УДК 351.865

Є. В. Котух,
к. т. н., доцент кафедри комп'ютерних наук, Сумський державний університет, м. Суми
ORCID ID: 0000-0003-4997-620X

DOI: 10.32702/2306-6814.2021.13—14.58

РОЗВИТОК ПУБЛІЧНО-ПРИВАТНОГО ПАРТНЕРСТВА У СФЕРІ КІБЕРБЕЗПЕКИ

Ye. Kotukh,
PhD in Technical Sciences, Associate Professor of the Department of Computer Science, Sumy State University, Sumy

DEVELOPMENT OF PUBLIC-PRIVATE PARTNERSHIP IN THE FIELD OF CYBERSECURITY

Визначено, що для публічно-приватних партнерств, орієнтованих на кібербезпеку, саме ступінь спільних наслідків пов'язує його учасників. Таке призначення зумовлює для публічного сектора необхідність визначити кібербезпеку приватних організацій як проблему національної безпеки, а отже, визнати відповідальність уряду за її забезпечення. Приватний сектор у свою чергу створює, управляє та підтримує системи, технології та процеси, що складають критичну інфраструктуру, забезпечення кібербезпеки якої є складовою забезпечення національної безпеки. Доведено, що загрози в кіберпросторі вимірюються двома факторами: вони повинні мати намір заподіяти певної шкоди, і вони повинні мати здатність це зробити. Наявність можливостей, але відсутність наміру використовувати їх, по суті, усуває будь-які загрози. З'ясовано, що слід звертати особливу увагу на дві складові партнерства: обмеження ролей та обмін інформацією. Доведено, що проведене дослідження актуалізує питання вимірювання ефективності партнерства, для того щоб однозначно з'ясувати, чи демонструють члени партнерства взаємно вдосконалений кіберзахист у результаті своїх партнерських відносин.

It is determined that for public-private partnerships focused on cybersecurity, it is the degree of common consequences that connects its participants. This designation necessitates the need for the public sector to identify the cybersecurity of private organizations as a national security issue, and thus to recognize the government's responsibility for ensuring it. The private sector, in turn, creates, manages, and maintains the systems, technologies, and processes that make up critical infrastructure, cybersecurity of which is a part of national security. It is proven that threats in cyberspace are measured by two factors: they must intend to cause some harm, and they must have the ability to do so. The availability of opportunities, but the lack of intention to use them, essentially eliminates any threats. It was found that two components of the partnership should be given special attention: role limitation and information exchange.

It has been found that modern business constructions create whole environments where the public and private sectors actively and successfully cooperate: sometimes as a customer and supplier, sometimes through supervision and compliance, sometimes as partners. These arrangements usually pursue common goals of obtaining certain positive results, but in some cases partnerships are formed as a defensive response to common opponents. This is the main goal of the partnership in the field of cybersecurity.

It was found that the partnership should highlight the union of potential victims, the purpose of which should be clearly motivated by the benefits of full cooperation in the process of strengthening security. Using risk management approaches, it can be stated that enhanced security should be commensurate with the reduction of successful exploitation of known vulnerabilities, deterrence or apprehension of intruders identified as a result of information exchange, or implementation of enhanced security strategies to detect and protect or access critical information. It is identified that the implementation of a system of performance indicators can be beneficial to both public and private partners, as it can encourage additional participation and identify areas of partnership that need improvement. For the public sector, indicators can focus on participation in the industry, the number of unique malicious signatures submitted by member groups, or some calculation of the time and resources spent on partnership tasks, such as meetings or dissemination of information.

Ключові слова: кібербезпека, кіберпростір, публічно-приватне партнерство, публічний сектор, приватний сектор, органи влади, приватні організації.

Key words: cybersecurity, cyberspace, public-private partnership, public sector, private sector, authorities, private organizations.

