АКТУАЛЬНІ ПИТАННЯ РОЗВИТКУ ДЕРЖАВНО-ПРИВАТНОЇ ВЗАЄМОДІЇ У СФЕРІ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ

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

Критична потреба в розвитку державно-приватної взаємодії в галузі кібербезпеки обумовлена в сучасному світі низкою причин, серед яких експерти називають насамперед такі:

- активна приватизація деяких секторів критичної інфраструктури (що є не лише українським, але й глобальним трендом), внаслідок якої державні органи не можуть самостійно гарантувати повноту захисту критичної інформаційної інфраструктури;

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

- накопичення великої кількості електронних інформаційних ресурсів, які мають важливе значення для діяльності як приватних власників, так і органів державного управління;
- залежність інфраструктури від інформаційно-телекомунікаційних систем та їхньої вразливості;
- зростаюча конвергенція комп'ютерних мереж, внаслідок чого ураження однієї з інформаційно-комунікаційних систем може суттєво позначитися на функціонуванні інших;
- у підприємств малого та середнього бізнесу зазвичай бракує повноважень і ресурсів для повноцінного захисту власної інформаційної інфраструктури, тому вони зацікавлені в отриманні відповідних послуг від державних органів та/або від крупних корпорацій.[1]

Саме тому **різні форми державно-приватного партнерства розглядаються нині як один з основних інструментів побудови ефективних систем кіберзахисту і широко застосовуються в міжнародній практиці**. «В ідеалі» це дозволяє поєднати у формуванні національної системи кібербезпеки розмаїття ресурсів приватного (суспільного) сектору з системністю методичного державного регулювання кібербезпеки.

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

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

І в Законі, і в Стратегії затверджується, що державно-приватна взаємодія є одним із принципів забезпечення кібербезпеки в Україні, а також одним зі шляхів функціонування національної системи кібербезпеки, зокрема за допомогою «обміну інформацією про інциденти кібербезпеки, реалізації спільних наукових та дослідницьких проектів, навчання та підвищення кваліфікації кадрів у цій сфері». Стаття 10 «Державно-приватна взаємодія у сфері кібербезпеки» визначає основні напрями та види діяльності, де доцільним є вдаватися до ДПВ у сфері кібербезпеки.[2]

Як у цих базових документах, так й у відповідних підзаконних актах держава незмінно декларує готовність до системної роботи довкола розвитку державно-приватної взаємодії (ДПВ) у сфері забезпечення кібербезпеки. Так, у розпорядженні Кабінету Міністрів України від 10 березня 2017 р. № 155-р «Про затвердження плану заходів на 2017 рік з реалізації Стратегії кібербезпеки України» в якості одного з пріоритетних напрямів дій також визначене «формування стратегічних напрямів державно-приватної взаємодії у сфері кібербезпеки та пріоритетів, на які спрямовуються спільні зусилля для протидії кіберзагрозам».[3]

Зауваження щодо необхідності «розробити та запровадити механізми державно-приватного партнерства для управління кіберзахистом критичної інформаційної інфраструктури у запобіганні кіберзагрозам та в умовах кризових ситуацій, надзвичайного стану в особливий період» міститься також у рекомендаціях Парламентських слухань «Реформи галузі інформаційно-комунікаційних технологій та розвиток інформаційного простору України», що відбулися у лютому 2016 року.[4]

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

---

[2] http://w1.c1.rada.gov.ua/pls/zweb2/webproc34?id=&pf3511=55657&pf35401=429339; http://www.president.gov.ua/documents/962016-19836

[3] http://www.kmu.gov.ua/control/uk/cardnpd?docid=249807504

[4] http://zakon3.rada.gov.ua/laws/show/1073-19

- відповідні **нормативні положення сформульовані дуже широко, при цьому спостерігається гострий дефіцит пов'язаних підзаконних актів**, спрямованих на розвиток і конкретизацію даних положень[*]. Насамперед, це стосується галузевого регулювання захисту об'єктів кібербезпеки (з урахуванням специфіки різних секторів економіки), унормування інституту незалежних аудиторів і, зрештою, визначення правового змісту самого поняття «державно-приватна взаємодія»;

