ДЕРЖАВНО-ПРИВАТНЕ ПАРТНЕРСТВО У СФЕРІ КІБЕРБЕЗПЕКИ: ДОСВІД ВЕЛИКОЇ БРИТАНІЇ

У часи тотального проникнення ІКТ в усі сфери життя суспільства, залежності функціонування державних та приватних установ від захищеності об'єктів критичної інфраструктури, ефективне державно-приватне партнерство у сфері кібербезпеки стає життєво важливим елементом системи національної безпеки держави. 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 державно-приватного партнерства є актуальним для України з точки зору підходів та механізмів співпраці, особливо зважаючи на те, що Стратегією кібербезпеки України, що ухвалена 2016 року, державно-приватне партнерство було визначено як один з головних принципів забезпечення кібербезпеки.

1. Нормативно-правова та інституційна база державно-приватного партнерства у сфері кібербезпеки

1.1. Державно-приватне партнерство як форма державних закупівель

Державно-приватне партнерство у будь-якій сфері функціонування держави можна розуміти широко – як сукупність будь-яких спільних заходів державного та приватного сектору, спрямованих на досягнення певних цілей. З іншого боку, державно-приватне партнерство також виступає механізмом взаємодії між державою та приватним сектором, за допомогою якого реалізуються проекти у певній сфері, тобто по суті є формою державних

закупівель. На законодавчому рівні у Великій Британії закріплення поняття державно-приватного партнерства можна знайти в Акті про державні ресурси та рахунки 2000 року (Government Resources and Accounts Act), де зазначено, що державно-приватне партнерство – 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»[1]. Відповідальним за механізм державно-приватного партнерства 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 державно-приватного партнерства. Так, у 1992 році Міністерством фінансів була запущена схема Private Finance Initiative (PFI), за якою приватні компанії підписують довгострокові контракти з державними установами, розробляють відповідно до вимог установи, фінансують та управляють певними (переважно інфраструктурними) проектами; після виконання проекту держава продовж кількох десятиліть сплачує постачальнику за використання реалізованого об'єкту[2]. У 2012 PFI була оновлена та замінена на Private Finance 2; згідно з PF2 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 державно-приватного партнерства[3]. Станом на березень 2016 року налічувалось 716 проектів PFI та PF2, з яких 686 були виконані та за які держава почала виплачувати кошти; загальна

[1] https://www.legislation.gov.uk/ukpga/2000/20/pdfs/ukpga_20000020_en.pdf
[2]https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/205112/pf2_infrastructure_new_approach_to_public_private_parnerships_051212.pdf.
[3]https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/579271/PFI_and_PF2_projects_2016_summary_data.pdf.

вартість проектів складала 59,4 млрд фунтів стерлінгів (проекти з найбільшою сукупною вартістю реалізовувались на замовлення Департаменту охорони здоров'я (майже 13 млрд фунтів), Міністерства оборони (9,5 млрд фунтів), Департаменту освіти (близько 8,6 млрд фунтів), та Департаменту транспорту (7,8 млрд фунтів)[4]. Серед цих діючих у 2016 році проектів у сфері IT-інфраструктури та комунікацій були, зокрема: проект Defence Fixed Telecommunications Service, який у 1997 році на замовлення Міністерства оборони Великої Британії почала реалізовувати British Telecom, загальна вартість склала 312,2 млн фунтів; проект запуску у 2008 супутника Skynet 5 від Airbus Defence & Space на замовлення Міноборони, загальна вартість – понад 1,3 млрд. фунтів; розпочатий у 2002 році проект впровадження автоматизованої системи управління справами Compass CMS від CGI Group у Королівській прокурорській службі, загальна вартість – 2,9 млн фунтів[5].

Поряд зі схемами державно-приватного партнерства у Великобританії 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 році ініціатива «G-Cloud», в рамках якої державні структури можуть закуповувати послуги у провайдерів хмарних сервісів. Компанії різних розмірів можуть раз на рік подавати заявки та бути обраними в якості постачальників одного з трьох видів хмарних сервісів – хостингу, програмного забезпечення та послуг підтримки[6]. Державні структури отримують доступ до он-лайн магазину Digital Marketplace, де можуть придбати необхідні хмарні сервіси від обраних компаній. Крім того, на Digital Marketplace державні органи можуть знаходити послуги експертів у сфері цифрових технологій в рамках програми

[4] там само.
[5] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/579881/current_projects_as_at_31_March_2016.xlsx.
[6] https://www.gov.uk/guidance/the-g-cloud-framework-on-the-digital-marketplace.

