# НОРМАТИВНО-ПРАВОВІ ТА ОРГАНІЗАЦІЙНІ ЗАСАДИ ДЕРЖАВНО-ПРИВАТНОГО ПАРТНЕРСТВА США У СФЕРІ КІБЕРБЕЗПЕКИ

Сьогодні інтегрованість мереж державного та приватного секторів стає все 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 в галузі кібербезпеки та забезпеченні цілісності мережевої інфраструктури.

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

Як державний так і приватний сектори отримують користь від спільної роботи над ініціативами з кібербезпеки. Оскільки приватний сектор контролює більшу частину критичної інфраструктури, яка часто є привабливою для дій кіберзлочинців, багато приватних компаній вже мають програми з кібербезпеки, володіють спеціальними знаннями та досвідом у вирішенні потенційних загроз. Державний сектор, зі свого боку, має ширші

[1] Киберготовность США 2.0 // https://digital.report/kibergotovnost-ssha-2-0-vvedenie/

можливості для розслідування кіберзлочинів та переслідування кіберзлочинців.

Вперше 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))[2] від 1998 року, 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 «Публічно-приватне партнерство» констатує наступне: «*Оскільки цілі нападів на нашу критичну інфраструктуру, ймовірно, включатимуть як об'єкти в сфері економіки, так і урядові, зменшення нашої потенційної вразливості вимагає тісно узгоджених 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 сектора. Разом ці дві особи, а також відомства та корпорації, які вони представляють, сприяють розробці галузевого плану національної інфраструктури шляхом:

- оцінки вразливості сектору до кібер- або фізичних атак;
- надавання рекомендацій щодо усунення вразливості;

[2] Presidential Decision Directive/NSC-63 // https://fas.org/irp/offdocs/pdd/pdd-63.htm

- пропозиції щодо системи виявлення та запобігання спробам потужних атак;
- розробки плану для оповіщення про атаки, з подальшим швидким відновленням мінімально необхідного потенціалу після атаки.

Під час підготовки галузевих планів *Державний координатор з питань безпеки, захисту інфраструктури та протидії тероризму* (*National Coordinator for Security, Infrastructure Protection and Counter-Terrorism*) разом з представниками провідного федерального агентства галузі та представником Національної економічної ради (*National Economic Council*)[3] 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*). Мета організації – виконувати функції з оцінки загроз, попередження, виявлення вразливостей державної критичної інфраструктури та сприяння правоохоронним органам у розслідуванні та реагуванні. NIPC включав 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*). Дані центри створюються як неприбуткові організації, які 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

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

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 Центри обміну та аналізу, ті, у яких такі Центри відсутні, отримують такі послуги від зовнішніх постачальників. Зокрема, Центр обміну та аналізу інформації фінансових інститутів (FS-ISAC) надає допомогу у визначенні, запобіганні та реагуванні в разі кібер-інцидентів та при спробі кібер-фальсифікації. З цією метою Центру 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 зі своєчасного повідомлення про можливі кіберзагрози та інші загрози у міжнародному масштабі. В рамках своєї співпраці з 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 кібер-атак у відношенні кількох банків США в 2012-2013 рр. FS-ISAC надавав допомогу деяким з банків в оцінці серйозності та захисту від таких атак завдяки обміну інформацією між ними в режимі реального часу. FS-ISAC також здійснює кроки в напрямку розповсюдження своєї системи обміну інформацією з участю організацій у Великобританії та Європі*[4].

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 розробки 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

[4] https://digital.report/kibergotovnost-ssha-2-0-obmen-informatsiey/

злочинності та розробляє шляхи запобігання та реагування на комп'ютерні злочини неповнолітніми».

Окремо варто наголосити на ініціативах Б. Обами в питанні обміну інформації про кіберзагрози в інтересах посилення захищеності віртуального простору. Так, у 2011 році 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 і 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 слідувати визначеним правилам щодо обмеження її зберігання та використання. План наказує Міністерству внутрішньої безпеки і Генеральній прокуратурі розробити для федерального уряду інструкції по отриманню, зберіганню, використанню та розкриттю 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 або 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 … У той же час, пропозиція передбачає надійний контроль за конфіденційністю, щоб

гарантувати, що така інформація не зачіпає особисту приватність та громадянські свободи»[5].

Таким чином обов'язки NIPC були передані Міністерству внутрішньої безпеки і в даний час входять до сфери діяльності NCCIC, який є центром координації дій в разі кіберінцидентів на федеральному рівні, рівні штатів, на місцевому, територіальному, міжнародному рівнях і в приватному секторі. Він несе відповідальність за інформування та координацію реагування на кіберінциденти, зниження ризиків і відновлювальні заходи в основному відносно федеральних мереж, при співробітництві з приватним сектором, громадянським суспільством, правоохоронними органами, розвідкою, цивільною обороною, а також міжнародними організаціями[6].

