

3. ДСТУ ISO/IEC 15408-1:2017 Інформаційні технології. Методи захисту. Критерії оцінки. Частина 1. Вступ та загальна модель (ISO/IEC 15408-1:2009, IDT)
4. ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for Cybersecurity. – 2012-07
5. Dutt, V., Ahn, Y. S., & Gonzalez, C.: Cyber situation awareness modeling detection of cyber-attacks with instance-based learning theory. Human Factors: The Journal of the Human Factors and Ergonomics Society, 55(3), 605-618 (2013).
6. D. Ding, Z. Wang, Q.-L. Han, G. Wei, Security control for a class of discretetime stochastic nonlinear systems subject to deception attacks, IEEE Trans. Syst. Man Cybern. Syst. doi:10.1109/TSMC.2016.2616544.
7. Sridhar, S., Govindarasu, M.: ‘Model-based attack detection and mitigation for automatic generation control’, IEEE Trans. Smart Grid, 2014, 5, (2), pp. 580–591.

Ключові слова: кіберпростір, кіберфізичні система, кібератака, кібербезпека.

Ключевые слова: киберпространство, киберфизическая система, кибератака, кибербезопасность.

Keywords: cyberspace, cyberphysical system, cyberattack, cybersecurity.

Колосенко Андрій Андрійович

*Національний університет «Одеська юридична академія»,
студентка 4-го курсу факультету кібербезпеки та інформаційних
технологій*

ІНСТИТУТ ДЕРЖАВНО-ПРИВАТНОГО ПАРТНЕРСТВА ЯК ОДИН З МЕХАНІЗМІВ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ

У часи невпинного технічного прогресу, діяльність держави, підприємств та організацій нерозривно пов'язана з інформаційно-комунікаційними технологіями.

Так, забезпечення безпеки та конфіденційності інформації, захищеності об'єктів критичної інфраструктури почало займати пріоритетне значення для будь-яких державних, так й приватних установ, в зв'язку з чим значних змін зазнали відносини між державною владою та приватним сектором економіки, а взаємодія між такими суб'єктами почала сприйматись як один з найбільш перспективних механізмів забезпечення кібербезпеки та національної безпеки держави в цілому.

Вказана взаємодія пояснюється тим, що в умовах сучасних реалій кібертероризм, кіберзлочинність та інформаційні війни змушують державу шукати та залучати приватні організації для того, щоб протидіяти вказаним явищам.

З метою вирішення вищезазначених проблем в Україні набув розвитку інститут Державно-приватного партнерства (далі – ДПП), який фактично необхідно розуміти як сукупність спільних заходів державного та приватного сектору, з метою досягнення попередньо обумовлених сторонами цілей.

Сьогодні ДПП визнається майже усіма світовими країнами, а також приватними підприємствами, як ключовий елемент функціонування ефективної та прогресивної системи протидії кіберзлочинності та забезпечення кібербезпеки держави. Майже кожна стратегія кібербезпеки (державного або наддержавного рівня) або нормативно-правові акти державних структур містять положення про необхідність розбудови інституту державно-приватного партнерства.

Проте, вказаний механізм взаємодії держави та бізнесу в Україні потребує значних змін та рушійних дій, про що добре відомо й державній владі. Оновлена редакції Стратегії кібербезпеки, яка була прийнята 14 травня 2021 року, наголошує, що на даний момент в Україні відсутня дієва модель державно-приватного партнерства у сфері забезпечення кібербезпеки [1].

Однак, варто зазначити, що станом на сьогоднішній день, на українському ринку кібербезпеки вже функціонує достатня кількість підприємств, які мають великий досвід та технічні рішення в зазначеній сфері. Їх діяльність пов'язана з виявленням мережових атак, розслідуванням кіберзлочинів, отриманням доказів під час обстеження комп'ютерних та інформаційних систем, проведенні комп'ютерних експертиз.

Такі компанії разом з державними органами безпеки та оборони безумовно можуть своєю взаємодією позитивно вплинути на забезпечення кібербезпеки України.

При цьому, можна виокремити наступні форми реалізації такої взаємодії: укладення договорів щодо надання послуг і виконання вищезазначених робіт, отримання консультацій по поточній діяльності, розробка спільних рішень та пропозицій щодо реалізації державної політики в сфері кібербезпеки, проведення спільних заходів з метою інформаційного забезпечення державних, приватних підприємств та громадян з питання дотримання заходів із забезпечення кібербезпеки тощо [2].

Крім того, ДПП може позитивно вплинути і на вітчизняний сектор економіки, оскільки такий механізм надає змогу залучити додаткові інвестиції у фінансування високобюджетних проектів.

Варто зазначити, що державою разом з приватним сектором проводяться ряд тематичних заходів в сфері інформаційної безпеки.

