ДЕРЖАВНО-ПРИВАТНЕ ПАРТНЕРСТВО У СФЕРІ КІБЕРБЕЗПЕКИ: КЕЙС НІМЕЧЧИНИ

Німеччина є однією із ключових країн, форми державно-приватного партнерства якої працюють як один із основних інструментів ефективної системи кіберзахисту країни. Позаяк під безпосереднім контролем держави в Україні перебуває лише частина національної критичної інформаційної інфраструктури, існує гранична потреба у розвитку державно-приватної взаємодії в галузі кібербезпеки. Досвід Німеччини в цьому сенсі був би важливим і для України з метою розробки власної стратегії такого партнерства і подальшої успішної її імплементації.

За даними цифрової промислової асоціації Німеччини Bitkom 53 % німецьких компаній вже стали жертвами економічного кібершпигунства[1]. Згідно опитування «Захисту бізнесу в цифровому світі» (*Business Protection in the Digital World*) кожного року втрачається більше 55 млрд євро через шпигунство, саботаж або крадіжку даних у німецькій промисловості. У опитуванні взяли участь 1069 менеджерів та співробітників служби охорони[2].

Згідно аналізу BitCom та Німецької внутрішньої розвідувальної служби (BfV), менше третини компаній звернулися до уряду за допомогу після кібератаки. Основною мотивацією браку повідомлення про кібератаку є небажання завдати шкоди репутації. Промисловість набагато випереджає у плані технологічної просунутості порівняно з їхніми урядовими партнери. Уряд може сприяти адміністративними ресурсам, на які приватний сектор не може мати законно впливу.

На стратегічному та операційному рівні федеральний уряд Німеччини, керуючись цілісним підходом до захисту критичної інфраструктури, що

1 https://www.bitkom.org/Presse/Anhaenge-an-PIs/2017/07-Juli/Bitkom-Charts-Wirtschaftsschutz-in-der-digitalen-Welt-21-07-2017.pdf

2 https://www.verfassungsschutz.de/embed/annual-report-2016-summary.pdf.

здійснюється в рамках впровадження Національної стратегії для захисту критичної інфраструктури (стратегія CIP), у 2005 р. розробив та почав втілювати План державно-приватного партнерства КРІТІС («*Umsetzungsplan KRITIS*»), і вже у 2006 р. він почав реалізуватись у співпраці з операторами критичної інфраструктури. З опублікуванням плану імплементації у 2007 р. це державно-приватне співробітництво під назвою «UP КРІТІС» почало діяти.

Головною метою даного співробітництва є покращення захисту критичної інфраструктури у різних секторах безпеки. У Німеччині підприємства та об'єкти в галузі постачання енергетики, інформаційних технологій та телекомунікації, транспорту та торгівлі, охорони здоров'я, продовольчого та водопостачання, фінансово-страхового сектора, державного та адміністративного управління, а також засобів масової інформації та культури є складовими критичної інфраструктури держави.

Одним із напрямів державно-приватного партнерства ініційованого Німеччиною є заохочення співпраці між державними та приватними організаціями на ранніх етапах дослідницького та інноваційного процесу в країні (та в Європейському Союзі в цілому) з метою синхронізації доступу до інноваційних та надійних європейських рішень – продуктів, послуг та програмного забезпечення для ІКТ.

1. Нормативно-правове забезпечення державно-приватного партнерства у сфері кібербезпеки Німеччини

Федеральний уряд Німеччини продемонстрував своє міжнародне зобов'язання захищати міжнародну спільноту від кіберзлочинів шляхом підписання (2001 р.) і ратифікації (2009 р.) Конвенції Ради Європи про кіберзлочинність[3], а також роботою на національному рівні для забезпечення її виконання. Крім того, Німеччина підписала та ратифікувала додаткові протоколи до Конвенції про кіберзлочинність, яка стосується криміналізації

3 http://zakon0.rada.gov.ua/laws/show/994_575

расистських та ксенофобських дій, вчинених через комп'ютерні системи. У своїй національної стратегії кіберзахисту 2011 р. Німеччина знову підтвердила свою прихильність справі міжнародної гармонізації кібербезпеки[4].

Кримінальний кодекс Німеччини регулює сферу кібернетичних злочинів у частині визначення понять, суті злочину та наслідків за вчинений злочин на кшталт комп'ютерного шахрайства, втручання в дані, комп'ютерного саботажу, корпоративного шпіонажу даних, фішингу, а також інших злочинних дій у кіберпросторі[5].