«Digital Outcomes and Specialists», а також отримати фізичний обсяг місця у дата-центрі в рамках програми «Crown Hosting Data Centres» (спільне підприємство, створене урядом та компанією Ark Data Centres Limited)[7]. У 2015 році Королівська комерційна служба запустила програму закупівлі консалтингових послуг у сфері кібербезпеки «Cyber Security Services» – державні структури отримали змогу обирати визначених приватних постачальників послуг з розробки політик безпеки даних, оцінки та управління ризиками, управління інцидентами, розробки безпекової архітектури установи тощо[8].

1.2. Стратегічний та інституційний аспект державно-приватного партнерства

На стратегічному рівні державно-приватне партнерство (у його широкому розумінні) у сфері кібербезпеки визначено однією з основ сталого функціонування безпекової системи держави. Стратегія кібербезпеки Великобританії, ухвалена на період 2011-2015 років, визначала ключову роль приватного сектору для кібербезпеки, оскільки переважна більшість потужностей та технологій знаходиться у руках приватних компаній. У рамках встановлення партнерства з приватним сектором держава вживала заходів щодо обміну інформацією про кіберзагрози, управлінням кіберінцидентами, розбудови спроможностей кібербезпеки, розробки галузевих стандартів кібербезпеки[9]. За результатами оцінки урядом виконання Стратегії 2011-2015 рр.[10] можна стверджувати, що у напрямку розбудови партнерства з приватним сектором було зроблено чимало кроків. Із загального 5-річного обсягу фінансування, виділеного урядом на реалізацію Стратегії (близько 860 млн. фунтів), близько 61,1 млн. фунтів

[7] https://www.gov.uk/guidance/the-crown-hosting-data-centres-framework-on-the-digital-marketplace.
[8] http://www.government-online.net/cyber-security-consultancy-framework-for-uk-public-sector/.
[9] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf.
[10] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/516331/UK_Cyber_Security_Strategy_Annual_Report_2016.pdf.

було витрачено лише на залучення бізнесу до співпраці та підвищення його обізнаності у питаннях кібербезпеки; найбільше коштів було виділено на підвищення спроможності держави виявляти та ліквідовувати найнебезпечніші загрози – 441,8 млн фунтів[11].

Чинна Стратегія кібербезпеки на 2016-2021 рр. наголошує, що «бізнес зменшить потенційні кіберзагрози, лише якщо буде оцінювати та мінімізувати ризики для своїх критичних систем та конфіденційних даних, інвестуючи у людський капітал, технології та управління»[12]. 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, стійкість систем, має розв'язувати кіберінциденти та нести юридичну відповідальність за наслідки можливих кібератак. Нова Стратегія передбачає збільшене у понад 2 рази фінансування – 1,9 млрд фунтів, а головною метою держави проголошує «зробити Сполучене Королівство найбільш безпечним місцем для життя та ведення бізнесу он-лайн»[13].

Слід зазначити, що одним з найпомітніших результатів виконання попередньої 5-річної Стратегії стало об'єднання у жовтні 2016 року 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)[14]. 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.

---

[11] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf.

[12] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

[13] там само.

[14] https://www.ncsc.gov.uk/information/about-ncsc.

У 2017 році зусилля Королівської комерційної служби у напрямку закупівель консалтингових послуг були об'єднані з зусиллями Національного центру кібербезпеки, що вилилось у впровадження рамкової програми «Cyber Security Services 2». Зокрема, програма була значно розширена – на додачу до постачальників консалтингових послуг були додані 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[15].

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[16]), 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[17].

1.3. Законодавче регулювання порушень базових правил кібербезпеки

Розглядаючи законодавчий аспект державно-приватного партнерства у

[15] http://ccs-agreements.cabinetoffice.gov.uk/DF_NCSC_Certs.
[16] https://www.ncsc.gov.uk/information/about-ncsc.
[17] https://www.cpni.gov.uk/critical-national-infrastructure-0.

