УДК 343.9: 004.49
DOI https://doi.org/10.32782/2524-0374/2023-9/5

ТРЕТЯ НАЦІОНАЛЬНА СТРАТЕГІЯ КІБЕРБЕЗПЕКИ ВЕЛИКОЇ БРИТАНІЇ: ПОЛІТИКА «НА МАЙБУТНЄ» В ДИНАМІЧНОМУ ТЕХНІЧНОМУ СЕРЕДОВИЩІ

THE THIRD NATIONAL CYBER SECURITY STRATEGY OF GREAT BRITAIN: POLICY "FOR THE FUTURE" IN A DYNAMIC TECHNICAL ENVIRONMENT

Мацелик М.О., к.ю.н., доцент,
доцент кафедри теоретико-правових дисциплін
Навчально-науковий інститут права Державного податкового університету

Санжарова Г.Ф., старший викладач
кафедри романської філології та порівняльно-типологічного мовознавства
Київський університет імені Бориса Грінченка

Санжаров В.А., к.і.н.,
старший викладач кафедри теоретико-правових дисциплін
Навчально-науковий інститут права Державного податкового університету

Стаття присвячена дослідженню особливостей англійської концепції кібербезпеки та її інституційного і законодавчого наповнення. Можна стверджувати, що Сполучене Королівство є однією з провідних цифрових націй світу і має один з найбільш інтегрованих підходів до національної кібербезпеки. Відзначено, що мета кібербезпеки Великобританії полягає в 1) мінімізації серйозних збоїв («захист»); 2) максимізації економічного процвітання і застосуванні наступальної стратегії дій у кіберпросторі («стримування»); 3) збільшенні можливостей просувати себе у світі, поширювати вплив за кордоном і діяти глобально в національних інтересах («розвиток»).

Констатовано, що Сполучене Королівство Великої Британії та Північної Ірландії є однією з провідних економік світу: це, з одного боку, робить країну привабливою мішенню для кіберзлочинців і стратегічних противників, а з другого, – дозволяє залучати значні національні ресурси для розвитку новітніх кібертехнологій. Це актуалізувало розробку надійної протидії викликам динамічного середовища загроз. Способи протидії інформаційним ризикам та кіберзагрозам різних країн формуються по-різному. Автори вважають найхарактернішою рисою концепції кібербезпеки Великої Британії розробку політики орієнтованої «на майбутнє» в динамічному технічному середовищі.

Деякі дослідники вважають, що Велика Британія демонструє прихильність «відкритому та безпечному глобальному Інтернету» саме через те, що це надає їй переваги перед іншими країнами. Це чимось нагадує часи видачі каперських патентів і боротьби за «вільне море». Відзначено, що урядова кібербезпекова політика Великої Британії за останні п'ять років дійсно стала більш інтервенціоналістською, випереджальною, націленою на наступальні дії проти ворожих акторів у кіберпросторі.

Автори вважають безперечним, що Велика Британія відносно добре підготовлена до вирішення широкого спектру сучасних проблем кібербезпеки, незважаючи на існування певних стратегічних викликів (Brexit та російська підривна діяльність). Зроблено висновок, що у Великій Британії створено відповідну екосистему для розвитку та підтримки сектору кібербезпеки, яка задовольняє поточні вимоги національної безпеки, а уряд планує протидію майбутнім загрозам та готується до завчасної імплементації новітніх технологій.

Ключові слова: кіберпростір, кібербезпека, кіберзлочин, кібернетична екосистема, Національна стратегія кібербезпеки, Національний Центр Кібербезпеки.

The article is devoted to the study of the peculiarities of the English concept of cyber security and its institutional and legislative content. The UK is arguably one of the world's leading digital nations and has one of the most integrated approaches to national cyber security. It is noted that the UK's cyber security objective is to 1) minimize serious disruptions ("protection"); 2) maximizing economic prosperity and applying an offensive strategy of actions in cyberspace ("deterrence"); 3) increasing opportunities to promote oneself in the world, spread influence abroad and act globally in national interests ("development").