- суперечливими є норми, що визначають **порядок впровадження аудиту інформаційної безпеки на об'єктах НКІІ, встановлюють вимоги до аудиторів інформаційної безпеки і визначають порядок їх атестації**.[*] Оскільки значуща частина таких об'єктів вочевидь знаходиться у недержавній власності, є вагомі підстави вважати, що визначені законодавством регулятивно-наглядові повноваження державних суб'єктів у цій галузі є надмірними і об'єктивно створюють передумови для зловживань, тиску на недержавний сектор (передусім, бізнес) і створення корупційних схем. Наприклад, Державна служба спеціального зв'язку та захисту інформації України, згідно з цими нормами, визначальною мірою контролює створення та діяльність інституту аудиторів (включаючи незалежних), формування вимог до проведення аудиторських перевірок і сертифікації об'єктів критичної інфраструктури, а Служба безпеки України має право негласно перевіряти готовність таких об'єктів до можливих кібератак та кіберінцидентів;

- Законом «Про основні засади забезпечення кібербезпеки України» встановлено, що порядок та методика здійснення аудиту кібербезпеки здійснюється на основі міжнародних стандартів, проте в його прикінцевих та перехідних положеннях немає жодної згадки про чинний Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», згідно зі статтею 7 якого «державні інформаційні ресурси або інформація з

[*] Станом на жовтень 2017 року.

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

обмеженим доступом, вимога щодо захисту якої встановлена законом, повинні оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю». Очевидно, що під дію цієї норми потрапляють практично всі об'єкти критичної інформаційної інфраструктури, значна кількість яких знаходиться в недержавному секторі (наприклад, в енергетиці, транспортній системі, телеком-індустрії, фармацевтиці тощо). Поряд із цим і сама **Комплексна система захисту інформації (КСЗІ), базована на українському стандарті КСЗІ НД ТЗІ 2.5-004-99, і вимога її обов'язкового застосування на об'єктах НКІІ здебільшого піддається гострій критиці у вітчизняних експертних та бізнесових колах**.[5]

Питання стандартизації у сфері кібербезпеки та захисту інформації є предметом постійних дискусій між вітчизняною професійною спільнотою і профільними державними органами. На даний момент в Україні в якості єдиного (крім банківського сектору) державного стандарту технічного захисту інформації діє серія нормативних документів, центральним з яких є НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу»[6]. Стандарт розроблений на основі т. зв. Канадських критеріїв безпеки комп'ютерних систем (*Canadian Trusted Computer Product Evaluation Criteria (CTCPEC)*)[*], а також з урахуванням прийнятого у 2005 році міжнародних «Загальних критеріїв» (*Common Criteria for Information Technology Security Evaluation* (ISO 15408)[*]. На відміну від найпоширенішої у світі серії ISO/IEC 27000, яка сфокусована на менеджменті інформаційної безпеки, критерієм захищеності інформації в НД ТЗІ 2.5-004-

[5] http://uz.ligazakon.ua/ua/magazine_article/EA010553; https://ain.ua/2017/06/10/kiberbezpeka-v-nebezpeci; http://infosafe.ua/article-6; http://ko.com.ua/kiberbezopasnost_v_ukraine_diskussiya_121089;

[6] http://web.archive.org/web/20121202025850/http://am-soft.ua/files/KSZI/2.5-004-99.pdf ; http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=89740&cat_id=89734

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

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

99 є відповідність архітектури та параметрів програмно-апаратних засобів об’єкта чіткому регламенту – комплексній системі захисту інформації (КСЗІ). **З точки зору фахівців, сама ідея, внутрішня структура і модель впровадження КСЗІ здебільшого не відповідає вимогам сучасного кіберзахисту, особливо в недержавному секторі**. Зазвичай експерти вказують на такі її недоліки:

- *недостатня гнучкість.* Концепція КСЗІ вимагає ретельного документування архітектури та всіх налаштувань системи захисту інформації, а при внесенні будь-яких змін – складного й бюрократизованого процесу переатестації (до кількох місяців). Досить очевидно, що така статична модель захисту мало корелює з динамікою та розмаїттям бізнес-процесів, та й взагалі є не зовсім неадекватною викликам сучасного кіберпростору;
- *громіздкість.* Підходи НДТЗІ, що вимагають створення великої кількості документації, є занадто громіздкими для приватного бізнесу;
- *обмежені можливості масштабування.* КСЗІ/НДТЗІ не підходять для великих організацій/підприємств, наприклад, для заводів, де можуть використовуватися великі розподілені системи спостереження та керування промисловими процесами (наприклад, SCADA/АСК ТП[7]);[8]
- *застаріла концепція захисту/захищеності.* Модель КСЗІ/НДТЗІ орієнтована на захист інформації в інформаційно-комунікаційній (комп’ютерній) системі як такій, без урахування конкретних безпекових потреб об’єкту кіберзахисту в цілому. Як свідчить міжнародний досвід, у сучасних умовах значно більший ефект дає проактивний, т. зв. ризик-орієнтований підхід, який передбачає моніторинг, імовірнісний аналіз та оцінювання ризиків (за шкалою – від прийнятних до неприпустимих) суб'єкта господарювання у певній екосистемі з метою дотримання кібербезпеки шляхом управління цими ризиками.