кібербезпеці, 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[18]). Компанії, які працюють з персональними даними, підпадають під дію Акту про захист даних (Data Protection Act) 1998 року та Положення про конфіденційність та електронні комунікації (Privacy and Electronic Communications (EC Directive) Regulations) 2003 року (британський законодавчий акт, яким була імпелементована відповідна Директива ЄС 2002/58/ЕС про обробку 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 он-лайн тощо)[19].

У випадку кібератаки, яка призвела до знищення чи крадіжки персональних даних, компанії мають повідомити Офіс інформаційного комісара (Information Commissioner's Office, ICO) – підзвітну безпосередньо парламенту структуру, яка фінансується Департаментом цифрового розвитку, культури, медіа та спорту. ICO розглядає кожну конкретну ситуацію та визначає, чи призначати штраф (максимальний розмір – до 500 тис. фунтів[20]). Серед найрезонансніших випадків накладання на компанії Великої Британії штрафів за кіберінциденти можна згадати справу Інтернет-провайдера TalkTalk. Так, у жовтні 2015 року 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

[18]https://www.hldataprotection.com/2016/12/articles/international-eu-privacy/the-uks-cybersecurity-regulatory-landscape-an-overview/.
[19]https://ico.org.uk/for-organisations/guide-to-pecr/.
[20]http://www.computerweekly.com/news/450423941/Government-to-strengthen-UK-data-protection-law.

15 тис. осіб. Хоча компанія і повідомила ICO про інцидент, регулятор стягнув з неї 400 тис. фунтів штрафу за недотримання базових вимог захисту даних користувачів[21]. Дещо інша ситуація склалася навколо інциденту в компанії Uber; у жовтні 2016 року 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 за видалення даних[22]. Станом на середину грудня 2017 року ситуація розслідується ICO та NCSC; хоча викрадені дані не були чутливими, до Uber може бути застосовано штраф за порушення вимог до безпеки даних користувачів.

З 9 травня 2018 року процедура повідомлення про кіберінциденти має стати обов'язковою у Великій Британії через набуття чинності новим законодавством ЄС, зокрема Директиви ЄС щодо мережевої та інформаційної безпеки (The Network and Information Security Directive, NIS) 2016 року. 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[23].

Загальний регламент захисту даних (General Data Protection Regulation, GDPR) 2016 року (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 клієнтам, проводити регулярні оцінки стану захищеності даних. Крім того, GDPR визначає необхідність надавати користувачам більший контроль

[21] https://www.theguardian.com/business/2016/oct/05/talktalk-hit-with-record-400k-fine-over-cyber-attack.
[22] https://www.theguardian.com/technology/2017/nov/22/uber-failed-to-tell-uk-authorities-of-data-breach-says-no-10.
[23] 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.

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[24], 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 року 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 року Європарламент проголосував за зміни, а станом на початок січня 2018 року пропозиція нового положення проходить процедуру обговорення державами-членами ЄС[25]. 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[26]. 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[27]. Питання того, яким саме чином ці норми будуть впроваджені – шляхом включення Регламенту до національного

[24] http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf.
[25] https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications.
[26] там само.
[27] https://publications.parliament.uk/pa/cm201617/cmselect/cmeuleg/71-xxix/7109.htm.

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»[28]. 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»[29], 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 обсязі до 25 травня 2018 року[30]. Регламент має бути імплементований у британське законодавство новим Актом про захист даних, який нині проходить слухання у парламенті.

2. Співробітництво держави та приватного сектору у сфері кібербезпеки

2.1. Британський ринок кібербезпеки

Велика Британія – держава з одним з найдинамічніших, інноваційних та потужних ринків кібербезпеки у Європі та світі. За останніх сім років загальний обсяг британського ринку кібербезпеки зріс на майже півтора мільярди доларів – з 2,4 млрд фунтів стерлінгів у 2010 році до майже

[28] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/579442/Cyber_Security_Regulation_and_Incentives_Review.pdf.
[29] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/636207/NIS_Directive_-_Public_Consultation__1_.pdf.
[30] https://ico.org.uk/media/about-the-ico/documents/2014356/international-strategy-03.pdf.