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

- 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 в сфері кіберпростору та телекомунікацій;
- служінні для зацікавлених сторін як національний центр передового досвіду та експерт з питань кібербезпеки та телекомунікацій;

[5] Cybersecurity Legislative Proposal // https://obamawhitehouse.archives.gov/the-press-office/2011/05/12/fact-sheet-cybersecurity-legislative-proposal
[6] National Cybersecurity and Communications Integration Center // https://www.us-cert.gov/nccic

- захисті приватності та конституційних прав американського народу під час виконання своєї місії[7].

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 № 13636 «Про підвищення кібербезпеки в сфері критичної інфраструктури» (Improving Critical Infrastructure Cybersecurity)[8], підписаний в лютому 2013 р., Виконавчий указ № 13691 «Про обмін інформацією з кібер-безпеки в приватному секторі» (Private Sector Cybersecurity Information Sharing)[9], підписаний в лютому 2015 р. Ці документи вказують на необхідність збільшення обсягів, своєчасності і якості обміну інформацією про кібер-загрози між приватним сектором і урядом, а також наголошують на доцільності більш тісної співпраці в сфері аналізу інформації за участю всіх зацікавлених сторін.

Особливу увагу Указ № 13691 приділяв 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, в рамках якого такі ж угоди про обмін інформацією міг би укладати і NCCIC. Крім того, Указ передбачає включення Міністерства внутрішньої безпеки в список федеральних агентств, які можуть видавати схвалення і підписувати угоди

[7] National Cybersecurity and Communications Integration Center // https://www.dhs.gov/national-cybersecurity-and-communications-integration-center
[8] Executive Order -- Improving Critical Infrastructure Cybersecurity. EXECUTIVE ORDER // https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity
[9] Executive Order 13691—Promoting Private Sector Cybersecurity Information Sharing // https://www.dhs.gov/sites/default/files/publications/2015-03714.pdf

про обмін секретною інформацією для того, щоб дозволити приватним компаніям отримати доступ до секретної інформації про наявні кіберзагрози. Указ № 13691 також містить положення про необхідність створення дієвих механізмів захисту приватності і 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 в галузі кібернетики в приватному секторі, уповноважує Міністерство внутрішньої безпеки[10]:

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

Здійснювати постійну, спільну та всеохоплюючу координацією з ISAO через NCCIC, який координує обмін інформацією в галузі кібербезпеки та проводить аналіз в середовищі партнерів приватного сектора і федерального уряду.

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

Стандарти ISAO полягають у принципах:

- добровільності – участь у формуванні ISAO не є обов'язковою. Скоріше вона має бути абсолютно необов'язковою та добровільною;
- прозорості – за допомогою спільного та прозорого процесу, органи державного та приватного секторів матимуть змогу надавати інформацію про розроблені стандарти;

[10] Information Sharing and Analysis Organizations (ISAOs) // https://www.dhs.gov/isao#

- інклюзивності – учасники з будь-якого сектора, некомерційного або комерційного, експертного або новачка, повинні мати можливість брати участь у створенні власної ISAO;
- дієвості – учасники отримають корисний та практичний набір стандартів та найкращих практик для використання в якості керівництва, якщо вони вирішать брати участь у створенні ISAO;
- гнучкості – стандарти не мають перешкоджати формуванню ISAO або завдавати шкоди поточним процесам існуючих організацій, що здійснюють обмін інформацією.

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

Окремим документом, що фіксує процедури співпраці між приватними компаніями і урядовими установами в сфері інформаційної безпеки є р **Акт про обмін інформацією в сфері кібербезпеки** (*Cybersecurity Information Sharing Act, CISA*)[11]**,** затверджений Конгресом наприкінці 2015 року. Відповідно до нього організації, які на добровільній основі обмінювалися інформацією про кібер-загрози 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

[11] https://www.fpc.gov/19081/

від можливих судових позовів з боку користувачів, якщо передана органам влади інформація про кіберзагрози містить персональні дані.

Акт зобов'язує Міністерство внутрішньої безпеки: 1) одержувати інформацію про кіберзагрози і 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.

В рамках виконання Акту Міністерство внутрішньої безпеки розробило систему автоматичного обміну індикаторами (*Automated Indicator Sharing, AIS*)[12], яка дозволяє отримувати нові індикатори кіберзагроз від підприємств приватного сектору і урядових організацій автоматично, а також стимулює співпрацю приватного сектору з NCCIC в питаннях підготовки їх мереж до автоматичного обміну такими індикаторами. Мета програми AIS – автоматичне надання інформації організаціям-учасницям, в т. ч. Федеральним міністерствам і агентствам, приватним компаніям і Центрам обміну і аналізу інформації (ISACs).