[7] https://goo.gl/p1V2tU
[8] https://ain.ua/2017/06/10/kiberbezpeka-v-nebezpeci

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

По-перше, це **серія міжнародних стандартів ISO/IEC 27000**[9], розроблена Міжнародною організацією з стандартизації (ISO) спільно з Міжнародною електротехнічною комісією (IEC), яка постійно доповнюється новими документами. Серія, по суті, являє собою модель (фреймворк) для розробки, впровадження, функціонування, моніторингу, аналізу, підтримки та поліпшення системи менеджменту інформаційної безпеки як на загальному рівні (27001), так і в окремих секторах та галузях – фінанси, транспорт, енергетика, охорона здоров'я, оператори зв'язку, хмарні обчислення, інфраструктурні проекти, аудит і сертифікація тощо.

Впровадження системи управління інформаційною безпекою (СУІБ) відповідно до ISO/IEC 27000 дозволяє оптимізувати процес захисту інформаційних ресурсів і управління ризиками для цих ресурсів. У нашій країні статус державного стандарту отримала перша версія ISO/IEC 27001 (найновішою є ISO/IEC 27001:2013), проте де-факто імплементований він лише в банківській сфері – у вигляді вимог СОУ Н НБУ 65.1 СУІБ 1.0: 2010[10] (згідно з законом «Про основні засади забезпечення кібербезпеки України» Національний банк України є одним з суб'єктів національної системи кібербезпеки). Практичне застосування ISO/IEC 27001 в інших галузях української економіки та бізнесу поки залишається відкритим через нормативно-правову неврегульованість.

[9] https://www.iso.org/isoiec-27001-information-security.html
[10] https://kyianyn.files.wordpress.com/2010/12/nbu-27001.pdf

Одним із найбільш авторитетних і відомих у світі є також ***National Institute of Standarts and Technology Cybersecurity Framework (NIST CSF)***[11] – розроблений американським Інститутом стандартів і технологій для організацій приватного сектору США комплекс методологій та рекомендацій щодо зниження ІТ-ризиків, запобігання, моніторингу і реагування на кібератаки. Фреймворк є відкритим, призначений виключно для добровільного використання і є достатньо «гнучким» для адаптації в різних умовах/країнах, що зумовило його поширеність у світі. Уперше *NIST CSF* був випущений у 2014 році, у поточному році винесений на обговорення проект (*draft version*) версії 1.1.[12]

Треба відзначити, що **нормальною світовою практикою є розробка і застосування у разі необхідності альтернативних або призначених для тих чи інших секторів недержавного сектора стандартів та фреймворків з кібербезпеки**. Серед іншого, **це дозволяє уникати надмірної регуляторної монополізації, недоброчесної конкуренції й корупції, що є нині особливо актуальним для України.** Наприклад, хоча близько 70 % приватних організацій у США сьогодні віддають перевагу *NIST Cybersecurity Framework*[13], в американському енергетичному секторі діють стандарти *NERC CIP*[14], розроблені Північноамериканською корпорацією з забезпечення надійності електросистем (*North American Electric Reliability Corporation*), яка, до речі, є неприбутковою недержавною організацією. Варто наголосити, що саме ці стандарти рекомендують запровадити в українському ПЕК експерти київського відділення ISACA.

Довідково: ***ISACA*** *– міжнародна професійна неприбуткова асоціація, орієнтована на ІТ-менеджмент. Об'єднує фахівців в області ІТ-аудиту, ІТ-консалтингу, управління ІТ-ризиками та інформаційною безпекою. Основним завданням асоціації є розробка і формалізація єдиних ефективних підходів до оцінки та управління ІТ-процесами та ІТ-системами. (Докладніше див. http://www.isaca.org.ua/) У листопаді 2014 року Адміністрація Державної служби спеціального зв'язку та захисту інформації України та*

[11] https://www.nist.gov/cyberframework
[12] https://www.nist.gov/cyberframework/draft-version-11
[13] "NIST Cybersecurity Framework Adoption Hampered By Costs, Survey Finds". Information Week Dark Reading. Retrieved 2016-08-02.
[14] http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

київське відділення ISACA уклали меморандум про співробітництво у сфері кібербезпеки та інформаційних технологій. У галузі аудиту і стандартизації IT організація має низку напрацювань і розробок, які становлять безсумнівний інтерес з точки зору зміцнення національної системи кібернетичної безпеки. Зокрема:

CobiT *(акронім англ. Control Objectives for Information and Related Technology («Контрольні цілі для інформаційних та суміжних технологій») – відкритий міжнародний IT-стандарт, який, у свою чергу, містить низку документів зі стандартами щодо оптимізації управління IT: аудитом IT та IT-безпекою. Створено Асоціацією з аудиту та контролю інформаційних система (ISACA) спільно із Інститутом управлінням IT (IT Governance Institute – ITGI). Перше видання – 1996 рік. У 2012 році відбувся реліз поточної версії – CobiT 5.*[15]

ITAF *– (Information Technology Assurance Framework) – еталонна модель використання кращих практик, до якої можуть звертатися фахівці з аудиту та підтвердження довіри до інформаційних систем (ІС) за настановами, для дослідження політик і процедур, отримання програм аудиту та підтвердження довіри, а також формування ефективних звітів.*[16]

Такі рекомендації зустрічають розуміння в українському бізнесі. Так, саме згідно з *NERC CIP* (у комплексі зі стандартами *NIST 800-SERIES, IEC 62443* та *ISO 27000*) побудований та сертифікований захист критичної IT-інфраструктури в ТОВ ДТЕК Енерго. Крім того, самим Міністерством енергетики та вугільної промисловості України зміцнення кібербезпеки українського паливно-енергетичного комплексу також мислиться як створення комплексної галузевої системи кібербезпеки, причому з орієнтацією саме на кращі міжнародні норми та практики.[17] У «Типовому положенні про інформаційну безпеку підприємств ПЕК», розміщеному на офіційному веб-порталі міністерства, міститься положення щодо «реалізації вимог міжнародних стандартів з інформаційної безпеки *ISO 27000-series, ISA 099-series* та *IEC 62443*».[18] Останні два – спеціалізовані відкриті стандарти, оптимізовані в тому числі для застосування на об'єктах критичної інфраструктури приватної форми власності. Таким чином, можна говорити про те, що в українському ПЕК вже зараз триває формування єдиного пакету галузевих стандартів з інформаційної безпеки.

На отримання міжнародної сертифікації в галузі інформаційної безпеки орієнтовані в Україні також й інші приватні гравці, у тому числі крупні.

[15] http://www.isaca.org.ua/index.php/standards
[16] Там само.
[17] http://mpe.kmu.gov.ua/minugol/control/publish/article?art_id=245224502
[18] http://195.78.68.67/minugol/doccatalog/document?id=245167627

Наприклад, компанія *De Novo*, найбільший в Україні провайдер хмарових сервісів, яка має сертифікат відповідності вимогам українським стандартам КСЗІ для свого сервісу *G-Cloud* (хмара для органів державної влади), водночас впровадила у середині 2017 року систему управління інформаційною безпекою (СУІБ) і отримала сертифікат відповідності згідно з міжнародним стандартом *ISO 27001*.[19]

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

Здійснення державно-приватного партнерства в Україні регулюється Законом «Про державно-приватне партнерство» (від 1 липня 2010 р. № 2404-VI з останніми змінами та доповненнями від 24.11.2015р.). Згідно з змістом проекти державно-приватного партнерства (ДПП) повинні відповідати таким основним критеріям: 1) мати довготривалий характер (понад 5 років); 2) передбачати передання приватному партнеру частини ризиків у процесі реалізації проектів; 3) мати вищі техніко-економічні показники ефективності, ніж у разі реалізації без участі приватного партнера.

Водночас, хоча базові положення Закону відповідають сучасним європейським правовим нормам та практикам, він, за оцінками експертів, має й певні недоліки. По перше, не встановлено мінімальну частку участі у проекті приватного партнера (зокрема, у розвинених країнах мінімальна частка приватного фінансування складає 25 %). У зв’язку з цим навіть мінімальна частка приватного фінансування у спільному проекті дозволяє відносити його до категорії ДПП, перекладаючи більшу частину відповідальності на державу. По-друге, відсутні чітко визначені механізми практичної реалізації (визначення етапів реалізації проектів ДПП, створення мотивації для іноземних інвесторів тощо). По-третє, залишається не

[19] https://www.de-novo.biz/uk/novini-ta-istoriyi-uspihu/novini/bezpeka-hmarnih-servisiv-de-novo-pidtverdzhena-sertifikatom-iso-27001/

визначеною роль Державного фонду регіонального розвитку у фінансуванні проектів ДПП.[20]