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Сучасні бізнес-конструкції створюють цілі середовища, де публічний і приватний сектор активно та успішно співпрацюють — іноді як клієнт і постачальник, іноді через нагляд і дотримання, іноді як партнери. Ці домовленості зазвичай переслідують спільні цілі отримання певних позитивних результатів, але в деяких випадках партнерські відносини формуються як захисна відповідь спільним противникам. Саме така мета партнерства є головною у сфері забезпечення кібербезпеки. На думку науковців, значення публічно-приватного партнерства (ППП) у сферах безпеки полягає в зменшенні дублювання зусиль, посиленні міжгалузевої комунікації, підвищенні ефективності та досягненні цілей захисту краще, ніж у ситуації, коли уряд або бізнес діють незалежно. Коли ці цілі досягнуті, інвестиції в ППП є цінними, життєздатними та змушують учасників продовжувати партнерство і надалі. Якщо ці цілі не досягнуті, учасники можуть втратити віру в домовленості, робити менший внесок, можливо, звинуватити один одного у неефективності та, ймовірно, шукатимуть альтернативні шляхи вирішення своїх потреб у кібербезпеці. На жаль, практика ППП у багатьох країнах, що демонструє негативне ставлення сторін до цих партнерських відносин, а також стабільно високі показники вразливості та експлуатації зловмисними організаціями операцій з комп'ютерними мережами (CNO) свідчать про те, що багато цілей ППП не досягаються повною мірою.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Кібербезпеці у цілому та публічно-приватному партнерству у цій сфері зокрема присвятили свої праці Е. Гівенс, В. Грейман, Е. Етціоні, С. Ліндер, Д. Льюіс, М. Карр, Т. Мур та ін. Проте невирішеність низки проблемних питань щодо створення та розвитку ППП у сфері кібербезпеки у практичній площині актуалізує доцільність проведення подальших досліджень у цьому напрямі.

МЕТА СТАТТІ

Метою статті є визначення основних аспектів формування та забезпечення публічно-приватного партнерства у сфері кібербезпеки.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ ДОСЛІДЖЕННЯ З ПОВНИМ ОБГРУНТУВАННЯМ ОТРИМАНИХ НАУКОВИХ РЕЗУЛЬТАТІВ

ППП як захисна модель покладається на те, що кожен учасник вносить щось унікальне в партнерство, що може пом'якшити слабкі сторони та посилити сильні сторони. Але у той час як публічний сектор передусім мотивований питаннями національної безпеки, приватний сектор насамперед мотивується прибутком. Карр пише, що "саме ця диз'юнктура лежить в основі напруженості у цьому партнерстві" [1, с. 44]. Часто, і підживлюючись цими відмінностями, партнерство захмарюється уявленням про те, що одна сторона робить недостатній внесок або вносить більше, ніж інша. Це сприйняття дисба-

лансу у відносинах викликає подальшу напругу. Тому хоча велика увага науковців і практиків приділяється необхідності створення ППП для поліпшення кіберзахисту, необхідними є також дослідження, що стосуються того, чому ці партнерства є неефективними. Зокрема, слід постійно отримувати відповіді на наступні запитання, пов'язані зі зниженням ефективності ППП у кібердоменах:

1. Які існують проблеми в обміні інформацією між партнерами і яким чином це впливає на партнерство у цілому?

2. Чи демонструють члени ППП взаємно вдосконалений кіберзахист у результаті своїх партнерських відносин?

3. Які об'єктивні відмінності впливають на спонукання сторін рухатись до ефективного та взаємовигідного партнерства?

Загроза зловмисних CNO є динамічною та екзистенціальною: вона завжди змінюється та постійно присутня. Протидія загрозі в міру її розвитку вимагає від ключових лідерів та осіб, що приймають рішення в публічному та приватному секторі, запроваджувати ППП як життєздатну оборонну модель, робити адекватний та необхідний внесок у партнерство та постійно вимірювати й оцінювати зміни в кібербезпеці відповідних організацій в результаті ППП. Усі партнерські відносини прагнуть зменшити індивідуальні витрати на спільні завдання та використати загальні дії та заходи членів на свою користь. Однак, щоб досягти ці дві цілі, партнери також повинні справедливо враховувати внески іншою сторони.