Розділ 93-95 Кримінального кодексу Німеччини пов'язаний із визначенням таємниць національної безпеки[6] та закон 1994 р. «Про необхідність класифікації даних»[7], що вважаються таємними та критичними для захисту суспільних інтересів, параграф 4 якого окреслює чотирирівневу систему рівнів засекречування. Рівні призначаються відповідно до рівня ризику, пов'язаного з розголошенням секретної інформації.

Національна стратегія захисту критичної інфраструктури 2009 р. (Стратегія CIP)[8] була хронологічно першим стратегічним документом, що містить відповідні визначення «критичної інфраструктури» та «захисту від атак на критичну інфраструктуру»[9].

Наступним кроком у стратегічному плануванні був **Національний план захисту інформаційної інфраструктури, який у 2011 р.** був перейменований у **Національну стратегію кібербезпеки[10],** що посилив можливості правоохоронних органів, Федеральної агенції та приватного сектору у боротьбі з кіберзлочинністю, а також зробив наголос на захисті країни від шпигунства та

4 http://www.potomacinstitute.org/images/CRI/CRI_Germany_Profile_PIPS.pdf
5 Federal Ministry of Justice and Consumer Protection, (2015), https://www.gesetze-im-internet.de/englisch_stgb/
6 https://www.gesetze-im-internet.de/englisch_stgb/
7 http://www.gesetze-im-internet.de/
8 http://www.bmi.bund.de/cae/servlet/contentblob/598730/publicationFile/34416/kritis.pdf
9http://www.bmi.bund.de/cae/servlet/contentblob/121734/publicationFile/13577/Nationaler_Plan_Schutz_Informationsinfrastrukturen.pdf
[10]https://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_download.pdf?__blob=publicationFile

саботажу. Саме ця стратегія окремим розділом прописує рамку **спільних інститутів для бізнесу/приватного сектору та правоохоронних органів**, й як це сформульовано в Законі **Про інформаційну безпеку (IT-Sicherheitsgesetz)** в 2015 р., усі подальші кроки мають з цим узгоджуватися[11]. Додаткового розвитку ця сфера державно-приватного партнерства (ДПП) отримала у Стратегії кіберзахисту 2016 р. – **Cyber Sicherheits Strategie[12].**

Безпосередньо сфера ДПП в галузі кібербезпеки між операторами критично важливої інфраструктури та відповідними державними органами регулюється планом реалізації **Umsetzungsplan KRITIS des Nationalen Plans zum Schutz der Informationsinfrastrukturen 2014 p.**[13]. Однією з пріоритетних цілей державно-приватного партнерства, яке закріплене в законодавстві під назвою UP KRITIS, є «спільна оцінка кібербезпеки та реакція на неї»[14]. Ця національна ініціатива між державою Німеччиною та операторами критичної інфраструктури ініційована з метою захисту стратегічної інформаційної інфраструктури.

2. Ключові елементи Національної стратегії кібербезпеки в частині державно-приватного партнерства

Стратегія кібербезпеки Німеччини була прийнята в 2011 р. як комплексна стратегія, що включає основоположні принципи, чіткі цілі та план впровадження стратегічних напрямів та завдань, спрямованих на:

- захист критичної інфраструктури та IT-систем;
- зміцнення інформаційної безпеки державного управління шляхом прийняття єдиної «федеральної мережі»;
- створення Національного центру кібер-реагування;

11https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl115s1324.pdf#__bgbl__%2F%2F*%5B%40attr_id%3D%27I_2017_75_inhaltsverz%27%5D__1512488189939

12 https://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf

13https://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/kritis_download.pdf?__blob=publicationFile

14https://www.kritis.bund.de/SubSites/Kritis/EN/activities/national/cipimplementationplan/cipimplementationplan_node.html

- створення Національної ради з питань кіберзлочинності для покращення співпраці між державним сектором та приватним сектором;
- сприяння ефективній міжнародній координації кібербезпеки;
- розвиток інновації в IT індустрії;
- підготовка кваліфікованого персоналу в федеральних органах влади;
- ефективне використання таких інструментів державного сектору, як законодавчі повноваження, для боротьби з насильством у сфері кібератак[15].