3,5 млрд фунтів у 2017[31]. Збільшується також частка експорту продукції та послуг кібербезпеки у загальному безпековому експорті Великої Британії. Так, у 2016 році кібербезпека склала 34 % усього обсягу безпекового експорту, або понад 1,5 млрд[32].

Разом із 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 справа стосується 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 році було зафіксовано 3,6 млн. випадків он-лайн шахрайства та 2 млн випадків неправомірного використання комп'ютерів, що загалом на 8 % більше, ніж минулого року[33]. За результатами оцінки порушень кібербезпеки у період з жовтня 2016 по січень 2017 року, проведеної урядовим Департаментом культури, медіа та спорту, 46 % опитаних з 1523 компаній зазнали хоча б однієї кібератаки або порушення безпеки за останній рік; одна компанія у середньому втрачає 1570 фунтів стерлінгів на одній атаці (для великої компанії ця цифра складає 19 тис. фунтів, для середнього бізнесу – 3070, для малого – 1380)[34]. Переважна більшість

[31]https://www.statista.com/statistics/289173/uk-cyber-security-private-enterprises-segment-size/.
[32]https://www.gov.uk/government/publications/uk-defence-and-security-export-figures-2016/uk-defence-and-security-export-statistics-for-2016.
[33]http://www.bbc.com/news/uk-38675683.
[34]https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/609186/Cyber_Security_Breaches_Survey_2017_main_report_PUBLIC.pdf.

порушень пов’язана з відкриттям шахрайських електронних повідомлень, вірусами, шкідливим ПЗ та програмами-вимагачами [29], що свідчить про значний вплив людського фактору 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[35]. Такі факти порушень на низовому рівні можуть призводити до суттєвих збитків на рівні національної економіки, тому одним із важливих напрямків державно-приватного співробітництва стає впровадження базових рекомендацій з кібербезпеки у різних компаніях.

2.2. Програми співробітництва держави та бізнесу

Одним з найпомітніших та найефективніших проектів державно-приватного партнерства у сфері кібербезпеки можна назвати започатковане у 2013 році 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 та динамічному середовищі, посилюючи ситуаційну обізнаність та зменшуючи вплив на бізнес у Сполученому Королівстві»[36]. 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 по боротьбі зі злочинністю). Отримуючи інформацію про порушення безпеки в інформаційних системах компаній,

[35] там само.

[36] https://www.ncsc.gov.uk/content/files/protected_files/news_files/The%20Cyber%20Threat%20to%20UK%20Business%20%28b%29.pdf.

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 року членами CISP були понад 2800 організацій та 8000 осіб[37], за рік роботи рівень залучення до партнерства збільшився на 43 %[38].

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 році 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[39]. Згодом у 2016 році Cyber Streetwise була перейменована на Cyber Aware[40], 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[41].

У 2014 році 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,

---

[37] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/516331/UK_Cyber_Security_Strategy_Annual_Report_2016.pdf.

[38] http://www.computerweekly.com/news/450427340/UK-National-Cyber-Security-Centre-looks-to-future-in-annual-review.

[39] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/273330/cyber_streetwise_open_for_business.pdf.

[40] https://www.cyberaware.gov.uk/.

[41] https://www.ncsc.gov.uk/content/files/protected_files/news_files/The%20Cyber%20Threat%20to%20UK%20Business%20%28b%29.pdf.

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[42]. 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[43]. Серед інших прикладів рекомендаційних матеріалів для бізнесу слід також назвати «10 кроків до кібербезпеки», розроблені GCHQ у 2015 році[44].

З 2015 року 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 Level39, надавши малому і середньому бізнесу та стартапам можливість демонструвати їх пропозиції потенційним клієнтам та інвесторам у спеціально обладнаних приміщеннях[45]. Станом на жовтень 2017 року до Cyber Growth Partnership входять 570 компаній та організацій, серед яких Cisco, KPMG, Barclays, платформа технологічних компаній techUK та багато інших[46]. Ця програма сприяє функціонуванню потужного хабу представників сектору кібербезпеки Великобританії.

---

[42] https://www.cyberessentials.ncsc.gov.uk/about.html.

[43] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/516331/UK_Cyber_Security_Strategy_Annual_Report_2016.pdf.

[44] https://www.ncsc.gov.uk/guidance/10-steps-cyber-security.

[45] https://cyberexchange.uk.net/#/cdc.