Ймовірно, найбільш очевидний прояв ППП відбувається стосовно критичної інфраструктури: публічний сектор має вимоги до технологій чи можливостей і платить приватному сектору за створення, інтеграцію чи інше управління цією вимогою. Публічний сектор реінвестує себе в партнерство, коли потім включає готовий продукт або послугу в якісь національні можливості. Але оскільки це стосується кібербезпеки, використання та цілі впровадження моделей партнерства можуть бути дещо складнішими. Тим не менше, Грейман бачить у цих партнерствах великі можливості, зазначаючи, що дедалі більш розподілена та взаємопов'язана природа сучасних технологічних систем повинна створювати більш динамічні партнерські відносини, які швидко розвиваються та йдуть в ногу із загрозами та вразливими місцями [4].

Втім, не всі дослідники налаштовані оптимістично з цього питання. Наприклад, Карр називає ППП у сфері забезпечення кібербезпеки "однозначно проблематичним" і стверджує, що "небажання політиків претендувати на повноваження держави вводити жорсткіші заходи з кібербезпеки... поряд із неприязним ставленням приватного сектору до прийняття відповідальності або підзвітності за національну безпеку, залишає партнерство без чітких меж відповідальності та підзвітності" [1, с. 43]. Подібним чином Грейман стверджує про існування свого роду "кіберпарадоксу", де перетинання між публічним та приватним секторами призвело до переплутування операцій національної безпеки та розвідки з кібербезпекою та конкурентоспроможністю підприємств, викликаючи зіткнення цілей [4]. Звичайно, парадокс полягає в тому, що цілі діяльності обох сторін вимагають отримання певних кіберданих, але жодна зі сторін не хоче, щоб її використовувала для цього інша. Цей парадокс суттєво сприяє виникненню проблем у партнерстві, тому питання "балансу" завжди має посідати у ньому важливе місце. Також важливо постійно наголошувати, що вплив зловмисного CNO є спільним знаменником, необхідним для об'єднання публічних та приватних організацій для забезпечення їхньої безпеки. До того ж, кожна ітерація з боку публічного сектору має заохочувати приватний сектор розробляти технології, необхідні для посилення кіберзахисту критичної інфраструктури країни, інвестувати в системи виявлення та запобігання і розробляти найкращі практики, необхідні для вимірювання ефективності ППП.

Для ППП, орієнтованих на кібербезпеку, саме ступінь спільних наслідків пов'язує його учасників. Таке призначення зумовлює для публічного сектора необхідність визначити кібербезпеку приватних організацій як проблему національної безпеки, а отже, визнати відповідальність уряду за її забезпечення. Приватний сектор у свою чергу створює, управляє та підтримує системи, технології та процеси, що складають критичну інфраструктуру, забезпечення кібербезпеки якої є складовою забезпечення національної безпеки.

Загрози в кіберпросторі вимірюються двома факторами: вони повинні мати намір заподіяти певної шкоди, і вони повинні мати здатність це зробити. Наявність можливостей, але відсутність наміру використовувати їх, по суті, усуває будь-які загрози. Звичайно, намір стосується мотивації зловмисників того, що рухає їх до якоїсь мети. Мотивація у цій сфері може варіюватися від простого хуліганства, до політичної активності та шпигунства, спрямованого на інші держави. Часто мотивація визначає, наскільки стійкою може бути певна загроза, і якщо її можна з'ясувати, то це може мати певний зв'язок із можливостями, які може використовувати загроза. У широкому розумінні можливості стосуються тактики, техніки та процедур, до яких загроза має доступ і буде використовувати їх для заподіяння шкоди у відповідності до визначеної мети. У суто технічному розумінні можливості щодо кіберзагроз конкретно стосуються експлойтів та шкідливих програм, якими користується загроза. Можливості також можуть містити широкий спектр інструментів — від програм з відкритим кодом до спеціально розроблених шкідливих програм, що надаються державними спецслужбами. Звичайно, мотивацію можна затуманити, оголошуючи незрозумілі цілі, і багато можливостей можна отримати в Інтернеті, що у сукупності ускладнює виявлення типу загрози. Проте впевненість у з'ясуванні як умислу, так і передбачуваних для використання можливостей може допомогти у визначенні категорії загрози.