Національна стратегія кіберзахисту 2011 р. уповноважила Федеральну агенцію з питань інформаційної безпеки (BSI) створити Національний центр кібер-реагування (National CyberAbwehrzentrum, NCAZ BSI), який би забезпечував кращу координацію дій щодо атак та більш оперативний обмін інформацією між урядом та приватним сектором. NCAZ BSI створює умови усім компетентним органам для оперативного реагування на серйозні інциденти, а також проводить аналіз та оцінку небезпек, координує співпрацю з місцевими та галузевими організаціями з врегулювання кризових ситуацій[16].

Окрім прямої участі Федеральної агенції з питань захисту Конституції (*Bundesamt für Verfassungsschutz, BfV*) та Федерального відомства з питань цивільного захисту та ліквідації наслідків стихійних лих (*Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, BBK*), усі інші урядові органи, що займаються питаннями кібербезпеки, у тому числі Федеральна служба кримінальної поліції (*Bundeskriminalamt, BKA*), Федеральна поліція (*Bundespolizei, BPOL*), Митна кримінологічна служба (*Zollkriminalamt, ZKA*), Федеральна розвідувальна служба (*Bundesnachrichtendienst, BND*), Бундесвер та інші органи, що здійснюють нагляд за критичною інфраструктурою та операторами у рамках центру активно співпрацюють з приватним сектором.

15https://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile
16 Federal Ministry of the Interior, “Cyber Security Strategy for Germany.”

Німеччина провела кілька національних навчань із питань кібербезпеки для державних установ та окремих операторів критичної інфраструктури. Одне з них у 2011 р. стосувалося підготовки до кризових ситуацій і було спрямоване на розуміння урядом механізму реагування на багатосторонні атаки, включаючи розподілені атаки типу «відмова в обслуговуванні» (DDoS), напади на критичну інфраструктуру, потрапляння шкідливих програм у банківські системи, та втручання в координацію системами управління руху літаків[17]. Німеччина також бере участь у багатонаціональних навчаннях, організованих Європейським Союзом та Організацією Північноатлантичного договору (НАТО). Незважаючи на кількість навчань, проведених в останні роки, план впровадження Центру рекомендував провести більше «вправ для перевірки та оновлення існуючих концепцій». Нарешті, внутрішня розвідувальна служба BfV – Німеччина публікує щорічні звіти про кіберзагрози, до прикладу у доповіді 2016 р. зазначено, що Росія та Китай є провідними джерелами кібератак на Німеччину. Також було виявлено, що Німеччина бачить загрозу інформаційній безпеці в Ірані[18].

3. Суб'єкти виконання державної стратегії

Німеччина має високу інституційну здатність реагувати на різні елементи кіберзлочинності. Німецький національний центр кібер-реагування (Das Nationale Cyber-Abwehrzentrum (NCA) / German National Cyber Response Centre)[19], Федеральна агенція з питань інформаційної безпеки (BSI) та Федеральна агенція кримінальної поліції (BKA) спільно об'єднують зусилля, спрямовані на боротьбу з кіберзлочинністю. Зокрема NCA поєднує у собі ресурси різних державних установ, включаючи федеральну поліцію та

17 NATO Science for Peace and Security Series, Information and Communications Security, vol.35, (IOS Press, February 2014): 12,

18 Joe Uchill, "German Intelligence Blames Russia, China for Cyberattacks," The Hill, June 28, 2016, http://thehill.com/ policy/cybersecurity/285202-german-intelligence-blames-russia-china-for-cyber-attacks?utm_source=&utm_medium=email&utm_campaign=2679.

19 https://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf , p.28

зовнішню розвідувальну службу, а також бізнес сектору[20].

3.1. Федеральна агенція з питань інформаційної безпеки (BSI)[21]

Агенція **вивчає ризики безпеки**, пов'язані з використанням ІКТ, та **розробляє превентивні заходи безпеки**, надає інформацію про ризики та загрози, пов'язані з використанням інформаційних технологій, і **пропонує вирішення**[22]. Робота цієї агенції включає також тестування ІТ-безпеки та оцінку ІКТ-систем, у тому числі **їх розробку у співпраці з представниками галузі.** Навіть у технічно захищених інформаційних та телекомунікаційних системах ризики та збитки можуть виникнути внаслідок неадекватного адміністрування або неналежного використання. Щоб звести до мінімуму або уникнути цих ризиків, агенція **працює з різними цільовими групами,** у т.ч консультує виробників, дистриб'юторів та користувачів інформаційних технологій, а також аналізує розвиток та тенденції розвитку інформаційних технологій. Агенція складається із п'яти департаментів, одного центрального та чотирьох спеціалізованих підрозділів. Кожен відділ складається з одного-трьох підрозділів, кожен з яких у свою чергу містить ряд структурних підрозділів[23].

