Добржанська О.Л., [*] ***Демцов А.А.*** [**]

КІБЕРБЕЗПЕКА ЯК ФЕНОМЕН МІЖНАРОДНИХ ВІДНОСИН НА ПРИКЛАДІ ФЕДЕРАТИВНОЇ РЕСПУБЛІКИ НІМЕЧЧИНИ

Ця стаття висвітлює поняття, актуальність, загрози кіберпростору; нормативно–правові акти, принципи і цілі стратегії кібербезпеки. В основу статті було покладено нову національну стратегію кібербезпеки ФРН. Аналізуються різні проблеми в кібер–просторі та практичні шляхи їх розв'язання.

Ключові слова: кіберпростір, кібербезпека, інформаційні інфраструктури, інформаційні технології.

Эта статья освещает понятия, актуальность, угрозы киберпространства; нормативно–правовые акты, принципы и цели стратегии кибербезопасности. В основу было положено новую национальную стратегию кибербезопасности ФРГ. Анализируются различные проблемы в киберпространстве и практические пути их решения.

Ключевые слова: киберпространство, кибербезопасность, информационные инфраструктуры, информационные технологии.

This article highlights the concept of relevance, the threat of cyber space, regulations, principles and goals of the strategy of cyber security. The basis was laid new national strategy for cyber–security in Germany. The various issues in cyber space and practical solutions.

Keywords: cyber space, cyber security, information infrastructure, information technology.

Результатом стрімкого розвитку науково технічного прогресу стала глобальна інформатизація та формування кіберпростору, що вплинуло майже на всі сфери людської життєдіяльності та призвело до активних дебатів в соціальних науках. Кіберпростір як нова стадія суспільного розвитку не тільки прискорює цивілізацію та оптимізує міжнародно-політичні процеси, він створює свої теорії, підходи та дисципліни, що досліджують якісно нові механізми соціальної системи породжені віртуальною реальністю.

Сучасні держави залюбки переорієнтовуються на активне використання інформаційно–комунікативні технологій вибудовуючи нову інформаційну інфраструктуру, в свою чергу, стаючи заручниками її надійності. ІТ–продукти і компоненти, що містять помилки; виведення з ладу інформаційної мережі, або «серйозні» атаки в кіберпросторі можуть призвести до значних економічних збитків та спричинити проблеми на рівні адміністративного функціонування будь–якої країни. Тому, доступність, цілісність, автентичність і

[*] кандидат політичних наук, доцент кафедри міжнародної інформації Інституту міжнародних відносин Київського національного університету імені Тараса Шевченка

[**] студент 4 курсу спеціальності «міжнародна інформація» Інституту міжнародних відносин Київського національного університету імені Тараса Шевченка

конфіденційність кіберпростору і даних, що у ньому розташовані, стали життєво–необхідними питаннями XXI–го століття, а забезпечення кібербезпеки – найважливішим колективним завданням для держави, економіки і суспільства в національному і міжнародному контексті [1].

За останні роки спостерігається збільшення кількісних та зростання якісних показників атак на інформаційні інфраструктури; одночасно зростає і їх професіоналізація. Кібератаки походять як з середини країни, так із–за кордону. Доступність і розповсюдження кіберпростору дозволяють проводити завуальовані атаки і при цьому уражені системи використовуються в злочинних цілях як інструменти нападу. Високотехнологічні віруси сильно обмежують можливості захисту і зворотного відслідковування. Зазвичай, при атаках неможливо визначити ні особу ні витоки нападника. Злочинці, терористи і особи контррозвідки використовують кіберпростір як поле своєї діяльності не зупиняючись перед державними кордонами. Також за такими атаками можуть стояти військові операції.

Перш за все, економічно обґрунтована тенденція розвивати і застосовувати інформаційні системи в індустріальних сферах на базі стандартних компонентів пов'язаних з кіберпростором призводить до нових загроз. Досвід з вірусом Stuxnet показав, що важливі промислові галузеві інфраструктури більше не є виключенням цілеспрямованих IT–атак [3].

Отож дослідження цих негативних явищ в кіберпросторі набуває виняткового сенсу, а його наукове висвітлення забезпечує розуміння сукупності перетворень, які відбуваються в глобальній мережі Інтернет.

Мета дослідження полягає у з'ясуванні концептуальних підходів забезпечення безпеки в кіберпросторі, впровадження права і захист найважливіших інформаційних інфраструктур. Ці аспекти потребують активної участі держави як в середині країни, так і у співпраці з міжнародними партнерами. Стратегія кібербезпеки (за рахунок розподілу відповідальності держави, економіки і суспільства) буде успішною лише тоді, коли усі учасники будуть разом дотримуватись своїх відповідних обов'язків. Це ж саме стосується і у міжнародному контексті.