В рамках реалізації даного Акту, операційна система AIS запрацювала з березня 2016 року, 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, що стосуються приватності та громадянських свобод (що стосуються обміну цими показниками), та керівництво для федеральних установ щодо обміну інформацією, якою володіє уряд. Серед цих документів, зокрема, наступні[13]:

- Заходи із захисту та обміну індикаторами кіберзагроз (*Sharing of Cyber Threat Indicators and Defensive Measures*)

[12] Automated Indicator Sharing (AIS) // https://www.us-cert.gov/ais
[13] Там само

- Керівництво зі сприяння недержавним суб'єктам щодо обміну індикаторами кібер-загроз 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 кібер-загроз 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 державно-приватного партнерства (ДПП) Міністерства внутрішньої безпеки з приватним сектором для обміну інформацією про кіберзагрози стало укладання **Угод про співпрацю в галузі досліджень і розробок** (*Cooperative Research and Development Agreements, CRADA*)[14], які є частиною реалізації більш всеосяжної Програми зі співробітництва та обміну кіберінформацією (*Cyber Information Sharing and Collaboration Program, CISCP*)[15].

> *Ключовим напрямком діяльності CISCP є двосторонній обмін інформацією: партнери CISCP надають індикатори зафіксованих кібер-загроз та інформації про кібер-інциденти та виявлені вразливі місця Міністерству внутрішньої безпеки, якими потім передаються Міністерством з іншими партнерами CISCP у анонімному та збірному форматі. Після отримання даних аналітики CISCP редагують інформацію про власника та персональну інформацію та аналізують дані у співпраці з державними та галузевими партнерами для вироблення точних, актуальних, своєчасних та аналітичних документів. В даний час ці документи втілюються у формі: Бюлетні індикаторів, Аналітичні звіти, Пріоритетні оповіщення, Рекомендовані практики.*

[14] Cooperative Research and Development Agreements (CRADAs) // https://www.fda.gov/ScienceResearch/CollaborativeOpportunities/CooperativeResearchandDevelopmentAgreementsCRADAs/default.htm

[15] Cyber Information Sharing and Collaboration Program (CISCP) // https://www.dhs.gov/ciscp

Крім іншого, Спільна національна оперативна група кібер-розслідувань (*National Cyber Investigative Joint Task Force, NCIJTF* )[16], спільно з іншими федеральними кібер-центрами та органами вдосконалюють систему кібер-безпеки ФБР **Cyber Guardian system**, з метою підвищення якості процесу створення і використання звітів про кібер-загрози, а також оповіщення компаній, які вже були цілями шкідливої кібер-діяльності. В рамках цієї діяльності різні кібер-центри створили і поширили більш 10,000 звітів про кібер-загрози і розіслали понад 2,000 повідомлень про них станом на липень 2015 р. Нарешті, в лютому 2015 р Президент 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 кібер-загрози[17]. CTIIC в даний час служить 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[18], 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 сектора, в цій ініціативі беруть участь міжнародні представники з Канади, Австралії, Великобританії, 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 в галузі

[16]National Cyber Investigative Joint Task Force // https://www.fbi.gov/investigate/cyber/national-cyber-investigative-joint-task-force
[17] The Cyber Threat Intelligence Integration Center // https://www.dni.gov/index.php/ctiic-who-we-are
[18] National Cyber-Forensics & Training Alliance // http://www.ncfta.net/

охорони порядку, безпеки бізнесу, а також з дослідницьких кіл, з метою запобігання ризиків і протиправної діяльності, а також для збору інформації, необхідної для переслідування злочинців.

Співпраця з партнерами призвела до відкриття безлічі кримінальних та цивільних розслідувань, які інакше могли залишитися нерозглянутими. 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*)[19] в 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 запобігання найбільш комплексних кібер-загроз.

> *Центр поводить зустрічі раз на два тижні 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 їх запобігання, а також бере активну участь у дослідницькій роботі в цій галузі, співпрацюючи з приватним сектором і університетами.*

**Незважаючи на значні зусилля, які докладає уряд в галузі досліджень, більшість інновацій та інвестицій в цій галузі реалізуються приватним сектором.** Інноваційні центри в сфері кібер-безпеки 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, анти-спам програми, і ПО з протидії зломів мереж. Всього інвестиції в ІКТ в США склали 133 млрд доларів, або 41 % від загального обсягу інвестицій в дослідження в країні, який склав 323 млрд доларів станом на 2013 р Станом

[19] Advanced Cyber Security Center // https://www.acscenter.org/

на той же рік, за оцінками фахівців, ІКТ-сектор становив лише 4,6 % від всієї економіки США, але ця частка зростає приблизно на 1 % щороку в останні два роки[20]. З урахуванням високої залежності економіки США від ІКТ-сектора (в т. ч. Досліджень в 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 прийомі на роботу нових фахівців, а також привести до відкриття офісів Міністерства в Кремнієвій долині і Бостоні.