It has been established that the United Kingdom of Great Britain and Northern Ireland is one of the world's leading economies: on the one hand, this makes the country an attractive target for cybercriminals and strategic adversaries, and on the other, it allows attracting significant national resources for the development of the latest cyber technologies. This actualized the development of a reliable response to the challenges of a dynamic threat environment. Ways of countering information risks and cyber threats in different countries are formed in different ways. The authors believe that the most characteristic feature of the concept of cyber security of Great Britain is the development of a 'future-oriented' policy in a dynamic technical environment.

Some researchers believe that the UK is showing a commitment to an 'open and secure global internet' precisely because it gives it an advantage over other countries. It is somewhat reminiscent of the times of issuing 'lettres of marque' and fighting for the 'free sea'. It is noted that the government's cyber security policy of Great Britain has indeed become more interventionist, anticipatory, aimed at offensive actions against hostile actors in cyberspace over the past five years.

The authors believe that it is indisputable that Great Britain is relatively well prepared to solve a wide range of modern cyber security problems, despite the existence of certain strategic challenges (Brexit and Russian subversive activities). It is concluded that the UK has an appropriate ecosystem for the development and support of a cyber security sector that meets current national security requirements, and that the government plans to counter future threats and prepare for the early implementation of the latest technologies.

Key words: cyberspace, cybersecurity, cybercrime, cyber ecosystem, National cyber security strategy, National Cyber Security Centre.

Актуальність. Оцінка ризиків національної безпеки (NSRA) 2015 року визнала кіберзагрози (кібератаки ворожих держав і широкомасштабної організованої кіберзлочинності) «першим рівнем» (висока ймовірність, високий вплив) ризику для Великобританії протягом п'яти років, поряд із тероризмом, міждержавними війнами, пандемією та стихійними лихами. На думку розробників стратегії кібербезпеки, деякі держави та групи, які мають державну підтримку, регулярно намагаються проникнути в британські мережі, щоб отримати політичні, дипломатичні, технологічні, комерційні та стратегічні переваги, насамперед у державному, оборонному, фінансовому, енергетичному та телекомунікаційному секторах [1, с. 18]. Проте більшість найсерйозніших кіберзлочинів проти Великобританії становлять шахрайство, крадіжка і здирство – менш витончені, але найпоширеніші кіберзлочини проти окремих осіб і невеликих організацій. Обсяги шахрайства у дистанційному банківському обслуговуванні, включа-

ючи шахрайське зняття платежів з банківського рахунку клієнта за допомогою інтернет-банкінгу, збільшилося на 64% і склало 133,5 млн. фунтів у 2015 р. [1, с. 18]. 21 жовтня 2015 р. британський постачальник послуг зв'язку «TalkTalk» повідомив про успішну кібератаку на нього і можливий витік клієнтських даних: компанія «TalkTalk» втратила приблизно 60 млн. фунтів і 95000 клієнтів, а вартість її акцій різко впала [1, с. 20].

Аналіз останніх досліджень і публікацій. Кібербезпекові проблеми стають дедалі актуальнішими для будь-якої з країн світу і, безумовно, потребують правового визначення. Правознаці все частіше звертаються до вивчення досвіду протидії кіберзлочинності як на національному інституційно-законодавчому рівні окремих країн (М. О. Мацелик, О. А. Павлюх, А. Є. Шевченко та інші) [2, с. 219–227; 3, с. 71–73; 4, с. 38–41; 5, с. 151–160; 6, с. 80–82; 7, с. 67–68], так і на міжнародному (В. В. Топчій, О. М. Бодунова та інші) [8, с. 857–860; 9, с. 187–194]. Національна стратегія кібербезпеки Великобританії багато в чому суттєво відрізняється від принципів реагування на кіберзагрози решти країн світу і тому потребує дослідницької уваги.

Мета статті полягає в дослідженні англійської концепції кібербезпеки, її інституційного і законодавчого наповнення, особливостей її планування та реалізації.

Виклад основного матеріалу. Перша національна стратегія кібербезпеки Великобританії (NCSS) була опублікована в 2009 році [10] з наступними ітераціями в 2011 і 2016 роках. Поточна NCSS, розроблена як друга п'ятирічна (2016–2021) і видана у листопаді 2016 року, сформулювала амбітні національні цілі в стратегічній сфері кіберпростору: запровадження змін в використанні інструментів і можливостей боротьби з кіберзлочинністю, щоб розпізнати виклики, пов'язані з новітніми технологіями та діяти на випередження [1, с. 18].

