УДК 351.865

[https://doi.org/10.52058/2708-7530-2021-2\(8\)-125-136](https://doi.org/10.52058/2708-7530-2021-2(8)-125-136)

Котух Євген Володимирович кандидат технічних наук, доцент кафедри доцент кафедри комп'ютерних наук, Сумський Державний Університет, м. Суми, тел.: (050) 338-26-93, адреса для листування – просп. Московський, 75, кім. 41, м. Харків, 61001, <https://orcid.org/0000-0003-4997-620X>

РЕАЛІЗАЦІЯ НАЦІОНАЛЬНИХ СТРАТЕГІЙ КІБЕРБЕЗПЕКИ: СИЛОВИЙ АСПЕКТ

Анотація. Швидкі темпи технологічного розвитку в галузі інформаційно-комунікаційних технологій призвели до того, що нації та народи стали більш залежними від кіберінфраструктури у своєму житті. Окрім можливостей, широке використання інформаційних технологій спричиняє й загрози критично важливим інфраструктурам та активам, необхідним для функціонування суспільства в цілому та економіки зокрема. Кібербезпека стала однією з найсерйозніших проблем національної безпеки.

У цьому дослідженні стратегії кібербезпеки обрані через їхні специфічні особливості, такі як досвід у розробці кіберстратегій, економічна сила та наявність публікації стратегічного документа. Розглянуто досвід тих країн, які зосередили свою увагу на силовому аспекті кібербезпеки (запобіганні кібератакам на свою уразливу інформаційну інфраструктуру та ключові ресурси для підтримки свого суспільства). Відсутність широко прийнятих методів для оцінки ефективності кіберстратегій свідчить про те, що ця нова ера формування політики в галузі кібербезпеки все ще перебуває на початковому етапі, хоча ще у 2003 р. США першими підготували та опублікували національну стратегію кібербезпеки. За останні десять років 35 інших держав видали свій документ про національну стратегію кібербезпеки.

Широке використання ІТ-систем для особистих цілей та ділових функцій зробило уряди держав залежними від цих систем. Не зважаючи на те, що перші кіберзагрози базувались на жартах і жазі до слави, в останнє десятиліття з'явилися хакери, орієнтовані на прибуток, а років шість як кіберпростір використовується країнами як поле для застосування специфічної військової сили. Для того, щоб впоратися з викликами та ризиками кіберпростору та максимально використати його можливості, країни розглядають кібербезпеку як невід'ємну частину власної національної безпеки.

Ключові слова: кібербезпека, кіберпростір, стратегія, військові кібероперації, розвідка, контррозвідка; кіберзлочинність.

Kotukh Yevhen Volodymyrovych Candidate of Technical Sciences, Associate Professor of Computer Sciences Department, Sumy State University, Sumy, Sumy, tel. : (050) 338-26-93, address for correspondence - Moscow Ave., 75, room. 41, Kharkiv, 61001, <https://orcid.org/0000-0003-4997-620X>

IMPLEMENTATION OF NATIONAL CYBERSECURITY STRATEGIES: THE POWER ASPECT

Abstract. The rapid pace of technological development in the field of information and communication technologies has led to the fact that nations and peoples have become more dependent on cyber infrastructure in their lives. In addition to opportunities, the widespread use of information technology poses a threat to critical infrastructures and assets necessary for the functioning of society in general and the economy in particular. Cybersecurity has become one of the most serious national security issues. In this study, cybersecurity strategies are selected because of their specific features, such as experience in developing cyber strategies, economic strength, and the availability of a strategic document. The experience of those countries that focused on the force aspect of cybersecurity (prevention of cyber attacks on their vulnerable information infrastructure and key resources to support their society) is considered. The lack of widely accepted methods for assessing the effectiveness of cyber strategies suggests that this new era of cybersecurity policy-making is still in its infancy, although in 2003 the United States was the first to prepare and publish a national cybersecurity strategy. Over the past ten years, 35 other countries have issued their National Cyber Security Strategy Paper. The widespread use of IT systems for personal purposes and business functions has made governments dependent on these systems. Although the first cyber threats were based on jokes and the thirst for fame, profit-oriented hackers have emerged in the last decade, and for six years countries have been used as cyberspace as a field for the use of specific military force. In order to meet the challenges and risks of cyberspace and make the most of it, countries view cybersecurity as an integral part of their own national security.