У своєму дослідженні з економіки поліпшення кібербезпеки Мур визначив чотири основні проблеми в кіберпросторі: крадіжка інтернет-ідентифікаційних даних, промислове кібершпигунство, порушення захисту критичної інфраструктури та ботнети [7, с. 4]. Мур пропонує ці категорії не лише як основу для розгортання кібербезпеки, але і як цілі, що спрямовують усі зусилля з кібербезпеки. Накладання цих цілей на ППП ілюструє, що як публічний, так і приватний сектор чутливі до впли-

ву цих проблем, і це має бути достатньою причиною для стимулювання співпраці та більш підзвітного партнерства.

Однак Мур також визначає три бар'єри для покращення кібербезпеки, — невідповідні стимули, інформаційні асиметрії та зовнішні ефекти, — які, якщо їх не врахувати належним чином, закладають основу для неминучої неефективності кібербезпеки [7, с. 7]. У своїй роботі Мур описує "невідповідні стимули" як явища, що виникають в результаті компромісу між безпекою та ефективністю [7, с. 7]. Чим складнішою є система безпека або чим більше шарів безпеки вона має, тим менша ефективність буде відчуватися. Так, Мур зазначає, що якби банки не пропонували Інтернет-банкінг, вони були б значно менш схильні до злому. Однак їхні клієнти також мали б менший доступ до своїх грошей, а витрати на управління філіями були б для банку значними. Окремо вимоги до низьких витрат можуть вплинути на придбання дешевшого, але менш безпечного програмного забезпечення, що потенційно може створити вразливі місця або можливості для зловмисників.

Як правило, "інформаційна асиметрія" — це нездатність знати правду про інформацію (наприклад, що є точним, що є перебільшеним) або які мотивації передують тому, якою інформацією обмінюються, і чому. По суті, інформаційні асиметрії вселяють сумнів у надійності даних, якими обмінюються сторони. Якщо розглядати їх як елементи ризику, стає зрозумілим, що цей бар'єр може суттєво вплинути на точні розрахунки поширеності загрози, масштабу вразливості, впливу шкідливого CNO чи ефективності контрзаходів. Це, звичайно, може вплинути на готовність, пріоритети безпеки чи інвестиції та може призвести до додаткових проблем.

Нарешті, Мур описує зовнішні ефекти, або ефекти "переливу" в кібербезпеці. У цьому разі зовнішні ефекти стосуються того, як взаємозв'язок речей може або надати користь, або бути вразливим для великих спільнот користувачів. По суті, оскільки технологічна галузь має тенденції до домінуючих фірм, їх потреба полягає в тому, щоб бути сумісними з більшістю сторонніх постачальників, а звернення до найширшої бази спонукає їх спочатку до зростання частки ринку, а лише потім — до впровадження безпеки [7, с. 8]. Така мотивація сприяє впровадженню незахищеного програмного забезпечення для користувачів з подальшим постійним його виправленням та удосконаленням. Тобто заохочується розповсюдження небезпечного програмного забезпечення на ринку, що перешкоджає розробці та впровадженню захищеної інфраструктури та стримує інвестиції в безпеку.

Поряд із зазначеними бар'єрами ще однією проблемою, яка негативно впливає на ППП, є те, що влучно висловила Карр: те, що відповідає найкращим інтересам суспільства щодо кібербезпеки не завжди відповідає найкращим інтересам приватного сектору; соціальні вигоди не є значущими з точки зору прибутковості, яким би бажаним не був результат [1, с. 57].

У своїй роботі над ідеологічною філософією ППП Ліндер описує партнерство як "акомодаційне — вони стримують привид оптової продажу та в обмін обіцяють вигідну співпрацю з державою" [6, с. 39]. Цей опис свідчить про те, що за певного моменту учасники очікують на більше, ніж дають самі, тобто утримуються від надто активних дій, покладаючись у цьому на інших. Але проблема полягає в тому, що якщо всі партнери підуть таким чином, виграш для всіх буде мінімальним, а партнерство взагалі стане марним зусиллям. Дві складові ППП демонструють цю ідею "стримування": обмеження ролей та обмін інформацією. Розглянемо їх.

