Юлія КРИХТІНА
доктор наук з державного управління,
доцент кафедри менеджменту, публічного управління
та HR-технологій УкрДУЗТ,
м. Харків
Владлен ТОРОПОВ
здобувач вищої освіти ОС «Магістр»
спеціальності «Публічне управління та адміністрування»
УкрДУЗТ,
м. Харків

ДЕРЖАВНО-ПРИВАТНЕ ПАРТНЕРСТВО В КОНТЕКСТІ ЗАБЕЗПЕЧЕННЯ СТРАТЕГІЇ КІБЕРБЕЗПЕКИ УКРАЇНИ

Державно-приватне партнерство (ДПП) у сфері кібербезпеки - це співпраця державних органів і приватних компаній з метою забезпечення безпеки інформаційної інфраструктури країни від кіберзагроз.

У рамках ДПП держава може надавати підтримку приватним компаніям в формі фінансової допомоги, спільних досліджень, обміну інформацією про кіберзагрози та технічне сприяння у випадку кібератак. Приватні компанії, зі свого боку, можуть надавати свої знання та досвід в сфері кібербезпеки, використовувати нові технології та інструменти для покращення безпеки інформаційної інфраструктури країни, а також надавати державним органам доступ до своїх інформаційних ресурсів для моніторингу кіберзагроз.

ДПП у сфері кібербезпеки є важливим елементом національної безпеки, оскільки дозволяє забезпечити ефективний захист від кіберзагроз, збільшити кількість ресурсів, використовуваних для боротьби з кіберзлочинністю та забезпечити ефективний відповідь на кібератаки.

Європейське агентство безпеки мереж та інформації (ENISA) визнає, що кібербезпека є критично важливою для економіки та суспільства в цілому. Це означає, що кібербезпека повинна бути в центрі уваги держав, приватних компаній та громадян. Проте для ефективного розвитку кібербезпеки в ЄС потрібне державно-приватне партнерство.

ENISA вказує на те, що у держави є великий обсяг ресурсів та доступ до важливої інформації, які можуть допомогти у запобіганні кібератакам та розробці відповідних стратегій кібербезпеки. З іншого боку, приватні компанії мають доступ до великої кількості технологій та експертизи, які можуть допомогти у захисті від кіберзагроз та покращенні кібербезпеки.

Отже, державно-приватне партнерство дозволяє об'єднати ресурси та експертизу, щоб ефективно боротися з кіберзагрозами та підвищити рівень кібербезпеки в ЄС. Це також дозволить створити кращу координацію та співпрацю між державними органами, приватним сектором та громадськістю.

ENISA наголошує на необхідності створення сприятливого середовища для державно-приватного партнерства, зокрема шляхом сприяння обміну інформацією та знаннями, забезпечення фінансової підтримки та стимулювання інновацій. Напрямки можливого ДПП визначаються такі: оброблення інцидентів та управління кризами; дослідження та аналіз; розробка передової практики та рекомендацій; обмін інформацією; ранні попередження; в навчання; підвищення рівня обізнаності; технічна оцінка; визначення стандартів; довідкова служба; управління кризовими ситуаціями; планування стійкості; планування надзвичайних ситуацій; аудит безпеки; стратегічне планування; аналіз ризиків.

У зв’язку з цим ENISA надає такі рекомендації щодо поліпшення державно-приватного партнерства [2]:

1) мотивація приватного сектору для участі повинна бути пріоритетним завданням при формуванні ДПП, для успішної та ефективної якого необхідні ресурси;

2) учасники повинні погодитися з правовими основами при створенні ДПП. Поки немає юридичної бази для співпраці, весь процес створення та розвитку ДПП буде повільним і неефективним. Правовою основою може бути національний правовий акт або Меморандум про взаєморозуміння, оскільки кібербезпека - це міжгоризонтальна сфера, в якій, як правило, багато державних структур залучаються разом з різними приватними компаніями;

3) державні установи повинні керувати ДПП або національним планом дій щодо ДПП для усунення розбіжностей між ключовими державними установами: Міністерство внутрішніх справ, Міністерство оборони, Міністерство економіки та розвитку. Державні установи, які беруть участь у ДПП, повинні знати заздалегідь чого вони хочуть досягти, що сприятиме їхньому внеску та що приватний сектор повинен сприяти;

4) ДПП зобов'язані інвестувати у внутрішнє приватне та приватне співробітництво та державно-державне співробітництво ДПП - це співпраця приватно-приватного, публічно-державного та приватно-публічного. Правильний рівень діалогу та взаєморозуміння між державними установами часто є запорукою успішного ДПП. Те саме стосується приватного сектору. Успішне ДПП інтегрує не лише приватну адміністрацію та галузь, але й різні суб'єкти господарювання (наприклад, енергетичні компанії, банки, телекомунікації);

5) учасники ДПП повинні інвестувати у відкриту комунікацію та прагматичний підхід до побудови ДПП;

6) представникам уряду слід дозволити брати участь у засіданнях за угодою про нерозголошення;

7) малі та середні підприємства (МСП) також повинні брати участь у ДПП.

Таким чином, можна зробити висновок, що державно-приватне партнерство щодо кібербезпеки є складовим елементом Стратегії кібербезпеки України, та може бути реалізовано в напрямках самого широкого спектра: від взаємодії в нормативному регулюванні до навчання і спільного планування заходів із забезпечення стійкості щодо кіберінцидентів.

Стратегія кібербезпеки України [4] базується на законі "Про основні засади забезпечення кібербезпеки України" [5]. Стратегія кібербезпеки України одним із принципів забезпечення кібербезпеки України визначає державно-приватне партнерство, широку співпрацю з громадянським суспільством у сфері забезпечення кібербезпеки та кіберзахисту. Головною метою стратегії є

забезпечення надійності, стійкості та безпеки інформаційно-телекомунікаційних систем (ІТС) та захист національних інтересів України у кіберпросторі.

Основні напрямки стратегії кібербезпеки України:

1. Створення національної системи кібербезпеки, яка має забезпечувати взаємодію всіх зацікавлених сторін в області кібербезпеки та виконувати координаційні функції.

2. Забезпечення стійкості та безпеки ІТС України за допомогою запобігання, виявлення та реагування на кібератаки та інші загрози в кіберпросторі.

3. Розвиток кваліфікації кадрів в області кібербезпеки та створення умов для залучення та збереження кваліфікованих фахівців.

4. Розвиток національного законодавства у галузі кібербезпеки та участь у міжнародних ініціативах у цій області.

5. Розвиток інформаційної культури в суспільстві та підвищення обізнаності громадян щодо кібербезпеки.

6. Забезпечення захисту інформації, що становить державну та комерційну таємницю, та відповідальне використання персональних даних громадян.

7. Розробка та впровадження нових технологій захисту інформації та протидії кіберзагрозам.

Список використаних джерел

1. Про державно-приватне партнерство: Закон України від 01.07.2010 р. № 2404-VI. URL: https://zakon.rada.gov.ua/laws/show/2404-17.

2. Public Private Partnerships (PPP) - Cooperative models. URL:: https://www.enisa.europa.eu/ publications/public-private-partnerships-ppp-cooperative-models.

3. Основи кіберпростору, кібербезпеки та кіберзахисту : навч. посіб. Київ : Ліра-К, 2020. 554 с.

4. Рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#n7.

5. Закон України «Про основні засади забезпечення кібербезпеки України» (2017). Retrieved from: https://zakon.rada.gov.ua/laws/show/2163-19#Text