Keywords: cybersecurity, cyberspace, strategy, military cyber operations, intelligence, counterintelligence, cybercrime.

Постановка проблеми. Швидкий поступ комп'ютерних технологій, вкорінення інформаційних та комунікаційних технологій змушує уряди держав та пересічних громадян приділяти все більшу увагу безпеці кіберпростору. Адже

окрім можливостей, що несуть цифрові технології, вони ж спричиняють і нові загрози – для критичної інфраструктури, економіки, суспільства в цілому та окремих його членів, а останнім часом, і для сфери національної безпеки.

Сьогодні близько 50 країн світу вже мають загальнодержавні мережі кібербезпеки, які здатні досить швидко акумулювати сили та засоби публічних органів і приватного сектору для протидії кіберзагрозам, тим самим забезпечуючи кібербезпеку своїх країн.

Аналіз останніх досліджень і публікацій. Проблемам протистоянь у кіберпросторі присвятили свої роботи С. Гейкен та Р. Кларк; на питання аналізу стратегій кібербезпеки звертають увагу Дж. Гілі, А. Клімбург, М. Макміллан. Проте, яке саме місце у сфері кібербезпеки посідає силовий аспект (військова компонента) поки що залишається поза увагою науковців.

Мета статті – дослідження особливостей державних стратегій у царині кібербезпеки з точки зору відображення у них військової компоненти.

Виклад основного матеріалу. Як показує аналіз, стратегії кібербезпеки (в силовому аспекті) більшості держав зосереджують увагу на трьох основних сферах: 1) військові кібероперації; 2) розвідка і контррозвідка; 3) боротьба з кіберзлочинністю. Для того, щоб краще зрозуміти сутність наявних національних стратегій кібербезпеки стосовно зазначених сфер нижче у даному параграфі розглянемо особливості цих стратегій, розроблених у таких країнах як США, Великобританія, Німеччина, Франція, Нідерланди, Індія.

Одночасно з виникненням кіберзагроз протягом останніх десятиліть відбулись фундаментальні зміни у сприйнятті безпеки *військовими силами*. Зростання залежності від інтернет-технологій означає також зростання вразливості мереж і ймовірності атак, спрямованих на об'єкти критичної інфраструктури. Ці зміни змусили керівництва країн переглянути власні підходи до сприйняття загроз та механізми підтримки безпеки для боротьби з кіберзагрозами. Протягом останніх чотирьох років спостерігається тенденція з боку керівних органів до публікації стратегій кібербезпеки, котрі становлять основне джерело інформації про те, як військові сили трактують кіберпростір і як формують стратегії кібербезпеки.

Вага, що надається воєнному підходу до кіберпростору в стратегічних документах, проаналізованих в цьому дослідженні, значно відрізняється в кожній державі. У деяких державах для вирішення головних питань, пов'язаних з кіберпростором, застосовується воєнний підхід, тоді як в деяких інших державах найбільше уваги отримують інші питання, наприклад – боротьба з кіберзлочинністю.

Можна із впевненістю сказати, що у стратегії безпеки кіберпростору США переважає військовий підхід, оскільки влада у Вашингтоні все частіше називає

кіберзагрози проблемою національної безпеки. У Стратегії національної безпеки, опублікованій Білим домом у 2010 р., «масштабні кібератаки» вважають загрозою для США нарівні з тероризмом, стихійними лихами і пандеміями, наголошуючи на їхньому асиметричному характері [1]. Ще одним пунктом, що демонструє сприйняття кіберзагроз розробниками стратегії в США, є внесення цифрової інфраструктури до списку стратегічних активів, що повинні бути захищеними.

«Наша цифрова інфраструктура, таким чином, є національним стратегічним активом, а її захист – так само як захист приватної та цивільної свободи – є одним із пріоритетів національної безпеки» [1, с. 27].