Через глобальне об'єднання в мережу IT–систем можуть виникнути збої в інформаційних структурах інших країн, що опосередковано відобразяться на Україні. Посилення кібер–безпеки потребує впровадження міжнародних правил поведінки, стандартів і норм.

Досягнення мети дослідження можливе лише у поєднанні внутрішньо – і зовнішньополітичних заходів, а також при урегулюванні спірних питань у правовому вимірі. Додатково поняття кібербезпека необхідно уточнювати за допомогою уніфікації нормативно–правових документів по розробці спільних мінімальних правил з учасниками і партнерами. Подолання швидкозростаючої злочинності в кіберпросторі можливе лише у тісній співпраці з правоохоронними органами у всьому світі.

Реалізація завдань здійснюється шляхом впровадження Національної стратегії кібербезпеки задля забезпечення безпеки у кіберпросторі. Внаслідок цього буде досягнуто економічне і суспільне процвітання країни. За важливістю і охороноздатністю кібер–безпека повинна забезпечити мережеві інформаційні інфраструктури на належному рівні, не завдаючи шкоди користувачам кіберпростору. При цьому рівень безпеки кіберпростору дасть в результаті суму всіх національних і міжнародних заходів щодо захисту доступу до інформаційної і комунікаційної техніки, а також єдність, автентичність і конфіденційність даних, що там розташовані.

Кібербезпека може супроводжуватись лише в рамках всеохоплюючого застосування. Це потребує подальшого підвищення інформаційного обміну і координації. На першому місці у стратегії кібербезпеки – цивільне використання і заходи протидії. Вони будуть до-

повнюватись загальнодержавними запобіжними заходами щодо захисту своєї власної дієздатності, і закріплюватись в рамках основоположних мандатів. Враховуючи глобальний характер інформаційно–комунікаційних технологій важливе значення має міжнародна координація точок зору з питань співробітництва у зовнішній політиці і у сфері політики безпеки [2].

За стратегією кібербезпеки ФРН федеральний уряд застосовує заходи на основі вже створених структур до відповідних рівнів загроз за наступними стратегічними напрямками:

1. Захист найважливіших інформаційних інфраструктур. В центрі уваги кібербезпеки лежить захист найважливіших інформаційних структур. Безпека має важливе значення в постійно зростаючих майже всіх найважливіших інфраструктурах. Держава і економіка повинні створити більш точний стратегічний і організаційний базис для посилення інтеграції на основі інтенсивного обміну інформацією [1].

Для того, щоб розбудовувати існуючу співпрацю через впровадження плану CIP необхідно буде перевірити юридичні його зобов'язання. За участі Національної ради кібербезпеки перевірятиметься залучення додаткових галузей і сильніше враховуватиметься запровадження нових актуальних технологій. У подальшому необхідно вияснити, чи слід і в яких випадках необхідно попередньо встановити заходи безпеки, а також необхідні права і в яких випадках при конкретних загрозах. Крім цього буде перевірятись необхідність «гармонізації» управління підтримки у робочому стані найважливіших інформаційних інфраструктур за умов ІТ–криз [3].

2. ІТ–системи безпеки ФРН. Захист інфраструктур потребує більшої надійності ІТ–систем громадян, а також малих та середніх підприємств. Користувачі потребують інформацію, яка відповідала б їхнім потребам і не суперечила сама собі про ризики, які пов'язані з ІТ–системами і самостійно застосовувати заходи безпеки, щодо безпеки свідомої поведінки у кіберпросторі. В рамках спільних ініціатив суспільні групи будуть забезпечуватись цілеспрямованою інформацією і консультаціями. Крім цього, буде перевірено рівень відповідальності провайдерів і докладено всіх зусиль для того, щоб відповідні продукти і сервіси безпеки зі сторони провайдерів для користувачів були доступними у вигляді звичайної пропозиції.

Будуть запроваджені основні функції безпеки у масове використання через цілеспрямоване зацікавлення і стимулювання (наприклад, електронне посвідчення особи або De–Mail), що будуть сертифіковані на рівні держави. Для підтримки малих та середніх підприємств у використанні безпечних ІТ–систем у Федеральному міністерстві економіки і технологій за участі ділових кіл буде створено цільову групу «ІТ–безпека в економіці» [1].

3. Посилення ІТ–безпеки в публічному управлінні. Публічне управління ще сильніше захистить свої ІТ–системи. Державні установи повинні бути зразком відносно захисту даних. Основою електронного обміну даними і вербальної комунікації буде загальна, універсальна і надійна сітьова інфраструктура Федеральної адміністрації («федеральна сіть») [1].