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

Функцію спеціально уповноваженого органу з питань державно-приватного партнерства виконує в Україні Міністерство економічного розвитку і торгівлі України (МЕРТ). Згідно з його даними, протягом 2016 р. в Україні була практично відсутня ДПВ у сфері забезпечення кібербезпеки (договори, укладені в цій галузі, могли відноситися хіба що до тих нерубрикованих 2,9 % угод, що фігурують у таблиці у стовпчику «Інше».)[21] Дані з інших джерел переконливо свідчать, що у 2017 р. ситуація принципово не змінилася, що є закономірним, враховуючи крайню нерозвиненість нормативної бази, а також відсутність відповідної державної галузевої та комунікативної політики. **Нині не лише в українських експертних, бізнесових та управлінських колах, але й у суспільстві широко представлені наративи та рішення щодо інформаційної та кібернетичної**

[20] http://www.niss.gov.ua/articles/1239/
[21] http://www.me.gov.ua/Documents/Detail?lang=uk-UA&id=ed00a2ba-480a-4979-84eb-d610a0827a8c&title=ZagalniiOgliad

безпеки, але вони майже ніколи не асоціюються з ДПВ. Таким чином, на даному етапі для створення платформи державно-приватної взаємодії у сфері кібербезпеки державою прийняті лише базові рамкові нормативні акти, проте не налагоджений діалог з експертними колами та суспільством і не створено жодних інституційно-правових інструментів такої взаємодії.

Разом із цим **як недержавний сектор в Україні, так і державні відомства (поки що – деякі з них) демонструють значний потенціал для формування повноцінної платформи ДПВ у загальнонаціональних масштабах**. Наприклад, саме на засадах державно-приватної взаємодії триває робота над створенням в Україні потужного центру з кібербезпеки на базі ДК «Укроборонпром». Крім представників РНБОУ, Міністерства оборони, СБУ, ДССЗЗІ, Департаменту кіберполіції, фахівців НАТО, консультантів турецької державної компанії *HAVELSAN* та спеціалістів НТУУ «КПІ», у проекті беруть участь громадська неприбуткова організація «Українська академія кібербезпеки»[22] й українська команда «білих» хакерів *DCUA* (одна з найсильніших у світі).[23] Проект державного концерну «Укроборонпром» *Cyber Guard* був реалізований у партнерстві з приватними компаніями для захисту від кібератак приватних і державних установ України.[24]

З кінця 2015 р. в Україні, крім державного *CERT-UA*, діє офіційно акредитований міжнародною мережею *FIRST*[25] приватний центр реагування та боротьби з кіберінцидентами (*computer emergency response team*, або *CERT*). Ідеться про вітчизняну компанію *CyS-Centrum*, яка

[22] http://www.uacs.kiev.ua/; https://youcontrol.com.ua/catalog/company_details/40380087/

[23] https://www.unian.ua/science/1861316-v-ukrajini-za-pidtrimki-nato-stvoryat-ediniy-tsentr-z-kiberbezpeki.html; https://www.ukrinform.ua/rubric-technology/2206034-v-ukraini-stvorat-edinij-centr-kiberbezpeki-dopomozut-bili-hakeri-dcua.html

[24] https://cyberguard.com.ua/

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

спеціалізується на моніторингу й нейтралізації ІБ-загроз з використанням апаратно-програмних рішень власної розробки, а також на консалтингу в сфері інформаційної безпеки.[26]

Ще у квітні 2015 р. МВС України та корпорація «Майкрософт» підписали Меморандум про взаєморозуміння, який засвідчив взаємну зацікавленість у співпраці в галузі захисту даних, інформаційної та кібербезпеки. У листопаді 2017 р. подібний же меморандум, спрямований на організацію взаємодії в побудові комплексних рішень технічного забезпечення відомчої діяльності в масштабах держави, застосування інновацій у сфері держуправління, а також оптимізації наявного ресурсу, був підписаний представниками Національної поліції України та компанії «Майкрософт Україна».[27]

Особливо високу динаміку розвитку ДПВ демонструє Департамент кіберполіції Національної поліції України. Зокрема, з 2016 року налагоджена системна співпраця між відомством і українськими профільними компаніями *ProtectMaster* (protectmaster.org) і *Berezha Security* (berezhasecurity.com), а також з громадською організацією «Експертів кібербезпеки» (залучення фахівців, обмін даними, проведення спільних конференцій, тренінгів для держслужбовців). Департаментом також організовано регулярний обмін інформацією та досвідом з фахівцями з Національного Університету Радіоелектроніки (ХНУРЕ) і Національного аерокосмічного університету ім. М.Є. Жуковського (ХАІ). Крім того, за підрахунками спеціалістів кіберполіції, у декілька разів збільшити ефективність реагування на кіберзагрози дозволило розміщення онлайн-форми зворотного зв'язку на її сайті. [28]