Будучи національним органом з питань кібербезпеки для Німеччини, Агенція формує політику та діяльність інформаційної безпеки шляхом запобігання, виявлення та реагування. Агенція видає попередження про шкідливе програмне забезпечення та вразливі місця в ІТ-продуктах і сервісах, поширює інформацію як зацікавленим сторонам, так і широкій громадськості, і рекомендує контрзаходи. Агенція також відповідає за підтримку інформаційного

---

20 Center for Strategic and International Studies, "Cybersecurity and Cyberwarfare," (2011), http:// unidir.org/files/publications/pdfs/ cybersecurity-and-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf .

21 Федеральне агентство вищого рівня, яке відповідає за управління ІКТ та забезпечення безпеки зв'язку для уряду Німеччини. Сфера його компетенції та відповідальності включає в себе безпеку комп'ютерних систем, захист критичної інфраструктури, безпеку Інтернету, криптографію, контрслужбу, сертифікацію продуктів безпеки та акредитацію лабораторій тестування безпеки. Агенство розташоване у Бонні та має понад 600 співробітників.

22 https://www.bsi.bund.de/EN/TheBSI/Functions/functions_node.html

23https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/BSI/org_chart_IFG_pdf.pdf?__blob=publicationFile&v=7

обміну з більш ніж 50 000 приватних установ[24].

Німеччина має **мережу комп'ютерних служб кризового реагування** (network of computer emergency response teams - CERTs), з національною CERT - **CERT-BUND**[25], тісно співпрацюючи з державним органами та неурядовими структурами кризового реагування.

У Німеччині з 1991 р. було створено кілька комп'ютерних груп (CERT) та їх еквівалентів. У 1994 р. Агенція створила першу комп'ютерну команду з надзвичайних ситуацій (BSI-CERT) для федеральних установ як віртуальну структуру, що зосереджувала свої зусилля на зборі інформації. У 2001 р. BSI-CERT був перейменований в **CERT-Bund**, який **слугував центральною платформою комунікації для здійснення превентивних, реактивних та активних заходів щодо інцидентів у галузі кібербезпеки**. Сьогодні **CERT-Bund** тісно **співпрацює як з державними, так і з неурядовими CERT**.

3.2. Німецький національний центр кібер-реагування (Nationales Cyber-Abwehrzentrum, NCAZ / German National Cyber Response Centre)

У 2011 р. уряд Німеччини створив Національний центр швидкого реагування на кібератаки. NCAZ об'єднує ресурси з кіберзахисту Федеральної агенції з питань інформаційної безпеки, Федерального відомства із захисту Конституції, Федеральної розвідувальної служби, Федеральної поліції, слідчого управління Митниці Німеччини, Бундесверу, Федерального управління цивільного захисту та допомоги при стихійних лихах, і Федерального відомства кримінальної поліції, а також співпрацює з наглядовими органами операторів критично важливої інфраструктури, у межах своїх статутних обов'язків і повноважень. Основою взаємодії є «угода про співпрацю» відповідних органів і

24https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Magazin/BSI-Magazin_2017-01.pdf?__blob=publicationFile&v=4
25 https://www.bsi.bund.de/EN/Topics/IT-Crisis-Management/CERT-Bund/cert-bund_node.html

відомств Німеччини[26].

NCAZ також уповноважений **співпрацювати з будь-якими інститутами ЄС** безпосередньо, з використанням ресурсів існуючих органів країн ЄС, що займаються питаннями кіберзахисту. **Центр співпрацює з Європейським агентством з мережевої та інформаційної безпеки ENISA**, директор якого Удо Хельмбрехт раніше займав пост президента Федеральної агенції з питань інформаційної безпеки, а президент NCAZ Міхаель Ханг входить до Наглядової ради ENISA.