1. Обмеження ролей. Ролі партнерства визначаються менше альтруїзмом, а більше унікальними обставинами, які визначають рівень прихильності сторін до цього партнерства. Наприклад, приватна організація може брати участь у партнерстві через певні, колись визначені, зобов'язання. Цей вид обов'язкової участі може не перетворитися на активну участь і, натомість, може бути пасивним, тобто сторона партнерства прийматиме інформацію, але не надаватиме її іншим партнерам. Таким чином, хоча спільне занепокоєння може бути обов'язковим, ролі та обов'язки для суб'єктів у партнерських відносинах повинні бути чітко визначені, або інакше партнерства стикаються з невдачею. Іншими словами, публічний партнер зобов'язаний виконувати свої обов'язки та юридичні повноваження, тоді як приватний партнер чимось заохочується. Хоча і дещо ненауково, але прихильність до ППП може вимірюватися загальним розподілом часу, ресурсів, грошей, впливом на суспільне сприйняття або навіть порогами, за якими ризик буде прийнятий, або проігнорований.

Центральні органи влади можуть встановити певні стандарти у сфері кібербезпеки і вони наділені повноваженнями забезпечувати дотримання цих стандартів. Однак, як показує практика інших країн, уряди останнім часом широко встановлюють операційні стандарти та стандарти безпеки у публічних організаціях, але неохоче роблять це для приватного сектору. І це ставить потенційні сторони партнерства у нерівні умови. Тобто подібний підхід зводить повноцінне двобічне партнерство лише до "залучення" приватного сектора до здійснення заходів з кібербезпеки. Втім, це не позбавлене певного сенсу, оскільки занадто велике втручання уряду може мати негативні наслідки для економічної потужності приватного сектору.

Таким чином, публічний сектор часто виявляє, що пропонує ті чи інші стимули приватному сектору для поліпшення співпраці та передачі даних, включаючи рішення та дії щодо пом'якшення негативних наслідків та винагороди за дотримання вимог і стандартів. Хоча з точки зору публічних осіб ці заохочення можна розглядати і як потенційні проблеми, чекаючи, що з часом заохочення трансформуватимуться у зростаючі витрати для публічного сектора. Тобто публічний сектор значною мірою покладається на таке собі "саморегулювання" приватного сектора стосовно забезпечення кібербезпеки. Але у такому разі публічний сектор повинен самостійно оцінити, чи саморегулювання в приватному секторі належним чином захищає інформаційні системи критичної інфраструктури від кіберзагроз і чи адекватно правила партнерства примушують приватний сектор ділитися з публічним партнером даними про кіберзагрози, вразливості та шкідливий вплив.

Приватні організації схильні зосереджуватися на короткотермінових витратах та вигодах на шкоду довгостроковим наслідкам [2]. Такий підхід до діяльності керує розумінням приватним сектором кіберзагроз, їх впливу та їхнього внеску в ППП. Наприклад, стався злам бази особистих даних працівників приватної компанії з вантажоперевезень. Хоча цей злам, ймовірно, вплине на осіб, які працюють у компанії, але вплив на безперервність ділових операцій буде майже відсутнім. І якщо цей тип порушення даних не призведе до передбачуваних перебоїв у роботі, витрати на поліпшення кібербезпеки навколо того, як, де і чому зберігаються ці дані, швидше за все, не будуть пріоритетними.