[46] https://cyberexchange.uk.net/media/admin/resources/Cyber%20Exchange%20Newsletter%20Oct%2017%20FINAL.pdf.

Прогресивним напрямком державно-приватного партнерства є безпосереднє залучення представників бізнесу до роботи у Національному центрі кібербезпеки. Запущена у лютому 2017 року 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)[47]. Впродовж 2017-2018 рр. планується залучити 100 фахівців з приватних компаній. Нині NCSC не має оцінки проміжних результатів реалізації програми, однак перші залучені фахівці вже розпочали писати відгуки про їх залучення до роботи Центру, які в цілому можна назвати позитивними; доступними зараз є більше 20 позицій, що може свідчити про відносно позитивну динаміку набору людей.

Поряд із програмами загального спрямування, які координуються з єдиного Національного центра кібербезпеки, різні урядові департаменти розробляють рекомендації по дотриманню базових правил кібербезпеки у своїх сферах. Так, наприклад, Департамент транспорту у 2016 році підготував рекомендації з кібербезпеки для залізничних перевізників[48]. Департамент у справах бізнесу, енергетики та промислової стратегії на початку 2017 року розробив окрему Стратегію кібербезпеки для цивільного ядерного сектору, який на сьогодні забезпечує близько 18 % потреб Великої Британії в електроенергії[49] Пізніше цього 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[50]. Департамент охорони здоров'я підготував вимоги до забезпечення безпеки даних провайдерами послуг у сфері охорони

[47] https://www.ncsc.gov.uk/information/industry-100.

[48] https://www.rssb.co.uk/Library/improving-industry-performance/2016-02-cyber-security-rail-cyber-security-guidance-to-industry.pdf.

[49] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/591619/170213_-_Civil_Nuclear_Cyber_Security_Strategy.pdf.

[50] https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles/the-key-principles-of-vehicle-cyber-security-for-connected-and-automated-vehicles.

здоров'я[51]. 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 щороку, з яких 10 млн фунтів призначатиметься на підтримку стартапів[52]. У січні 2016 року Департамент цифрового розвитку, культури, медіа та спорту запустив спільно з акселератором Cyber London та Центром безпеки інформаційних технологій при Королівському університеті Белфасту програму ранньої підтримки стартапів, бюджет якої склав 250 тис. фунтів[53]. Програма згодом отримала назву «HutZero» та передбачає 6-місячний інтенсивний курс для 20 майбутніх підприємців[54]. У березні 2016 року 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 Великобританії представлена дочірньою компанією O2 – 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 напрямках. Зокрема після відбору спеціальною комісією у складі представників держави, Wayra UK, Telefónica Group та інвесторів, компанія матиме змогу отримати грант на 25 тис. фунтів, доступ до широкої мережі ресурсів та експертів, а також приміщення для

[51] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/655876/171027_2017-18_Data_Security_Requirements.pdf.
[52] https://techcrunch.com/2017/10/18/gchq-cyber-accelerator-doubles-down-for-second-intake/.
[53] https://www.gov.uk/government/news/making-cyberspace-cyber-safe-new-government-initiative-for-cyber-startups-will-drive-innovation.
[54] http://www.hutzero.co.uk/.

початкового ведення діяльності[55]. За результатами першого набору програми, що тривав 9 місяців, сім стартапів загалом зібрали понад 2,7 млн фунтів[56].

2.3. Підтримка освітніх та дослідницьких ініціатив

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 галузі фізики та інженерних наук забезпечують залучення приватного сектору до фінансової допомоги університетам, при яких створюються центри вивчення передового досвіду у сфері кібербезпеки (на 2017 рік такі центри діяли у 14 британських університетах[57]). Обсяг інвестицій варіюється від 10 тис. фунтів для малого бізнесу (до 10 співробітників) до 500 тис. фунтів для великих компаній (понад 250 співробітників), або ж компанії можуть допомагати обладнанням та іншими ресурсами. Впродовж наступних 5 років 24 компанії, серед яких IBM, Cisco, Airbus, Hewllett Packard та інші, інвестують у дослідження понад 8 млн фунтів[58].