Як зазначено в Національній стратегії кіберзахисту 2011 р., Німецький національний центр кібер-реагування відповідає за координацію реагування на інциденти та обмін інформацією в цілому. Однією із найгостріших потреб було створення ініціативи/платформи, до складу якої входили б представники промисловості та неурядових організацій, здатних надавати поточну та достовірну інформацію в галузі кібербезпеки на національному рівні та консультувати зацікавлені сторони у попередженні та пом'якшенні кібер-інцидентів. У співпраці з Національним центром кібер-реагування Альянс з питань кібербезпеки (галузевої платформи для співпраці та обміну інформацією, створений у 2012 р.) реалізується форма співпраці між державними органами, академічним та приватним простором, а також підприємствами, що представляють особливий громадський інтерес.

Сприяючи національному обміну інформацією, **Національний IT ситуаційний центр**[27] (Nationales IT-Lagezentrum[28]), яким є також складовою

---

26 Die Strategie der Bundesregierung zur Bekämpfung der Internetkriminalität — Das Nationale Cyber-Abwehrzentrum Antwort der Bundesregierung vom 2. Mai 2011 (Drucksache 17/5694) auf die Kleine Anfrage der Abgeordneten Petra Pau, Jan Korte, Petra Sitte, weiterer Abgeordneter und der Fraktion DIE LINKE. (Drucksache 17/5560), PDF.

27 Ситуаційний центр надає Центру кіберзахисту звіти про ситуацію, довідкову інформацію про інциденти, пов'язані з інформаційною безпекою, та інформацію / попередження вразливості. Щоб отримати додаткову інформацію для оцінки ситуації та виконання порядку захисту, питання також задаються цілеспрямованим чином. Центр кіберзахисту надає рейтинги, доповнення та довгостроковий ситуаційний аналіз з його більш широкої міжвідомчої перспективи та відповідей на питання.

28 https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/Aktivitaeten/IT-Lagezentrum/lagezentrum_node.html

частиною **Федеральної агенції з питань кібербезпеки**, ***стежить за національною та глобальною ситуацією в сфері безпеки IT***, з метою швидкого ***виявлення та аналізу серйозних інцидентів*** у галузі інформаційної безпеки та рекомендує захисні заходи. У випадку ***кризи*** ця структура може розширити свою спроможність і **трансформуватися в Національний центр критичного IT реагування** (Nationales IT-Krisenreaktionszentrum[29]). Цей центр концентрує можливості для подолання IT-криз, охоплюючи всі національні аспекти, включаючи державні мережі та критичні інфраструктури.

4. Закон Про інформаційну безпеку Німеччини 2015

У липні 2015 р. у Німеччині був прийнятий **закон Про інформаційну безпеку**[30] з метою запобігання атакам на важливі інформаційні системи. Закон визначає мінімальні стандарти кібербезпеки для більш ніж 2 тисяч компаній операторів критичної інфраструктури. Відповідно до закону ці мінімальні вимоги до безпеки мають забезпечуватися шляхом вдосконалення доступності, автентичності, конфіденційності та цілісності IT-безпеки у всій Німеччині; підвищенням безпеки Інтернету для громадян; кращим захистом критично важливої інфраструктури національного значення[31].

Згідно закону оператори критичної інфраструктури зобов'язані встановити належні системи інформаційної безпеки на власних підприємствах під час надання ними послуг, зобов’язані обновлювати цю систему кожні два роки. Оператори також зобов’язані повідомляти про серйозні кіберінциденти BSI – обов'язок повідомляти про кібератаки мають оператори атомних електростанцій, телекомунікаційних компаній, а також починаючи із травня 2016 р. згідно оновленої стратегії кібербезпеки, оператори критичної інфраструктури в секторі енергетики, інформаційних та телекомунікаційних технологій, продуктів

29https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/Aktivitaeten/IT-Krisenreaktionszentrum/itkrisenreaktionszentrum_node.html
30 https://www.gesetze-im-internet.de/englisch_bdsg/
31Watson Farley & Williams, “Briefing: The New German IT Security Act,” February 2016, http://www.wfw.com/wp-content/ uploads/2016/02/WFW-Briefing-GermanyIT-Security-Feb-2016-EN-15-Feb.pdf

харчування та водного секторів. Обов'язкова звітність про інциденти операторів критичної інфраструктури в галузі фінансів, страхування та транспортних секторів, а також здоров'я існували з моменту вступу в силу постанови про зміну до діючого положення про KPITIC 30 червня 2017 р.[32]

Закон[33] вимагає від BSI проводити аудит безпеки організацій, що займаються критичною інфраструктурою один раз на два роки. Цей закон також розширив повноваження Федеральної служби кримінальної поліції для розслідування злочинів, пов'язаних із хакерськими атаками на федеральні IT-системи[34]. Закон також вимагає обов'язкової звітності від федеральних органів влади щодо інцидентів в галузі кібербезпеки перед Федеральною агенцією з питань інформаційної безпеки. Ненімецькі компанії, що є операторами критичної інфраструктури в Німеччині, також підпадають під дію закону.