Зосередження уваги на короткотермінових витратах також сприяє зменшенню кількості повідомлень про зловмисні CNO з двох, здавалося б, протилежних причин: 1) це занадто шкідливо і може коштувати грошей, або 2) це не має значення і не варто витрат. У першому випадку існує думка, що обмін подібною інформацією може спричинити шкоду для публічності або призведе до судових процесів щодо відповідальності за шкоду приватним особам [2]. Це може також стосуватися витрат, що стосуються зовнішніх факторів — наслідків поширення порушень кібербезпеки на інші організації або на інших осіб. Наприклад, зловмисник може зламати приватну комп'ютерну мережу і зробити її частиною ботмережі, що спричинить відмову в обслуговуванні екстреної служби, такої як швидка допомога. Тобто вразливість у першій, не критично важливій системі, сприяла віктимізації критично важливої системи. Подібному можна було б запобігти, якщо б власник першої мережи вкладав достатньо коштів у її кіберзахист.

2. Обмін інформацією. Обмін інформацією, як правило, є найбільш часто рекламованою перевагою ППП, однак цінність практики та даних, що передаються, зменшується за рахунок внутрішнього контролю як у публічному, так і в приватному секторах. Маркетинг цих партнерських відносин часто описує результат обміну інформацією як своєчасну, актуальну, точну та ефективну інформацію. Що стосується кібербезпеки, обмін даними, як очікується, має інформувати загальну базу знань про загрози, можливості, вразливості, які використовують зловмисники, і методи, за допомогою яких їх можна виявити, заперечити або порушити. Обмін інформацією може створити спільноти інтересів, покращити відносини між внутрішніми та зовнішніми партнерами і є основою для поліпшення кібербезпеки.

Проте Карр визначає кілька безпосередніх проблем у даному процесі: не завжди зрозуміло, що означають дані або яка їх цінність у більшому контексті або для партнерів; певна інформація може виявити слабкі місця, якими може скористатися конкуренти; існують проблеми з класифікацією інформації, що обмежують те, як дані можуть використовуватися і з ким можна ділитися тими чи іншими даними [1]. Додаткові бар'єри для ефективного обміну інформацією можуть також включати побоювання щодо розголошення наданої інформації з негативними наслідками від цього, а також певне постійним потоком інформації, що представляє сумнівну цінність для сторони партнерства.

Цінність обміну інформацією як вигоди зменшується, коли партнери не розуміють, що від них очікується, якщо не передбачено заходів, які забезпечують відповідність внесків партнерів, а також коли партнери роблять припущення щодо недостатнього внеску свого партнера. Щодо останнього пункту, Гівенс описує це як причину, що дозволяє апатії просочуватися в партнерство [3]. Коли один учасник припускає, що він непропорційно порівняно з іншими виграє від партнерства, незалежно від якості поданих ним даних, він, як правило, інвестує у партнерство менше.

Обмін інформацією може спричинити нерозуміння інформаційних потреб партнерів. Одне з проведених досліджень щодо обміну інформацією в рамках ППП з питань кібербезпеки показало, що інформаційні потреби в публічному та приватному секторі дуже різняться передусім це стосувалося конфіденційності [5]. Так, дослідження виявило, що спільна інформація поділялась на дві категорії: технічні індикатори загроз та контекстна інформація. Технічні індикатори загроз — це специфічні, загальні та повторювані форми інформації, які піддаються анонімізації, стандартизації та швидким формам розповсюдження. Контекстна інформація, навпаки, стосується детальної інформації про учасників партнерства та можливі загрози і створює більший ризик для конфіденційності та несанкціонованого розкриття секретної інформації. Розмежування двох зазначених категорій мало на меті визначити те, як із цими даними слід поводитись: обробляти, передавати (і кому саме) чи ділитися (і з ким саме). Але на практиці далеко не завжди було присутнім розуміння, що ці дві категорії даних мають різну аудиторію, різні наслідки від їх використання і вимагають різних режимів розповсюдження та обробки, що призводило до різного роду інцидентів і негативно впливало на партнерство загалом.

