливість проведення консультацій з галузевими асоціаціями щодо формування платформ державно-приватного партнерства в сфері кібербезпеки. Розглянути можливість покладання на такі платформи обов’язку проведення Огляду стану кібербезпеки в певній галузі, на базі єдиної методологічної основи (там де це можливо), що в подальшому могли б

стати основою формування загальнонаціонального огляду з кібербезпекової тематики.

2. З огляду на те, що значна кількість об’єктів критичної інфраструктури не лише знаходяться у власності приватних суб’єктів, але порушення їх роботи може вплинути на життєдіяльність навколишніх територій (які є зоною відповідальності та уваги місцевих органів державної влади органів місцевого самоврядування), доречним є розширення кола учасників державно-приватного партнерства, включаючи в його структуру регіональну та місцеву владу, а також структури цивільного захисту населення.

3. За прикладом Німеччини суб’єктам національної системи кібербезпеки доцільно розширювати співпрацю з науковими та освітніми закладами з метою пошуку нових, динамічніших рішень в інтересах кібербезпеки, в т.ч. тих об’єктів критичної інфраструктури, які не завжди з’являються у фокусі уваги відповідних органів (мости, тунелі, дороги).

4. Спільно із науковими та освітніми структурами, а також заінтересованими приватними структурами розглянути можливість проведення щорічних інформаційно-пропагандистських заходів «Кібергігієна» в сфері підвищення обізнаності населення з основами кібербезпеки, інформуючи їх при цьому про основні виклики та форми кіберзлочинів, формуючи належну кібергігієну користувачів.

5. Випрацювати механізми більш широкого донесення до бізнесу важливості ІТ-безпеки. Сама сфера має стати більш зрозумілою та відчутним з точки зору ризиків та можливих рішень. Інформаційна робота не повинна обмежуватися основними месиджами в ЗМІ, але повинна призводити до зацікавлення сторін та підвищення свідомості щодо необхідності підтримки ІТ-безпеки внутрішньо та співдії назовні із державою.

6. Спільно з освітніми та бізнес структурами розглянути можливість створення постійно діючих безкоштовних курсів підвищення кваліфікації для ІТ-фахівців, що безпосередньо займаються питанням убезпечення інформаційних систем (з акцентом на підприємства малого та середнього бізнесу, де рівень кібербезпеки традиційно найнижчий).

7. Великий масив критично важливої інформації часто має гриф обмеженого доступу. Водночас без чіткої та своєчасної інформації про наявні загрози неможливо ефективно управляти ризиками. Це може передбачати переоцінку критеріїв віднесення інформації до такої, що регулюється грифами таємності з метою зробити таку інформацію більш доступною для приватного сектору (особливо для великих компаній).

Бойко В.О.
Відділ інформаційної безпеки та розвитку інформаційного суспільства
Національний інститут стратегічних досліджень
травень 2018