У частині питань приватного сектору закон регулює діяльність операторів онлайн ресурсів та інших постачальників послуг щодо захисту використовуваних ними IT-систем та рівня захищеності цих систем від несанкціонованого доступу до персональних (клієнтських) даних. З цією метою повинні використовуватись найсучасніші технічні та організаційні процедури шифрування. Також телекомунікаційні компанії тепер повинні повідомляти своїх клієнтів про будь-які порушення та зловживання їх мережею. Оператори критичної інфраструктури та їх промислові асоціації можуть запропонувати галузеві стандарти безпеки, які можуть бути визнані BSI, якщо ці стандарти дійсно запобігають перебоям і гарантують цілісність, автентичність та конфіденційність відповідної інфраструктури[35].

Протягом двох років після прийняття закону всі оператори зобов’язані

---

[32] https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/IT-SiG/FAQ/faq_it_sig_node.html

33https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl115s1324.pdf#__bgbl__%2F%2F*%5B%40attr_id%3D%27I_2017_75_inhaltsverz%27%5D__1512488189939

34https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl115s1324.pdf#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl115s1324.pdf%27%5D__1511459742552

[35] http://www.wfw.com/wp-content/uploads/2016/02/WFW-Briefing-Germany-IT-Security-Feb-2016-EN-15-Feb.pdf

були здійснити належні організаційні та технічні заходи безпеки для захисту IT-систем, їх компонентів або процесів, що мають відношення до функціонування критичної інфраструктури. Крім того, оператори об'єктів критичної інфраструктури зобов'язані проходити аудит або сертифікацію безпеки IT щонайменше кожні два роки.

Цей закон мав на меті врегулювати низку попередніх недоопрацювань правових положень, втім для бізнесу та підприємств галузі залишається під питанням, хто є частиною KRITIS і якими є наслідки закону про IT-безпеку. Відтак, за відгуком індустрії та бізнес-спільноти визначення оператора критичної інфраструктури не є достатньо прозорим зокрема через те, що у законі 2015 р. для компаній малого і середнього бізнесу не було розмежування сфери застосування закону. За опитуванням PwC[36] близько 18 % компаній зареєстрованих в Німеччині юридично можуть підпадати під поняття оператора, визначеного у законодавстві. Згідно аналізу KPMG[37] кількість «непевних» компаній є ще вищою.

У лютому 2016 р. був опублікований проект урядової постанови, який частково вирішував це питання, втім низка асоціацій інформаційної безпеки такі як VDE (Асоціація електричних, електронних та інформаційних технологій Е.В.), VKU Асоціація житлово-комунального господарства (Verband Kommunaler Unternehmen) або DVGW (Німецької асоціації для газу і води) бачать необхідність у подальшій специфікації[38]. Тако все ще не вирішеним залишається питання членства в UP KRITIS: за визначенням Федеральної агенції державно-приватного співробітництва таке членство є добровільним, але у випадку, коли організація не є членом UP KRITIS, вона можете підпадати під санкції згідно закону 2015 р.

36 https://next.pwc.de/wikri-2016/infrastruktur-unter-besonderem-schutz.html
37 https://home.kpmg.com/de/de/home/services/advisory/consulting/security-consulting/it-sicherheitsgesetz.html
38 https://www.security-insider.de/was-kritis-fuer-unternehmen-bedeutet-a-536376/

5. UP KRITIS та інші форми державно-приватної співпраці в Німеччині

UP KRITIS є фінансованою з боку держави ініціативою державно-приватного партнерства між операторами критичної інфраструктури та відповідними державними органами. Однією з явних цілей UP KRITIS є спільна оцінка стану кібербезпеки та вироблення механізму реагування на кіберінциденти. Як форма державно-приватної співпраці між операторами критичної інфраструктури, їх асоціаціями та відповідними державними органами КРІТІС сконцентрований на декількох напрямах діяльності.