Буде і надалі завзято реалізовуватись існуючий «Федеральний план трансформації» для Федеральної адміністрації. Будь–яке погіршення ситуації в області ІТ–безпеки може бути скоригованим. Ефективна ІТ–безпека потребує сильних організаційних структур у всіх органах влади; тому ресурси повинні використовуватись відповідно централізовано і розосереджено. Для сприяння впровадження повинні передбачуватись довгострокові загальнодержавні інвестиції в ІТ–безпеку, узгоджені з боку влади, в рамках держбюджету.

Буде посилюватись оперативна співпраця з країнами безпосередньо у сфері CERT, при підтримці Ради ІТ–планування [3].

4. Національний центр кіберзахисту. Для оптимізації оперативної співпраці усіх державних установ і покращення координації заходів щодо захисту проти ІТ– випадків було створено Національний центр кіберзахисту. Він працює під керівництвом Федерального відомства з інформаційної безпеки (BSI) і при безпосередній участі Федерального відомства захисту конституції (BfV), а також Федерального відомства з питань захисту населення і допомоги при стихійних лихах (BBK) [3].

Співпраця в Національному центрі кіберзахисту здійснюється у суворій відповідності до законних завдань і компетенції усіх установ, що приймають участь, на основі угод про співпрацю. Федеральне управління кримінальної поліції (BKA), Федеральна поліція (BPol), Митне управління (ZKA), Федеральна служба розвідки і контррозвідки (BND), Збройні сили, а також служби нагляду за користувачами найважливіших інфраструктур взаємно співпрацюють у відповідності до своїх законних завдань і компетенцій.

Швидкий і вузьковідомчий обмін інформацією про вразливі місця ІТ–продуктів, форми нападу і злочинців надасть можливість Національному центру кіберзахисту аналізувати ІТ–випадки і давати узгоджені рекомендації щодо протидії. Для того, щоб захиститись від злочинності і шпіонажу в кіберпросторі, необхідно врахувати належним чином економічні інтереси. При цьому необхідно дотримуватися відповідальності. Кожна задіяна дійова особа відбирає з спільно розробленої національної кібербезпеки охоплені їм заходи, і погоджує їх з компетентними установами, крім того, з економічними і науковими партнерами.

Найбільшої ефективності попереджувальних заходів безпеки можна досягти за допомогою запобігань на ранніх етапах і превентивних дій. Центр кіберзахисту буде надавати Національній раді кібербезпеки регулярні і пов'язані з подіями рекомендації [2].

Якщо ситуація в сфері кібербезпеки досягає масштабів безпосередньо майбутньої кризи чи кризи, що настала, тоді Національний центр кіберзахисту буде підпорядковуватись безпосередньо секретарю Міністерства внутрішніх справ, який очолює штаб по управлінню кризами [1].

5. Національна рада кібербезпеки. Виявлення і усунення конструктивних причин криз – важливий превентивний інструмент у кібербезпеці. Тому буде організована співпраця в рамках федерального уряду, а також між державою і економікою під відповідальністю уповноважених осіб федерального уряду з ІТ–питань і буде створено Національну раду кібербезпеки. Представники – відомство федерального канцлера, а також заступник міністра, департаменти закордонних справ, Міністерство внутрішніх справ, Міністерство оборони, Міністерство економіки і технології, Міністерство юстиції, Міністерство фінансів, Міністерство освіти, а також представники країн.

Представники бізнесу будуть залучатись в якості асоційованих членів. Представники науки будуть задіяні у випадку необхідності. Національна рада кібербезпеки повинна координувати політичне застосування превентивних інструментів у кібербезпеці між державою і економікою. Робота Національної ради кібербезпеки доповнює і з'єднує один з одним завдання Федерації ІТ–управління і Ради ІТ–планування у сфері кібербезпеки на політично–стратегічному рівні [1].

6. Ефективна боротьба зі злочинністю у кіберпросторі. Посилюються можливості правоохоронних органів, Федеральної служби безпеки в сфері ІТ і економіки в контексті подолання ІКТ–злочинності (стосовно захисту від шпіонажу і диверсій).

Проекти по стимулюванню економічно нерозвинених країн–партнерів служать також для подолання кіберзлочинності. Щоб справитися зі зростаючими викликами глобально діючої кіберзлочинності буде проведено всеохоплююче загальне узгодження в області кримінального права на основі конвенції Ради Європи «Про комп'ютерну злочинність». Буде також розглянуто питання про необхідність створення нових договорів у цій сфері на рівні ООН [1].