Перша національна стратегія кібербезпеки (NCSS) 2009 року [10] була започаткована разом із урядовою програмою «Цифрової Британії» [11], яка ставила за мету зберегти позиції провідної цифрової економіки та суспільства. Згідно з NCSS-2016, «майбутнє безпеки та процвітання Великої Британії ґрунтується на цифрових засадах». Сполучене Королівство створює більше 10 відсотків свого валового внутрішнього продукту в цифровій економіці, це найвища частка в G-20. Кіберпростір розглядається урядом насамперед як можливість сприяти національному економічному процвітанню за рахунок співпраці трьох головних рушійних сил держави-ринку-технологій. Компанії національного масштабу, наприклад, такі як «BT» і «Nominet UK» (офіційний реєстр доменних імен .uk) на «Форумі управління Інтернетом Великобританії» представляють погляди промисловості та третього сектору державним органам, що розробляють кібербезпекову політику. Таке бачення перспектив було закріплене в «Законі про цифрову економіку» (2017).

Перша Національна стратегія кібербезпеки (NCSS) 2009 року містила короткий розділ, у якому зазначалося, що інструменти кібербезпеки повинні відповідати критеріям необхідності та пропорційності та що «чітка етична основа та належні гарантії використання є важливими для того, щоб не зловживати потужністю цих інструментів» [10]. В наступних «Стратегіях» це твердження більше не зустрічається. Деякі дослідники вважають, що Велика Британія демонструє прихильність «відкритому та безпечному глобальному Інтернету» саме через те, що надає їй переваги перед іншими країнами. Як і багато колишніх імперських держав, Велика Британія підтримує тісні зв'язки зі своїми колишніми колоніями, в даному випадку через керівництво Співдружністю націй. Сполучене Королівство виступає джерелом порад і допомоги для 52 інших країн у цій міжурядовій організації та, відповідно, для 2,5-мільярдного населення, яке в ній проживає. Це дає Великій Британії унікальний доступ до країн на всіх континентах і дозволяє їй формувати кібербезпеку для досягнення власних національних інтересів, особливо після виходу з Європейського Союзу.

У Великобританії жодне державне відомство чи агентство не несе одноосібної відповідальності за кібербезпеку. Кабінет міністрів відповідає за розробку політики кібербезпеки та впровадження Національної програми кібербезпеки, а безпосередньо координвцією дій різних структур займається Управління кібербезпеки та урядової безпеки (CGSD) в його складі. В травні 2013 р. при Міністерстві Оборони було створено «Кібергрупу об'єднаних сил» (JFCyG), наступницю «Групи оборонних кібероперацій», завданням якої є забезпечення операційної переваги в кіберпросторі. Об'єднані кіберпідрозділи в Челтенгемі та Коршамі забезпечують наступальний і оборонний потенціал відповідно. Велика Британія була першою країною у світі, яка визнала розвиток «повного спектру військових кіберпотенціалів». Партнерство з кіберзахисту між Міністерством оборони та промисловістю відпрацьовує захисні технології для ланцюгів оборонного постачання від кіберзагроз. Велика Британія взяла участь в процесі створення «Талліннського посібника» Спільного центру передового досвіду кіберзахисту НАТО, який визначив, що кібервійна регулюється тими ж міжнародними правовими рамками, які формують і обмежують інші види використання військової сили [12]. «Стратегія» закликала забезпечувати готовність НАТО до конфліктів XXI століття, які розгортатимуться і в кіберпросторі, і на полі бою [1, с. 64].