Передусім, підготовка та реалізація спільних рекомендацій для держави та приватного сектору у сфері кіберзахисту. Робоча група UP KRITIS виробила два основних підходи, що випрацьовувались у рамках навчань «Раннє виявлення та пом'якшення наслідків кіберзагроз», а також «Надзвичайні та кризові дії щодо критичних інфраструктур у випадку кіберзагроз». Ці підходи були випрацювані в рамках серії навчань LÜKEX. Зокрема, у межах навчань «Bundessonderlage IT 2009» («Німецька федеральна спеціальна IT-ситуація 2009») та «Eltville 13» члени UP KRITIS змогли інтенсивно відпрацювати критичні сценарії кіберзагроз, визначити потенціал поліпшення, а також розробити рішення для подолання криз у критичних процесах[39].

Наступний напрям – кризовий менеджмент, з якого було проведено дводенні тренінги в Академії управління кризовими ситуаціями, відбулось планування реакції в надзвичайних ситуаціях та цивільного захисту у Федеральній агенції з питань цивільного захисту та ліквідації наслідків стихійних лих (AKNZ (Academy for Crisis Management, Emergency Planning and Civil Protection of the Federal Office of Civil Protection and Disaster Assistance (BBK) з метою посилення та поглиблення співпраці між державним та приватним секторами у конкретних кризових ситуаціях. Дослідження

[39] http://docplayer.net/35662795-Up-kritis-public-private-partnership-for-critical-infrastructure-protection-basis-and-goals.html

потенційних кризових сценаріїв сприяло тому, що задіяні організації змогли розробити спільну думку про можливі IT-кризи та відповідні схеми скоординованої діяльності.

З метою забезпечення кращого національного та міжнародного співробітництва UP KRITIS регулярно інформує національних партнерів про відповідні європейські заходи щодо захисту критичної інфраструктури. Також рішення прийняті членами UP KRITIS були представлені на європейському рівні, таким чином маючи можливість впливати на рішення, прийняті в європейських структурах на ранніх стадіях, посилюючи інтереси UP KRITIS та Німеччини в цілому.

UP KRITIS об'єднує різні структури кризового менеджменту між секторами, а також продовжує розширювати спільні структури та процеси кризових комунікацій. За необхідності створюються додаткові форми комунікації в окремих галузях.

Усі організації, що діють в галузі критичної інфраструктури і мають свої представництва в Німеччині, можуть подати заявку на участь у UP KRITIS. Учасники призначають представників своєї організації, яким надається доступ до інформаційних продуктів UP KRITIS, а також до інформації, наданої Альянсом з питань кібербезпеки, та конфіденційну інформацію про ситуацію та попередження кіберзагроз, що надається Національною агенцією з інформаційної безпеки.

Водночас крім UP KRITIS існують й інші майданчики державно-приватного співробітництва.

Зокрема, **Альянс для кібербезпеки – це ініціатива федерального уряду Німеччини**, у рамках якої основні інформаційно-технологічні компанії, як державні, так і приватні, обмінюються інформацією, створюють та розширюють

базу знань з метою посилення кібербезпеки в Німеччині [40].

Окрім Альянсу, існує ряд інших майданчиків для швидкого обміну інформацією та евентуального реагування вже недержаного типу, який об'єднує бізнес кола в незалежні асоціації. Наприклад, **Рада з питань кібербезпеки Німеччини** – незалежна асоціація з кібербезпеки, що складається з членів приватних організацій-операторів критичної інфраструктури[41]. Рада є політично нейтральною і має на меті консультування компаній, державних органів та політиків щодо посилення кібербезпеки у боротьбі з кіберзлочинністю.

Членами асоціації є великі та середні підприємства, оператори критичної інфраструктури, федеральні землі (наприклад, Північний Рейн-Вестфалія, Нижня Саксонія), муніципалітети (наприклад, місто Франкфурт на Майні), а також експерти та політичні особи, які приймають рішення щодо кібербезпеки. Через своїх членів асоціація налічує близько 3 мільйонів працівників бізнесу та 1,8 мільйонів членів інших об'єднань та асоціацій.

Серед основних цілей діяльності – посилення співпраці між розробниками політики, урядовими структурами, бізнесом та науковими установами для покращення кіберзахисту, впровадження ініціатив та проектів, спрямованих на популяризацію кібербезпеки, створення німецької мережі кібербезпеки в європейському та міжнародному контексті.