Окремим, але не менш важливим напрямком 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[59]. Серед ключових проектів у цьому напрямку можна назвати програму «CyberFirst», що організовується Національним центром

[55] https://wayra.co.uk/gchq/.
[56] https://www.ncsc.gov.uk/news/firms-urged-apply-groundbreaking-gchq-cyber-start-scheme.
[57] https://www.ncsc.gov.uk/articles/academic-centres-excellence-cyber-security-research.
[58] https://www.ncsc.gov.uk/articles/cyber-invest.
[59] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

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 для першокурсників, які планують будувати кар'єру у цій сфері; для талановитих студентів також є можливість пройти 3-річну програму професійної підготовки «CyberFirst Degree Apprenticeship»[60].

Більше того, NCSC станом на 2017 рік встановив партнерство з 25-ма 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[61]. У планах Великої Британії до 2020 року: підготовка 6000 підлітків в 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[62]. Для представників бізнесу наразі є чимало безкоштовних он-лайн курсів[63].

ВИСНОВКИ

1. Державно-приватне партнерство у сфері кібербезпеки у Великій Британії розглядається у широкому контексті як один ключових механізмів попередження та мінімізації кіберзагроз національній безпеці, необхідна передумова забезпечення національної стійкості та одна з основ процвітання держави у цифровому просторі. Державно-приватне партнерство як механізм державних закупівель також відіграє важливу роль у забезпеченні державних структур якісними послугами, зокрема, у сфері цифрових технологій.

2. Ринок кібербезпеки Великої Британії розвивається дуже динамічно,

[60] https://www.ncsc.gov.uk/articles/cyber-first-bursary-scheme.
[61] https://www.ncsc.gov.uk/Academics-and-researchers.
[62] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.
[63] https://www.gov.uk/government/collections/cyber-security-training-for-business.

і для забезпечення його захищеності і 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. Перед обличчям спільної загрози для держави та приватного сектору ефективнішою є злагоджена взаємодія та спільна розробка механізмів протидії кіберзагрозам.

3. 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.

4. 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 з впровадження високих стандартів кібербезпеки, у тому числі – галузевих.

5. Попри активність держави у напрямку розбудови партнерства, бізнес не завжди добровільно попереджає державні структури про загрози, з якими стикається і які можна попередити, що обумовлює необхідність більш жорсткого регулювання.

РЕКОМЕНДАЦІЇ

1. Стаття 10 Закону України «Про основні засади забезпечення кібербезпеки України», який був прийнятий 5 жовтня 2017 року та набуває чинності 9 травня 2018 року, містить перелік шляхів здійснення «державно-приватної взаємодії» у сфері кібербезпеки[64], який потребує подальшої конкретизації. Передусім, вбачається необхідним внесення однозначності у понятійний апарат, зокрема надання чіткого визначення «державно-

[64] http://zakon2.rada.gov.ua/laws/show/2163-19.

приватної взаємодії», про яку йде мова в Законі та «державно-приватного партнерства», про яке згадується у Стратегії кібербезпеки України.

2. Розглянути можливість запровадження подібного британському CISP захищеного он-лайн механізму обміну інформацією про кібернетичні загрози між представниками індустрії кібербезпеки та електронних комунікацій з одного боку та державних структур, зокрема, Служби безпеки України, Департаменту кіберполіції Національної поліції України, Державного центру кіберзахисту та протидії кіберзагрозам та його підрозділу CERT-UA, – 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.

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

5. Доцільним є ініціювати розробку 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 з дотримання базових правил кібербезпеки. Крім того, необхідною також є розробка (зусиллями СБУ, Кіберполіції та CERT-UA) поглиблених галузевих рекомендацій для підприємств та установ критичної інфраструктури.

6. З метою перейняття практичного досвіду приватного сектору у питаннях попередження кіберзагроз, реагування на кіберінциденти та захисту інформаційних систем ключові суб'єкти 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 в рамках Трастового фонду Україна-НАТО з питань кібербезпеки.

7. Для забезпечення додаткового наукового та інформаційного забезпечення суб'єктів національної системи кібербезпеки доцільним вбачається створення при ключових ВНЗ України центрів вивчення передового досвіду у сфері кіберпезпеки. В якості пілотного проекту 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.

А.В. Покровська

Т.О. Ісакова

відділ інформаційної безпеки та

розвитку інформаційного суспільства

Національного інституту стратегічних досліджень