Широкомасштабні кібератаки – не єдиний вимір кіберзагроз. Можливості, що надає інтернет, активно використовують транснаціональні терористичні групи, для яких кіберпростір є середовищем не лише для пропаганди, вербування чи хакерства, але також для викрадання коштів, фінансування терористичних атак та отримання конфіденційної інформації про безпеку. У Стратегії звернено увагу на використання терористами кіберпростору з метою підризу глобальної довіри до міжнародних фінансових систем як на основну складову ланцюга «злочин-тероризм» [1, с. 49].

Для більш детального вивчення воєнного підходу США до кіберпростору варто поглянути ближче на Стратегію кібербезпеки Міністерства оборони США, частина якої була оприлюднена в 2011 р. На самому початку документу вказано, що Міністерство оборони розглядає кіберпростір як операційний простір «для організації, тренування та оснащення» [2]. З цього документа можна зробити висновок, що основною причиною воєнного підходу США до кіберпростору, згідно з яким кіберзагрози вважаються загрозами для національної безпеки, є залежність критичної інфраструктури держави від мереж. Описуючи критичну інфраструктуру США, у Міністерстві оборони виокремлюють п'ять послуг, надавці яких є стратегічно важливими для національної безпеки: енергетика, банківська справа і фінанси, система транспортування, система комунікацій і оборонна промисловість [3]. Важливо зазначити, що об'єкти критичної інфраструктури, визначені Міністерством оборони, контролюються переважно приватним сектором. Оскільки питання підтримки безпеки мереж, що належать приватному сектору, є темою для окремої дискусії, очевидно є необхідність створення нової структурної організації між державою та приватним сектором, що підтримуватиме хиткий баланс між безпекою і конфіденційністю з повагою до ліберальних цінностей.

Хоч в стратегічних документах США не згадується інституційна основа стратегій кібербезпеки, варто відзначити створення у 2010 р. Кіберкомандування США – спеціального підрозділу у складі Стратегічного командування Збройних сил США, що спеціалізується на протидії кіберзагрозам. Створення

Кіберкомандування дало початок ще одній важливій дискусії в контексті стратегії кібербезпеки США: яку позицію займають США з приводу захисту кіберпростору – оборонну чи наступальну?

У сухопутних, військово-повітряних і військово-морських силах можна простежити більш чіткий розподіл між наступальними та оборонними силами. Однак проведення такого ж чіткого розподілу між цими сферами в кіберпросторі є більш складним завданням. Незважаючи на те, що в документах з питань кібербезпеки основним завданням визначено оборону, існують конкретні практики, які вказують на те, що США розглядають саме «активну оборону». Ті, хто вважають, що в основі стратегії кібербезпеки повинен бути наступальний підхід, стверджують, що вища вартість забезпечення стійкості є одним з перших факторів, які повинні мотивувати керівництво держави до вибору наступальних засобів.

За словами Дж. Гілі: «Кібербезпека є надзвичайно дорогою; вона передбачає величезні інвестиції фінансових і людських ресурсів для налаштування організацій, технологій та процесів (навіть базових рис людської поведінки) відповідно до процедур інформаційної безпеки» [4]. Наголошуючи на обов'язковому передбаченні наступальних заходів в стратегії кібербезпеки, Дж. Гілі вказує, що самих лише оборонних заходів недостатньо для підтримки мережевої безпеки: «Наприкінці 1990-х у Міністерстві оборони США чітко визначили оборону одним із пріоритетів, вважаючи, що традиційні військові сили здатні стримати будь-якого потенційного противника без застосування наступального потенціалу. Однак якби власні кіберсистеми Міністерства оборони зазнали вторгнення, усі ці традиційні військові сили залишились би глухими і сліпими» [4].

У стратегічних документах США немає прямих посилань на наступальний потенціал у сфері кібербезпеки, однак на практиці число доказів свідчить про те, що Вашингтон вбачає у військових засобах для підтримки кібербезпеки ефективний стримувальний актив для досягнення зовнішньополітичних цілей. Інцидент з вірусом Stuxnet, незважаючи на відкритість питання його дипломатичної ефективності, показав, що кіберзброя може бути використана для атаки на стратегічні об'єкти. Варто також мати на увазі те, що трансформація американської воєнної стратегії після подій 11 вересня 2001 р. привела до того, що американські лідери обирають превентивні операції, ймовірність чого є також досить високою в умовах кібервійни з ускладненою атрибуцією.