ВИСНОВКИ

1. Сфера державно-приватного партнерства в Німеччині у галузі кібербезпеки між операторами критично важливої інфраструктури та відповідними державними органами регулюється планом реалізації UP KRITIS (Umsetzungsplan KRITIS des Nationalen Plans zum Schutz der Informationsinfrastrukturen 2014 р). Основним завданням UP KRITIS є підготовка та реалізація спільних рекомендацій для держави та приватного сектору у сфері

40 http://isalliance.org/cyber-security-counsel-of-germany/
41 http://www.cybersicherheitsrat.de/english/about-us/

кіберзахисту.

2. Водночас UP KRITIS регулярно інформує національних партнерів про відповідні європейські заходи щодо захисту критичної інфраструктури. Рішення, прийняті членами UP KRITIS, представляються на розгляд європейських структур, впливаючи на європейський порядок денний на ранніх стадіях, посилюючи інтереси Німеччини в даному секторі безпеки.

3. Додатково до вищезгаданої національної ініціативи, керуючись Національною стратегією кіберзахисту 2011 р., Федеральна агенція з питань інформаційної безпеки (BSI) має кілька інших структур, зокрема Національний центр кібер-реагування (National CyberAbwehrzentrum, NCAZ BSI), який покликаний забезпечувати кращу координацію дій щодо атак та більш оперативний обмін інформацією між урядом та приватним сектором. NCAZ BSI створює умови усім компетентним органам для оперативного реагуваня на серйозні інциденти, а також проводить аналіз та оцінку небезпек, координує співпрацю з місцевими та галузевими організаціями щодо врегулювання кризових ситуацій.

4. Існують також інші майданчики співпраці, що мають змішане приватно-державне фінансування, на кшталт Альянсу для кібер-безпеки, ініціативи федерального уряду Німеччини, у рамках якої основні гравці, як державні, так і приватні, обмінюються інформацією, створюють та розширюють базу даних з метою посилення кібербезпеки в Німеччині.

5. На даному етапі, незважаючи на значну кількість механізмів, створених в інтересах реалізації ДПП, відповідна система в Німеччині все ще знаходиться на етапі становлення, а значна кількість питань (особливо у сфері ДПП щодо об’єктів критичної інфраструктури) об’єктивно залишається не вирішеними.

РЕКОМЕНДАЦІЇ

1. Суб’єктам національної системи кібербезпеки, на виконання п. 6. ст. 10 Закону України «Про основні засади забезпечення кібербезпеки України» спільно з представниками національної інформаційної індустрії сформувати пул експертів, які можуть залучатися до:

- розслідування кіберінцидентів на об’єкти критичної інфраструктури та подолання наслідків;
- для комунікування інцидентів у засобах масової інформації;
- до програм підвищення кваліфікації співробітників структур національної системи кібербезпеки та для співробітників об’єктів критичної інфраструктури.

Пул експертів може бути сформовано за галузевим принципом із регулярним щорічним переглядом.

2. На виконання пп. 3, п.3. ст. 8 Закону України «Про основні засади забезпечення кібербезпеки України» опрацювати можливість впровадження досвіду Німеччини в частині затвердження суб’єктами національної системи кібербезпеки, які безпосередньо відповідають за питання вироблення та контролю за дотриманням стандартів у цій сфері, для операторів об’єктів критичної інфраструктури тих галузевих стандартів кібербезпеки, що будуть запропоновані самими операторами.

3. Під час процедури формування Планів дій із реалізації Стратегії кібербезпеки України (зокрема тих, які відносяться до пп. 6., п. 4.3 Розділу «Пріоритети та напрями забезпечення кібербезпеки України») врахувати необхідність розширення заходів, спрямованих на реалізацію державно-приватного партнерства. Зокрема, передбачити можливість створення українського аналогу КРІТІС, до функцій та завдань якого мають бути віднесені:

- підготовка реалізації спільних рекомендацій для державного і

приватного сектору у сфері кібербезпеки;

- проведення тренінгів для сторін ДПП;
- взаємодія з міжнародними партнерами та аналогічними структурами;
- кризові комунікації;
- інформування національних партнерів про відповідні європейські структури щодо захисту критичної інфраструктури
- визначення порядку долучення учасників до цієї платформи.

В.О. Бойко
Відділ інформаційної безпеки
та розвитку інформаційного суспільства
Національного інституту стратегічних досліджень