В 2016 році англійський уряд визнав недостатніми масштаби та темп змін у сфері кібербезпеки і залежність від ринку для стимулювання національних інновацій [1, с. 27]. Аби «суттєво трансформувати» кібербезпеку Великої Британії були залучені фінансові інвестиції в розмірі 1,9 мільярда фунтів стерлінгів протягом наступних п'яти років. Кібербезпека є однією з небагатьох сфер, яка отримала додаткове фінансування, коли інші бюджети були скорочені через перегляд витрат і заходи фінансової економії. Відтоді урядова політика відносно кіберпростору стала більш інтервенціоністською, націленою на наступальні дії проти «ворожих акторів» у кіберпросторі. Програма активного кіберзахисту (ACD) зменшила за допомогою автоматизованих засобів кількість і наслідки поширених кіберзагроз у державному секторі. Створення «Національної наступальної кіберпрограми» (NOCP) [1, с. 51] у Міністерстві оборони та британському агентстві сигнальної розвідки (GCHQ) позначає нинішню «Національну стратегію кібербезпеки» (NCSS) як більш «наступальну» за орієнтацією, ніж її оборонно налаштовані попередниці. «Стратегія» відзначає «we have the means to take offensive action in cyberspace, should we choose to do so» («у нас є засоби для наступальних дій у кіберпросторі, якщо ми вирішимо це зробити») [1, с. 25, 51]. Варто відзначити публічне приписування урядом Великобританії програми-вимагача WannaCry Північній Кореї та ряду агресивних кібероперацій російській федерації та заохочування міжнародної спільноти до просування міжнародних норм відповідальної поведінки держав у кіберпросторі і скоординованих відповідей на кіберінциденти в існуючих міжнародних правових рамках.

Підтримці інновацій в сфері кібербезпеки сприяють нові освітні, дослідницькі і навчальні програми [1, с. 55–56], насамперед збільшення до 19 кількості акредитованих академічних центрів передового досвіду з досліджень кібербезпеки (ACE-CSR) в університетах Великобританії.

В Сполученому Королівстві Великої Британії та Північної Ірландії відсутня єдина національна правова база кібербезпеки. Парламент Великої Британії мало безпосередньо бере участь у політиці та стратегії кібербез-

пеки, відповідальність за які лежить на уряді, але відіграє важливу роль у формуванні правового середовища в цій сфері. Велика Британія була однією з перших країн, яка визнала необхідність криміналізації певних комп'ютерних злочинів, що призвело до прийняття «Закону про зловживання комп'ютером» (1990 р.). «Закон про тяжкі злочини» 2015 року визнав незаконним широкий спектр дій з несанкціонованого доступу до даних і комп'ютерних систем. Нещодавні поправки підвищили тарифи за деякі правопорушення, а також криміналізували зловмисні кібер-дії британських громадян за межами території Великобританії. Ухвалений парламентом в 2916 році «Закон про повноваження щодо слідства» (IPA), який прозвали «Хартією шпигунів» (реакція на Едварда Сноудена), розширив повноваження британських спецслужб щодо електронного спостереження. Хоча закон вигідно контрастує із законодавством США про стеження (завдяки більшій прозорості і більшим гарантіям щодо його використання) та практикою розвідувального співтовариства, його сприйняли в суспільстві як наступ на громадянські свободи і дрейф в бік авторитаризму. Проте Великобританія вважає свій уряд радше фасилітатором і гарантом багатостороннього управління, ніж інструментом контролю над глобальним Інтернетом.

Ключовим напрямком законотворчої діяльності є захист даних. Існуюче законодавство включає «Закон про захист даних» (1998 р.) і «Положення про конфіденційність і електронний зв'язок» (2003 р.), які застосовуються до всіх організацій, що обробляють особисту інформацію про живих осіб, із визначенням їхніх обов'язків і покарань за недотримання. Деякі положення були посилені включенням до британського законодавства «Загального регламенту захисту даних Європейського Союзу» (GDPR) у травні 2018 року. Новий «Закон про захист даних» 2018 року посилив систему захисту даних і стимулював покращення кібербезпеки. Сполучене Королівство Великої Британії та Північної Ірландії було і залишається членом більшості організацій та установ, які займаються технічними, регуляторними та політичними аспектами управління Інтернетом з моменту їх заснування. Воно було одним із перших підписантів Конвенції Ради Європи про кіберзлочинність (2001), яка прагне гармонізувати міжнародне законодавство та операції з боротьби з кіберзлочинністю, хоча ратифікувала Конвенцію лише в 2011 році. Поки незрозумілі наслідки виходу Великої Британії з Європейського Союзу в 2019 році щодо контролю за кіберзлочинністю, обміну розвідувальною інформацією про загрози та її участі в роботі Агентства ЄС з мережевої та інформаційної безпеки (ENISA).