Безсумнівно, США – не єдина держава, що прагне використовувати власний кіберпотенціал для захисту мереж шляхом здійснення наступальних заходів. *Великобританія* є ще однією державою, що висловлюється на підтримку наступальних заходів. Пріоритетом «Стратегії кібербезпеки Великобританії»

визначено боротьбу з кіберзлочинністю, в результаті чого країна має стати найбезпечнішим середовищем для ведення бізнесу (тобто економічно-орієнтований підхід), однак Міністерство оборони Великобританії водночас має у своєму активі наступальні кіберзасоби [5].

З метою покращення стану кібербезпеки у сфері воєнних поставок, Великобританія сформувала Партнерство з питань кібероборони і захисту (Defence Cyber Protection Partnership, DCP) і продовжує зосереджуватись на найкращих практиках, усвідомленні і пропорційних стандартах. У 2015 р. було офіційно запущено модель кібербезпеки для оборони, однак її реалізація затрималась і відбулась у другому кварталі 2016 р. [6]. Для ведення кібервійни було сформовано підрозділ збройних сил під назвою 77-а Бригада (77th Brigade) [6].

Як вказано у звітах, одним із основних кроків Великобританії на шляху до активної кібероборони є співпраця з окремими хакерами, навіть якщо деякі з них були ув'язнені. Стверджується, що держава планує залучити таких комп'ютерних хакерів до створеного нещодавно підрозділу з питань кіберзахисту – Об'єднаної резервної групи з питань кібербезпеки (Joint Cyber Reserve Unit, JCRU), про що уряд Великобританії оголосив у вересні 2012 р. Міністерство оборони розробило ініціативу вартістю 500 млн. фунтів для набору до резерву сотень комп'ютерних експертів для забезпечення оборони держави поряд із з регулярними військовими силами. Діяльність Об'єднаної резервної групи спрямована на зміцнення національної безпеки шляхом захисту комп'ютерних мереж і критичних даних, а також на здійснення превентивних наступальних операцій в кіберпросторі [7].

У свою чергу, на думку представників *Німеччини*, кібератака – це атака на ІТ-систему держави, ціллю якої є доступність, конфіденційність та цілісність інформаційних систем. Німеччина не згадує про воєнний потенціал у своїй стратегії, але водночас працює над завершенням створення спеціального Кіберінформаційного командування з центром кібероперацій, а також Центру з питань кібербезпеки Збройних сил Німеччини (Bundeswehr cyber-security centre) на 13800 працівників [8].

Індія ще не сформувала власне кіберкомандування, але за наказом Кабінету Міністрів (Cabinet Note) формуванням Командування керує Генерал Інтегрованого оборонного штабу (Integrated Defence Staff, IDS) [8]. Станом на сьогодні визначені агентства – Розвідувальне управління Міністерства оборони (англ. Defence Intelligence Agency, DIA) і Національна організація технічних досліджень (National Technical Research Organization, NTRO) – проводять наступальні кібероперації за потребою. У Національній організації технічних досліджень Індії згадується, що одним із компонентів її місії є реакція на кіберзагрози, однак не говориться про захист кіберкордонів шляхом активного

кіберзахисту, як це вказано в документах Великобританії, США і Німеччини. США і Німеччина говорять про кібервійну, натомість Індія окрім кібервійни враховує також ризики, пов'язані з хмарними обчисленнями.

Збір *розвідувальної інформації* в кіберпросторі не вимагає втручання до іноземного територіального суверенітету шляхом відправлення агентів за кордон, агенти, як правило, залишаються у своїх країнах. Оскільки така ситуація не порушує норм міжнародного законодавства, збирання розвідувальної інформації в кіберпросторі рідко викликає занепокоєння у сфері міжнародного права. Більше того, міжнародне право не забороняє країнам шпигувати за кордоном або карати шпигунів на своїй території.