7. Ефективна співпраця у кібербезпеці в Європі та у світі. Безпека в глобальному кіберпросторі досягається лише за допомогою сукупності узгоджених засобів та методів на національному і міжнародному рівнях.

На рівні Європейського Союзу (ЄС) ФРН буде сприяти відповідним заходам, які складуть в результаті план дій для захисту найважливіших інформаційних інфраструктур. Крім того, ФРН буде сприяти пролонгації і помірному розширенню мандату Європейського агентства з безпеки мереж та інформації (ENISA), приймаючи до уваги зміни загроз в сфері ІКТ, а також об'єднання ІТ–компетенцій в інститути ЄС. Європейська стратегія національної безпеки і цифровий порядок денний стануть вказівками для подальшої діяльності.

Буде сформовано зовнішню кіберполітику таким чином, щоб інтереси Німеччини та ідеї щодо кібербезпеки в міжнародних організаціях, таких як Організація Об'єднаних Націй, ОБСЄ, Рада Європи, ОЕСР та НАТО були узгоджені. Посилений багатосторонній підхід покликаний необхідністю аналізування і прийняття рішень одностайно. Мова також йде про створення можливого числа держав, які підпишуть кодекс державних дій у кіберпросторі, який включатиме посилення заходів щодо безпеки. На рівні G8 ФРН прагне активізувати оборону проти ботнетів.

НАТО – основа трансатлантичної безпеки. НАТО повинна послідовно розглянути кібербезпеку у всьому спектрі її завдань. ФРН схвалює прихильність альянсу на користь єдиних стандартів безпеки, які країни–учасниці можуть в добровільному порядку прийняти для громадянських найважливіших інфраструктур. Це передбачено в новій стратегічній концепції НАТО [4].

8. Використання надійних і достовірних інформаційних технологій. Потрібно забезпечити можливість доступу до надійних ІТ–систем і ІТ–компонентів. Розвиток інноваційних програм захисту для покращення безпеки буде прискорюватись, враховуючи суспільні та економічні аспекти. Тому ФРН буде продовжувати розвивати відповідні дослідження в ІТ–безпеці і найважливіших інфраструктурах.

Крім того, ФРН зміцнить технологічний суверенітет і науковий потенціал по всім стратегічним напрямкам ІТ–діяльності, включаючи політичні стратегії та їх удосконалення. Всюди, де це має сенс, особливо в Європі, ФРН хоче об'єднати свої сили зі своїми партнерами і союзниками. Німеччина виступає за технологічне різноманіття. Мета полягає у використанні компонентів безпеки, які пройшли міжнародну сертифікацію в критично важливих галузях [5].

Підсумовуючи наведені спостереження, можна зробити наступні висновки:

- в ході глобальної інформатизації виникла принципово нове середовище протиборства конкуруючих держав - кіберпростір та сформувались нові фактори міжнародної безпеки. Поява нових загроз породила невідкладну політичну необхідність контролю (управління, врегулювання) кіберпростору та прийняття відповідних юридичних норм як на регіональному так і на глобальному рівнях.
- «Стратегія безпеки кіберпростору ФРН» (Cyber-Sicherheitsstrategie) є своєчасною відповіддю на виклики та загрози сучасного світу, що надасть можливість якщо не запо-

бігання, то принаймні, більш швидкого, узгодженого і компетентного реагування на інциденти у сфері кібербезпеки.

• Уряд Федеративної Республіки Німеччини активно працює задля забезпечення кібербезпеки країни, при цьому намагаючись не втручатися і не обмежувати сферу економічних, інформаційних, освітніх та інших зручних послуг, які німецьке суспільство отримує через мережу Інтернет.

Література

1. Bundesministerium des Innern. Cyber–Sicherheitsstrategie für Deutschland. Februar 2011. [Електронний ресурс] – Режим доступу: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cyber.pdf?__blob=publicationFile
2. Müller Klaus–Rainer: IT–Sicherheit mit System. 3. Auflage. Vieweg, 2008, ISBN 3–8348–0368–5
3. Rosenbach Markel. Nationales Cyber–Abwehrzentrum. Spiegel OnlineNetzwelt, 21 März 2011. [Електронний ресурс] – Режим доступу: http://www.spiegel.de/netzwelt/netzpolitik/0,1518,747140,00.html
4. Tietz Axel, Wiele Johannes: Awareness ist nur ein Anfang. Informationsdienst IT–Grundschutz, Nr. 5/6, S. 28–30, Mai 2009, ISSN 1862–4375
5. Wendzel Steffen, Plötner Johannes: Praxisbuch Netzwerksicherheit. Galileo Computing, 2007, ISBN 978–3–89842–828–6