У вересні 2017 р. за сприяння Української Асоціації операторів зв’язку «Телас» було підписано меморандум про співпрацю між Департаментом

[26] https://cys-centrum.com/ru
[27] https://www.npu.gov.ua/uk/publish/article/1422098;
[28] https://cyberpolice.gov.ua/news/kiberpolicziya-vzayemodiye-z-855/; https://protectmaster.org/novosti/101-kompaniya-protectmaster-aktivno-vzaimodeystvuet-s-gosudarstvom.html

кіберполіції й дата-оператором lifecell, за умовами якого останній на безоплатній основі передав Департаменту систему власної розробки для екстреного інформування в умовах надзвичайних ситуацій *Emergency Notification System (ENS)*. Серед іншого, система дає змогу локалізувати кіберзагрозу й уникнути її розповсюдження за допомогою оперативного інформування про небезпеки завчасно визначених груп отримувачів через голосові виклики, SMS та електронні листи. За повідомленнями керівництва, *ENS* вже успішно пройшла тестування й її абонентами можуть стати як державні, так і приватні компанії, включаючи об'єкти критичної інфраструктури.[29]

Одним із найбільш важливих та перспективних напрямів державно-приватної взаємодії у сфері кібербезпеки є освітній напрям – підготовка кваліфікованих кадрів і всіляке поширення серед працівників компаній та пересічних користувачів культури інформаційної та кібернетичної безпеки (запуск загальнонаціональної програми «комп'ютерного лікнепу»).

Відомо, що Україна має значний потенціал у цій галузі. Бакалаврів та магістрів за спеціальністю «Кібербезпека» готують 44 вітчизняних ВНЗ (у тому числі при профільних відомствах – ДССЗЗІ, СБУ, МВС, МО України, розвідувальних органах) й обсяги державного замовлення на цих фахівців останніми роками постійно зростає.[30] Діють та розвиваються також спеціалізовані державні та комерційні центри підвищення кваліфікації та тренінгу. Разом із цим як експерти-освітяни, так і професійна ІТ-спільнота констатують наявність системних проблем у цій сфері. Наприклад, у річному звіті VIII Українського форуму з управління Інтернетом IGF-UA (жовтень 2017 р.) вказується на:

- відсутність належного рівня кваліфікації в підготовці сучасних фахівців з питань кібербезпеки та інформаційної безпеки в закладах освіти;

[29]. https://goo.gl/Ef2ZNH; https://hromadskeradio.org/ru/news/2017/09/26/kiberpoliciya-zaprovadzhuye-v-ukrayini-globalnu-systemu-spovishchennya-pro-zagrozy; https://www.epravda.com.ua/news/2017/09/26/629504/
[30] https://osvita.ua/vnz/guide/search-17-0-0-42-43-0.html

- низькій рівень зарплатні професорсько-викладацького складу в інститутах та фінансування фахівців у державних компаніях;
- застарілу навчальну програму з підготовки фахівців з питань кібербезпеки та інформаційної безпеки;
- відсутність координації в системі освіти між замовниками кадрів та закладами освіти;
- відірваність фахівців з інформаційної та кібербезпеки від міжнародної системи стандартизації;
- брак наукових досліджень з проблем кібербезпеки.[31]

Експертні дослідження свідчать, що в сучасному світі підготовка кадрів із кібербезпеки не може обмежуватися лише отриманням вищої освіти у ВНЗ за відповідною спеціальністю. Для збереження належної конкурентоспроможності та професійного рівня цим фахівцям необхідно перманентно підвищувати свою кваліфікацію на засадах т.зв. концепції безперервної освіти (або «освіти протягом життя»), множинність форм та методів якої відкриває ще один широкий та перспективний напрям для галузевої ДПВ. Можливі декілька варіантів роботи в цьому напрямі, серед яких перепідготовка в рамках післядипломної освіти фахівців у споріднених з кібернетичною безпекою спеціальностей, застосування нелінійної схеми підготовки фахівців, використання потенційних можливостей неформальної освіти для підвищення кваліфікації діючих фахівців через проведення тренінгів, семінарів, міжнародних стажувань тощо.[32]

Критично важливим є також забезпечення належного рівня обізнаності персоналу компаній та установ в питаннях кібернетичної та інформаційної безпеки, – знову ж таки спільними зусиллями приватних та державних суб'єктів. Форми ДПВ тут можуть бути різноманітними: спільні семінари, тренінги, онлайн-курси, залучення науково-аналітичних та консалтингових

[31] http://igf-ua.org/wp-content/uploads/2017/11/Ukrainian-IGF-UA_2017_Annual_Report_UKR.docx
[32] http://pgp-journal.kiev.ua/archive/2017/3/45.pdf; http://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/szi_2016_2_3.pdf
http://inau.ua/doc/6/all

компаній всіх форм власності та багато іншого. Крім того, необхідними є регулярні тестування (навчання) на проникнення, моделювання загроз, грамотність поведінки працівників/користувачів в мережі (дотримання елементарних правил онлайн-безпеки, стійкість до спроб фішингу тощо).