Однак, слід зазначити, що чіткого розподілу між кіберзлочинном, кіберкрадіжкою і кібершпигунством досі немає. Протиріччя також спостерігається в розрізненні військової кіберактивності, кіберзлочинності і кібершпигунства. Що станеться, якщо група хакерів за певної допомоги від держави А здійснить кібероперацію проти комп'ютерних мереж держави Б, спрямовану на заволодіння конфіденційною інформацією про військові таємниці держави Б? Чи такі дії можна вважати кіберзлочинном, за котрий слід карати хакерів, військовою діяльністю чи кібершпигунством?

Не говорячи вже про невизначені сірі зони, кібершпигунство є найбільш небезпечною частиною діяльності, спрямованої проти кібербезпеки, що вражає як приватний, так і публічний сектори. Велика кількість викраденої інтелектуальної власності та пов'язані з цим проблеми спонукали багато організацій вжити додаткових заходів безпеки. Окрім організацій, особливу увагу кібершпигунству приділяють також самі держави, фіксуючи це у планах дій щодо підтримки безпеки. Викрадена інформація є не лише значною втратою в аспекті наукових досліджень і розвитку, але також чинником, що значно підриває довіру до відповідного відомства.

У кіберстратегії *США* немає конкретних згадок про кібершпигунство. Однак право власності, промислове шпигунство, а також захист конфіденційних даних, що належать сфері бізнесу і державі – ці питання розглядаються у відповідних стратегічних документах [2]. Крім цього, стратегія кібербезпеки Міністерства оборони США пов'язує діяльність по боротьбі з кібершпигунством із зусиллями по встановленню особистостей нападників і хакерів. Вирішення складних завдань атрибуції кібератак покладається на особливі підрозділи кіберрозвідки [3].

Міністерство оборони *Великобританії* спільно з Агентствами безпеки та розвідки і Центром урядового зв'язку (Government Communications Headquarters, GCHQ) відіграють головну роль у виявленні кіберзагроз і нівелюванні ризиків, пов'язаних з ними. Кіберстратегії також передбачають певні бюджетні асигнування, виділені для цих агентств. Так, у 2018 році на виявлення кіберзагроз

було заплановано виділити 157 млн. фунтів [6].

Зменшення вразливості до кібершпигунства є одним із перших кроків, до яких вдалось керівництво *Нідерландів*. У Стратегії кібербезпеки цієї держави зазначено, що розвиток технічного потенціалу йтиме поруч з корегуванням правових процедур в аспекті контркіберрозвідки. Стратегія також містить заклик, звернений до публічних організацій, до тісної співпраці з метою протидії кібершпигунству, особливо тому, що виникає з-за кордону [9].

У стратегії кібербезпеки *Німеччини* кібершпигунству надається такої ж ваги як в інших стратегіях. Окрема частина документу присвячена цьому питанню [10].

В *Індії* розвідка і контррозвідка була важливим елементом геополітичної стратегії з найдавніших часів. Тому не дивно, що Індія у своїх стратегічних документах, пов'язаних з кібербезпекою, згадує про глобальну співпрацю між агентствами безпеки різних держав та проводить постійні діалоги для ефективного обміну інформацією.

Кіберзлочинність – вид кримінальної діяльності, що здійснюється за допомогою комп'ютерів чи Інтернету [11]. Як і в багатьох інших сферах кіберпростору, тут бракує чіткого окреслення деталей, яке могло б нас задовольнити. Так, кіберзлочини можна розділити на дві основних групи. Дуже поширеними є злочини, спрямовані на заволодіння персональною інформацією здебільшого з метою крадіжки грошей за допомогою експлойтів і прогаєлів в безпеці. Основна частина злочинів цієї групи зосереджена на ідентичності – крадіжки і фішинг. Зловмисники, за допомогою шкідливого програмного забезпечення, що створює копії усіх натиснень клавіш, можуть отримати паролі та втрутитись у фінансові зв'язки, створюючи проблеми не лише для індивідуальних користувачів, а й для великих компаній.

В інших сферах здійснюються більш поважні злочини – це стосується кібератак з конкретними інституційними цілями, спрямованими на затримку надання послуг державних установ. DDoS/DoS-атаки (розподілені атаки на відмову в обслуговуванні), спрямовані проти адміністративних мереж, можуть також бути спрямованими проти відомств, що є критично важливими для підтримки повсякденного життя людей – транспортна система, енергетика, банківська сфера.

