Бойко О.

«Європейське приватно-державне співробітництво у сфері кібербезпеки: підходи до формування та нормативно-правові засади». Аналітична записка

Одним із пріоритетних завдань Стратегії кібербезпеки України є налагодження співробітництва між суб'єктами забезпечення кіберзахисту критичної інфраструктури, розвиток державно-приватного партнерства у запобіганні кіберзагрозам, реагуванні на кібератаки та кіберінциденти, усуненні їх наслідків, зокрема в умовах кризових ситуацій, надзвичайного і воєнного стану, в особливий період [1]. Водночас реальні процеси налагодження ефективного державно-приватного партнерства у сфері кібербезпеки поки що знаходяться в початковому стані, а чинні форми такого партнерства обмежуються діяльністю Громадських рад при основних суб'єктах національної системи кібербезпеки держави (Національний інститут стратегічних досліджень).

На противагу цьому ЄС, який активно розбудовує власні спроможності для забезпечення кібербезпеки держав-членів, так само здійснює і масштабну діяльність у налагоджені державно-приватного партнерства у сфері кібербезпеки.

Сучасний стан *acquis communautaire* [2] у галузі кібербезпеки на загальноєвропейському рівні знаходиться в точці свого найінтенсивнішого розвитку. З огляду на системність характеру загроз для кібербезпеки у поєднанні з постійним зростанням кіберзлочинності в останні роки, Європейська Комісія у співпраці з країнами-членами ЄС, іншими інституціями Європейського Союзу та відповідними зацікавленими сторонами розробила узгоджену політику дій, що має регулювати цей сектор.

Згідно проведеного у 2017 р. Pricewaterhouse Cooper опитування, [3] щонайменше 80 % європейських компаній досвідчили принаймні одного інциденту протягом останніх трьох років у галузі кібербезпеки.

У липні 2016 р. Європейська Комісія після ряду громадських консультацій з усіма зацікавленими сторонами підписала угоду в галузі індустрії кібербезпеки, тим самим активізувавши зусилля, спрямовані на боротьбу з кібер-загрозами у формі державно-приватного партнерства [4].

План дій, ініційований Європейською Комісією (Agreement with industry on cybersecurity and steps up efforts to tackle cyber-threats), [5] окреслив рамки державно-приватного партнерства в галузі кібербезпеки, що надалі

---

[1] http://zakon2.rada.gov.ua/laws/show/96/2016#n11

[2] Acquis communautaire (з фр. доробок спільноти) сукупність спільних прав і зобов'язань, обов'язкових до виконання для всіх країн-членів ЄС. Доробок постійно змінюється і узагальнюється. правова система Європейського Союзу, яка включає акти законодавства Європейського Союзу (але не обмежується ними), прийняті в рамках Європейського співтовариства, Спільної зовнішньої політики та політики безпеки і Співпраці у сфері юстиції та внутрішніх справ

[3] Огляд глобального стану інформаційної безпеки 2017, http://www.pwc.com/gx/en/issues/cybersecurity/information-security-survey.html

[4] http://europa.eu/rapid/press-release_IP-16-2321_en.htm

[5] http://europa.eu/rapid/press-release_IP-16-2321_en.htm

регулюватимуть цю сферу правових та економічних відносин. На реалізацію цієї стратегії було виділено 450 млн євро, основним джерелом перерозподілу коштів є програма досліджень та інновацій «Горизонт 2020». Також учасники ринку кібербезпеки представлені Європейською організацією з кібербезпеки (ECSO) задекларували намір реалізації своїх інвестицій у рамках цієї ініціативи.

Метою партнерства є створення платформи для кібербезпеки різних секторів, таких, як енергетика, охорона здоров'я, транспорт і фінанси, а також включення в цей процес органів влади, науково-дослідних центрів та інших зацікавлених сторін, платформи, яка розвивала б дослідницький та інноваційний потенціал сектору. Така співпраця покликана зменшити негативний ефект роздробленості ринку кібербезпеки ЄС, неповної його врегульованості, що виявляється у різниці в процедурах сертифікації, з тим, щоб кожен постачальник послуги в галузі кібербезпеки міг реалізувати свою діяльність у кожній країні-члені ЄС однаково, легко уникаючи політики протекціонізму.

Ці рамки співпраці підкреслюють особливу важливість інновацій, що з'являються на перетині інтересів вищезгаданих учасників ринку – від нішевих ринків, на кшталт криптографії, з одного боку, до добре розвинутих ринків з новими бізнес-моделями (наприклад, ринок антивірусного програмного забезпечення). Цією ініціативою Європейська Комісія намагалась полегшити доступ до виходу на нові ринки підприємствам малого та середнього бізнесу, що працюють у галузі кібербезпеки…

Повний текст