ВИСНОВКИ З ПРОВЕДЕНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ЦЬОМУ НАПРЯМІ

Наведені у статті матеріали безумовно актуалізують питання вимірювання ефективності партнерства, для того, щоб однозначно з'ясувати, чи демонструють члени ППП взаємно вдосконалений кіберзахист у результаті своїх партнерських відносин. Номінальні зміни в показниках вторгнення за рік, зібрані компаніями з кібербезпеки та реагування на інциденти, не дозволяють говорити про ППП як джерело вдосконалення, хоча не можна і вважати, що партнерства не мають певного впливу. Натомість можна обгрунтовано припустити, що навіть пасивне залучення до обміну інформацією повинно призвести до певного поліпшення, але без вбудованої системи показників, що вимірює вдосконалення, ці партнерські стосунки приречені на посередність.

Як ніщо інше, ці партнерські відносини повинні висувати на перший план союз потенційних жертв, мета яких повинна бути чітко мотивована перевагами повного співробітництва в процесі посилення безпеки. Використовуючи підходи управління ризиками, можна за-

значити, що посилена безпека повинна співвідноситися із зменшенням успішної експлуатації відомих вразливостей, стримуванням або затриманням зловмисників, виявлених у результаті обміну інформацією або впровадженням вдосконалених захисних стратегій для виявлення та захисту критичної інформації або доступу до неї. Крім того, впровадження системи показників ефективності може бути корисним як публічним, так і приватним партнерам, оскільки може заохотити додаткову участь та визначити сфери партнерства, які потребують вдосконалення. Для публічного сектора показники можуть бути зосереджені на показниках участі в галузі, кількості унікальних шкідливих підписів, внесених групами-членами, або на деякий розрахунок часу та ресурсів, що витрачаються на виконання завдань партнерства, таких як зустрічі чи розповсюдження інформації. Визначення таких показників має стати подальшим напрямом дослідження з розглянутої проблематики.

Література:

1. Carr M. (2016). Public Provate Partnerships in National Security Strategies. International Affairs, pp. 43—62.

2. Etzioni A. (2014). The private sector: A reluctant partner in cybersecurity. Georgetown Journal of International Affairs, pp. 69—78.

3. Givens A.N.B. (2013). Realizing the promise of public private partnerships in U.S. critical infrastructure protection. International Journal of Critical Infrastructure Protection, pp. 39—50.

4. Greiman V. (2015). Public private partnerships in cyberspace: Building a sustainable collaboration. URL: https://search.proquest.com/docview/1781336082?-accountid=28902 (дата звернення 17.05.2021).

5. Lewis D.E. (2015). Cyber Threat Information Sharing — Recommendations for Congress and the Administration. Washington, DC: Center for Strategic and International Studies.

6. Linder S.H. Coming to Terms With the Public-Private Partnership: A Grammar of Multiple Meanings. American Behavioral Scientist. 1999. 43 (1). Pp. 35—51.

7. Moore T. (2010). Introducing the Economics of Cybersecurity: Principles and Policy Options. Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy. Washington, D.C.: National Academy of Sciences, pp. 3—23.

References:

1. Carr, M. (2016), "Public Provate Partnerships in National Security Strategies", International Affairs, pp. 43—62.

2. Etzioni, A. (2014), "The private sector: A reluctant partner in cybersecurity", Georgetown Journal of International Affairs, pp. 69—78.

3. Givens, A. N. B. (2013), "Realizing the promise of public private partnerships in U.S. critical infrastructure protection", International Journal of Critical Infrastructure Protection, pp. 39—50.

4. Greiman, V. (2015), "Public private partnerships in cyberspace: Building a sustainable collaboration", available at: https://search.proquest.com/docview/1781336082?accountid=28902. (Accessed 17 May 2021).

5. Lewis, D. E. (2015), Cyber Threat Information Sharing — Recommendations for Congress and the Administration, Center for Strategic and International Studies, Washington, DC.

6. Linder, Stephen H. (1999), "Coming to Terms with the Public-Private Partnership: A Grammar of Multiple Meanings", American Behavioural Scientist, vol. 43 (1), pp. 35—51.

7. Moore, T. (2010), Introducing the Economics of Cybersecurity: Principles and Policy Options. Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy, National Academy of Sciences, Washington, D.C., pp. 3—23.

Стаття надійшла до редакції 23.06.2021 р.