Боротьба з кіберзлочинністю є багатовимірним завданням. Цілями кіберзлочинців є різноманітні мережі – від воєнних до університетських. Кожне відомство має власні проблеми у сфері кібербезпеки, але через брак комплексного підходу в багатьох державах та транснаціональний характер кіберзлочинів, різні відомства вживають власних заходів безпеки для протидії кіберзлочинам. Утім, зі зростанням числа кіберзлочинів, що становить загрозу для національної безпеки, керівники різних публічних організацій розпочали брати участь у спільній

боротьбі з кіберзлочинністю., у тому числі, на міжнародному рівні. І першим міжнародним договором стала Будапештська конвенція про кіберзлочинність (також: Конвенція про кіберзлочинність), ціллю якої є гармонізація національного законодавства, оновлення методів розслідування і розвиток міжнародної співпраці для більш ефективної протидії кіберзлочинності [2]. Крім того, боротьба з кіберзлочинністю є однією зі сфер, що має велику потребу у публічно-приватній співпраці, тому активна підтримка приватних компаній у сфері кібербезпеки зі сторони держави набуває стратегічного значення [8].

Великобританію можна справедливо назвати державою, що докладає багато зусиль для боротьби з кіберзлочинами. Середня сума збитків від кіберзлочинності для великих організацій Великобританії становить у середньому 4,1 млн. фунтів/рік [13]. Тому свого часу для підтримки безпечного бізнес-кіберсередовища керівництво Великобританії виділило 860 млн. фунтів на Національну програму кібербезпеки, яка тривала з квітня 2011 р. по березень 2016 р. [6].

Більше того, першою і головною метою Стратегії кібербезпеки Великобританії є саме підтримка безпеки бізнесу. Для досягнення цього у документі передбачено певні законодавчі поправки, розвиток кіберпотенціалу і нарощення потенціалу правоохоронних органів [5]. Також Стратегія містила три конкретних кроки для розвитку потенціалу кібербезпеки:

- запуск Національного агентства з питань кіберзлочинності – нового органу для боротьби з кіберзлочинністю;
- дотримання плану дій, затвердженого під час Лондонської конференції 2012 року з питань кібербезпеки, для впровадження схваленої міжнародною групою «дорожньої карти» стосовно користування кіберпростором;
- створення єдиної системи звітування для громадян і малого бізнесу для повідомлення про кіберзлочини, так щоб злочинну дію було зафіксовано і правоохоронні органи могли визначити масштаб кіберзлочину (включно з впливом злочину на окремих осіб, організації та економіку в цілому).

Але зрозуміло й те, що самотійна боротьба з кіберзлочинністю не принесе користі жодній державі, так само як боротьба одного солдата проти цілої армії. Гарантія цілковитої кібербезпеки в національному кіберпросторі при існуванні небезпечного глобального кіберпростору є неправдивою обіцянкою.

Саме тому такі держави як Великобританія та США голосно і однозначно говорять про необхідність розробки плану дій для покращення глобальної співпраці і боротьби з кіберзагрозами і тероризмом. У США доклали величезних зусиль для створення міжнародної основи з метою відділення її від стратегій кібербезпеки для запобігання кіберзлочинам. Не зупиняючись на цьому, США також працювали і продовжують працювати над створенням правової системи для пристосування до швидких змін і видозмін кіберзлочинів. Додатково, у Стратегії

кібербезпеки США оголошено про намір вести міжнародну війну проти кіберзлочинності в 2011 р. До речі, загальна сума збитків, завданих американській економіці кіберзлочинами за останні десять років, становить у середньому 15 млрд. дол./рік [13].