Статтею 10 чинного закону «Про основні засади забезпечення кібербезпеки України» «створення системи підготовки кадрів» та «підвищення цифрової грамотності громадян» визначено як один із напрямів ДПВ у сфері кібербезпеки. Поряд із цим значною мірою невирішеним залишається питання інституційно-правового забезпечення повноцінної реалізації даної норми.

Вкрай важливим є постійний та системний обмін даними щодо актуальних кіберзагроз і можливостей (інструментів) боротьби з ними. Для цього оптимальним було б **створення та підтримка на основі широкої ДПВ національної системами обміну даними про кіберінциденти та їх реєстр.** Це дозволило б підрозділам з ІТ-безпеки компаній та установ перевіряти маркери компрометації, відслідковувати, кому ще розсилалися аналогічні зразки шкідливого програмного забезпечення, обмінюватися індикаторами атак, убезпечуючи таким чином свої об’єкти від кіберзлочинців.[33]

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

[33] http://yur-gazeta.com/publications/practice/inshe/sybercrime-sistemi-zahistu-naroshchuyut-myazi.html

(бюрократичних) та комерційних організаціях, а також недостатня інтероперабельність їх інформаційних інфраструктур.[34]

З іншого боку, **в міжнародній практиці для обміну інформацією про атаки та загрози, розслідувань кібератак, експертної підтримки тощо широко та успішно практикується ДПВ з галузевими асоціаціями й приватними компаніями, що спеціалізуються на ІБ-рішеннях**.[35] Вітчизняний потенціал і чинне законодавство (статті 7 та 10 закону «Про основні засади забезпечення кібербезпеки України») цілком дозволяють налагодити в Україні ДПВ на цьому напрямі, ба-більше, існують окремі приклади її успішної реалізації (див. вище). Водночас для того, щоб така взаємодія набула в нашій країні системного загальнонаціонального характеру, потрібні інституційні важелі (наприклад, у вигляді організованих державою постійно діючих платформ для комунікації й налагодження співробітництва) та відповідний нормативно-правовий інструментарій для її стимулювання/регулювання і юридичного оформлення. Нині все це повноцінно не реалізоване.

З точки зору українських фахівців[36], які спеціально досліджували світовий досвід державно-приватної взаємодії у забезпеченні кібербезпеки, найдоцільніше організовувати її на таких принципах і засадах:

- формування відносин довіри між державними суб'єктами (регуляторами) кібербезпеки і керівництвом приватних підприємств;
- створення умов, за яких приватні об'єкти кіберзахисту добровільно приводитимуть свої програми управління ризиками у відповідність до вимог регулятора (галузевих регуляторів) та надаватимуть всю необхідну інформацію в інтересах захисту критичної інфраструктури;

---

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

[35] http://www.isaca.org.ua/index.php/press-center/events/176-poperedni-propozytsii-ho-isaka-kyiv-shchodo-pokrashchennia-zakonu-pro-osnovni-zasady-zabezpechennia-kiberbezpeky-ukrainy; http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article;jsessionid=346CC9B7A46A60C4647388BCBDF134B3.app1?art_id=166495&cat_id=97586

[36] Там само.

- постійне врахування галузевої специфіки процесів інформатизації та дотримання кібербезпеки у різних секторах економіки, запровадження інституту галузевих регуляторів;
- основними контактними (координуючими) суб'єктами захисту критичної інфраструктури повинні бути тільки державні установи;
- діяльність державних структур унормована (суворо регламентована) у стосунках з приватним сектором – у розвитку ДПВ належить використовувати інструментарій пільг і привілеїв;
- створення співтовариств для обміну інформацією (наприклад, на основі концепції *Information Exchange Model*, як це реалізовано у Великій Британії[37]);
- організація CERT у різних галузях і на різних рівнях;
- розробка та розвиток у рамках ДПВ спільних автоматизованих систем моніторингу кібератак (на кшталт польської системи *ARAKIS-GOV*[38]).