Так, з 2018 року Державна служба спеціального зв'язку та захисту інформації України та Комітетом електронних комунікацій ТПП України розпочато проведення щорічного заходу під назвою «Місяць кібербезпеки».

У жовтні 2019 та 2020 року він був проведений вдруге та відповідно втретє, участь в таких заходах взяли участь близько 100 компаній як з України, так й зі всього світу. Ключовими подіями заходу стали: Міжнародний форум «Кібербезпека. Захисти свій бізнес!», «LEGAL CYBERSECURITY FORUM», РКІ-форум з проблематики електронного підпису та інфраструктури відкритих ключів.

Подібні заходи присвячені підвищенню обізнаності приватного сектору і пересічних громадян про кібербезпеку і розвиток державно-приватного партнерства.

В свою чергу, зі сторони українських ІТ-компаній за останні роки були розроблені та запропоновані органам державної влади та звичайним користувачам власні антивірусні продукти.

Прикладом такого продукту, який отримав сертифікацію Держспецзв'язком України, є програмне забезпечення «Zillya! Антивірус для Бізнесу» однойменної компанії Zillya. Антивірус пропонує користувачам комплексний захист комп'ютерної системи та мереж від всіх типів кібератак та кіберзагроз з можливістю централізованого управління та оновлення антивірусних баз.

Іншим своєрідним проявом державно-приватного партнерства може слугувати взаємодія держструктур з окремими групами «білих» хакерів. Так, протягом 2017-2019 років спільнотою «Український КіберАльянс» з метою підтримки інформаційної безпеки в Україні проводились заходи, спрямовані на виявлення вразливостей в об'єктах критичної інформаційної інфраструктури українських державних органів і організацій стратегічного значення [3].

Під час таких заходів було виявлено більше тисячі різних вразливостей інформаційних систем державних установ, в тому числі НАЕК «Енергоатом», команди реагування на кіберінциденти CERT-UA та Національної поліції.

Тобто можна спостерігати, що окремі компанії, організації та спілки громадян вже досить ефективно кооперуються з суб'єктами державної влади.

Водночас, така кооперація має набути характер системності, що пояснюється щоденним зростанням загроз в сфері інформаційних технологій.

Прискорити такий процес можливо шляхом об'єднання основних компаній ринку кібербезпеки у відповідні асоціації, до яких, крім приватного сектора, долучаться також представники державних структур.

Взагалі, в Україні на ринку кібербезпеки діє досить багато приватних асоціацій, серед них можна виділити такі: Всеукраїнська асоціація “Інформаційна безпека та інформаційні технології”, громадська організація ISACA, Центр реагування на комп'ютерні надзвичайні події “CERT”, тощо [2].

Однак, створення організаційної структури на рівні держави дозволить всім зацікавленим сторонам протидії кіберзлочинності формувати та здійснювати оптимальну та ефективну політику забезпечення інформаційної безпеки на різних рівнях, що дозволить в межах ДПП досягнути стратегічних цілей держави у вказаній сфері.

Отже, як висновок можна зазначити, що для прискорення розвитку інституту ДПП у сфері забезпечення кібербезпеки в Україні необхідним є:

- розробка та ефективна реалізації стратегії розвитку недержавного сектора, який надасть змогу забезпечувати належний рівень кібербезпеки як державних структур, так й приватно-комерційного бізнесу, враховуючи інтереси кожної зі сторін;

- реформування та вдосконалення системи кооперації державних та приватних структур на міжнародному, національному, міжрегіональному, місцевому рівнях шляхом створення відповідних організацій та асоціації;

- укладання та забезпечення виконання партнерських угод за участю держави та провідних вітчизняних ІТ-компаній;

- створення та забезпечення реалізації проектів для забезпечення обміну досвідом, технічних рішень та об'єднання ресурсів між державою та приватним сектором.

Список використаних джерел:

1. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України №447/2021. URL: <https://www.president.gov.ua/documents/4472021-40013> (дата звернення 04.11.2021р.)

2. Заскока Ю.В. Державно-приватне партнерство в сфері кібербезпеки України: стан та проблеми забезпечення. Наукові перспективи № 9 2021. URL: <https://goo.su/97V0> (дата звернення 04.11.2021р.)

3. Український кіберальянс (Ukrainian Cyber Alliance). URL: <https://goo.su/97v3> (дата звернення 04.11.2021р.)

Ключові слова: державно-правове партнерство, кібербезпека, інформаційна безпека.

Ключевые слова: государственно-правовое партнерство, кибербезопасность, информационная безопасность.

Keywords: state-legal partnership, cybersecurity, information security.

Науковий керівник: к.т.н., доц. Кухаренко С.В.