Натомість із Стратегії кібербезпеки *Німеччини* можна побачити, що кіберзлочинність не вважається найважливішим питанням, адже боротьба з кіберзлочинністю є однією з десяти цілей, перерахованих наприкінці стратегічного документу. Німеччина прагне найняти кращих спеціалістів до правоохоронних відомств і створити сприятливу платформу для того, щоб Федеральне управління з питань інформаційної безпеки (Federal Office for Information Security) могло діяти спільно з представниками приватного сектору для отримання високих результатів для країни у боротьбі з кіберзагрозами; цим держава показує свій намір виробити ширшу національну перспективу. Одночасно ведеться боротьба з кібершпигунством і робота з використанням отриманих розвідданих. Керівництво Німеччини також виразило готовність тісно співпрацювати з міжнародними структурами, включно з Радою Європи і ООН, зокрема у сфері обміну інформацією [10]. Тому попри всі зусилля та ініціативи, можна із впевненістю сказати, що Німеччина не працює над питанням загроз кіберзлочинності як над одним із пріоритетів кіберстратегії. І це дещо дивно, оскільки Німеччина посідає другу позицію після США за збитками, завданими кіберзлочинністю – у середньому 5,950 млрд. дол./рік за останні десять років [13].

Нідерланди у своїй національній стратегії мають тенденцію до застосування правового підходу. У контексті кіберзлочинності, стратегія Нідерландів стосується в основному розробки сумісних законів, вдосконалення методів розслідування і деяких додаткових аспектів для підтримки попередніх кроків. Розвиток потенціалу правоохоронних органів для боротьби із кіберзлочинністю також входить до переліку заходів, передбачених стратегічним документом [9].

Франція, надаючи меншого значення кіберзлочинності, єдиним засобом для боротьби з нею вважає посилення законодавчих заходів. Стратегія кібербезпеки Франції передбачає також міжнародну співпрацю у сфері протидії кіберзлочинності [14].

Індія суттєво потерпає від шахрайства у сфері інтернет-банкінгу та кредитних карток, наприклад, Індійська комп'ютерна команда з реагування на надзвичайні ситуації (Indian Computer Emergency Readiness Team, CERT-In) повідомила про 49455 інцидентів у сфері кібербезпеки лише за один 2016 р. [8]. У Стратегії кібербезпеки Індії зазначається про ефективні механізми підтримки верховенства права, що впроваджуються законодавчим шляхом, а також про те, що усвідомлення небезпечності кіберзлочинів залишається найкращим засобом їх попередження [13].

Література:

1. The White House (May 2010). *National Security Strategy*. Washington. Retrieved from http://www.whitehouse.gov/sites/default/files/rssviewer/national_security_strategy.pdf
2. The White House, (2011). *International Strategy for Cyberspace, Prosperity, Security, and Openness in a Networked World*. Washington. Retrieved from http://www.whitehouse.gov/sites/default/files/rssviewer/international_strategy_for_cyberspace.pdf
3. US Department of Defense, Department of Defense Strategy for Operating in Cyberspace, July 2011 (2011). Washington. Retrieved from <http://www.defense.gov/news/d20110714cyber.pdf>
4. Healey J, (2012). *Lessons From Our Cyber Past: The First Military Cyber Units* (Washington DC: Atlantic Council). Retrieved from <http://www.acus.org/event/lessons-our-cyber-past-first-military-cyber-units/transcripts>
5. The UK Cabinet Office (2011). *The UK Cyber Security Strategy Protecting and promoting the UK in a digital world*. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf
6. Macmillan Morse, A. (2019). *The UK Cyber Security Strategy: Landscape Review*. National Audit Office, London Oxford University Press.
7. The Guardian (2013). *Ex-hackers could be recruited to UK cyberdefence force*. Retrieved from <http://www.theguardian.com/technology/2013/oct/22/uk-cyber-defence-force-ex-hackers-gcha>
8. Klimburg, A. and Healey, J. (2012). *Strategic Goals & Stakeholders* in Alexander Klimburg (Ed.), *National Cyber Security Framework Manual*, NATO CCD COE Publication, Talinn.
9. Netherlands Ministry of Security and Justice. (2011). *De Nationale Cyber Security Strategie: Slagkracht Door Samenwerking*. Retrieved from <http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2011/02/22/nationale-cyber-security-strategie-slagkracht-door-samenwerking/de-nationale-cyber-security-strategie-definitief.pdf>
10. The Dutch Ministry of Security and Justice (2011). *The National Cyber Security Strategy*. Retrieved from <https://www.enisa.europa.eu/media/news-items/dutch-cyber-security-strategy-2011>
11. Oxford Dictionaries. Retrieved from <http://www.oxforddictionaries.com/definition/english/cybercrime?a=cyber+crime>
12. Council of Europe (2001). *Convention on Cyber Crime*. Retrieved from <http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm>
13. Ponemon Institute (2012). *Cost of Cyber Crime Study: United States* Retrieved from [http://www.ponemon.org/local/upload/file/2012 US Cost of Cyber Crime Study FINAL6%20.pdf](http://www.ponemon.org/local/upload/file/2012%20US%20Cost%20of%20Cyber%20Crime%20Study%20FINAL6%20.pdf)
14. French Network and Information Security Agency, (2011). *Information Systems Defense and Security France's Strategy*. Retrieved from <http://www.ssi.gouv.fr/IMG/pdf/2011-02-15>
15. Discussion Draft of National Cyber Security Policy Version on April 6, 2011 (2011). Department of Information Technology, Ministry of Communications and Information Technology, New Delhi, India. Retrieved from http://www.mit.gov.in/sites/upload_files/dit/files/ncsp_060411.pdf