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

ВИСНОВКИ

1. Широке **застосування державно-приватного партнерства у побудові національних систем кібербезпеки є сталим глобальним трендом**, ефективність якого підтверджена міжнародною практикою. Тому без розгалуженої, інтегрованої у міжнародні кібербезпекові структури, проактивної й оптимізованої для повноцінної участі всіх стейкхолдерів системи ДПВ у сфері кібербезпеки неможливим є створення в Україні: 1) ефективної системи національної безпеки; 2) сучасної цифрової економіки, базованої на перспективних інноваційних технологіях (що вже сьогодні є

[37] Там само. С. 58-59.
[38] http://www.cert.gov.pl/cee/arakis-gov-system/78,ARAKIS-GOV-system.html

критично важливим для конкурентного розвитку нашої держави); 3) створення передумов для сталого суспільного і людського розвитку в середньо- та довгостроковій перспективі.

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

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

3. Як недержавний сектор в Україні, так і державні відомства подекуди демонструють **значний потенціал для створення загальнонаціональної системи державно-приватної взаємодії у сфері кібербезпеки**. Поряд із цим станом на осінь 2017 р. **в Україні триває формування лише окремих її елементів, сама ж система як така поки відсутня**.

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

У зв’язку з викладеним вище **пропонується:**

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

2. Кабінету Міністрів України спільно з іншими суб’єктами забезпечення кібербезпеки, МЕРТ, МІП, ПАТ «НСТУ» та із залученням інших національних мовників – розглянути питання налагодження **широкого експертного та громадського обговорення створення платформи**

державно-приватної взаємодії у сфері кібербезпеки (підзаконні акти, єдині та галузеві нормативні вимоги інформаційної безпеки, формування реєстру об'єктів НКІІ, стандартизація, сертифікація, аудит, технічне забезпечення, інтероперабельність систем тощо). Забезпечити належну публічність і достатній медіа-супровід цього обговорення: онлайн-майданчик(и), веб-трансляції, підготовку відповідних телепрограм та інших форм ТБ-промоушена. Оприлюднити результати обговорення.

3. Кабінету Міністрів України, суб'єктам національної системи кібербезпеки – базуючись на результатах означеного обговорення, нормах чинного законодавства та верифікованих експертних даних, **розробити:**

1) єдині критерії та процедури віднесення об'єктів до національної критичної інформаційної інфраструктури;

2) обов'язкові *загальні* вимоги до інформаційної безпеки об'єктів НКІІ, у тому числі під час їх створення, введення в експлуатацію, експлуатації та модернізації з урахуванням міжнародних стандартів. Визначити відповідно до вимог Закону України «Про основні засади забезпечення кібербезпеки України» суб'єктів забезпечення кібербезпеки у галузях та/або окремих об'єктах і зобов'язати їх **розробити обов'язкові *галузеві* вимоги (стандарти) інформаційної безпеки об'єктів НКІІ** з урахуванням локальної специфіки.

4. Суб'єктам забезпечення кібербезпеки в Україні (відповідно до меж їх компетенції) спільно з Міністерством економічного розвитку і торгівлі – розробити **Концепцію організації державно-приватної взаємодії у сфері забезпечення кібербезпеки** з визначенням:

- нормативно-правових актів, в яких затверджено загальні (спільні для всіх), а також галузеві вимоги до здійснення ДПВ;
- стейкхолдерів ДПВ (можливо – у вигляді відповідного реєстру-додатку);
- методології оцінки ризиків (на основі міжнародних стандартів та практик);

- типових моделей-проектів ДПВ з визначенням правових, інституційних, інвестиційних та інших механізмів їх реалізації;
- порядку сертифікації аудиторів та проведення аудиту (з посиланням на відповідні нормативно-правові акти);
- механізму налагодження безперервного багатостороннього обміну відповідною інформацією між усіма учасниками ДПВ;
- джерел та механізмів стимулювання ДПВ;
- шляхів і механізмів підтримки досліджень та розробок (ДіР), а також підготовки проектів концептуальних документів у сфері кібербезпеки в рамках ДПВ;
- порядку проведення навчань, тренінгів тощо.

5. Означену Концепцію доцільно ввести в дію Постановою Кабінету Міністрів України в рамках заходів по реалізації положень Закону України «Про основні засади забезпечення кібербезпеки України», прийнятого Верховною Радою України 5.10.2017р.

6. ДССЗЗІ України та іншим суб'єктами національної системи кібербезпеки – розглянути питання інституційного, ресурсного і нормативно-правового забезпечення **подальшого розширення ДПВ з галузевими асоціаціями та іншими недержавними акторами в галузі обміну інформації про кіберінциденти**, експертного та технічного співробітництва, у запобіганні та розслідуваннях кібератак (у контексті створення загальнонаціональної системи обміну даними про кіберінциденти).

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

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

С.Л. Гнатюк
відділ інформаційної безпеки та розвитку інформаційного суспільства