Висновки. Основні висновки можна сформулювати наступним чином: 1) у Великій Британії створено відповідну екосистему для розвитку та підтримки сектору кібербезпеки, яка задовольняє поточні вимоги національної безпеки; 2) вплив кіберзлочинності на Сполучене королівство і його економічні інтереси зменшився; 3) уряд планує протидію майбутнім загрозам та готується до завчасної імплементації новітніх технологій; 4) Велика Британія приділяє велику увагу підготовці фахівців з кібербезпеки щоб задовольнити зростаючі потреби все більш цифрової економіки у державному і приватному секторах, а також в обороні; 5) Сполучене Королівство є загальновизнаним світовим лідером у галузі досліджень і розробок у сфері кібербезпеки та постоянно вдосконалює свою кібербезпекову наукову та промислову інфраструктуру; 6) уряд Великої Британії обрав наступальну, випереджаючу стратегію боротьби з кіберзагрозами.

ЛІТЕРАТУРА

1. National cyber security strategy, 2016–2021 URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf (дата звернення: 26.07.2023).
2. Павлюх О.А., Санжарова Г.Ф., Санжаров В.А. Виклики сучасної кібербезпеки: інституційні і правові відповіді Німеччини. *Ірпінський юридичний часопис. Серія: право*. 2023. Вип. 3 (12). С. 219–227.
3. Санжарова Г.Ф., Мацелик М.О., Санжаров В.А. Еволюція стратегії кібербезпеки Німеччини протягом останніх трьох десятиліть: інституційний та правничий виміри. *Наукові тренди постіндустріального суспільства: матеріали IV Міжнародної наукової конференції*, м. Суми, 31 березня 2023 р. Вінниця: Європейська наукова платформа, 2023. С. 71–73.
4. Shevchenko A.E., Pavliukh O.A., Sanzharova G F. Germany's National Legal Framework in the Field of Cyber Security. *International scientific conference «Topical issues of modern jurisprudence»: conference proceedings (April 5–6, 2023. Częstochowa, Republic of Poland)*. Riga, Latvia: Baltija Publishing, 2023. P. 38–41.
5. Колосов О.О. Особливості протидії кіберзлочинам у Сполучених Штатах Америки. *Ірпінський юридичний часопис. Серія: право*. 2023. Вип. 1 (10). С. 151–160.
6. Шевченко А.Є., Павлюх О.А., Санжаров В.А. Питання кібербезпеки в сучасному італійському законодавстві: національний безпековий периметр. *Наукові тренди постіндустріального суспільства: матеріали IV Міжнародної наукової конференції*, м.Суми, 31 березня 2023 р. Вінниця: Європейська наукова платформа, 2023. С. 80–82.
7. Приказюк Н.В., Гуменюк Л.С. Дорожня карта впровадження кібер-страхування в Україні. *Innovation and Sustainability*. 2021. № 1. С. 64–72.
8. Павлюх О.А., Санжарова Г.Ф. Кіберзлочинність: проблеми дослідження та методи правового реагування. *Актуальні питання юридичної науки в дослідженнях молодих вчених: збірник матеріалів Всеукраїнської науково-практичної конференції до Дня науки та 30-річчя Національної академії правових наук України* (м. Київ, 18 травня 2023 р.). Одеса : Видавництво «Юридика», 2023. С. 857–860.
9. Топчій В.В., Бодунова О.М. Система кримінальних правопорушень у сфері інформаційних технологій: міжнародно-правовий вимір. *Ірпінський юридичний часопис. Серія: право*. 2023. Вип. 1 (10). С. 187–194.
10. Cyber security strategy of the United Kingdom: Safety, security and resilience in cyber space. URL: http:/www.cabinetoffice.gov.uk/media/216620/ css0906.pdf (дата звернення: 26.07.2023).
11. Digital Britain: Final report. URL: www.gov.uk/government/uploads/ system/uploads/attachment_data/file/228844/7650.pdf (дата звернення: 26.07.2023).
12. Tallinn manual 2.0 on the international law applicable to cyber operations / ed. M.N. Schmitt. Cambridge: Cambridge University Press, 2017.