References:

1. The White House (May 2010). *National Security Strategy*. Washington. Retrieved from

- http://www.whitehouse.gov/sites/default/files/rssviewer/national_security_strategy.pdf
2. The White House, (2011). *International Strategy for Cyberspace, Prosperity, Security, and Openness in a Networked World*. Washington. Retrieved from http://www.whitehouse.gov/sites/default/files/rssviewer/international_strategy_for_cyberspace.pdf
 3. US Department of Defense, Department of Defense Strategy for Operating in Cyberspace, July 2011 (2011). Washington. Retrieved from <http://www.defense.eov/news/d20110714cyber.pdf>
 4. Healey J, (2012). *Lessons From Our Cyber Past: The First Military Cyber Units* (Washington DC: Atlantic Council). Retrieved from <http://www.acus.org/event/lessons-our-cyber-past-first-military-cyber-units/transcripts>
 5. The UK Cabinet Office (2011). *The UK Cyber Security Strategy Protecting and promoting the UK in a digital world*. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf
 6. Macmillan Morse, A. (2019). *The UK Cyber Security Strategy: Landscape Review*. National Audit Office, London Oxford University Press.
 7. The Guardian (2013). *Ex-hackers could be recruited to UK cyberdefence force*. Retrieved from <http://www.theguardian.com/technology/2013/oct/22/uk-cvber-defence-force-ex-hackers-gcha>
 8. Klimburg, A. and Healey, J. (2012). *Strategic Goals & Stakeholders* in Alexander Klimburg (Ed.), *National Cyber Security Framework Manual*, NATO CCD COE Publication, Talinn.
 9. Netherlands Ministry of Security and Justice. (2011). *De Nationale Cyber Security Strategie: Slagkracht Door Samenwerking*. Retrieved from <http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2011/02/22/nationale-cyber-security-strategie-slagkracht-door-samenwerking/de-nationale-cyber-security-strategie-definitief.pdf>
 10. The Dutch Ministry of Security and Justice (2011). *The National Cyber Security Strategy*. Retrieved from <https://www.enisa.europa.eu/media/news-items/dutch-cvber-securitv-strategy-2011>
 11. Oxford Dictionaries. Retrieved from <http://www.oxforddictionaries.com/definition/english/cvbercrime?a=cvber+crime>
 12. Council of Europe (2001). *Convention on Cyber Crime*. Retrieved from <http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm>
 13. Ponemon Institute (2012). *Cost of Cyber Crime Study: United States* Retrieved from [http://www.ponemon.org/local/upload/file/2012 US Cost of Cyber Crime Study FINAL6%20.pdf](http://www.ponemon.org/local/upload/file/2012%20US%20Cost%20of%20Cyber%20Crime%20Study%20FINAL6%20.pdf)
 14. French Network and Information Security Agency, (2011). *Information Systems Defense and Security France's Strategy*. Retrieved from <http://www.ssi.gouv.fr/IMG/pdf/2011-02-15>
 15. Discussion Draft of National Cyber Security Policy Version on April 6, 2011 (2011). Department of Information Technology, Ministry of Communications and Information Technology, New Delhi, India. Retrieved from http://www.mit.gov.in/sites/upload_files/dit/files/ncsp_060411.pdf