Практика встановлення ДПП у сфері кібербезпеки демонструє, що незважаючи на те, що ДПП можуть бути вигідними як для приватного сектору так і для уряду, не всі приватні компанії налагоджують таке партнерство. Одним з ключових стримуючих факторів стає 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, тому обмін інформацією не повинен зводитися до односторонніх відносин. Крім того, деякі приватні компанії також непокоїть, що передача конфіденційної інформації може зашкодити їхній репутації або що передана інформація не буде повністю конфіденційною.

## ВИСНОВКИ

1. Одним з ключових інструментів захисту кіберпростору США сьогодні все активніше стає партнерство між урядом та приватними компаніями. Взаємні інтереси та взаємозв’язки у кіберсфері сприяють налагодженню активної співпраці та виробленню нових методів протидії кіберзагрозам. Захищений кіберпростір дозволяє вільно та безпечно

[20] Киберготовность США 2.0 // https://digital.report/kibergotovnost-ssha-2-0-vvedenie/

здійснювати свою діяльність як уряду, так і приватним установам, що має важливе значення для збереження стійкості і надійності державної інфраструктури та ключових ресурсів, а також для економічної та національної безпеки.

2. Одним з основних напрямків взаємодії стає взаємний обмін інформацією про кіберзагрози між урядом та приватним сектором, що знайшли своє втілення в законодавчих та інституційних ініціативах. Зокрема, питанню спільного захисту кіберпростору були присвячені наступні документи: Директива про рішення Президента № 63 «Про захист критичної інфраструктури» 1998 року, План з регулювання у сфері кібербезпеки, Міжнародна стратегія для кіберпростору, Виконавчий указ № 13636 «Про підвищення кібербезпеки в сфері критичної інфраструктури», Виконавчий указ № 13691 «Про обмін інформацією з кібербезпеки в приватному секторі» тощо. В практичній площині своє втілення знайшли, зокрема, Центр захисту державної інфраструктури в межах ФБР (NIPC), Центр з обміну та аналізу інформації (ISAC), Національний центр кібербезпеки і інтегрованих комунікацій (NCCIC), організації з обміну та аналізу інформації (ISAOs).

3. Водночас така співпраця виявила як переваги так і недоліки такої взаємодії. З одного боку, ДПП у сфері кіберпростору допомогла відкрити та розслідувати безліч кримінальних та цивільних злочинів, сприяла у попередження кібератак, а також створенні нових методів попередження та протидії кіберзагрозам. З іншого – така взаємодія все далі викликає все більше занепокоєння з боку представників приватних компаній через однонаправленість інформаційного обміну, надмірну закритість державних органів, що викликає сумніви у питанні доцільності такої співпраці.

## РЕКОМЕНДАЦІЇ

*Державній службі спеціального зв'язку та захисту інформації*

1. При розробці 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 розробки практичних механізмів залучення фізичних та юридичних осіб до кіберзахисту державних інформаційних державних електронних інформаційних ресурсів в рамках програм державно-приватного партнерства, в т.ч. – використовуючи досвід ISAC або ISAO.

2. 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 в якості консультантів при її створенні фахівців Міністерства внутрішньої безпеки США, які відповідають за підтримку та реалізацію CISCP.

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

4. Задіяти механізм регулярного діалогу між приватними компаніями та урядом (семінари, форуми, тренінги) задля просування та реалізації ініціатив державно-приватного партнерства у кіберпросторі. Одним з 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.

5. 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 в частині питань, які пов'язані з кібербезпекою.

6. Актуалізувати питання підготовки «Огляду сектору кібербезпеки» із залученням всіх зацікавлених сторін, що має охарактеризувати поточний стан кібербезпекової сфери України, її ресурсного потенціалу та шляхів оптимізації спроможностей кібербезпекового сектору.

*Службі безпеки України*

7. Розглянути можливість включення тематики ДПП до програм, що реалізуються у межах Трастового фонду Україна - НАТО з питань кібербезпеки.

*Міністерству закордонних справ України*

8. З метою залучення досвіду міжнародних партнерів в частині розробки нових механізмів ДПП 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 ДПП в сфері кібербезпеки.

*Т.О.Ісакова*
Відділ інформаційної безпеки
та розвитку інформаційного суспільства